Glossar der Informationssicherheit und Netzpolitik

Zum diesem Text

Dies ist (quasi) die alphabetische Version der Inhalte auf meiner Haupt-Webpräsenz: https://sicherheitskultur.at/

Monatliche Nachrichten versende ich im **Newsletter**, zu abonieren auf https://sicherheitskultur.at/contact.htm#newsletter

Autor: Philipp Schaumann

Früher ‚Berater für Informationssicherheit', unterrichtet noch, vor allem Algorithmen-Ethik und andere Themen rund um Nachhaltigkeit. Im Rahmen des C3W.AT (https://c3w.at/) auch an Schulen aktiv (https://c3w.at/schule/).

Anregungen, Fragen und Korrekturen bitte an
philippschaumann (bei) mailbox {punkt} org

Die aktuelle Version steht immer auf https://sicherheitskultur.at/pdfs/Informationssicherheit.pdf

Erstellt unter reichlicher Verwendung von Wikipedia (http://wikipedia.org/) und vielen anderen Quellen.

Ausführlichere Erklärungen zu den Stichworten finden sich auf wikipedia.org, entweder in der deutschen oder der englischen Version

Disclaimer
Das vorliegende Glossar wurde sorgfältig zusammengestellt und soweit möglich aktualisiert. Fehler oder veraltete Informationen sind aber nicht auszuschließen. Der Autor übernimmt deshalb keine Haftung für etwaige Fehler, ist aber für Hinweise dankbar.

Copyright-Hinweis
Das Copyright für diese Zusammenstellung des Materials liegt bei Philipp Schaumann.

Diese Zusammenstellung ist lizensiert unter der Creative Commons Attribution-Noncommercial-Share Alike 2.0 Austria Lizenz. Natürlich gelten auch die Regeln des Fair Use und über Ausnahmen bzgl. der Lizenz kann jederzeit mit dem Autor gesprochen werden

0 day: →Zero Day

19-Zoll Rack: standardisiertes Metallregal mit fester Breite, Tiefe und Einbauelementen, aber variabler Höhe für IT-Geräte (→Server, →Router, →Switches, u.a.). Zumindest Lüftung ist zumeist integriert, manchmal auch Kühlung. Pro Rack gibt es zumeist nur einen →Bildschirm, →Tastatur und →Maus, verbindbar mit jedem →Rechner im Rack über →KVM-Switch. Große →Rechenzentren bestehen aus vielen Gängen die von diesen Racks gebildet werden plus Strom- und Kühlungsluftzuführung. Die US-→Cloud Anbieter haben es geschafft, durch neue Techologien ihre Kosten für das →Hosting drastisch zu senken und können daher standardisierte Rechen-Umgebungen wie →EC2 günstig anbieten. Problematisch ist, dass diese Dienste meist in den USA gehostet werden und mittels →CLOUD Act die US-Firmen immer zur Datenherausgabe gezwungen werden können

2020: 1. Jahr der Covid-19-Pandemie mit vielen Ereignissen in der IT-Welt, z.B. einem Boom von →Webkonferenzsystemen nicht nur für virtuelle Abteilungsmeetings, sondern auch für Events aller Art, z.B. wissenschaftliche Konferenzen, aber auch Dinge wie Yoga Kurse (die die traditionellen →Videokonferenz-Systeme stark in den Hintergrund geschoben haben) und damit verbunden z.B. →Headsets und neue Begriffe wie →Zoom-Bombing. Dazu kam flächendeckend →Home Office (soweit die →Internet-Anbindungen in der Fläche das hergeben <schluchz>). Sehr neu waren auch die angedachten, geforderten oder implementierten →Corona Apps mit ihren eigenen Herausforderungen (z.B. Corona Warn Apps, Tracing Apps, Impf-Apps, e-Immunitätsausweis, e-Kontakt-Tagebuch, Quarantäne-Tagebuch, etc.). Weitere Stichworte für 2020 sind →Solarwinds, →Streaming, →Social Viewing, →Cloud-Gaming, →Smart Trainer mit →Zwift-Anbindung und →Watopia-Landschaften statt Besuch im Fitness-Center. Bei Lockdown Boom von →Webshops auch für eher traditionalle Händler, mit noch stärkerer Dominanz von und riesigen Gewinnen für →Amazon. Bisher nicht erlaubte →Telemedizin wurde (vorläufig) erlaubt. Auch →Bargeld kam 2020 verstärkt in Bedrängnis, ebenso die herkömmliche Kriminalität, die gegenüber →Cybercrime immer mehr in den Hintergrund rutscht, stark im Wachsen weil sehr lukrativ und ungefährlich für die Täter ist →Ransomware gegen Firmen und Behörden, auch in der Kombination mit →Datendiebstahl und Drohung mit der Veröffentlichung der →Daten

23andMe: Unternehmen, das sehr erschwingliche →DNA Analysen anbietet. →Google ist finanziell beteiligt. 2013 verbietet die US FDA dass medizinische Informationen aus der Genanalyse ausgelesen werden dürfen, da

Benutzer auf Grund dieser vagen Wahrscheinlichkeitsaussagen zu unüberlegten Handlungen neigen könnten. 23andMe vermarktet daher ihre Analysen sehr günstig (ab 99$) und ohne Aussagen zu Gesundheitsfragen. Anderseits wird 2014 bekannt, dass das Unternehmen die →Daten der Benutzer (mit deren pauschaler Zustimmung) an Genentech verkauft, die sie für ihre Forschungen nutzen wollen. Wieder ein Beispiel, bei dem die Benutzer nicht die Kunden sind, sondern das Produkt

2D-Barcode: statt den Strichcodes (z.B. bei →EAN) wird hierbei ein flächiges Muster zur Codierung von →Daten verwendet, z.B. →QR-Codes. Siehe →Semacode

2FA: →2-Faktor Authentisierung

2-Faktor Authentisierung: (2FA, auch „starke Authentisierung“) →Authentisierung durch 2 Faktoren. Diese kommen aus den Bereichen „Wissen“ (PIN,Passwort), „Besitz“ (→Smartcard, →Smartphone, →OTP) oder „Eigenschaft“ (→Biometrie). 2-Faktor-Authentisierung ist sicherer als ein einfaches →Passwort da z.B. einfaches Abfangen eines →Passworts (z.B. über →Phishing oder →Keylogging) nicht mehr ausreicht. 2FA wird von →PSD2 für Banken vorgeschrieben. →Angriffe sind aber leider weiterhin möglich (wenn auch etwas aufwendiger für die Angreifer). So führt die →Phishing →Website direkt nach der Eingabe des →Passworts eine automatisiertes →Login bei der Bank durch, triggert dadurch den 2. Faktor (z.B. →SMS) und fragt diesen auch sofort ab

2G: (GSM) 2. Generation der →Handy-Netze ab 1991. Vorteile gegenüber Vorläufergeneration: (leider schwache) →Verschlüsselung der Luftschnittstelle (→A5), bessere Ausnutzung der Frequenzbandbreiten durch digitale Übertragung, neuer Datendienst →SMS. Weiterentwicklungen für schnelleren Datentransfer waren →GPRS (2.5G) und EDGE (2.75G). GPRS hat ein gegenüber GSM verbessertes Sicherheitskonzept. Einige Länder haben ihre 2G-Netze abgeschaltet um die Frequenzen neu nutzen zu können, dort können alte Handys nicht mehr verwendet werden. Siehe →3G, →4G, →5G

2. Kanal: →Out-of-band Kanal

3G: (UMTS) 3. Generation der →Handy-Netze ab 2001 für schnellere Datenübertragung durch spread spectrum Übertragung. →UMTS in Europa, Japan, China, CDMA in USA und Südkorea. Siehe →2G, →4G, →5G

3rd party cookies: →Cookies die von einer anderen als der vom Benutzer besuchten Website stammen, z.B. aus einem Werbeblock der auf der Website geschaltet ist. Diese Cookies werden seit ca. 2016 immer aktiver durch die →Web Browser blockiert und dadurch mehr und mehr durch →Web bugs (Tracking Pixel) ersetzt

3D Drucker: (im Technoslang auch →Maker oder →Fabber genannt) Technologie bei der sog. →Feedstock (Plastik, Kunstharz, Keramik, Metall oder Beton) durch ein Gerät ähnlich zum Inkjet-Drucker in Schichten aufgetragen werden, wodurch bei Nutzung von leicht zu entfernendem Füllmaterial auch komplexe 3-dimensionale Objekte entstehen. Es gibt eine Szene im Internet, in der die notwendigen Dateien zur Steuerung und Quellen für Feedstock publiziert gestellt werden. Als Probleme werden das durch diese Technologie mögliche Umgehen von Gesetzen gesehen, z.B. →Copyright von geschützten Objekten, z.B. Ersatzteilen. In den USA wird auch der Druck von Waffen (der bereits technisch möglich ist) als Problem gesehen. Ein wichtiges Ziel der Entwickler ist der Bau eines „→Replikators“: ein 3D Drucker der sich selbst vervielfältigen kann

3D Face: staatlich gefördertes Projekt zur besseren →Gesichtserkennung. Siehe →Biometrie

3-D Secure: →XML basierendes Protokoll für zusätzliche Sicherheit bei Online-→Kreditkartentransaktionen, implementiert als ‚Verified by Visa’ und ‚MasterCard SecureCode’. Bei Einsatz dieses Verfahrens übernimmt die Kreditkartenorganisation die →Haftung gegenüber dem Händler, der sonst zumeist der Geschädigte ist. Bei der Umsetzung werden jedoch erhebliche Fehler gemacht, so dass neue →Schwachstellen entstanden sind. Siehe →CNP

3P: (pills, porn and poker) Siehe →Spamvertising

419: (419-Scam, Nigeria-Scam) Article 419 im Nigerian Criminal Code behandelt →Betrug. Der Begriff wird für alle Arten von Betrug verwendet, in denen das Opfer ein →E-Mail (früher →Fax) erhält, in dem ein großer Betrag als Anteil an einem mehr oder weniger legalen Geldtransfer versprochen wird. Das Opfer verliert Geld, entweder durch die Zahlung von angeblichen Gebühren oder weil das Opfer Kontonummern, Briefpapier und ähnliches an die Täter sendet, die damit das Konto des Opfers leerräumen

4-Augen-Prinzip: (engl. Dual Control) bzw. Mehr-Augen-Prinzip. Einer der 2 Aspekte von →Segregation of Duty“-Prinzips. Hierbei müssen gewisse Aktionen von 2 oder mehr Personen →autorisiert werden. Ziel ist die Verhinderung von unerwünschtem Verhalten, z.B. →Betrug durch interne Mitarbeiter

4chan: lockere Gruppe rund um eine Bulletin-Board →Website 4chan.org, die durch zumeist unpolitische Aktionen auf sich aufmerksam macht, z.B. die Manipulation der Time 100-Wahlen und anderer Publikumsabstimmungen. Sie sind verantwortlich für Web-„→Memes“ wie LOLcats und andere. Angeblich ist

→Anonymous eine Abspaltung von 4chan. Eine weitere Abspaltung ist →8chan. Wegen problematischen Inhalten kommt es immer wieder vor, dass 4chan keinen →Hoster oder →ISP findet

4G: (LTE, Mobile WiMAX) 4. Generation der →Handy-Netze ab 2009. All-IP packet-switched Technologie. Siehe →2G, →3G, →5G

5G: 5. Generation der →Handy-Netze ab 2020. Ziel ist vor allem Anbindung von IoT-Geräten mit sehr geringer →Latency (Verzögerung) und sehr hohen Übertragungsraten. Kritisch diskutiert werden im Rahmen der 5G-Einführung mögliche Gesundheitsschäden durch ihre elektro-magnetische Strahlung, siehe →Handy-Strahlung. Leider wurden viele der IT-Sicherheitsschwächen der vorigen Generationen aus Kompatibilitätsgründen in den 5G-Standard übernommen. Außerdem wurden einige Sicherheitsfeatures als „optional" eingestuft. Zusätzlich kommt hinzu, dass das →Protokoll extrem komplex ist (und damit anfällig für Programmierfehler). Aus technischen Gründen müssen viele Funktionalitäten sowohl in den base stations implementiert werden wie auch in zentralen Teilen der hierarchischen Infrastruktur. Dies wird über →Virtualisierungen gelöst und bietete weitere Möglichkeiten für Fehler und Schwachstellen. Auch die von den Sicherheitsbehörden (→Law Enforcement Access) gewünschten Schnittstellen zum →Abhören mussten alle implementiert werden. Siehe →2G, →4G, →4G

6-degree of separation: (small world network) Behauptung, dass jeder Mensch mit jedem anderen Menschen über lediglich 6 Verbindungen (hops) verknüpft ist. Die →NSA wertet zu jedem Verdächtigen das Umfeld von bis zu 3 „Hops" aus. Siehe auch Netze-von-Netzen

6to4: Tunneling-Protokoll um →IPv6-Pakete über →IPv4 transportieren zu können. Siehe →Teredo

8chan: Message-board ohne Moderation, nichts wird gelöscht. Seite 2013 Abspaltung von →4chan. Traurige Berühmtheit hat 8chan in 2019 gewonnen, weil dort mehrere rechtsextreme Attentäter, z.B. der Christchurch Mörder u.a. ihre Taten vorher angekündigt, übertragen und gerechtfertigt haben. Die →Website zeigte auch davor und danach immer wieder rechtsradikale Inhalte, Hass-Postings und -kriminalität und Publizität für Attentate. 8chan kam unter Druck, als es mit →dDoS angegriffen wurde und keinen Schutz von →CDN-Firmen wie Cloudflare bekam die gegen solche →Angriffe schützen können. Danach rebranding als 8kun

8. EU-Richtlinie: →EuroSOX

A5: Strom→verschlüsselung, eingesetzt bei →GSM. Es existiert eine Reihe von →Angriffen, allerdings nur für →targeted attacks geeignet. 2013 wird bekannt, dass der britische Geheimdienst für das traditionell eingesetzte Verfahren A5/1 eine sehr kurze Schlüssellänge durchsetzen konnte (64 bit, davon 10 immer Null). Daher kann die →NSA vermutlich alle →GSM Gespräche entschlüsseln. Es soll auf A5/3 umgestellt werden. GSM-Technologie ist zwar eigentlich veraltet, Angreifer mit einem →IMSI-Catcher können aber, sofern das Gerät und Telefonnetz noch GSM unterstützt das Gerät zu GSM „zwingen"

AAA: (authentication, authorization and accounting) →Authentifizierung, →Autorisierung und Abrechnung der vom →Benutzer genutzen Ressourcen. Siehe →Provisioning, →Identity Management, →IAM

AACS: (Advanced Access Content System) →Kopierschutzsystem für hochauflösende →DVDs. Über eine →Blacklist mit „geknackten" Geräte-IDs, die auf jeder solchen HDTV-Video DVD enthalten sein wird, kann nachträglich das Abspielen von DVDs auf diesem Gerätetyp verhindert werden. (Das ältere →CSS konnte nur ganze Gerätetypen sperren.) Zur →Verschlüsselung wird →AES eingesetzt. Jan. 2007 wird von „Cracks" berichtet und das Sperren von WinDVD Player wird erwogen. Siehe →DRM, →ICT

Abhören: unbefugtes Erlangen von →Informationen durch Verletzung der →Vertraulichkeit einer →Datenübertragung (oft durch „Knacken" einer →Verschlüsselung) oder durch Platzierung eines Gerätes zur Aufzeichnung oder Übertragung eines Gespräches, zumeist als →targeted attack. Nur an zentralen Stellen, z.B. Telefondienstanbieter →skalierbar für viele Verbindungen. Siehe →Überwachung, →wiretap, →NARUS, →IP-Hijacking, →Man-in-the-Middle, →TKÜ, →RFS, →A5, →Audio Mining, →Lawful Intercept, →SINA-Box, →ETSI, http://sicherheitskultur.at/abhoeren.htm

Abort: früher bei →Mainframes: (manchmal gewolltes) Ende eines →Programmes (bzw. →Prozesses) in einem →Rechner. Heute wird zumeist →Crash verwendet. Siehe →Absturz

Absender: Ursprung einer →Nachricht. Siehe →Authentizität

Absturz: in der IT: wenn ein →Programm oder das →Betriebssystem entweder „hängt" (d.h. auf keine Eingabe mehr reagiert) oder die Ausführung beendet („abstürzt"), d.h. die Sequenz dieser →Computerbefehle (z.B. eines Programms) ungeplant verlässt. Behebung oft durch →Neustart, entweder nur des „abgestürzten" Programms oder des →Betriebssystems, d.h. in der Regel des Rechners. Siehe →Programmabsturz, →Abort, →Crash

ACAP: (Automated Content Access Protocol) neuer Vorschlag um →Bots von →Suchmaschinen und anderen →Crawlern mitzuteilen, welche Inhalte von →Websites in welcher Form genutzt werden können. Geht über →robots.txt hinaus, da es auch differenzierte

Nutzungsformen wie „Publizieren auf der eigenen Website“ erlauben kann. Dies betrifft →Copyright und →Creative Commons

ACARS: (Aircraft Communications Addressing and Reporting System) Datenprotokoll zwischen Flugzeugen und Bodenstationen. Kaum Sicherheitsfeatures. Die Daten fließen ins FMS (Flight Management System) im Cockpit. 2013 konnten →Verwundbarkeiten gezeigt werden. Auf diese Weise könnte eine Angreifer einen falschen „flight plan“ in das FMS laden. Solche →Angriffe scheinen aber aus dem Entertainment System nicht möglich zu sein. Siehe auch →ADS-B

Acceptance: Zeitpunkt an dem ein System vom Business-Kunden (nicht nur IT) getestet und als voll funktionsfähig akzeptiert wurde. Dies sollte Sicherheitstests mit einschließen. Der Zeitpunkt wird i.d.R. juristische Bedeutung haben, z.B. Eigentumsübergang oder Beginn der Gewährleistung

Access: (engl.) **Zugang** oder **Zutritt** (zu Räumlichkeiten oder Rechnern) oder **Zugriff** (zu Daten oder Anwendungen, Diensten), oft falsch übersetzt. Siehe →ACL, →MAC, →DAC, →RBAC, →Computer crime

Access Control List: →ACL

Access Point: (AP) Gerät in einem →Funk-LAN, zu dem sich die anderen Geräte verbinden. Beim unautorisierten Eindringen in solche Netze wird eine nichtautorisierte Verbindung zu diesem AP hergestellt. Zum Teil als öffentliche APs realisiert, dann →hotspot genannt. Falsche APs können durch Angreifer vorgespielt werden, dann ist ein →Man-in-the-Middle-Angriff möglich. Da →Smartphones mit eingeschaltetem WLAN zu jedem Access Point eine Verbindungsanfrage senden und dabei ihre →MAC-Adresse hinterlassen können alle Access Points die von der Straße aus erreichbar sind für →Tracking verwendet werden. Dies geschieht z.B. aktiv innerhalb von Geschäften und Shopping Centern. Fast alle Access Points verwenden heute eine →Virtualisierung. Dh. dass auf einer →Hardware mehrere logische Netzwerke mit unterschiedlichen →SSIDs implementiert werden können. Dadurch können z.B. Heimnutzer ein getrenntes Netz für Gäste anbieten

Account: (engl. Konto) in der IT der Benutzerzugang zu einem Rechner oder den Diensten eines Providers, z.B. eines Online-Dienstes (Web, →E-Mail, News, →Chat), identifiziert durch eine →Benutzerkennung. In der Regel geschützt durch →PIN oder →Passwort. →AAA, →Privileged Account, →Fake Account

Accountability: Zusammen mit →Vertraulichkeit, →Verfügbarkeit und →Integrität eine der Grundlagen der →Informationssicherheit. Aktionen einer Entität (Person, Computer, etc.) können dieser sicher und eindeutig zugeordnet werden. Siehe auch →Spoofing, →Privileged Account

Account Takover: →Identity Theft

ACE: (Access Control Entry) Eintrag in → Active Directory zur Kontrolle von →Zugriffen

ACH: →Automated Clearing House

ACL: (access control list) Konzept, →Zugriffsrechte zu Objekten (Programme, Hardwarekomponenten, Netze) durch geeignete Regeln zu beschränken. Diese Regeln beinhalten zumeist 2 Aspekte: ***Wer*** darf ***was***, d.h. →Authentisierung und → Autorisierung. Siehe →MAC, →DAC, →RBAC

Acquirer: (acquiring bank) →Kreditkarten

ACS: (Access Control System oder Access Control Server) herstellerspezifische Abkürzung für Geräte oder Systeme zur →Zugriffskontrolle

ACTA: (Anti-Counterfeiting Trade Agreement) internationale Handelsvereinbarung über die Unterstützung beim Vorgehen gegen →Raubkopien. Siehe auch →SOPA, →PRO-IP, →DMCA

ActionScript: →JavaScript-ähnliche Programmiersprache für →Websites, enthalten in →Flash, wirft Sicherheitsprobleme analog zu Javascript auf, kann z.B. auch auf →XHR zugreifen und ist, da enthalten im Flash-Object, schwer automatisiert zu scannen. Kann für →JIT-Spraying ausgenutzt werden

Active Content: Inhalte von →Websites, die entweder interaktiv sind (z.B. Umfragen oder →Opt-in Optionen) oder dynamische Inhalte, z.B. →Java →Applets, →JavaScript (→AJAX), →Flash oder →ActiveX Komponenten. Siehe →ReCoB, →IEController, →chroot

Active Directory: (AD) →Verzeichnisdienst von →Microsoft, wird u.a. für →Authentifizierungen verwendet. Siehe →ADAM

Active Noise Cancellation: (ANC) Feature in →Headsets und Kopfhörern bei der die Außengeräusche aktiv unterdrückt werden indem ein gespiegeltes Signal mit den Außengeräuschen diese aufhebt. Sehr angenehm in öffentlichen Verkehrsmitteln und Flugzeugen. Auch in →Airpods verfügbar

Active Scripting: obsolete →Microsoft Technologie die es erlaubte, im →Webbrowser lokale →Scripts auszuführen, z.B. zur lokalen Überprüfung von Eingabe-Daten. Active Scripting stellte eine potentielle →Verwundbarkeit dar, da auf diese Weise viele →Browserfunktionen ohne Information des Benutzers angesprochen werden konnten. Es konnte zwar im Browser abgeschaltet werden, dann funktionierte aber z.B. beim MS Internet Explorer auch die Anzeige von →PDF-Dateien nicht mehr. Heute durch →.NET Techniken ersetzt. Siehe →ActiveX

ActiveX: obsolete Technologie von →Microsoft basierend auf dem Component Object Model (COM)-Konzept. Dabei entstand leicht transportierbarer Code, der z.B. über →Websites auf Zielrechner geladen und dort ausgeführt wurde. Diese Programme konnten dabei auf alle Rechnerfunktionen zugreifen, kein Schutz durch →Sandbox-Modell wie bei Java →Applet. Siehe auch →killbit http://www.cert.org/reports/activeX_report.pdf

ActivityPub: seit 2018 standardisiertes Protokoll für dezentrales →social networking. Analog zu →SMTP für →E-Mail und →http für →Websites erlaubt dieses Protokoll das Erzeugen, Löschen und Verändern von Inhalten (→Content) auf anderen →Servern über eine einheitliche Schnittstelle. Wichtige Implementierungen sind →Mastodon, →Nextcloud (file hosting), →Peertube (video upload und streaming), →Friendica, →PixelFed (Photo sharing), →Pleroma, →Hubzilla, Funkwhale (eine Alternative zu Soundcloud) und WriteFreely (→Blogging). Siehe auch →Fediverse

Acxiom Corp: US →Daten-Aggregator, bekannt geworden u.a. durch "Verluste" von persönlichen Daten. http://sicherheitskultur.at/privacy_loss.htm#privat

AD: (→Active Directory)

ADAM: (Active Directory Application Mode) Implementierung von →Active Directory, die im User Mode läuft. Umbenannt 2008 nach →AD LDS (Lightweight Directory Services)

Ad-Aware: bekanntes Programm zum überprüfen von Rechnern auf →Malicious Code, z.B. →Spyware und →Adware. Für die Privatnutzung kostenlos erhältlich von http://www.lavasoft.de/support/download/

Adblock Plus: (ADP) →Blocking Tool zur Verhinderung von →Tracking durch →Advertising Networks. Zeigt dem Benutzer an, wer ihn →tracken will, erlaubt gezieltes Blockieren der Tracking Elemente und blockiert im Gegensatz zu →Ghostery auch noch die Werbung selbst

AD FS: (Active Directory Federation Services) →SSO-Komponente für →Windows-→Server die mittels Austausch von software-tokens automatisierte →Authentisierung auch zwischen unterschiedlichen Organisationen erlaubt. Kompatibel mit →SAML. AD FS beruht auf →claims-based authentication

Ad hoc wireless network: Modus bei →WLAN, bei der keine Verbindung zu einem →AP hergestellt wird (Infrastruktur Mode), sondern Geräte direkt untereinander Verbindung aufnehmen. Dies zu erlauben, stellt ein Sicherheitsrisiko dar

Admin Approval Mode: Modus in →Windows Vista, bei der der →Administrator trotz eines →Accounts mit erweiterten Rechten mit Standardrechten arbeitet, z.B. bei →E-Mail oder Surfen und für Aktionen die erweiterte Rechte erfordern in einem →Pop-Up die Nutzung erweiterter Recht explizit bestätigen müssen

Administration: in der IT: Tätigkeiten der →Administratoren

Administrator: Systemverwalter von →EDV-Ressourcen. Hat eine Kontroll- und Wartungsverantwortung für →Netze, Netzkomponenten, →Server, →Client-Systeme, Software-→Programme (→Anwendungen). Fehler, Nachlässigkeit oder böse Absichten bei der Arbeit führen zu →Verwundbarkeiten. Die →Passworte der Administratoren müssen extra sicher geschützt werden und ihre Aktivitäten auf kritischen Systemen sollten zu Audit-Zwecken protokolliert werden. Siehe →Datendiebstahl

Admin-Rechte: etwas schlampiger Begriff für erweiterte Rechte bei →Rechnern, speziell unter MS→Windows. →Schadsoftware nutzt aus, dass viele Benutzeraktivitäten erweiterte Rechte benötigen und daher viele Anwender immer mit erweiterten Rechten arbeiten, auch beim Surfen im →Internet. Auf diese Weise kann →Schadsoftware leicht auf Systembereiche zugreifen. Für die Arbeit der →Administratoren sollen statt der sog. „local admins“ (mit statischen →Passworten die allen Administratoren bekannt sind) sog. „domain admins“ genutzt werden, die personengebunden sind, dieser Person entsprechende Rechte auf vielen →Systemen geben und leicht zentral gesperrt werden können. Siehe →Vista, →Admin Approval Mode

Address-Spoofing: Vorspiegeln einer falschen →IP-Adresse, z.B. weil die vorgespiegelte Adresse für Zugang →autorisiert ist. Wird auch für →dDoS →Angriffe genutzt, wobei die →Packets mit der →IP-Adresse des Opfers gesendet werden und dann mittels →Reflection, z.B. von einem →DNS-Server oder →NTP-Server gegen das Opfer gesendet werden

Adobe: (Adobe Systems) Softwareunternehmen mit Produkten wie Adobe Acrobat (+ kostenlosem →PDF-Reader) oder →Flash, die mittlerweile bei →Verwundbarkeitsstatistiken deutlich vor →Microsoft liegen. 2013 hat Adobe die Zugangsdaten für 150 Mio Benutzeraccounts „verloren“

ADP: →Adblock Plus

Adresse: 1) →IP-Adresse

2) →E-Mail

3) In einigen →Messaging Systemen wird die Telefonnummer als Adresse verwendet

Adressbuch: Sammlung der Daten der Kontakte einer Person in einem →Smartphone oder auf einem →PC. Es wird mehr und mehr üblich, dass →Social Networks jeglicher Form (z.B. auch →Messaging Dienste) den Benutzer

auffordern, sein Adressbuch zum Betreiber zu exportieren, damit dieser die Kontakte des Nutzers ebenfalls anwerben kann (oft im Namen des Nutzers). Dies ist rechtlich sehr problematisch, da der Nutzer nicht das Recht hat, die →personenbezogenen Daten seiner Kontakte weiter zu geben. Siehe auch →Kontakte

ADS: →Active Directory Server

ADS-B: (Automatic Dependent Surveillance-Broadcast) in Verkehrsflugzeugen verwendet, ersetzt Radar indem es Position, Geschwindigkeit und Kennung digital aussendet. Andere Flugzeuge kennen ihre eigene Position auf Grund von →GPS und können sich damit orientieren. Da es keinerlei Sicherheitsfeatures enthält konnte 2013 gezeigt werden, wie das System für Angriffe genutzt werden kann. Dabei kommt →software-defined radio zum Einsatz. Siehe auch →ACARS, →GPS Jammer

ADSL: (Asymmetric Digital Subscriber Line) Modem-Technologie, die es ermöglicht, über Standard-Telefonleitungen Internetanbindungen über eine kurze Entfernung, aber mit hoher Geschwindigkeit anzubieten (bis 6 Mbps) (asymmetrisch, da der „Download" schneller ausgelegt wird als der „Upload"). Speziell im privaten Bereich genutzt. Siehe →DSL, →xDSL

Adversary: (engl. Gegner) Personen, Gruppen oder Organisationen gegen die eine Person, Gruppe oder Organisation sich verteidigen muss. D.h. die Annahme eines bestimmten Gegners, seiner Möglichkeiten und seiner Motivation bestimmt das →Threat Assessment. Beispiel: →Global Adversary. Siehe auch: →Angreifer

Adversial Learning: Untermenge von machine learning in der →AI, bei der es darum geht aus →Angriffen automatisiert Pattern zu erkennen und ebenso automatisiert diese zu Blockieren. Eingesetzt im →Facebook Immune System. Im Gegensatz zum normalen machine learning soll hierbei verhindert werden, dass die „Lehrenden", d.h. die Angreifer, merken, dass sie eine künstliche Intelligenz trainieren. Dabei soll die Lernphase möglichst kurz, die Phase in der der Angreifer merkt, dass sein Angriff erkannt ist, jedoch möglichst lang sein

Ad ID: →Advertising ID

Advertising ID: Datenelement auf →Smartphones auf das alle →Apps immer Zugriff haben und das daher für das →Tracking von Personen eingesetzt werden kann. Auf →iOS können sie ganz entfernt werden. Sie sind auf iOS und →Android als default aktiviert, können durch den Nutzer auf einen neuen Wert gesetzt werden. Danach beginnt aber die Datensammlung aufs Neue. Falls nicht gleichzeitig auch die →Cookies auf dem Gerät gelöscht werden, so wird die alte und die neue Ad ID verknüpft

Advertising Network: Firmen, die auf →Websites für ihre Auftraggeber Werbung schalten und dies heute immer über →behavioural advertising tun, d.h. sie →Tracken das Benutzerverhalten und versuchen die Werbung gezielt nach den vermeintlichen Interessen des Benutzers zu platzieren. Dabei kommt zumeist →Real-time bidding (RTB) und →Data Management Platform (DMP) Software zum Einsatz

Advertising: Das Geschäftsmodell vieler Firmen die im →Internet kostenlose Dienste anbieten, z.B. →Suchmaschinen beruht auf der Platzierung von Werbung auf ihren Seiten. Durch die Auswertung von möglichst genauen persönlichen →Daten einer Person (→data mining) ist →targeted advertising (→behavioural advertising) möglich

Adware: Programme die meist unerwünscht und heimlich auf einem Rechner installiert werden (→Trojaner) und die →Pop-ups oder ähnliche Mechanismen verwenden, um Werbung zu präsentieren. Dies ist zu unterscheiden von →Spyware im engeren Sinne, die Informationen wie →Passworte u.ä. ausspioniert. Aber auch Adware liefert meist Informationen über das Surfverhalten der Benutzer zurück, damit die Reklame gezielter präsentiert werden kann. Siehe →PUP, →Ad-Aware, →EULA

Adwords: →Google Angebot, bei der Werbetreibende Stichworte selektieren, bei deren Suche ihre Anzeige geschaltet wird. Im Augenblick der Suche des Nutzers wird unter allen Werbetreibenden mit diesem Stichwort eine „Auktion" veranstaltet um die Reihung der Anzeigen zu bestimmen. Durch die marktbeherrschende Stellung von Google als →Suchmaschine ergibt sich auch hier eine Marktdominanz. Werbetreibende kommen um Adwords nur schwer herum. Angreifer haben es bereits geschafft, auf diese Weise auch →Malware zu verteilen

AES: (Advanced Encryption Standard) von der US-Regierung durchgeführtes Verfahren zur Auswahl eines standardisierten symmetrischen →Verschlüsselungsalgorithmus. Das ursprüngliche Standard-Verfahren, →DES, ist im Jahr 2002 durch →Rijndael ersetzt worden

Affiliate Network: Begriff aus dem Marketing. Dort stellen Affiliates Händlern Plattformen für Werbung und Vertrieb zur Verfügung. Im →Internet bieten Betrüger ähnliche Dienste an, z.B. die Bewerbung einer →Website oder einer →Smartphone →App. Abhängig vom Bezahlmodell werden von den Affiliates manchmal betrügerische Methoden eingesetzt, z.B. das ungefragte Installieren von vielen →Apps auf einem Gerät in das der Betrüger eindringen konnte, so dass der Affiliate seine Provision bekommt. Anderseits kommt es auch vor, dass ehrliche Affiliates von Betrügern dafür missbraucht werden, →Schadsoftware auf

→Smartphones zu installieren

AFIS: (Automated Fingerprint Identification System) Verfahren zur →Authentifizierung von Personen an Hand von →Fingerabdrücken

AFS: (Andrew File System) Zugriffsmethode auf →Dateien über ein →Netzwerk, Verbesserung zu →NFS, speziell im Hinblick auf Sicherheit und Skalierbarkeit. Siehe →File system

After image: bei →Datenbanken: Speicherung des Zustands nach einer Änderung, genutzt für →forward recovery. Siehe →before image

Agent: Softwareprogramm welches Aufträge annimmt und selbstständig ausführt, heute oft in der Form sog. →Bots im →Internet oder für →Monitoring von →Events

Age verification: (Altersbestimmung) Online nur sehr schwierig möglich. In Österreich für Zigarettenautomaten (>17) implementiert indem auf österreichische →Bankomatkarten eine Altersangabe geschrieben wird. Touristen können daher Zigaretten am Automaten nur mit Hilfe eines erwachsenen Österreichers kaufen. In den USA siehe →COPPA

AGI: (artificial general intelligence) →artificial intelligence

A-GPS: (Assisted GPS) →GPS-Implementierung für →Smartphones und anderen Geräten in Mobilfunknetzen. Es soll die Problematik lösen dass die vollständige Berechnung einer Position ohne „Vorwissen" über die ungefähre Position bei schwächeren →CPUs bis zu 12 Minuten dauern kann. Die Unterstützung kann z.B. so aussehen, dass ein sog. Assistance Server beim Mobilfunk→netzbetreiber dem Gerät die genaue Zeit und auf Grundlage der Koordinaten der Funkzelle eine Liste der Satelliten gibt, die das Gerät „sehen" sollte und die ungefähre Position. Dieser externe Server kann auch Rechenkapazität für die Verarbeitung der (möglicherweise fragmentarischen) Satelliten-Daten der zur Verfügung stellen. Problematisch ist das jedoch, da die Übertragung dieser Informationen unverschlüsselt passiert und z.B. in einem unsicheren →WLAN nicht nur diese Daten abhören und verändern kann, sondern auch das Smartphone so zu konfigurieren, dass in Zukunft alle diese Anfragen über den →Server eines Angreifers geleitet werden

AI: (künstliche Intelligenz, KI) →artificial intelligence

AI Act: → Artificial Intelligence Act

AIR: (Adobe Integrated Runtime) →browserunabhängige →Laufzeitumgebung für →Flash. Kritisiert wird, dass voller Zugriff mit den jeweiligen →Benutzerrechten zum →Dateisystem besteht. Flash ist seit 2020 nicht mehr unterstützt

Airgap: Fehlende Verbindung zwischen 2 Datennetzen um zu verhindern, dass →Schadsoftware oder →Angriffe aus dem einen Netz in das andere propagieren, oft bei →SCADA Systemen eingesetzt. →Stuxnet hat gezeigt, dass z.B.mittels →USB-Sticks solche Angriffe sehr wohl über Airgaps hinweg propagieren können

AirTag: (Apple AirTag) kleines Gerät, das an Objekte (wie z.B. Schlüssel) befestigt werden soll, um diese über das „Find My …" von →iOS und →MacOS geortet werden soll. Der Tag wird mit einem Apple-Gerät „gepairt", d.h. logisch verknüpft. Es enthält eine kleine Batterie und sendet mittels →NFC, →Bluetooth Low Energy und →UWB Signale die von anderen Apple-Geräten (neuer Produktion) verstanden werden. Diese anderen Geräte können das „gepairte" Gerät sein, sofern es in der Nähe des Tags ist, oder auch ein fremdes Apple-Gerät in dem „Find My …" aktiviert ist. Auf diese Weise können auch Tags geortet werden, die nicht in Funknähe des gepairten Apple-Geräts sind. Als problematisch wird gesehen, dass →Stalker (z.B. frühere oder aktuelle Partner) diesen Tag heimlich platzieren können um den Standort des „Opfers" zu erkunden. Ähnliche Geräte gibt es auch von anderen Anbietern (auch für →Android), diese brauchen oder für entfernte Ortung ein anderes Gerät das die →App desselben Hersteller installiert hat. Hier hat →Apple erhebliche Vorteile durch die hohe Verbreitung

AIS: (Account Information Security) Programm von VISA zur Stärkung der Sicherheit von →Kreditkarten. Die Einhaltung von →PCI ist Teil des Programms

AIT: (automatic identification technology) Oberbegriff für Technologien, die eine automatisierte →Identifizierung von Dingen, Menschen (oder Tieren) erlauben, z.B. →Barcodes (→EAN, →Magnetstreifen, →OCR, →RFID, →Biometrie, →Voice recognition)

Ajax: (Asynchronous →JavaScript and XML) Form der Programmierung im →Web, die eine stärkere Interaktivität von →Websites erlaubt, d.h. einen für den Benutzer transparenten Datenaustausch im Hintergrund, z.B. dynamisches Nachladen von Inhalten (→XMLHttpRequest). Ajax ist eine Sammlung von Technologien, z.B. →XHTML, →CSS, JavaScript, →DOM und →XML. Auf Grund der Komplexität von Ajax-Anwendungen und der Kommunikation im Hintergrund ergeben sich neue Möglichkeiten für →Angriffe, z.B. mittels →XSS oder →MITM. Verwundbarkeiten werden entdeckt mittels →Sprajax oder →JSON, die auch bereits aktiv genutzt werden. Daher empfiehlt das →BSI solche →Anwendungen in kritischen Umgebungen nur über →Terminalserverimplementierungen zu nutzen. Siehe →ReCoB, →IEController

Akamai: wichtiges →Content Delivery Network (CDN). Akamai unterhält →Server in vielen

Ländern und hostet den statischen →Content von anderen Anbietern, z.B. →Facebook. So werden statische Inhalte wie z.B. Icons, →Javascript, aber auch Profilbilder von static.facebook.com geladen, das zu Akamai gehört. Dies kann datenschutzrechtlich problematisch sein wenn auf diese Weise datenschutzrechtlich geschützte Inhalte außerhalb der EU gehostet werden ohne dass der Benutzer darüber informiert wurde, bzw. zusgestimmt hat

Akkreditierung: von Prüfstellen ausgestellte Beglaubigung von Fähigkeiten, verbunden mit der Bevollmächtigung, Tätigkeiten bestimmter Art auszuführen, z.B. Berechtigung zur Ausstellung von →Zertifikaten oder für →Audits

Aktienbetrug: im →Internet durch→"pump-and-dump" Aktionen, bei denen über →Spam eine Aktie im Cent-Bereich („penny stock") beworben wird und der Betrüger nach Anstieg des Kurses verkauft, während die anderen, die auch verdienen wollen, noch am Kaufen sind

Alarm: Nachricht, dass ein →Vorfall eingetreten ist, oft automatisch im Rahmen von →Monitoring. Siehe →AoIP

Alarmplan: Teil eines →Notfallplanes, bzw. →Disaster Recovery. Listet die Kontaktdaten (z.B. Telefonnummern) der Personen oder Institutionen, die in einem →Katastrophenfall informiert werden müssen

ALE: (Annualized Loss Expectancy) erwartete Schäden pro Jahr für 1 Schadensereignis: (ARO, Annualized Rate of Occurrence) * (SLE, Single Loss Exposure Value). Die Kosten für die Sicherheitsmaßnahmen sollten die ALO nicht überschreiten. Extrem schwer abzuschätzen und daher kaum sinnvoll nutzbar. Siehe →Risiko, →ROI

Alert: Kommunikation zu einem →Human-in-the-Loop über die Notwendigkeit einer Sicherheitsentscheidung. Dies kann so implementiert werden, dass ohne eine Entscheidung die Anwendung blockiert ist oder auch so dass der Alert auch ignoriert werden kann. Sehr führt ein Alert der →Benutzer zu einer suboptimalen Sicherheitsentscheidung, siehe Browserwarnungen

Alexa: Dienst im →Internet der ein Ranking von Millionen von →Websites nach Besucherzahlen erstellt. Wichtig für Websites, die von Werbung leben

ALG: (→application level gateway)

Algorithmenethik: (kaum zu trennen von →Datenethik) neue Disziplin bei der es darum geht, sicherzustellen, dass Entscheidungen die von Algorithmen getroffen werden zu keiner Verletzung unserer ethischen Normen führt. Seit spätestens 2017 werden viele Vorschläge und Konzepte diskutiert. 2019 hat in Deutschland eine →Datenethikkommission entsprechende Vorschläge unterbreitet die auch als Grundlage für die für 2020 geplante Implementierung einer Regelung auf EU-Ebene dienen könnten. Ursachen solcher Verletzungen können u.a. sein: ungeeigneter →Algorithmus, ungeeignete Trainingsdaten, Trainingsdaten die traditionelle Vorurteile enthalten und an den Algorithmus weitergeben, ungeeignete Wahl der ausgewerteten Variablen, falsches Setzen von Schwellenwerten. Ziel der Algorithemenethik soll sein, dass die Entscheidungen fair sind, ohne Vorurteile, ohne Diskriminierungen. Es muss nachvollziehbar sein, warum der Algorithmus zu seiner Entscheidung kam damit eine Revisionsmöglichkeit durch einen menschlichen Entscheider sinnvoll möglich ist

Algorithmus: Handlungsvorschrift zur Lösung eines Problems, in der IT realisiert in →Programmen →Skripts, o.ä.Fehler oder ungenaue Definitionen führen zu →Schwachstellen. Ebenfalls kann problematisch sein, dass Algorithmen wie der →Google page rank Algorithmus nicht transparent und kontrollierbar sind und weitgehende Auswirkungen im realen Leben haben können, wenn z.B. gewisse →Websites nicht mehr als „relevant" eingestuft werden oder wenn gewiesse Nachrichten von →Facebook dem Benutzer nicht mehr präsentiert werden. Andere problematische Algorithmen werden zur Abschätzung der →Kreditwürdigkeit (oder anderen →Ratings) einer Person eingesetzt. Dies bietet weitgehende Möglichkeiten für Manipulation (http://sicherheitskultur.at/Manipulation.htm). Siehe auch →Shor-Algorithmus, →big data

Alibaba: Riesiger Internetkonzern in China der so wie →Tencent umfassende Services im Web und vor allem auf →Smartphones anbietet. Dabei werden Dienste wie →Social Networks mit →Messaging Apps und Zahlungsdiensten (→Alipay) kombiniert. Die dabei anfallenden Daten der Nutzer werden auch mit der Regierung geteilt, siehe →Social Credit System (SCS)

Alipay: einer der 2 großen Zahlungsdienstanbieter, jetzt im Besitz von →Ant Financial, einem Teil von →Alibaba. Die Alipay App wickelt zusammen mit den Konkurrenten →WeChat Pay einen erheblichen Teil der Zahlungen in China ab.,Alipay expandiert aber auch in andere Länder Asiens, wie auch die Tourismuszentren in Australien, Nordamerika und Europa

Alphabet: Mutterkonzern von →Google

Altersverifikation: im →Internet stellt das Feststellen des wirklichen Alters einer Person eine große Herausforderung dar. Volljährigkeit wird oft über den Besitz einer →Kreditkarte verifiziert, was mit dem Alter nicht viel zu tun hat. Ebenso schwierig ist es, dass in zu schützenden Bereichen, z.B. in →virtuellen Welten spezielle Inseln nur für Kinder in →Second Life keine Erwachsenen sind, die dort Opfer suchen

Altpapier: häufig übersehene →Schwachstelle des Schutzes von →Vertraulichkeit und →Privatsphäre, im beruflichen oder privat. Die Lösung ist konsequentes →Schreddern

AMA: (Advanced Measurement Approach) auch „fortgeschrittener Messansatz“, wird im Bankensektor als ein Instrument zur Messung des →operationellen →Risikos (→OpRisk) im Rahmen von →Basel II genutzt. Dabei werden 3 Elemente genutzt: interne Verlustdaten, externe Verlustdaten, Scenario Analysis („Zukunftsvorhersagen“ durch interne „Experten“ nach Kenntnisnahme der Verlustdaten) und business environment and internal control factors.

Amazon: großer US-Konzern der ursprünglich als online Buchhändler groß wurde, dann aber Angebote vieler anderer Händler übernommen hat und mittlerweile große Teile des Handels weltweit mehr und mehr dominiert (was durchaus als problematisch gesehen wird, auch weil Amazon mittels Steuertricks i.d.R. lokal keine Steuern zahlt – Auslagerung von Gewinnen in Steueroasen wie Irland, Niederlande, Luxemburg. Durch die Suche auf der Amazon-Website fallen riesige Mengen von Daten über die Interessen der Internetnutzer an (selbst wenn der Nutzer dann nicht dort kauft). Amazon ist daher heute einer der big player bei Daten und →Überwachungskapitalismus. Diese Macht wird ergänzt durch die →Amazon Web Services, d.h. riesige →Rechenzentren über die ganze Welt verteilt die auf Grund sehr fortgeschrittener Software und Energie-Management recht kostengünstige →Hosting-Services anbieten und die viele der bekannten Internetservices betreiben.

Mit Amazon Prime mischt die Firma auch im →Streaming Markt (und auch bei Serien in Eigenproduktion) mit und macht nicht nur →Netflix, sondern auch den traditionellen Fernsehsendern starke Konkurrenz

Amazon Echo: der „intelligente“ Lautsprecher (→smart speaker) von →Amazon die über eine →Internet-Verbindung mit den →Servern von →Amazon verbunden sind und dort die Sprachkommandos der Nutzer auswerten und verbale Antworten zurückliefern. Kann für Abfragen, z.B. →Wikipedia und für Bestellungen bei Amazon genutzt werden. Aus Sicht der →Privatsphäre ist dies ähnlich problematisch wie alle diese „smart speaker“ die Gespräche in Wohnungen auswerten

Amazon Ring: in Europa wohl nicht verfügbare „smarte“ Türklingel, die mittels einer →Kamera die Umgebung vor der Tür filmt und mittels der →App Neighbors auch mit anderen (und üblicherweise auch mit der lokalen Polizeit teil, diese hat oft direkten →Zugriff auf alle diese Geräte. Das Gerät hat einen gewissen Gruselfaktor und ist wohl mit den europäischen →Datenschutz-Vorstellungen nicht ganz kompatibel

Amazon Web Services: (AWS) →EC2

Amplification: (engl. für Verstärkung) wird für →dDoS-→Angriffe eingesetzt, indem ein Protokoll ausgenutzt wird, bei dem auf eine kurze Anfrage eine lange Antwort gesendet wird. Beispiele sind →DNS Amplification oder das →NTP →Protokoll. Dabei werden bei manchen Protokollen Verstärkungen von bis zu 1000 erreicht. Siehe →DNS Amplification

AMR: (Automatic Meter Reading) vor allem in den USA eingesetzte Technolgie bei der analoge Gas-, Wasser- oder Stromzähler so umgerüstet werden, dass der Zähler über eine drahtlose Verbindung seinen Zählerstand in kurzen Abständen überträgt. Zum Ablesen fährt jemand in die Nachbarschaft und kann automatisiert alle Geräte im Umkreis zwischen 300 und 700 Metern ablesen. Diese Verbindungen sind unverschlüsselt und können leicht mittels →USRP abgehört werden. Auf diese Weise können auch Diebe festgestellen welche Häuser gerade unbewohnt sind. Dies ist eine Privatsphäreverletzung. Siehe auch →Smart Meter

AMT: (Active Management Technology) Intel-Entwicklung für Zwecke der Fernwartung von →PCs. Ist in Chipsätzen integriert und erlaubt einen →Zugriff auf Geräte, manchmal auch in ausgeschaltetem Zustand. Entspricht von der Funktionalität her →BMC. Erlaubt →KVM-Zugriffe und auch Anti-Diebstahl Funktionalitäten wie Remote-→Wipe wie sie auch bei →iOS und →Android geboten werden

ANC: →Active Noise Cancellation

Android: →Betriebssystem für mobile Geräte (→Smartphones, →Tabletts) von →Google. Wird als →Quellcode zur Verfügung gestellt und von Handy-→Netzbetreibern angepasst. Dies führt dazu, dass →Sicherheitsupdates oft nur sehr verspätet, oder auf Grund der Marktfragmentierung nie- 2014 waren 19000 Varianten im Einsatz) zur Verfügung stehen (→Obsoleszenz) (im Gegensatz zu →iOS und →Windows Phone 7). Daraus resultiert eine erhebliche Unsicherheit; eine weitere sind die vielen alternativen →Markets für →Apps, die dazu führen, dass 2011 ca. 50000 Malware-Apps (bzw. Versionen von →Malware) pro Tag berichtet werden. Positiv ist, dass bei →Android (und Windows 8 →Metro) jede →App in einem eigenen →User Account ausgeführt wird. 2015 zeigt eine Studie, dass auf Grund der fehlenden Sicherheitspatches für die meisten Modelle, über 80% aller Geräte ständig eingreifbar sind. Siehe →NAND lock, →Google Play, →Bouncer, →Rooting

Angreifer: Personen oder Organisationen, die einen →Angriff durchführen. Wichtige Gruppen sind: Kriminelle, →Industriespione, rogue →Hacker, →Malware Entwickler, →Hacktivisten, Saboteure, Cyberkrieger. Ca. 50% sind interne Angreifer. Siehe auch →Adversary,

http://sicherheitskultur.at/Angreifer_im_Internet.htm

Angriff: Versuch der Verletzung der →Informationssicherheit, d.h. der →Vertraulichkeit, der → Integrität oder der →Verfügbarkeit von Informationen, z.B. durch →DoS. Angriffe können aktiv sein, z.B. durch →Port Scan und Eindringen durch Ausnutzen von →Verwundbarkeiten, oder passiv, z.B. durch →Lauschangriff auf Gespräche oder →Datenübertragungen. Siehe →Attack Signature, →Targeted Attacks, →Cyberwar, →Hactivism, →Reflector Attack, →skalierbar, →survival time, →Watering Hole Attack

Angriffsfläche: die Summe der möglichen Angriffswege/Angriffsmöglichkeiten für einen →Angreifer. Die Angriffsfläche vergrößert sich z.B. drastisch, wenn eine Funktionalität im → Internet, statt im internen Firmennetz erreichbar ist. Zur Reduzierung von Angriffsflächen wird z.B. eine →Firewall eingesetzt, die die Angriffsmöglichkeiten auf die →Ports einschränkt, die in der Firewall frei gegeben sind. Andere Beispiele für reduzierte Angriffsflächen sind reduzierte Funktionalitäten, Verbot von →Datei Upload. Das Beheben von →Verwundbarkeiten gehört nicht zur Reduzierung der Angriffsfläche, sondern soll sicherstellen, dass die gewünschten Funktionalitäten sicher implementiert sind

angularJS: Programmbibliothek die von →Google entwickelt und gepflegt wird und für →JavaScript-Programmierung verwendet wird. Sie dient vor allem zur →Programmierung von single-page →Webseiten, d.h. zur Manipulation des →DOMs

Anhang: (engl. →Attachment)

AN.ON: →JAP, →Mix

Anonymer Remailer: im →Internet verfügbarer →E-Mail-Dienst, der als Mailknoten E-Mails weiterleitet, nachdem er vorher die Absenderinformationen entfernt. Wenn der Empfänger an den Remailer antwortet, so setzt dieser wieder die Originalinformationen ein und kann das E-Mail an den Versender weiterleiten. Über eine Beschlagnahme der dafür verwendeten →Datenbank können Polizeistellen die →Anonymität aufheben

Anonymisierer: Verfahren die dem Internet-Nutzer Anonymität verschaffen und →Data Mining oder →Consumer Profiling behindern sollen. Bevor eine Anfrage an den →Webserver weitergeschickt wird, ersetzt der Anonymisierer (→Proxy Server) die →IP-Adresse des Benutzers und filtert evtl. auch. →Cookies aus dem Datenstrom. Allerdings gibt es auch bei der Nutzung dieser Dienste keine wirklich sichere Anonymität, denn diese Dienste verschleiern ja nur die →IP-Adresse, andere Profilisierungstools wie →Cookies, aber auch die Profilierung des Geräts selbst (und seiner Software-Versionen) ist immer noch möglich. Siehe →Mix, →JAP, →TOR

Anonymisierung: Vorgang, bei der aus →Daten alle die Elemente entfernt werden, die die Zuordnung dieser Daten zu 1 Person ermöglichen, wie Name, Anschrift, Telefonnummer, etc. Ob diese Daten danach wirklich anonym sind, hängt davon ob, wie groß die Menge der durch die verbleibenden Daten beschriebenen Personen dann immer noch ist. Denn wenn z.B. Geschlecht, Altersgrupp und Postleitzahl erhalten bleiben, so kann bei kleinen Orten immer noch die Person gefunden werden. Dieser Vorgang wird unter →De-Anonymisierung beschrieben. Sehr oft findet aber statt Anonymisierung eine →Pseudonymisierung statt, die noch leichter aufzuheben ist. →Zero-Click Angriff, →Zero-Day Exploit

Anonymisierungsdienste: technologische Angebote die eine Rückverfolgung von →IP-Adressen sehr schwierig machen. Dazu gehört z.B. →TOR, aber auch verschiedene →VPN-Anbieter. Diese Dienste werden legitim eingesetzt um politischer Verfolgung zu entgehen aber auch illegitim um Verbrechen zu begehen

Anonymität: in der IT die Möglichkeit eines →Benutzers, Information und Beratung ohne Preisgabe seiner →Identität zu erhalten. In der Informations- und Kommunikationstechnik geht es hierbei auch um die Verschleierung von Aufenthaltsorten oder Kommunikationsbeziehungen von Benutzern. Die Anonymität geht durch moderne Technologien immer stärker verloren, auch das →Internet erlaubt kein wirklich anonymes Arbeiten. Siehe →IP Traceback, →Privatsphäre, →Anonymisierer, →Pseudonymisierung, →Pseudonymität, →De-personalization, →Kundenkarte, →De-anonymisierung, →Device Fingerprint, →TOR http://sicherheitskultur.at/anonymity.htm

Anonymous: aus →4chan hervorgegangene →Hacktivismus-Gruppierung die durch die Aktionen rund um →WikiLeaks bekannt wurde und ihre Aktivitäten im Gegensatz zu →4chan politisch sieht. Sie schrecken jedoch auch nicht vor Aktionen zurück, die unter →Cybercrime subsummiert werden, z.B. →DoS, Eindringen in →Websites, →Datendiebstahl, etc. Bekannt wurde der →Angriff auf →HBGary Federal

ANPR: (automatic number plate recognition) automatisches Erkennen von Nummernschildern von vorbeifahrenden Autos. Für Geschwindigkeitskontrolle und Überwachungen verwendet. Wird in Ö auch für die Implementierung der PKW-Maut auf Autobahnen genutzt, in anderen Ländern auch für andere Mautstraßen oder Mautbrücken. Siehe →Section Control, →ENLETS, →Tracking

ANSI (American National Standards Institute): US-amerikanische Standardisierungsbehörde, 1918 gegründet. Siehe →DIN, →öNorm

Ant Financial: Teil von →Alibaba Group, früher bekannt als →Alipay

Antivirus-Programm: →Malware-Schutz

Anweisung: (engl. →instruction) →Programmcode

Anwender: →Benutzer

Anwendungsprogramm: →Programm zur Bearbeitung der Anwenderproblemstellungen (im Gegensatz zur Systemsoftware →Betriebssystem)

AoIP: (Alarm-over-IP) Übertragung von →Alarm-Nachrichten über →IP-Verbindungen womit sehr einfach die ständige →Verfügbarkeit der Verbindung geprüft werden kann und auch sehr leicht differenzierte Detailinformationen mitgegeben werden können

AP: →Access Point

APACS: (Association for Payment Clearing Services) UK-Organisation für Banken, →Kreditkarten-Unternehmen, etc. Kümmert sich auch um Sicherheitsfragen. Siehe →PISCE, →ISAC

API: (Application Programming Interface) Schnittstelle, über die ein →Programm Dienste oder →Daten von einem anderen Programm anfordern kann, z.B. →MAPI für →E-Mail, →Open Social, etc. Solche Interfaces können entweder lokal auf 1 →Rechner interagieren, oder auch über →Netzwerke wie das →Internet (→TCP/IP) mit kompatiblen Komponenten kommunizieren. Siehe auch →Middleware

APN: → Apple Push Notification

App:
a) Software Applikation (→Programm) für →Smartphones. Diese können sehr leicht Sicherheitsprobleme darstellen, da sie auf persönliche Daten (wie Telefonbuch), interne →Sensoren wie →GPS, und auf mehrere Drahtlos-Netzwerke zugreifen können und dabei leicht die →Privatsphäre verletzt werden kann. Apps werden oft aus →app stores geladen und zumeist in →Sandboxes ausgeführt. Solche Sandboxen sind weitgehend wirkungslos falls das Gerät einem →Jail-break, bzw. →Rooting unterzogen wurde. . Siehe →user permission fatigue

Apps werden oft über →Affiliate Networks beworben oder verteilt, von denen manche mit betrügerischen Methoden arbeiten und versuchen, auf den Geräten auch ungefragt Software zu installieren, bzw. sogar das Gerät zu rooten.

Des Weiteren sind →Man-in-the-Middle Angriffe leicht möglich, da die Benutzer einer App das →Zertifikat der →Website von der die Daten geladen werden, nicht überprüfen kann (falls überhaupt →HTTPS eingesetzt wird)

b) →Programme die in →Social Networks angeboten werden und im Context des →Benutzers ablaufen. Der Benutzer muss einmal zustimmen, dann haben solche Apps →Zugriff auf fast alle →Profildaten des Benutzers

AppArmor: →LSM-basierte Sicherheitserweiterung für →Linux, bei der für einzelne →Programme →Zugriffsrechte differenziert definiert werden können

Apple: Computerfirma mit einem alternativen Konzept zum →Windows-→PC, gegründet in den 70iger Jahren, bekannt für innovative Konzepte und den Ruf einer einfachen Benutzbarkeit. Auf Grund eines deutlich höheren Preises und einer geschlossenen Architektur im Vergleich zum PC geringere Marktanteile, dadurch früher gegenüber dem PC auch weniger angegriffen durch →Malware. Dies wird aktuell durch ihr recht geschlossenes System, automatisierte Updates und Malware-Schutz auszugleichen. Wichtig für Apple ist der hohe Marktanteil bei →Smartphones (iPhone, →iOS) und →Tablets (→iPad). Siehe auch →AirTag

Apple Pay: drahtloses Zahlungssystem auf →NFC Basis (Apple gibt im Gegensatz zu →Google und →Android die NFC Schnittstelle nicht für →Apps frei und verhindert damit alternative Zahlungslösung auf →iOS Geräten). Dabei erfährt der Händler nichts über die Bankverbindung des Kunden, da für die Zahlungsauslösung nicht die →Kredit-, →Debit- oder →Bankomatkarte des Kunden genutzt wird, sondern eine „tokenised“ Karte die während des sog. →Enrollment erzeugt wurde. Selbst wenn die selbe Karte auf einem anderen Gerät noch mal genutzt wird so wird eine neue Kartennummer erzeugt. Apple und die Bank erfahren den Namen des Händlers, Datum, Uhrzeit und Betrag. App verspricht, diese →Daten nicht zu sammeln oder auszuwerten. Apple Pay erfüllt die Anforderungen der →2 Faktor Authentisierung des →PSD2. Durch das Enrollment wird der Besitz des Geräts als 1 Faktor gerechnet. Ein 2. Faktor entsteht wenn der Nutzer das Gerät vor der Nutzung entsperren muss, entweder über →PIN, d.h. Wissen oder →Biometrie, d.h. „sein“

Apple Push Notification: (APN) Dienst von Apple für die →iOS-Systeme. Um trotz fehlendem Multitasking trotzdem →Apps „aufwecken“ zu können (die nicht im foreground laufen) hat →Apple diesen Service entwickelt. Dabei wird jeder App bei der Installation eine eindeutige ID vergeben, über diese kann dann ein →Server Nachrichten an diese App (die sich für diesen Dienst registriert hat) schicken. Implementiert wird dies, indem der Server der die Nachrichten verschicken will einen zentralen Apple-Server anspricht, der die Nachricht dann an das →iPhone weiterleitet, wodurch dann diese App in den foreground kommt. Die Funktionalität wurde später auch für →MacOS angeboten. Siehe →Google Cloud Messaging (GCM)

Applet: in Java geschriebenes kleines Programm, i.d.Regel von einer →Website geladen und am Zielrechner innerhalb des →Webbrowsers ausgeführt. Auf Grund des →Sandbox-Modell hat dieses Programm nur eingeschränkten Zugriff zu den Funktionen des Zielrechners. Trotzdem kam es im Laufe von 2012 und 2013 zu zahlreichen →Verwundbarkeiten bei →Java Code (JRE, →Java Runtime Environment) die für →Angriffe genutzt wurden. Siehe auch →Flash, →Quicktime, →Silverlight

Appliance: (engl. Gerät, Vorrichtung) bezeichnet ein Gerät, bei der vom Hersteller Hardware und Software bereits integriert wurden. Solche Appliances zeichnen sich in der Regel durch leichtere Administration aus. Häufige Verwendung als →Firewall

Application Level gateway: (ALG) Absicherung einer Anwendung durch eine Komponente, die den spezifischen →Datenverkehr einer →Anwendung versteht und kontrollieren kann. Erlaubt komplizierte →NAT- und →Port-Zuweisungen, z.B. für →SIP, RTSP (Real-time Streaming Protocol) und eine detaillierte Analyse der Eingaben für die Anwendung. Im Gegensatz zum →Proxy für die Anwendung transparent. Ein Beispiel ist →Web Application Firewall

Application Security: Konzepte zur Absicherung von →Anwendungen gegen →Angriffe, speziell auch aus dem →Internet, hauptsächlich durch das Finden von →Schwachstellen in der Software. Siehe →Business Logic Flaw, →OWASP, →FireBug, →Fuzzing, →WebInspect, →Network Security, →Desktop Security

App store: →Website mit dem Angebot von Anwendungen (applications, heute, →Apps) für einen bestimmten Typ von →Smartphone. Beispiele sind →Google Play für →Android Apps, iTunes App Store für →iOS Apps und Mac App Store für →MacOS Systeme. Einige Hersteller unterziehen diese Apps mehr oder weniger gründlichen Sicherheitstests, siehe →Bouncer. Leider gelangen immer wieder betrügerische Apps in diese Stores, diese können oft (z.B. bei iOS) auch wieder vom Gerät entfernt werden (**remote application removal**). Diese Feature ist aber nicht unumstritten, da diese Funktionalität auch für Zensur genutzt werden kann. Ebenso ist umstritten, dass Apple und Google 30% der Umsätze einfordern, die von den App Entwicklern über die Apps eingenommen werden (z.B. Musikverkäufe oder In-App-Käufe in Spielen). Diese Marge ist erheblich und stellt sicher, dass z.B. Bücher nie über Apps verkauft werden können (die Margen sind zu gering). Spotify hat sich vergeblich dagegen gewehrt, ebenso EPIC (Fortnite) für ihre In-Game Verkäufe. In China verlangt Huawei für die Spiele in seinem App-Store 50% Provision von →Tencent

App Wrapping: Technik der →Virtualisierung bei der ein →Programm automatisiert so verändert wird, dass der →Befehlscode in einer ‚geschützten' Umgebung ausgeführt wird und →Zugriffe zum eigentlichen →Betriebssystem durch diese Umgebung realisiert und kontrolliert werden. Beispiele sind Thinapp für →Windows und →Mobile Horizon für →Smartphones

APT: (Advanced Persistent Threat) neues Schlagwort für eine Situation bei der es einem Angreifer gelingt, sich langfristig in einem Computernetz „einzunisten" und dort systematisch Informationen zu sammeln oder Schaden anzurichten. Wird hauptsächlich zu →Wirtschaftsspionage eingesetzt, bzw. bei Aktionen wie →Stuxnet. APT sind zielgerichtet, was bei anderen →Angriffen mittels →Spyware nicht immer der Fall ist. Sehr oft beginnt ein APT-Angriff mit →Social Engineering (z.B. gefälschtem →E-Mail) auf einen eigentlich unwichtigen Rechner. Manchmal werden Firmen-PCs auch infiziert, indem →Websites identifiziert werden, die von vielen Mitarbeitern dieser Firma oder dieser Branche genutzt werden („watering holes"). Dieser →Webserver wird dann übernommen, dort eine →Schadsoftware installiert, die mittels →Zero-Day Verwundbarkeiten die PCs der Besucher dieser Website infizieren kann. Auf diesen Besucher-PCs wird dann eine Software zur Fernsteuerung (→RAT) installiert und sog. →lateral movements innerhalb des Firmennetzes führen zum eigentlichen Ziel, entweder →data leakage oder →Sabotage wie bei →Stuxnet. APTs sollen über spezielle Systeme erkannt werden, die Events korrelieren und Anomalien im Netz aufzuspüren versuchen, z.B. →SIEM. Siehe auch →Pass-the-Hash, →Process injection

APT1: (auch Unit 61398) geheime Einheit in der chinesischen Volksbefreiungsarmee (→PLA), spezialisiert auf das Eindringen in andere Rechner mittels →APT-→Angriffen. Entsprecht der Einheit →TAO in der →NSA

APWG: (Anti-Phishing Working Group) intern. Organisation zum Datenaustausch über und zur Bekämpfung von →Phishing

AR: →Augmented Reality

Arbeitspeicher: Teil eines →Rechners (oder auch →Smartphones), in dem →Programme (und →Daten temporär während ihrer Verareitung im →Prozessor) gespeichert sind. Siehe →Speicher

Archivierung: sicheres Aufbewahren von →Critical Records. Dies beinhaltet mehrere Kopien und deren →Auslagerung. Grund sind z.Teil gesetztliche →Aufbewahrungsvorschriften oder geschäftliche Erfordernisse

ARDA: (Advanced Research Development Activity) US-amerikanische Forschungseinrichtung zur Unterstützung der →NSA und →DHS,

z.B. bei der Auswertung großer Datenmengen (→Data Mining). Heute umbenannt in Disruptive Technology Office, DTO (disruptive technology = neue Technologie, die die bestehenden Technologien ersetzt und ablöst)

ARG: (Alternate Reality Game) spezielle Form eines →LARP, bei dem mittels Kommunikationsmedium (Telefon, →E-Mail, Brief) eine alternative Realität zu erzeugen. Die Spieler agieren →IRL und werden von einem Game Designer gesteuert und die Aufgabe haben, Probleme zu lösen. Auch ARGs sind (wie LARPs) für Lehrzwecke eingesetzt worden

ARGE DATEN: sehr aktive Organisation in Ö, die sich um Belange des →Datenschutzes kümmert. http://www.argedaten.at/

ARM: (Advanced RISC Machine) heute viel verwendete →CPU-Architektur nach dem →RISC-Konzept, entwickelt und hergestellt von der gleichnamigen Firma. ARM-CPUs zeichnen wie alle RISC-CPUs sich durch vergleichsweise geringe Zahl von Schaltelementen und Stromverbrauch aus. ARM-CPUs werden oft in →Smartphones, →Laptos, →Tablets verwendet, sowie in →Embedded Systems und seit 2020 auch für Rechner von →Apple

ARP: (Address Resolution Protocol) Teil von →Layer 2 des →OSI Schichtenmodells der →Ethernet-Implementierung, übersetzt die →IP-Adresse eines Rechners in die →MAC Adresse des Netzwerkinterfaces (RFC 826). Letzter Schritt vor der „Zustellung" der Daten im Zielgerät. →Man-in-the-Middle →Angriffe innerhalb des gleichen Subnetzes sind durch **ARP Cache Poisoning** möglich

Art.8 EMRK: (→Europäische Menschenrechtskonvention) definiert das Recht auf →Privatsphäre, in einigen Punkten weitergehend als das ö. →DSG2000

Art.29 Data Protection Working Party: bis Mai 2018 Arbeitsgruppe der EU, zusammengesetzt mit Vertretern aller Datenschutzkomissionen der EU-Länder, die sich mit →Datenschutz beschäftigt und sehr interessante Dokumente herausgab, z.B. zu →Suchmaschinen. Siehe →EMRK, →ENISA, →European Data Protection Initiative, →Data Protection Directive. Seit Mai 2018 ersetzt durch → European Data Protection Board (EDPB)

Artificial intelligence: (AI, künstliche Intelligenz) Schlagwort für den Versuch, →Software zu entwickeln, die →Rechnern ermöglicht, Aufgaben zu bewältigen, die traditionell nur von Menschen erledigt werden können (z.B. →Turing Test). Dabei wird unterschieden zwischen „schwacher AI", das sind die AI-Systeme die wir heute nutzen, z.B. →neuronale Netze für Bild- oder Spracherkennung, Sprachübersetzung, →Algorithmen für Routenplanung, aber auch Systeme die z.B. mittels →Deep Learning Spiele wie Schach und Go beherrschen und dabei jeden Menschen sicher schlagen können (→DeepMind).

Dem gegenüber steht das Konzept der „starken AI" (auch AGI = artificial general intelligence), die (noch ?) nicht existiert und die sich dadurch auszeichnet, dass diese Maschine ALLE Probleme besser löst als ein Mensch. Die Idee dabei ist, dass solche Systeme natürlich auch bessere AI-Systeme als wir Menschen bauen können und dass es dazu zu einer →Intelligence Explosion (auch →singularity genannt) kommen könnte deren Ausgang für die Menschen ungewiss ist (siehe Szenario des Filmes „Matrix").

Sicherheitsrelevant z.B. durch →Captchas bzw. die Versuche, diese zu „knacken" (→"cracking"). Es stehen heute sog. →Chatbots zur Verfügung, denen es gelingt, durch automatisierte Dialoge betrügerische Situationen oder pädophile Kontakte zumindest vorzubereiten. Als Gegenmaßnahme wird versucht, solche Chatbots automatisiert zu erkennen. Es wurde behauptet, dass z.B. bis zu 85% der Teilnehmer in Yahoo-Chatrooms (obsolet) bereits →bots sind. →Facebook und →Twitter versuchen sehr aktiv gegen bots vorzugehen und löschen viele solcher Accounts. Diese können aber sehr leicht auch automaisiert wieder angelegt werden. Siehe auch →Adversial Learning.

Problematisch sind auch sog. →Deepfakes, das sind mittels AI hergestellte Fälschungen von Videos mit deren Hilfe Personen in unerwünschten Situationen, z.B. Pornofilm gezeigt werden kann und falsche Aussagen in den Mund gelegt bekommen. Problematisch ist auch, dass AI-Systeme auf der Grundlage von →Deep Learning nicht in der Lage sind, ihre Entscheidungen zu erklären (→explainability). D.h. die zum Teil für uns Menschen absurden Fehler bei der Bilderkennung sind nicht leicht zu vermeiden, was z.B. bei →autonomen Fahrzeugen sehr problematisch ist.

Bedrohliche Szenarien werden rund um →Intelligence Explosion (→Singularity) diskutiert: sich verselbständigende Super-Intelligenzen die rein auf Grund ihrer übermenschlichen Intelligenz die Menschen automatisch dominieren. Siehe auch →Roboter, →autonome Fahrzeuge, →Meme, →Artificial Intelligence Act

Artificial Intelligence Act: (AI Act) in 2020 von der EU vorgeschlagene Regulation mit der →Algorithmen einer Produktregulierung unterworfen werden sollen (mit entsprechenden ‚Gütesiegeln') wenn diese Algorithmen geeignet sind, in die Rechte von Menschen einzugreifen, z.B. wenn sie diskriminierend wirken. Die geplante Regulation teilt Algorithmen in 4 Klassen ein. Die oberste Klasse ist ‚prohibited' weil ‚unacceptable risk', z.B. social →scoring durch Regierungen. Die

unterste Klasse ist ‚minimal or no risk', d.h. diese Klasse von Algorithmen ist ohne Einschränkung einsetzbar. Die Klasse ‚high risk' sind z.B. medizinische Geräte oder Algorithmen die über Job-Bewerbungen entscheiden. Diese Systeme müssen einer Bewertung unterzogen werden bevor sie auf den Markt gebracht werden können (analog zu Technikfolgenabschätzung). Die verbleibende Klasse ‚transparency risk' kann sich mit der Klasse ‚high risk' überschneiden und verlangt noch zusätzlichen Informationspflichten, dies betrifft z.B. automatisierte →Bots, die sich als solche zu erkennen haben. Siehe https://sicherheitskultur.at/Newsletter/Newsletter_171.htm#thema1

artificial persona: siehe →Bot

AS2: (Applicability Statement 2) Standard für den Austausch von →EDI-Dokumenten über →HTTP, geschaffen durch →EDIINT. Der Datenaustausch ist unabhängig vom Format der Dokumente, z.B. →XML. Neben HTTP kann auch HTTPS oder →S/MIME für den Datentransport verwendet werden. Mittels →Zertifikaten wird eine →Verschlüsselung und →Signatur erzeugt

ASCII (American Standard Code for Information Interchange) der (de-facto) Standard für die Codierung von Texten. Leider erlaubt ASCII nur 7 bits für Zeichen, d.h. die Umlaute können nicht vernünftig dargestellt werden. Dies ist eine Quelle von Frustration und Fehlern. So können in →E-Mails nur durch Nutzung der sog. →MIME-Erweiterungen Umlaute dargestellt werden. Eine moderne Methode zur Textdarstellung verwendet →Unicode, das auch asiatische Alphabete unterstützt

ASLR: (Adress Space Layout Randomization) Technik, z.B. in OpenBSD, →Mac OS, →Vista und XP SP2, um zu erreichen, dass ein Angreifer nicht weiß, an welcher Stelle im Speicher eine bestimmte Funktion geladen ist. →Skype verwendet ähnliche Tricks. Wird mittels →JIT-Spraying angegriffen

ASP:
1) **Application Service Provider.** Anbieter von EDV-Diensten, die über Datenkommunikationsanbindung genutzt werden, ähnlich zu →Outsourcing. Dabei sollen durch →SLAs die jeweiligen Sicherheits- und Verfügbarkeitsanforderungen festgelegt werden

2) **Active Server Pages** von →Microsoft entwickelte Methode, dynamische Webseiten zu generieren, Konkurrenz zu Produkten wie Cold Fusion und Technologien wie →JSP (Java Server Pages) oder →- im →Open Source Bereich. Alle diese Technologien fallen unter Server Side Scripting (d.h. sie werden im →Webserver ausgeführt), im Gegensatz zu Client Side Scripting durch →Active Scripting oder →JavaScript/Jscript

Asprox: →Fast-Flux →Botnetz. Siehe →Rock Phish Gang

Assembler: (to assemble=zusammenbauen) sehr „maschinen-nahe" Programmiersprache, bei dem Computer-Instruktionen (→Code) und Speicheradressen direkt verwendet werden, im Gegensatz zu →Compilern, die „höhere" Programmiersprachen nutzen (Fortran, Java, C, C++, C#) die abstrakte Datenstrukturen und wiederverwendbare Routinen erlauben.

Assembler sind langsamer zu programmieren, aber erzeugen sehr kompakte Programme. Sie werden z.B. für →Embedded Systems oder →Firmware eingesezt, aber auch für manche Formen von →Schadsoftware wie z.B. Viren

Asset: Begriff aus dem →Risikomanagement. Alles was für ein Unternehmen Wert hat (Dinge, Programme, Know-how, Geld, Zeit, Marktanteile, Brandname, Ruf, Image, Kundenzufriedenheit, Goodwill, juristische Rechte, Ansprüche). Assets sind mit angemessenem Aufwand zu schützen

Asset Classification: Bewertung von Objekten, z.B. →Dateien oder anderer →Daten in einer →Datenbank bzgl. Ihres Schutzbedarfs, z.B. in Hinsicht auf →Vertraulichkeit. Wird selten durchgeführt, da sehr aufwendig. Es gibt Versuche zu einer automatisierten Klassifizierung. Wenn Asset Classification durchgeführt würde, so würde dies →DLP stark vereinfachen

Astroturfing: in →Social Networks, →Blogs und überall wo Kommentare abgegeben werden können das Manipulieren von Meinungen z.B. durch →Sock puppets. Diese Dienste werden kommerziell angeboten, bzw. über →Crowdsourcing Services wie ShortTask durchgeführt (→Crowdturfing). 2011 wird berichtet, dass die Manipulation von Meinungen zu Politik oder Produkten bei einigen Anbietern über 90% der angebotenen Aufgaben darstellen. Siehe auch →Fake Accounts, →Twitter Bombe

Asymmetrische Verschlüsselung: →Verschlüsselung

ATA: Hardware-Spezifikation für den Anschluss von →Magnetplatten u.ä. Erlaubt das Setzen von →Passworten zur Kontrolle von unautorisierten →Zugriffen

ATM:
1) **Asynchronous Transfer Mode**: Datenübertragungsmethode die es Anbietern erlaubt, Hochgeschwindigkeitsverbindungen mit garantierter Durchsatzleistung für mehrere Kunden in einem einzigen Übertragungskanal zu bündeln. Es können darüber beliebige Protokolle übertragen werden. Relevant für →QoS, da einzelnen Kunden garantierte Bandbreiten zugewiesen werden können. Übertragungsraten liegen dabei höher als 155 Mbps

2) **Automated Teller Machine**, engl. für Geldausgabeautomaten, (Bankomat). Sicherheitsproblematisch wenn die →PIN-Eingabe ausgespäht wird. Die Sicherheit hängt auch davon

ab, dass die Geräte →tamper-proof sind. Erfunden 1967 von Barclays Bank, damals „Robot Cashier“ genannt. Siehe →Bankomatkarte, →Skimming

Autonome Fahrzeuge: Fahrzeuge jeglicher Art, die mittels Sensoren und geeigneter Software (z.B. →Deep Learning) selbständig am Verkehr teilnehmen können. Ab 2017 werden diese von vielen Firmen auch im Straßenverkehr gestestet, bisher noch immer mit Aufsicht durch einen Fahrer. Für die Sicherheit, auch bei widrigen Umständen wie schlechter Sicht, gibt es noch viele offene Fragen, z.B. Haftung und Zulassungsanforderungen. Der Übergang zu solchen autonomen Fahrzeugen sind Fahrer-Assistenzsysteme, die in der EU in 2022 Bremsassistenten verpflichtend werden. Siehe https://www.philipps-welt.info/autonom

Attribution: Zuordnung zwischen einem Täter (actor) und einer Tat. Sehr schwierig bei →Angriffen im →Internet, z.B. →Cybercrime und →Cyberwar. →Plausible Deniability ermöglicht es den Beschuldigten sehr oft, die Verantwortung z.B durch Verweis auf →Hacktivisten von sich zu weisen (auch wenn diese vielleicht als →Proxy aktiv sind). Bei der Untersuchung von solchen Vorfällen wird nach sog. →Indicators of Compromise gesucht.

Attribution ist sehr schwierig wenn die Angreifer →“hop points„ oder einen →Anonymisierer wie →TOR oder andere Mittel verwenden um die Spuren zu verwischen. So speichert z.B. beim Übersetzen eines →Programmes in Maschinen→code (auch bei Schadprogrammen) der →Compiler die Spracheinstellung des →PCs im Maschinencode als Kommentar ab. Aber auch diese Einstellung lässt sich vor der Compilierung leicht ändern. Kommentare im Programm oder die Bekennerschreiben werden auch auf sprachliche oder kulturelle Eigenheiten untersucht, aber alles dies ist auch fälschbar.

Attribution ist ein wichtiger Faktor gerade beim Thema Cyberwar, wo die Militärs sich ein Recht auf Selbstverteidigung durch Gegenangriff vorbehalten. Dort kann eine falsche Zuordnung (z.B. auf Grund von bewusst gelegten falschen Spuren, z.B. Hop Points in anderen Ländern), zu einer Katastrophe führen. Die Behauptung man kenne die Angreifer kann wenn sie nicht als Bluff enttarnt wird, sehr wirksam sein, weil alle anderen dann glauben (könnten), dass der Beschuldiger Möglichkeiten hat, Angreifer zu identifizieren, was Teil der Abschreckung sein könnte. Dies wird auch im Fall →Sony 2014/15 spekuliert

ATS: →Automated Targeting System

Attachment: Anhang an ein →E-Mail, mit dessen Hilfe eine beliebige Datei transportiert werden kann, Teil des →MIME-Formats. Auf diese Weise kann auch →Malicious Code übertragen werden, dies soll durch →Content Filtering verhindert werden

Attack: →Angriff

Attack Signature, Attack Pattern: der für einen →Angriff typische Netzwerkverkehr (Inhalt und Folge von →IP-Paketen) oder Folge von Systemaufrufen auf einem Rechner. Wird von →IDS für die Erkennung eines Angriffs genutzt. Kann sich auch auf eine Folge von Systemaufrufen beziehen, an denen ein im Rechner selbst residentes Überwachungsprogramm einen Angriff erkennen könnte

Attack Tree: Methode der →Risikoanalyse, bei der man sich in die Rolle des Angreifers versetzt und die verschiedenen Möglichkeiten für eine bestimmte Verletzung der →Informationssicherheit, sei es Vertraulichkeit, Verfügbarkeit, etc., durchspielt

Attagging: →Angriff mittels →QR-Code

Audio Mining: Form des →Lauschangriffs. Methode, mit der man gesprochenen Text nach Schlüsselwörtern durchforstet. Dies ermöglicht die Suche in einer Audio-Datei oder von Telefonaten. Auch 'audio indexing' genannt

Audit: ursprünglich englische Bezeichnung für Rechnungsprüfung. Im →Qualitätsmanagement: systematischer, unabhängiger und dokumentierter →Prozess zur Erlangung von Nachweisen bzgl. der Einhaltung interner oder externer Regeln und zu deren objektiver Auswertung (Beispiel auch Code-Audit in der Programmierung). In der IT- und Informationssicherheit sind solche nachträglichen Kontrollen ein wichtiger Faktor überall dort, wo z.B. →Zugriffe für legitimierte Personen gewährt werden müssen, aber Missbrauch durch diese Personen möglich ist. Neuere Entwicklungen, z.B. →Sarbanes-Oxley Act oder →Basel II erfordern eine immer stärkere Betrachtung der →Informationssicherheit im Rahmen von Audits, z.B. durch Nutzung von →CobiT oder →SAS 70. Siehe →SMM, →comply or explain

Audit-Log: Datei mit den Log-Einträgen von Ereignissen (→Events) in Rechnersystemen und Netzen zum Zweck der Nachvollziehbarkeit. Dabei soll für alle Ereignisse ein EDV-Nutzer als eindeutiger Verursacher des Ereignisses identifizierbar sein. Dies führt zu →Accountability eines Prozesses oder Systems. Diese Information können im Rahmen eines →SIEMs auch für Zwecke der →Informationssicherheit verwendet werden

Audit-Trail: Menge von Logdaten, die gemeinsam eine direkte eindeutige Zuordnung eines Ereignisses zu einem Verursacher erlauben

Auditor: Person mit dem Auftrag Qualität, Korrektheit und/oder Sicherheit einer Aktivität unabhängig und objektiv zu verifizieren

Aufbewahrungsfrist: Dauer der Verpflichtung zur Aufbewahrung für wesentliche Geschäftsinformationen, meist gesetzlich geregelt, z.B. 7

Jahre für Buchhaltungsunterlagen, 30 Jahre für Gesundheitsbefunde oder Sparbücher. Sichere Aufbewahrung schließt auch die Verfügbarkeit nach einem →Katastrophenfall ein, d.h. erfordert oft auch die Auslagerung einer Kopie und oft auch →Fälschungssicherheit

Aufbewahrungsvorschrift: gesetzliche oder anderweitige Regel, die besagt, wie lang →Aufbewahrungsfristen dauern

Auftraggeber: (engl. →Controller) im →Datenschutz derjenige, der den Auftrag für eine Datenverarbeitung (von →personenbezogenen Daten) an einen →Dienstleister vergibt und damit die Verantwortung für die Rechtmäßigkeit dieser Verarbeitung übernimmt. Sein Dienstleister muss durch ein →SLA und regelmäßige Kontrollen zur Einhaltung der Gesetze gebracht werden

Augmented Reality: (AR) computergestützte Erweiterung der Realitätswahrnehmung, z.B. durch Einblendung von zusätzlichen Informationen in Video-Darstellungen, z.B. Daten aus anderen Systemen oder →Sensoren. Wird z.B. als Heads-Up Display in Militärflugzeugen eingesetzt oder seit 2013 bei →Google Glas und 2014 bei →Oculus Rift. Wird zu Verletzungen der →Privatsphäre führen da es oft mit einer Kamera kombiniert wird und mittels →Gesichtserkennung automatisch Informationen über andere Menschen einblenden kann. Wenn die Geräte immer kleiner werden führt das zu einer Situation dass Menschen ständig damit rechnen müssen, dass ihr Verhalten aufgezeichnet wird. Siehe →wearable computing, →virtual reality

Ausfall: Nicht-Verfügbarkeit von →Systemen, →Daten oder →Services. Siehe →RTO, →RPO, →Disaster Recovery

Ausfallwahrscheinlichkeit: Wahrscheinlichkeit, dass ein Gerät oder System ausfällt. Siehe →Fehlerbaumanalyse, →Verfügbarkeit

Auslagerung: Kopie archivierter Dokumente und → Backup-Medien an einem sicheren Ort gelagert um auch nach →Katastrophen für →Desaster Recovery zur Verfügung zu stehen

Authentication: →Authentisierung

Authentication Token:

1) Gerät das eine Information produziert, die zur →Authentisierung einer Person genutzt wird

2) Datensatz der zwischen Systemen ausgetauscht wird um zu bestätigen, dass eine bestimmte Person oder Service authentifiziert ist (→Kerberos)

Authentifizierung: →Authentisierung

Authentisierung: (=Authentifizierung) (engl. Authentication) →Verifizierung der →Identität (→Identifizierung) einer Person (oder Objektes). Authentisierung gibt die Sicherheit, dass die Person genau die ist, die sie zu sein vorgibt. Heute werden dafür meist (noch) →Passworte eingesetzt, die für →Websites in →Datenbanken gespeichert werden, innerhalb von Firmen wird zumeist →Active Directory eingesetzt. Besser als Passworte ist →2-Faktor-Authentisierung mit →Biometrie oder →OTP-Konzepten. Die Trennung zwischen „nur" Passworten und stärkeren Verfahren wird bei →Risk-based-Authentication (RBA) dynamisch „errechnet", z.B. auf Grund von Faktoren wie „anderer →IP-Adresse" wie früher. Ein Beispiel für eine ältere Technologie ist das →RADIUS Protokoll. Eine Alternative zu Passworten ist →Biometrie (→Fingerprint oder →Gesichtserkennung) oder →Zertifikate, z.B. auf →SmartCards oder →OTP-Geräte oder -Implementierungen. Siehe →AAA, →EAP, →Out-of-band Authentisierung, →SRP, →JAAS, →Oauth, →eID, →TOTP, →HOTP, →Nitrokey, →Yubikey, →Google Authenticator, →keyless system. Abgegrenzt von →Autorisierung

Authentizität: Echtheit von Gegenständen oder →Nachrichten, für letztere auch die sichere Zuordnung von →Absender oder Ursprung und die →Integrität der Nachricht, realisiert über Nutzung eines Message Authentication Codes (MAC). Siehe →Verbindlichkeit

Authorization: →Autorisierung

Auto: moderne Autos enthalten 50 - 70 integrierte →Prozessoren (→embedded systems), die typischerweise mittels →CAN-bus miteinander verbunden werden und an dem nicht nur →Systeme wie Engine Control Module, Electronic Brake Control Module, Transmission Control Module, →TPMS und Body Control Module angeschlossen sind, sondern auch das Autoradio (das zumeist auch verwendet wird um alle Blinker- und Warngeräusche zu erzeugen und daher eng mit den anderen Fahrzeugprozessoren gekoppelt sein muss), die Klimananlage, die Airbags, die Diebstahlsicherung, das Navi, die Instrumentierung im Armaturenbrett, der elektronische Türöffner und das Telematic-Module, das über GSM (Handy) eine Lokalisierung und Blockierung des gestohlenen Autos erlaubt.

Die Komponenten werden über mehrere →Bus-Systeme (→CAN) miteinander gekoppelt. Wie bei jedem Bus-basierenden System kann jede Komponente am Bus alle anderen Komponenten kommunizieren. Es findet fast keine →Authentisierung der Komponenten statt. Bei Design wird Sicherheit weitgehend ignoriert und durch unerlaubt in das System eingefügte Kommandos können gefährliche Zustände erreicht werden, z.B. de-aktivieren der Bremsen.

Es konnte 2013 gezeigt werden, dass z.B. ein ‚böses' Autoradio sicherheitsrelevante Komponenten wie die Bremsen beinflussen kann. Ebenfalls problematisch sind ‚keyless' Systeme bei denen der Motor ohne mechanischen Schlüssel gestartet wird. Solche Systeme

werden über →kryptographische Verfahren abgesichert, jedoch haben sie immer die →Schwachstelle der →Key recovery für den Fall, dass der rechtmäßige Besitzer den Schlüssel verloren hat.

Eine weitere Herausforderung ist die Absicherung der computer-gesteuerten Fahrzeuge die Fehler in der Steuerung haben könnten oder manipuliert sein könnten. 2014 haben Wissenschaftler ein kleines Modul vorgestellt, das von außen in das Bus-System integriert werden kann und dann drahtlos Kommandos von Angreifern empfangen kann.

Außerdem werden seit einiger Zeit mehr und mehr Fahrzeuge über →Handy-Technologie vernetzt, z.B. für einen automatischen Notruf wenn Airbags auslösen (wird 2015 als →eCall in der EU Pflicht). Ebenfalls Pflicht werden Systeme die Reifenunterdruck erkennen (→TPMS). Eine Lösung geht über einen Vergleich der Umdrehungszahlen der 4 Räder, der andere, unsichere Weg misst den Reifendruck im Ventil und sendet diesen drahtlos unverschlüsselt zum Bordcomputer; dies könnte manipuliert werden.

→Google experimentiert seit einigen Jahren mit selbstfahrenden Autos (→autonomous car), 2015 stellen alle Hersteller ähnliche Modelle mit mehr oder weniger großen Selbständigkeit vor. Vor der Einführung solcher Technologien sind noch eine Reihe von Haftungs- und →Ethikfragen zu klären.

2014 wurde ein Standard verabschiedet, über den Autos sich gegenseitig über Geschwindigkeit und Position informieren sollen, um auf diese Weise Unfälle aktiv zu vermeiden (die Regeln für kooperative intelligente Transportsysteme, →C-ITS, der →ETSI). Auch eine Kommunikation mit Verkehrszeichen ist dann natürlich möglich und eine vollständige Überwachung wäre sichergestellt.

Siehe →PLC, →M2M, →On-Board-Diagnose http://sicherheitskultur.at/notizen_1_10.htm#auto

Automated Clearing House: (ACH) Form der Geldüberweisung und Abbuchungen zwischen Bankkonten in den USA bei der die →Identität von Sender und Empfänger nicht geprüft wird und eine Rückerstattung nur dann möglich ist, wenn die gesamte geforderte Summe auf dem Konto ist. Wird daher gern für →Money Mule Aktivitäten genutzt

Automated Targeting System: (ATS) System des →DHS das für alle Personen, die die US-Grenzen überschreiten oder in Ex- und Import tätig sind, auf Basis einer Datenauswertung eine →Risiko-Zuordnung bzgl. →Terrorismus oder →Kriminalität vornimmt. Ursprünge liegen in den 90er Jahren. Es gibt keine Möglichkeit der Einsicht oder Korrektur

Automatic Update: Funktionalität in →Windows 2000 (SP2), Windows XP und →Vista, die eine automatische Installation von →Patches realisert. Wird in →SUS und →WSUS genutzt. Nicht zu Verwechseln mit dem Update über Internet Explorer

Automation Bias: psychologer Effekt, dass die menschliche Wachsamkeit nachlässt wenn Überwacher wissen, dass ein automatisches System eigentlich alle Ereignisse entdecken sollte. Dies ist ein Sicherheitsproblem, z.B. in Kernreaktoren. Siehe →Primary Effect, →Vigilance decrement

Automobil: →Auto

Autonmous car: →Autonome Fahrzeuge

Autonome Fahrzeuge: großes Thema seit ca. 2004 mit DARPA Grand Challenge, aber die Entwicklungen hatten viel früher begonnen. Ab 1950 wurde ernsthaft daran geforscht. Ab ca. 2010 wird auf breiter Front geforscht. →Google experimentiert seit ca. 2011 mit selbständigen Fahrzeugen im öffentlichen Verkehr. 2015 stellen alle Auto-Hersteller mehr oder weniger selbständige Fahrzeuge vor (oft als Parkhilfe oder nur für Autobahnstrecken). Solche Fahrzeuge werden in 5 Klassen eingeteilt: von einfachen Assistenzsystemen für bestimmte einfachere Situation bis zu „steering wheel optional“. Dabei entstehen zahlreiche noch nicht gelöste technische Herausforderungen für billige →Sensoren, aber auch Probleme der IT-Sicherheit gegen un→autorisierte →Zugriffe bis hin zu den Auswirkungen auf Raumplanung und die Gesellschaft. Auch Fragen der Vernetzung sind relevant, siehe →C-ITS. Autonome Fahrzeuge werfen auch bei →Ethik komplexe Probleme auf. So muss die Elektronik in einer kritischen Situation in denen ein Unfall unvermeidbar ist, Optimierungen dahingehend treffen, dass die Schäden minimiert werden. Schwierig ist z.B. die Bewertung zwischen einer geringen Wahrscheinlichkeit dass ein Mensch verletzt wird verglichen mit einer sehr hohen Wahrscheinlichkeit eines sehr großen Materialschadens. Siehe auch →situational crime prevention. Zumeist ebenfalls geforderte Vernetzung der Fahrzeuge wirft riesige Probleme der →Privatsphäre auf. Viele Details auf http://philipps-welt.info/autonom.htm

Autonome Waffen: die Mehrzahl der in 2019 eingesetzten automatischen Waffen, z.B. →Drohnen, stehen noch unter menschlicher Kontrolle (→human-in-the-loop). Es gibt jedoch auch bereits Systeme, die so schnell reagieren müssen, dass dies nicht möglich ist, z.B. das israelische Raketen-Abwehrsystem Iron Dome. Es wird in →AI-Kreisen diskutiert, ob es möglich sein wird (ähnlich zu den →Robotergesetzen die sich natürlich für Waffen ausschließen) Regeln in solche Waffen zu implementieren, die eine Einhaltung der Kriegsrechtsregeln sicherstellen (z.B. Schutz von Nicht-Kombatanten). Proponenten sagen, dass ein Roboter auf Grund der fehlenden Emotionen und der fehlenden Gefahr für das

eigene Leben evtl. sogar solche Schutzregeln stärker beachten könnte. Ab 2017 werden große Fortschritte bei der Entwicklung gemacht und auch Schutzgesetze diskutiert (mit jedoch geringer Aussicht auf internationale Umsetzung). Siehe auch →man-in-the-loop und http://philipps-welt.info/robots.htm#killbot

Autorisierung: Prozess, bei dem festgestellt wird, zu welchen Aktivitäten ein Benutzer berechtigt ist. Der Vorgang ist oft, aber nicht notwendigerweise mit der →Authentisierung gekoppelt, Gegenbeispiel ist →claims-based authorization. Siehe →AAA, →RBAC

Availability: Begriff aus der IT-Sicherheit, →Verfügbarkeit eines Systems oder einer Anwendung

Avatar: in der IT eine künstliche Person oder ein grafischer Stellvertreter einer echten Person in einer →virtuellen Welt wie →Second Life oder →MMORPGs, beispielsweise in einem Computerspiel. Diebstahl von Avataren oder von Ausstattungen von Avataren wird 2005 zu einem Sicherheitsproblem

AV-Software, AV System: →Malware-Schutz

Awareness: (engl. Bewusstsein) in der →Informationssicherheit verwendet, um den Bewusstseinsstand der →Anwender in Bezug auf →Informationssicherheit zu bezeichnen. Awareness-Programme in Unternehmen sollen den Kenntnisstand, z.B. bzgl. →Bedrohungen wie →Social Engineering verbessern und die Akzeptanz bzgl. Regeln der →Security Policy erhöhen

AWS: (Amazon Web Services) →EC2

AYIYA: (Anything In Anything) Tunneling Protokoll mit dem u.a. →IPv6 Datenverkehr in →IPv4 Netzen übertragen warden können. Nutzt →Port 5072. Siehe →Teredo, →TSP

B2B: (Business to Business) →E-Commerce zwischen Firmen, siehe →EDI

B2C: (Business to Consumer) →E-Commerce zwischen einer Firma und einer Privatperson, z.B. Einkauf auf einem →Web Portal

BAC: (Basic Access Control) standardisierte →Verschlüsselung der Daten im →ePass. Die Daten der →MRC werden als →Schlüssel verwendet. Dies wird kritisiert, da diese Daten z.B. beim Einchecken im Hotel frei zugänglich sind und die effektive Schlüssellänge in einigen Ländern nur 28 bit beträgt. Siehe →EAC

Backbone: in der Regel sehr schnelle Datenverbindung, zumeist auf der Basis von →Lichtleitern. Der Betriff wird sehr oft verwendet für die Internet-Backbones, d.h. die Verbindungen zwischen den großen Exchanges (→IXP).

Backdoor: (engl. Hintertür)

1) →Programme, die auf einem fremden →PC installiert und von Angreifern benutzt werden können, um diesen PC zu kontrollieren (speziell bei →targeted attacks). Um Backdoors unbemerkt zu installieren, werden oft →Trojaner (als Beipack zu →Freeware wie einem Bildschirmschoner, einem Spiel oder bei →Raubkopien) verwendet, zum Teil werden auch →Schwachstellen (z.B. fehlende →Sicherheitspatches) ausgenutzt. Ein Beispiel sind →RAT
2) Hintertüren die Entwickler in Programmen eingebaut haben, z.B. um für Wartungszwecke leichten Zugang zu solchen Systemen zu haben. Ein Beispiel sind fest eingebaute →Accounts des Herstellers, über die auf diese Systeme zugegriffen werden kann. Es wird immer wieder behauptet, dass in bestimmten Systemen solche Hintertüren sind, manchmal werden diese auch im Internet veröffentlicht, was dann zu einer erheblichen →Schwachstelle des Systems führt. Solche Hintertüren werden zum Teil auch auf Anforderung von Polizei- oder anderen Überwachungsbehörden eingerichtet und heißen dann →Law Enforcment Access

background noise: (auch: Internet Background Noise, IBN) Im →Internet durch Rechner erzeugt, die mit →Würmern infiziert sind und die bis zu ihrer Reinigung ständig versuchen, andere Rechner zu infizieren. Eine weitere Quelle des IBN sind →port scans mit dem Ziel, verwundbare Rechner zu finden. http://www.switch.ch/security/services/IBN/

Back Hacking: Versuch, einen →Hacker aufzuspüren, indem man seinen Weg durch das Computernetz zurückverfolgt und evt. auch den Hacker selbst anzugreifen. Allerdings versuchen Hacker beim Eindringen in Systeme genau diese Spuren zu verwischen

Back Orifice: →Trojaner, →Backdoor

Backscatter: Datenverkehr der entsteht wenn ein →SMTP-Server →Spam ablehnt und dann eine non-delivery Nachricht an den vermeintlichen Absender versendet. Siehe →Spoofing

Backscatter X-ray: Nutzung von Röntgenstrahlung zur Darstellung von Menschen ohne Kleidung (→Nacktscanner). Im Gegensatz zur medizinischen „Durchleuchtung“ wird hierbei die rückwärtige Streuung eines sehr dünnen Röntgenstrahles ausgenutzt. Diese hängt von der atomaren Zusammensetzung der jeweiligen Stelle ab und kann daher z.B Metalle deutlich von organischen Materialien unterscheiden

BackTrack: Sammlung von Tools für Netzwerksicherheit und →Penetrationstests auf →Linux-Basis, basierend auf →SLAX. Wie alle solche Tools können sie für →Angriff oder Testen der eigenen Verteidigungsmaßnahmen genutzt werden. Angeblich die Grundlage für die Entwicklungen von →FinFisher

Backup: (Datensicherung) →Daten werden in regelmäßigen Abständen mit Hilfe von definier-

ten →Prozessen von Produktions-→Magnetplatten auf andere →Datenträger (meist →Magnetbänder, heute auch oft Magnetplatten) kopiert. Bei Datensicherungen wird unterschieden zwischen **voll** (alle Dateien der betroffenen Verzeichnisse werden gesichert), **differentiell** (Sicherung nur der Dateien, die seit der letzten vollen Sicherung verändert wurden) und **inkrementell** (Sicherung der geänderten Dateien seit der letzten vollen oder inkrementellen Sicherung). Siehe →Split, →Mirroring, →Clone, →Restore, →Recovery, →Sychronisation, →Snapshot, →Backup-Fenster. http://sicherheitskultur.at/Datensicherung

Backup-Fenster: Zeitspanne die für → Datensicherung zur Verfügung steht. Hintergrund ist, dass eine Datensicherung von aktiven (d.h. geöffneten) →Dateien nicht möglich ist und daher für die Sicherung die Anwendungen beendet sein müssen. Traditionell die Nachtstunden nach dem Tagesabschluss. Bei 24-Stundenbetrieb ist das Fenster Null, es müssen andere Sicherungsmethoden, z.B. →Split oder →BCV angewendet werden. Siehe →VTL

Backup-Rechenzentrum: weiteres →Rechenzentrum an einem anderen Ort zwecks →Business Continuity und →Disaster Recovery, zumeist über eine schnelle Verbindung (→Fibre Channel) angebunden, die →Magnetplatten sind oft gespiegelt (→Mirroring)

Backup-to-Disk: →VTL

Balabit: Ungarische Firma, bekannt für syslog-ng und BalaBit Shell Control Box (SCB), eine Software mit deren Hilfe anderweitig schwer zu protokollierende direkte →Zugriffe von →Administratoren auf →Betriebssystem- und →Datenbankebene protokolliert und auditiert werden können. →Audit

Balanced Score Card: (BSC) Methode um die Visionen eines Unternehmens zu implementieren. Kernpunkte dabei sind: Vorgaben (objectives), Messpunkte, Ziele, Initiativen. Jeweils unter den Gesichtspunkten: Finanzen, Kunden, interne →Geschäftsprozesse, lernen und Wachstum. Siehe http://www.valuebasedmanagement.net/methods_balanced scorecard.html

BAN-Verfahren: (Burrows, Abadi, Needham) formales Verfahren das mit formaler Logik die Sicherheit eines →Protokolls, z.B. für →e-Banking beweisen kann

Bankensoftware: Siehe →Clark-Wilson, doppelte →Buchführung, →Gramm-Leach-Bliley Act →4-Augen-Prinzip, →Funktionstrennung

Bankgeheimnis: In den diversen Bankengesetzen verankerte →Vertraulichkeitsbestimmungen die beim →Datendiebstahl von Bankdaten (neben dem →Datenschutz) verletzt werden. Siehe →Liechtenstein-CD

Bankomat: (→ATM)

Bankomatkarte: Plastikkarte zum Abheben von Bargeld am →Bankomaten oder für direkte Bezahlung am →POS-Terminal. →Authentisierung heute in vielen Ländern (vor allem in der EU) nur über integrierte →SmartCard und →PIN (→EMV-Protokoll), im Ausland jedoch immer noch über →Magnetstreifen plus →PIN, d.h. leicht zu fälschen wenn mittels →Skimming die Informationen auf dem Magnetstreifen (→Track 2) und PIN ausgelesen wurden. Im Geschäft mit Bankomatkarte zu zahlen bedeutet Verlust der →Anonymität, so wie bei Nutzung einer Kredit- oder →Kundenkarte. Siehe →Skimming, →Secure Element

Bank run 2010: Aktion auf →Facebook bei der in ganz Europa Bankkunden am gleichen Tag ihre Bankguthaben abheben sollten um das Bankensystem zu destabilisieren. Dies ist ein Beispiel für →Slacktivism

Barcamp: (auch Unkonferenz) ein in der IT-Szene recht beliebtes Format für Tagungen und Workshops bei denen kein festes Programm vorgegeben wird, sondern die Teilnehmer zu Beginn Themenvorschläge machen zu denen dann entweder Impulsvorträge mit anschließenden Diskussionen oder einfach nur Diskussionen angeboten werden. Zum Beispiel im Zusammenhang mit →Open Government genutzt

Barcode: System zum Codieren von digitalen →Daten in gedruckter Form. Bekannt ist das Strichcodesystem von →EAN. Modernere Verfahren arbeiten 2-dimensional, können mehr Daten codieren (z.B. auf elektronischen Bahnfahrkarten) und werden immer öfter sicherheitsrelevant, siehe →Semacode

Bargeld: im Gegensatz zu →Kreditkarten und Überweisungen (sog. Giralgeld - von den Banken herausgegebenes „Buchgeld“) die Möglichkeit von anonymen Zahlungen, daher für viele Regierungen ein Dorn im Auge. In der EU müssen seit 1.1.2008 bei Bargeldzahlungen über 15000€ die Personalien erfasst werden. In →2020 starker Trend zu kontaktlosem Bezahlen, d.h. bargeldlos, z.B. mittels →Kreditkarte oder →Bankomatkarte mit →NFC-Funktionaliltät, aber auch auf der Basis von →Smartphones (z.B. →Apple Pay, → Android Pay, →Alipay, →WeChat Pay, etc.) und auch durch die Idee von digitalen Währungen die von Zentralbanken herausgegeben werden könnten ("Central Bank Digital Currencies" (CBDC)). Zentralbanken „lieben“ bargeldlose Zahlungen da sie davon ausgehen, dass damit Geldwäsche und unversteuerte Zahlungen reduziert werden können

Basel II: (Basel II Capital Accord) durch die Bank of International Settlements eingeführtes System, nach dem alle Banken 1) Risikomanagement für sich selbst einführen müssen, auf Grund deren Ergebnisse die notwendigen Eigenkapitalwerte für diese Bank festgesetzt

werden (→Kreditrisiko, →Marktrisiko, operationelles Risiko, →AMA) und 2) Risikoüberprüfung für Bankkunden, auf Grund der die Zinssätze für Kredite für diesen Kunden festgesetzt werden

Baseline: 1) Im →Projektmanagement der Stand des Projektplans, der genehmigt wurde. In →Configuration Management (nach →ITIL) unterschiedlich gebraucht, z.B. eine zu einem gewissen Zeitpunkt vorgefundene Konfiguration.
2) Bei →Intrusion Detection Systems der Betriebszustand (z.B. Datenverkehr), der als „korrekt" aufgefasst wird

Baseline Control: Begriff aus der Informationssicherheit. →Grundschutz, die minimalen Schutzmaßnahmen, die auf jeden Fall erfüllt sein müssen. Siehe →Control

Baseline Security: →Grundschutz, der minimale Schutzmaßnahmen definiert, die auf jeden Fall erfüllt sein müssen. Siehe →Grundschutzhandbuch

Base Station: das Funkgerät das für den Betrieb eines Handymasten erforderlich ist. Dort meldet sich das Handy an und meldet seine Position an das →Home location register. Dann können Gespräche zugestellt werden

Basic Access Control: Verfahren zum Schutz der persönlichen Daten in den modernen →RFID-Pässen gegen unbefugtes Abhören. Siehe →MRZ, →ePass

Bastion Host: Bezeichnung für einen Rechner, der gegen →Angriffe besonders geschützt ist

Bayesian Analysis: statistisches Verfahren, das unter anderem in der Analyse von →E-Mails in Bezug auf →Spam eingesetzt wird. Im Rahmen von →Big Data Analysen bekommt diese Technik eine immer größere Bedeutung. http://plato.stanford.edu/entries/epistemology-bayesian/

BBB: →BigBlueButton

BBS: (Bulletin Board System) frühe Version dessen, was heute als →Chat-Funktionalität in →Messaging-Diensten integriert ist. BBS sind älter als das →Internet. Technisch versierte Menschen implementierten sie auf sog. Terminals (d.h. Text-→Bildschirme) die mittels →Modem mit →Computern verbunden waren und die mittels geeignetes Software auf den zentralen Rechnern (oft →Mainframes oder Minicomputer – die Größe typischerweise bis zu heutiger 19-Zoll-Rack-Größe) dort an Diskussionsforen teilnehmen konnten

BCD: 1) (Boot Configuration Data) Nachfolger von boot.ini beim Startup von Windows →Vista

3) (binary coded decimal) Zahlendarstellung in einigen →Computern bei denen die →Zahlendarstellung nicht wie üblich auf dem Binärsystem (‚Zweierland') beruht sondern die Zehnerstellen des Dezimalsystems jeweils in 1 Byte dargestellt wird. Wurde speziell in der Frühzeit der Computertechnik genutzt da es die Vorteile der Genauigkeit und Geschwindigkeit von ganzzahligen Darstellungen auch für Zahlen mit Dezimalstellen (z.B. Geld) liefert

BCI: (→Brain Computer Interface)

BCM: →Business Continuity Management

BCP: →Business Continuity Planing

BCP38: Best practise Dokument der Internet Engineering Task Force für zur Verhinderung von →DNS Amplification durch →Ingress Filtering. D.h. von innen im Netz eines →ISPs werden nur →IP-Pakete weitergeleitet, deren Quell-Adressen auch im internen Netz liegen

Bcrypt: spezielles →Hash Verfahren, das langsam ist und beim Einsatz zur Sicherung von →Passworten →Brute-Force →Angriffe erschwert. Siehe auch →PBKDF2, →Scrypt

BCV: (business continuity volume) spezielle Form des Disk →Mirroring zur Erhöhung der →Verfügbarkeit, siehe →split

BDC: (Backup Domain Controller) →PDC

BDS: → Breach Detection System

BDSG: →Bundesdatenschutzgesetz

Beacon: (engl. Leuchtfeuer) 1) →web beacon 2) problematische Funktionalität der →Social Networking →Website Facebook, bei der Aktivitäten, z.B. Einkäufe auf Partnersites allen Kontakten mitgeteilt werden. →Privatsphäre

BEC (Business E-Mail Compromise): →CEO Betrug

Bedrohung: (engl.threat) Umstand, der direkt oder indirekt zu einer Sicherheitsverletzung führen kann. Setzt in der Regel eine →Verwundbarkeit voraus. Oft wird fälschlicherweise →Risiko gesagt, wo Bedrohung korrekter wäre

Bedrohungsanalyse: (Threat analysis) systematische Bewertung ob die getroffenen Sicherheitsmaßnahmen für die angenommene Bedrohung ausreichend sind. Dafür muss man Annahmen über die Gegner (adversary) und ihre Fähigkeiten und Resourcen machen. So ist z.B. der Schutz gegen einen →global adversary wie die →NSA deutlich aufwendiger als gegen →Cyberkriminelle oder nur →Script Kiddies

Befehl: in der IT →Computerbefehl

Befehlssatz: die Menge der Instruktionen die bei einer bestimmten →CPU-Architektur implementiert sind.

Before image: bei →Datenbanken: Speicherung des Zustands vor einer Änderung, genutzt für die →Wiederherstellung eines früheren korrekten Stands nach Fehlern, →Undo

Behavioural advertising: Werbung die auf

der Basis von User →Tracking platziert wird, d.h. →Advertising Networks versuchen, auf der Basis des Benutzerverhaltens auf anderen Websites und seiner Suchanfragen herauszufinden, wofür sich ein Besucher interessiert und dann auf anderen →Websites die das gleiche Tracking-Unternehmen verwenden gezielt Werbung zu platzieren, siehe auch →targeted advertisment, →retargeting

Behaviour-based pricing: Möglichkeit, durch Auswertung des bisherigen Kaufverhaltens eines Kunden abzuschätzen, wie preissensitive dieser Kunde ist, d.h. ob er nur bei (anscheinenden) Sonderangeboten kauft oder ob er auch bei erhöhten Preisen „treu" bleibt („price discrimination"). Auf Grund der detaillierten Informationen die durch →data mining möglich sind, sind solche Praktiken heute möglich

Bell-LaPadula: Sicherheitsmodell hinter dem →MLS-Konzept des →Orange Books zur Erreichung von →Vetraulichkeit. Siehe →Clark-Wilson

Benchmark: vergleichende Messung, in der IT meist als Geschwindigkeitsmessung mit individuellen oder standardisierten →Programmen, z.B. LINPACK. Beim →Risikomanagement der Vergleich mit anderen Unternehmen, für die →Informationssicherheit auch durch →Mystery Activity. →ISO 27004

Benutzer: (engl. User) auch Anwender genannt. Jemand, der eine IT-Ressource (→ Rechner, →Bildschirm, →Anwendung, →Website) benutzt. Ein Benutzer sollte immer in die Sicherheitsregeln eingewiesen sein und sich vor der Nutzung →authentifizieren. Benutzer im →Internet erstellen heute sehr oft → Content und übernehmen damit auch eine juristische Verantwortung, z.B.für den →Datenschutz oder →Urheberrechte. Siehe →Identity Management, →AAA, →Provisionierung

Benutzeraccount: →Account

Benutzerfreundlichkeit: Oft als Gegensatz zur →Informationssicherheit gesehen, da viele Sicherheitsmaßnahmen zusätzlichen Aufwand erfordern (z.B. längere →Passworte), aber es gibt auch Verfahren die sicher und bequem sind, z.B. →Single Sign-On

Benutzerkennung: (engl. Username) Datenelement das eine der →Identitäten einer Person darstellt, heute oft eine →E-Mail-Adresse. Kann auch ein einfacher String sein, oft selbst gewählt. Sie stellt die Verbindung zu einem →Account her. Bei selbstgewählten Benutzerkennungen kann es sich um →Nicknames handeln. Benutzerkennungen können entweder öffentlich bekannt sein (Beispiel Nickname oder E-Mail-Adresse) oder „privat" wie die Benutzerkennung bei →e-Banking. Siehe auch →Enumeration,

Benutzerprofil: Sammlung von Informationen über →Benutzer von →Websites oder →Social Networks, die entweder vom Benutzer selbst eingegeben wurden oder durch Beobachten seines Verhaltens gesammelt wurden. Dies kann bis zur Auswertung der →E-Mail-Inhalte bei →Gmail führen. Diese Profile erlauben es Werbetreibenden, Werbung zielgruppen-orientiert zu platzieren. Siehe →Web beacon, →Web bug, →Data mining, →Vertraulichkeit, →P3P, →Datenschutz, →Privatsphäre

Benutzerrechte: →Admin-Rechte

Benutzerpsychologie: vernachlässigter Teil der Informationssicherheit, beschäftigt sich z.B. mit der Frage, warum Regeln ignoriert werden obwohl deren Sinn rational evtl. sogar verstanden wird

Best Practice: (auch Stand der Technik, state of the art)

1) vorbildliche Lösungen oder Verfahrenswiesen, die zu Spitzenleistungen führen, sind "best practice".

2) das Vorgehen, solche Verfahren zu ermitteln und für die Verbesserung der eigenen Prozesse zu nutzen, oft als Weiterführung von →Benchmarking. Best Practise ist ein pragmatisches Verfahren. Es systematisiert vorhandene Erfahrungen erfolgreicher Organisationen (oft auch Konkurrenten) oder Anwender usw., vergleicht unterschiedliche Lösungen, die in der Praxis eingesetzt werden, bewertet sie anhand betrieblicher Ziele und legt auf dieser Grundlage fest, welche Gestaltungen und Verfahrensweisen am besten zur Zielerreichung beitragen. Beispiel ist z.B. →ITIL. Siehe →Standards

Betriebsrat: muss (in Ö) bei vielen Sicherheitsmaßnahmen involviert werden, immer dann, wenn Protollierungsmaßnahmen potentiell „die Menschenwürde berühren könnten". http://sicherheitskultur.at/Eisberg_jus.htm

Betriebssystem: (engl. OS, operating system) →Programme (Steuer- und Dienstprogramme) eines Rechners, die die Funktionsfähigkeit sicherstellen und die richtige Abwicklung von Anwendungsprogrammen steuern. Die Abstimmung des Betriebssystems auf die Hardware ist wichtig. Unvermeidbare Fehler im Betriebssystem führen zu →Absturz oder →Verwundbarkeiten. Siehe →Virtualisierung

Betroffener: im →Datenschutz der von der Datenverarbeitung betroffene, engl. →„data subject", im Gegensatz zu →data controller oder →data owner. Ihm/ihr stehen die sog. →Betroffenenrechte zu

Betroffenenrechte: im →Datenschutz nach der →DSGVO die Rechte der sog. →„data subject", z.B. Recht auf Auskunft, Löschung, →Datenportabilität

Betrug: Täuschung zur Erringung eines Vorteils, siehe →Wirtschaftskriminalität. Siehe →419

Bewegungsprofil: →Standortdaten

Bezahldienste: Services im →Internet für den Austausch von Geld, z.B. beim Einkauf im Internet, oder aber auch bei Erpressungen wie →Ransomware. Bei betrügerischen Aktivitäten ist es für die Täter wichtig, dass der Dienst →anonym genutzt werden kann und nicht wie →Kreditkarten, →PayPal oder Überweisungen zurückverfolgbar ist. Anonym ist z.B. die virtuelle Währung →Bitcoin, aber auch Dienste wie →paysafecard, WebMoney, Liberty Reserve (2013 durch US-Behörden geschlossen), Robbokassa, Upay, Ukash. Siehe →e-Geld

BGP: (Border Gateway Protocol) Protokoll, das →ISPs benutzen, um Routinginformation auszutauschen. Endkunden müssen sich mit diesem Protokoll nur beschäftigen, wenn sie z.B. aus Ausfallsicherheitsgründen, eine redundante Anbindung an zwei ISPs benötigen. Designfehler im Protokoll erlauben →IP-Hijaking und andere →Angriffe

BHO: (browser helper object) →Programme, die mit dem →Webbrowser gestartet werden und zusätzliche Funktionalitäten anbieten. Wird oft für →Spyware, →Phishing und andere Schadsoftware verwendet

BIA: (→Business Impact Analyse)

BIC: (Bank Identifier Code, auch →SWIFT-code) 8-11-stelliger Code für Banken im internationalen Zahlungsverkehr (ISO 9361, mit Ländercode ISO 3366-1), verwendet bei →SWIFT und →SEPA

BigBlueButton: (BBB) →Open-Source →Webkonferenzsystem seit 2007, oft verwendet an Universitäten die dafür eigene Instanzen aufsetzen. Einige Bundesländer in D. hosten Instanzen. In 2020 (home-learning) oft durch kommerzielle Dienste ersetzt da die →Internet-Anbindung zu den Studenten dann außerhalb des eigenen Netzes liegt. Enthält viele Features wie z.B. Break-out Räume, Teilen des →Bildschirms, öffentliche und private →Chats, Integration in Lernplattformen wie Moodle, ILIAS, Chamilo, Stud.IP und OpenOLAT. Heute ist die →Software mittels →WebRTC mit jedem modernen →Webbrowser nutzbar

Big Brother: Begriff für →Überwachungsstaat, geprägt im Buch „1984“ von George Orwell (der eigentlich Eric Blair hieß). Heute genutzt als Synonum für einen Überwachungsstaat, aber auch für die Schnüffelaktivitäten von „Little Brothers“, d.h. Privatfirmen die persönliche →Daten sammeln, z.B. →Daten-Aggregatoren

Big Data: 2011 neues Schlagwort für →Data Mining. Es wurde zu Marketing Zwecken geprägt um damit eine neue Qualität das Data Mining zu bezeichnen. Dieser Begriff erweckt natürlich auch Anklänge an →Big Brother, die nicht ganz unberechtigt sind. Es gibt um die Auswertung sehr großer Datenmengen durch →Algorithmen, die auf statistischen Methoden beruhen und durch das Erkennen von Korrelationen (d.h. statistischen Zusammenhängen) auch Schlüsse auf zukünftige Ereignisse erlauben und deren Ursachen zu kennen. Sehr problematisch (und ein Missbrauch der statistischen Methoden) wird es, wenn solche Rückschlüsse auf einzelne Personen angewendet werden, z.B. um ihnen z.B. auf Grund der Analyse ihrer →Facebook-→friends und des Wohnorts Kredite oder Job-Interviews zu verweigern. Wird im Rahmen eines →SIEM auch für →Informationssicherheit eingesetzt. Ab ca. 2018 wird das Schlagwort mehr und mehr durch das neue →Data Science ersetzt. Siehe auch →Sentiment Analyse, →Big Five, →Neural Network,
http://sicherheitskultur.at/data_mining.htm

Big Five: in der Psychologie ein Persönlichkeitskonzept, bei dem für eine Person (i.d.Regel durch Fragebogen) das Ausmaß von folgenden Faktoren bestimmt wird: Neurotizismus, Extraversion, Offenheit für Erfahrungen, Gewissenhaftigkeit und Verträglichkeit. Es hat sich gezeigt, dass diese Fragebogen nicht notwendig sind, wenn die Bewerter →Zugriff z.B. auf die →Tweets oder →Facebook-Postings oder Facebook-→Likes einer Person haben. Es konnte z.B. gezeigt werden, dass die „Treffer-Rate“ von Familienmitgliedern schlechter ist als die Auswertung der Likes.

Ob sich auf diese Weise wirklich die Persönlichkeit beschreiben lässt, ist nicht so wichtig, die Methode wird leider trotzdem eingesetzt und erlaubt z.B. eine automatisierte Persönlichkeitsanalyse von Bewerbern deren →Social Network Auftritte bekannt sind

Bildschirm: Standard-Ausgabegeräte für →PCs, bei Laptops integriert, bei →Servern zumeist nur einmal im →Rack vorhanden. Kann über →Van Eck Strahlung zu einem Sicherheitsproblem werden (ein älterer Begriff dafür war zu Zeit der →Mainframes →Terminal. Umgangssprachlich wird bei →Webkonferenzsystemen von „Bildschirm-Teilen“ gesprochen wenn ein Teilnehmer die Inhalte eines seiner Anwendungsfensters „free gibt“. Wenn beim Anlegen von öffentlichen Web-Events Fehler gemacht werden, so kann es zum →Zoom-Bombing kommen

Bildschirmschoner: →Programm, das automatisch aktiviert wird wenn ein →Rechner eine bestimmte Zeit inaktiv ist. Die Reaktivierung des Rechners kann über →Passwort geschützt werden. Installation dieses Programmes selbst kann aber zu →Schadsoftware führen

Bildschirmsperre: Sperren (manuell oder automatisiert) eines →Rechners (oder →Handys oder →Smartphones) der nicht aktiv genutzt wird. Verhindert, bzw. erschwert unautorisierte →Zugriffe. Jedoch nicht ausreichend wenn z.B. ein →Laptop in falsche Hände fällt oder bei →Angriff via →Firewire.

Früher (vor 2000) zumeist integriert in einen →Bildschirmschoner. Heute bei →Smartphones noch wichtiger da diese viel öfter verloren gehen und oft sehr private Daten enthalten. Ca. 1/3 der Benutzer nutzt KEINE Bildschirmsperre, die Implementierungen sind unterschiedlich sicher (bzw. werden zumeist mit Trivial-→PINs wie 0000 oder 1234 gesichert und leicht zu knacken. Bei dem sog. →Swipe kann der Ablauf oft über Fettspuren auf dem Schirm gut gesehen werden, daher nicht wirklich sicher

Biometrie: alle →Authentisierungs-Verfahren, die →biometrische Merkmale zur Identifizierung einer Person heranziehen. Siehe http://www.biometrics.org/ und ftp://ftp.jrc.es/pub/EURdoc/eur21585en.pdf zur Problematik. Alle biometrischen Verfahren arbeiten analog, d.h. eine 100% →Identifizierung von Personen ist nicht möglich, dadurch entstehen →False Positive und →False Negative. Problematisch ist auch die fehlende Möglichkeit der →Revocation im Falle einer Kompromitierung. Ganz neue sind Versuche auf der Basis von →Brain Computer Interface

Biometrische Merkmale: natürliche Körpermerkmale wie →Fingerabdrücke, →Stimme, Gesichtsform (siehe →Stimm-Erkennung, →Face Recognition), Handform, Venenstruktur auf dem Handrücken oder der Handinnenseite, →Iris-Erkennung, →Retina-Erkennung oder auch der Ablauf einer Unterschrift (Form und Verlauf des Drucks auf die Unterlage). In Zukunft wird auch →DNA dazu gehören. Eine Sammlung von biometrischen Merkmalen für die Entwicklung von Algorithmen ist auf http://biosecure.it-sudparis.eu/AB/

BIOS: (Basic Input/Output System) in einem →EPROM-Chip auf dem →Motherboard eines →Rechners implementiertes →Programm, das für das Starten des →Rechners und die Kommunikation mit den Hardwarekomponenten, wie z.B. Magnetplatten, zuständig ist. Im BIOS können eine Reihe von Sicherheitstechnologien implementiert werden, so z.B. ein →Passwort-Schutz, der nichtautorisierte Veränderungen am Rechner zumindest sehr erschwert. BIOS wird abgelöst durch →UEFI. Die →NSA untersucht im Rahmen ihrer Offensive-Planungen auch, wie das BIOS der Systeme eines Gegners zerstört werden kann oder wie über →Malware im BIOS (das auf den gesamten Speicher zugreifen kann und von →Virenschutzsoftware nicht gefunden wird) Daten auf einem Rechner ausgelesen und ins →Internet übertragen werden können. Solche Angriffe sind aber zumeist recht system-spezifisch und setzen eine gewisse Einheitlichkeit voraus.

Im Rahmen der Leaks von →Edward Snowden wird bekannt, dass die →NSA mit ihrer →TAO-Abteilung sog. →Implants, d.h. →Malware für BIOS erstellt und einsetzt. Forscher haben dann herausgefunden, dass der Code von UEFI zahlreiche Schwachstellen aufweist, die zwar zum Teil korrigiert wurden, aber natürlich nicht in Systemen, die bereits produziert sind. Theoretisch wäre dies auch für bereits ausgelieferte Systeme möglich, aber es ist nicht einfach genug um vollständig automatisiert zu werden, bzw. die Hersteller haben keinen entsprechenden Kontakt zu den Geräten mehr.

Forscher konnten zeigen, dass sie sogar das spezielle System →Tails angreifen konnten, das von einem externen Device wie →DVD oder →USB-Stick gestartet wird und nur im Speicher läuft

Birthday paradox: überraschende Tatsache, dass bei 23 anwesenden Personen mit über 50% →Wahrscheinlichkeit 2 am gleichen Tag Geburtstag haben, bei 50 Personen sogar über 97 %. Wird bei →Angriffen auf →Verschlüsselungen verwendet

Bit: kleinste Speichereinheit in einem →Computer→speicher, kann entweder den Wert 0 oder 1 speichern. Nächstgrößere Einheit ist →Byte

Bitcoin: virtuelle Währung seit 2009, basierend auf →open-source software und einem →P2P-network. Das Konzept beruht auf einer →Blockchain-Technologie, bei der alle Transaktionen die je getätigt wurden in einer sehr langen Kette ewig präsent bleiben. Auf diese Weise sind alle Zahlungen immer sichtbar, aber anonym. Die Sicherheit beruht auf →digitalen Signaturen die sicherzustellen, dass das Geld nur vom Besitzer und nur einmal ausgegeben werden kann. Auf Grund der kryptographischen Basis wird BitCoin auch als →Cryptocurrency bezeichnet. (Sehr gutes Tutorial auf http://www.michaelnielsen.org/ddi/how-the-bitcoin-protocol-actually-works/)

Die Rechenoperationen zur Bestätigung von Zahlungen dienen als Basis für die Erzeugung neuer „Münzen“ wird als →Mining bezeichnet. Langwierige kryptografische Rechenoperationen (→proof-of-work) sollen die dezentrale Erzeugung von „Münzen“ („minting“ oder „mining“) aufwendig genug machen um die Versorgung mit neuem Geld begrenzen zu können. Sie erfordern eine hohe Rechenleistung. Betrüger nutzen →Zombie-Rechner/ →Botnetze dafür. So wie andere Cryptocurrencies ist Bitcoin eine starke Vereinfachung des ‚Inkassos‘ für Erpresser jeglicher Art, z.B. →Ransomware. Sie sind jedoch üblicherweise pseudonym, aber NICHT anonym. D.h. Polizeibehörden haben (mit einigem Aufwand) sehr wohl Möglichkeiten an die →Identitäten der Nutzer zu kommen.

Die Umrechnungskurse zu realen Währungen werden auf einer speziellen Börse bestimmt. Gegner behaupten, dass die Währung für Geldwäsche genutzt werden kann (so wie

→Bargeld).

Das Geld wird in sog. →Wallet gehalten. Diebstahl dieser Wallets erlaubt die missbräuchliche Nutzung und findet über Einbrüche in Bitcoin-Börsen wie Bitfloor, Bitcoinica oder Mt.Gox statt. →dDoS-→Angriffe gegen Mt.Gox haben 2013 den Kurs zum Absturz gebracht, der Dienst Instawallet mit dem Benutzer ihre Bitcoins verwalten können wurde 2013 angegriffen und die Guthaben von Kunden scheinen zum Teil verloren zu sein. Verlust der →Passworte zu Wallets führt zum Verlust des Geldes.

Die Europäische Nationalbank hat 2013 eine Studie zu Bitcoin und anderen virtual currencies verfasst. Sie sieht derzeit keinen Handlungsbedarf. Die US-Behörde FinCEN hat Guidelines erlassen, nach denen alle die mit Bitcoin zu tun haben, eine Registrierung als Money Service Business brauchen. Dies wird als teilweise Anerkennung gesehen. Mehr juristische Aspekte unter →virtual currencies.

2015 beginnen Universitäten, etablierte Firmen und Banken die Konzepte und die Mathematik hinter Bitcoin (die Blockchain) für andere Aktivitäten zu nutzen, z.B. das Protokollieren von Finanztransaktionen oder →Multi-Party Computation

Bitfrost: Sicherheitskonzept der →OLPC-Initiative

BitLocker: Technologie in Windows (ab Vista) zum →Verschlüsseln von →Festplatten →Volumes unter (optionaler) Nutzung des →TPM-Chips. (auch mit →USB-basierten Schlüsseln). Nicht verfügbar in Windows 10 home, über in Windows 10 Professional, einfach zu aktivieren. Siehe →Festplattenverschlüsselung, →Truecrypt, →Veracrypt

BITS: (Background Intelligent Transfer Service) Dienst in Windows für die Übertragung von zeit-unkritischen Daten mit niedriger Priorität. Wird u.a. für die Verteilung von →Patches und →Instant Messaging genutzt

BitTorrent: Protokoll, genutzt für →P2P →Filesharing / →Tauschbörse. Sehr dezentral, daher schwer zu überwachen. 2011 ist dies der größte Teil des illegalen Dateiaustauschs, 2012 werden 150 Mio aktive Nutzer berichtet. Die →Dateien werden nicht von einer festen Quelle geladen, sondern einzelne Fragmente von unterschiedlichen Rechnern. →ISPs versuchen zum Teil, diesen →Datenverkehr zu regulieren, u.a. weil es hohe Bandbreitenanforderungen darstellt (40 – 70%). Dies erfordert →Deep Packet Inspection. Siehe →Hadopi, →WebTorrent

Blackberry: ursprünglich spezielles Gerät nur zum Abruf von →E-Mails. Auf Grund der ursprünglich eingeschränkten Funktionalität (das Gerät enthielt ein →GSM-Handy, konnte jedoch früher nicht zum Telefonieren, sondern nur zum Austausch von E-Mails verwendet werden) war die Zahl der Sicherheits→bedrohungen reduziert und die Bedienung vergleichsweise einfach. Danach wurde die „Blackberry-, bzw. →RIM-Funktionalität" auch auf anderen →Smartphones angeboten. Positiv war die zentrale Administrierbarkeit der Geräte. 2013 suchte die Firma RIM einen Käufer, da auch die neue Version, die separate virtuelle Geräte für Privat- und Firmennutzung bietet, nicht genug angenommen wurde. 2019 obsolet

Black hat: in der IT

1) Begriff für einen →Hacker mit bösen Absichten. Dazu gehören neben den „freiberuflichen" Entwicklern von →Schadsoft-ware wie →Trojanern und →Viren auch (je nach Definition) auch die Mitarbeiter der verschiedenen Geheimdienste und der Firmen die →Zero Days verkaufen, wie →Hacking Team, FinFisher, →Vupen. Siehe auch → Wassenaar Arrangement, →white hat, →Wassenaar
2) Sicherheitskonferenz in Las Vegas, mehr oder weniger parallel mit →DEF CON

Blacklist: (BL) Verfahren im Kampf gegen → Spam und →Schadsoftware. Bekannte Spam-Versender werden über ihre →IP-Adresse auf eine Liste von gesperrten Adressen gesetzt, von denen dann kein →E-Mail akzeptiert wird. (siehe auch →DNSBL) →Virenschutz- und andere Sicherheitssoftware vergleicht alle potentiell gefährlichen Versender, bzw. Programme gegen die Liste, die ständig aktualisiert werden muss. Sicherer ist eine →Whitelist, deren Pflegeaufwand jedoch lokal durchgeführt werden muss. Siehe →Greylist

Blackout: Zusammenbruch der Stromversorgung in einem größeren Gebiet. In modernen Gesellschaften ein sehr problematisches Ereignis da ohne Strom die Informationsgesellschaft nicht funktionieren kann, aber auch eigentlich physikalische Systeme wie die Wasservorsorgung und Heizung damit nicht mehr funktionieren, siehe →Cyber-Physical Systems. Siehe auch →Smart Grid. Ursachen für Blackout sind typischerweise entweder Instabilitäten im Netz, Störungen der Hochspannungsverteilung z.B. durch Eis, aber in Zukunft möglicherweise auch →Angriffe aus dem →Internet. Dies ist Thema des Buches: Blackout – Morgen ist es zu spät.

Black Swan: extrem seltenes Ereignis mit hohem Schaden. Der Begriff wurde populär durch Nassim Nicholas Taleb in Bezug auf die Finanzkrise ab 2010 die u.a. dadurch ausgelöst wurde, dass das Platzen der Immobilienblase in den USA nicht berücksichtigt worden war. Das Ignorieren von seltenen Ereignissen ist aber auch typisch für die Informationssicherheit, für Firmen z.B. in Bezug auf →APTs, für Privatleute z.B. Verlust aller ihrer Daten durch Plattencrash

Blended Threats: moderne Angriffstechnik von →Schadsoftware, z.B. kombinieren →Würmer oft viele Angriffs- und Schadmethoden: Angriffe durch Scannen nach →Schwachstellen in seiner Umgebung, Versenden von →E-Mail mit →Anhängen mit →Viren, Infektion von →Websites und Einfügen von schädlichem →Javascript-Code, Scannen nach Netzwerk-Shares auf die der Benutzer Zugriff hat, etc. Schadmethoden: Installation von →Keyloggern, →RAT zur Erzeugung eines →Trojaners, etc.

Blitzschutz: Überspannungsfilter zum Schutz elektronischer Anlagen vor induzierten Überspannungen bei Blitzeinschlägen. Dies betrifft sowohl Stromversorgung der Geräte wie auch Datenleitungen. Dabei genügt oft die Induktion durch die Ströme im Blitzableiter, um erhebliche Schäden zu verursachen. Daher sollten Blitzableiter in der Nähe von elektronischen Geräten abgeschirmt sein. Blitz ist die zweithäufigste Ursache für →Katastrophen in →Rechnerräumen

Blockchain: spezielle verteilte Datenbanktechnologie die die Grundlage für →Bitcoin (und andere →cryptocurrencies) darstellt. Das Projekt →Ethereum will auf dieser Basis →Smart Contracts implementieren, die „Turing Complete" sind, d.h. beliebige (Rechen-) Aufgaben lösen können. Fälschungssicherheit wird durch kryptographische Operationen wie →Digitale Signatur und →Proof-of-work erreicht. (Sehr gutes Tutorial auf http://www.michaelnielsen.org/ddi/how-the-bitcoin-protocol-actually-works/)

Blocking Tools: →Software die bestimmtes Verhalten verhindern soll, z.B. →Behavioural Advertising durch →Advertising Networks. Bekannt sind die beiden Produkte →Ghostery und →ADP.

Blockverschlüsselung: symmetrisches →Verschlüsselungsverfahren, bei dem Daten fester Blocklänge verschlüsselt werden, Beispiele sind →DES, →IDEA, →Blowfish

Blog: Kurzform von Weblog, Form eines Online-Tagebuchs im Internet. Autoren stellen regelmäßig, oft täglich, Beiträge mit ihren Gedanken und/oder Erlebnissen ein. Es gibt mittlerweile viele Millionen Blogs, die erfolgreichsten haben eine Leserzahl, die mit Zeitungsauflagen vergleichbar ist und einen entsprechenden Einfluss haben. Spezielle Weblog Publishing Systeme erlauben eine einfache Implementierung. Auch →SPAM, →Phishing und →Malware werden über die Kommentare von Blogs verteilt. Siehe →Twitter, →Astroturfing, →Blogosphäre

Blogosphäre: die Summe aller →Blogs, wird verwendet um auf die Möglichkeiten, aber auch die Gefahren hinzuweisen die aus der engen Verknüpfung in der Form von Communities entstehen. Unabhängig von der Frage, wie effektiv oder uneffektiv die Blogosphäre (inkl. der →social networks) wirklich ist, so wird sie von totalitären Systemen als →Bedrohung gesehen

Blowfish: symmetrischer →Algorithmus für →Blockverschlüsselung mit 128-bit Schlüssellänge, ohne →Lizenzgebühr verwendbar und gilt heute noch als sicher (2004)

Bluecode: österreichischer Zahlungsanbieter der auf der Grundlage von →EAN Codes ein Bezahlen an →Bankomatkassen erfolgreich anbietet aber in Zukunft wohl auf →QR Code wie er in China für solche Zahlungen genutzt wird umsteigen wird

Bluetooth: Technologie zum Aufbau von →wireless networks, auch für ad-hoc Vernetzungen. Es erlaubt Geschwindigkeiten von bis zu 1 Mbps und je nach Geräteklasse Reichweiten von bis zu 10 Metern (Class 2), bzw. 100 Metern (Class 1). Normalerweise besteht ein Netz aus bis zu 8 Geräten, in Zukunft werden solche →Piconets zu sog. →Scatternets verbunden werden können. Bei dem Design des Standards wurden Authentisierung (in der Form von →Pairings) und Verschlüsselung bereits integriert, daher gilt es als sicherer als die anderen Wireless-Technologien. Allerdings gibt es mittlerweile (2004) auch Angriffe auf Bluetooth. Dies zum einen auf Grund fehlerhafter Implementierungen, speziell im Handy-Bereich, zum anderen über →Social Engineering, z.B. durch Versand von →MMS und auf Grund der Permanenz der einmal gemachten Pairings. Gründungsmitglieder der Buetooth-Organisation sind Ericsson, IBM, Intel, Nokia and Toshiba. Siehe http://www.bluetooth.com/ und speziell http://www.bluetooth.com/upload/24Security_Paper.PDF →Bluejacking, →Bluesnarfing

Bluetooth Low Energy: (BLE) drahtlose Verbindung auf der Basis des Bluetooth-Protokolls bis zu 10 Metern, aber mit deutlich geringerem Stromverbrauch, deswegen auch für batterie-betriebene Geräte geeignet, z.B. die →Apple →Airtag oder bei den →Corona Apps (Corona Warn Apps) bei denen verhindert werden soll, dass der ununterbrochene Betrieb nicht die Batterie zu sehr belasten soll. Mittels BLE können auch sog. →Mesh-Netze aus vielen Geräten aufgebaut werden

Bluejacking: →Angriff auf →Bluetooth-Gerät ohne dass →Pairing notwendig ist. Über die Visitenkartenfunktion wird eine Botschaft (auch mit Link) zu dem anderen Gerät gesendet.

Blue Screen of Death: (BSOD) Seit Windows 1.0 führt ein →Absturz von MS →Windows-Systemen zu einem Schirm, auf dem der Error-Code mit einem blauen Hintergrund dargestellt wird. Für Windows 11 gibt es Gerüchte, dass dort ein schwarzer Hintergrund eingesetzt werden könnte

Bluesnarfing: →Angriff auf →Bluetooth-Gerät nach erfolgtem →Pairing (z.B. wenn das Gerät

des Opfers unbeaufsichtigt war). Damit hat der Angreifer →Zugriff auf →Daten (Adressen, Termine, getätigte Anrufe) und Funktionen des Geräts (z.B. →Handy)

BMC: (Baseboard Management Controller) →IPMI

Boleto: (Boleto Bancário, Bank-Ticket) brasilianisches System für Bezahlungen, sowohl im Internet und in Banken, Post und einigen Supermarkets. Ist seit 2015 auch Angriffsziel von Betrügern

Booter: dDoS-as-a-service Dienst um →IP-Adressen für eine begrenzte Zeit nicht erreichbar zu machen (oft auch Stresser genannt). Siehe →Denial of Service

Bootkit: spezielle Form des →Rootkits bei dem die →Schadsoftware bereits sehr früh beim Starten des Systems (boot process) geladen wird

BOSS: (BSI OSS Security Suite) vom →BSI herausgegebene CD mit →Hacking, bzw. Security Tools, z.B. →Nessus und →Ethereal

Bot: (heute zum Teil auch „artificial persona“ genannt) Bot ist Abkürzung von robot. →Programme, die im →Internet automatische Aufgaben ausführen, z.B. das Internet im Auftrag von Suchmaschinen durchsucht um die Indizes zu erstellen. Diese werden auch →Crawler genannt. Es gibt unerwünschte bots, z.B. die, welche für →Spammer das Internet nach →E-Mail-Adressen durchsuchen und →Botnets, bestehend aus →Zombie-PCs. Eine neue Form sind →Socialbots. Eine wichtige Forderung ist, dass solche Systeme sich als künstlich identifizieren sollten, denn sie können (und haben) den öffentlichen Diskurs durch massenhaftes Posten auf →Twitter oder →Facebook, aber auch durch automatisierte Eingaben an US-Abgeordnete in Wahlen und Parlamentsentscheidungen in den USA eingemischt. Auch als →Google einen Bot vorgestellt hat, der im Auftrag von Nutzern des Google Assistenten Telefonate mit Menschen führt und sich dabei nicht als Maschine zu erkennen gab wurde dies heftig kritisiert. Solche Systeme werden immer perfekter, siehe →Deep fakes, und werden (früher oder später) Menschen teuschend echt immitieren können

Siehe →Spambot, →Chatbot, →ACAP

Botnet: Netz mit vielen →Zombies. Wird seit Ende 2004 für kriminelle Aktivitäten, z.B. →dDoS und →Phishing eingesetzt. Es gibt Netze bis zu 1 Mio Rechnern (2014 auch 2 Mio Rechner), oft gesteuert über IRC →Chat Software. 2013 kommt oft auch Peer-to-Peer (→P2P)-basierte Steuerung dazu, d.h. die infizierten Systeme kommunizieren direkt mit anderen Zombies. Auf diese Weise sind die Systeme auch dann noch arbeitsfähig, wenn zentrale Control-Server (C&C Server) abgeschaltet werden. Eine weitere Entwicklung sind →TOR-basierte Botnets, die auf Grund der →Anonymisierung der →IP-Adressen sehr schwer zu bekämpfen sind.

→Microsoft hat gemeinsam mit anderen Security Firmen seit 2012 immer wieder ganze Botnets (in Millionengröße) von den Betreibern übernommen (nach Freigabe durch ein US-Gericht) und versucht dann die Betroffenen PC zu warnen. Die Übernahme und das Still-Legen eines Botnets ist nicht unproblematisch, da es bei infizierten PCs evt. zu neuen Störungen kommen kann, die theoretisch schwerwiegende Auswirkungen haben könnte, falls z.B. der infizierte PC ein →medizinisches Gerät steuert. Die Betreiber solcher Netze nennt man →Botherder. Botspy ist ein Tool zur Beobachtung von Botnetzen. Siehe →Zombienetz, →Fast flux

Botherder: Teil der sehr arbeitsteiligen Organisation der →Botnetze. Er konzentriert sich auf Aufbau und Betrieb der Netze, die er dann an →Phisher, →Spammer und andere „vermietet“. Siehe http://sicherheitskultur.at/spam.htm#zusammen

Bouncer: →Programm das im →Google Play →App Store eingesetzt wird um bösartige →Apps zu finden und zu verhindern. Dabei wird eine statische Analyse des →Quellcodes eingesetzt sowie eine Simulation der App in einer geschützten Umgebung, die jedoch →Zugriff zum →Internet hat. Bösartige Apps können Bouncer austricksen indem sie z.B. die „bösen“ Funktionalitäten erst später über einen extern steuerbaren Parameter aktivieren

BPO: (Business Process Outsourcing) Auslagern eines →Geschäftsprozesses an einen externen Anbieter. Geeignet nur für Prozesse, die nicht die Kernkompetenz eines Unternehmens berührt und wo einfache, wohl-definierte Schnittstellen zu den In-house Prozessen definiert werden können, z.B. für Logistik. Dabei ist wichtig, dass Sicherheitsaspekte durch entsprechende →SLAs geregelt werden

BPR: (Business Process Re-engineering) strukturierte Methode zur Neugestaltung von →Geschäftsprozessen. Ziel ist eine Erhöhung der Produktivität oder der Sicherheit. Siehe →Re-engineering

Brain-Computer Interface: (BCI) Geräte um →Computer durch Gehirnaktivitäten zu steuern. Dies soll vor allem für Behinderte genutzt werden, die weder →Maus noch →Tastatur nutzen können. Aber auch das Militär ist sehr interessiert. Die 2 Hauptforschungsgebiete sind 2014: Eingabe von Richtungen (z.B. rechts/links) mittels Gedanken und erkennen von interner Sprache. BCI kann in der 2. Funktion auch genutzt werden um →Privatsphäre zu verletzen. Dazu eignet sich z.B. bereits die →P300 Reaktion, die immer dann auftritt, wenn etwas wahrgenommen wird, das eine Bedeutung für die Person hat, z.B. ein ihm bekanntes Gesicht oder Objekt. Dieser

Impuls wird über ein EEG-Gerät abgegriffen und kann nicht unterdrückt werden. Er kann daher dazu genutzt werden, um an Informationen zu kommen, die die Person verheimlichen möchte. Wird auch eingesetzt um bei Behinderungen eine Interaktion zu ermöglichen, z.B. das Eingeben eines Textes durch Konzentration auf aufblitzende Buchstaben (P300 Speller).

Andere Anwendungen sind im Bereich der Computerspiele, angeboten von Firmen wie Emotiv oder NeuroSky. Dabei werden zusätzlich zu der EEG (Elektroenzephalogramm)- Funktionalität Augen- oder Stirmbewegungen übertragen. Durch solche Anwendungen sinken die Preise für die Geräte, entstehen bequeme →USB-Interfaces und Programmbibliotheken. Siehe →Quantified self, →Wearable computing, →Lifebits

Cognitive →Biometrics ist eine andere mögliche Anwendung bei der es darum geht, BCI-Geräte für →Identifizierung und →Authentisierung einzusetzen.

Es gibt auch (umstrittene) Versuche zum Einsatz bei der Verbrechensaufklärung. Mehr dazu unter →P300.

Mit BCI verwandt sind auch →Neuroprothesen. Dabei geht es um den Anschluss von Geräten an Nervenleitungen, z.B. für Cochlear Implants oder Anschlüsse an Sehnerven. BCI und diese Forschungen dienen (derzeit) primär der Hilfe für Kranke, aber natürlich ist auch das Militär an solchen Entwicklungen sehr interessiert, z.B. zum schnelleren Steuern von Waffen. Es gibt darüber hinaus auch Zielsetzungen die in Richtung →Transhumanismus gehen

Brain Drain: beschreibt den Verlust an klugen Köpfen, den Abfluss an Wissenskapital im Gegensatz zu 'Brain Gain' (Zuwachs an Wissen)

Brandeis: Louis Brandeis 1856-1941, Richter der ca. 1890 wg. der Verfügbarkeit von tragbaren Photoapparaten die im US-Recht noch immer gültigen Kernsätze zur →Privatsphäre definiert hat

Brand-Protection: Service-Angebot zum Schutz gegen →Domainnamen-Piraterie, Typo-Squatting und begrügerischen →Websites. Enthält das Entdecken von solchen Domain-Namen und deren Beseitigung, oft durch Kontakt mit dem zuständigen Registrar. Siehe →Take-down

Brandschutz: Maßnahmen zur Entdeckung und Verhinderung von Bränden, eingesetzt u.a. in →Rechnerräumen. Dies sind Brandmelder und automatische Löscher, z.B. Gas (Verdrängung des Sauerstoffs auf < 13,8% durch inerte, d.h. nicht-brennbare Gase [Argon, Stickstoff, Inergen, Argonite]), chemisch, d.h. durch Wärmeentzug aus der Flamme [HFC-227ea, HFC-23, Novec 1230]) oder mittels aktiver →Brandvermeidung. Kohlendioxid ist wegen der Personengefährdung in →Rechenzentren problematisch

Brandvermeidung: im Gegensatz zum → Brandschutz wird bei der aktiven Brandvermeidung die Entstehung des Feuers durch permanente Absenkung des Sauerstoffgehalts verhindert. Der genaue Wert ergibt sich aus der Art der brennbaren Stoffe. Arbeiten ist weiterhin möglich, eine Absenkung auf 15% entspricht ca. 3.000 Meter Höhe. Eine Gesundheitsuntersuchung für →Administratoren ist jedoch erforderlich. Siehe →Oxy Reduct

Breach Detection System: (BDS) Konzept für neues Sicherheitskonzept zur Erkennung von →targeted attacks, Erweiterung von →Intrusion Prevention System (IPS). Das System nutzt bei der Erkennung alle Schritte der sog. →kill chain, nämlich a) Erkennen der →Infektion, b) Erkennen des „callback“ zum → C&C server, c) Entdeckung →Malware die die weitere Arbeit tun soll, d) Entdeckung der Exfiltration von →Daten, e) Entdeckung der Versuche des infizierten PCs weitere Systeme zu erreichen, z.B. über →SMB und an weitere Benutzer →Credentials zu kommen. Diese Systeme lesen den Datenverkehr im Netz um diese Events zu erkennen

Brick: (engl. Backstein) in der IT wenn bei einer Änderung an einer →Firmware, z.B. →BIOS ein Zustand entsteht, bei dem das Gerät nicht wieder gestartet werden kann. 2015 wird bekannt, dass die →NSA dies als eine der Methoden im →Cyberwar betrachtet. Auch als Verb: to brick s.th. Siehe auch: over-the-air provisioning

Bring your own device: (BYOD) Konzept bei dem ein Unternehmen den Mitarbeitern freistellt, ihre eigenen Arbeitsgeräte zur Arbeit zu nutzen. Dies können →Laptops sein, →Tablets und/oder →Smartphones. Oft werden solche Konzepte unterstützt, indem die Firma einen finanziellen Zuschuss bietet. Wenn private Geräte unbekannten Sicherheitszustands auf Firmendaten zugreifen oder diese sogar speichern entstehen natürlich neue Sicherheitsherausforderungen. Dies soll z.B. für mobile Geräte durch →MDM gelöst werden, aber auch durch Desktop-→Virtualisierungen wie →Citrix oder →Terminalserver. Beim Einsatz von MDM sollten Mitarbeiter i.d.R. Einschränkungen akzeptieren, z.B. längere →Passworte, →Verschlüsselungen und das Recht auf →Remote Wipe.

Juristische Fragen die aus der Vermischung von privaten und dienstlichen Daten entstehen (z.B. private Musik) und Haftungsprobleme bei Schäden, z.B. Verantwortlichkeit bei Datenverlust durch Verlust des Geräts sind weitgehend ungeklärt. So könnten z.B. bei einer Beweissicherung von Firmendaten auch die Privatgeräte beschlagnahmt und ausgewertet werden, da sich auch dort Firmendaten befinden können. Siehe auch →Shadow-IT

Broadcast: (Rundruf)

1) →Message auf einem Netz das an alle Teilnehmer dieses Netzes gesendet wird, wird z.B. von →ARP und →DHCP verwendet wenn die Adresse des Geräts noch unbekannt ist. Broadcast-Sturm ist ein →DoS→Angriff

2) Übertragung von Mediainformationen (Ton, Bild) an viele Teilnehmer für passiven Empfang ohne Steuerungsmöglichkeit durch den Empfänger (Gegensatz zum Download oder Abruf, juristisch im Rahmen der →Urheberrechtsregelungen ein großer Unterschied). Siehe →DVB-H, →DVB-T

Browser: (kurz für Web-Browser) Software zum Betrachten von →Informationen, heute zumeist →Webbrowser, mit dessen Hilfe Inhalte auf →Websites betrachtet und navigiert werden können. Eine der wichtigsten Funktionen ist das →Rendering, d.h. die Übersetzung der →HTML-Inhalte in eine graphische Darstellung. Bekannte Webbrowser sind etwa Mozilla Firefox, Google →Chrome, Apple Safari und Microsoft Internet Explorer (jetzt Microsoft Edge). Zur Geschichte siehe →World Wide Web. Siehe auch →Javascript, →single-page application. →Verwundbarkeiten und →Schwachstellen in Webbrowsern können erhebliche Sicherheitslücken darstellen. Siehe →BHO, →BrowserID, →Man-in-the-Browser, →Cloud Browser

Browser-Fingerprint: →Fingerprint, →Device Fingerprint

Browser helper object: →BHO

BrowserID: 2011 vorgeschlagenes Verfahren für die →Authentisierung auf →Websites. Im Gegensatz zu →OpenID wird die →E-Mail-Adresse als Identifizierung genutzt und das Verfahren muss in die →Webbrowser integriert werden

Browsing: Kurzform von Web-browsing = im →World wide Web →Webseiten aufrufen. Siehe →Browser

Brute Force Angriff: Begriff der →Hackersprache. Ein 'Angriff mit roher Gewalt' ist z.B. der Versuch, mit Hilfe von Wortlisten oder durch das systematische Ausprobieren von Zeichenfolgen das →Passwort zu finden, das einem bestimmten →Hashwert entspricht. Bei einem →Dictionary Attack werden dabei nur solche Begriffe gehasht, die entweder in Wörterbüchern verschiedener Sprachen zu finden sind, oder aber bei einem der vielen Passwort-Diebstählen erbeutet wurden. Brute Force wird auch verwendet, um durch systematisches Durchsuchen aller möglichen Schlüssel verschlüsselte Dokumente zu lesen oder durch Ausprobieren aller →PINs andere Sicherungen zu unterlaufen. Dabei kommen oft auch →GPUs zum Einsatz. Siehe →Rainbow Tables. Als Verteidigung kommen extra langsame →Passwort-Hashing Algorithmen zum Einsatz

BS25999: Code of Practise for →Business Continuity Management, leider kostenpflichtig

BS 7799: British Standard, der Vorläufer von →ISO 17799

BSA: (Business Software Alliance) Vereinigung der Software-Hersteller. Verfolgt →Raubkopien und Hersteller, die mit nicht-lizenzierter Software arbeiten

BSC: →Balanced Score Card

BSI: 1. das bundesdeutsche **Bundesamt für Sicherheit in der Informationstechnik** wurde 1990 gegründet und ist der Nachfolger der deutschen Zentralstelle für das Chiffrierwesen. Das BSI berät Behörden und setzt Rahmenbedingungen für Kryptographieanwendungen in Deutschland. Daneben bietet es unter anderem auch als Dienstleistung die Bewertung, also die Zertifizierung der Sicherheitseigenschaften von informationstechnischen Systemen an. Wichtigstes Angebot ist das →Grundschutzhandbuch. http://www.bsi.de. Siehe auch →DANE
2. **British Standards Institut**, spezialisiert auf ISO 14001 Umweltmanagement, ISO 9000 Quality Management, ISO 17799 Information Security. http://www.bsi-global.com/

Buchführung, doppelte: (engl. Double Entry) wichtiges, fast 1000 Jahre altes Sicherheitsprinzip, bei dem jede Geldbewegung mit 2 Einträgen gebucht wird, deren Summe zu jedem Zeitpunkt und für jeden Geschäftsbereich Null ergeben muss. Ziel ist die Verhinderung von →Betrug durch interne Mitarbeiter. Siehe →GoB, →IFRS, →Zapper

Buddy List: in →Messaging Diensten eine Liste von Kommunikationspartnern. Wird bei Angriffen über →Instant Messaging verwendet, in dem sich →Malware an alle diese Personen versendet. Da es sich um Bekannte des Absenders handelt, besteht eine große Gefahr, dass die Datei oder der →Link akzeptiert wird

Buffer overflow: (engl. Pufferüberlauf) leider sehr häufige →Schwachstelle in →Programmen, bei der die Menge der Eingabedaten die Größe des dafür vorgesehen Speicherbereiches überschreitet und die eingelesenen Daten Programmteile überschreiben. Könnte leicht verhindert werden, indem die Größe der Eingabe immer überprüft wird. Siehe →Bug, →DEP

Bug: engl. Bezeichnung für „Wanze“ oder „Käfer“,
1) umgangssprachliche Bezeichnung für einen Fehler (bzw. unerwünschtes und unerwartetes Verhalten) eines →Programms oder →Betriebssystems. Ursache ist oft die Komplexität des IT-→Systems. Siehe →Fehler

2) In der physischen Sicherheit eine „Abhörwanze“ (dieses Zimmer ist „verwanzt“, d.h. enthält versteckte Abhörgeräte, die entweder drahtlos ihre →Daten senden (und dadurch entdeckt werden könnten), oder die Daten

speichern und für eine Abholung bereit halten

Bug bounty: Konzept, bei dem →White Hat Researcher welche neue →Verwundbarkeiten (→Zero Days), d.h. →Fehler in →Programmen in →Software entdecken, und dann im Rahmen von →Responsible →Disclosure Geld bekommen, Wird zum Teil direkt von den betroffenen Firmen angeboten, oder z.B. durch →HackerOne. Das erste Bug Bounty Programm war 1995 durch Netscape. 2015 genutzt durch →Google, →Facebook, →Microsoft, HP, Yahoo und vielen anderen (http://www.bugsheet.com/bug-bounties). Alternative für die Researcher ist der noch lukrativere Verkauf an Firmen, die →Zero Day Exploits kommerziell ankaufen und an Regierungen (z.B. →NSA oder andere Geheimdienste oder Polizeibehörden) weiterverkaufen. In beiden Fällen kann der Verkauf mit dem →Wassenaar Abkommen kollidieren.

Bugzilla: web-basiertes Tool zum Management von →Bugs, erhältlich als →Open Source

Bullet-proof Webhoster: Betreiber von →Webservern, der in Ländern ohne Auslieferungsvertrag sitzt und alle Versuche zur Sperrung von →Websites mit illegalen Aktivitäten ignoriert. Eingesetzt für →Spamming, Kinderpornographie, →Raubkopien, →Phishing-Websites, u.ä.

BULLRUN: Name der →NSA für Aktivitäten um →Verschlüsselungen leichter „knackbar" zu machen. Dazu gehört Beeinflussung von Standardisierungsgremien (z.B. Schwächung eines →Random Number Generators), von Firmen die Verschlüsselungs-Hardware oder Software herstellen (z.B. Einbau von →Backdoors) u.ä. Bekannt wird dies durch →Edward Snowden. Siehe auch →Crypto Wars

Bundesdatenschutzgesetz: (BDSG) in D. Gesetz, das die Einhaltung des Datenschutzes regelt. →Datenschutzgesetz

Bundestrojaner: →Staatstrojaner

Bürgerkarte: Erweiterung einer →Smartcard mit →digitaler Signatur durch eine Personenbindung, in Ö z.B. durch Verlinkung zum →ZMR (Melderegister)

Bürgerportale: deutsches Projekt für eine sichere Infrastruktur für →E-Mail (De-Mail) die eine vertrauliche, verbindliche und nachvollziehbare elektronische Kommunikation ermöglicht, die auch offizielle Zustellungen (Einschreiben) erlaubt. Für die →Authentifizierung wird →e-Perso eingesetzt. Bei Datenschützern umstritten

Bus: in der IT: Technologie um mehrere digitale Geräte miteinander zu vernetzen ohne dass jedes der Geräte mit jedem anderen verbunden werden muss. Dies ist die häufigste Technik und in der IT überall zu finden, Beispiele sind →USB, -→CAN, →ESB, aber auch die Verbindung zwischen dem →Motherboard eines →PCs und Komponenten wie →Grafikkarten. Bus-Systeme werden häufig auf Geschwindigkeit ausgelegt und Aspekte wie →Verschlüsselung und →Authentisierung selten implementiert

Businessethik: Anwendung der Regeln für ethisches Verhalten in der Geschäftswelt, z.B. durch Berücksichtigung aller →Stakeholder, auch →Nachhaltigkeit oder →Corporate Social Responsibility genannt. Nicht alles Verhalten was gesetzes-konform ist, ist auch ethisch, jedoch erlaubt ethisches Verhalten nur dann Gesetzesübertretungen wenn deutlich ist, dass die Gesetze unethisch sind. Ethische Fragen sind z.B. im Bereich von →responsible disclosure ein großes Thema (→ethical hacker), aber auch im Bereich →Überwachung und →AI können IT-Entwickler immer wieder mit ethischen Fragen konfrontiert sein.

Business Continuity: Aufrechterhaltung der →Geschäftsprozesse, d.h. auch des IT-Systems, durch →Risikoabschätzung und Ergreifen von Gegenmaßnahmen im Sinne von Präventivmaßnahmen. Es beinhaltet auch die Planungen für eine →Wiederherstellung der vollen EDV-Kapazität nach einem →Disaster Recovery Fall/ →Katastrophenfall. Seit 2006 gibt es →BS25999-1:2006 als Code of Practise zum Thema

Business Continuity Planung: (BCP) vorbeugende Aktivitäten zur Erzielung von →Business Continuity

Business Impact Analysis: (BIA) Schritt im Rahmen einer →Risikoanalyse. Bestimmung der Auswirkungen, die ein →Incident auf den Geschäftsbetrieb hat. Dies schließt finanzielle Auswirkungen ein, aber auch Imageschäden, juristische Aspekte, etc.

Business Intelligence: Oberbegriff für Software, die in einem Unternehmen eingesetzt wird, um Daten zu sammeln, zu speichern und zu verarbeiten - und hierdurch unternehmensorientierter sowie besser entscheiden zu können, oft verwendet im Zusammenhang mit →CRM

Business Logic Flaw: →Schwachstellen, die durch Denkfehler bei der Entwicklung von →Anwendungen entstehen. Ausgenutzt z.B. durch →Forced Browsing

Business Recovery: Aktivitäten zur möglichst schnellen →Wiederherstellung des Geschäftsbetriebs nach einer ungeplanten Unterbrechung

Business Recovery Planung: Planen und Dokumentieren von systematischen Abläufen für →Business Recovery. Die Planung ist Teil von →Business Continuity

BYOD: →Bring your own device

Byte: Anzahl von →Bits zum Speichern 1 Zeichens, nach dem Bit, die nächstgrößere Speichereinheit. Heute werden fast immer 8 bit

für 1 Byte verwendet, bei →Fernschreibern ohne Kleinbuchstaben reichten 4 bit, bei frühen Rechnern wurden auch 5 oder 6 bit verwendet. →Speichergrößen werden in Byte angegeben (z.B. KB=Kilobyte = 1024 Byte, MB=Megabyte = 1 048 576 = 1024^2, GB=Gigabyte = 1 073 741 824= 1024^3, TB=Terabyte = 1000 GB, PT=Petabyte = 1000 TB). Diese „krummen" Zahlen entstehen dadurch, dass wegen des Binärsystems für Kilo nicht wie in der Wissenschaft üblich 1000, sondern 1024 verwendet werden

Byte-Reihenfolge: →Endianness

C2: Command & Control. In der IT zumeist der →Server bei dem sich eine →Malware nach der →Infektion eines anderen →Rechners meldet um z.B. weitere →Schadsoftware nachzuladen oder →Daten zu exfiltrieren (→dataleak)

CA: (Certificate Authority) →Zertifizierungsstelle, die öffentliche →Schlüssel für digitale →Signaturen beglaubigt, d.h. sich für ihre Echtheit verbürgt. Dazu unterschreibt die CA mit ihrem geheimen Schlüssel die öffentlichen Schlüssel der Anwender und stellt bei Bedarf die signierten öffentlichen Schlüssel in einem Verzeichnis zur Verfügung. Die CA kann die dazu notwendigen Schlüsselpaare (geheimer und öffentlicher Schlüssel) auch selbst generieren. 2011 werden zahlreiche CAs, deren →Zertifikaten von →Browsern vertraut wird, angegriffen und es werden betrügerische Zertifikate erstellt, die u.a. von Regierungen für →Man-in-the-Middle →Angriffe genutzt werden. Die Überprüfung der →Identität der Antragsteller wird häufig von Registration Authorities (→RA) übernommen, die dann über eine geeignete Verbindung z.B. →Webbrowser mit →HTTPS, auf die CA zugreifen. Siehe →web-of-trust.

2011 kam es zu zahlreichen Sicherheitsverletzungen bei →Certificate Authorities, daher wird 2012 ein neues Verfahren, →Sovereign Keys, vorgeschlagen Zu den Angriffen:

http://sicherheitskultur.at/notizen_1_11.htm#iran

CAA: →Certificate Authority Authorisation

CAcert: gemeinschaftsbetriebene nicht-kommerzielle →Zertifizierungsstelle (Root-CA), die kostenfrei →X.509-Zertifikate ausstellt. Die Überprüfung der →Identität findet durch ein →web-of-trust statt

Cache: temporärer Zwischenspeicher in einem →System, in dem →Daten, die bei der Nutzung des Systems anfallen, für eine bestimmte Zeit gespeichert werden. Ziel ist, bei einem nochmaligen →Zugriff auf die gleichen Daten einen schnelleren Zugriff zu ermöglichen. Caches werden vielfältig genutzt, z.B. in →Datenbanken, →Proxys und →Webbrowsern. In letzteren stellen sie manchmal ein Sicherheitsproblem dar, da z.B. bei der Nutzung eines →Internetcafés vertrauliche Daten im Cache gespeichert sein können. Webbrowser bieten die Möglichkeit, den Cache explizit zu löschen. Siehe →Private Browsing

Cain: →open-source Tool zum Auflisten von Netzen, Cracken von →Passworten in Übertragungsprotokollen und für →Man-in-the-Middle Angriffe. Wird für →Angriffe und →Penetration Tests genutzt

California Security Breach Information Act: Gesetz (SB-1386, 2003), das Firmen und Behörden zwingt, beim Verlust von personenbezogenen Daten die Betroffenen zu informieren. Hat zu einer Welle von Informationen über solche Verletzungen geführt. Ähnliche Gesetze wurden mittlerweile in vielen US-Bundesstaaten eingeführt. Als Folge wurde →XPS entwickelt. Siehe →DLP

Call Back: historisches Verfahren der Einwahl in ein Rechnersystem oder Netz, bei der die Sicherheit bei →Zugriff per →Modem durch einen Rückruf aus dem Netz zum Rechner des EDV-Nutzers hergestellt wird. Meist in Verbindung mit →RAS genutzt. Wird heute weitgehend durch →Internet-Verbindungen und Absicherung über →VPN ersetzt

Call Center: Dienstleistungsstelle innerhalb oder außerhalb eines Unternehmens, bei der Kunden anrufen können oder von dem aus Kunden angerufen werden. Thema für Informationssicherheit da es →Rogue Call Center gibt, die gegen entsprechende Zahlung →Social Engineering Angriffe (in vielen Sprachen) durchführen

Caller ID spoofing: Vorspiegeln einer falschen Telefonnummer, z.B. um damit die Sprachbox eines anderen Teilnehmers abzuhören. Lässt sich mittels →VoIP Services sehr leicht implementieren. →Phreaking

CAN: (Controller area network) →Bus, der in modernen →Autos die Komponenten verlinkt. Wie bei jeder Bus-Kommunikation reicht Zugriff zu einer Komponente um alle anderen Komponenten am Bus zu erreichen. Siehe auch →Automobil.

CAN-Spam Act: US-Gesetz (2003) gegen das Versenden von →Spam, Inhalt z.B. das →Opt-out Prinzip. Wird generell als sehr „zahnlos" betrachtet

Canvas Fingerprinting: 2014 neues Verfahren um einzelne PCs im Netz erkennen und tracken zu können. Dabei wird ausgenutzt, dass es minimale Unterschiede gibt, wie jeder Rechner einen Text auf einem Bildschirm darstellt. Dies kann als Erkennung genutzt werden und findet auch real statt. Solche Techniken ergänzen die sog. →Evercookies

Carnivore: (wörtl. Fleischfresser) ursprünglicher Name einer Software, entwickelt für die US-Bundespolizei FBI. Damit können im →Internet transportierte →E-Mails automatisiert nach verdächtigen Begriffen durchsucht

werden. Weil 'Carnivore' dann doch zu unangenehme Assoziationen wecken könnte, wurde das Programm mittlerweile offiziell in 'Digital Collection System' umbenannt

CAP: (Chip Authentication Program) Vereinfachung des →EMV-Protokoll um unter Nutzung eines kleinen (offline) Geräts und einer →Smartcard, z.B. →Bankomatkarte, eine →2-Faktor →Authentifizierung eines →Benutzers und ein Signieren von Bank-Transaktionen durchzuführen. Es wurden →Schwachstellen im →Protokoll aufgezeigt. Eine derzeit in Ö pilotierte Implementierung heißt →CardTAN. →DPA ist eine andere Implementierung solcher Funktionalitäten

Capacity Management: nach →ITIL die Prozesse, die sicherstellen, dass alle momentanen und zukünftigen Kapazitäts- und Leistungs-Aspekte erfüllbar sind und kostenwirksam erbracht werden können

CAPPS II: (Computer Assisted Passenger Pre-Screening) US-Programm zur Überwachung (→screening) von Flugpassagieren, entwickelt durch die →TSA. Nach Protesten heute ersetzt durch → Secure Flight

Captcha: (Completely Automated Public →Turing test to tell Computers and Humans Apart) Technologie zur Unterscheidung von Rechnern (→Programmen) und Menschen. Zumeist werden dabei schwierige →OCR-Aufgaben gestellt. Eingesetzt z.B. von →Freemailern zum Erschweren von automatisierten →Spam-Angriffen. Es findet ein Wettlauf zwischen den Entwicklern neuer Captchas und →Hackern statt, die mit neuen Algorithmen diese doch „knacken“ können. Dieser Wettlauf treibt einige Gebiete im Bereich →AI voran. Außerdem werden Captchas oft auch an Menschen weitergereicht, die unter einem Vorwand dazu gebracht werden, die Aufgabe zu lösen (z.B., aber nicht nur →Mechanical Turk, →Crowdturfing). 2011 gibt es Firmen wie decaptcher.com, die das Knacken von Captchas gegen geringe Gebühr anbieten (1$ pro 1000 Captchas). Dieser Service wird i.d.Regel durch eine Mischung aus automatisierter Erkennung (AI) und Handarbeit erbracht. Seit ca. 2017 dominiert der von →Google angebotene →ReCAPTCHA Dienst immer mehr den Markt

Captive Outsourcing: →Outsourcing

Capture: beim Einsatz von Biometrie die erste Phase, bei der das →biometrische Merkmal erfasst und in ein →Template umgewandelt wird. Siehe →CBEFF

Capture&Replay:

1) →Angriff, bei der →Daten einer →Datenübertragung aufgezeichnet und später nochmals gesendet werden ohne dass der Empfänger dies als Fälschung bemerkt
2) Technik bei →Software Tests, bei der eine Sitzung aufgezeichnet wird und für →Regression Testing wiederholt wird

Capture the Flag: Form von →LAPG. In der IT-Security wird damit bezeichnet, wenn mehrere Teams versuchen, ihre eigenen IT-Systeme zu schützen und in die Systeme der anderen Spieler einzudringen. Wird auf großen Konferenzen wie DEFCON angeboten, aber auch zu Schulungszwecken

Carding: Kriminelle Aktivitäten in Bezug auf →Kreditkarten (oder →Bankomatkarten): Diebstahl der K-Daten (zumeist in großem Umfang), Handel mit diesen (Online-Börsen), dann Nutzung der Daten für Betrug (→CNP). Die Täter werden Carder genannt. Siehe →Identity Theft, →Data Leakage, →Phishing

CardSpace: (Windows CardSpace, vorm. →InfoCard) Nachfolger zu →Microsoft →Passport. →Identitätsmanagement-Client für Open-Identity-Plattform Geneva (d.h. →Federated Identity Framework wie →OpenID), mit dessen Hilfe der Benutzer in →Web definieren und kontrollieren kann, welche Informationen jede →Website über ihn sehen kann. Verwendet digitale →Signaturen und kann auch für →Authentifizierungen eingesetzt werden. Der Austausch erfolgt mittels WS-Federation →Protocol (→Microsoft/ IBM) oder →SAML

CardTAN: →CAP

Carrier-grade NAT: (CGN, CGNAT) Verfahren um mit den immer knapper werdenden →IPv4-Adressen umzugehen ohne zu →IPv6 zu wechseln. Es ist ein IPv4-Netzwerkdesign, bei welchem Netzbetreiber die Endstellen ihrer Kunden mit sog. →privaten →IP-Adressen ausstattet um diese dann über ein →NAT-Verfahren auf Betreiber-Ebene in öffentliche IPv4-Adressen zu übersetzen. In einem solchen Netz kann eingehender Datenverkehr nur begrenzt implementiert werden (z.B. eigene →Webserver - im Gegensatz zum ausgehenden Datenverkehr auf den die anderen Geräte lediglich „Antworten“ senden)

CASB: →Cloud Access Security Broker

CBDC: (Central Bank Digital Currencies) Form von →Stablecoin, eine digitale Währung. Viele staatliche Zentralbanken erwägen deren Einführung (die für Europa auf Grund des gut ausgebauten Bankensystems, siehe →SEPA nicht wirklich notwendig ist) weil in weniger entwickelten Ländern viele Bürger, aber auch kleine Unternehmen schlechten, d.h. teuren oder gar keinen →Zugang zum (speziell internationalen) Bankensystem haben. Das Überweisen von Geld in andere Länder, z.B. von Menschen die im Ausland arbeiten, ist oft mit sehr hohen Gebühren verbunden. Die Zenatralbanken wollen damit →Facebook und seiner geplanten Einführung von →Libra zuvor kommen

CBEFF: (Common Biometric Exchange File Format) angestrebte Standardisierung von

→Fingerprint Templates um eine Kompatibilität zwischen unterschiedlichen Technologien zu erreichen. Speichert nicht das Bild des Fingers, sondern ein daraus berechnetes →„Template“. Sehr relevant für Pässe mit →biometrischen Merkmalen

CBIR: (content based image retrieval) Technologie für →Suchmaschinen um Bilder am Inhalt zu erkennen, entweder durch Erkennen des Objektes oder der Person oder über Farbe und Struktur. Auch von Interesse bei der →Überwachung und →data mining in Bildarchiven. Siehe →Face Recognition

C&C Server: →Command and Control Server

CCC: 1) →Chaos Computer Club

2) →Cybercrime Convention

CCIA: (Computer & Communications Industry Association) Industrievereinigung der Computer-Industrie. Sie kümmert sich u.a. im Sicherheitsfragen und hat in diesem Zusammenhang eine Studie "CyberInsecurity: The Cost of Monopoly" herausgegeben. Ein anderes Projekt ist die Open Source and Industry Alliance (OSAIA). http://www.ccianet.org/

CCITT: (Comité Consultatif International Téléphonique et Télégraphique) Unterorganisation der →ITU, die sich um Standardisierungen kümmert. Sie ist z.B. zuständig für die „V.xxx..“ Standards der Modems oder die →“X.xxx“ Standards

CCMP: (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) Teil von →WPA, sicherer als →TKIP, verwendet →AES

CCTV: (closed-circuit television) engl. Bezeichnung für Videoüberwachung. In englischen Städten sehr verbreitet zur →Überwachung des öffentlichen Raumes. In England ist bei der Bevölkerung ein Gewöhnungseffekt eingetreten. Die Wirksamkeit bei der Verhinderung von Verbrechen konnte nicht gezeigt werden, lediglich eine Verschiebung der Orte. Siehe →Videoüberwachung. Ein spezieller Fall sind die smart →doorbells von →Amazon und →Google, die von Privaten betrieben werden aber ebenfalls Videos mit Nachbarn und/oder Polizei austauschen

cDc: →cult of the dead cow

CDMA: (Code Division Multiplex Access) modernes Verfahren zur drahtlosen Übertragung von mehreren Datenströmen auf derselben Frequenz ohne Nutzung von Zeitscheiben. Siehe →3G

CDN: (Content Delivery Network), bekannt ist →Akamai, Cloudflare, Amazon Cloudfront und viele andere. CDNs werden von Website-Betreibern eingesetzt, um statische Elemente wie z.B. Bilder (aber auch viel genutzte →JavaScript Bibliotheken wie Jquery) möglichst nah am Endkunden zu platzieren und auf diese Weise bei der eigenen Internet-Anbindung zu sparen. Zu den CDN Kunden gehören alle großen Portalbetreiber, wie z.B. auch →Google und →Facebook, vor allem aber auch →Streaming-Dienste. Bei CDN Betreibern fallen durch den Abruf der →Dateien durch die →Browser der →Benutzer große Mengen von Benutzerdaten an (z.B. welcher Browsertyp auf welchem →Betriebssystem aus welchem Land unm welche Uhrzeit auf welcher →Website welche Inhalte abgerufen hat), d.h. sie sind ein wichtiger Bestandteil der →Tracking Infrastruktur. Wenn Javascript Komponenten auf einem CDN-Cache geändert werden, so können damit andere Websites beeinflusst werden

CEO Betrug: (BEC = Business E-Mail Compromise) Begriff der eine spezielle Form von →Phishing beschreibt. Dabei bekommt der Mitarbeiter eines Unternehmens, sehr oft in der Buchhaltung ein Mail das angeblich von einem der Manager kommt und um dringende vertrauliche Zahlungen bittet. Die Schäden die dabei entstehen sind sehr oft in Millionenhöhe (Deutschland 2015 – 2018 mind. 165 Mio Euro, weltweit in 2018 mehr als 1 Milliarde USD). Siehe →Deepfake

CERT: (Computer Emergency Response Team) die ursprüngliche Organisation ist jetzt umbenannt in US-CERT, da jetzt Teil von →DHS. CERT bezeichnet Sicherheitsorganisationen, die sich zum Ziel gesetzt haben, Betreibern von Computernetzwerken oder -systemen bei der Abwehr von →Angriffen zu helfen. Sie sind Warnungs- und Ansprechstellen. Es gibt CERT-Organisationen die für Länder zuständig sind, z.B. cert.at, oder für einzelne Behörden, z.B. govcert.at oder auch nur für eine Firma. Es gibt auch spezialisierte CERTs wie →ICS-CERT, spezialisiert auf Industrial Control Systems, und CERT-EU für die Einrichtungen, und Behörden der →EU. Siehe auch http://www.cert.org/

Certificate Authority: →CA

Certificate Authority Authorisation: (CAA) Vorgeschlagenes Verfahren gegen →Man-in-the-Middle →Angriffe mit gefälschten →SSL-Zertifikaten. Dabei wird ein spezieller →DNS-record genutzt, damit der Betreiber einer →Website welche →CA berechtigt ist, SSL-Zertifikate für seine Website auszustellen. Alternative Verfahren sind →HPKP, →OCSP und →Certificate Transparency

Certificate Pinning: Da seit ca. 2011 zahlreiche →CAs kompromititiert wurden und zwar auch solche, die in →Browsern und →Betriebssystemen als „trusted“ integriert sind wird für →Smartphone →Apps und andere →Programme die nicht wie ein Browser mit vielen Gegenstellen kommunizieren müssen, sondern einen festen →Server als Gegenstelle haben, dass diese nur dem 1 Server „trusten“ und die vor-integrierten →Zertfikate ignorieren

sollen. →Google verwendet diese Technik im →Web-Browser →Chrome bei allen Zugriffen zu Google-Diensten. Auf diese Weise wurde 2011 die Fälschung von Zertifikaten bei dem niederländischen CA DigiNotar entdeckt

Certificate Practice Statement: (CPS) verbindliches Dokument eines Anbieters sicherer Zertifikate (→Certificate Authority), in dem das Vorgehen bei Zertifizierungen sowie technische und organisatorische Anforderungen an Einheiten der Zertifizierungshierarchie definiert sind. http://www.ietf.org/rfc/rfc3647.txt

Certificate Revocation List: (CRL, Widerrufsliste) veröffentlichte Liste auf der die Nummern aller gesperrten (suspendierten) und widerrufenen (revocated) Zertifikate seitens des Zertifikatsanbieters veröffentlicht werden. Weitgehend durch →OCSP ersetzt, aber auch dieses funktioniert nicht wirklich. Neuere Vorschläge sind →Certificate Transparency und →Certificate Authority Authentication. http://www.ietf.org/rfc/rfc3280.txt

Certificate Transparency: (CT) Initiative, u.a. von →Google, bei →Websites die →SSL-Zertifikate nutzen deren Details im Netz an in mehreren entsprechenden Logs verfügbar machen sollen, so dass ein →Browser prüfen kann, ob das Zertifikat das von der Website präsentiert wird, wirklich das ist, das die Website verwendet oder ob das Zertifikat durch einen →Man-in-the-Middle Angriff verändert wurde (wie das zum →Abhören durch Regierungsstellen wie die →NSA oder den iranischen Geheimdienst der Fall ist). Die Notwendigkeit ergibt sich daraus, dass den →Certificate Authorities leider nicht mehr getraut werden kann. Alternative Verfahren sind →HPKP, →Certificate Authority Authentication und →HPKP. Die früheren Verfahren wie →OCSP und →CRL gelten als gescheitert

Cfengine: →open-source Programm zum →Configuration Management auf →Unix Systemen. Configuration Management ist eine der Komponenten zum sicheren Betrieb von →Rechnern

CGI:

1. (Computer-generated imagery) Erzeugung von graphischen Darstellungen mittels →Computer-→Algorithmen, entweder für 2D Darstellungen (Bilder) oder auch in 3D für Spiele (→Games) oder Filme. 2019 auf eine neue Stufe gebracht einmal durch die sog. →Deepfakes auf der Grundlage von →Deep Learning →AI-Systemen, aber auch durch die neue Idee, animierte Versionen von verstorbenen Schauspielern in neuen Filmen einzusetzen

2.(Common Gateway Interface) historisch erste Methode, um dynamische Web-Inhalte auf einer →Website anzubieten. Dabei wird der →HTML Code der zum →Webbrowser übertragen wird, von einem →Programm (z.B. nach Abfrage einer →Datenbank) des →Webservers dynamisch erzeugt. Leider stellen Implementierungsfehler eine häufige →Schwachstelle dar

CGMS-A: (Copy Generation Management System–Analog) →Kopierschutz für analoge Videosignale, verwendet in vielen Geräten, kann mit →VEIL kombiniert werden

CGNAT, CGN: (→Carrier-grade NAT)

Challenge-Response: Verfahren, bei denen eine →Authentisierung nicht auf einem einfachen Senden eines Textstrings beruht, sondern auf einem Dialog, der für einen Angreifer keine Informationen liefert, die er für einen →Angriff ausnützen könnte. Siehe →CHAP

Challenge Handshake Authentication Protocol: →CHAP

Change Management: nach →ITIL die →Prozesse die notwendig sind, um Veränderungen an Systemen oder Prozeduren in geregelter Weise durchführen zu können. Eng verknüpft mit →Configuration Management und →Release Management

Change Request: →RfC

Chaos Computer Club: 1981 in Berlin gegründete „galaktische Gemeinschaft von Lebewesen, unabhängig von Alter, Geschlecht und Rasse sowie gesellschaftlicher Stellung, die sich grenzüberschreitend für Informationsfreiheit einsetzt“, Vereinigung von →Hackern und anderen Interessierten an Informationssicherheit, die früher durch spektakuläre Aktionen auf →Schwachstellen von Computer-Sicherheitssystemen aufmerksam machten und heute vor allem Öffentlichkeitsarbeit betreiben und jährlich einen sehr breit besuchten Kongress veranstalten (letzte Woche des Jahres). http://www.ccc.de. Wiener Zweigstelle ist https://c3w.at/

Chaos macht Schule: (CmS) Initiative des CCC in Deutschland und Österreich, bei der AktivistInnen (→Hacker) in Schulen gehen und dort über Themen wie →Privatsphäre, →Tracking, →Hacking, →Passworte, etc. aufklären. Die Mitglieder sind mehrheitlich der Meinung, dass das derzeitige Schulsystem solche Themen nicht ausreichend und qualifiziert behandelt. Anderseits ist den Aktivitsten bewusst, dass solche Privat-Initiativen nur ein ‚Tropfen auf den heißen Stein‘ sein können. Zu finden auf https://projekte.c3w.at/chaos_macht_schule oder https://www.ccc.de/de/schule

CHAP: (Challenge Handshake Authentication Protocol) Methode, um eine sichere Datenverbindung aufzubauen und ein “Replay“ eines abgehörten Passworts zu verhindern. Bei der Verbindungsanfrage schickt der Server eine Nachricht (Challenge) an den Client. Dieser übermittelt dann den Benutzernamen und die Response, die über ein →Hash-Verfahren aus dem übermittelten Challenge berechnet wird.

Wenn diese Rückmeldung mit dem vom Server berechneten Wert übereinstimmt, wird der Zugang erlaubt, ansonsten wird der Benutzer abgewiesen. Ein anderer Schutz gegen einen →Replay-Angriff ist das →OTP

Chargeback: Rückgängigmachen einer Zahlung per →Kreditkarte in dem der Kunde den Geschäftsvorgang bestreitet. Der Händler muss den Beweis der Transaktion erbringen, was bei →Internet-Transaktionen sehr schwer ist. Auf diese Weise kann mit (gestohlenen) →Kreditkarten-Daten Schaden angerichtet werden

Chat: Austausch von Nachrichten mit einem oder mehreren Personen. Implementiert als →Chatroom oder →Messaging wie z.B. →WhatsApp

Chatbot: →Bot-Implementierung auf der Grundlage von →AI mit dem Ziel der Automatisierung von →Chatroom Dialogen. Es wird behauptet, dass bis zu 85% der Teilnehmer in Yahoo-Chatrooms bereits →bots sind. Der Einsatz von Chatbots geschieht entweder mit dem Ziel der Kosteneinsparung, z.B. bei Kundenberatungen, aber auch zu kriminellen Zwecken wie Betrug oder pädophilen Kontakten. Als Gegenmaßnahme wird versucht, solche Chatbots zu erkennen

Chat Room: →Website, die eine gleichzeitige Kommunikation mehrerer Teilnehmer miteinander mittels Texteingaben ermöglicht. Ist heute Teil vieler →Social Nertworks, →Messaging Dienste, aber auch →Webmail-Implementierungen. Wird auch oft für Kundenanfragen eingesetzt, entweder automatisiert oder mit Personen besetzt. Wird im kriminellen Bereich für die Verteilung von →Spam oder →Schadsoftware verwendet, aber auch für Betrug und im Bereich Pädophilie. Siehe →Chatten, →Chatbot

Chatten: die Kommunikation von zwei oder mehreren Personen über Web Anwendungen in sog. →Chat Rooms oder auch →Social Networks, bzw. als Teil von →MMORPGs, fast immer durch Eintippen von Texten, oft stark verkürzt in Jargon wie LOL u.ä. Hierbei können auch Dateien ausgetauscht werden, bzw. →URLs vermittelt, dies kann für die →Infektion eines →Rechners durch →Malware genutzt werden. Siehe auch → Messaging Dienste

Cheat: Bei Computerspielen (→Games) Hilfestellungen, entweder in der Form von verbalen Tipps, speziellen „Codes“ die die Entwickler für das Austesten des Spieles eingebaut haben, aber z.Teil auch →Programme, die z.B. bei →MMORPGs wie →World of Warcraft, als →Bot Aktionen für den Benutzer ausführen, die das Spiel halb-automatisiert ablaufen lassen. In solchen Cheats ist oft auch →Schadcode enthalten

Checksum: (engl. Prüfsumme) redundante Prüfinformation, die die →Integrität von →Daten sicherstellen soll. Siehe →Hash, →Luhn, →CRC, →ECC, →IBAN

Chief Content Officer (CCO): Führungskraft, die sich in einem Unternehmen um die Inhalte der →Website kümmert. Siehe →Chief Information Officer

Chief Executive Officer (CEO): oberster Manager eines Unternehmens. Oftmals als 'Vorstandsvorsitzender' oder 'Geschäftsführer' bezeichnet

Chief Financial Officer (CFO): diejenige Person einer Unternehmensleitung, die sich um die Finanzplanung kümmert ('Finanzvorstand')

Chief Information Officer (CIO): Führungskraft, die für die interne Kommunikation, die verschiedenen Informationssysteme sowie für den →Internet-Auftritt eines Unternehmens verantwortlich ist. Nicht sehr häufig. Siehe →Chief Content Officer

Chief Privacy Officer (CPO): englische Rollenbezeichnung vergleichbar mit dem deutschen „Datenschutzbeauftragten“

Chief Information Security Officer (CISO): Führungskraft, die für den Bereich der Information Security verantwortlich ist

Chief Knowledge Officer (CKO): führender Mitarbeiter, dessen Aufgabe es ist, das in einem Unternehmen vorhandene Wissen zu sammeln, zu strukturieren und den Mitarbeitern zugänglich zu machen

Chief Marketing Officer (CMO): offizielle Bezeichnung für den Vorstand der Marketingabteilung eines Unternehmens

Chief Operating Officer (COO): Leiter des operativen Geschäftes, eine Funktion, die in den meisten Unternehmen vom CEO wahrgenommen wird. Gibt es einen COO, ist dieser unter dem CEO angesiedelt und kümmert sich um das laufende Geschäft, während der 'CEO' für die Visionen und Strategien zuständig ist

Chief Technology Officer (CTO): der Leiter der Abteilung für technische Entwicklung, wird manchmal auch für den Leiter der internen IT vewendet

Chip: Kurzform von Computer-Chip. Integrierter Schaltkreis, der beliebige Funktionalitäten haben kann (→Prozessor, →Arbeitsspeicher, etc.). Der Begriff wird heute sehr oft verwendet für Schaltkreise die in →Smartcards integriert sind (cryptochip), z.B. bei →Bankomat- oder →Kreditkarten, →SIMs oder →USIMs in →Handys oder →RFID oder →NFC Chips in Ausweisen, Pässen oder Bezahlsystemen

Chipkarte: →anderer Begriff für Smartcard. Beispiele für Chipkarten sind Bankomat- und Kreditkarten wenn sie wie in Europa üblich, einen Chip enthalten, aber auch Karten für Zutrittssysteme, elektronische Karten öffentliche Verkehrsmittel und viele andere. Sie können kontaktbehaftet oder kontaktlos sein, im letzteren Fall nutzen sie dann meist →NFC

Chip-n-PIN: im angelsächsischen Sprachraum der Begriff der für →Bankomat- (und andere) Karten mit →EMV-Protokoll (implementiert in einem →Secure Element) verwendet wird. Soll in den USA in 2015 eingeführt werden, Grund sind die riesigen Mengen von gestohlenen →Kreditkarten-Daten in den USA in 2012-14 (z.B. Home Depot 56 Mio, Target 100 Mio, 8 Firmen in 2012 zusammen 160 Mio)

Choice Architecture: Theorie, die beschreibt, wie Menschen und ihre Entscheidungen dadurch beeinflusst werden können, wie man ihnen die Optionen anbietet und darstellt, z.B. →Opt-In vs. →Opt-Out. Das Beeinflussen von Menschen ohne dass sie es merken wird auch unter dem Begriff „→Nudge“ beschrieben. Relevant ist dies alles bei Werbung und um Kaufentscheidungen zu erreichen, aber auch Gesellschaften zu „lenken“ (was die ursprüngliche Bedeutung von →Social Engineering ist)

ChoicePoint: US →data-aggregator, bekannt u.a. wegen "Verlusten" von personenbezogenen Daten und riesigen Datensammlungen. http://sicherheitskultur.at/privacy_loss.htm#privat

Choke Point: zentrale Resource, die eine leichtere Kontrolle von →Zugängen oder →Zugriffen ermöglicht, z.B. →Firewall oder →Proxy, gleichzeitig potentieller →Single Point of Failure

Chrome: →Webbrowser von →Google bei dem einige neue Sicherheitstechniken implementiert wurden oder geplant sind: →certificate pinning, channel binding (siehe →OAuth und →SSL). Seit ca. 202 ist dies der meistgenutzte Webbrowser

Chromebook: seit 2011 →Laptops die das →Betriebssystem Chrome OS nutzen, das auf →Linux basiert. Anwendungsprogramme laufen dort üblicherweise direkt im →Chrome →Webbrowser, →Daten werden dann nicht lokal auf dem Gerät, sondern in →Cloud-Systemen gespeichert. So werden für Office-Anwendungen üblicherweise →Programme der →G Suite, z.B. →Google Docs genutzt (→single-page Application). 2020 werden sogar →Spiele auf diese Weise angeboten (→Streaming).

Durch die Cloud-Basierung sind die Geräte leicht austauschbar, weil sie keine lokalen Daten und Einstellungen haben. Sie brauchen daher immer einen →Internetzugang. Aus →Datenschutz-Sicht ist die enge Verknüpfung mit einem →Google-Konto natürlich negativ zu bewerten. Eine Kompatibilität der Anwendungen mit →Android→Apps wird angestrebt.

Chrome OS: →Chromebook

Chromium: →Open-Source →Webbrowser auf der Basis von →Google →Chrome. Die Softwarebasis von Chromium wird auch von Microsoft Ege und Opera genutzt

chroot: (change root) →Sandbox-Technologie unter →Linux und →Unix

CIFS: (Common Internet File System) Protokoll zum Zugriff auf entfernte →Dateien und Dateisysteme, verbesserte Version des →SMB Protokolls von →Windows analog zu →NFS. Erlaubt den Zugriff auch über →Internet. Wenn die entsprechenden →Ports (139/tcp 445/tcp) durch die →Firewall erreichbar sind, kann auf diese Weise auch →Schadsoftware angreifen. http://www.microsoft.com/mind/1196/cifs.asp

CIO: (→Chief information officer)

CIP: (→Critical Infrastructure Protection)

CIPAV: (Computer and Internet Protocol Address Verifier) in den USA durch das FBI nach richterlichem Durchsuchungsbefehl eingesetzte →Forensic Software, Funktionsumfang nicht ganz klar, entspricht wohl dem von anderen →Spyware-Programmen, wird als →Trojaner auf den Zielrechner gebracht. Entspricht wohl dem →Bundestrojaner. Siehe →RFS

CISC: (Complex instruction set computer) →CPU-Architekturkonzept, heute z.B. umgesetzt in der →x86-Architektur) das erst nachträglich so benannt wurde um es vom →RISC-Konzpet abzugrenzen. Während ganz frühe →Rechner nur sehr wenige →Befehle implementiert hatten gab es ab ca. 1960 z.B. in den Großrechnern von →IBM mehr und mehr Instruktionen um auch die komplexen Speicher-Move und →BCD-Befehle in →Cobol als →Hardware zu implementieren. Die RISC-Architektur hat dann aber gezeigt, dass ein Implementieren mittels einer Befehlsfolge einfacherer Befehle schneller sein kann

CISO: (→Chief information security officer)

CISP: (Cardholder Information Security Program) Sicherheitsprogramm der Visa-→Kreditkarten-Organisation. Beruhend auf →PCI Security Standard

Citizen Lab: Organisation mit Nähe zur Universität von Toronto die mit anderen in aller Welt zusammenarbeitet und vor allem elektronische →Überwachungsaktivitäten gegen Journalisten und Oppositionelle aufdeckt

Citrix: →ICA

C-ITS: Regeln für kooperative intelligente Transportsysteme, verabschiedet durch die →ETSI. Unterschieden werden V2V (vehicle to vehicle), V2I (vehicle to infrastructure), zusammengefasst als V2X. Bevorzugte technische Lösung für die Übertragung ist →DSRC (Dedicated Short Range Communication) mit einer Reichweite von ca. 300 Metern. Car2Car ist ein Konsortium aus interessierten europäischen Firmen. Im Zusammenhang mit

→autonomen Fahrzeugen wird sehr oft auch die Vernetzung der Fahrzeuge untereinander und mit der Infrastruktur gefordert. Siehe auch →Auto und http://philipps-welt.info/autonom.htm#vernetz

Claims-based authorization: →Autorisierung {d.h. Ausstattung mit gewissen (→Zugriffs)-Rechten} auf der Basis von Claims, d.h. Behauptungen, die durch bei der Autorisierung bestätigt werden. Z.B. sind in Ö Zigaretten erst ab 18 Jahren käuflich. Um zu verifizieren, dass jemand älter als 18 Jahre ist wird bei einer claims-based Autorisierung nicht das Geburtsdatum weitergegeben, sondern nur das Faktum, dass die Person älter als 18 ist, d.h. dass die Behauptung stimmt

Clark-Wilson: Sicherheitsmodell zur Erreichung von →Integrität in Computersystemen. Wichtiges Designprinzip für →Bankensoftware. Siehe →Bell-LaPadula

Clean Desk Policy: Anweisung zum Aufräumen des Schreibtisches um das Risiko des unberechtigten Zuganges oder Zugriffes zu Informationen zu verringern und die Beschädigung oder das Entwenden von Papieren und →Datenträgern zu erschweren

Clearnet: Begriff der den Gegensatz zum →Darknet aufzeigen soll und das typische →Internet mit einer über die im Protokoll enthaltenen →IP-Adressen nur sehr begrenzten Benutzeranonymität und das von →Suchmaschinen indiziert werden

Click farm: manuelle oder automatisierte Methode um „clicks“ zu erzeugen, z.B. →Facebook „Likes“, →Twitter Follower oder →Click fraud

Click fraud: Betrug im Bereich der Werbung im →Web, z.B. durch das künstliche Erzeugen von →Zugriffen bei Bezahlmodellen wie → Pay-per-click (Werber zahlt nur für Besuche auf seiner Website) statt →Pay-per-view (Werber zahlt für das Zeigen der Anzeige). Click-fraud wird zum Teil über →Botnets und automatisierte Klicks im Hintergrund ohne dass der Benutzer dies sieht, implementiert

Clickjacking: →Angriff, bei der „böse“ Inhalte, z.B. in einem →iFrame mittels →JavaScript Inhalte einer →Webpage so verändern, dass das Klicken eines Buttons einen anderen als den geplanten Effekt hat. Eine Variante davon ist →Click-fraud, eine andere →SEO. Siehe →DOM

Clickstream: Aufzeichnung aller Clicks eines Benutzers, normalerweise auf einem →Server, bzw. bei einem →ISP. Dies kann sich auf eine einzelne →Website beziehen (und damit bei der Analyse der →Usability / Benutzbarkeit dienen) oder auch auf das Verhalten des Benutzers über einen längeren Zeitraum. Gerüchteweise werden solche Clickstream von ISPs für 40 cents pro Benutzer pro Monat angeboten

Client: 1) (engl. →Kunde) Abnehmer von Leistungen, auch intern

2) im →**Client-Server** Konzept →Programm auf dem Rechner des Anwenders (→Desktop oder →Laptop), das über ein →Protokoll mit einem entsprechenden →Server-→Programm kommuniziert. Der Client übernimmt zumindest die Darstellung auf dem Bildschirm (→Thin Client, z.B. →Citrix oder →Webbrowser), oft jedoch auch weitere lokale Verarbeitungsaufgaben (→Fat Client). Siehe →Client-side exposure

Client Puzzle Protocol: (→CPP)

Client-side exposure: →Verwundbarkeit die dadurch entsteht, dass Komponenten einer →Client-Server-Anwendung (z.B. Scripts oder Konfigurationsdateien) durch den Benutzer manipulierbar sind. Im Fall von →webbrowser-basierten Anwendungen können dies z.B. →JavaScript oder →AJAX-Teile sein. Dies ist eine Verletzung von →Trust boundaryies und stellt eine Herausforderungen von →SaaS und →Cloud computing dar.

Clone, Cloning: Herstellung einer exakten Kopie eines →Datenträgers, z.B. aus Gründen der schnellen Wiederherstellung im Katastrophenfall, zur Sicherung von Beweisen im Rahmen von →Forensics oder einen →Angriff auf eine elektronische Identifierung (→EPC, →RFID) durchzuführen. Siehe →Disaster Recovery, →Backup, →EPC

Cloud: →Cloud Computing

Cloud Access Security Broker: (CASB) →Software die von Firmen eingesetzt wird damit ihre Mitarbeiter sicher auf →Cloud Dienste wie →O365 oder →Google Docs zugreifen können. Dabei werden die Cloud-Dienste für diese Firmen so konfiguriert dass ein →Zugriff nur über dieses →Gateway möglich ist. Ziel ist es, die →Phishing →Angriffe gegen diese Mitarbeiterkonten deutlich zu erschweren. Zusätzlich können verschiedene Überwachungen zum Einsatz kommen, z.B. auch →Data Leak Prevention

CLOUD Act: US-Gesetz das US-Firmen zwingt, die Daten von nicht-US Bürgern auch dann an US Behörden zu übermitteln, wenn diese nicht in den USA gespeichert sind

Cloud Computing: (auch →Shadow IT genannt) Konzept bei dem IT-Dienste on-demand (d.h. flexibel bei Bedarf) angeboten werden. Dies können →Hardware- und/oder →Software-Infrastrukturen sein (wie Amazons →EC2), oder auch fertige Anwendungen wie bei →SaaS (z.B. →Webmail). →OpenStack ist ein Framework für die Erstellung und Administration von öffentlichen oder privaten

Cloud-Lösungen. Probleme bei der Nutzung von externen Clouds (im Gegensatz zu →Private Clouds) für Firmen sind:

- Lokalität - der Nutzer weiß nicht, auf welchem physischen System in welchem Land seine →Anwendung und seine →Daten verarbeitet und gespeichert werden. Dies ist problematisch u.a. für →Datenschutz und →Compliance. Europäisches Datenschutzrecht verlangt vom →Data Owner, d.h. vom Auftraggeber, dass er sicherstellt dass personenbezogene Daten nur dort gespeichert und verarbeitet werden, wo dies nach EU-Regeln erlaubt ist. Ähnliche Probleme ergeben sich aus dem Bankenrecht. Siehe →Localization

- Geltendes Recht – US-Anbieter haben 2011 verkündet, dass sie auch bei einer Speicherung in Europa sehr wohl US-Gesetzen wie →Patriot Act folgen müssen und die →Daten den US-Behörden zur Verfügung stellen – dies ergibt Probleme mit Datenschutz und Bankengesetzen. Wenn die Daten auf Grund eines NSL angefordert werden so darf der Betreiber den Kunden nicht einmal über die Beschlagnahme informieren.

- Verschlüsselungsimplementierung – die von Anbietern oft zitierte →Verschlüsselung besteht fast immer darin, dass die →Daten beim →Zugriff über das →Internet mit →https verschlüsselt sind und dann auf den →Servern eine symmetrische Verschlüsselung eingesetzt wird, bei denen die Schlüssel jedoch unter Kontrolle der Betreiber stehen (→SSE, z.B. Amazon Webservice S3, im Gegensatz zum AWS JDK for Java, das client-seitige Verschlüsselung erlaubt). Vom Sicherheitsaspekt akzeptabel sind lediglich solche Implementierungen, wo die →Schlüssel vom Nutzer selbst verwaltet werden (→Spider Oak)

- Sicherheitsimplementierung – die Qualität der Implementierung der Sicherheitsmaßnahmen ist nur schwer nachprüfbar und gerade wegen der Verfügbarkeit (zumeist) im →Internet extra kritisch. Möglichkeiten für eine →Auditierung sind kaum gegeben, jedoch in einigen Bereichen wegen →Compliance notwendig

- →Mandantentrennung – solche Services sind nur dann kostengünstig wenn viele Nutzer auf dem gleichen System „gehostet“ werden, die Trennung der Nutzer ist unterschiedlich gut.

- Flexibilität bei Anbieterwechsel – solche Services sind in der Regel mit „vendor-lock-in“ verbunden, ein Abzug der Daten ist auf sehr schwierig und damit teuer

- SLA – die Flexibilität der Anbieter bei Verhandlungen bzgl. →SLAs ist aus gutem Grund zumeist sehr begrenzt

Es ergeben sich bei Cloud Computing neue →Angriffsvarianten, z.B. →Colocation Angriffe. Anderseits nutzen vermehrt die Angreifer virtuelle Server in der Cloud (bezahlt über →Bitcoin oder andere anonyme Währungen) um kurzfristig große Rechenleistungen oder schnelle Internetanbindungen zur Verfügung zu haben, z.B. zum →Cracken von →Passwort-→Hashes oder für →dDoS.

Die Rechenzentren die für die großen Cloud Lösungen genutzt werden zeichnen sich i.d.R. durch erheblich größere Energie-Effektivität aus, als dies bei traditionellen Rechenzentren der Fall ist. Siehe →Grid computing, →SaaS, →Outsourcing

Der Markt für externe Cloud Lösungen ist geprägt durch eine starke Konzentrierung. 4 Anbieter (Amazon Web Services →AWS, →Microsoft, →IBM und →Google) haben zusammen mehr als die Hälfte des Umsatzes

Cloud Dienste: Systeme wie →iOS, aber auch →Windows 8 bieten sehr viele Dienste nur bei Nutzung von externen →Servern, d.h. „in-the-cloud“ an. Vorteile sind die →Verfügbarkeit der →Daten auf mehreren Geräten, Nachteil ist der Verlust an Sicherheit, da die Daten, um bequem verfügbar zu sein, i.d.Regel unverschlüsselt gespeichert werden (siehe →iCloud) Eine große Angriffsfläche bieten alle Cloud Dienste durch Funktionalitäten wie →Passwort-Recovery, da speziell die kostenlosen Dienste sich keine komplexen Prozeduren leisten können, d.h. Rücksetzen über →E-Mail an einen anderen Account, der evtl. bereits „geknackt ist. Siehe auch →Shadow-IT

Cloud file storage: Dienste die es erlauben, →Dateien im →Internet zu speichern um sie entweder über andere Geräte zuzugreifen oder mit anderen Benutzern zu teilen. Diese Dienste verschlüsseln in der Regel die →Daten auf dem Transport, haben jedoch →Zugriff auf die Daten auf den Servern (sonst könnten die Daten nicht über →Webrowser direkt dargestellt werden). Dies betrifft z.B. auch →iCloud, →Dropbox, Live Mesh, SugarSync. Alle US-Dienste stellen die Daten auch US-Behörden zur Verfügung. Sicherere Speicherdienstanbieter sind →WUALA und →SpiderOak. Sie nutzen, so wie das korrekt ist, →Schlüssel die nur auf den Endgeräten des Benutzers gespeichert sind. Dadurch haben auch →Administratoren keinen Zugriff. Siehe auch →Shadow-IT

Cloud-Gaming: Spiele, die nicht implementiert sondern im →Webbrowser gespielt werden, siehe →Gaming

Cluster: 1) Verbund gleichartiger Ressourcen. Oft werden damit Gruppen von Rechnern beschrieben, die gemeinsam eine Aufgabe erledigen. Siehe →Hochverfügbarkeit, →Load Sharing, →Hot Standby, →Fail-over

2) interne Speichereinheit auf einer →Magnetplatte, kleinste Speichereinheit für 1 Datei. Der nicht verwendete Teil des Clusters wird File →Slack genannt. Die jeweilige Größe eines Clusters hängt von der Kapazität der Magnetplatte und von der Art des Dateisystems ab (z.B. →FAT oder →NTFS).

CME: (Common Malware Enumeration) Vereinheitlichung der Bezeichnung von →Schadsoftware durch die →US-CERT

CMM: (Capability Maturity Model, auch CMMI, CMM Integration) →Best Practise-Standard im Bereich Softwareentwicklung, entwickelt durch das Software Engineering Institute (SEI) der Carnegie Mellon University. Dabei wird jede Entwicklungsorganisation in eine von 5 Klassen eingeteilt, abhängig davon, wie viele der Best Practise-Regeln implementiert werden. Derzeit (2006) sind ca. 75% auf der 1. Stufe. Siehe →CobiT, →ISO/IEC 21827, →SMM

CMMI: →CMM

CMS: (Content Management System) Software zur Unterstützung einer Implementierung und Administration von →Website-Inhalten. Ein solches System sollte z.B. den Genehmigungsfluss für neue Inhalte unterstützen und automatisch Code erzeugen, der gegen Angriffe wie →XSS oder →SQL-Injection schützt. Siehe →CSP

CNI: (critical national infrastructure) alle Systeme und Einrichtungen, die für ein geordnetes Funktionieren eines Staats notwendig sind. Neben Gesundheits-, Energie- und Wasserversorgung gehört heute auch die IT-Infrastruktur dazu. Europäische Initiativen dazu sind u.a.EPCIP und CIWIN. Siehe →Cyber Storm, →IXP, →Common mode failure

CNP: (Card not Present) bei →Kreditkarten die Zahlung im Internet oder am Telefon, d.h. ohne dass der Händler die Karte sehen und die Unterschrift prüfen kann, bzw. die Karte durch einen geeigneten Leser führen kann. Für CNP-Betrug werden Kreditkartennummern verwendet, die mittels →Cybercrime erlangt wurden. CNP-Nutzung stellt zwar (immer noch) nur einen geringen Teil der Kreditkartennutzung dar, aber einen erheblichen Teil des Kreditkartenbetrugs

CobiT: (Control Objectives for Information and related Technology) Zusammenführung von 41 nationalen und internationalen Standards aus den Bereichen Sicherheit, →Qualitätssicherung und IT, durch das „IT Governance Institute“ (ITGI, http://itgi.org), propagiert und genutzt durch die →ISACA, sehr prozessorientiert, genutzt von IT-Auditoren und geht über Sicherheitsaspekte hinaus auch zu Effizienz. Benutzt das →CMM Maturity Modell. http://www.isaca.org/cobit.htm

COCOMO: (**CO**nstructive **CO**st **Mo**del) mathematische Methode zum Abschätzung von Projektkosten und –fertigstellung auf der Basis von historischen Projektdaten und aktuellen Projekt-Charakteristiken. Kann auch für IT-Projekte genutzt werden

Code Audit: Überprüfung eines →Programms auf die Einhaltung von Programmierregeln (→Coding Styles) z.B. bzgl. Sicherheit. Siehe →Audit, →Walkthrough

Code Obfuscation: (auch program obfuscation) eine der Formen von →Obfuscation. Beschreibt das Verändern von →Programmcode so, dass durch Analyse des Codes die Funktionalität im Detail nicht erkennbar ist. Ziel ist das Erschweren von →Reverse Engineering (z.B. Verhindern von →Raubkopien bei →DRM-→Verschlüsselungen). Wichtig immer dann, wenn Programme nicth auf geschützten →Servern, sondern beim Kunden oder Nutzer ablaufen, z.B. →Java →Applets o.ä. Wird seit Anfang 2000 als Teilgebiet der →Kryptographie betrachtet, ohne dass dabei wirkliche Umsetzungen entstanden sind. Kann vermutlich auch nur in Spezialfällen wirklich gelingen.

Wird von den Cyberkriminellen auch zum Verbergen von „bösen“ →JavaScripts vor → Malware-Schutz verwendet. In diesem Fall reicht das Spektrum von einfachem →Scambling bis zu wirklicher →Verschlüsselung des Codes und der Anforderungen des dynamisch erzeugten →Schlüssels mittels →AJAX →XMLHttpRequest. Siehe →Dynamic Code Obfuscation

Code Signing: Nutzung einer digitalen →Signatur zur Sicherstellung der →Authentizität eines →Programms. Setzt ein vertrauenswürdiges Programm für die Überprüfung voraus. Siehe →Trust

Coding Styles: →Code Audit

COI: →Community of Interest

Cold Site: →Rechnerraum für →Cold Standby

Cold-Standby, Cold Site: Verfahren der →Hochverfügbarkeit, bei dem nur einer von 2 Rechnern aktiv in Produktion ist, der andere nach einer Umschaltzeit normalerweise im Minutenbereich die Last übernehmen kann. Im Gegensatz dazu →Hot Standby, siehe →Failover, →Hochverfügbarkeit

Collective Intelligence: Schlagwort für das Sammeln von →Daten vieler Menschen durch automatisierte →Überwachung (z.B. Auswertung von Standortinformation der →Handys oder Anfragen in →Suchmaschinen). Ziel ist nicht nur Lernen über das Verhalten der Einzelnen sondern auch die Interaktionen in der Gruppe, verwandt mit →Data Mining im Bereich →CRM. Problematisch sind die Auswirkungen auf die →Privatsphäre, weil die konsequente und sichere →Anonymisierung der Daten sehr schwierig ist

Collision: 1) bei →Ethernet (oder anderen →Bus-Systemen) wenn 2 Nachrichten gleich-

zeitig auf einen Kanal gegeben werden. Hat lediglich Performance Probleme

2) beim →IP-Protokoll wenn dem Endgerät einer Verbindung im Fall von →Fragmentation 2 Pakete mit gleicher Identifikation vorliegen. Kann zum Umgehen von →NIPS genutzt werden, siehe →Evasion

3) bei →Hash Algorithmen wenn unterschiedliche →Dateien den gleichen Hash-Wert ergeben

Colocation: →Server mehrerer Firmen werden in 1 →Data Center betrieben. Dabei muss auf ausreichende Trennung geachtet werden, bei preiswerten Angeboten (viele Firmen in 1 →Rack oder auf 1 physikalischen Server, →Virtualisierung) sehr schwierig zu implementieren. Extreme Form von Colocation ist →Cloud Services

Colocation Attack: Angriff der →Verwundbarkeiten ausnutzt, die sich aus gemeinsam genutzten Ressourcen ergeben, speziell bei →Cloud Services, bei denen Ressourcen dynamisch zugeordnet werden und z.B. auf neu zugewiesenen →Magnetplattenbereichen noch →Daten von anderen Firmen liegen können

Combination Key: Möglichkeit des →Link Keys bei der Herstellung eines →Pairings zwischen 2 →Bluetooth-Geräten. Combination Keys bleiben nicht permanent gespeichert. Sie sind daher sicherer, aber auch unbequemer, allerdings besteht während des Pairings auch eine erhöhte Mithörgefahr

Command and Control Server: (C&C Server) wichtiger Teil eines →Botnets und bei →APTs. In beiden Fällen versuchen sich die infizierten →PCs auf den C&C Server zu verbinden um von dort Instruktionen und weitere Programmteile zu laden, z.B. die Ziele von →dDoS-Angriffen oder →Spam-Mails. Dieser Datenverkehr wird oft über →IRC-Kanäle geführt, zum Überwinden von →Firewalls aber häufig auch über →http. Durch Unterbindung dieser Kommunikation zum C&C Server, z.B. durch →IPS, können diese →Infektionen erkannt und kann die Gefahr durch solche Angriffe reduziert werden

Common Criteria/ ISO 15408: die "Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik/ Common Criteria for Information Technology Security Evaluation (CC), Version 2.1", im August 1999 fertig gestellt. Bewertungskriterien der Sicherheit von Hardware und Software. Nachfolger des →Orange Books →TCSEC

Common Mode Failure: Ausfälle trotz →Redundanz, wenn mehrere Ressourcen gemeinsame Abhängigkeiten haben. Z.B. unabhängige →Internet-Anbindungen im gleichen Kabelschacht, gemeinsame Abhängigkeit fast aller Ressourcen von der Stromversorgung. Siehe →Single point of failure, →CNI

Community of Interest: (COI) bei →Data Mining die Menge der Kommunikationsteilnehmer, die mit einem bestimmen „Knoten" „verbunden" sind (kommuniziert haben oder verlinkt sind). Siehe →Hancock

Compartmentalization: →Sicherheitskonzept: Auftrennung eines komplexen →Systems in einzelne Teile mit Grenzen und wohl-definierten Übergängen, z.B. durch Schnittstellen

Compiler: (to compile=zusammenstellen) Siehe →Assembler

Compliance: in der Informationssicherheit: gesetzes- und vorschriftstreues Handeln (z.B. mit →SOX, →HIPAA, →Gramm-Leach-Bliley, →PCI-DSS oder anderen Vorschriften oder Gesetzen). Das Thema hat ein eigenes Kapitel in der →ISO 27001. Dort wird unter diesem Stichpunkt auch Audit behandelt. Compliant zu sein bedeutet aber nicht unbedingt, sicher zu sein. Siehe →comply or explain

„Comply or Explain": Prinzip bei Compliance Anforderungen. Es bedeutet, dass gegenüber den Auditoren entweder nachgewiesen warden muss, dass die Vorgaben eingehalten wurde oder warum die Vorgaben in diesem Fall nicht relevant sind. Für solche Erklärungen ist in der Regel eine →Risikoanalyse erforderlich

Component Failure Impact Analysis: (CFIA) Analyse der Auswirkungen von Komponentenausfällen in Hardware oder Software, ein Aspekt von →Hochverfügbarkeit

Computer: (engl.Rechner) schwammig gebrauchter Begriff, zumeist →Server oder →PC (→Desktop, →Laptop). Formal jedes Gerät, das Informationen mit Hilfe von programmierbaren →Computerbefehlen verarbeiten kann. Dazu gehören heute auch →Smartphones, →PDAs, aber eigentlich auch →Handys und viele →Embedded Systems, z.B. in konventionellen Maschinen. Alle Computer sind angreifbar, zumindest auf Grund kaum vermeidbarer →Schwachstellen in den eingesetzten →Programmen, oft auch auf anderen Wegen, z.B. →Side Channel Angriffe

Computerbefehl: →Befehlssatz, →Programmcode, →instruction

Computerkriminalität, Computer Crime: →Cybercrime

Computernetz: →Netz(werk) zur Kopplung von →Computern zwecks →Datenübertragung Siehe →Datennetz, →Netz

Computervirus: →Virus

Concurrent Copy: →Mirroring

Configuration Management: systematische Verwaltung von Informationen über alle eingesetzten Systemen, Teil des →ITIL-Konzeptes. Eng verknüpft mit →Change Management. Siehe →cfengine

Consistency Group: bei →IBM Magnetplattenspeichern eine konsistente Kopie einer Gruppe von →Magnetplatten. Siehe →Daten-

sicherung, →BCV

Consumer Profiling: (→Benutzerprofil)

Contact scraping: Technik von →Social Networking →Websites, bei denen ein Internet-Nutzer dazu gebracht wird, seine →Adressbücher (E-Mail-Kontaktliste) frei zu geben. Dann werden sehr oft im Namen des Nutzers Einladungen an alle seine Kontakte verschickt, seinem →Netzwerk beizutreten. Wenn die Kontakte dieser Datenübermittlung nicht vorher zugestimmt hatten, so stellt diese eine Verletzung des →Datenschutzes durch den Nutzer durch. Bei einem Betritt des Kontaktes wird bei diesem der Vorgang fortgesetzt

Containervirtualisierung: Methode zur Virtualisierung von Anwendungen die zwar Einschränkungen gegenüber der Hypervisor Virtualisierung hat, dafür aber sehr resourcenschonend ist da z.B. der System-kernel weiterhin geteilt wird. Diese →Programme werden dann z.B. von einer →Software wie →Kubernetes verwaltet (z.B. gestartet). Diese Programme implementieren in der Regel nur einfache Routinen – komplexe Anwendungen nutzen dann viele unterschiedliche Container für unterschiedliche Funktionen.

Continuity Management: nach →ITIL die Prozesse, die sicherstellen, dass die benötigten IT-Ressourcen auch im →Katastrophenfall verfügbar sind oder in vorher vereinbarten Zeiträumen wiederhergestellt werden können. Siehe →Business Continuity

Content: Inhalte, speziell im →Internet, im Gegensatz z.B. zu →Programmen. Die Erstellung von Content wurde noch 1995 als die größte Herausforderung des Internets gesehen, daher kauften damals IT-Firmen Media-Unternehmen wie Filmverlage oder Medienkonzerne. Zur größten Überraschung wurde dann dass die Erstellung von Content ab ca. 2000 von den →Benutzern selbst erledigt wurde, z.B. durch sog. →Homepages, d.h. privaten →Websites, →Blogs, →Profile auf →Social Networks, aber auch Entwicklungen wie →Wikipedia. Content unterliegt i.d. Regel dem Schutz durch →Urheberrechte, trotzdem werden Inhalte sehr oft (erlaubt oder unerlaubt) weiterverwendet. Weit verbreitete Regeln für die Nutzung von Inhalten sind in den →Creative Common Lizensen beschrieben, diese stehen in gewissem Gegensatz zum →Copyright. Siehe auch →Chief Content Officer, →Active Content, →Content Blocking,

Content Blocking: →Content Filtering

Content Delivery Network: (CDN), das bekannteste ist →Akamai

Content Filtering: Analyse des Inhalts von →E-Mails, →Webseiten oder anderen Daten aus dem →Internet bezüglich →Malicious Code, d.h. →Viren, →Würmer, etc. oder unerwünschten Inhalten. Dies kann im einfachsten Fall über das Erkennen von Schlüsselbegriffen oder über das Suchen von Datenpattern geschehen. Ein Spezialfall ist das Blockieren von Web-Adressen (→URL-Blocking), →UAM

Content Security Policy: (→CSP)

Content Vectoring Protocol: →CVP

Context Collapse: Effekt auf →Social Network →Websites dass →Benutzer (im Gegensatz zum realen Leben) nur mit einer →Identität auftreten und unterschiedliche Zielgruppen wie Freunde, Kollegen und Familie zumeist die gleichen Informationen bekommen. Dies führt zumeist zu einer Vermischung der „öffentlichen“ und der privaten Person und dann zu Verletzungen der →Privatsphäre. →Google+ (heute obsolet) versuchte 2011 mit „circles“ dieses Problem zu lindern, →Facebook zieht mit ähnlichen Möglichkeiten seine →Friends zu ordnen, nach

Contextual Computing: Schlagwort (2014) zur Bescheibung von Diensten wie →Google Now oder Cortana von →Microsoft bei denen aus den →Daten die ein einem →Smartphone zur Verfügung stehen und gezielt gesammelt werden (typische Aufenthaltsorte oder Ortsveränderungen des Nutzers zu den jeweiligen Tageszeiten, Inhalte von E-Mails, z.B. mit Verabredungen oder Termine aus dem Kalender in Verbindung mit externen Daten wie z.B. Wetter oder Verkehrszustand bei öffentlichen Verkehrsmitteln oder Staumeldungen) gezielte persönliche Verhaltensvorschläge gemacht werden. Da auf diese Weise die Nutzer subtil gesteuert werden (→Nudge) kann dies auch für Manipulationen missbraucht werden

Contextual Discovery: beschreibt die Situation, wo ein →Programm, typischerweise auf einem →Smartphone, selbständig Suchanfragen stellt die sich aus dem Zusammenhang (Uhrzeit, Ort des Benutzers, dem Inhalt des Kalenders für diesen Tag, Wetter, etc.) für diesen Benutzer interessant sein könnten. So würden in fremden Städten abhängig vom Interessentsprofil Sehenswürdigkeit vorgeschlagen, Geschäfte und Restaurants, alternative Verkehrswege auf Grund aktueller Staus, etc. Vorschläge können von songs bis soul mates reichen.

Um zu funktioneren setzt dies aber einen erheblichen Eingriff in die →Privatsphäre voraus und öffnet Tür und Tor für Manipilation durch meistbietende Werbetreibende

Contingency Plan: →Notfallplan, →Desaster Recovery Plan

Control: in der Informationssicherheit: →Schutzmaßnahme (oft fälschlich mit ‚Kontrolle’ übersetzt). Siehe →CobiT

Controller: (deutsch →Auftraggeber) im →Datenschutz derjenige, der den Auftrag für eine Datenverarbeitung gibt und damit die Verantwortung für die Rechtmäßigkeit übernimmt. Sein →Dienstleister muss durch ein

→SLA und regelmäßige Kontrollen zur Einhaltung der Gesetze gebracht werden

Cookie: (engl: Keks, neuerdings http-Cookie) Datensatz, den ein →Webserver auf dem Rechner eines Web-Nutzers temporär oder permanent abspeichert. Besteht aus einem Namen, einem Wert (String) und einem →URL-Pfad für den dieser Datensatz später wieder sichtbar ist. Außerdem hat ein Cookie eine definierte Lebensdauer. Cookies sind den →Domainen zugeordnet die sie gesetzt haben. Wann immer der Benutzer später mit dieser →Domain-Adresse kommuniziert, werden die entsprechenden Cookie-Daten übertragen. Mit Cookies kann ein Webserver feststellen, ob ein Web-Browser bereits früher mit ihm kommuniziert hat. Cookies helfen im positiven Fall die Benutzereinstellungen beizubehalten, können aber auch →datenschutzrechtliche Relevanz haben. Die →Art.29 Behörde der EU postuliert, dass durch das Setzen des Cookies auf dem Rechner des Benutzers eine Datenvearbeitung innerhalb der EU stattfindet, weswegen EU-Recht zur Anwendung kommt.

Man unterscheidet zwischen 1st party cookies, wenn diese von der →Website stammen von der auch die Inhalte kommen und →3rd party cookies die von anderen →Websites stammen, z.B. um →Tracking Informationen zu gewinnen. Dazu wird z.B. eine 1x1 pixel Graphik angefordert (→Web bug). Wenn diese Graphik vom Webserver geliefert wird so können →Tracking Daten an diese →Website (=→Domaine) geliefert werden und von dieser Domaine auch ein Cookie gesetzt werden. Weil (speziell 3rd Party)-Cookies immer öfter blockiert oder gesetzlich eingeschränkt werden arbeiten Tracking Firmen zunehmend mit Techniken wie →Device Fingerprints und sog. →Evercookies. Siehe →Flash Cookie, →DOM Storage. 2014 kommt neu →Canvas Fingerprinting als alternative Tracking Methode dazu.

Da die →DSGVO Einschränkungen, bzw. Zustimmungsverpflichtungen bzgl. Cookies enthält haben sich seit ca. 2020 →Cookie Walls verbreitet

Cookie Wall: eine von →Dark Pattern Technik bei denen Benutzer einer →Website entweder explizit oder implizit durch ein sehr kompliziertes Verfahren zum Vermeiden von Cookies zu Akzeptieren von Cookies „gezwungen“ werden falls sie auf die Website zugreifen wollen. Dies ist eigentlich nicht im Sinne der DSGVO. Die →ePrivacy Regulation will/sollte hier eingreifen. Der Begriff wurde analog zu →Paywall geprägt

CORBA: (Common Object Request Broker Architecture) objekt-orientierte Methode um Anwendungen auf verschiedenen inkompatiblen Systemen zu integrieren. Enthält →APIs, Kommunikationsprotokolle, Objekt- und Servicebeschreibungen. Stellt eine standardisierte Methode eines →rpc dar

Corporate Culture: Unternehmenskultur; Philosophie einer Firma, die folgende Punkte umfasst: Ziele, die über die rein wirtschaftlichen Aspekte hinausgehen, externe Kommunikation des Unternehmensbildes (→Corporate Identity), Umgang mit den Mitarbeitern, etc. →Unternehmenskultur, →Businessethik

Corporate Identity (CI): inneres und äußeres Erscheinungsbild eines Unternehmens. CI umfasst die gesamte Unternehmenskommunikation, also Marketing, Werbung, Presse- und PR-Arbeit, außerdem die Darstellung des Unternehmens durch ein einheitliches Logo und Design. Sie spiegelt die →Corporate Culture wieder und ist darauf ausgerichtet, das Image des Unternehmens zu verbessern

Corporate Social Responsibility: (CSR) Anwendung der Regeln für ethisches Verhalten in der Geschäftswelt, z.B. durch Berücksichtigung aller →Stakeholder (ISO 26000). Siehe →Nachhaltigkeit

COPPA: (Children's Online Privacy Protection Act) US-Gesetz zum Schutz der →Privatsphäre von Kindern (<13 Jahre), das US-→Websites einhalten müssen bei denen persönliche →Daten anfallen und dass dadurch auch für uns relevant ist. Kern des Problems ist die Online-Altersfeststellung (→age verification). Die Kinder nach dem Geburtstag zu fragen ist nicht unbedingt geeignet, daher wird oft eine Zustimmung der Eltern verlangt („Verifiable Parental Consent“). Dies wird zum Teil über die Eingabe einer →Kreditkarten-Nummer oder über Brief oder →Fax implementiert. Wenn das Kind unter 13 ist, so haben die Eltern Einsichts- und Löschungsrechte, wenn die Eltern >12 bestätigen so hat das Kind Schutz der Privatsphäre auch gegenüber den Eltern. Eine Studie zeigt 2011, dass viele Eltern ihren Kindern bei der Registrierung für →Facebook (FB) helfen indem sie auch 12-jährigen bestätigen, dass sie bereits 13 sind, da auf FB nur Kinder >12 mitmachen können. Durch diese falsche Altersangabe wird der vom Gesetzgeber beabsichtigte Schutz der Minderjährigen verhindert, denn Daten von Kindern <13 unterliegen einem verschärften →Datenschutz und dürfen z.B. nicht für Werbezwecke verwendet werden. http://www.coppa.org/

Copyleft: Schutzverfahren für freie Software (→Open Source) und andere Inhalte, das einen bestimmten Aspekt des →Copyrights (bzw.→Urheberrechts) in sein Gegenteil zu verkehren versucht. Copyleft erzwingt die Freiheit von Weiterbearbeitungen und Weiterentwicklungen eines freien Ur-Werkes, um dadurch die unfreie Vereinnahmung freier Werke zu verhindern. Siehe →Lizenz, →Creative Commons, →Public Domain

Copyright: bezeichnet im angloamerikani-

schen Rechtskreis das Recht, eine Sache bzw. ein Werk zu vervielfältigen, ähnlich zu, aber nicht identisch mit dem deutschen →Lizenz-, →Urheberrecht. Wird durch →DRM eingeschränkt. In D. und Ö. gibt es ein Recht auf →Privatkopie, jedoch eingeschränkt, wenn →Kopierschutz eingesetzt wird. Siehe →Copyleft, →intellectual property, →Creative Commons, →Upload-Filter

Core: (engl. Kern) einzelner →Prozessor eines Multicore-Chips. Zum Teil werden Resourcen wie L2 oder L3 cachen dabei geteilt, ansonsten entspricht ein Core einer →CPU und wird lizenztechnisch bei Software-→Lizenzen zumeist auch so bewertet

Corona Apps: während der Covid-19 Pandemie in 2020, 2021 wurden eine ganze Reihe von →Smartphone →Apps entwickelt die oft sehr unterschiedliche Funktionen aufwiesen, z.B. Corona Warn Apps, Tracing Apps, Impf-Apps, Immunitätsausweis, Kontakt-Tagebuch, Quarantäne-Tagebuch, etc.).

Wie diese Aufzählung zeigt, wurden für viele Funktionalitäten Apps vorschlagen oder entwickelt. Dabei gibt es fast immer Konflikte zwischen dem Nutzen für den Einzelnen oder der Allgemeinheit und dem →Datenschutz (weswegen von einigen Politikern der Wunsch nach weniger Datenschutz geäußert wurde). Bei den Warn-Apps geht es darum, dass eine App die Nähe von anderen Personen feststellen soll, die Dauer der Nähe und betroffene Kontakt-Personen im Fall einer Erkrankung warnen soll. Dabei wurde zuerst das Protokoll →PEPP-PT vorgeschlagen, das eine zentrale pseudonyme Speicherung aller Kontakte gebracht hätte. Gegen diese Implementierung gab es Proteste aus der Zivilgesellschaft (z.B. →CCC oder epicenter works) die als Alternative →DP-3T vorschlugen, bei dem alle Kontakte lokale gespeichert werden und eine pseudonyme Benachrichtigung erst bei einer Erkrankung passiert. Die zentrale Lösung hätte Vorteile für die Bewertung der Wirksamkeit von „Lockdown"-Maßnahmen gebracht. Entschieden hat letztendlich eine Kooperation von →Google und →Apple, die sich für DP-3T entschieden und dafür eine gemeinsames →API entwickelten (ohne die eine Umsetzung aus mehreren technischen Gründen nicht möglich gewesen wäre). Diese API soll nach Ende von Covid-19 aus Datenschutzgründen auch zentral de-aktiviert werden. Die Feststellung der Nähe läuft in der API über →Bluetooth LE (Low Energy) – was ziemlich aktuelle Geräte voraussetzt.

Das Datenschutzkonzept sieht so aus: Dezentrale Speicherung von Random-Kontakt-Token im Gerät, bei Infektion Hochladen der Token zum zentralen Server und Versand der Token an alle Geräte. Um einen Missbrauch durch falsche Infektionsmeldungen zu verhindern muss beim Setzen des Infektionsstatus eine →Identifizierung der Person durch Verknüpfung mit dem →QR-Code des positiven Tests gesichert werden. Der Qellcode der App ist →Open-Source. Die Akzeptanz ist zum Teil begrenzt, die Downloadzahlen sind für D: >24 Mio, Ö: >1,3 Mio., CH: > 2 Mio. Höhere Downloadzahlen würden eine höhere Effektivität bedeuten, anderseits sind viele Tausend Warnungen versendet worden. Andere Implementierungen z.B. in Korea oder Singapur auf anderer technischer Grundlage greifen z.B. sehr tief in den Datenschutz der Bürger ein.

Weitere Typen von Apps werden (vor allem in anderen Ländern mit geringerem Datenschutz-Niveau) rund um Covid-19 eingesetzt und noch eingesetzt werden. So wird die Registrierung von Besuchen in Restaurants oder Geschäften oft mittels →'QR-Code einscannen' umgesetzt (als Ersatz für die in D eingesetzten Zettel, oft falsch ausgefüllt und auch prompt durch die Polizei missbraucht).

Vorgeschlagen werden auch Apps die eine Impfung und/oder überstandene Krankheit dokumentieren um daran Privilegien wie freies Reisen zu knüpfen (elektronischer Impfpass, elektronischer Immunitätsnachweis). Da dies i.d.Regel zentrale Speicherung voraussetzt (in Ö Zugriff auf →ELGA) ist dies aus vielfälltigen Gründen problematisch – trotzdem wird es solche Implementierungen sicher geben

Cortana: Service auf (mittlerweile obsoleten) Windows-→Smartphones der Benutzern auf Grund von gesammelten →Daten persönliche Ratschläge für ihr Verhalten gibt (→personal assistant), Fragen beantwortet und einfache Aufgaben erledigt. Wird meist über Sprachsteuerung genutzt. Zur Problematik siehe →Contextual Computing

COS: (Card Operating System) Betriebssystem, das auf einer → Smartcard mit Kryptoprocessor implementiert ist (im Gegensatz zu reinen Speicherkarten). Beispiele sind: ISO 7816 Norm (95% Weltmarkt): CardOS (Siemens), StarCOS, StarPOS (Gieseke & Devrient), MCOS, MPCOS, MPCOS-EMV (Gemplus), PayFlex, CryptoFlex (Schlumberger), TCOS (Telesec–Deutsche Telekom), Micardo (ORGA), ca. 20 weitere Hersteller. Java (3% Weltmarkt): Cyberflex (Schlumberger), GemXpresso (Gemplus), Open Plattform (VISA). Andere Typen (2% Weltmarkt): Windows for Smartcards (→Microsoft), Multos (Maosco)

COSO: (Committee of Sponsoring Organizations, "Treadway Commission") 1985 gegründete private Initiative zur Stärkung von →Governance im Unternehmen durch →Risikomanagement und systematische Kontrollen. Veröffentlichte „Internal Integrated →Control Framework". http://www.coso.org, →SOX

CO-TRAVELLER: →NSA-Aktivität, die die

täglich gesammelten Milliarden von →Handy →Standortdaten auswertet und daraus Erkenntnisse über Verbindungen und Aktivitäten von Personen gewinnt

COTS: (Commercial off-the-shelf software or hardware) Verwendung von fertigen Lösungen im Gegensatz zur Entwicklung "in-house". Hauptsächlich zum Einsparen von Kosten verwendet, kann aber auch sicherheitsrelevant sein, da Standard-Sicherheitslösungen oft besser sind als „Selbstgeschneidertes"

CPP: (Client Puzzle Protocol) siehe →proof-of-work

CPS: 1) →Certificate Practice Statement

2) →Cyber-physical System

CPU: (central processing unit) „Herz" eines Rechners, die logischen Schaltkreise, die die →Computerbefehle „exekutieren". Heute fast immer als Multi-→Core Chip realisiert. Zusammen mit →Speicher die Hauptkomponente eines →Rechners

CPU-Architektur: Definition von →Befehlssatz, Darstellung von Zahlen (→integer, →real), →Byte-Reihenfolge, etc.. Dabei werden verschiedene Konstruktionsprinzipien unterschieden, zB. →RISC (ein Beispiel ist →ARM) oder →CISC (mit dem Beispiel →x86)

Crash: →Absturz

Crack: Knacken eines →Kopierschutzes bei Software (→Programmen, →Betriebssystem), Musik oder Videos. Die von Herstellern kostenlos verbreiteten, 30 Tage lauffähigen Testversionen von Programmen sind häufig als 'gecrackte' voll lauffähige Software im Internet zu finden, z.B. http://www.geocities.com/TimesSquare/Lair/7602/crack.html. Diese illegalen Versionen können mit →Malware infiziert sein. Siehe →Password Recovery

Cracker: 'Computerfachleute', die sich illegal Zutritt zu fremden Computernetzen verschaffen und dort →Daten und Informationen sammeln, abziehen, manipulieren oder zerstören. Siehe →Hacker, →Computerkriminalität

Cracking: Umgehen eines Schutzes, oft durch →Re-Engineering. Ziel ist sehr oft die Erstellung von →Raubkopien. Ein weiteres Ziel kann es sein, unbefugt auf →Daten oder Dienste zuzugreifen, z.B. durch Cracken der →Verschlüsselung einer →DVD (→AACS, →CSS) oder der Codes eines Satellitenempfängers.

CrashPlan: →Cloud service, siehe →Dropbox

Crawler: automatisches Programm, welches das →Internet nach bestimmten Kriterien durchsucht, z.B. als →Bot einer →Suchmaschine, oder auch um →Websites mit verwertbaren Inhalten zu finden (legal oder illegal). Siehe →ACAP

CRC: (cyclic redundancy check) Methode zur Erstellung einer →Prüfsumme zur Entdeckung von Fehlern in →Übertragungen. Nicht geeignet für kryptographische Verfahren (→Hash)

Creative Commons: Form des →Urheberrechts, bzw. →Copyrights (→intellectual property, IP) von Werken, das eine flexible Gestaltung durch den Urheber erlaubt. Von vollkommen freier Verwendung („no rights reserverd") bis zu spezifisch eingeschränkten Verwendungen („some rights reserved"). Für Software wird oft →GPL verwendet

Credentials: Bescheinigung einer Fähigkeit oder eine →Berechtigung, in der IT oft →Benutzername und →Passwort, bzw. →OTP-Token

Creditial Leak: →Passwort Leak

Credential Spraying: →Passwort Spraying

Credential Stuffing: →Passworte aus →Passwort-Leaks werden für Login-Versuche bei anderen →Webservern oder Diensten verwendet. Dies gelingt leider recht oft, weil Nutzer das kompromittierte Passwort bei mehr als einer →Website verwendet hat. Daher ist die Wiederverwendung von Passworten eine der größten Bedrohungen für →Accounts im Internet, noch größer als die Ntzung von mittelschwachen Passworten

Credit freeze: Schutzmöglichkeit in den USA gegen →Identity Theft: verhindern dass für diese Person (man selbst) eine Kreditauskunft erteilt wird oder ein Kredit vergeben

Critical Infrastructure Protection: (CIP) Schlagwort das den Schutz von technischen Systemen beschreibt, die für das Überleben einer modernen Gesellschaft notwendig sind. Dies ist vor allem Stromversorgung, die jedoch wiederum vom Funktionieren einer digitalen Kommunikation abhängt. Dazu zählt auch die Versorgung mit Lebensmitteln, die wiederum verfügbare Transportmittel und –wege voraussetzt, sowie auch Bargeldversorgung. Der Schutz kritischer Infrastruktur wurde seit ca. 2010 sehr stark zum Thema, auch bei der →EU. Ereignisse wie →Stuxnet und viele andere →Angriffe gegen →SCADA Systeme haben gezeigt, dass die Elemente der kritischen Infrastruktur Angriffsziele für Gegner eines Staates sein können und dass sie durch ihre Vernetzung im →Internet auch sehr angreifbar sind. Siehe → Cyber-physical System

Critical Records: Geschäftsdokumente (elektronisch oder in anderer Form) deren Verlust oder Veränderung ernste Auswirkungen hätte. Solche Dokumente müssen identifiziert und sorgfältig archiviert werden. Siehe →Archivierung

CRL: →Certificate Revocation List

Cross-Origin Resource Sharing: Feature in →HTML5 die es erlaubt, vom →Browser auf Browser-Objekte zuzugreifen, die von anderen

→Domains geladen wurde. Dies verhindert in →HTML4 die →Same Origin Policy. Dies wurde nun aufgeweicht um zu ermöglichen, dass Funktionalitäten von anderen →Websites leichter eingebunden werden können. Problematisch ist, dass der →Benutzer nicht gefragt wird und diese Anfragen im Context bereits bestehender Sitzungen mit allen Rechten dieses Benutzers ausgeführt werden

Cross-site scripting: →XSS

Cross-site request forgery: →CSRF

Crowdturfing: Manipulation von Meinungen zu Politik oder Produkten durch bezahlte Aktivitäten in →Social Networks, →Blogs und auf →Websites die Kommentare erlauben. Wenn damit eine einzelne Firma beauftragt wird, so läuft das unter →Astroturfing

Crowdsourcing: Vergeben von kleinen schlecht bezahlten Aufträgen die nur durch Menschen erledigt werden können (z.B. das Beurteilen von Fotos) an Internetnutzer, oft in Entwicklungsländern. Ein großer Anteil dient bösartigen Zwecken, siehe →Crowdturfing.

Crowdturfing: bösartige Nutzung von →Crowdsourcing. Ein Beispiel ist das „Knacken" von →CAPTCHAs, aber auch das Anlegen von →Accounts in →Social Networking Dienste für →Spam, Manipulation von Auktionen. Diese kommerziellen Dienste die in großem Umfang zur Verfügung stehen hebeln das Sicherheitskonzept aus, das davon ausgeht, dass böswillige Aktionen nicht gleichzeitig von einer großen Zahl von Menschen ausgeführt werden können. Ein anderer Aspekt ist das Manipulieren von Meinungen durch viele Beiträge in →Blog-Websites, →Astroturfing genannt

Crypting: bezeichnet einen Service für Anbieter von →Schadsoftware, bei dem eine solche Software gegen die heute installierte Schutzsoftware gestestet wird. Wenn die Schutzsoftware Alarm gibt, so wendet der Service spezielle →Obfuscation Software an bis die Schadsoftware nicht mehr als solche erkannt wird. Dies wird FUD (fully undetectable) genannt

CryptoParty: Treffen von Menschen mit dem Ziel, sich gegenseitig grundlegende Verschlüsselungstechniken (zum Beispiel →Tor, →VPN, →PGP, →Festplattenverschlüsselung und sichere →Messaging Dienste beizubringen. Zu finden z.B. auf https://cryptoparty.at

Crypto Wars: als 1. Crypto War werden die Bemühungen der US-Behörden bezeichnet, den Export von →Verschlüsselungssoftware (oder -hardware) dem Handel mit Waffen gleichzusetzen. Das ging so weit, dass →Webbrowser wie →Netscape in der „international edition" nur 56-bit Verschlüsselung einsetzen durften (um eine leichteres Entschlüsseln durch die →NSA zu ermöglichen). Erst 1996 wurde Software von den Regeln für Waffenhandel ausgenommen. 1991 war die →Phil Zimmermanns →PGP sichere Kryptographie weltweit verfügbar.

Ebenfalls unter Crypto War werden die Aktivitäten der →NSA verstanden, die Verschlüsselungen in →GSM →A5/1 bewusst unsicher zu machen und die Aktivitäten rund um das →BULLRUN Programm. Dies wird zum Teil als 2. Crypto War bezeichnet.

Als 3. Crypto War wird zum Teil bezeichnet, dass in 2015 nach den Terroranschlägen in Paris die Sicherheitsbehörden der westlichen Ländern ein Verbot der sicheren Verschlüsselung fordern, bzw. nur Verschlüsselung erlauben wollen, wenn die Schlüssel staatlich hinterlegt sind. Dies wird in 2015 heftig und kontrovers diskutiert und ist ein Beispiel für →IGL. Alle wichtigen Krypto-Experten sind für eine starke Verschlüsselung, die →NSA scheint zuzustimmen, das FBI möchte einfach abhören können. Seit ca. 2018 gibt es starke Bemühungen, auch innerhalb der EU, →end-to-end →Verschlüsselung zu verbieten. Als Gründe werden Terrorismus und Gewalt-gegen-Kinder (fälschlich „Kinderpornographie")

CSIRT: (Computer Security Incident Response Team) untersucht →Vorfälle der →Informationssicherheit. Siehe →Incident Management

CSI: 1) (Computer Security Institute) US-Organisation von Security Professionals, gibt jährliche Report auf der Basis von Umfragen heraus

2) (Crime Scene Investigation) →forensische Arbeiten auch im Fall von →Computercrime

CSI-Stick: kleines Gerät, das →Speicher von →Handies auslesen kann um →SMS, letzte Anrufe, Telefonbuch, etc. zu analysieren

CSP:

1) (Cryptographic Service Provider) Software (basierend auf dem MS CryptoAPI), die in Verbindung mit einem kryptographischen Gerät kryptographische Algorithmen implementiert. Wird z.B. in Verbindung mit →Smartcards eingesetzt und dann vom jeweiligen Anbieter für ein spezifisches →COS bereit gestellt

2) (Content Security Policy) neuer Versuch 2011 gegen →XSS. Über neue →http-Header kann ein →Website-Entwickler verhindern, dass mittels präparierter →URL oder →HTML-Injektion in den Inhalt eingefügter →Javascript Code ausgeführt wird. Durch die Nutzung von CSP wird die →Same Origin Policy deaktiviert. Javascript kann dann nur noch gezielt von dafür freigegebenen Quellen nachgeladen werden kann. Auch Events wie on-click müssen explizit freigegeben werden. Ineffektiv ist dieser Schutz, wenn ein →Man-in-the-Middle oder →Man-in-the-Browser diesen HTML-Tag entfernt oder wenn dem Angreifer ein persistent XSS

gelingt, d.h. der Schadcode in das →CMS einfügen kann. CSP ist 2013 in den → Browsern →Chrome und teilweise Firefox und Safari unterstützt und muss auf jeder einzelnen Website aktiv (mühsam) eingebaut werden. Letzteres kann dadurch erleichtert werden dass →CMS dies automatisieren können

Crypter: Begriff aus dem Bereich →Schadsoftware. →Software, die Schadprogramme so verschlüsselt, dass sie von →Malware-Schutz nicht erkannt werden. Dabei kommt ein Crypter Stub zum Einsatz, ein kleiner Programmteil der ausführbar ist und den Rest der Software entschlüsselt

Cryptochip: spezielle Form eines Microchips der für →kryptographische Operation und die sichere Speicherung von →Schlüsseln verwendet wird, integriert in →HSMs, aber auch →Bankomatkarten und ähnliches. Siehe →Chip

Cryptocurrency: virtuelle Währungen deren Sicherheit auf kryptografischen Operationen beruht. Beispiele sind →Bitcoin, →Dash, →Ethereum und weitere. Siehe https://en.wikipedia.org/wiki/List_of_cryptocurrencies

Cryptocurrencies werden derzeit (2019) vor allem für Spekulationen und kriminelle Aktivitäten genutzt, z.B. →Ransomware. Sie sind üblicherweise pseudonym, aber NICHT anonym. D.h. Polizeibehörden haben (mit einigem Aufwand) sehr wohl Möglichkeiten an die →Identitäten der Nutzer zu kommen. Áb ca. 2019 wird aber auch über sog. →Stablecoins nachgedacht. Dies sind kryptographische Währungen die an andere Währungen oder Währungskörbe gebunden sind. So arbeitet die chinesische Zentralbank schon eine Weile an einer Cryptowährung. Auch die von →Facebook geplante Libra wäre ein Stablecoin. Auch andere Zentralbanken erwägen solche Zahlungsoptionen ("Central Bank Digital Currencies" (CBDC)). Jede Abschaffung von →Bargeld würde jedoch eine deutliche Erhöhung der →Überwachungsmöglichkeiten bedeuten

Cryptolocker: eine der Implementierungen von →Ransomware

Cryptowährung: →Cryptocurrency

CSR: →Corporate Social Responsibility

CSRF: (Cross Site Request Forgery) →Angriff, bei dem Inhalte einer →Website →Zugriffe auf eine andere Website realisieren die z.B. in einem →E-Mail verlinkt wird oder zur gleichen Zeit im →Browser offen ist, z.B. über →HTML-IMG-Tag. Dieser Zugriff kann für den Benutzer unsichtbar eine Formular-Eingabe simulieren und damit Benutzereingaben vortäuschen die im →Account des Benutzers, z.B. im →e-Banking durchgeführt werden. Nicht zu verwechseln mit →XSS. Gut erkärt auf https://www.troyhunt.com/promiscuous-cookies-and-their-impending-death-via-the-samesite-policy/ Siehe auch →SOP, →SSRF

CSS:

1) (Cascading Style Sheet) Sprache, die Formatierungen für →HTML, →XHTML und →XML definiert. Siehe →DHTML, →DOM

2) (Content Scrambling System) →Kopierschutz auf →DVD-Medien. Seit 1999 gibt es das Programm DeCSS, mit dem sich der Schutz umgehen lässt. Siehe →DRM

3) (Cross-site scripting) →XSS

CT: →Certificate Transparency

CTF: →Capture the Flag

CTL: (certificate trust list) Liste von digitalen →Zertifikaten oder →CAs, deren →Zertifikate ohne Rückfrage von einem Clientrechner akzeptiert werden. Solche Listen werden manchmal als Ersatz für die →Directory einer →PKI dar. Die →Webbrowser enthalten eine Liste von „trusted CAs“ deren Zertifkate ohne Rückfrage beim Benutzer akzeptiert werden. Dies stellt für diese CA einen erheblichen Geschäftsvorteil da, da solche Rückfragen oft zur Verunsicherung des →Benutzers beitragen

cult of the dead cow (cDc): legendäres →Hackerkollektiv, gegründet 1984 in Texas. Berühmt/berüchtigt durch die Fernwartungssoftware →Back Orifice, die auch illegal eingesetzt wurde. Sie gelten als einer der Begründer des →Hacktivismus

cURL: (Client for URLs oder Curl URL Request Library) →Programmbibliothek und command line Tool (→Shell) zum Abruf von →Webseiten durch Eingabe der →URL. Dabei können sogar mittels →POST-request →Daten an die Webseite übertragen werden. Die Antwort erfolgt als HTML-Text, das im →Web-Browser übliche →Rendering findet nicht statt

CURL: →Programmiersprache für interaktive Internetanwendungen, nicht sehr weit genutzt. Weitgehend durch →Javascript-basierte Programmierungen ersetzt

CVE: (Common Vulnerability and Exposure) Verfahren für die eindeutige Identifizierung von entdeckten Schwachstellen. Wird von den Anbietern von →IDS Systemen und →Vulnerability Scannern verwendet, verwaltet durch →MITRE

CVP: (Content Vectoring Protocol) Verfahren zum Austausch von Daten zwischen einer →Firewall und einem → Malware-Schutz

CVSS: (Common Vulnerability Scoring System) Initiative der →FIRST, um den Schwachstellen, die mittels →CVE katalogisiert werden, ein →Rating bzgl. ihrer Gefährlichkeit zuzuordnen. Dabei wird die lokale oder entfernte Wirksamkeit, die Schwere der Auswirkungen eines Angriffs und andere Parameter berücksichtigt. Der Wert 10 ist das Maximum und 9,8 kommt immer wieder mal

vor ☹

CVV: (card verification value) von VISA verwendeter Begriff (Mastercard verwendet CVC, card verification code) für Technologie zur Reduktion von →Kreditkarten-Betrug. CVV1 ist auf der Magnetspur enthalten und für Online-Bezahlung verwendet („card present"), CVV2 3 Ziffern auf der Rückseite aufgedruckt und beim Bezahlen auf →Websites verwendet („card not present"). CVV dürfen nach den →PCI-DSS-Regeln nicht vom Händler gespeichert werden

Cyberattack: vom Militär verwendeter Fachbegriff für den Angriffsaspekt von →Cyberwar: to deliberate actions to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and/or programs resident in or transiting these systems or networks. Spionageaktivitäten wie das Eindringen in fremde Computersysteme fallen nicht unter diese Definition

Cyber Bullying: auch **Cyber Mobbing**, Nutzung moderner Kommunikationsmittel (z.B. dem →Internet) um anderen Menschen durch üble Nachrede, (anonyme) Drohungen, →Stalking, zu schaden, oft unter Ausnutzung der (vermeintlichen) →Anonymität. Siehe auch →Doxing, →SWATting, →Revenche-Porn, →Sexting

Cybercrime: ungenau definierter Begriff, 1) Angriffe gegen Rechner, d.h. Eindringen in ein IT-System, Datenveränderung oder -diebstahl, bzw. (fälschlich) 2) Verbrechen, die mittels →Computer begangen werden. Siehe →Cybercrime Economy, →eCrime, →Money Mule, →Meldestelle, →EU

Cybercrime Convention: (CCC) 2001 vom Europarat in Budapest verabschiedet. Ziel ist die Bereitstellung von Gesetzen und Vorgehensweisen zur Bekämpfung "verschiedener Arten kriminellen Verhaltens gegen →Computer Systeme, →Netzwerke und →Daten". Die Mitgliedsstaaten stellen unter Strafe: widerrechtlicher Zugriff auf Computersysteme, Abfangen von Daten, Störung der Funktionsfähigkeit, Missbrauch von →Programmen oder →Zugangsdaten, Datenfälschung. Strafbarkeit (je nach Land) meist nur bei Absicht einer Straftat oder um sich einen Vorteil oder anderen einen Nachteil zu verschaffen

Cybercrime Economy: Summe aller →Cybercrime Aktivitäten (im Sinne der 2. Definition) und den Beteiligten. Zeichnet sich durch sehr weitgehende Arbeitsteilung und hohe Professionalisierung aus. Beteiligt sind z.B. →Hacker, →Spammer, →Bullet-proof Webhoster, →Botnetz-Betreiber und Teile der →organisierten Kriminalität, →Paysafecard

Cyberfraud: Betrug beim Einkaufen im Internet. Die häufigste Form ist der →Kreditkartenbetrug, die Bestellung mit gestohlenen oder erfundenen Kartennummern. Außerdem kommt es vor, dass bezahlte Produkte z. B. nach einer Online-Auktion nicht geliefert werden. Siehe →eBay, →Fraud-Detection

Cybergrooming: Versuch von Erwachsenen im →Internet (z.B. →Chatroom, →Social Networks wie →Snapchat, →Instagram oder →TikTok), →Chat-Funktionen in Online-Spielen oder →virtual world →Plattformen wie →Second Life oder →Habbo Hotel) illegitime Kontakte mit Kindern und Jugendlichen herzustellen und entweder einen offline-Kontakt zu verabreden oder die Opfer zu →Sexting zu überreden. Eine große Herausforderung ist die →Altersverifikation, d.h. Erwachsene haben es leicht, sich als Kinder auszugeben. Es wird versucht, dieses Problem durch Beobachtung der Interaktionen zu behandeln, entweder durch menschliche Moderatoren oder auch mittels →AI (→Chatbot). Kindesmissbrauch findet aber vor allem in der Familie und im direkten Umfeld statt und nicht überwiegend nach Anbahnung im Internet

Cyber-physical System: (CPS) jede Kombination von IT-Komponenten mit physischen Elementen die physische Veränderungen hervorrufen können, z.B. die Steuerung von Industrieanlagen mittels →SCADA und →ICS Technologien. Viele dieser Systeme gehören in der Bereich Critical Infrastructure (siehe →CIP). Weitere Themen sind →Smart grid, →Home Automation, →Internet of Things, →C-IST (z.B. →V2V, →V2I), aber auch →e-Health. Diese System zeichnen sich dadurch aus, dass sie auf Grund ihrer IT-Komponenten (die meist auch vernetzt sind) leicht angreifbar sind und auf Grund der physischen Komponenten Schäden →IRL (in real live) erzeugen können

Cyberspionage: →Industriespionage imit Mittelns des →Internets. D.h. Erlangen von vertraulichen →Informationen durch Eindringen in fremde Computernetze oder Computersysteme. Ein wichtiges Mittel dabei sind → Zero Day →Attacken um damit den →Malwareschutz des Unternehemens zu unterlaufen. Eine weitere wichtige Angriffsmethode ist dabei →Social Engineering. Solche →Angriffe werden auch als →APT bezeichnet und sind, da gezielt und oft hartnäckig, auf die Dauer kaum zu verhindern. Daher wird in diesem Zusammenhang heute immer öfter eine effiziente Entdeckung der Infiltration des internen Netzes und der internen Systeme gefordert, z.B, durch →IPS. Siehe auch →Bundestrojaner, →Flame, →FinFisher/ FinSpy, →Attribution

Cybersquatting: →Domainnamen-Piraterie

Cyber Storm: Codename für eine Übung des US-→DHS zur Simulation von Angriffen auf die Infrastruktur mittels IT (→CNI). Teilnehmer u.a. →US-CERT und viele andere Organisationen

Cyberterror: falsches Schlagwort, das den Begriff →Terrorismus entwertet. Besser → Cybercrime, bzw. →Cyberwar

Cyberwar: (Cyber warfare - Krieg im Cyber-

space) Kriegsführung, die darauf abzielt, Informationsnetze und -systeme des Gegners zu überwachen, zu manipulieren (z.B. durch →Desinformation), zu stören oder auszuschalten. Beinhaltet →Angriffe auf staatliche oder private →Computernetze oder IT-→Systeme von Staaten, entweder um Druck auf diese Staaten auszuüben oder um konventionelle Kriegshandlungen zu unterstützen. Dabei ist relativ unumstritten, dass die bisherigen Regeln der Kriegsführung weiter gelten, so z.B. die Forderung nach militärischer Notwendigkeit einer bestimmten Kriegshandlung, der Proportionalität der Aktionen und der Minimierung von Kollateralschäden. Und auch das Recht auf Selbstverteidigung eines Landes wird allgemein anerkannt.

Gemessen“ werden Angriffe im Cyberspace mit vergleichbaren →kinetischen Waffen, obwohl im Cyberwar andere „Waffen“ genutzt werden, z.B. durch →dDoS oder Blockieren der →Internetverbindungen durch Störung von →Routing oder →DNS-Servern oder →Schadsoftware, die gezielt Rechner und Infrastruktursysteme mit bestimmten Länder- und Zeitzoneneinstellungen angreift. Kritisch in diesem Zusammenhang ist die starke →Verwundbarkeit der →SCADA- und →ICS-Systeme als Teil der sog. „kritischen Infrastruktur“ (einschließlich der extremen Verwundbarkeit und Angriffsbarkeit der Strom- und Wasserversorgung von den IT-Systemen, die heute zumeist mit dem →Internet verbunden sind).

Im Rahmen der Diskussion zu Cyberwar wird unterschieden zwischen strategischen Einsätzen (gegen alle Ziele, auch Wirtschaft und Öffentlichkeit), taktischen (gegen militärische Ziele) und operationellen (spezifisch zur Unterstützung einer einzelnen Operation). Angriffe auf IT-Systeme sind, wie auch bei →Cyberspionage, von kriminellen Aktivitäten oder →Hacktivismus meist nicht zu unterscheiden und könnten schlimmstenfalls mangels einer klaren →Identifizierung des Angreifers (→attribution) zu einer Eskalation zu konventioneller Kriegsführung münden. Heute wird oft →OIO oder →Cyberattack verwendet. Manchmal wird →Stuxnet als erster Einsatz von Mitteln eines Cyberwars bezeichnet, da dort mit großem Aufwand ein politisches Ziel verfolgt wurde.

Die Nutzung des Schlagworts Cyberwar ist umstritten, da die herkömliche Definition von Krieg: „2 identifizierte Gegner bekämpfen sich aktiv um ein politisches Ziel zu erreichen“ hier fast nie erfüllt ist. Der Angreifer ist zumeist nicht identifiziert und das politische Ziel ist oft nicht klar. Die oft als Cyberwar genannten Beispiele wie →Stuxnet oder →Flame waren einseitige Angriffe für die →Cyber terror treffender ist. Viele andere angebliche Beispiele sind eher →Cyberspionage, bzw. →APT.

2015 wird bekannt, dass es auch seit vielen Jahren Offensive-Planungen bei der →NSA gibt, mit dem Ziel sog. D Weapons im Krieg einzusetzen um durch großflächiges Zerstören der IT-Infrastruktur des Gegners ein Land zu lähmen. Siehe auch →Brick

http://sicherheitskultur.at/Angreifer_im_Internet.htm#cyberwar

DAC: (Discretionary access control) →Zugriffskontrolle in →TCSEC und →Vista, Win7. Zugriff wird erlaubt auf der Basis der Rechte des →Benutzers und den Gruppen, denen er angehört. Zumeist implementiert mittels Owner-Konzept, der Zugriffsrechte für sein Objekt definieren kann. →MULTICS

DANE: Technologie zur Verifizierung von →Zertifikaten auf der Basis von →DNSSEC. Dabei sollen mittels eines signierten TLSA-Records im →DNS-Eintrag sichergestellt werden, dass vor dem Aufbau einer Verbindung zu einem →Server die →Identität des Servers geprüft werden kann. Diese Prüfung müsste beim web-browsen im →Browser passieren, bei der Verbindung zwischen Mail-Servern vor dem Aufbau der →SMTP-Verbindung. Eigentlich gute Idee, als problematisch wird gesehen, dass es auf der hierarchischen Struktur des DNS-Konzepts mit →ICANN an der Spitze beruht und auch für DNS-→Amplification Angriffe genutzt werden könnte. DANE mit →TLS in Verbindung mit →DNSSEC bilden die Grundlage der →BSI Richtlnie TR-03108 zu sicherem E-Mail, nicht jedoch die bisherige Implementierung von →EmiG

Darknet: Bezeichnung für ein Netz, das durch →Verschlüsselung und Technologien wie →TOR versucht, die Identität der Teilnehmer geheim zu halten. Die 2 wichtigesten Implementierungen sind auf der Basis von →P2P oder mittels →TOR. Wird von politischen Aktivisten mit der Zielsetzung propagiert, politische Unterdrückung zu unterlaufen, kann auch für →Filesharing zum Unterlaufen von →Copyright verwendet werden, ebenso wie für illegale Aktivitäten wie Drogenhandel. Siehe →Darknet market (DNM) Sehr sinnvolle Anwendungen für →Websites die nur über →TOR erreichbar ist →Whistleblowing. Es gibt in Darkent Dropsites von Zeitungen wie Süddeutsche, Spiegel, derStandard, New York Times, Guardian, über die dort vertrauliche Dokumente hinterlegt werden können ohne dass die eigene Identität, z.B. über die →IP-Adresse, zu sehen ist.

In P2P-Netzen ist dieTeilnahme an Aktivitäten oft nur durch Einladung möglich. Es entstehen dann geschlossene Benutzergruppen.

Darknet market (DNM): →e-Commerce →Websites die als →TOR hidden service implementiert sind und für illegale Aktivitäten verwendet werden. Ursprünge kann man in den 70igern im Cannabis Handel im frühen ARPANET sehen. In den 80igern gab es

ähnliche Aktivitäten in →newsgroups. 2006 war dann The Farmer's Market eine der frühen Handelswebsite, ab 2010 auch als →TOR Hidden Service. Silk Road war nach der Schließung von Farmer's Market durch →LE ein wichtiger Nachfolger. Die Nutzung von TOR und →Bitcoin und Feedback Systeme ergaben den Standard für andere. Silk Road wurde 2013 geschlossen. Danach entstanden zahlreiche ähnliche Services wie Silk Road 2.0, das aber 2014 auch bereits geschlossen wurde. 2014 begannen auch die Aktivitäten an →OpenBazaar. 2017 wurden die großen Märkte Hansa und AlphaBay zuerst von →LE übernommen, deren Kunden überwacht und dann vom Netz genommen. Viele Details auf https://en.wikipedia.org/wiki/Darknet_market

Dark Pattern: Begriff der die (Psycho-)Tricks bezeichnet, die verwendet werden um die sog. →stickyness einer →App (oder seltener →Website) zu erreichen, d.h. lange vor dem Bildschirm zu verweilen, Online-Käufe zu tätigen (z.B. indem ständig angezeigt wird, dass das Angebot knapp wird und Zeitdruck erzeugt wird oder fälschliche Discounts gezeigt werden) oder persönliche Informationen preiszugeben (z.B. durch →Cookie Wall die die Nutzung ohne „freiwillige" Zustimmung verhindert).

Eine Möglichkeit gegen so etwas juristisch vorzugehen könnten Gesetze gegen den unlauteren Wettbewerb sein, jedoch wird auch regulatorischer Handlungsbedarf gesehen. Die geplante →ePrivacy Regulation könnte hier auch helfen. Hier eine Analyse dazu https://www.tab-beim-bundestag.de/de/pdf/publikationen/themenprofile/Themenkurzprofil-030.pdf

Dash: Implementierung einer →Cryptocurrency. Wird bei →Ransomware genutzt

Dashboard: (engl. Armaturenbrett eines Autos) in der IT Visualisierungssoftware, die Betriebszustände (auch Sicherheitsstatus), aber auch allgemeine Statusinformationen eines Unternehmens, z.B. bez. Personalfragen, Verkaufsumsätze, Kundenzufriedenheit, o.ä. in graphischer Form anzeigt. Siehe →KPI, →Balanced Score Card

DASD: (Direct Access Storage Device) →Magnetplatten bei IBM Mainframes

Data: (engl. →Daten)

Data Aggregator: (Datensammler) Firmen wie →ChoicePoint, →LexisNexis, →Acxiom, Epsilon, Equifax, Harte-Hanks, Merkle, Intelius, Meredith Corp. oder in Ö →LifeStyle und 123people, die durch das systematische Ankaufen von →personenbezogenen Daten umfassende Datensammlungen für Marketing-, aber auch Kreditauskunft und andere →Reputation-Dienste anlegen. Datenquellen sind in den USA z.B →Freedom of Information Act, aber auch die Datensammlungen die beim →Zugriff auf die →Smartphone-Daten bei der Installation von Smartphone-→Apps entstehen („→permissioned data", da die Benutzer bei der Installation der App der Datensammlung zustimmen). Auswertung z.B. durch →Data Mining. Siehe →Privatsphäre, →Kundenkarte, →Big Brother

http://sicherheitskultur.at/privacy_loss.htm#privat

Database: (engl. Datenbank) strukturierte Sammlung von vielen Informationen in einer gemeinsamen Einheit, Zugriff findet über ein spezielles Programm statt, oft auf einem separaten Rechner (Datenbankserver), oft aus Gründen der →Verfügbarkeit auf einem →Cluster. Große Sammlungen von vertraulichen, z.B. →personenbezogenen Daten in solchen Datenbanken haben einen hohen Schutzbedarf bzgl. →Vertraulichkeit. Siehe →Wallet, →TDE

Die →Datensicherung von Daten in Datenbanken erfordert spezielle Software, da Datenbanken zumeist ständig aktiv (offen) sind und offene →Dateien wegen der Nutzung von →Cache keinem konsistenten Zustand aufweisen. Es sind verschiedene Strategien möglich, z.B. offline („herunterfahren"), über Exports oder Online (mittels Transaction Logs, →Journals). Siehe →RMAN

Data Breach: der Verlust von →Daten, i.d. Regel durch einen →Angriff von innen oder außen. Zumeist bleiben die Daten dabei dem →Data Owner erhalten, aber andere Personen können ebenfalls über diese Daten verfügen. Für diesen Angriff wird üblicherweise eine Sicherheitslücke ausgenutzt, diese besteht aber sehr oft in Fehlkonfigurationen von →Systemen (z.B. →Cloud Systeme), erfolgreichen →Phishing Angriffen untersützt durch fehlende Absicherungen der →Zugriffe, z.B. über →2 Faktor Authentisierung. Wenn personenbezogene Daten betroffen sind so müssen EU-Firmen alle Data Breaches an die Behörden melden

Data Broker: →Data Aggregator

Data Center: Ort auf dem viele →Server aufgestellt sind. Im Fall von →Colocation auch Server unterschiedlicher Firmen. Die Sicherheit eines Data Centers hängt von der →räumlichen, der →personellen und →logischen Sicherheit ab. Bei →Cloud Anbietern werden viele Data Center über die ganze Welt verteilt. Der (eigentlich interne) Datenverkehr zur Synchronisierung der →Daten auf den Servern wird über →Lichtleiter geführt, die entweder mit anderen Firmen geteilt werden (z.B. als Teil der Internet-→Backbones) oder dediziert sind. 2013 wird bekannt, dass die →NSA diese Verbindungen abhört und damit an die internen Daten vieler Cloud Anbieter kommt. Diese reagieren mit verstärkter →Verschlüsselung der Verbindungen. Siehe →Localization

Data Cleaning: in einer →Datenbank aufräumen und z. B. „Karteileichen", falsche Adressen, widersprüchliche oder unvollständige

Datensätze bereinigen

Data Controller: →Data owner

Data Leak: (auch data leakage) unautorisiertes Entfernen von →Daten aus einem Unternehmen, z.B. durch →Hacker, Unachtsamkeit (verlorenes →Notebook oder →Smartphone), Fahrlässigkeit (mangelnde →Verschlüsselung) oder kriminelle Mitarbeiter. Siehe →DLP, →Identity Theft, muss nach der →DSGVO nach spätestens 72 Std. an die Datenschutzbehörde gemeldet werden

Data Leak Prevention: (DLP) Produkte, die als Folge des →California Security Breach Information Act entwickelt wurden. Es geht darum, einen →Vertraulichkeitsverlust von →sensiblen Daten zu verhindern, z.B. durch Kontrolle von →USB-Ports und →E-Mail-Verkehr. Dies erfordert entweder eine generelle Blockierung von →Datentransfer-Möglichkeiten oder eine →Datenklassifizierung. Diese kann optimalerweise bereits bei der Erstellung jedes Datenobjekts durch den →Data Owner erfolgen, was jedoch fast nirgendwo der Fall ist. Alternativ findet eine automatisierte Klassifizierung statt (z.B. durch erkennen der Struktur von →Kreditkarten- oder Kontonummern), entweder flächendeckend oder erst bei versuchtem Datentransfer. Zum Teil soll →DRM für DLP eingesetzt werden. Siehe →XPS

Data Localization: →Localization

Data Management Platform: (DMP) →Software die für Werbung im →Internet eingesetzt wird. Dabei führen Firmen wie Nielsen, Salesforce, Oracle und SAP die Daten die über Internetnutzer (zumeist in pseudonymer Form) unter verschiedenen Pseudonymen (wie →Advertising ID oder verschiedenen →Cookie IDs) vorliegen zusammen und helfen auf diese Weise beim →Real-time Bidding

Data Minimization: Konzept aus dem →Datenschutz: es darf immer nur die kleinste Menge von →Daten verarbeitet werden, die für den definierten Zweck benötigt wird. Das Konzept kann grundsätzlich bei Sicherheitsthemen zu einer Reduzierung der →Angriffsflächen und damit der →Bedrohungen führen

Data Mining: (ab 2011 auch Big Data genannt) statistische Modelle und Verfahren der künstlichen Intelligenz mit deren Hilfe entscheidungsrelevante Informationen aus Datenbanken extrahiert werden können. Wird sehr erfolgreich im Bereich →CRM (Customer Relationship Management) eingesetzt und kann dort zur Erstellung von Kundenprofilen (→Benutzerprofil) verwendet werden (→Suchmaschinen). Die kommerzielle Nutzung liegt in →targeted advertising (→behavioural advertising).

Von staatlichen Behörden wird Data Mining zur Überwachung von unerwünschten Aktivitäten eingesetzt. Dabei ist zu unterscheiden zwischen der Analyse der Kommunikation einzelner Personen (→Überwachung) und der generellen Suche nach auffälligem Verhalten, z.B. durch Auswertung eines →Social Graphs durch mathematische Methoden (was u.ä. sehr viele →False positive bringt und zu einem →Präventionsstaat führen kann. Kommerzielle Implementierung: →Recorded Future. Wichtige Tools sind →Hadoop, →MapReduce und →sog. NoSQL databases. Gemeinsam haben quasi alle diese Tools, dass Performance über allem steht, d.h. Sicherheitsfeatures wie →Logging, →Authentisierung, →Autorisierung von →Zugriffen u.ä. werden typischerweise alle geopfert. Dies ist besonders problematisch, wenn diese Datenbanken direkt im Internet erreichbar sind, was 2015 im Fall von MongoDB und anderen dramatisch gezeigt wurde. Aber auch →SQL Injection-Angriffe (bzw. alternative Methoden über Eingabefelder auf Webpages) sind gegen NoSQL Datenbanken sehr oft möglich

Siehe auch →Web beacon, →Collective Intelligence, →Rasterfahndung, →Privatsphäre, →LI, →NIMD, →Hancock, →COI, →CBIR, →IIS, →Behaviour-based pricing, →Neural Network
http://sicherheitskultur.at/data_mining.htm

Data Owner: (deutsch Dateneigner) ab 2013 zumeist →Data Controller genannt, der Verantwortliche für die Sicherheit und Korrektheit von →Daten. Diese Rolle sollte fast immer im „Business" angesiedelt sein, im Fachbereich, auf keinen Fall beim →Dienstleister, der die Datenverarbeitung im Auftrag (nach Vorgabe eines →SLAs) durchführt. Eine Ausnahme bildet die Situation wie z.B. im Rahmen von →Social Networks, wo die „Kontrolle" über die Daten zwischen dem →Benutzer der Daten einstellt und dem Dienstleister, der weitere Nutzungsdaten sammelt, aufgeteilt ist (siehe →Tracking)

Data Protection Directive: (→Directive 95/46/EC) ursprüngliche Grundlage aller →Datenschutzgesetze in der →EU. Eng verknüft mit Artikel 8 der European Convention on Human Rights (ECHR), dem Schutz der →Privatsphäre, Familie, Wohnung und Kommunikation. 2018 abgelöst durch die →Datenschutzgrundverordnung

Data Recovery Services: Unternehmen, die logisch (z.B. durch Löschen) oder physikalisch (z.B. durch →Wasser, →Feuer) zerstörte Daten von →Datenträgern, wie →Festplatten, →CDs oder →Magnetbänder, wiederherstellen versuchen. Durch spezielle Hardware und Software können z.T. Daten auch nach Überschreiben oder →Formatieren wiederhergestellt werden. Wird bei →Desaster Recovery oder in der →Forensic eingesetzt

Data Retention: generell Aufbewahrung von

Daten, z.B. um den Auflagen bezüglich →Archivierung zu erfüllen. In der heutigen Diskussion (2005/06) meist die Fristen für die Aufbewahrung der →Verkehrs- und →Standortdaten von Telefon und →Internet. Europäische Anbieter wehren sich gegen eine zu lange Aufbewahrung, da dies Kosten verursacht. Datenschützer wehren sich gegen die Aufbewahrung, weil auch Verbindungdaten eine Einschränkung der →Privatsphäre darstellen. Siehe →Vorratsdatenspeicherung

Data Science: seit ca. 2018 neues Schlagwort, Nachfolger von →Big Data. Es beinhaltet alle statistischen Methoden von →data mining, schließt aber auch den Einsatz von AI-Methoden wie →Deep Learning ein. Der Einsatz kann problematisch sein und zu ethischen Verletzungen führen, siehe →Algorithmenethik

Data Shadow: (engl. für 'Datenschatten') Spur an Informationen die man hinterlässt, wenn man z.B. mit →Kreditkarte oder →Bankomatkarte zahlt, online einkauft, eine Kundenkarte verwendet oder →E-Mails verschickt. →Privatsphäre

Data subject: im →Datenschutz der von der Datenverarbeitung betroffenen, deutsch →„Betroffener"

Datei: (engl. file) „Sammlung" von →Daten auf einer →Magnetplatte, →CD-ROM oder anderem Speichermedium, der unter einem Namen angesprochen werden kann. Im Gegensatz dazu →Datenbank

Dateisystem: (engl. →file system)

Daten: (engl. data) Plural von Datum, das Gegebene (auch noch deutlich im Französischen données) eigentlich „Fakten", „Angaben". Daten sind schriftlich, akustisch oder bildlich ausgedrückte, wirkliche oder gedachte Sachverhalte. Daten bestehen aus Zeichen-, Signal- und Reizfolgen. Sie sind objektiv wahrnehmbar und verwertbar, unterscheiden sich aber von →Informationen. In der IT werden Daten als →Bytefolgen dargestellt. Siehe auch →personen-bezogene Daten, →sensible Daten, →Data Owner, →Datei

Daten-Aggregatoren: →Data Aggregator

Datenaustausch: Transfer von →Daten (→Datenübertragung) über →Datennetze, früher oft dedizierte Datenverbindungen, heute zumeist via →Internet. Siehe →Datenträgeraustausch

Datenbank: →Database

Datendiebstahl: Entwenden von →Daten zur unautorisierten Veröffentlichung oder zum Verkauf im kriminellen Untergrund (→Cybercrime). Möglich ist auch ein Verkauf an Behörden (→Liechtenstein-CD), bzw. Veröffentlichung aus politischen Gründen (→Hacktivismus, →WikiLeaks, →Ransomware)
http://sicherheitskultur.at/notizen_1_10.htm#diebstahl

Dateneigentum: unter diesem Schlagwort wird diskutiert, ob wegen des steigenden ökonomischen Werts digitaler →Daten eine gesetzliche Regelung von Nutzungs- und Verwertungsrechten erfolgen soll. Nach geltendem europäischem Recht ist „Eigentum" an körperliche Gegenstände gebunden. Daher können bei Daten nur Nutzungsrechte, → Zugriffsrechte u.ä. bestehen. Daten zeichnen sich vor allem durch sog. „Nicht-Rivalität", d.h. die Verwendung durch eine Person behindert nicht die gleichzeitige Verwendung durch andere. Der Begriff wird auch manchmal im Zusammenhang mit →Intellectual Property (IP) verwendet. Der Begriff entstand nicht rund um →Datenschutz, sondern auf Initiative der deutschen Automobilindustrie die damit z.B. einen Anspruch auf die von →Sensoren in einem modernen →Auto erzeugten Datenmengen herleiten möchte.

Nicht zu verwechseln mit dem →Dateneigener des →Datenschutzrechts

Dateneigner: →Data Owner

Datenethik: Siehe →Algorithmenethik

Datenethikkommission: (DEK) von der deutschen Bundesregierung 2018 eingesetztes Gremium das ethische Standards für die Nutzen von →Big Data, →Algorithmen und →AI-Systemen erarbeitet hat. 2019 wurden entsprechende Vorschläge unterbreitet die auch als Grundlage für die für 2020 geplante Implementierung einer Regelung auf EU-Ebene dienen könnten. In anderen europäischen Ländern gibt es ähnliche Initiativen. Inhaltliche Details siehe →Algorithmenethik

Datengeheimnis: →Vertraulichkeit

Datenintegrität: →Integrität

Datenklassifizierung: (Teil von →Asset Klassifizierung) Einteilung von →Daten nach →Vertraulichkeits-, →Integritäts- und →Verfügbarkeitsbedarf. Wichtige Aufgabe, meistens jedoch vernachlässigt. Siehe →Risiko Management, →DLP

Datennetz: Einrichtung für eine →Datenübertragung, heute bestehend z.B. aus →Routern, Repeatern, Verkabelung, wie z.B. →Fibre Optics, →Standleitungen, Technologien wie →ATM, →ADSL, etc.

Datenportabilität: eines der →Betroffenenrechte aus der →DSGVO. Es bezeichnet, dass der →Dienstleister die →Daten des Nutzers auf Anfrage in maschinenlesbarer Form zur Verfügung stellen muss. Ziel ist, dass diese Daten dann von einem anderen Dienstleister im gleichen Funktionssegment, z.B. →social networking leicht übernommen werden können. Dies soll die Konkurrenz stärken, hat aber bisher nicht diesen Erfolg. Wurde von den großen Firmen wie →Google, →Amazon, →Apple, →Facebook sehr zügig implemen-

tiert, kleinere Unternehmen tun sich deutlich schwerer damit

Datenrettung: technische Verfahren um zerstörte →Daten, speziell auf →Magnetplatten oder →Magnetbändern wiederherzustellen. Dabei geht es um Daten, die durch logische oder mechanische Fehler oder höhere Gewalt gelöscht oder zerstört wurden

Datensafe: Schutz elektronischer →Datenträger gegen →Feuer, (Lösch)-→Wasser, unbefugten Zugriff, Strahlen und Erdbeben. Dabei müssen Normen wie z.B. EN 1047-1, S120 DIS bzgl. Brandschutz oder EN 1143-1 (Widerstandsgrad II) gegen Einbruch erfüllt werden

Datenschutz: Schutz des allgemeinen Persönlichkeitsrechts, insbesondere den Anspruch auf Achtung der →Privatsphäre von natürlichen Personen (Menschen, im Gesetz →Betroffene, engl. →data subject) (zumeist auch juristischer Personen) vor einer missbräuchlichen Verwendung, Verarbeitung, Speicherung, Übermittlung, Löschung ihrer personenbezogenen Daten. Die Verantwortung liegt immer beim →Auftraggeber (engl. →Controller, →Data owner) und i.d.Regel nicht bei einem evtl. mit der Durchführung beauftragten →Dienstleister (service provider). Eine etwas andere Situation liebt vor, wenn die Datenverarbeitung durch einen →Diensteanbieter wie den Betreiber eiens Social Networks durchgeführt wird.

Wichtig: ein Dienstleister hat die Verantwortung nur im Rahmen des von ihm unterzeichneten →SLAs und es gibt kein →Konzernprivileg, d.h. eine →Datenübermittlung von personen-bezogenen Daten innerhalb eines Konzerns bedarf einer offiziellen Genehmigung und ebenso eine →Datenüberlassung an Dienstleister. Ein wichtiger Aspekt ist →Data Minimization.

Siehe →sensible Daten, →Selbstbestimmung, →personen-bezogene Daten

Datenschutzbeauftragter: (DSB) Position in einem Unternehmen oder Behörde, verantwortlich für alle Fragen des Datenschutzes, in D. Pflicht wenn personenbezogene Daten erhoben, verarbeitet oder genutzt werden (in § 4f und § 4g des →Bundesdatenschutzgesetzes (BDSG) geregelt). In Ö. optional

Datenschutzbehörde: Seit 2014 die österreichische Behörde, die für den →Datenschutz zuständig ist und das →DVR betreibt. Das Register ist jetzt für jeden einsehbar und zeigt, welche Datenverarbeitungen durch Firmen eingemeldet wurden.

Datenschutzerkärung: (engl. Privacy Statement) Text auf einer →Website in der der Betreiber erklärt, wie er mit personenbezogenen →Daten oder →E-Mail-Adressen umgeht. Relevant für jede Website, da immer die Nutzungsdaten protokolliert werden. Siehe →Google Analytics, →P3P

Datenschutzgesetz (DSG 2000): früheres österreichisches Datenschutzgesetz, setzte die Rahmenbedingungen für den Umgang mit Personendaten. Im §1 wird der Datenschutz in verfassungsmäßigen Rang erhoben. Dieses Grundrecht auf →Datenschutz bewirkt einen Anspruch auf Geheimhaltung personenbezogegner Daten. Darunter sind der Schutz vor Ermittlung dieser Daten, sowie der Schutz vor deren Weitergabe zu verstehen. In Deutschland →Bundesdatenschutzgesetz

Datenschutzgrundverordnung (DSGVO), engl. GDPR (General Data Protection Regulation. Seit Mai 2918 in Kraft. Sie hält an den Grundsätzen der früheren →Datenschutzrichtlinie fest (Zweckbindung der Verarbeitung, notwendige Rechtsgrundlage für die Verarbeitung, Rechte der Betroffenen wie Auskunft, Löschung, →Datenportabilität, etc.). Neu sind die deutlich höheren Maximalstrafen, die bisher aber noch nicht wirklich ausgereizt wurden. Überschießendes Ergebnis ist eine Flut von →Datenschutzerklärungen und expliziten Zustimmsersuchen, die zum Teil nicht notwendig, zum Teil nicht rechtsgültig sind (wenn sie z.B. nicht auf Freiwilligkeit beruhen), siehe Flut an →Cookie-Zustimmungen auf allen →Websites

Datenschutzkomission: frühere österreichische Behörde für den →Datenschutz, jetzt →Datenschutzbehörde

Datenschutzrichtlinie: (europäische D.) 1995 erlassene Richtlinie der EU (95/46/EG) zum Schutz der →Privatsphäre von natürlichen Personen bei der Verarbeitung von personenbezogenen →Daten. Sie war in lokale Gesetze umzusetzen. Sie wurde durch die →DSGVO abgelöst.

Datensicherung: (engl: →Backup)

Datenspiegelung: automatisches Kopieren eines Datenbestandes mit Hilfe von geeigneter Hardware oder Software. Siehe →Hochverfügbarkeit, →Desaster Recovery

Datenträger: physikalisches Medium, auf dem Daten aufbewahrt werden können. Beispiele sind Disketten (Floppies), →Lochkarten (historisch), Magnetbänder, CD, →DVD, Papier für Druckausgabe, heute oft →USB-Speicher

Datenträgeraustausch: früher vor allem von Banken genutzter physischer Transport von maschinell lesbaren Datenaufzeichnungen, z.B. von Disketten oder Magnetbändern. Dabei kann es zu Verletzungen von →Vertraulichkeit, →Integrität und →Verfügbarkeit kommen

Datenüberlassung: wenn Daten einem →Dienstleister für die Durchführung der Datenverarbeitung im Auftrag des →Data owners überlassen werden. Erfordert i.d.Regel eine Dienstleistervereinbarung und ein →SLA

Datenübermittlung: Weitergabe von Daten an eine anderes Unternehmen (evtl. im gemein-

samen Konzern) für eigene Zwecke, Bedarf bei personen-bezogenen Daten immer der Zustimmung des Betroffenen

Datenübertragung: technisches Versenden von Daten über →Datennetze. Möglicher Punkt für einen →Angriff auf die →Informationssicherheit

Datenverarbeitungssystem: frühere Bezeichnung für IT-System (EDV-System); Computer, DV-Anlage, Datenverarbeitungsanlage, DV-System, Rechenanlage, Rechensystem, Rechner. Alle diese Worte bezeichnen eine heute ausschließlich elektronisch arbeitende Einheit, die mittels gespeicherter Programme automatisch Daten verarbeiten, also mathematische, umformende, übertragende und speichernde Operationen durchführen kann

Datenverkehr: →Datenübertragung

dDoS: (distributed Denial of Service) →Denial of Service Angriff

DD-WRT: Firmware für →WLAN- →Router die unter →GPL angeboten wird und durch Verwundbarkeiten ermöglicht, dass diese Geräte in →Botnets integriert werden

De-Anonymisierung: Bearbeitung →anonymer oder →pseudonymisierter →Daten dergestalt, dass danach die Zuordnung zu 1 Person möglich ist (→PII). Dies geschieht z.B. durch Kombinieren der Daten aus verschiedenen Quellen, z.B. die zusätzliche Nutzung von Daten von einer →Social Networking Website, bei der der Benutzer unter vollem Namen auftritt. Dies stellt dann zumeist eine Verletzung der →Privatsphäre dar. Siehe http://sicherheitskultur.at/Glaeserner_Mensch.htm#deanom

Debit Card: Variante der „Geldkarte“, bei der das Konto sofort belastet wird, z.B. eine →Bankomatkarte. Im Gegensatz dazu →Kreditkarte. Damit mit Debitkarten auch im →Internet gezahlt werden kann wird die Kartennummer auf die Länge und das Format der Kreditkartennummer gebracht. Dies geschieht in Österreich ab 2018. Debit- und Kreditkarten können „tokenisiert“ werden. Dies geschieht beim →Enrollment für einen Zahlungsdienst wie →Apple Pay oder →HCE bei der Implementierung von →Google Pay

Debugging: Fachbegriff in der IT für Fehlersuche. Leider zu wenig und zu unsystematisch eingesetzt, dadurch bleiben viele →Programmierfehler in den →Programmen und bilden so die Quelle der →Schwachstellen. Für die Fehlersuche werden oft zusätzliche →Logs eingesetzt, die manchmal Quelle von →Vertraulichkeitsverletzungen sein können, wenn z.B. →Passworte im Klartext in Logfiles abgelegt werden

decompression bomb: →Angriff gegen →Virenschutzsoftware, bei dem mittels →E-Mail-Anhängen →Dateien verschickt werden, die komprimierte Archive in →zip- oder rar-Format enthalten. Dafür wird eine Datei mit sehr vielen gleichen Zeichen (im 100 MB-Bereich) mehrfach in ein solches komprimiertes Archiv eingebracht. Wenn der → Malware-Schutz die einzelnen Dateien überprüfen will, so muss er alle diese Dateien dekomprimieren und verbraucht dabei evtl. mehr Plattenplatz, als der Server zur Verfügung hat, was zu einem →DoS führen kann

DeCSS: →DVD

DECT: (Digital Enhanced Cordless Telecommunications) Standard für Schnurlos-Telefone in Firmenumgebungen mit Betriebserlaubnis bis mindestens 2013. Es gibt strahlungsarme DECT-Telefone deren Sendeleistung variabel ist, für die Sicherheit werden →Authentifizierung und (optionale) →Verschlüsselung verwendet. In Verbindung mit →VoIP-Implementierungen können DECT-Gateways oder die Nachfolge →VoWLAN eingesetzt werden. Ende 2008 lassen die Gespräche leicht mit einer Zusatzkarte im →PC abhören

Deduplication: Verfahren um zu verhindern, dass identische Datenblöcke mehrfach gespeichert werden, z.B. indem ein Mailserver erkennt, dass der gleiche Anhang bereits anderweitig gespeichert ist oder indem ein →Filesystem gleiche Datenblöcke erkennt und intern verlinkt. Kann bei falscher Implementierung für →Angriffe genutzt werden. Siehe →Dropbox

Deepfake: Täuschend echte Fälschungen von Ton- und oder Video-Aufnahmen bei denen mit Hilfe von →Deep Learning (Generative Adversarial Networks =GAN) Personen falsche Texte oder Taten unterstellt werden. So werden die Köpfe von prominenten Personen in Pornofilme montiert oder Politikern falsche Inhalte „in den Mund gelegt“. In 2019 zeigt eine Studie, dass in 96% aller Fälle Frauen davon betroffen sind. Für den Laien sind solche Fälschungen schwer zu erkennen. Ton-Deepfakes werden auch für →CEO Betrug eingesetzt, indem der →Angreifer mit der Stimme des Chefs anruft. Siehe →CGI

Deep Learning: Teil des Konzepts von Machine Learning, was wiederum ein Untergebiet von Artificial Intelligence (AI) ist. Bei Deep Learning werden sog. künstliche →neuronale Netze eingesetzt. Diese Systeme haben das Gebiet der AI weit vorangebracht, vor allem auf Gebieten wie Sprach- und Bilderkennung, Übersetzung, Analyse und Filterung in →Social Networks und auch Brettspielen wie z.B. Go, Diese Systeme werden auch bei den Sensoren in →autonomen Fahrzeugen eingesetzt. Sehr problematisch ist bei diesen Systemen, dass diese (derzeit) keine Möglichkeit haben, ihre „Entscheidungen“ zu erklären. Dafür brauchte es „Explainable AI“ (→explainability). Dieses Forschungsgebiet ist erst am Anfang. Das Nicht-Erklären-Können ist z.B. bei der Unfall-

Analyse ein großes Problem, ebenso wenn Algorithmen Entscheidungen über Menschen fällen diese aber nicht erklären können. Ein Beispiel für den Einsatz von Deep Learning für Angriffe sind →Deepfakes für →CEO Betrug. Der Einsatz von Artificial Intelligence bei Angriff und Verteidigung in Bezug auf IT-Security wird seit ca. 2018 viel diskutiert

DeepMind: 2010 in London gegründete Firma, die 2014 von Google aufgekauft wurde, führend bei der Entwicklung von →Machine Learning Systemen. DeepMind wurde vor allem bekannt durch den Sieg von AlphaGo gegen den Weltmeister und die Weiterentwicklung AlphaZero. Dieses System lernt (fast) beliebige Spiele (z.B. Schach, Go, Shogi) indem es gegen sich selbst spielt. Die dabei entstehenden, zum Teil ungewöhnlichen Strategien kann das System nicht ‚artikulieren' (fehlende →Explainability). 2020 wurde AlphaFold für Proteinfaltung eingesetzt, ein bisher nicht gelöstes IT-Problem. DeepMind arbeitet auch an einem Konzept „Neural Turing machine", das →Deep Learning mit einer →Turing Machine verbinden soll

Deep packet inspection: (DPI) Vorgang, bei der ein Gerät in einer Datenübertragungskette nicht nur die Header-Informationen der →IP-→Pakete auswertet, sondern die Applicationsinhalte inspiziert, analysiert und wahlweise aufzeichnet. Dies kann auch dann geschehen wenn die Pakete verschlüsselt sind, da bestimmte Protokolle u.a. an typischer Länge der Pakete erkannt werden oder an typischen Textstrings im Zuge der Schlüsselvereinbarung. Auf diese Weise wird z.B. →P2P →Filesharing auch bei verschlüsselten →Protokollen erkannt und von →ISPs zum Teil gedrosselt oder blockiert. Ziel kann die Erkennung von →Spam, →Schadsoftware, Priorisierung von Datentypen wie →VoIP, aber auch →Data Mining, →Überwachung der Kommunikation und Zensur sein. Dies wird u.a. als Gegenmaßnahme zu →Copyright-Verletzungen vorgeschlagen, aber auch heftig kritisiert. Wenn ein ISP auf diese Weise Kenntnis von Inhalten bekommt kann dies auch komplexe →Haftungsauswirkungen haben. Dies ist eine verschärfte Ausprägung von →LI. Geheimdienste wünschen sich immer wieder diese Funktionalität, bzw. in den USA ist dies mittels →NARUS-Geräten bereits implementiert

Deep Web: a) Begriff für die →Webseiten, die nicht von →Suchmaschinen indiziert werden. 2012 gibt es geschätzte 190 Mio Websites mit 8,42 Milliarden Webseiten die indiziert werden. Das Deep Web wird auf 500mal so groß geschätzt. Dies sind z.B. Webseiten die sich nur über Suchanfragen öffnen und nicht direkt verlinkt sind, →Websites die nur nach Eingabe einer Benutzerkennung erreichbar sind, Inhalte die nur mittels →Flash oder ähnlicher Dienste zugänglich sind, oder Webseiten auf die nirgendwo verlinkt wird

b) auch genutzt für →Websites, die im öffentlichen →Internet erreichbar sind, da sie innerhalb des →TOR-Netzwerks gehostet sind, →TOR Hidden Service

DEF CON: Sicherheitskonferenz in Las Vegas, mehr oder weniger parallel mit →Black Hat

Defacement: Eindringen in eine →Website mit dem Ziel, den Inhalt zu verändern, ohne finanzielle Motive. Entweder eine Form des →Hacktivismus, oder „for the →LULZ"

Defender: (Windows Defender) Anti-→Spyware Tool von Microsoft, das früher kostenlos erhältlich war, heute nur noch in →Vista enthalten ist

Defense in Depth: →Sicherheitskonzept das besagt dass man sich nie auf eine einzelne Schutzmaßnahme verlassen darf, weil jede Versagen kann (→Murphys Law). Die Maßnahmen sollten die Verhinderung und die Entdeckung eines Angriffs abdecken, aber auch den Fall abdecken, dass ein Angriff erfolgreich war

DEK: →Datenethikkommission

De-Mail: →Bürgerportale

Deming Kreis, Deming Circle: →PDCA-Zyklus

Demilitarized Zone: (DMZ) separates Netz einer →Firewall, in dem Rechner mit Außenkontakten platziert werden. Die Bezeichnung kommt von der Pufferzone, die zwischen Nordkorea und Südkorea aufgestellt wurde, die ihrem Krieg in den frühen fünfziger Jahren folgte

Deniability: Möglichkeit zur glaubhaften Leugnung einer Behauptung, Gegensatz zu →non-repudiation. Siehe →OTR, →Truecrypt, →Steganographie. Gegensatz: →Non-Repudiation

Deniable File System: →DFS

Deniable Operating System: Technik, bei der die Existenz eines (virtuellen) →Betriebssystems auf einem Rechner nicht nachgewiesen werden kann. Siehe →TrueCrypt

Denial of Service: (DoS-Attacke, bzw. dDoS, Distributed Denial of Service). Lahmlegen von Rechnern, bzw. Diensten.

In →IP-Netzen ein →Angriff, bei dem ein Rechner durch eine große Zahl von Anfragen (z.B. →synflood oder →HTTPflood) einen Angriff auf Rechner oder Netzwerke durchführt. Die verwendeten Anfragen können entweder legitim oder illegitim sein. Einen gewissen Schutz bietet ein →IDS oder →IDP System. Bei einem distributed denial of service (→dDoS) Angriff werden zahlreiche, von dem →Hacker bereits unter Kontrolle gebrachte Rechner (→Zombienetz) zu einem koordinierten Angriff auf das gleiche Ziel verwendet (→„Drohnen", →„Zombies"). Ziel ist heute meist das →Erpressen von Geld, aber auch

sehr oft →Hacktivismus. Firmen wie CloudFlare bieten Services an um große DNS-Angriffe abzuwehren. Sie verwenden →NetFlow zum beobachten der Datenflüsse und →RSVP (Flowspec) für deren Änderung um Angriffen „auszuweichen". Siehe →amplification, →Reflector Attack, →DNS amplification, →Downtime, →LOIC. http://sicherheitskultur.at/spam.htm#zusammen

2013 gibt dDoS-as-a-service: sog. →Booter oder →Stresser bieten für geringe Gebühren eine IP-Adresse für die Dauer von 1 Minute (für 10 USD) oder auch länger im Netz nicht erreichbar zu machen. Solche Dienste werden z.B. gegen Privatleute eingesetzt, z.B. von Gamern, die damit den Internet-Anschluss eines Kontrahenten für 1 Minute lahm legen in der sie den →Avatar dieses Gamers besiegen können. Ebenso können →Skype- und andere →VoIP-Verbindungen, aber auch reguläre →POT-Telefonverbindungen gezielt überlastet werden, z.B. um eine Benachrichtigung zu verhindern. Oder Opfer von →Phishing werden daran gehindert, die →Website oder den Helpdesk der Bank zu erreichen.

Denial of Service ist aber z.B. auch durch →Jamming von drahtlosen Übertragungen wie →GSM, →UMTS oder →LTE möglich und verhindert auf diese Weise die Kommunikation

Department of Homeland Security: (DHS) nach 9/11 etablierte US-Behörde, die frühere Sicherheitsbehörden vereinigt. Sie enthält u.a. Coast Guard, Secret Service, →TSA, Immigration and Customs, →NCSD. Siehe →Automated Targeting System, →Secure Flight, →TIA

DEP: (Data Execution Prevention) Verhindern der →Code-Ausführung in Datenbereichen im Speicher, implementiert in →Mac OS, →Windows XP SP2 aufwärts auf geeigneten →Prozessoren (AMD NX-bit oder Intel XD-Bit Funktion auf →Page-Basis). Traditionell unterstützen →x86-Prozessoren non-executable →Speicher nur in der Form von →Segmenten, die wiederum in den →Betriebssystemen nicht unterstützt werden. Soll →Buffer-Overflow →Angriffe verhindern

De-perimeterisation: →Jericho Forum

Depersonalization: →Pseudonomisierung

DER: (direct-recording electronic) Wahlmaschinen zur sofortigen Erfassung von Wählerstimmen. Sehr sicherheitsrelevant, da die →Vertraulichkeit der Wahlentscheidung trotz der Notwendigkeit gegeben sein muss, sicher zu stellen, dass jeder Wähler nur einmal wählt. Oft wird wegen dem Wunsch der Möglichkeit einer Zählung „per Hand" auch eine Protokollierungsmöglichkeit implementiert. Gleichzeitig muss sichergestellt sein, dass die Software nicht manipuliert wurde. Siehe →e-Voting

DES: (data encryption standard) symmetrischer →Verschlüsselungsalgorithmus. Von IBM entwickelt und 1974 veröffentlicht. Es war bis 2002 der offizielle Standard der amerikanischen NIST (National Institute for Standards and Technology). Es handelt sich um ein symmetrisches Schlüsselverfahren. Auf Grund der beschränkten Schlüssellänge von nur 56-bit gilt das Verfahren heute nicht mehr als sicher und wird heute meist durch →3DES oder andere Verfahren ersetzt. Die →NIST hat 2002 einen neuen Standard erlassen: →AES

Desaster Recovery: (DR) leicht inkorrekte Bezeichnung, da Mischung aus deutsch (Desaster) und englisch (recovery). Korrekt →disaster recovery

Desinformation: Erzeugen und Verbreiten von falschen →Informationen, eine Verletzung der →Integrität von Informationen. Siehe →OIO, →Information Warfare

Desktop: Rechner (→PC), zumeist mit separatem →Bildschirm, →Tastatur und →Maus, auf dem entweder lokale Anwendungen ausgeführt werden oder im →Client-Server Modus Ergebnisse von zentralen Anwendungen präsentiert werden, z.B. →Webseiten oder mittels →Terminalserver. Im Gegensatz dazu als mobile Variante →Laptop, →Tablett oder →Smartphone

Desktop Security: Konzept zur lokalen Absicherung des Rechners eines →Anwenders, z.B. durch →Virenschutz und restriktive →Benutzerrechte. Siehe →Network Security, →Application Security

Device Fingerprint: Sammeln von Informationen die das →Tracking eines Nutzers im →Internet erlaubt. Bei einem →Webbrowser (z.B. implementiert mittels →Javascript). Dazu gehören z.B. Systemversion, Bildschirmauflösung, Sprache, Zeitzone, installierte Fonts, installierte Plugins, etc.). Speziell Font Detection (mittels Javascript oder →Flash) ergibt 17 bit Entropie und ergibt eine fast eindeutige Identifizierung eines →Rechners im →Internet auch ohne die Nutzung von →Cookies. Gegenmaßnahmen wie Nutzung des →TOR-Browsers oder →No-Script erhöhen auf Grund ihrer geringen Nutzung die Identifizierungsrate. Viele der Daten sind browser-unabhängig und erlauben browser-unabhängiges Tracking, selbst im →Private-Browsing Modus. Nutzung 2013 bereits ca. 1% der →Alexa-Websites. 2014 kommt →Canvas Fingerprint dazu

Mit gewissen Einschränkungen lässt sich eine weitgehende Identifizierung von Nutzern sogar ganz ohne Mitwirkung des Geräts des Nutzers erreichen, z.B. über geringe Anomalien der internen Uhren, die von Webservern ausgewertet werden können. →Anonymität im Internet ist nicht wirklich möglich

DFS:
1) (Distributed File System) →Dateien sind über mehr als 1 physiche →Magnetplatte verteilt. →Verfügbarkeit muss durch entspre-

chende Spiegelungen sichergestellt sein

2) (Deniable File System) Funktionalität, bei der die Existenz des →Filesystem geleugnet werden kann, da es keine erkennbaren Spuren hinterlässt. Soll verhindern, dass jemand durch Zwang zur Preisgabe eines →Schlüssels gezwungen werden kann. Führt jedoch dazu, dass auch niemand die Nicht-Existenz eines DFS beweisen kann, was in Fällen wo der Angreifer den Schlüssel durch Gewalt erzwingen will für jemand ohne DFS sehr unangenehm ist. Implementiert von →TrueCrypt als →Hidden →Volumes

DGA: →Domain Generation Algorithmus

DHCP: (Dynamic Host Configuration Protocol) Standard bei →IPv4 zur dynamischen Vergabe von →IP-Adressen zu Rechnern. Wird hauptsächlich in →LANs und für Workstations, aber auch von →ISPs und für →GPRS und →UMTS eingesetzt. Implementierungsfehler in den entsprechenden Servern oder das Vorspiegeln eines falschen Servers können zu Sicherheitsproblemen führen. Wird bei →IPv6 durch →ICMPv6 oder →DHCPv6 ersetzt

DHCPv6: eine der Methoden unter →IPv6 zur Vergabe von →IP Adressen. Eine andere Methode ist →ICMPv6

DHE: (manchmal auch EDH genannt) Diffie-Hellman Ephemeral. Auf dem →Diffie-Hellman Key Exchange beruhende Variation, die →PFS implementiert

DHS: →Department of Homeland Security

DHTML: (Dynamic HTML) Kombination aus →HTML, →CSS und →DOM, die mittels →JavaScript das Aussehen der →Webseite dynamisch verändern kann, ähnlich zu →AJAX, aber älter

Diaspora: eine Form von föderiertem →Social Network, beruht auf dem gleichnamigen Protokoll. D.h. unterschiedliche Instanzen von Diaspora können untereinander Daten austauschen ohne dass es eine zentrale Benutzerverwaltung wie bei →walled gardens wie →Facebook oder →Twitter der Fall ist

Dictionary Attack:

1) Technik um →Passworte zu knacken, indem gängige Worte, auch mit angehängten Zahlen, als Passworte ausprobiert werden. Zumeist werden dabei Begriffe ausprobiert, die entweder in Wörterbüchern verschiedener Sprachen zu finden sind, oder aber bei einem der vielen Passwort-Diebstählen erbeutet wurden, oft werden dabei auch 2 Worte kombiniert und mit Zahlen im Ende ergänzt. Beim Berechnen der →Hashes kommen oft auch →GPUs zum Einsatz. Siehe →Rainbow Tables

2) Methode um durch die Kombination von Vor- und Nachnamen, bzw. Abkürzungen derselben (auch mit angehängten Zahlen) →E-Mail-Adressen für →Spam-Zwecke zu finden

Diensteanbieter: nicht nur →ISPs, sondern auch wer z.B. im →Internet auf einer →Website Texte oder Bilder veröffentlicht, egal ob selbst erstellt oder von den Nutzern dieses Dienstes, z.B eines →Blogs oder →Social Networks. Es können daraus →Haftungen entstehen. In Ö definiert in § 3 →ECG. Siehe auch →Dienstleister

Dienstleister: Firma, die (i.d.Regel im Auftrag) eine Datenverarbeitung durchführt. Diese Beauftragung sollte in Form eines →SLAs erfolgen. Über dieses SLA hinaus hat der Dienstleister nur sehr begrenzte juristische Verpflichtungen. Anders wird die Situation wenn der Dienstleister (als →Diensteanbieter), wie z.B. als Betreiber eines →Social Networks oder →Blogs seine Dienste direkt den →Benutzern anbietet. Dann ist der Benutzer für seine Inhalte und der Dienstleister für die bei der Nutzung dieser Inhalte gesammelten Daten (z.B. →Tracking) verantwortlich. Es gelten für Dienstleister auf jeden Fall die Verpflichtungen nach den Telekommunikationsgesetzen, aber auch weitere Verpflichtungen, siehe →Diensteanbieter

Diffie-Hellman Key Exchange: (D-H) Protokoll aus dem Bereich der →Kryptographie zur Erzeugung, bzw. Austausch eines geheimen →Schlüssels zwischen zwei Kommunikationspartnern den nur diese beiden kennen. Ohne zusätzliche Maßnahmen anfällig gegen →Man-in-the-Middle Angriffe da dieses Protokoll allein keine →Authentisierung der Kommunikationspartner abbildet. Wird als →DHE eingesetzt um →PFS zu erreichen. Siehe →ZRTP, →PSK, →SRP

Digital Collection System: →Carnivore

Digitale Gewalt: bezeichnet die Situation wo ein Partner oder Ex-Partner in einer Beziehung digitale Methoden verwendet um den anderen Partner zu überwachen oder zu terrorisieren. Dabei wird z.B. eine →Überwachungssoftware auf einem →PC oder eine →Spy-App auf einem →Smartphone installiert. Dadurch kann der Angreifer mehr oder weniger vollständig am Leben des Opfers teilnehmen. Eine weitere Form der digitalen Gewalt gibt es rund um →IoT und Smart Home, → Home Automation. Ein Ex-Partner der weiterhin →Zugang zum →WLAN der früheren Wohnung und weiteren Systemen hat kann damit tief in das Leben des anderen Partners eindringen, wenn er oder sie z.B. →Zugriff auf →Kameras oder Türschlösser hat

Digital Markets Act: (DMA) Ende 2020 zusammen mit dem Digital Services Act (DSA) von der EU vorgeschlagene neue Regulation. Im DMA geht es vor allem um Einschränkung der Möglichkeiten für sog. →Gatekeeper. Das sind Betreiber von digitalen →Plattformen, speziell Konzerne mit monopolartiger Macht in ihrem jeweiligen Segment. Ihnen sollen einige "unfaire Praktiken" verboten werden, die sie

auf Grund ihrer Monopolstellung ausüben. Zu den Gatekeepern gehören Intermediation Services, d.h. Marktplätze wie →Amazon, Airbnb, Booking.com, Reise-, Energie- und Taxi-Plattformen, →Suchmaschinen, →Social Networks, Videosharing, number-independent interpersonal electronic communication services (d.h. →Messaging Dienste, die nicht direkt an Telefonnummern gebunden sind, d.h. →Whatsapp, →Signal, →Skype, etc.), →Betriebssysteme (speziell im Blick →iOS und →Android), →Cloud-Dienste und →Werbenetzwerke.

Es geht z.B. um vorinstallierte Apps, das Verhalten von Amazon gegenüber seinen Händlern, Regeln die z.B. Verbieten, dass Hotels oder Geschäfte vor Ort billiger sein dürfen als auf booking.com oder Amazon, und vieles Es geht aber auch darum, dass alle Social Networks und Messaging Dienste kompatibel werden sollen. Das entspricht der Idee des →Fediverse, das dies bereits seit 2008 bietet, geeignete →Protokolle für diese Interoperabilität liegen vor, teilweise sogar als →Standards.

Digital Rights Management: →DRM

Digital Services Act: (DSA) von der EU in 2020 vorgeschlagenes Regelungspaket, das unter anderem Haftungs- und Sicherheitsvorschriften für digitale Plattformen, Dienste und Produkte schaffen und die e-Commerce Directive aus 2000 aktualisieren soll. Siehe auch →Digital Markets Act (DMA)

Digital Signage: →Plakat

Digitale Signatur: verwendet zur Feststellung der →Authentizität von elektronischen Nachrichten oder Dokumenten. (Nachweis, dass das Dokument nicht verändert wurde und wirklich vom angegebenen Autor stammt). Digitale Signaturen beruhen in der Regel auf asymmetrischen Kryptoalgorithmen, wie beispielsweise dem RSA-Algorithmus. Dabei wird ein sog. →Hash-Wert über das Dokument mit dem privaten Schlüssel des Autors verschlüsselt. Die Rechtswirksamkeit einer digitalen Signatur wird in Ö. durch das Signaturgesetz festgelegt. Verwirrend ist die Vielfalt mit unterschiedlichen Einsatzgebieten, in D: **einfache** Signatur, **fortgeschrittene** Signatur und **qualifizierte** Signatur, in Ö: **einfache** Signatur, **fortgeschrittene** Signatur und **sichere** Signatur, die im Wesentlichen der **qualifizierten** Signatur in D. entspricht. Daneben in Ö Verwaltungssignatur gemäß § 25 des E-Government-Gesetzes

Digital Watermark: →elektronisches Wasserzeichen

Digitales Zertifikat: →Zertifikat

DIME: (Dark Internet Mail Environment) Initiative von →Phil Zimmermann (→PGP), Ladar Levison (→Lavabit) und anderen für eine end-to-end →Verschüsselung von →E-Mail, die einfacher zu nutzen ist als →PGP

DIN: (Deutsches Institut für Normung e.V.) deutsche Normungsbehörde hat zahlreiche sicherheitsrelevante Standards erlassen. Siehe →ANSI, →öNorm

Directive: EU-Directive. Eine Richtlinie der →EU, die erst in das jeweilige nationale Recht umgesetzt werden muss. Z.B. →Data Protection Directive, →E-Privacy Directive. Siehe →Regulation

Directory: in der IT:

1) →Verzeichnisdienst
2) anderer Name für Verzeichnisstruktur von Dateien, auch Folder, Catalog

Disaster Recovery: (DR) alle Prozesse und Vorkehrungen für eine schnelle Wiederaufnahme der →Geschäftsprozesse nach einer →Katastrophe (Naturkatastrophe, Unfall, →Feuer, →Wasser, →Terrorismus, etc.). Dies geschieht entweder in vollem Umfang oder als eingeschränkter, aber angemessener Notbetrieb. Details der Planung werden im →Katastrophenplan (→Notfallplan) festgelegt. Dazu gehören z.B. →Backup-Rechenzentren an anderen Orten. Siehe →RTO, →RPO, →Datenrettung, →Business Continuity, →Backup

Disclosure: in der IT-Security das Veröffentlichen von →Schwachstellen (zum Teil zusammen mit →Exploits). „Responsible D." bezeichnet, wenn der Hersteller zuerst eine Frist für die Erstellung eines →Patches erhält, „full and immediate D." eine sofortige breite Veröffentlichung. Siehe auch →bug bounty

Discounting: Abwerten von zukünftigen Schäden gegenüber augenblicklichen Vorteilen oder gegenwärtigen Gewinnen gegenüber höheren zukünftigen Gewinnen bei der Betrachtung von →Risiken oder anderen Entscheidungen in Bezug auf →Sicherheit. So ist wird die Möglichkeit eines zukünftigen Schadens durch fehlende →Datensicherung geringer bewertet als die augenblickliche Bequemlichkeit keine Sicherung zu machen. Oder die augenblickliche Bequemlichkeit eines einfachen →Passworts wird wichtiger eingeschätzt als die Vermeidung eines möglicherweise eintretenden Nachteils in der Zukunft. Siehe →Sicherheitspsychologie

DISHFIRE: →NSA Aktivität zum Abfangen von →SMS-Nachrichten, vor allem „entgangene Anrufe", „roaming Hinweise", Benachrichtigungen über Kreditkartenrechnungen und andere Banknachrichtungen, z.B. Zahlungen und auch die →mTAN SMS die Hinweise auf Zahlungen und damit Vernetzungen bieten

Disk: →Magnetplatte

Disk Encryption: →Festplattenverschlüsselung

Disk Mirroring: →Mirror

Disruption: „disruptive innovation" Schlagwort geprägt durch Clayton M.Christensen 1997 in

„The Innvator's Dilemma". Umstrittenes Konzept, das besagt dass Startups mit eigentlich schlechteren (aber billigeren) Produkten die herkömmlichen Industrien oder Systeme ablösen. Beispiele sind Uber gegen Taxis, →MOOC, →Blogs gegen Journalismus, AirBNB gegen Hotels, Billigflüge gegen Full-Service, Reisebüros gegen Travel-→Websites, →PCs gegen →Mainframes. Die Behauptung, dass solche „disruption" nur durch Startups passieren kann ist kaum belegt

Distributed DOS-Attacken (dDoS): →Denial of Service.

DKIM: (Domain Keys Identified Mail) von Yahoo und Cisco entwickeltes Verfahren zur Vermeidung von →Spam und →Phishing. Dabei werden alle ausgehenden Mails mit dem →Private Key der →Domain signiert. Auf diese Weise kann die →Integrität und →Authentizität gesichert werden. Die Domaine des E-Mail-Absenders muss mit der Domain übereinstimmen, deren digitale →Signatur verwendet wurde. Soll 2012 durch →DMARC erweitert werden

DLL-Injection: →Process injection

DLP: →data leak prevention

DMA: 1) (Direct Memory Access) →Zugriff (lesend oder schreibend) auf →Hauptspeicher ohne Beteiligung der →CPU. Wird genutzt um hohe Übertragungsraten zu implementieren ohne parallele Rechenoperationen zu behindern. Kann genutzt werden um z.B. die digitalen →Schlüssel einer →Festplattenverschlüsselung oder die →Passworte für →Betriebssystemzugriff auszulesen. Dies setzt aber voraus, dass der Angreifer Zugriff auf ein laufendes System mit einer entsprechenden Feature hat, z.B. →PCMCIA, →Firewire, →USB 3

2) →Direct Markets Act

DMCA: (Digital Millennium Copyright Act) umstrittenes Gesetz in den USA, das so weit geht, nicht nur Verletzungen des →Copyright unter Strafe zu stellen, sondern auch die Herstellung und den Vertrieb von Produkten mit denen → Kopierschutz umgangen werden kann. →DRM

DMZ: →Demilitarized Zone

DNA: Abfolge von sog. Basen (A, C, G, T) in einem DNA Molekül, der Erbsubstanz. DNA Moleküle bilden Gene, d.h. Stränge auf einem Chromosom, das für ein bestimmtes Eiweiß codiert. DNA ist für die Sicherheit auf mehreren Gebieten relevant:

1) **DNA Analyse** kann Informationen über genetische Herkunft oder statistische Anfälligkeiten für Krankheiten geben. Die so gewonnen Informationen sind extrem sensibel und könnten zur Diskriminierung (z.B. Verhindern des →Zugangs zu Versicherungsschutz) genutzt werden. Sie müssen entsprechend geschützt werden. Siehe auch →Privatsphäre, →PGP, →23andMe)

2) als →**biometrisches Merkmal**. Nicht-codierende DNA Sequenzen werden für die →Identifizierung eingesetzt, derzeit noch hauptsächlich in der →Forensic. Nicht-codierende DNA Sequenzen haben größere Variabilität und damit Trennschärfe. Das Verfahren ist besser zum Ausschluss von Verdächtigen geeignet als für eine Anklage (Gefahr von →False Positives, z.B. durch Rückenmarkspende oder evtl. nicht bekannte Verwandschaft)

3) **Vollständige DNA Sequenzen** die anonym zu Forschungszwecken veröffentlicht wurden wurden 2013 in DNA →Datenbanken wieder erkannt, die zum Zweck der Genealogie (Ahnenforschung) aufgebaut wurden. Die Erkenntnis ist, dass vollständige DNA Sequenzen nie sicher anonym bleiben können

4) DNA soll auch für „forensic phenotyping" eingesetzt werden. Dabei geht es darum, aus einer Analyse von Genen auf äußere Faktoren wie Hautfarbe, Haarfarbe und ethnische Zugehörigkeit (ethnic inference) zu schließen. 2014 noch mit sehr großen Unsicherheiten verbunden, daher problematisch, in D. verboten

DMARC: 2012 Vorschlag zur Verbesserung der →Spamerkennung. Die bisher genutzten Verfahren →SPF und →DKIM leiden darunter, dass das Empfängersystem beim Fehlen einer positiven Identifizierung sehr oft im Zweifelsfall trotzdem das →E-Mail zustellt, da auch reputable Unternehmen oft schlampig beim →E-Mailversand sind. Durch DMARC werden zusätzliche →DNS-records eingeführt die dem Empfängersystem sagen, was bei einer negativen Verifizierung mit dem E-Mail passieren soll. Das Absendesystem kann auch vorgeben, ob und wie es über die Nicht-Verifizierung informiert werden möchte, hierdurch ist →Debugging der Spam-Erkennung möglich. http://dmarc.org/

DMCA: (Digital Millennium →Copyright Act 1998) US-Gesetz das 2 Verträge der World Intellectual Property Organization (WIPO) umsetzt und nicht nur →Raubkopien selbst illegal macht, sondern auch Technologien, die bei der Erstellung eingesetzt werden können. In der EU wurden die beiden Verträge als Copyright Directive (EUCD) umgesetzt. Die Verträge geben Immunität für →ISPs, die für Copyright-Verletzungen über ihre Netze nicht verantwortlich sind, ebenso für →Websites (wie →Youtube) wenn sie von den Raubkopien nicht profitieren und bei Benachrichtung unverzüglich entfernen. Siehe →ACTA, PRO-IP

DNM: →darknet market

DNS: (Domain Name System) Schema, mit dem →Domain Names in 4-teillige numerische →IP-Adressen umgewandelt werden, Grundlage der Adressierung im →Internet. Implementiert durch viele →DNS Server. Diese

Server sind auch beliebte Angriffsziele, da mit ihrer Hilfe →DoS, →dDoS, →Phishing und andere →Angriffe ausgeführt werden können (z.B. →DNS Cache Poisoning oder →DNS →Amplification mittels open DNS resolvers). Siehe →Reverse DNS Lookup, →DNSSEC, →DNS over TLS, →IDN, →ICANN

DNSBL: →Blacklist, die sich über das →DNS-Protokoll abfragen lässt

DNS Amplification: →Angriff bei dem „open DNS resolvers" dazu gebracht werden, dass sie Antworten auf vorgebliche DNS Anfragen (mit gefälschter →IP-Adresse) an das Opfer senden. Auf diese Weise kann im Rahmen eines →dDoS eine vielfach größere Datenmenge erzeugt werden als das angreifende →Botnet selbst senden könnte. Open DNS resolver sind solche, die auch Anfragen beantworten, die nicht aus ihrem „Service Gebiet" stammen. Dies ist spezifiziert als →BCP38

DNS Cache Poisoning: Verfahren für →Man-in-the-Middle Angriffe über Manipulation von →DNS-Servern

DNS over TLS: (DoT) Seit 2019 verfügbares Verfahren, bei dem die →DNS Abfragen über →TLS verschlüsselt gesendet werden. Problematisch ist dabei, dass diese Provider im →Webbrowser konfiguriert werden müssen und bei Beibehaltung des Defaults 1 Provider alle DNS-Abfragen einer großen Zahl von Nutzern bekommen (in denen durchaus sensible Informationen stecken). Angeboten haben ich 2019 →Google, Cloudflare und andere. Nutzer müssen aktiv einen Anbieter ihres Vertrauens auswählen

DNSSEC: (Domain Name System Security Extensions) Erweiterung zum DNS-Protokoll, um →Angriffe auf und über das →DNS-System zu erschweren. Es nutzt →Authentifizierung und →digitale Signaturen, kann aber nur durch gemeinsame und koordinierte Aktion vieler Parteien eingeführt werden, unterstützt auf Client-Seite erst in Windows 7 oder Windows Server 2008 R2

DNS Server: Rechner, der das →DNS Schema implementiert. Firmen mit →Webauftritt unterhalten meist eigene DNS Server, meist sogar redundant. Ein Ausfall des DNS Servers legt meist alle Internetfunktionen lahm, d.h. kein →Websurfen, kein →E-Mail mehr

DNT: (→Do-not-track Header)

Dokument: →Datenträger und die aufgezeichneten Daten, die normalerweise dauerhaft und von einem Menschen oder einer Maschine gelesen werden können [ISO 2382/4]

DOM: (Document Object Model) →API und logische Repräsentierung von →HTML und →XML-Inhalten (üblicherweise einer →Webseite in einem →Webbrowser). →JavaScript und ähnliche Sprachen erlauben eine Manipulation des gesamten DOMs, d.h. →BHOs oder in einer Webseite eingebundene →iFrames können andere Teile des DOMs verändern, z.B. →URLs. Dies kann für →Angriffe genutzt werden, z.B. →Clickjacking. Siehe →DHTML

DOM Storage: (auch Web Storage, HTML5 Speicher oder Supercookies) neue Technik damit eine →Website Informationen in einem →Browser speichern kann. Neu in →HTML5 und ersetzt die bisherigen →Cookies. Kann wie diese auch für →Tracking der Benutzer genutzt werden. Bei Verwendung vieler solcher Speichermöglichkeiten (Cookie, →HTML 5 Store, →Flash Cookie) wird es für den Benutzer fast unmöglich, alle Tracking-Elemente zu entfernen

Domain: 1) Namensstruktur im →Internet. Top-Level Domain sind entweder Länderkennungen (.at: Österreich, .de: Deutschland, ...) oder andere Kategorien (edu education com commercial org organization mil military). Die vollständige Domäne (→Domain Name) besteht aus einem Begriff oder Namen plus der top level Domain (z.B. orf.at). Siehe →NXDOMAIN

2) lokaler Sicherheitsbereich mit zentraler Verwaltung der Ressourcen in einem →Netz mit →Windows-Rechnern. Siehe →PDC, →Active Directory

Domain Controller: →PDC

Domain Name: Internetadresse einer Organisation im →Internet, z.B. sicherheitskultur.at. →Domaine

Domainnamen-Piraterie, Domain Squatting, Cybersquatting: Registrieren von →Domain Namen mit dem Ziel, sie später mit Gewinn zu verkaufen (z.B. an ein Unternehmen oder eine prominente Person gleichen Namens) oder für →PPC zu nutzen (bezahlte Werbung, zumeist für die Konkurrenz des Unternehmens). Streitigkeiten um Domainnamen sollen über →UDRP gelöst werden. Siehe →Domain Parking, →Traffic Diversion

Domain Generation Algorithmus: (DGA) in →Botnetzen genutzte Technik um nach Ausschalten der zentralen →C&C Server oder nach →sinkholing weiterhin die Kontrolle über die infizierten Rechner zu behalten. Dabei werden über diesen „gut versteckten" →Algorithmus →Domain Namen als Zufallsketten erzeugt, die dann im Bedarfsfall von den Betreibern des Botnets registriert werden. Wenn solche Netze „lahm gelegt" werden sollen so müssen vorher auch diese Domains unter die Kontrolle der Sicherheitsaktivisten gebracht werden

Domain Parking: Registrierung von →Domain Namen die Ähnlichkeiten zu bekannten Domänen aufweisen und auf der Werbeinhalte zusammen mit „geklauten" Inhalten legitimer →Websites angeboten werden. Diese werden

leider auch von →Suchmaschinen indiziert und erzeugen auf diese Weise Werbeeinnahmen, direkt oder über →Search Arbitrage. Benutzer kommen auch bei fehlerhafter Eingabe auf diese Seiten, daher auch →Typosquatting. Für die Top 2000 Domänen gibt es ca. 80 000 Namensvariationen. Eignet sich auch für →Phishing oder Abfangen von vertippten →E-Mails

Dongle: 1) zu Sicherheitszwecken genutztes kleines Gerät, das in die serielle, die parallele oder →USB-Schnittstelle eingesetzt wird und z.B. sicherstellen kann, dass nur eine bestimmte Anzahl von →Anwendern eine lizensierte Software benutzen kann. Zum Teil sind die Geräte „transparent" konzipiert, d.h. das ursprüngliche Gerät an dieser Schnittstelle kann immer noch genutzt werden

2) Anhängsel an einem →Ethernet-Adapter (z.B. →PCMCIA) in einem →Notebook, in das das Netzwerkkabel eingesteckt wird

Do-not-track Header: (DNT) Funktionalität in modernen →Webbrowsern bei denen der Browser jeder →Website kommuniziert, dass der →Benutzer nicht wünscht, dass sein Verhalten einem →Tracking unterliegen soll. Unklar ist bisher, wie die Websites dies umsetzen, bzw. umsetzen sollten/müssen. So wäre zu klären, ob bereits jegliche Statistiken eines →Webserver als Tracking zu betrachten sind, oder nur wenn die Logs Personen zugeordnet werden (oder werden können). Wird 2013 fast vollständig ignoriert

Doorbell: Smart Doorbell (Türklingeln) →IoT-Geräte von →Amazon (Markenname Ring) oder von →Google (Markenname Nest). Diese Klingelsysteme sind mit Videokameras verbunden die nicht nur ein Betrachten des Eingangs vom Türöffner ermöglichen, sondern die Bilder auch in die jeweilige →Cloud streamen (bei Ring optional). Problematisch ist, dass diese Kameras auch den öffentlichen Raum abdecken und Polizeibehörden →Zugriff auf diese Videos durch einfache Erlaubnis des Wohnungs- oder Hausbesitzers bekommt statt durch Genehmigung durch einen Staatsanwalt. Für Ring gibt es eine →Social Networking App („Neighbors") mit deren Hilfe Inhalte mit Nachbarn und/oder der Polizei geteilt werden. In einigen Gemeinden, auch in Europa werden Geräte bezuschusst wenn die Nutzer bereit sind, der Polizei Zugriff zu geben.

Der Ring-Geräte gelten als recht unsicher, Account Details vieler Geräte sind im →Internet verfügbar, es gibt spezielle →Hacker Tools. Die Kameras sind zum Teil mit einer smarten Türöffnung verbunden, die Hackern ein Öffnen der Türen ermöglichen kann. Solche Kameras können nach einer Trennung vom Partner zu →digitaler Gewalt genutzt werden. Daher ist nach einer Trennung ein Zurücksetzen aller →Passworte wichtig

DoS: →Denial of Service

Double-Opt-In: Technik des →Permision Marketing, bei der der Kunde auf einer →Website seine Zustimmung (z.B. zum Erhalt von Werbemails) bestätigen muss, dann eine →E-Mail erhält und noch einmal bestätigen muss. So soll verhindert werden, dass jemand ohne seine Zustimmung teilnimmt. Siehe →Opt-In

Downgrading: Akzeptieren älterer Konventionen und Standards, kann zum Sicherheitsrisiko werden, wenn z.B. statt →SSL3 auch SSL2 akzeptiert wird

Download: (engl. herunterladen) →Daten und →Dateien aus dem →Internet holen, z.B. Programme, Texte, Bilder, Musikstücke, Videos, Filme. Da in →Programmen und anderen Objekten →Malicious Code enthalten sein kann nicht immer ungefährlich. Schutz dagegen bieten aktualisierter →Virenschutz und aktualisierte Software

Downtime: Ausfall eines Systems, z.B. Computer oder Netzwerks mit verminderter →Verfügbarkeit. Kann Folge von technischen Fehlern oder →Denial of Service Angriffen sein

Doxing: Hacker-Slang: die (persönlichen) →Daten einer fremden Person (oder einer Firma) veröffentlichen um dem Opfer zu schaden, z.B. der Angriff 2014 gegen →Sony oder →HBGary Federal oder die Veröffentlichung von persönlichen Daten oder Fotos von Prominenten. Dies wird jedoch auch oft als Form des Cyber Bullying (Cyber Mobbing) gegen beliebige Personen eingesetzt, oft in der Gamer-Szene, sehr oft gegen Frauen. Siehe auch →SWATting als Steigerungsform des Mobbings

DP-3T: (Decentralised Privacy-Preserving Proximity Tracing) →Protokoll zur Orten anderer →Apps in unmittelbarer Nähe, siehe →Corona Apps

DPA: 1) (data protection act) britisches →Datenschutz-Gesetz von 1988

2) (Differential power analysis) →side channel Angriff

3) (Dynamic passcode authentication), siehe →CAP

DPAPI: (Data Protection API) →API in →Windows ab Windows2000 zum →Verschlüsseln hauptsächlich von symmetrischen Schlüsseln. Die große Herausforderung dabei ist, dass diese verschlüsselt gespeichert sein sollten, die würde jedoch wieder einen neuen Schlüssel erforden. DPAPI löst dieses Problem indem der Master Key mit dem ‚user logon secret' (i.d.R. das →Passwort) generiert wird. Mit diesem Master Key werden dann alle →Daten verschlüsselt. Auf dem →Domain Controller wird ein ‚backup' abgelegt, z.B. für Fälle wenn das Passwort zentral zurückgesetzt wird

DPI: →Deep packet inspection

DR: (→Disaster Recovery)

DRAM: (Dynamic random access memory) Halbleiter-→Speicher, der flüchtig ist (→Remanence) (im Gegensatz zu SRAM) und daher ständig „refreshed" wird. Beispiel für DRAM ist „DDR SDRAM"

Drive-by-Infektion: heute dominierender →Angriff über präparierte →Website bei der →Malware ohne Interaktion mit dem →Anwender installiert wird (Infektion über Software wie z.B. NeoSploit). Verwendet →Verwundbarkeiten in →Anwendungen und →Active Content. Vorteil für den Angreifer ist, dass kein Eindringen in das Zielnetz und den Ziel-Rechner notwendig ist, der Benutzer ruft (unwissentlich) die Malware selbst ab. Siehe →iFrame, → Malware-Schutz

Driver: 1) Software im →Betriebssystem, die für die Kommunikation mit einem spezifischen Gerät zuständig ist. Gefährlicher →Angriffspunkt, wenn z.B. ein modifizierter Driver installiert wird, der zusätzliche Aktionen tut (z.B. weiterleiten von Daten, unterdrücken von Informationen). Letzteres wird z.B. bei einem →Root Kit verwendet, der die →Dateien der →Infektion für andere →Programme, z.B. auch →Virenschutz, ausblendet.Daher kann wirkliche Sicherheit nur für ein Gesamtsystem zertifiziert werden, nicht durch die →Zertifizierung von Einzelkomponenten. Siehe →TOE

2) Ursache, z.B. cost driver als Faktor der die Kosten beinflusst. Die Analyse von Drivern ist ein Punkt einer tiefer gehenden Sicherheitsanalyse, denn viele Probleme können nur durch Behebung der eigentlichen Ursachen, z.B. zu geringe Qualifikation oder Sicherheitskenntnisse der Beteiligten behoben werden

DRM: (Digital Rights Management) Technologien um die Verwendung und vor allem das Duplizieren von elektronischen →Dokumenten und →Dateien, z.B. Texte, Filme oder Musik (→mp3) zu beschränken. Hierunter fallen z.B. alle →Kopierschutztechnologien, aber auch weiterführende Technologien, die z.B. einschränken, wie oft ein Musikstück gehört werden kann. Gegen Profis weitestgehend wirkunglos, für normale Nutzung oft sehr behindernd. Siehe →DCMA, →AACS. DRM wird auch als Weg zu →DLP vorgeschlagen, setzt dann aber flächendeckende Bewertung alles Daten voraus (→Dateien und Datenbank-Inhalte) (→Asset Classification)

Drohne: unbemannte Flugzeuge die militärisch für direkte physische →Angriffe, aber auch für →Surveillance eingesetzt werden (mehr zu diesem Aspekt unter →UAV unmanned areal vehicle).

Immer kleinere und billigere Modelle sind 2013 auch für Private leistbar und über →Smartphones leicht zu steuern. Dies eröffnet neue Möglichkeiten für →Stalking

Dropbox: →Cloud Service zur Synchronisierung von →Dateien zwischen →Rechnern (und →Smartphones). Bequem zu nutzen, aber problematische Sicherheit da kein →Passwort für den →Zugriff notwendig ist, sondern nur eine Config-Datei, die falls auf einem anderen Rechner installiert, vollen Zugriff ermöglicht. Verwendet →Deduplication über →SHA-256 Hashes, was bei Manipulationen den Zugriff auf fremde Dateien ermöglichen kann. Außerdem lassen sich auf diese Weise auch Dateien auf Dropbox speichern ohne dass sie mit einem Account verknüpft sind (z.B. mit illegalen Inhalten). Dateien werden zwar nach dem Transport im →Data Center verschlüsselt, die →Schlüssel liegen jedoch unter Kontrolle des Betreibers und sind für alle →Benutzer einheitlich. Siehe auch →Shadow-IT

Alternative Angebote wie →SpiderOak und →Wuala unterstützen automatische →Verschlüsselung mit Kontrolle der →Schlüssel durch den Benutzer, was jedoch eine Wiederherstellung nach Schlüsselverlust verhindert. Live Mesh, SugarSync bieten diese Sicherheit nicht. →CrashPlan bietet lokale Verschlüsselung mit →Key Escrow

DropMyRights: →Programm unter →Windows um Anwendungen wie →E-Mail oder →Webbrowser ohne Privilegien ablaufen, obwohl der Benutzer →„Admin-Rechte" hat. Siehe →Safer, →root jail

Dropzone: →Server im →Internet, in den →Keylogger und andere →Schadsoftware auf einem infizierten →PC die gestohlenen →Daten ablegen. Durch Analyse der Daten in diesen Servern gewinnt man Informationen über die →Cybercrime Economy

DRP: (Disaster Recovery Plan) Wiederherstellungskonzept, →Disaster Recovery

Druckausgaben: oft ein Sicherheitsrisiko, z.B. wenn vertrauliche Informationen im Drucker verbleiben. Siehe →Multifunktionsprinter, →Fax, →Postkästen

Drucker: →Multifunktionsprinter

DAS: →Digital Services Act

DSB: →Datenschutzbeauftragter, in Österreich auch →Datenschutzbehörde, der Nachfolger der →Datenschutzkomission

DSE: (Desktop Search Engine) Sammelbegriff für Programme wie Google Desktop, die Dateien in einer lokalen Speicherumgebung genauso indizieren wie Seiten im →Internet. Sicherheitsrelevant, da viele dieser Programme Suchanfragen auch an den Anbieter der Software weiterleiten, sofern dies nicht bei der Konfiguration verhindert wird

DSig: →XML DSig

DSIN: (Deutschland sicher im Internet) wegen starker Industrienähe umstrittene Aufklärungskampagne zu Internet-Sicherheit. https://www.sicher-im-netz.de/

DSK: (→Datenschutzkomission)

DSL: (Digital Subscriber Line) gemeinsamer Name für verschiedene Techniken für eine schnelle Datenverbindung über das Telefonnetz. Eine weit verbreitete Technik ist →ADSL

DSP: (digital signal processing) hardware-Konzept der Signalverarbeitung, bei dem analoge Signale (Ton oder auch Funkfrequenzen) zuerst digitalisiert werden und dann mittels sehr schneller Spezialprozessoren verarbeitet werden. DSP ist die Grundlage der heutigen →Handys, aber auch von Technologien wie →Stimmerkennung und auch Erkennung von Emotionen aus der Stimme (→Privatsphäre). Siehe auch →Software-defined Radio

DTD: (Document Type Definition)

1) Definition der in einem →XML Dokument verwendeten "Tags",

2) in →HTML 4 verwendeter Standard zur Darstellung von Formatierungsregeln im Webbrowser

DSRC: (Dedicated Short Range Communication) mit einer Reichweite von ca. 300 Metern, geplant für den Einsatz bei →C-ITS

DTO: (Disruptive Technology Office) →ARDA

Dual control: →4-Augen-Prinzip

DuckduckGo: →Suchmaschine, eine der Alternativen zu der dominierenden von →Google. DuckduckGo bietet im Gegensatz dazu keine personalisierten Suchergebnisse, da sie keine →Daten der Nutzer sammeln. DuckduckGo sucht seine Ergebnisse aus 400 Quellen, z.B. aus →Wikipedia, aber auch anderen Suchmaschinen wie z.B. Bing, Yahoo! und Yandex. Sie verwenden auch einen eigenen →crawler

Dumpster Diving: Durchsuchen von Müll- und Altpapierbehältern nach Informationen z.B. zur Vorbereitung von →Social Engineering (Telefonlisten, Aktennotizen u.ä.) und →Wirtschaftsspionage

Dunbar Number: Zahl der Personen, mit denen Menschen eine nähere Beziehung haben können, wird zwischen 100 und 250 angegeben, oft wird 150 angenommen. Bezeichnend ist, dass die durchschnittliche Zahl von →friends auf →Social Networks wie →Facebook sehr weit darüber liegt. Als Grund wird oftmals →FoMo genannt. 2013 gibt es Social Networks, die bewusst die Zahl der Kontakte sehr niedrig halten

DVB-H: (Digital Video →Broadcasting–Handhelds) digitale Übertragung von Multimediadiensten an mobile Geräte mit geringer Auflösung und hoher Kompression (nicht als aktiver download sondern zeitgleich an alle Geräte). Gesendet wird über UHF-, VHF-oder L-Band Kanäle, d.h. die Geräte brauchen entsprechende Empfangseinrichtungen

DVB-T: (Digital Video Broadcasting Terrestrial) digitale Übertragung von Fernsehbildern über UHF- und VHF-Kanäle

DVD: (Digital Video Disk) digitales Speichermedium ähnlich einer CD-ROM, aber mit höher Kapazität (zwischen 4,7 und 8,5 GB) die es auch als beschreibbare Variante gibt. DVDs sind auf Grund ihrer hohen Kapazität mehr noch als CD-ROMs sicherheitsrelevant, da mit ihrer Hilfe große Datenmenge über die Unternehmensgrenzen hinweg transportiert werden können. Als →Kopierschutz wurden für kommerzielle Filme auf DVDs 8 Regional Playback Control (RPC)-Codes eingeführt. Damit soll verhindert werden, dass eine in Asien oder USA gekaufte DVD in Europa gespielt werden kann. Es sind jedoch entsprechende Freischaltcodes für alle Abspielgeräte im →Internet zu finden (http://www.dvd-sucht.de/codefree.php). Zum weiteren Schutz sind die meisten kommerziellen DVDs mit dem Content Scrambling System (→CSS) verschlüsselt. Das →Open-Source-Programms →DeCSS kann die Verschlüsselung umgehen. Siehe auch →Tails

DVP: (Digital Video Broadcasting) technischer Standard für die Übertragung von Rundfunk und Fernsehen in digitaler Form. Unterstützt auch die →Verschlüsselung des Signals für Pay-TV

DVR: (Datenverarbeitungsregister) zentrale Meldestelle für österreichische Unternehmen, die personenbezogene Daten verarbeiten. Es wird betrieben von der →Datenschutzbehörde und wurde durch eine Verordnung basierend auf dem österreichischen →DSG2000 eingerichtet. Das Register ist seit 2014 für jeden einsehbar und zeigt, welche Datenverarbeitungen durch Firmen eingemeldet wurden

Dynamic Code Obfuscation: automatisiertes Verändern des →Programmcodes einer →Schadsoftware mit dem Ziel, die →Patternerkennung eines →Malware-Schutzes zu überlisten. Siehe →Code Obfuscation, →Polymorphismus

Dynamic DNS: spezielle Form von →DNS, bei der die →IP-Adresse, die einer →Internet-→Domäne zugeordnet ist, wechseln kann. Dies ist z.b. notwendig, wenn der betreffende Rechner über einen →ISP angeschlossen ist, der bei jeder Verbindung eine neue Adresse vergibt (was bei →xDSL oft der Fall ist). Solche Tricks werden auch für →Angriffe im →Internet eingesetzt, wenn z.B. →Trojaner den Kontakt mit dem Steuerungsrechner über schnell wechselnde dynamische DNS-Einträge herstellen

Dynamic Host Configuration Protocol: →DHCP

E2EE: →End-to-end →Encryption

EAC: (Extended Access Control) verbesserte Verschlüsselung für den →ePass (wegen Kritik an →BAC). Jedoch nicht von der →ICAO standardisiert und nur für spezielle Daten

(→Fingerabdruck) vorgesehen

e-Administration: →e-Government

EAM: (Enterprise Application Integration) →Messaging

EAN: (European Article Numbering) 8-14-stelliges Barcode-System zur Markierung von Produkten in Läden. Als EAN·UCC heute auch in den USA im Einsatz. Wird heute meist durch →EPC (→RFID) abgelöst, eine Ausnahme ist aber z.B. der Zahlungsanbieter →Bluecode der auf der Grundlage ein Bezahlen an →Bankomatkassen erfolgreich anbietet aber in Zukunft wohl auf →QR Code wie er in China für solche Zahlungen genutzt wird umsteigen wird

EAP: (Extensible Authentication Protocol, RFC 2284) Teil von →IEEE 802.1x, eingesetzt für die →Authentifizierung in →LAN→Switches. In →Wireless Networks in IEEE 802.11i und →WPA verwendet. Es schließt einige Sicherheitslücken in →WEP. Es wurde ursprünglich für →PPP entwickelt und gilt für drahtlose Verbindungen als unsicher. EAP ist nur ein generelles Framework, es liegen zahlreiche inkompatible Implementierungen vor, z.B. →EAP-MD5, →PEAP, →EAP-TLS, →EAP-TTLS, →EAP-IKEv2, →EAP-FAST, →LEAP. EAP-SIM und EAP-AKE für →Handys

EAP-FAST: Cisco-Implementierung zur Verbesserung von →LEAP, gilt auch als unsicher und schwer zu implementieren

EAP-IKEv2: EAP-Variante auf der Basis von →IKE mit Client- und Server-→Zertifikaten

EAP-MD5: EAP-Variante auf der Basis von →MD5, gilt es sehr unsicher

EAP-TLS: EAP-Variante auf der Basis von →TLS und Client→Zertifikaten, was die Implementierung aufwendiger gestaltet

EAP-TTLS: EAP-Variante auf der Basis von →Server→Zertifikaten

EAS: (Electronic Article Surveyance) elektronische Diebstahlsicherung. Diese Tags enthalten im Gegensatz zu →EPCs keine Daten. Kein Standard, inkompatible Systeme im Markt

EasyPass: System an deutschen Flughäfen, bei denen die Passagiere vollautomatisch mittels ePass (oder in Zukunft →ePerso) und automatischer →Gesichtserkennung abgefertigt werden

e-Banking: (Electronic Banking) selbständiger Bankverkehr von (Privat-)Kunden über das →Internet. Dabei werden entweder →Webbrowser eingesetzt (zumeist für Privatkunden, dann zumeist Internet-Baking genannt) oder spezielle →Clientprogramme z.B. nach dem →MBS, →EBICS oder →HBCI. Erfunden 1983 durch die Nottingham Building Society. Es war in den USA bereits 1980 eingeführt worden, wurde aber 1983 wieder eingestellt. 1998 ist es in den USA bei den meisten Banken im Einsatz. Heute werden bei e-Banking sehr oft →single-page applications eingesetzt.

Alle Daten müssen bei e-banking verschlüsselt übertragen werden, zu diesem Zweck wird bei Browser-Lösungen in der Regel →SSL (bzw. heute →TLS) eingesetzt. →Phisher nutzen aus dass es sehr leicht ist, eine Bankenwebsite zu imitieren und dadurch Kunden zur Preisgabe ihrer →Passworte oder →PINs und von →TANs zu verleiten.

Schutz gegen solche →Angriffe soll durch den Einsatz eines 2. Kanals, z.B. →mTAN über →SMS für die →Autorisierung der Transaktionen erreicht werden. Andere Verfahren nutzen digitale →Zertifikate (bzw. →Schlüssel) auf →Smartcards die über einen Smartcard-Reader an einen PC angeschlossen werden oder über spezielle Geräte die das Zertifikat einer →Bankomatkarte einlesen können. Für die Berechnung des Sicherheitscodes den der Kunde für die Autorisierung eingibt muss der Kunde entweder selbst die Zielkontonummer eingeben oder die Transaktionsinformationen werden über einen sog. chipTAN →Flickercode automatisiert übertragen. Aus diesen Werten berechnet dann das Gerät auf Grundlage des Schlüssels der Smartcord einen →Hash-Wert mit dem der Benutzer die Überweisung autorisiert. (Siehe →CAP, →CardTAN). Auch solche Systeme lassen sich durch →Social Engineering austricksen, z.B. indem der Benutzer vorgegaukelt wird, es würde jetzt ein Test durchgeführt, für den er bestimmte Aufgaben erledigen muss, die dann für die Angreifer zu der nötigen Sicherheitszahl führen.

eBay: bekannteste →Website für private Versteigerungen. Daneben gibt es jede Menge regionale und/oder spezialisierte Websites. eBay und ähnliche Sites haben einen großen Einfluss auf den Handel allgemein, sie verwischen die Grenzen zwischen Privatverkäufen und kommerziellen Firmen. In Bezug auf Sicherheit relevant wegen dem →Rating-System und weil auch viele Kriminelle die Möglichkeiten von eBay für sich entdeckt haben. Siehe http://sicherheitskultur.at/PC-tipps.htm#11. Deutliche Sicherheitskritik bzgl. eBay (z.B. fehlende →Authentisierung der Anbieter) findet sich in http://de.wikipedia.org/wiki/Ebay

e-Billing: Versand von elektronischen Rechnungen. Um Betrug, z.B. Vorsteuerbetrug, zu vermeiden ist dabei eine digitale →Signatur vorgeschrieben. Die Rechnungen selbst können entweder in einem Format sein, das eine automatische Weiterverarbeitung in der IT ermöglicht (→EDI, →EDIFACT, →XML) oder in einem für Menschen lesbaren Format (z.B. →PDF). Die Erfüllung der gesetzlichen Vorschriften aus Steuergesetzen und Buchhaltungsvorschriften können die gesetzeskonforme Umsetzung aufwendig machen

eBook: Inhalte von Büchern in elektronischen Formaten zur Wiedergabe auf →PCs,

→Smartphones oder speziellen Lesegeräten (im Prinzip Smartphones). Wichtige Format sind das offene EPUB (das auf →XML, →CSS und →SVG basiert), bzw. firmen-eigene Format wie bei →Amazon (dessen Lesegeräte aber ebenfalls EPUB unterstützen). Diese Formate erlauben eine dynamische Anpassung der Seitenumbrüche, im Gegensatz zu →PDF, das zwar von allen diesen →Apps dargestellt werden kann, dessen A4-Format auf kleinen →Bildschirmen sehr mühsam ist. Problematisch ist an eBooks (wie auch beim →Streaming), dass die Inhalte nicht gekauft werden, sondern es wird nur ein Nutzungsrecht erworben, das aber (i.d.Regel) nicht weitergegeben werden kann. Trotzdem werden eBooks auch in Leihbibliotheken angeboten, spezielle Lizenzen und spezielle →Software regeln die Anzahl von Kopien die jeweils verliehen werden können. Viele eBooks werden mit →Kopierschutz implementiert, was zusätzliche Einschränkungen für Leser bedeuten kann (ohne Kopierschutz ist oft ein lokales Speichern weiterhin technisch möglich)

ebXML: Message Service Protocol, auf →XML basierendes Verfahren zum Austausch von Informationen zwischen Anwendungen, unabhängig von Protokoll oder Inhalt der Message (kann traditionelle →EDI Formate unterstützen)

EBICS: Kommunikationsverfahren für den →e-Banking zwischen Firmen und Banken. Dabei wird ein spezielles →Clientprogramm eingesetzt. Die Kommunikation erfolgt verschlüsselt und die Transaktionen sind signiert

EC2: (Amazon Elastic Compute Cloud) ist ein zentraler Bestandteil des Amazon Web Services (A.W.S.) Angebots. Es ist ein →Cloud Service bei dem →virtuelle →Server sehr kurzfristig (z.B. für wenige Stunden) zur Verfügung gestellt werden. Wird zum Teil auch für kriminelle Aktivitäten wie →Password-Cracking genutzt. EC2 bietet serverseitige →Verschlüsselung (→SSE), die sicherheitskonzeptionell nicht wirklich akzeptabel ist, aber auch ein →API für client-seitige Verschlüsselung. Solche →cloud-basierte Dienste sind sind eine Weiterentwicklung von →Housing und →Outsourcing. Siehe auch →Shadow-IT

Bei AWS implementieren viele bekannte Firmen (speziell Startups) ihre Internetdienste, z.B. Airbnb, Pinterest, Spotify, Dropbox. Andere Firmen bieten spezielle Dienste, z.B im Bereich →data mining. Siehe →Kubernetes

EC3: →Cybercrime Unit von Europol. Siehe →EU

eCall: Europäisches System, das ab 2018 verpflichtend in Neuwagen eingebaut sein muss und das bei einem Zusammenstoß im Straßenverkehr oder vergleichbaren Unglücken nach dem Auslösen der Airbags automatisch die einheitliche europäische Notrufnummer 112 anwählt und dort die mittels →GPS ermittelten Koordinaten und die Art des Treibstoffs übermittelt.

e-card: ersetzt in Ö den Papierkrankenschein und enthält derzeit (2011) lediglich Name, Geburtsdatum, Sozialversicherungsnummer. Technisch könnten auf dem Chip auch Gesundheitsdaten verschlüsselt gespeichert werden, dies wird aus Datenschutzgründen aber nicht durchgeführt. Der verwendete Chip unterstützt auch die →digitale Signatur. →e-Health, →ELGA

ECC: 1. →Error Correction Code 2. →Elliptic Curve Cryptography

ECG: (E-Commerce-Gesetz) Gesetz zu Fragen des →e-Commerce in Ö. Regelt u.a. die →Haftung von →Diensteanbietern

ECHELON: Abhörsystem, das von den USA (→NSA), Großbritannien (→GCHQ), Kanada und Australien seit den 60iger Jahren betrieben wird. Früher auf den Funk- und Telefonverkehr des Ostblocks ausgerichtet, werden heute vor allem Telefongespräche, →Fax und →E-Mails abgefangen. Echelon steht im Verdacht, zur Wirtschaftsspionage benutzt zu werden, was die Betreiber bestreiten. Verliert seit ca. 2008 immer mehr an Bedeutung gegenüber der →Internet-Überwachung. Siehe →Edward Snowden, →Semantic Forest. Siehe auch http://de.wikipedia.org/wiki/Echelon

Echo chamber, bzw. Filterblase: beschreibt die Situation, bei der Menschen immer nur den Meinungen, Positionen und Informationen ausgesetzt sind, die sie eh schon haben (so wie bei einem Stammtisch unter Gleichgesinnten).
Dies kann im →Internet auf 2 Arten auftreten. Zum einen haben wir den Echokammer-Effekt in →Social networks bei denen sich ähnlich denkende in Gruppen zusammenfinden und gegenseitig ihre Positionen verstärken. Dann gibt es den Filterblasen-Effekt (filter bubble) der durch →Algorithmen (z.B. →Suchmaschinen oder Vorschlagsalgorithmen in Social Networks oder auf →Youtube) entsteht, wenn Vorschläge für Inhalte oder Suchergebnisse auf der Basis früherer Aktivitäten getroffen werden. Dadurch werden die Nutzer immer wieder zu den gleichen Inhalten geführt

Echokammer: →Echo chamber

e-Commerce: (electronic commerce) Durchführung von kommerziellen Transaktionen über Kommunikationsnetze (heute meist das →Internet) und mit Hilfe von Computern. Konkret ist dies meist das Kaufen und Verkaufen von Waren oder Dienstleistungen und die Durchführung von finanziellen Transaktionen. Mangelnde Sicherheit, bzw. das subjektive Empfinden mangelnder Sicherheit, wird dabei oft als eines der Hemmnisse des →e-Commerce genannt. Auch die →Darknet markets fallen unter e-Commerce

Edge: 1) (Enhanced Data Rates for GSM Evolution) bezeichnet eine Technik zur Erhöhung der Datenrate in →GSM-Mobilfunknetzen durch effizientere Modulationsverfahren

2) (engl. Kante) →Zugangspunkt zu einem Netz (zB Firmennetz), implementiert z.B. als →Firewall, →Proxy, etc.

3) bei einem →Social Graph die Verbindung zwischen 2 Knoten der einen Kontakt abbildet. Kann gerichtet sein oder weitere Eigenschaften haben

Edge Server: Begriff für →Systeme, die einen →Zugang zu einem Netz ermöglichen, verwendetz.B. von →Microsoft, →Oracle oder →IBM WebSphere

EDI: (Electronic Data Interchange) frühe Form des →e-Commerce, seit den 80iger Jahren standardisiert. Der Austausch von Geschäftsdokumenten jeglicher Art (z.B. Rechnungen, Angebote, Zollerklärungen, Lieferscheine, etc.) unter Verwendung vorgegebener Formatierungsstandards. Traditionelles Format ist die US-amerikanische Norm →X.12, eine europäische Antwort darauf ist UN/ →EDIFACT. In Teilmärkten haben sich z.T. andere Normen durchgesetzt, so z.B. →HL7 im Gesundheitswesen und →Odette im Automobilbau. Heute werden oft neue Formate genutzt, die auf →XML-Technologie beruhen. Eine Standardisierung für viele verschiedene Fachgebiete findet z.B. unter →RosettaNet statt. Traditionell werden EDI-Dokumente unverschlüsselt und ohne digitale Signatur übertragen. Die Übertragung fand traditionell über →VANs statt. Dadurch wurde eine gewisse Sicherheit erreicht. Heute werden EDI-Dokumente oft über das →Internet versandt. Dafür werden die Dokumente heute oft verschlüsselt und signiert. Abgegrenzt von →Messaging

EDIFACT: (eigentlich UN/EDIFACT) Internationaler →EDI-Standard, sollte eigentlich →X.12 ablösen, hat dies jedoch wegen der hohen Umstellungskosten bestehender Anwendungen nie geschafft. Unterstützt in der Originalform weder Signatur noch Verschlüsselung

EDIINT: (EDI over the Internet) Arbeitsgruppe der Internet Engineering Task Force →IETF. Erarbeitet Standards für den Austausch von Geschäftsdokumenten (→EDI) über das →Internet

e-Discovery: ursprünglich US-Gesetzesänderung (Federal Rules of Civil Procedure), die besagt, dass Firmen für Informationen, die evtl. Beweis vor Gericht sein könnten, wissen müssen, ob diese verfügbar sind und falls ja, wo (einschließlich →Backup-Medien) und sie müssen die Informationen auf Anfrage fristgerecht zur Verfügung stellen können. Firmen können →Data Retention Regeln erstellen die zu einer fristgerechten Löschung führen, müssen diese jedoch strikt einhalten. E-Discovery schließt auch →Daten wie →Chat-Protokolle, →Voicemail, →Social Media Aktivitäten wie →Blogs, →Social Networks, etc. ein. Diese Regeln gelten mittlerweile auch in einigen anderen Ländern als der USA. In →Microsoft Exchange sind geeignete Funktionaliäten enthalten und können natürlich auch in anderen Ländern eingesetzt werden (mögliche Einschränkungen durch →Datenschutz sind natürlich möglich). Siehe →Legal Technology

eDonkey: (eDonkey2000) →Tauschbörse im →Internet. 2005 erreichte die →RIAA die Einstellung. Siehe →P2P, →Overnet

edu-card: →Smartcard für Schüler und Lehrer in Ö, derzeit noch im Pilotversuch. Kann ein →Zertifkat enthalten und auch zum Öffnen von →Türen verwendet werden, was ziemlich zwangsläufig zu einer →Protokollierung führt

EDVIRSP: umstrittene franz. Polizeidatenbank in der Personen ab 13 Jahre Alter gespeichert werden sollen. Im ersten Entwurf alle, bei denen der Verdacht besteht, dass sie in der Zukunft evtl. gegen die „öffentliche Ordnung“ verstoßen könnten, jetzt geändert auf „öffentliche Sicherheit“. Siehe →Präventionsstaat

Edward Snowden: →Whistleblower der als Mitarbeiter einer US-Sicherheitsfirma →Zugriff auf geheime →NSA-Papiere bekam, diese 2013 veröffentlichte und einige Aufregung auslöste, weil damit das Ausmaß der →Überwachung des →Internet-→Datenverkehrs öffentlich wurde. Siehe →PRISM, →XKeyscore, →Tempora, →Bullrun, →GCHQ.

2019 veröffentlichte er seine Erinnerungen als Buch. Die US-Regierung hat erfolgreich die Einnahmen aus dieser Veröffentlichungen einklagen können, da er als Ex-Geheimdienstmitarbeiter seine Texte vor der Veröffentlichung hätte genehmigen lassen müssen.

Ein zweifelloser Erfolg seiner Aktivitäten ist, dass bis dahin die →NSA die damals noch unverschlüsselten Datenströme zwischen den Rechenzentren z.B. von →Google mitgeschnitten hat. Google hat sehr schnell auf flächendende interne →Verschlüsselung umgestellt und durch Druck auf →Website-Betreiber dafür gesorgt, dass nun auch (fast) alle Websites →HTTS nutzen. Dabei hat die Initiative von →Let’s Encrypt sehr geholfen.

EEA: (European Economic Area) Wirtschaftsraum der größer ist als die EU, da er auch die ehemligen EFTA Länder enthält, mit Schweiz als Sonderfall

EEG: (Elektroenzephalogramm) →P300

EES: →Escrow Encryption Standard

EFI: (→Extensible Firmware Interface)

EFS: (Encrypting File System) →Verschlüsselung von Verzeichnissen und →Dateien auf →Windows Rechnern. Auf →Desktop Geräten ab Windows 2000 standardmäßig, kann zur Verschlüsselung von Dateien herangezogen

werden. Siehe →BitLocker

EFS basiert auf einem Verschlüsselungsverfahren unter Verwendung von zwei kryptografischen Schlüsseln. Der →symmetrische Schlüssel wird zur Verschlüsselung der →Daten verwendet, das →asymmetrische Schlüsselpaar dient der Verschlüsselung des symmetrischen Schlüssels. Bei richtiger Implementierung gilt diese Art der Datenverschlüsselung als ziemlich sicher.

Es ist jedoch zu beachten, dass EFS „nur" Dateien auf einem →Datenträger verschlüsselt. Wenn dieser Datenträger (z.B. diese Serverplatte) über Netzwerk erreichbar ist, dann ist die Übertragung der Daten über dieses Netz NICHT gesichert.

In →Windows XP (und Nachfolgern) Professional können auch „Offline Dateien" mit EFS verschlüsselt werden

eGK: (elektronische Gesundheitskarte) soll ab 2007 in Deutschland die Krankenversicherungskarte (eine reine Speicherkarte) ersetzen. Enthält im administrativen Pflichtteil die Versicherungsdaten, im freiwilligen Teil Gesundheitsinformationen, z.B. Notfallsdaten und eine elektronische Krankenakte. Die Karte ist aus Datenschutzgründen umstritten. 2019 wurden viele →Verwundbarkeiten, speziell bei der Registrierung von Karten für Ärzte, aufgezeigt, mit deren Hilfe ein →Angreifer auf Patientendaten in der elektronischen Patientenakte (→ePA) zugreifen könnte. Siehe →e-Health

Egress Filtering: Filtern von Daten auf dem Weg nach außen, z.B. um zu verhindern, dass ein intern installierter →Trojaner mit der Außenwelt Kontakt aufnimmt. Siehe →ingress filtering

e-Geld: Sammelbezeichnung für karten- und software-basiertes Geld (→Kartengeld, →Netzgeld)

Beispiele für Kartengeld sind die deutsche →GeldKarte oder die (jetzt obsolete) österreichische →Quick-Karte, bei der in einem Chip ein Geldbetrag „gespeichert" wurde, der bei Automaten und in Geschäften genutzt werden konnte.

Beispiele für Netzgeld sind z.B. →PayPal als „electronic money" (auch →paysafecard, →M-PESA, WebMoney, Perfect Money, Liberty Reserve (geschlossen in 2013 durch US-Behörden), Robbokassa, CashU, Upay, Ukash, die oft/zumeist →anonymes Bezahlen ermöglichen und für Kriminelle wichtig sind, →Geldwäsche) oder →virtual currencies wie →Bitcoin, → Facebook Credits, Nintendo Points oder Linden Dollar in →Second Life.

→Kreditkarten (im engeren Sinne) gehören nicht zu e-Geld, da diese eine Verknüpfung mit einem realen Konto darstellen. Siehe →Bargeld

e-Government: Einsatz von IT für Informationspräsentation, Kommunikation und Transaktionen von Regierung und Verwaltung, intern und mit Bürgern und Unternehmen

e-Health: neues Schlagwort für Konzepte wie →Telemedizin, Vernetzung im Gesundheitswesen oder für öffentliches Anbieten von Gesundheitsinformationen. Umstritten, wenn Aspekte des →Datenschutzes berührt werden und die Implementierungen mehr oder weniger große →Schwachstellen aufweisen. Siehe →eGK, →e-Card, →ELGA, →ePA

EICAR: (European Institute for Computer Antivirus Research) bekannt vor allem durch die EICAR-Testdatei, die zum Testen der Funktion von →Antivirensoftware eingesetzt wird, der sog. EICAR-Virus

eID: a) Sammelbegriff für elektronische Ausweise, die in den EU-Ländern eingeführt werden. Siehe →ePass, ePerso
b) eine Funktionalität des deutschen →ePerso bei der sich Privatstellen berechtigen lassen können auf nicht-hoheitliche Datenelemente des Chips zuzugreifen

Einmalpasswort: engl. →OTP, One-time–password, →Passwort

Eintrittswahrscheinlichkeit: in der →Risikoanalyse ein wichtiger, aber oft nur schwer bestimmbarer Faktor. Negative Ereignisse mit einer hohen Eintrittswahrscheinlichkeit stellen ein hohes Risiko dar. Als Basis können dienen:

- interne oder externe Statistiken
- Informationen aus Presse
- Effektivität der eigenen Schutzmaßnahmen
- Motivationsgrad möglicher Angreifer
- Aufwand und Kosten für Angreifer (z.B. ob Tools für den Angriff vorliegen, Automatisierungsmöglichkeiten)
- erwarteter Gewinn der Angreifer

e-Justice: oft synonym mit →elektronischem Rechtsverkehr, Einsatz von IT zwischen Judikative, Bürgern und Unternehmen

Electromagnetic Analysis: →Side Channel Angriff durch Analyse der elektromagnetischen Abstrahlung entweder während der Ausführung von →Computerbefehlen oder bei der Übertragung oder Darstellung von Ergebnissen. Siehe →Van Eck Strahlung

Electronic Vaulting: Sichern von →Daten für →Backup- oder →Archivierungszwecke über eine Datenleitung, oft als Service angeboten

Elektronische Rechung: →e-Billing-

Elektronischer Rechtsverkehr: (ELRV) Vornahme von Rechtsgeschäften auf elektronischem Weg, sitzt zumindest →digitale Signaturen voraus, um →Authentizität zu erzeugen. Siehe →e-Justice, e-Administration

Elektronisches Wasserzeichen: Markierung in elektronischen Dokumenten, mit denen sich Dokumente auch nach starken Veränderungen

identifizieren lassen. Im Gegensatz dazu die →digitale Signatur, wo auch minimale Veränderungen erkannt werden

Element: →Messaging →Software die das →Matrix →Protokoll nutzt und mit allen anderen Instanzen kommunizieren kann die auch dieses Protokoll unterstützen (föderierte Umgebung)

ELGA: (elektronischer Gesundheitsakt) in Ö nicht ganz unumstrittene Infrastruktur, durch die Gesundheitsdiensteanbieter (→GDA) mittels eines Dokumentenregisters (→registry) auf dezentral gespeicherte Krankenakten zugreifen können, die bei anderen GDAs gespeichert sind. Menschen können sich von diesem Dienst abmelden, dann stehen jedoch einzelne Features wie eMedikation (d.h. Rezepte die elektronisch an die Apotheke übermittelt werden, nicht zur Verfügung)

Elliptic Curve Cryptography: (ECC) →Verschlüsselung mittels eines alternativen mathematischen Verfahrens zu anderen →Public Key Algorithmen wie →RSA. ECC kommt mit kürzeren Schlüssellängen aus, wird daher oft auf →Smartcards eingesetzt. Auf dieser Basis sind auch digitale Signaturen (ECDSA) und Schlüsselaustausch (ECMQV) möglich. http://arstechnica.com/security/2013/10/a-relatively-easy-to-understand-primer-on-elliptic-curve-cryptography/

Embedded System: →Software, die in einem Gerät, bzw. Maschine oder Fahrzeug enthalten ist, oft in der Form eines →EPROMs. Alle Software ist inhärent fehlerbehaftet und damit eine Quelle für Fehler und →Schwachstellen. Heute ist ein großer Anteil der Probleme mit Autos software-generiert. Es sind auch gezielte →Angriffe gegen solche Geräte möglich, so hat 2011 ein Forscher drahtlos gesteuerte Insulinpumpen zur Abgabe einer tödlichen Dosis bringen können. Ein Riesenproblem ist bei diesen Systemen, dass es zumeist nicht möglich ist, nachträglich Fehlerkorrekturen zu machen, d.h. →Verwundbarkeiten bleiben bis zum Wegwerfen des Geräts erhalten. Diese Verwundbarkeiten liegen manchmal nicht in der eigentlichen Software, sondern in Bibliotheken die genutzt werden und selbst Fehler enthalten

E-Mail: Kurzform von ‚electronic mail', bezeichnet den Austausch von Nachrichten nach dem Store-and-Forward Prinzip, d.h. die Nachricht wird in einem standardisierten Format (→MIME, →S/MIME) zwischen verschiedenen Mailservern weitergereicht, bis sie den Endpunkt erreicht. Dort wird sie in einer →Mailbox für den Abruf durch den Empfänger bereitgehalten. Verwendete Protokolle waren früher oft →X.400, heute fast nur noch SMTP. SMTP-basierendes E-Mail wird leider heute oft für Angriffe durch →Malicious Code und →Phishing verwendet, da es keinerlei Sicherheitsvorkehrungen, z.B. →Authentifizierung des Absenders oder des Rechners des Absenders erlaubt. Durch die Verwendung von →digitalen Signaturen und →Verschlüsselung im S/MIME Format kann eine erhöhte, aber doch noch unzureichende Sicherheit bzgl. → Integrität, →Vertraulichkeit und →Zurechenbarkeit erreicht werden. Seit den Veröffentlichungen von →Edward Snowden werden die Mails zwischen den Mailservern fast nur noch verschlüsselt übertragen, und zwar mit →TLS/SMTP. Auch der Abruf über →POP3 oder →IMAP wird seitdem fast immer verschlüsselt. E-Mail wurde oft totgesagt, seine Stärke ist die Kompatibilität. Egal welche E-Mail-Software oder welchen Anbieter ein Nutzer verwendet, die Nachricht wird trotzdem (mit überschaubaren Kompatibilitätsproblemen, z.B. bei Umlauten) zugestellt und kann beantwortet werden. Dies soll bei →Messaging Diensten erst mittels →Digital Market Act erreicht werden. Siehe →MTA, →E-Mail-Flood

E-Mail-Flood: Form des →Denial of Service →Angriffs bei dem eine Mailbox mit einer großen Zahl von E-Mails gefüllt wird, so dass die legitimen Mails darin untergehen. Solche Angriffe sind kommerziell günstig zu haben: 100 000 E-Mail für 70 $. Wird z.B. (in Verbindung mit DoS gegen die Telefonleitungen) genutzt um in Verbindung mit einem anderen →Angriff zu verhindern, dass z.B. eine Beschwerdestelle oder Helpdesk z.B. während eines →Phishing-Angriffs erreichbar ist

E-Mail made in Germany: (EmiG) leicht umstrittene Initiative von einigen deutschen Serviceprovidern die als Antwort auf die →Edward Snowden Veröffentlichungen ihren Marktanteil stärken wollen indem sie untereinander nur noch verschlüsselt und nur mittels Verbindungen im Schengen-Raum kommunizieren wollen. Kritisiert werden, dass die Teilnehmer sehr strenge Aufnahmekriterien haben und nicht auf der Basis von weit verbreiteten Standards arbeiten wollen, sondern eigene Konzepte haben. Das →BSI hat 2015 die Richtline TR-03108 erlassen, die im Gegensatz zu EmiG auf →DANE mit →TLS in Verbindung mit →DNSSEC setzt

EME: (→Encrypted Media Extension)

EmiG: (→E-Mail made in Germany)

eMoney: →e-Geld

Emotionserkennung: die Analyse von audiovisuellen und anderen Signalen (z.B. Texten) zur Erkennung des Gefühlszustandes einer Person. Dieser Bereich der Forschung wird vor allem von den großen US-Firmen wie →Google, →Amazon, →Facebook betrieben. Ziel ist es, durch Kenntnis des augenblicklichen Gefühlszustandes noch präziser Werbung zu schalten und z.B. augenblickliche Empfindsamkeiten ausnutzen zu können um sogar in gewissem Maße eine Steuerung der Menschen zu erreichen

EMRK: (→Europaische Menschenrechts-konvention)

EMSCB: (European Multilateral Secure Computing Base) →open-source Alternative zu →NGSCB, die eine Software (→Turaya) zur Nutzung von →TPM herausbringt

EMV: (**E**uropay, **M**aster, **V**isa) Standard für die Implementierung von →Smartcards auf →Bankomat- und →Kredikarten im Einsatz bei →POS-Terminals als sicherer Ersatz für Magnetstreifen. Damit soll →Skimming verhindert werden. In den USA und vielen anderen Ländern (noch) nicht implementiert, daher fallen dort die Karten in den Magnetstreifenmodus mit seinen →Schwachstellen zurück. In England wird die Implementierung →Chip-n-PIN genannt, Chip-n-PIN soll in den USA in 2015 eingeführt werden.

EMV unterstützt für die Nutzung z.B. in Parkhäusern →Fallback zu „no authentication", d.h. nicht abgesichert. EMV verlangt in der Variante „SDA: Static Data Authentication" (im Gegensatz zu „DDA: Dynamic Data Authentication") keine verschlüsselte Kommunikation zwischen →PIN-Eingabe-Tastatur und Chip, daher können in diesem Fall auf dem Prozessorboard des Eingabegeräts die PIN und die Kontoinformationen in Klartext ausgelesen werden und dann für eine gefälschte Magnetstreifenkarte verwendet werden. Das EMV-Protokoll unterstützt auch →chip-basierte Kreditkarten. 2012 wurden Schwächen in den Anforderungen für die Generierung einer „unpredictable number" (→random number) aufgezeigt.

2013 wird EMC auch drahtlos mittels →NFC eingesetzt, was die Angriffsmöglichkeiten erhöht. Ebenfalls problematisch ist, dass das eigentlich nur für mechanische Kontakte zwischen →Chip und Lesegerät gedachte Protokoll ab 3013 auch für →NFC, d.h. drahtlos genutzt wird. Auf diese Weise kann ein Angreifer wenn er in der Nähe der Karte ist (z.B. U-Bahn) einige Statistik- und Identitätsdaten des Chips auslesen und bis zur Betragsgrenze bei der eine PIN-Bestätigung notwendig wird, auch Geld abbuchen. Allerdings braucht der Angreifer dafür eine Händler-ID von einem Kreditkartenunternehmen. Er wird daher nicht leicht anonym an das Geld kommen. Siehe →Geldkarte, →Quick, →CAP

EMV Cap: siehe →CAP

Encapsulating Security Payload (ESP): →IPSec-Header zur →Verschlüsselung des Inhalts eines →IP-Pakets. Bestandteil von →IPv6

Encrypted Media Extension: (EME) →Kopierschutz für Streaming Inhalte durch Erweiterung des →HTML5 Standards. Wird jetzt (2014, nach viel Druck) in allen →Browsern implementiert. Dabei werden die kommerziell erworbenen Inhalte mit dem Gerät verknüpft

Encryption: →Verschlüsselung

Endianness: bezeichnet die Byte-Reihenfolge in einem Wort eines →Computer→speichers oder bei einer →Datenübertragung. Üblicherweise ist die technische Speichereinheit in einem Computer (z.B. wenn →Daten aus einem Speicher in ein CPU-Register geladen werden) nicht das →Byte sondern ein Wort (z.B. 32 bit = 4 Byte). Wenn ein Text, bestehend aus 4 Zeichen, in 1 Wort gespeichert wird, so könnte das 1. Zeichen entweder rechts oder links im Wort abgelegt werden. Dabei bezeichnet ‚big-endian' die bei uns übliche Richtung von links nach rechts, ‚little-endian' von rechts nach links. Dies gilt auch für Datenübertragungen. Bei bitweisen seriellen Übertragungen wie z.B. RS-232 muss auch noch die Reihenfolge der →Bits definiert werden (RS-232 ist ‚little-endian')

Endpoint Security: (EPS) Begriff für alle Sicherheitsfragestellungen, die Kommunikationsendpunkte wie →PCs, →PDAs, etc. betreffen. Oft befinden sich diese Geräte außerhalb der Firmenumgebung. EPS betrifft den Schutz der Geräte selbst, z.B. durch →Personal Firewall und →Virenschutz, aber auch den Schutz der Netze vor möglicherweise infizierten Geräten. Dies erfordert die automatisierte Überprüfung des Sicherheitszustands des Gerätes und →differenzierte Zugriffskontrolle, möglicherweise →Quarantäne und Aktualisierung von →Patchzustand und →Virenschutz. IDC Definition: „centralized control of security policies on the client level [laptops, PDAs], and for network access points [internal desktops, kiosks and remote servers]". Siehe →TCP, →NAC, →NAP. Andere Anbieter sind Checkpoint, Symantec, Juniper, Qualys, 3Com, ISS, McAfee

End-to-end: →Verschlüsselungskonzept, bei dem die →Daten vom Initiator einer Verbindung bis zur Gegenstelle so verschlüsselt sind, dass nur die jeweiligen Endstellen die Daten entschlüsseln können. Im Gegensatz dazu z.B. Verschlüsselung auf Teilstrecken, z.B. zwischen 2 →Routern die die Verbindung über ein öffentliches Netz bilden. End-to-end bietet die höhere Sicherheit, verlagert aber das →Key handling in die Endgeräte (z.B. →Smartphones). End-to-End Verschlüsselung setzt sich seit den →Snowden-Veröffentlichungen immer stärker durch. 2020 wird es von fast allen Messaging Diensten oder Apps unterstützt. End-to-End Verschlüsselung wird durch die Behörden seit spätestens 2018 stark bekämpft weil dadurch →Messaging-Systeme nicht in der Lage sind, die Inhalte die Benutzer austauschen an Behörden zu liefern (→Crypto

Wars).

Als Hauptargument wird dabei sehr oft Kindesmissbrauch verwendet, so wie →Apple 2021 eine Implementierung der Überwachung auf den Endgeräten selbst vorschlägt. Dieses Thema wird oft als Startpunkt für Vorschläge zur Schwächung von Sicherheit verwendet

ENISA: (Europäische Agentur für Netz- und Informationssicherheit) 2004 von der →EU gegründete Einrichtung mit dem Ziel der Beratung und Koordination der Mitgliedsstaaten beim Aufbau kompatibler IT-Sicherheitsstandards für →IKT-Systeme. Arbeitet eng mit den europäischen →CERTs zusammen. http://www.enisa.europa.eu/. Siehe →EMRK, →Art.29

ENLETS: (European Network of Law Enforcement Services) ist eine Untergruppe der Law Enforcement Working Party des Europäischen Rats. Die wichtigsten Projekte ab 2014 sind: Nummernschilderkennung →ANPR, das Durchsetzen einer Technologie zum Anhalten von Fahrzeugen, →Videoüberwachung und auch →Open Source Intelligence und →Signal Intelligence (→SIGINT) durch geeignete →Sensoren, d.h. Überwachungsgeräte. Gerade die letzten Punkte zählen traditionellerweise nicht zu den Aufgaben von Polizei, sondern von Geheimdiensten

Entdeckung: eine der 3 Aufgaben des Sicherheitsmanagements: durch →Monitoring, →Alarmierung u.ä. möglichst schnell merken, dass ein →Incident passiert ist. Die anderen Aufgaben sind →Prävention und →Reaktion

Enterprise Storage System: Überbegriff für zentrale Speichersysteme, die für mehrere Rechner gemeinsam eingesetzt werden. Dies kann sowohl Plattensysteme wie auch Bandlaufwerke und Roboter enthalten. Wird oft mit dem Ziel der →Hochverfügbarkeit eingesetzt. Siehe →SAN, →Virtualisierung

Enrollment: Wichtiger Sicherheitsvorgang mit dem ein Service aktiviert wird, z.B. die Verknüpfung einer →Kredit-, →Debit- oder →Bankomatkarte mit einem →Smartphone für die Nutzung in →Apple Pay oder →Google Pay. Wenn diese Verknüpfung gut kryptographisch (z.B. über →Schlüssel die sicher auf dem Gerät gespeichert werden) geschieht so stellt diese Verknüpfung einen wichtigen Sicherheitsfaktor dar. Damit kann das so verknüpfte Gerät als 1 Faktor bei der →2 Faktor Authentisierung gerechnet werden = Besitz). Ein 2. Faktor entsteht wenn der Nutzer das Gerät vor der Nutzung entsperren muss, entweder über →PIN, d.h. Wissen oder →Biometrie, d.h. „sein“

Entropy: In der Informationswissenschaft der Informationsgehalt eines Datenelements, wichtig bei der verlustfreien Datenkompression (z.B. →Zip, →GIF, →PNG) und bei der Qualität von →Passworten

Enumeration: →Angriffsmethode bei der z.B. über systematisches Hochzählen Zugangsinformationen zu elektronischen Diensten gewonnen werden, z.B. durch Ausprobieren aller numerisch möglichen Telefonummern um →SMS-Empfänger zu finden. Dies liefert aber erst mal „nur“ die →Benutzerkennung, → Zugang zu den Diensten sollte eigentlich erst nach einer →Authentisierung möglich sein. Dies ist eine →Schwachstelle wenn z.B. die →Authentisierung aber z.B. durch einen nachfolgenden →Social Engineering →Angriff ausgehebelt werden kann, bzw. durch Einrichtung eines weiteren →Accounts mit dieser Kennung, z.B. in einigen →Messaging Diensten

ELENA: (elektronischer Einkommensnachweis, früher →JobCard) umstrittenes deutsches Projekt zur zentralen Speicherung der Einkommensdaten aller Firmenmitarbeiter und Vorgänge bei Arbeitsagenturen sowie Wohn- und Elterngeldstellen bei der Pensionsversicherung. Bürger können bei Besitz einer entsprechenden →Chipkarte und Lesers zugreifen. Mittlerweile (2011) gestoppt

ePass, ePass(port), e-passport: teilweise verwendete Bezeichnung für den →biometrischen Reisepass, der mittels →RFID ausgelesen werden kann und ein Bild des Ausweisinhabers und in D. (auf freiwilliger Basis) auch →Fingerprints auf einem Chip gespeichert enthält. Auf Grund von Protesten wurde eine →Verschlüsselung der drahtlosen Kommunikation eingeführt (→Basic Access Control). Die Nutzung weiterer biometrischer Merkmale ist geplant und aus Gründen des möglichen Missbrauchs umstritten. Aus der Wirtschaft wird bereits vorgeschlagen, die Datenbanken mit den biometrischen Daten auch für andere Zwecke zu nutzen. Die angebliche Fälschungssicherheit ist nicht gegeben, da derzeit (2008) nur 5 von 45 Ländern die dafür notwendige Public Key Directory (→PKD) einsetzen. Siehe →FIDIS, →RFIDIOt, →MRTD, →e-Perso

EPC: (Electronic Product Code) Nachfolger des →EAN zum Identifizieren von Waren zur Erleichterung des Supply Chains (Kette vom Hersteller zum Kunden). Benutzt →RFID-Technologie, aber mit deutlich höherer Frequenz und erlaubt Auslesen über viele Meter. Mit 96-bit Länge können nicht nur Produkte, sondern auch einzelne Waren bezeichnet werden. EPC verwendet die Nummerierung des →GTIN. Wenn beim Kauf der Chip nicht zerstört wird (KILL-command), kann der Käufer des Artikels drahtlos weiterverfolgt oder wiedererkannt werden. Dies berührt

Aspekte der →Privatsphäre. Das Design enthält eine TID (tag ID), die →Cloning erschweren könnte, jedoch nicht verwendet wird und enthält keine →Authentifizierung oder →Verschlüsselung. EPC wird trotzdem für US-Passcard und elektronische Führerscheine in den USA eingesetzt und ist über bis zu 50 Meter auslesbar. Siehe →ONS

ePerso: deutscher Personalausweis in Scheckkartengröße mit →RFID, →digitalem Photo und optionalen digitalen →Fingerabdrücken. Enthält ein →Zertifikat für „einfache" →digitale Signatur, kann für „qualifizierte" Signatur nach dem Signaturgesetz freigeschaltet werden. Siehe →PACE, http://www.personalausweisportal.de/

e-Person: umstrittenes Konzept einer (zukünftigen) weitgehend autonom agierenden Maschine für die ein eigener Rechtstatus mit Rechten, Pflichten (z.B. Steuerzahlung) und Verantwortung (d.h. Haftung) geschaffen werden soll (analog zu juristischen Personen). Dies wird u.a. bei der Haftung von Unfällen von →autonomen Fahrzeugen relevant. Bei der Umsetzung einer e-Person wären →Programmierer und Hersteller aus der Verantwortung. Die Versicherungsindustrie sieht hier neue Geschäftsfelder. 2017 hat sich das EU-Parlament damit beschäftigt, es gibt aber (zum Glück) erhebliche Widerstände gegen ein solches Konzept. Dies ist zu unterscheiden von →artificial personas, unter denen meist →Bot-Systeme verstanden werden. Bei diesen liegt die Problematik eher darin, dass sie sich als non-human zu erkennen geben sollten

ePHI: (Electronic Protected Health Information) schützenswerte Gesundheitsdaten in digitaler Form. Siehe →PHI, →eHealth, →HIPPA

EPROM: (Erasable Programmable Read-Only Memory) Technologie, bei der → Software in einem Chip gespeichert werden, der ein späteres Überschreiben des Programms erlaubt. Im Gegensatz zum normalen Speicherchip bleiben im EPROM die Daten auch im ausgeschalteten Zustand erhalten und kann im Normalbetrieb nicht überschrieben werden (read-only). Für die Löschung wird oft UV-Licht verwendet. Danach kann der Chip neu beschrieben werden. EPROMs werden z.B. für das →BIOS verwendet. Heute werden jedoch dafür auch oft (E)PROM in einem Flash-Speicher-Chip verwendet, die jederzeit eine Neu-Programmierung erlauben

Erpressung: Geschäftsmodell einiger →Hacker (oft in Verbindung mit der →organisierten Kriminalität). Gegen Firmen häufig über →DoS-Angriffe, gegen Private auch durch →Verschlüsselung von →Dateien oder „Entführung" von →E-Mails in →Webmail-Accounts (→RansomWare)

ePrivacy Regulation: geplante (Stand 2021) EU-Verordnung die die seite 2002 gültige ePrivacy Directive ablösen soll. Dabei werden in Ergänzung zur →DSGVO viele Details geregelt, z.B. →Cookie Handling oder die Bedeutung von →Metadata. Der 2021 vorgelegte Kompromiss wird sowohl von Seiten der Industrie wie auch der Datenschutz-NGOs kritisiert

ePA: (elektronische Patientenakte) soll ab 2021 nicht nur die Gesundheitsdaten von 73 Millionen Patienten in Deutschland zentral verwalten sondern auch zur sicheren Kommunikation der Praxen und Kliniken untereinander dienen. 2019 wurden viele →Verwundbarkeiten aufgezeigt. So wurde in Kernkomponenten für den Aufbau und die Absicherung des Gesamtnetzes stark veraltete Software identifziiert. In dem Design des Systems liegt offenbar der grundlegende Fehler vor, dass die Kompromitierung 1 Arztpraxis das Gesamtsystem bedroht. Denn wenn ein →Angreifer in 1 Praxisnetz eindringt so kann der von dort in das Gesamtsystem

E-Privacy Directive: →Directive on Privacy and Electronic Communications, auch → Cookie Directive genannt, beschäftigt sich mit confidentiality of information, treatment of traffic data, →spam und →cookies. Bei letzteren wird ein →Opt-in gefordert

EPS: (Electronic Payment Standard) Schnittstelle in die Online-Zahlungssysteme der österreichischen Banken. Ermöglicht Zahlungsservices durch Dritt-Anbieter ohne dass dieser die →PINs oder →TANs oder den Kontostand des Kunden weiß

Error Correction Code: (ECC) Verfahren bei dem durch zusätzliche Daten eine Fehlerkorrektur bei der →Datenübertragung oder Datenspeicherung möglich ist. Verfahren zur Sicherung von Daten-→Integrität

ESB: (Enterprise Service Bus) Abstraktionsschicht einer Service Oriented Architecture (→SOA), implementiert z.B. mittels →JMS. Siehe →Messaging, →Bus

ESCON: (Enterprise System Connection) Serielle IO-Technik (Lesen und Schreiben von Daten) für Großrechner

Escrow: Nutzung einer neutralen Instanz im Rahmen eines Geschäftsvorganges, z.B. für den Austausch Geld gegen Ware. In der IT verwendet für

1) →Key Escrow (Wiederherstellung des →Zugriffs auf →verschlüsselte Inhalte ohne den korrekten Schlüssels, z.B. nach Ausscheiden des Mitarbeiters und

2) für die Hinterlegung von →Quellcode von Programmen, so dass dieser auch nach einer evt. Auflösung des Software-Herstellers noch

verfügbar ist

Escrow Encryption Standard: (EES) Standard für Schlüsselhinterlegungsverfahren. Siehe →Key Escrow

ESMTP: Erweiterungen von →SMTP, auch in Richtung Verschlüsselung durch die Nutzung von →TLS

ESP: →Encapsulating Security Payload

ESS: (Embedded Security System) →TPM Chip von IBM, siehe →TCG. Die Client Software dazu heißt CSS (Client Security System)

Ether: Geldeinheit bei der virtuellen Währung →Ethereum. Siehe →Cryptocurrency

Ethereal: →open-source Tool zum Analysieren von Übertragungsprotokollen und zum Auflisten der Inhalte (→Protocol Analyzer). Wird für →Angriffe und →Penetration Tests genutzt, heute →Wireshark

Ethereum: Project, das auf →Blockchain-Technologie neben Zahlungen auch →Smart Contracts implementieren will, die „→Turing Complete“ sind, d.h. beliebige (Rechen-) Aufgaben lösen können. (Die Scripting Language von Bitcoin ist hingegen nur eingeschränkt.) Ethereum ist deswegen 2016 nach →Bitcoin das Blockchain-Projekt mit der höchsten Marktkapitalisierung, noch vor den etablierteren Währungen wie Litecoin und Ripple. Die Währungseinheit von Ethereum ist →Ether

Ethernet: Architektur für →LANs, 1976 von Xerox entwickelt und von der →IEEE als IEEE 802.3 standardisiert. Ursprünglich maximal 10 Mbps, heute auch als 1000 Mbps und 1 Gbps verfügbar

Ethical Hacker: 'guter' →Hacker, der in ein System eindringt, um dessen →Schwachstellen kennen zu lernen („White Hat“, im Gegensatz zum „Black Hat“). Anschließend informiert er die Betreiber über seine Aktion, damit sie ihr System verbessern (→responsible disclosure). Umstrittenes Vorgehen wenn dafür unautorisiert in fremde Systeme eingedrungen wurde, anstatt per Auftrag oder durch testen der →Software in eigenen Systemen)

Ethik: ein System von Normen das besagt, welches Verhalten „richtig“ ist. Ethik geht über gesetzes-konform hinaus – nicht alles was legal ist, ist auch ethisch. jedoch erlaubt ethisches Verhalten nur dann Gesetzesübertretungen wenn deutlich ist, dass die Gesetze unethisch sind. Ethische Fragen sind z.B. im Bereich von →responsible disclosure ein großes Thema (→ethical hacker), aber auch im Bereich →Überwachung und →AI können IT-Entwickler immer wieder mit ethischen Fragen konfrontiert sein. Siehe auch →Businessethik, →autonomous car, →Algorithmenethik

ETSI: (European Telecommunications Standards Institute) Non-profit Normungsorganisation der Telekommunikationsanbieter. Verantwortlich für Standards wie →GSM, →UMTS und →NGN, aber auch den Abhörstandard ES 201 671 und den Regeln für kooperative intelligente Transportsysteme (→C-ITS)

EU: (European Union) bei vielen Themen aus diesem Text relevant, Z.B. →EMKR, →ENISA, DEA (Digital Agenda for Europe) Grundlage in Bezug auf →Trust und Sicherheit für die Europe 2020 Strategy. EPCIP (=European Programme for Critical Infrastructure Protection, →CIP). EC3 (=European →Cybercrime Center), Teil von EUROPOL. Wichtig ist der Unterschied →Directive vs. →Regulation. In beiden wird oft Bezug genommen auf ICT (=Information and Communication Technology) und NIS (=Network and Information Security)

eUICC: embedded →UICC. →SIM-Karte die auch remote provisioining unterstützt, d.h. ein oder mehrere Mobilfunkanbieter können ihre →Authentisierungsinformationen in der Karte ablegen. Das würde z.B. ermöglichen, dass →Tablets oder →Autos in jedem Land einen lokalen Mobilfunkanbieter nutzen können

EULA: (End User Licence Agreement) bei der Installation von Software entweder durch Öffnen der Packung („Shrinkwrap-Agreement“) oder durch einen Accept-Button („Clickwrap-Agreement“) getroffene Vereinbarung. Die Rechtswirksamkeit solcher Verträge wird zumindest in Europa zum Teil bestritten. Diese Agreements sind G.rundlage für den Streit zwischen →Adware-Firmen und Anti-Spyware-Anbietern. Die Adware-Firmen sagen, dass ihre Programme (die als „Beipackung“ bei anderer Software mitinstalliert werden) keine illegale →Spyware sind, weil der Benutzer ja die EULA akzeptiert habe. Daher wird manche der Adware von kommerziellen Anbietern von Antiviren-Software ignoriert

Europäische Menschenrechtskonvention: (EMRK) §8 regelt den Recht auf Achtung des Privat- und Familienlebens, inkl. Telekommunikationsgeheimnis und ist daher Grundlage des →Datenschutz in Europa. Siehe →Art.29

European Data Protection Board (EDPB): Nachfolger der → Article 29 Data Protection Working Party

EuroSOX: (8.EU-Richtlinie) Umschreibung für Richtlinien der Europäischen Kommission, die an die →SOX-Gesetzgebung angelehnt sind. Korrekt: Richtlinie 2006/43/EG des Europäischen Parlaments und des Rates vom 17. Mai 2006 über Abschlussprüfungen von Jahresabschlüssen und konsolidierten Abschlüssen, zur Änderung der Richtlinien 78/660/EWG und 83/349/EWG des Rates und zur Aufhebung der Richtlinie 84/253/EWG des Rates

EUROSTAT: europäische Statistikbehörde, die sich auch um IT Sicherheits-→Benchmarking bemüht

Evasion: auch AET (Advanced Evasion Techniques) Tricks auf →IP-Ebene mit deren Hilfe Angreifer die Erkennung ihres →Datenverkehrs zur →IPS/IDS oder in →Firewalls verhindern. Beispiele sind z.B. Paket Fragmentation kombiniert mit Manipulationen der Pakete auf anderen Ebenen des →ISO-Modells

e-Vaulting: →Electronic Vaulting

EV-DO: (Evolution-Data Optimised, auch 1xEV-DO) Datenübertragungsstandard der 3. Generation (wie →UMTS) im Wirelessbereich, im Einsatz außerhalb von Europa. Gehört zur Klasse der CDMA2000 High Rate Packet Data Air Interface Protokolle. (→CDMA) Verwendet eine 42-bit Pseudo-noise (PN) Sequence und einen CAVE-Algorithmus (Cellular Authentication and Voice Encryption) zur Generierung eines 128-bit Shared Secret Data (SSD) Schlüssels und verwendet dann →AES. Gilt es sehr sicher

Event: sicherheitsrelevantes Ereignis, oft gemeldet im Rahmen von Security →Monitoring, kann →Incident Management triggern

e-Voting: Verfahren zur elektronischen Stimmabgabe. Problematisch ist dabei die Implementierung der Anforderungen an Wahlen: allgemein, unmittelbar, gleich, persönlich, frei und geheim. *Allgemein* bedeutet, dass jeder wählen kann, auch bei Behinderungen und ohne Notwendigkeit des Besitzes von speziellen Geräten. *Gleich* und *persönlich* bedeutet, dass die Wähler sicher identifiziert werden und ihr Wahlrecht gegen eine Wählerliste verifiziert werden muss, z.B. durch eine →Bürgerkarte. *Gleich* bedeutet, dass jeder nur einmal wählen darf. Die →Identifizierung bringt Probleme für die geheime Wahl. Es darf keine Möglichkeit bestehen, den Inhalt der Stimmabgabe auf die Person zurückzuführen. Anderseits soll die Wahl *auditierbar* sein, d.h. bei einer Anfechtung soll eine nachträgliche Kontrolle möglich sein. *Persönlich* bedeutet auch, dass verhindert wird, dass ein Wähler seine Stimme verkaufen kann, z.B. indem er einen Beweis für seine Stimmabgabe erbringt (dies ist auch bei Briefwahl problematisch). Auch soll eine Wahl unter Zwang verhindert werden. Die Manipulation des Prozesses, die Speicherung und die Auszählung darf nicht manipulierbar sein. Das System muss für den gesamten Wahltag zur Verfügung stehen

EV Certificate: (extended validation SSL Certificate) spezielles →SSL-→Zertifikate mit strengeren Prüfungsanforderungen beim Kauf des Zertifikats von der Zertifizierungsstelle, daher sicherer als die traditionellen SSL-Zertifikate. EV Zertifikate werden in der →URL Adresszeile des → Browser in grün angezeigt. Seit dem Erfolg von →Let's Encrypt mit kostenlosen, von allen →Browsern akzeptierten Zertifikaten die sich automatisiert installieren und aktualisieren lassen werden diese EV Certificates fast nur noch von Banken eingesetzt

Evercookies: neuer Begriff für →Cookies die ein Benutzer nicht (mehr) Löschen kann. Die Techniken bestehen i.d.Regel aus einer Kombination von „regulären" http-Cookies, → Flash-Cookies, Silverlight-Cookies und → HTML5-„local storage". Der Trick besteht darin, dass auf Lösch-Aktivitäten des Nutzers reagiert wird, indem die gerade gelöschten Cookies eines Typs aus den Informationen der anderen Cookies wiederhergestellt werden. Zusätzlich kommen sogar spezielle →PNG-Graphiken im →Cache des →Browser zum Einsatz. Siehe https://en.wikipedia.org/wiki/Evercookie

Exchange: 1) jegliche Art von Datenaustausch

2) Internet-Exchange, siehe →IXP

EXIF: Standard für die Kodierung der Seriennummer und Kameraeinstellungen einer digitalen Kamera in →JPEG- und →TIFF-Bildern. Wie alle →Metadaten können sie ungewollt Informationen preisgeben [Namen von fotografierten Personen (→face recognition), →GPS-Location, Datum der Aufnahme]. Siehe →Fingerprinting, →Image Tag

Explainability: Eine der Forderungen an AI-Systeme – sie sollen in der Lage sein, ihre Entscheidungen erklären zu können. Gerade bei Entscheidungen die auf der Grundlage von →Deep Learning oder →Machine Learning getroffen werden ist dies derzeit nicht der Fall. D.h. die zum Teil für uns Menschen absurden Fehler bei der Bilderkennung sind nicht leicht zu vermeiden, was z.B. bei →autonomen Fahrzeugen sehr problematisch ist

Exploit: in der IT: →Software, die eine →Schwachstelle ausnutzt und daher für einen →Angriff eingesetzt werden kann. Exploits werden in der Regel einige Zeit nach der Veröffentlichung einer Schwachstelle von →Hackern im Internet veröffentlicht. Durch immer bessere Zusammenarbeit und Arbeitsteilung bei den Hackern verkürzt sich diese Zeitspanne immer mehr. Siehe →Zero-Day-Exploit, →Zero-Click Exploit, →Vulnerability, →CVE

Exploit Bundle: bei →Schadsoftware die Kombination meherer Exploits zu einem Paket. Wenn der Benutzer die Datei öffnet oder die →Website besucht, so werden verschiedene Exploits „durchprobiert".

Intelligent Bundles prüfen dabei zuerst die

→Betriebssystemversion und welche andere verwundbare Software installiert ist und führen dann gezielt einen passenden Exploit aus. Unintelligent Bundles sind billiger und exekutieren einfach alle Exploits, was nicht immer zum erwünschten Erfolg führt

Extended Validation SSL Certificate: →EV Certificate

Extensible Firmware Interface: Nachfolger von →BIOS, die zentrale Schnittstelle zwischen der →Firmware, den einzelnen Komponenten eines →Rechners und dem →Betriebssystem

Extension (File Extension): im Unix oder MS →Windows System die letzten 3 oder 4 Buchstaben des Dateinamens, abgetrennt durch einen „ . “ (Punkt). Die Extension bestimmt, welches Programm von MS Windows gestartet wird. Da MS Windows so eingestellt werden kann, dass diese Extensions nicht gezeigt werden, ist es möglich, Benutzern ausführbare Dateien (.exe, .vbs, etc.) unterzuschieben, ohne dass sie dies erkennen können (z.B. *ihre_Daten.txt.vbs*, wobei .vbs vom System evtl. nicht gezeigt wird). Auf →Apple-Systemen wird die Zuordnung einer Datei zu einem Programm als Teil der Datei selbst gespeichert (Resource Fork). Extensions sind dort nicht nötig, bzw. haben keine funktionale Bedeutung

Externalität: wenn Kosten für irgendwas nicht vom Verursacher getragen werden sondern von einem Externen. Die Kosten bei den Externen sind sehr oft ein Vielfaches vom Gewinn den der Versursacher machen kann. So entstehen beim Versenden von →Spam erhebliche externe Kosten durch Nutzung der Bandbreite, Arbeit für die Entwicklung von Spam-Filtern, Arbeit beim Nutzer durch Löschen des Spams die alle nicht vom Spammer getragen werden. Beim Spamversand kommt oft noch hinzu, dass dafür →Rechner von Internetnutzern infiziert werden (→Botnet), deren Bereinigung für den Betroffenen wiederum ein Vielfaches von dem kostet, was der Angreifer dafür lukrieren konnte. Ebenso sprechen wir von Externaliltäten wenn eine Entscheidung, z.B. für die Nutzung einer bestimmten Technologie, Auswirkungen auf andere Menschen hat, die sich gar nicht für diese Technologie entschieden haben. Ein Beispiel dafür ist →Face Recognition. Auch Personen, die nicht in →Facebook (oder anderswo) aktiv sind werden nachdem sie von →friends getaggt worden sind, ab dann von entsprechenden Programmen erkannt

e-Voting: Durchführung von Wahlen mittels elektronischer Verfahren, entweder direkt (→ DER) oder über Papier und →OCR-Erfassung

exFAT: neues →File System von →Microsoft für →Flash Drives. Behebt viele Probleme von →FAT, ist aber nur unter →Vista verfügbar

FA: (Front End Adapter) Anschluss eines →Enterprise Storage Systems an ein →SAN

Fabber: Technoslang für →3D Drucker

Fabric: Hardware und Software, die →Enterprise Storage Systeme mit Rechnern verbindet. Als Fabric bezeichnet man eine →Fibre Channnel Architektur, bei der die Geräte netzartig miteinander verbunden sind. Dies steht im Gegensatz zum Ring und der Point-to-Point Architektur

Facebook: derzeit (2021) populärste →Social Networking →Plattform, die sich gerade in →Meta umbenannt hat. Die wichtigsten Angebote des Unternehmens sind das gleichnamige →Social Network, dazu →Instagram und der Messenger →Whatsapp.

Da das primäre Geschäftsmodell aller kommerziell betriebenen Plattformen auf dem Aufbau von →Benutzerprofilen beruht und den zugeordneten Datensammlungen, mit deren Hilfe Werbung effektiv (abhängig von Eigenschaften und Interessen des Betroffenen) platziert werden kann, führt dies zwangsläufig dazu, dass Datensammlungen entstehen die (direkt oder indirekt) Werbetreibenden zur Verfügung gestellt werden. Diese Profile bestehen nicht nur aus den Daten, die der Benutzer selbst eingibt, sondern auch aus dem was der Benutzer sonst noch im Web tut. Dies wird über →Like-Button auf den anderen →Websites erhoben, die auch dann Daten sammeln wenn der Benutzer gar nicht darauf klickt und selbst dann, wenn der Benutzer gar nicht bei FB angemeldet ist.

Seit ca. 2014 hat Facebook sein Geschäftsmodell immer wieder leicht geändert. Firmenaccounts konten zu Beginn kostenlos alle erreichen, die über „Like“ ihr Interesse bekundet hatten. Jetzt werden reguläre Postings auf Firmenaccounts nur noch einem kleinen Prozentsatz der „Fans“ zugestellt, außer es wird als Werbung bezahlt.

Dieses Geschäftsmodell von Facebook wird ausgenutzt und ausgehebelt durch →Click Farmen, d.h. manuelle oder automatisierte Betriebe die falsche Profile („fake profile“) erstellen und damit einen großen Erfolg im Publikum vorspielen. Grund ist, dass Popularität heute oft in Likes auf Facebook oder Followern auf →Twitter gemessen werden. Daher kaufen Firmen, Musiker und Politiker Fans und →Likes. Solchen falschen Likes verwirren die →Algorithmen von Facebook, denn außer diesem Like macht der falsche Benutzer keine weiteren Interaktionen, was wiederum auf vermeintliche Unattraktivität der Postings deutet. 2015 bestätigte Facebook, dass 7% der 1,39 Milliard. →Accounts „fake“ sind und 28 Mio „undesirable“, z.B.

→Spammer. Facebook unternimmt große Anstrengungen, falsche Accounts zu finden und zu schließen. So verlieren bei solchen Aktionen Firmen und Prominente oft einen sehr großen Teil ihrer Fans.

Wie bei allen kommerziell betriebenen Social Networks wird problematisiert, dass stark emotionalisierende und radikalisierende Postings zu längerer Verweildauer führen und daher von den Auswahl-→Algorithmen bevorzugt werden. Seit verstärkt rechtsradikale oder rassistische Inhalte zu Sperrungen führen weichen diese Nutzer auf Gab oder →Parler aus.

Zu den Datensammlungen gehört auch das Sammeln von Fotos, die mittels →Face Recognition automatisch Personen zugeordnet werden. FB-Benutzer können sich miittels Einstellungen daegegen wehren, automatisch auf Fotos markiert zu werden (→tagging), wer aber gar nicht auf FB vertreten ist und von einem anderen Benutzer markiert wird, wird darüber nicht informiert.

FB hat eine lange Tradition, neue Funktionen einzubauen, die als Voreinstellung weitere Profil-Informationen öffentlich zugänglich machen und vom Benutzer aktiv wieder auf „privat“ zurückgesetzt werden müssen. Außerdem besteht das Problem des →context collapse durch Vermischung von unterschiedlichen Rollen und Zielgruppen. Diese Problematik wollte →Google+ als Angriffspunkt gegen Facebook verwenden. 2012 wird von →Datenschützern die Timeline-Feature kritisiert, die für alle zwingend eingeführt wird. 2012 kauft Facebook die wachsende Konkurrenz →Instagram, 2014 den damals stark wachsenden →Messaging Dienst →WhatsApp.

Zur Problematik des „Teilens“ siehe →Share und zur Problematik der News Feed siehe →Zuckerberg's Law.

Facebook wird auch gern als →Open Source Research bei →Social Engineering und auch für →Angriffe genutzt. Geknackte Facebook-Accounts bringen fast so viel wie Internet-Banking-Accounts.

Siehe auch →friend, →friend-request, →Like-Jacking, →Socialbots, →Facebook Immune System, →Facebook Insights, →CDN, →Big Five

Facebook Connect: →AP, mit dem andere →Websites es ihren →Benutzern ermöglichen können, sich über ihre Facebook ID auf dieser Website anzumelden und →Daten zwischen ihren →Accounts auf den beiden →Websites auszutauschen. Für das Login wird →OAuth genutzt

Facebook Immune System: Schutzkonzept von →Facebook, das auf →AI beruht und versucht auf der Basis von →adversial learning →Angriffe (wie →Spam-, →Socialbots, →Malwareverteilung, →Phishing, und auch „gestohlene“ →Accounts und falsche →Identitäten, aber auch → Kettenbriefe) automatisiert zu erkennen und ebenso automatisiert Gegenmaßnahmen zu implementieren, die diesen Angriff so erschweren, dass er unprofitabel wird. Gegenmaßnahmen sind das Sperren von Eingaben (z.B. →URLs zu Phishing →Websites oder Malware), die Anforderung von zusätzlichen →Authentisierungen oder das Sperren von Accounts

Facebook Insights: spezieller Service für die Betreiber von sog. „Fansites“ auf FB. Dies sind FB-Auftritte von Firmen oder Organisationen. Wenn jemand „Fan“ einer Firma wird, so kann diese ab dann alle Daten sehen, die für „friends“ freigegeben sind. Mit Hilfe von FB Insights kann das Unternehmen weitgehende Statistiken und Analysen über die Besucher ihrer Fansite durchführen, bis herunter auf einzelne Benutzer, deren FB-Namen ebenfalls bekannt sind. Diese personen-bezogene Datenverarbeitung wird jedoch in den Nutzungsbedingungen von FB den Benutzern gar nicht mitgeteilt

Face ID: Von →Apple entwickeltes Verfahren für biometrisches Entsperrens bei →iPhone X. Dabei wird eine Infrarot-Kamera genutzt, die das Gesicht in Datenpunkte übersetzt, die gegen die internen Datenpunkte verglichen werden. Die Sicherheit dieses Verfahrens wird in 2017/18 intensiv getestet werden. Es kann pro Gerät (derzeit) immer nur 1 Person „enrollt“ sein. Dies steht im Gegensatz zu **Touch ID**, der →Fingerabdruck-Erkennung bei früheren Geräten. Siehe auch →Face recognition

Face recognition: (Gesichtserkennung) Form der →Biometrie, bei der die Details eines Gesichts zur →Identifizierung einer Person genutzt wird. Im Falle der Suche einer Person unter vielen Personen derzeit noch sehr fehlerbehaftet, soll jedoch zur →Überwachung eingesetzt werden (→Next Generation Identification). Bereits verfügbar ist automatisiertes Tagging von Personen auf Gesichtern auf →Facebook. Dadurch dass alle Facebook-Profilebilder so analysiert werden und auch alle sonstwie hochgeladenen Fotos ist bei FB eine riesige Sammlung von Gesichts-Profilen entstanden, die auch in anderen Anwendungen, z.B. →Google Glass genutzt werden können. Siehe →3D Face. Viele →Algorithmen in http://face-rec.org/algorithms/

Manchmal werden auch andere Algorithmen als Face Recognition bezeichnet, z.B. das „Entdecken“ eines Gesichts auf einem Bild, bzw. seine Zentrierung oder das automatische Erkennen von Alter und Geschlecht von Personen zu Werbezwecken, z.B. durch intelligente „→Plakate“ mit integrierter Kamera (→targeted

advertising)

FACTA: (Fair and Accurate Credit Transactions Act) US-Gesetz (2003) regelt einige Datenschutzaspekte bzgl. den →Kreditschutzorganisationen Equifax, Experian and TransUnion, z.B. können Bürger 1x im Jahr einen kostenlosen Report anfordern. Siehe →Red Flag Rules, →Schufa – nicht zu verwechseln mit →FATCA

Factory Reset: Vorgang bei dem ein digitales Gerät wieder auf seinen ursprünglichen Zustand zurückgesetzt wird. Alle →Daten und Programme die zwischenzeitlich installiert wurden werden gelöscht. Dies ist bei infizierten →Smartphones oft die einzige sichere Methode der Bereinigung, auch bei →Spy-Apps die ein (Ex-)Partner) (evt.) auf dem Gerät installiert hat

Fahrlässigkeit: grobe Fahrlässigkeit (oder Vorsatz) zieht üblicherweise eine zivilrechtliche →Haftung nach sich. Fahrlässigkeit wird als das Außer-Acht-lassen der gewöhnlich erforderlichen Sorgfalt verstanden und stellt damit eine Pflichtverletzung dar. Die Sorgfalt wird i.d.Regel am →Stand-der-Technik gemessen, dieser wiederum an Normen, →Standards und → Best-Practise Dokumenten

Fail-safe: →Sicherheitskonzept, bei dem beim Ausfall eines Gerätes oder Services ein sicherer Zustand erreicht wird. Beispiel: →Firewall-Ausfall sperrt den Datenverkehr vollständig, statt vollständig zu öffnen

Fail-over: Konzept im Bereich →Hochverfügbarkeit. Bei Ausfall eines Systems wird auf das Ersatzsystem umgeschaltet. Siehe →Hot-Standby, →Cold-Standby

FairPlay: →DRM-Verfahren von Apple zur Absicherung der über iTunes verkauften Musik für den iPOD, 2011 nicht mehr im Einsatz

Fair use: Nutzungskonzept im amerikanischen →Copyright-Recht, das bestimmte nicht autorisierte Nutzungen von geschütztem Material zugesteht, sofern sie der Förderung von "Progress of Science and useful Arts" dienen. Dabei geht es vor allem um sog. Derivate, d.h. neue Werke, die auf dem ursprünglichen Material beruhen. „Fair use“ ist nicht „vertragsfest“, d.h. kann durch Lizenzvertrag entzogen werden. Kontinentaleuropäische Entsprechung ist das sog. Schrankenrecht im →Urheberrecht, das jedoch „vertragsfest“ ist

Fallback: häufige konzeptionelle Sicherheitsschwachstelle, wenn aus Gründen der Rückwärtskompatibilität schwächere Sicherheitsverfahren ebenfalls unterstützt werden, z.B. →SSL mit kürzeren →Schlüsseln, alte Versionen von →SSH, Magnetstreifen statt →EMV-Chips auf →Bankomatkarten

Fälschungssicherheit: Sicherstellen der →Authentizität von Dokumenten, entweder über geeignete Write-only Medien (→WORM) oder →digitale Signatur

Fake: (Fälschung) Vortäuschen von falschen →Daten oder →Websites (z.B. für →Phishing), →Raubkopien, →Spoofing, →Deepfake

Fake News: Schlagwort das Nachrichteninhalte beschreibt, die den allgemein anerkannten Tatsachen wiedersprechen, z.B. „flat-earth“, Impfgegner-Nachrichten, Klimawandelleugner, Mondlandungsleugner, etc. Mit diesem Schlagwort werden aber auch als korrekt anerkannte Nachrichteninhalte als falsch denunziert. Fake-News sollen die Wahl von Trump in den USA und die Brexit-Abstimmung stark beeinflusst haben. Fake News haben ab 2018 zu Lynchmorden geführt (es wurden Nachrichten über angebliche Kindesmorde und ähnliches verbreitet). Dabei wurde speziell →Facebook stark dafür angegriffen, zu langsam solche aufhetzerischen Inhalte zu löschen. Siehe →Deepfake

False Negative, False Rejection: wenn bei →biometrischen Verfahren eine Person abgelehnt wird, obwohl mit ihrem →Template verglichen wird

False Positive, False Acceptance: wenn bei →biometrischen Verfahren eine Person akzeptiert wird, obwohl sie nicht mit ihrem →Template verglichen wird. Über Parameter lässt sich das Verhältnis der beiden Fehler einstellen, z.B. weniger false positive und gleichzeitig dafür mehr false negative

Faraday Käfig: (engl. F. cage) elektromagnetische Abschirmung zum Schutz gegen →Angriffe gegen RFID Chips (passives Mithören oder aktive Kommunikation, ePass) oder passives Mithören von elektromagnetischen Abstrahlungen, wie z.B. alten Röhren→bildschirmen oder auch Kabeln zu Flachbildschirmen (→Tempest, →Van-Eck-Strahlung)

FarmVille: 2009-2020 online Spiel als externes Angebot in →Facebook, zu spielen im →Webbrowser. War damals der Durchbruch für längeres Verweilen in Facebook

Fast flux: →DNS-Technik, mit der →Botnetze durch sich ständig ändernde DNS-Einträge selbst organisieren können ohne dass ein zentrales Command-and-Control Zentrum einen angreifbaren Schwachpunkt bilden würde

FAT: (File Allocation Table) MS-DOS→File System, das in den frühen MS→Windows Versionen (z.B. Win 98) verwendet wurde. Anfällig für Datenverluste. Siehe →NTFS, →exFAT

FATCA: (Foreign Account Tax Compliance Act) US-Gesetz, das nicht-US Banken zwingt, die →Daten ihrer US-Kunden an die US-Steuerbehörde zu melden (sofern der Kunde zustimmt) oder aber eine pauschale 30% Steuer auf alle ihre US-Einkünfte zu zahlen. Achtung: Nicht verwechseln mit →FACTA

Fat client: heute weniger genutzte traditionelle Methode im →Client-Server-Konzept, bei der auf dem →PC des Benutzers ein spezielles Client Programm installiert wird, z.B. SAP-Client. Alternativ dazu: →Thin Client oder mehr und mehr: →Single-Page Application im →Webbrowser

Fault-injection: Testmethode, um durch das Einfügen von fehlerhaftem Input Fehler zu provozieren. Genutzt für →Angriff gegen →Webserver durch Manipulation einer →Webseite, z.B. durch →SQL-Injection oder unter Ausnutzung von →JavaScript in Eingabefeldern. Siehe →OWASP

Fax: (Telefax) 1980 – ca.2000 eine der wichtigsten Kommunikationsmethoden für geschäftliche Zwecke. Dabei wurden Papierdokumente eingescannt und mittels eines geeigneten →Protocols von Telefon zu Telefon übertragen. Löste den →Fernschreiber ab (da nicht nur für reine Texte geeignet) und wurde dann durch →Internet-Kommunikation wie →E-mail (mit Dokumenten im Anhang) abgelöst. War oft ein Sicherheitsrisiko, z.B. wenn vertrauliche Informationen im Gerät verbleiben. Siehe →Postkästen, →Druckausgaben

FC: →Fibre Channel

FCP: (→Fibre Channel Protocol)

FC-SP: →Fibre Channel - Security Protocol, ein Framework für Sicherheitsfeatures für Fibre Channel-Umgebungen. Es enhält unterschiedliche Technologien, z.B. →Authentisierung der Gerät im →SAN und →Verschlüsselung der Daten während der Übertragung im SAN. Zu den Techniken gehört z.B. →LUN-Masking oder SAN-→Zoning. Ein Projekt des Technical Committee T11 of the InterNational Committee for Information Technology Standards (INCITS), http://www.sansecurity.com/faq/fc-sp-fibre-channel-security-protocol.shtml

Feature Phone: engl. Begriff zur Abgrenzung zwischen →Smartphones und ihren Vorgängermodellen deren Kommunikationsfunktionen sich auf Telefonieren (über →2G) und →SMS beschränk(t)en. Prominente Hersteller waren z.B. Nokia und Siemens. Modelle der letzten Generation enthielten zum Teil auch (sehr begrenzte) →Kameras

Federal Spyware: US-Version des →Bundestrojaners mit dem Namen →CIPAV

Federation, Federated Identity, Federation Services: Dabei bestätigt ein →Identity Provider (IdP) gegenüber einem Resource oder Service Provider (SP) mittels Austausch gewisser Token (z.B. signierte Datenpakete) entweder die →Identität einer Person oder eines Systems, oder auch nur einer Behauptung (assertion) (→claims-based authentication). Dies beruht auf einem expliziten Trust zwischen den Service Providern und den Identity Providern, oft sogar zwischen verschiedenen Organisationen (dadurch entsteht ein →Single Sign-on). Siehe →SAML, →OpenID, →Liberty Alliance, →Passport, →CardSpace, →Higgins, →PRIME, →AD FS, →WS FS

Fediverse: (federated universe, siehe https://fediverse.network/) bezeichnet ein alternatives Netzwerk föderierter, voneinander unabhängiger →Social Networks, →Mikroblogging-Diensten (alternativ zu →Twitter) und Webseiten für Online-Publikation oder Daten-Hosting. 2016 wurde das Konzept durch due Software →Mastodon populär. Als Kommunikationsprotokoll wird bei Mastodon das seit 2018 standardisierte →ActivityPub verwendet. Andere →Protokolle sind DFRN, →Diaspora, →OStatus. Ziel des Fediverse ist, aus den sog. →Walled Gardens auszubrechen und so wie bei den Diensten →Web-Browsing und →E-Mail mit standardisierten Protokollen wie →HTTP(S) und →SMTP eine Vielfalt von →Client- und →Serverimplementierungen beliebig miteinander kombinieren zu können. D.h. wer auf einem der Dienste eines dieser Server angemeldet ist, dessen Beiträge werden auch von Menschen gesehen, die auf einem der anderen föderierten Dienste aktiv sind. Das ist so als wenn Nutzer der 'Walled Garden' Dienste wie →Twitter, →Facebook, → Instagram, →Snapchat, →Weibo, →WeChat, →Xing, →LinkedIn, →TikTok, etc. jeweils die Postings aller dieser Dienste abonieren könnten. Ein Überblick über die jeweil verwendeten Protokolle ist auf https://en.wikipedia.org/wiki/Fediverse#Fediverse_software_platforms

Voraussetzung für den Austausch zwischen den Instanzen ist jedoch, dass die Admins des "Heim-Instanz" bei dem man registriert ist der anderen Instanz "vertraut". Da es keine zentralen Regeln gibt sondern jeweils lokale Regeln gelten so gibt es auch Implementierungen mit "unerwünschten" Inhalten wie z.B. Rassenhass. Europäische Instanzen sind jedoch mit solchen Instanzen (i.d.R.) nicht verknüpft

Feedstock: Material, mit dem →3D-Drucker gefüttert werden um Objekte zu erzugen. Derzeit meist Plastik-Granulat, Kunstharz, Keramik, Metall oder auch Beton. Es wird dabei nur 1 Werkstoff oder auch mehrere gleichzeitig verwendet

Fehler: bei menschlichen Fehlern kann zwischen „mistake“ (Entscheidung für eine Aktion, die nicht zum richtigen Ergebnis führen kann), „lapse“ (die richtige Entscheidung, aber bei der Durchführung wird ein Schritt ausgelassen) oder „slip“ (die richtige Entscheidung, aber bei der Durchführung tritt eine falsche Handlung auf) unterschieden werden. Zu Fehlern in →Programmen siehe →Bug

Fehlerbaumanalyse: Methode, um in komplexen Systemen →Schwachstellen und →Ausfallwahrscheinlichkeiten zu bestimmen.

Wird auch im →Qualitätsmanagement eingesetzt

Fernschreiber: Endgerät in einem →Telex-→Netz

Fernseher: ab 2014 zumeist im →Internet online und kann dadurch zu einer Gefährdung der →Privatsphäre werden. So wird immer wieder bekannt, dass Geräte die Liste der angesehen Sendungen übertragen, bzw. im Fall von Sprachsteuerung (statt Fernbedienung) auch die gesprochenen Worte im Wohnzimmer auswerten – und oft auch übertragen muss). Dies ist ähnlich zur Problematik der →Xbox

Fernwartung: Herausforderung für die IT-Sicherheit, da von fremden →Rechnern und →Netzen auf die eigenen Systeme zugegriffen wird. Der Durchgriff über →Modem oder →VPN ist unsicher, besser sind Konzepte auf der Basis von →Terminalserver. Siehe →Housing

Festplatte: →Magnetplatte

Festplattenverschlüsselung: Verfahren, das einzelne Dateien, Folders, oder ein →Volume verschlüsselt. Letzteres wird oft als ‚full disk encryption' bezeichnet. Dies ist nicht korrekt, denn es werden nie ganze →Magnetplatten, sondern nur maximal ein →Volume verschlüsselt. Solche Verschlüsselungen sind speziell bei →Laptops notwendig, da diese leicht in falsche Hände fallen. Wichtige Aspekte sind dabei die Möglichkeit der →Key Recovery und →PBA. Ein →Angriff ist leicht, wenn der Laptop zum Zeitpunkt des illegalen →Zugriffs „unter Strom" ist, z.B. „suspended" oder nur „locked". Beispiele für Festplattenverschlüsselungen sind →Bitlocker, FileVault 2, →TrueCrypt. →TCG standardisiert eine Festplattenverschlüsselung, die bereits in der Hardware aller zukünftigen Festplatten integriert sein soll

Feuer: häufigste Quelle von →Katastrophen in →Rechnerräumen (40%), zumeist ausgelöst durch Brandquellen in der Umgebung des Rechnerraums. Siehe →Brandschutz

FHE: (Fully →Homomorphic Encryption)

Fibre Optics: (Lichtwellenleiter) Glasfaserkabeln zur →Datenübertragung, oft genutzt bei der Kopplung von 2 →Rechnerräumen zum Platten→Mirroring für →Hochverfügbarkeit und →Business Continuity. 2013 wird durch →Edward Snowden bekannt, dass der britische Geheimdienst →GCHQ, zusammen mit der →NSA, die Lichtleiter über die sowohl der Internet-→Backbone Verkehr wie auch die Verbindungen zwischen Rechenzentren (→Data Center) läuft, systematisch abhört. Siehe →Fibre Channel

Fibre Channel: (FC) Lichtwellenleiter-basierende Technologie (→Fibre Optics) die für Speicher- und Datennetze genutzt wird. Sie benutzt das Fibre Channel Protokoll (FCP). Eine der dabei genutzten Architekturen ist das →Fabric

FIDIS: (Future of Identity in the Information Society) Projekt im Rahmen des 6. EU-Forschungs-Rahmenprogramms zur Untersuchung um die europäische Forschung hinsichtlich von →Identitäts- und →Identifizierungstechnologien zu integrieren. Das Projekt beschäftigt sich mit den damit verbundenen Sicherheits- und Datenschutzaspekten. Siehe →MRTD, →ePass. http://www.fidis.net/

FIDO Alliance: (Fast IDentity Online) Alliance – Seit 2013 Industrie Consortium das sich um Interoperabilität bei Geräten für starke →Authentisierung bemüht. Eine der Techniken ist →Universal 2nd Factor (U2F) von → Google, eine andere das →Universal Authentication Framework (UAF)

File: 1) →Datei

2) (als Verb, to file) ablegen eines Dokumentes

Filesharing: (auch →Tauschbörse) heute meist verwendet im Sinne von Austausch von Musik, Videos und anderen Dokumenten. Mal abgesehen von der Frage der Legalität können durch Ausnutzen von →Schwachstellen in den Abspielprogrammen, z.B. in →MP3- oder Video-Dateien oder →Bildschirmschoner wird →Malicious Code verteilt werden. Viele der für P2P verwendeten Client-Programme installieren →Trojaner als Form der Finanzierung der Software. Weiteres →Risiko sind Fehlkonfigurationen, die dazu führen, dass eine große Zahl von Geschäftsdokumenten versehentlich auch im →Internet publiziert wird. Mehr technische Details unter →P2P. Ab 2010 dominiert auf diesem Gebiet →BitTorrent. Siehe auch →RIAA, →Freenet, →Copyright, →Privatkopie, →Urheberrecht, →eDonkey, →HADOPI, →Napster, →KaZaa

File System: (Dateisystem) logische Anordnung von →Dateien und →Verzeichnissen und den für ihr Auffinden notwendigen Index-Informationen auf einem →Datenspeicher (→Volume einer →Magnetplatte, →CD-ROM, →Flash-Speicher, →Smartcard), bzw. als virtuelles File System (z.B. →Lustre, →NFS oder →AFS) →Zugriffsmethode auf →Dateien in einer verteilten Speicherumgebung. Aber auch →Verschlüsselungssoftware wie z.B. →Truecrypt oder →Veracrypt stellen ein Filesystem dar. Beispiele für reguläre Dateisysteme: →NTFS, →FAT, →exFAT, →HFS, →HDFS, →ZFS

FileVault: Technologie in →MacOS zum →Verschlüsseln von Daten auf →Magnetplatten. FileVault verschlüsselte nur den „home folder", FileVault 2 verschlüselt →Volumes. Siehe →Festplattenverschlüsselung, http://eprint.iacr.org/2012/374.pdf

Filterblase: →Filter Bubble

Filter Bubble: siehe →Echo Chamber

FIM: (File Integrity Monitoring) Technologie um jegliche Veränderungen an →Dateien automatisch zu entdecken. Siehe →Pitbull

Finance Management for IT Services: Nach →ITIL die kostenwirksame Verwaltung der IT-Komponenten und der finanziellen Ressourcen, die für die Erbringung von IT Services eingesetzt werden

Finanzmanager: euphemistische Berufsbezeichnung für Personen, die Gelder aus →Phishing durch Bargeldüberweisung an den Betrüger transferieren. Siehe →Geldwäsche

Fingerabdruck: →Fingerprint

Fingerprint:

1) der Fingerabdruck der Menschen kann für →biometrische →Authentifizierung eingesetzt werden (→AFIS). Leider gibt es eine Reihe von Möglichkeiten zum Fälschen von Fingerabdrücken da sie nicht vertraulich sind, sondern von Menschen überall in der Umwelt hinterlassen werden. Der →Chaos Computer Club hat mehrfach die Schwächen der Technik aufgezeigt. Fingerabdrücke haben auch den Nachteil, dass sie nicht geändert werden können, wenn sie in falsche Hände fallen (im Gegensatz zum →Passwort) und sind bei älteren Menschen oft nicht mehr deutlich genug. →Apple setzt bei den neuen Modellen →Touch ID troztdem zur →Authentisierung des Besitzers und →Autorisierung von Apple Pay Zahlungen ein

2) Textstring mit einem →HashCode eines (→SSL)-→Zertifikats, dessen Vergleich über einen weiteren Kanal, z.B. Telefon die Korrektheit eines SSL-Zertifikats beweist (→out-of-band)

Fingerprinting: in der IT alle Techniken, die →Identitäten feststellen, z.B. von Geräten. So kann z.B. über die Gang-Ungenauigkeiten der internen Uhren von PCs deren Identität auch nach einer →Anonymisierung noch festgestellt werden. Farblaserdrucker kodieren ihre Seriennummer in jedes gedruckte Bild, CD- und DVD-Brenner kodieren ebenfalls ihre Seriennummer (→RID, Recorder Identification Code), digitale Kameras speichern im →EXIF-Format nicht nur Blende und Belichtung, sondern auch die Seriennummer der Kamera. Zusätzlich lassen sich Kameras auch am sog. →sensor noise, d.h. leichten Fehlern im Aufnahmechip erkennen. →Handys senden mit der →IMEI ihre Seriennummer bei jedem Gespräch, Rechnernetzwerkkarten ihre (allerdings änderbare) →MAC-Adresse. Der Begriff wird auch benutzt, um →Angriffspattern zu beschreiben, z.B. haben sich →ISPs in einer „Fingerprint Sharing Alliance“ zusammengeschlossen, um gemeinsam →Würmer und →dDoS-Angriffe schneller erkennen zu können. Siehe →RID, →Device Fingerprint

FinFisher/FinSpy: kommerzielle Software für →Cyberspionage, die von einer deutsch/britischen Firma Gamma Software vertrieben wird und für →Lawful Intercept eingesetzt werden soll (→Bundestrojaner). Diese Software wurde jedoch 2012 vor allem auf den Rechnern von Oppositionellen von diktatorischen Regimen gefunden, d.h. sie wird zum Ausspähen von Oppositoinellen verwendet. Siehe auch →BackTrack, →Vupen, →NSO, →Hacking Team, →Black hat

Fintech: Schlagwort für Firmen (meist Startups) die im Finanzbereich mit neuen Technologien die Dominanz der herkömmlichen Banken angreifen, z.B. indem neue Zahlungsmethoden angeboten werden. Dabei werden typischerweise →Smartphones als Benutzerinterface eingesetzt. →Blockchain ist eine Technologie die dabei in einigen Bereichen angedacht wird (als in Form von →Smart Contracts). Banken versuchen mit diesem Trend umzugehen, indem sie mit solchen Firmen kooperieren

FinTS: (Financial Transaction Services) deutscher Standard für →e-Banking, Nachfolger von →HBCI. Unterstützt →Smartcards für gegenseitige →Authentisierung

FIPS-140: Federal Information Processing Standard (US-Norm) 140. “Security Requirements for Cryptographic Modules”. Normungsvorgaben für →Verschlüsselungsgeräte und –software

FireBug: →Plug-in zu Firefox zum Testen von →Webseiten und →Web-Applications, auch unter Sicherheitsgesichtspunkten

Firewall: (die, engl. Brandschutzmauer) Sicherheitssoftware oder –gerät (→Appliance) zum Schutz des eigenen Netzwerkes oder Rechners. Sie kontrolliert durch Filterung (→Paketfilter) sämtlicher eingehenden Daten, um das Netzwerk vor unerlaubten Zugriffen zu schützen. Die Filterung basiert auf der Selektion von →Port Nummern. In Verbindung vom Stateful Inspection können auch kompliziertere Protokolle, wie z.B. →FTP implementiert werden. In Verbindung mit zusätzlichem →Content Filtering kann sie auch für Virenschutz verwendet werden. Für PCs außerhalb von Firmennetzen sollten →Personal Firewalls eingesetzt werden. Siehe →Web Application Firewall. Siehe →Mental Model, →NGFW, →WAF

Firewire: (IEEE 1394) 1986 von Apple entwickelte Datenschnittstelle für →PCs. Sicherheitsrelevant, da über sie, ebenso wie über →USB, Firmendaten leicht das Unternehmen verlassen können, bzw. →Schadsoftware eingeschleust werden kann. Im Gegensatz zu USB 2 kann Firewire aber direkt in den Hauptspeicher eines →Rechners schreiben, d.h. bei einem unbeaufsichtigten gesperrten Rechner lässt sich z.B. die →Authentisierung ausschalten. →PCs ohne Firewire-Schnittstelle lassen

sich über →PCMCIA-Karten mit Firewire (o.ä.) angreifen

Firmware: Software die in Chips eingebettet ist, z.B. →Embedded Systems, aber auch im →BIOS, →UEFI oder →EFI, in der Regel wegen der Beschränkung auf winzige Speichergrößen in →Assembler programmiert. Fehler beim Update von Firmware können zu einem →Brick führen, kann als →Angriff im →Cyberwar genutzt werden. 2015 wird bekannt, dass die →NSA die Firmware von →Magnetplatten modfizieren und für ihre Zwecke verwenden kann. https://sicherheitskultur.at/notizen_1_15.htm#firm

FIPS-140: US-Standard für die Zertifizierung von kryptographischen Komponenten (Hardware und Software). Setzt voraus, dass das →Betriebssystem nach →TCSEC zertifiziert ist. Wird für die Bewertung von →HSM und →Smartcards verwendet

FIRST: (Forum of Incident Response and Security Teams) Organisation, die das →CVSS entwickelt hat

FISA: (Foreign Intelligence Surveyance Act, 1978) gesetzliche Grundlage in den USA für das Abhören von Telefonaten durch die Geheimdienste. Erforderte (usprünglich) einen Gerichtsbeschluss im Einzelfall und wurde daher 2008 erweitert, um nach einem Beschluss in einem geheimen FISC-Court auch →Daten in größerem Umfang sammeln und auswerten zu können. 2013 wird aufgedeckt, dass es eine Kooperation der →NSA mit →Microsoft, →Google, →Facebook, →Apple, →Youtube, →Skype, Paltalk, AOL und Yahoo gibt, die einen direkten →Zugriff ohne Gerichtsbeschluss ermöglicht. Siehe auch →NIMD, →PRISM

FISMA: (Federal Information Security Management Act of 2002) US-Gesetz zur Verbesserung der →Informationssicherheit bei Bundesbehörden

FIX: (Financial Information eXchange) Protokoll für den Austausch von Finanzdaten (vor allem im Wertpapierhandel) in automatisierter Form. Es wurde als moderne Alternative zur kostenpflichtigen Alternative →SWIFT entwickelt, das erhebliche Vertraulichkeitsprobleme hat. FIX beruht auf →TCP/IP und analog zum →Internet beruht es auf einer Peer-to-Peer (→P2P) Architektur ohne zentrale Server

Flame: (Flame/SkyWiper) Begriff für ein →Cyberspionage-Programm das vor allem in Nahen Osten eingesetzt wurde und das sehr gezielt Daten gestohlen hat, aber auch Gespräche abgehört und Bildschirminhalte übertragen. Es wurde jahrelang von den gängigen →Antiviren-Programmen nicht erkannt. Flame wird oft (fälschlicherweise) als Beispiel für →Cyberwar angeführt. Das Programm hat vergleichbare Fähigkeiten mit staatlicher Überwachungssoftware wie dem →Bundestrojaner. Siehe →APT

Flash: 1) proprietäre Entwicklungsumgebung (von Macromedia, heute Adobe) zur Erzeugung von Flash-„Filmen“ im SWF-Format zur Darstellung im →Webbrowser. Probleme sind →Schwachstellen in älteren Versionen und die vielfältigen Möglichkeiten von Flash auf →Dateien, Microfon und Videokamera zuzugreifen, d.h. gut geeignet für →Schadsoftware. Wird auch für →Device Fingerprinting verwendet. Flash→Browser-Plugin sind nicht-kompatibel mit →ASLR. Wird Ende 2020 eingestellt. Siehe →Silverlight, →SVG, →Quicktime, →AIR, →Flex, →FarmVille

2) **Flash-Speicher:** (Flash-EEPROM) werden zur Speicherung von digitalen Informationen auf kleinstem Raum, z.B. DiskOnChip, USB-Sticks, Speicherkarten für Digitalkameras, Mobiltelefone, Handhelds, MP3-Player, → SSD-„Platten“ in teueren →Laptops verwendet. Alle beweglichen Flash-Speicher können eine →Bedrohung der →Informationssicherheit darstellen, wenn auf diese Weise Informationen aus einem Unternehmen entfernt werden oder →Schadsoftware eingeschleppt wird, siehe →Stuxnet, →SSD

Flash-Speichermedien verfügen alle über **Wear Leveling**. Dies ist eine Schutzmechanismus gegen die Tatsache, dass das Schreiben von →Daten ein Vorgang ist, der im Gegensatz zu →Magnetplatten nicht beliebig oft ausgeführt werden kann ohne diese Speicherstelle zu zerstören. Daher wird beim Überschreiben einer Speicherstelle der neue Inhalt an eine andere Stelle geschrieben und der alte Inhalt als „leer“ markiert. Falls im Rahmen einer →Forensic-Untersuchung auf einem Flash-Speicher Beweise vermutet werden die gelöscht wurden so werden spezielle →Programme genutzt, die diese durch →Zugriff auf die „leeren“ Speicherbereiche wieder herstellen. Um bei einer Entsorgung eines Geräts mit Flash-Speicher, z.B. →Smartphone, keine vertraulichen Daten weiter zu geben müssen spezielle →Wipe-Programme eingesetzt werden, die trotz Wear Leveling Daten sicher löschen können. Siehe auch →exFAT

Flash Cookie: Technologie um bei →Internet-Nutzern →Daten auf ihrem →PC zu speichern und später abzurufen. Es dient dem →Profiling der Nutzer, zumeist zu Werbezwecken. Technisch handelt es sich um Local Shared Objects (→LSO), die vom Adobe →Flash Player erstellt werden. Sie können über die →Browser-Einstellungen nicht kontrolliert werden. Flash ist seit 2020 nicht mehr unterstützt. Siehe →Cookie

Flex: Entwicklungs- und Server-Plattform für →Flash-Anwendungen. Wird sicherheitstechnisch gut bewertet (wenn die Anwendungen unter Ausnutzung der Sicherheitsfeatures implementiert werden)

Flickercode: optische Kommunikation durch

Darstellung eines flickernden Bildes auf einem →Bildschirm zur Übertragung von Überweisungsdaten von der Bank zu einem nicht verbundenen Gerät, wird genutzt für die →Autorisierung von Überweisungen im →**e-Banking**

Floating Point: (Gleitkommazahl) →Zahlendarstellung

Flooding: in der IT →E-Mail-Flood, SMS-Flood, →Phone Flood, →Synflood, →HttpFlood

Flow: →NetFlow

Flowspec: →NetFlow

FMEA: (failure mode effect analysis) analytische Methode der Zuverlässigkeitstechnik, um im Rahmen des →Qualitätsmanagements bzw. Sicherheitsmanagements potenzielle →Schwachstellen zu finden. Siehe →TQM

FOAF: (friend of a friend) Teil des →semantischen Webs, Datendefinition um Verknüpfungen in →social networks formal darzustellen. Sicherheitsrelevant, da auf diese Weise eine automatische Auswertung dieser Verknüpfungen möglich ist und dies möglicherweise die →Privatsphäre berührt. Siehe →NIMD, →Socialbot

Folksonomy: Begriff für die Klassifizierung von Inhalten (→Websites, Bilder, etc.) durch viele Benutzer (z.B. die →tags auf Flickr.com). Alternative zu Konzepten wie →Semantic Web

FoMo: (fear of missing out, die Angst, etwas zu versäumen) in der Soziologie die Angst die heute vor allem durch →Social Networks erzeugt wird: Falls wir nicht jederzeit online sind, so könnten wir etwas versäumen. Die ständigen Vergleiche mit den Erfolgen anderer führt zur fixen Idee, dass andere mehr Spaß und mehr Erfolg haben als wir selbst. FoMo wird als Grund dafür genannt, dass es den meisten Menschen extrem schwer fällt, eine längere Zeit auf →E-Mail, →SMS, →Messaging und/oder Social Networks zu verzichten, siehe →Suchtcharakter, →Stickyness

Forced Browsing: →Angriffstechnik gegen →Websites, z.B. durch Erraten einer nicht verlinkten →URL, nutzt sog. →Business Logic Flaws aus

Forefront: kommerzielle Sicherheissoftware von →Microsoft fü Unternehmen, analog zu →OneCare

Forensics: Techniken, die nach einem Verbrechen oder Sicherheitsvorfall (Security Incident) zur Beweisgewinnung und -sicherung eingesetzt werden. In der IT entweder nach Angriffen auf die IT selbst (→Virenbefall, Installation eines →root kits) oder bei anderen Vergehen (z.B. unberechtigter →Zugriff), um Beweise auf IT-Geräten zu sichern (→E-Mail, Fotos). Dabei werden oft Tools wie enCase oder →osTriage eingesezt, die Abbilder von → Hauptspeicher und Datenträgern (z.B. →Magnetplatten) in gerichtsverwertbarer, d.h. beweissicherer Form machen. Wenn es darum geht, bereits gelöschte →Dateien zu sichern so werden zusätzlich oft →Data Recovery Services eingesetzt. Siehe →RFS, →MAC-Times, →CSI, →DANN

Fork: (engl. Gabelung) bei →Open Source Projekten wenn jemand einen bestimmten Stand des Quellcodes nimmt und diesen getrennt von dem Rest der Community weiterentwickelt. Forks führen zu einer Zerklüftung von Open Source Programmen, die ein einheitliches →Patch Management schwierig machen kann, z.B. bei →Android, vom dem es 2014 19000 Varianten im Einsatz gab

Form-grabbing: →Trojaner, die nach einer →Infektion eines →Rechners die Inhalte aller Web Formulare, z.B. →Benutzernamen, →Passworte und →PINs an den Angreifer versenden. Verwendet für →Phishing, →Keylogger

Forward Recovery: Wiederherstellung einer → Datenbank auf der Basis einer älteren Kopie und der nachfolgenden →Journals

FPGA: (Field Programmable Gate Array) Chips die z.B. für Image Processing in Plasma Fernsehbildschirmen eingesetzt werden, lassen sich auch als sehr schnelle →Passwort Cracker verwenden. Diese Chips werden aber auch in vielen anderen Systemen eingesetzt (industrial control, Sicherheitsfunktionen und militärische Lösungen) und haben eine JTAG-Schnittstelle (Joint Test Action Group) die für Debugging genutzt wird, aber auch Angriffsflächen bietet. Da diese in Hardware implementiert sind lässt sich dies im Feld kaum reparieren

Fractal: →Messaging →Software die das →Matrix →Protokoll nutzt und mit allen anderen Instanzen kommunizieren kann die auch dieses Protokoll unterstützen (föderierte Umgebung)

Fragmentierung: 1) auf einer →Magnetplatten wenn die →Daten einer →Datei nicht zusammenhängend gespeichert sind, hat nur Performance-Nachteile

2) bei →IP-Paketen wenn ein Datenpaket von einer Zwischenstelle im Netz in mehrere Pakete zerteilt wird. Die Notwendigkeit der Zusammenführung an der Endstelle kann zu →DoS-Angriffen genutzt werden und dies bietet auch Möglichkeiten, an einem →NIPS vorbei zu kommen

Frame Relay: →Datenübertragungsmethode, bei der verschiedene Sitzungen über einen gemeinsamen Übertragungskanal gesendet werden. Die Geschwindigkeit liegt dabei unter der für →ATM. Es kann eine minimale →Datenübertragungsrate garantiert werden.

→QoS

Fraud Alert: in den USA selbst-erzeugter Eintrag in →Kreditschutzdatenbanken dass möglicherweise →Identity Theft vorliegt. Siehe →credit freeze

Fraud-Detection: Konzept der →Kreditkarten-Organisationen zum Entdecken um Betrug während einer Kreditkarten-Transaktion. Wichtiger Spezialfall ist →CNP (Card not Present) Fraud, d.h. die Zahlung im Internet oder am Telefon. Zum Schutz wird →CVV oder Systeme wie →3-D Secure verwendet http://sicherheitskultur.at/haftung.htm#ccbetrug

Freedom of Information Act: US-Gesetz um den Bürgern besser zu erlauben, den Staat zu kontrollieren. Es bestimmt, dass alle Behördenakte öffentlich zugänglich sein müssen, wird heute von →Daten-Aggregatoren für Datensammlungen über Personen genutzt

Freemailer: kostenloser E-Mail-Service, meist über Webinterface (→Webmail). Finanziert über Bannerwerbung, populäre Beispiele sind hotmail.com, yahoo.com, web.de, gmx. Freemailer werden gern für →Spam verwendet, daher wird dort heute oft ein →Turing Test bei der Anmeldung durchgeführt (→Captcha)

Freenet: ein Projekt für eine Kommunikationsplatform die gegen zensurmaßnahmen gehärtet ist, entwickelt seit 2000. Dabei werden alle Inhalte dezentral gespeichert, es gibt daher keine Möglichkeit, das System zentral zu zerstören

Freeware: Software, die ohne Kosten im →Internet verfügbar ist. Leider wird diese Software oft über die bei der Installation ebenfalls installierten →Trojaner finanziert. Es gibt jedoch auch kommerzielle Programme, wie z.B. →PGP, →Ad-Aware, →Zonealarm, die für den Privatgebrauch kostenlos zur Verfügung gestellt werden, um für die kommerzielle Version zu werben

Frictionless sharing: Schlagwort von →Facebook das das Ziel beschreibt, dass Aktivitäten und Daten vollautomatisch mit den Kontakten in →Social Networks geteilt werden. Dies geschieht z.B. wenn die Kamera (oder das →Smartphone) alle Fotos automatisch im →Internet abspeichert und frei gibt. So eine Welt in der →Lifelogging mit frictionless sharing kombiniert ist wird im Buch „The Circle“ perfekt beschrieben

Friend: unglücklicher Begriffe für Kontakte in einigen →Social Networks, sehr oft auch genutzt für Personen ohne Kontakt im „realen“ Leben. An diesen Status sind zumeist erweiterte →Zugriffsrechte auf private Informationen verbunden, bzw. diese Friends werden automatisiert über Änderungen in Profilen informiert. Auf Grund der Zugriffsrechte ist der Friend-Status auch für →Angriffe wie das Verteilen von →Malware interessant (z.B. durch →Socialbots). Auch als Verb genutzt: „to friends s.b“ oder „to de-friend s.b“. Letzteres ist für beide Beteiligten mit sozialem Stress verbunden. Die Kontakte von Firmenseiten werden als „Fans“ bezeichnet. Im Rahmen von →Astroturfing werden 10000 „Friends“ oder Fans für 35000 Euro angeboten. Siehe auch →FOAF, →Social Graph, →FoMo, →Dunbar Number

Friendica: föderiertes →Social Network, Teil des →Fediverse. Da Friendica eine sehr große Zahl von →Protokollen unterstützt können deren Nutzer sehr weitreichend kommunizieren, es gibt sogar ein Interface zu →Twitter, WordPress, Tumblr und →RSS

Friend-request: Anfrage in →Social Networks, die →Profile zu verlinken. Untersuchungen zeigen, dass →friend requests von Unbekannten sehr leicht angenommen werden wenn deren Profil eine ausreichende Attraktivität hat (bis zu 20% Akzeptanz). Dies wird oft für →Social Engineering, zum Ausspähen von Informationen (→Data Mining) und zur Verteilung von →Schadsoftware genutzt (→Socialbot)

FriendFinder: Beispiel eines →Geolocation Dienstes, bei dem Mitglieder einer Gruppe sich gegenseitig lokalisieren können

FTC: (Federal Trade Commission) US-Behörde, die über den Hebel des fairen Wettbewerbs und des Konsumentenschutzes auch in Problemstellungen der →Informationssicherheit aktiv wird, z.B. im Bereich →Spam und bei der Einhaltung von →Privacy Statements.

FTP: (File Transfer Protocol) auf dem →TCP/IP-Protokoll basierendes Verfahren zum Austausch von Dateien in beide Richtungen. Auf Grund der Möglichkeit des anonymen Zugriffs und Fehlern in der Konfiguration ein manchmal nicht sehr sicheres Verfahren. Auf Grund einer komplizierten

Games: (Spiele) Computerspiele, ob am →PC oder →Smartphone, sind auf Grund ihrer Popularität auch ein →Angriffspunkt für Angreifer. Dies geschieht z.B. entweder über das Angebot von →Raubkopien, oder auch über sog. →Cheats. Spiele, die über das →Internet gespielt werden (→MMORPG) bieten viele Angriffspunkte durch Übernahme des → Accounts des Spielers. Dies kann zu einem Diebstahl von virtuellem Geld / Gold, Ausstattungen wie Waffen und des gesamten →Avatars führen. 2020 werden Spiele auch als →Single-Page Application im Rahmen von →Streaming (Cloud-Gaming, z.B. Dienste wie →Google Stadia, →Microsoft xCloud, → Amazon Luna, Onlive oder Gaikai) angeboten und sind dann z.B. auch auf →Chromebooks verfügbar, können aber natürlich nicht die Leistung von →Graphikkarten von High-End Gaming-→PCs bieten, die mittels →GPU Graphikleistungen bieten, wie sie in den 80iger Jahren noch speziellen Graphikcomputern wie

z.B. von SGI vorbehalten waren. 2020 können innerhalb von Spielen auch reale Veranstaltungen, z.B. Konzerte, realisiert werden. Siehe auch →virtual currency, →LARP, →RPG, →ARG,

Gamification: Schlagwort das beschreibt, dass Nutzer zu einer längeren oder intensiveren Nutzung eines Dienstes gebracht werden sollen, indem die Nutzung als Spiel, d.h. als Wettbewerb, implementiert wird, z.B. durch High-Score für denjenigen, der die meisten Beiträge in einem Forum postet und zu höheren Statuswerten oder →"Reputation Points" führt

GAN: (→Generic Access Network)

Gatekeeper:

1)Funktion von →Mac OS X, das →Schadsoftware erkennt und die Ausführung verhindert. Hat gegenüber den →Malwareschutzprogrammen auf →Windows sehr begrenzte Funktionalitäten

2) große →Internet-→Plattformen, siehe →Digital Market Act

Gateway: generischer Begriff für ein Gerät, das z.B. →Daten empfängt und weiterleitet. Dabei wird der Datenstrom oft in irgendeiner Form verändert (→Proxy für die Umsetzung von →IP-Adressen, →Media Gateway). Gateways können auch →Zugriff auf dahinterliegende Dienste bieten ohne dass eine direkte Datenweiterleitung stattfindet, z.B. →Citrix, →Cloud Access Security Broker

GCHQ: (Government Communications Headquarters) Teil des britischen Geheimdiensts, der mit technologischer Hilfe durch die →NSA, viele der Internet-→Backbone Verbindungen auf →Lichtleiter-Basis abhört. Bekannt wurde dies 2013 durch →Edward Snowden

GDA: (Gesundheitsdiensteanbieter) in Ö: lt. Gesundheitstelematikgesetz Teilnehmer am elektronischen Datenaustausch, z.B. Ärzte, Kliniken, Krankenkassen, etc. Nach der Umsetzung von →ELGA müssen diese ihre Krankenakten den anderen GDAs zugänglich machen, verwaltet über eine →Registry und können selbst auf andere zugreifen

GDPR: General Data Protection Regulation. Seit Mai 2918 in Kraft. Siehe →Datenschutzgrundverordnung

GDPS: (Geographically Dispersed Parallel Sysplex) Konzept und Technologien von IBM für →Disaster Recovery im Mainframe-Bereich. Beinhaltet das Konzept, dass die aktiven Produktionssysteme am entfernten Standort stehen sollen (schnellere Wiederherstellung)

Gefällt mir: →Like-Button

Gegner: →Adversary

GeldKarte: deutsche Implementierung des →e-Geld mit einer bargeldlosen Bezahlung kleiner Beträge ohne Eingabe einer →PIN. Sie ist auch ohne Bindung an ein Konto möglich. Nach der Bezahlung findet ein Abgleich bei einer Verrechnungsstelle statt, daher ist trotz „→Anonymität" eine Wiederherstellung bei zerstörten Chip (→Smartcard) auf der Karte möglich. Siehe →EMV

Geldwäsche: Einschleusen illegaler Erlöse aus Straftaten (zum Beispiel aus Drogenhandel, →Erpressung, →Phishing) in den legalen Finanz- und Wirtschaftskreislauf. Eingesetzt u.a. nach Erpressung mit →dDoS oder →Phishing. Bei Verdacht auf Geldwäsche muss die Polizei die „Vortat" beweisen, was oft schwierig ist. Siehe →„Finanzmanager", →Western Union, →e-Geld, →KYC

Generic Access Network: (GAN) →Unlicensed Mobile Access

Genetic Algorithm: Verfahren beim dem Mittels der Simulation von Mutationen versucht wird, sich einem gewünschten Endzustand anzunähern. Wurde beim →Angriff auf →Iriserkennung genutzt. Voraussetzung dafür ist, dass es eine Bewertungsfunktion gibt, die die ‚Nähe' zum gewünschten Ergebnis bewerten kann

Geneva: Open-Identity-Plattform von Microsoft. Siehe →Cardspace

Geoblocking: Sperren von Diensten in bestimmten geographischen Gebieten. Z.B. ab 2015 das Sperren von →Bankomatkarten für nicht-europäische Länder in denen noch die Magnetstreifen statt der →Chipkarten genutzt werden. Der Kunde mus vor einem Urlaub die anderen Regionen gezielt freischalten. Dies soll →Skimming für die Betrüger uninteressant machen. Wird von →Streaming Diensten wie →Netflix eingesetzt wenn sie die Urheberrechte für ein bestimmtes Gebiet nicht haben. In diesen Fällen wird der Ort des Nutzers über die →IP-Adresse ermittelt. →VPN-Dienste werden dann oft eingesetzt, wenn diese Blockierung umgangen werden soll. Geoblocking wird auch im Glücksspielbereich eingesetzt wenn die notwendigen Lizensen fehlen

Geofencing: Erweiterung von →Geolocation. Für eine in Bezug auf den Aufenthaltsort überwachte Person, z.B. Kind oder Partner mit →Handy oder zu Hausarrest verurteilter Verbrecher wird ein Bereich definiert, bei dessen Überschreitung ein →Alarm ausgelöst wird. In der Regeln implementiert über eine Fußfessel oder eine →App auf einem →Smartphone. Erfordert juristisch die Zustimmung der Person, wird aber oft heimlich zu →Stalking Zwecken gemacht

Geolocation: Festellung des geographischen Aufenthaltsorts einer Person (entweder durch die Person selbst oder durch Fremde), z.B. mittels Ortung eines →Handys (silent →SMS oder →SS7-Kommandos), über →GPS in Kameras, →Smartphones, Autos (Diebstahlschutz, →Fleet Managment), →ANPR, →Sec-

tion Control oder →Navigationsgeräten. Oder über die →IP-Adresse bei einem →Rechner im →Internet. So kann →Überwachung stattfinden, aber auch Dienste wie →FriendFinder, lokal fokusierte Werbung, etc. angeboten werden.

Tödlich wirkt Geolocation wenn es eingesetzt wird, um Ziele für die US-→Drohnen (→UAV, unmanned areal vehicle) zu identifizieren. Dabei wird getötet, wer in der Nähe des Handys ist (bzw. der jeweiligen SIM-Karte die eine bestimmte Telefonnummer [→IMSI] repräsentiert), auch wenn das Gerät weiterverborgt wurde. Einige UAVs können auch „virtual →base station" enthalten. Dort meldet sich das Handy der Zielperson an und kann entweder über die SIM oder die →IMEI erkannt werden (→GILGAMESH). Im Programm → VICTORYDANCE werden auch WLAN-Verbindungen vom UAV identifiziert.

Siehe auch →Standortdaten, →Skype

Geschäftsprozess: Grundlage jeder Planung zu Informationssicherheit ist die Unterstützung und Absicherung von Geschäftsprozessen. Speziell bei →Business Continuity Planungen steht dies im Mittelpunk

Gesichtserkennung: →Face Recognition

Gesundheitsapp: →Smartphone →Apps die mittels →Sensoren und/oder Eingaben der Nutzer →Daten über Gesundheitsparameter der Nutzer sammeln und in aller Regel zentral in der →Cloud des Anbieters speichern. Auch diese App-Anbieter leben fast immer von Werbung, d.h. sie vermarkten die zum Teil recht sensiblen Daten großzügig (z.B. Menstruations-App die auch Details der sexuellen Aktivitäten tracken). So wurde nachgewiesen dass viele der Apps die Daten an die großen Werbenetze wie z.B. →Facebook weitergeben. Dies geschieht oft indirekt durch die Einbundung von →SDKs die Facebook zur Verfügung stellt. Die Nutzer stimmen durch Akzeptieren der (ungelesenen) AGBs zu. Trotzdem kann sich in einigen Fällen nicht nur eine Verletzung von Ethikregeln, sondern auch dem →Datenschutzgesetz vorliegen

Ghost: (oder Ghost Image) Erstellung einer speziellen Kopie des Inhalts einer Magnetplatte, die eine leichte Wiederherstellung im Rahmen von →Disaster Recovery ermöglicht

Ghostery: →Blocking Tool zur Verhinderung von →Tracking durch →Advertising Networks. Zeigt dem Benutzer an, wer ihn tracken will und erlaubt gezieltes Blockieren der Tracking Elemente

GIF: Datenformat für Bilder im →Internet, wichtige andere sind →JPEG und →PNG. In GIF-Dateien selbst kann →Malicious Code versteckt sein (z.B. in der Form von →PHP-Scripts), zusätzlich wird solcher manchmal im →E-Mail als GIF getarnt. Mit Hilfe von →Steganographie können auch Nachrichten in diesen Bildern versteckt werden. Im GIF-Format lassen sich auch Strichzeichnungen mit weißem Hintergrund sauber darstellen (im Gegensatz zu JPEG, das eher für Fotos geeignet ist)

GILGAMESH: Project, bei dem →UAVs mit „virtual →base stations" ausgerüstet werden damit die →Handys der Zielpersonen sich dort automatisch anmelden, was eine hohe Präzision bei der →Geolocation erlaubt

GINA: (Graphical Identification and Authentication) Login-Fenster für alle Windows Systeme. Alternative →Authentifizierungsmethoden und →SSO-Software muss sich damit "einigen" (z.B. in Form einer GINA-Chain)

GitHub: von →Microsoft übernommenes Unternehmen das ein →Cloud-System für →Quellcode-Verwaltung betreibt. Ab 2019 ist es das wohl meistgenutzte System, durch die Cloud-Implementierung sehr gut für die Kooperation zwischen verteilt arbeitenden Entwicklern geeignet. Enthält auch Funktionalitäten für die Kommunikation zwischen Entwicklern (z.B. Feature Requests, Bitte um Hilfestellung). Dabei kommt es leider durch Nachlässigkeit auch immer wieder dazu, dass Entwickler sensible Teile des →Programmcodes (z.B. →Schlüssel u.ä.) in der Anfrage veröffentlichen und damit Sicherheitsrisiken darstellen

Glass: →Google Glass

GLBA: →Gramm-Leach-Bliley Act

Gleitkomma: (floating point) →Zahlendarstellung

Global Adversary: Spezialfall des →Adversary. Ein Gegner, der global agieren kann. Paradebeispiel ist die →NSA. Ein Schutz gegen einen solchen Gegner ist sehr schwierig. So ist z.B. das Konzept des →TOR Anonymisierungsnetzwerks nicht dafür ausgelegt vor einem global adversary zu schützen, der den Datenverkehr beim Eintritt und dem Austritt aus dem Netzwerk kontrollieren kann und dadurch zeitliche Korrelationen herstellen. TOR ist konzipiert zum Schutz gegen eine Organisation, die nur im eigenen Land die Netze unter Kontrolle hat

Globus Toolkit: von der Global Alliance Organisation standardisierte Software für →Grid Computing. Dabei wird nicht nur der Datenaustausch abgehandelt, sondern über die Grid Security Infrastructure (GSI) auch Sicherheitsaspekte wie →Authentisierung

Gmail: kostenloser →Webmail-Dienst von →Google der über Werbung finanziert wird. Zum Aufbau eines →Benutzerprofils wertet Google dafür die Inhalte der →E-Mails aus

GN: (Group Ad-Hoc Network) Netz aus →Bluetooth-Geräten. Siehe →PAN

GNU project: 1983 von Richard Stallman vom

MIT ins Leben gerufen Bewegung zum Erstellen von (hauptsächlich) →public-domain Software die dann unter der GNU →GPL Lizenz genutzt werden kann

GNU Radio: public-domain Software zur Simulation von Systemen die (hoch)frequente Wellen nutzen und traditionell analoge Systeme durch digitale Signalverarbeitung ersetzen. Als Hardware wird dabei →Software-defined Radio eingesetzt. Wird oft für die Demonstration von Angriffen und Protokollverwundbarkeiten verwendet, z.B. →RFID, elektronische Pässe, drathlose Türöffner, etc. Wird im Zusammenhang mit →USRP genutzt

GoB: →Grundsätze ordnungsmäßiger Buchführung

Going Dark: →Lawful Intercept

Google: Gegründet 1998. Seit 2015 umbenannt in →Alphabet mit Google als einer der Tochterfirmen. Seit 2003 die →Internet-Suchmaschine mit einem überaus dominierenden Marktanteil. Bietet unter dem Konzernnamen →Alphabet sehr viele zumeist für die Nutzer kostenlose Dienste an, z.B. →Gmail, →Android, →Google Glass, →Google Play, Google Maps, Google Translate, Google Docs, Google Cloud, →Sidewalk Labs. Google finanziert sich primär durch Werbung, die sie auf Grund der extremen Kenntnisse die sie über alle Nutzer im Internet (plus alle →Android-Nutzer, zusätzliche Daten gewinnen sie auch →Sidewalk Labs) gewinnen können sehr präzise platzieren können, siehe →targeted advertising (→behavioural advertising). Siehe auch →Adwords. Mittels →AI können rechts detaillierte Persönlichkeitsanalysen durchgeführt werden. Google gilt als Erfinder des →Überwachungskapitalismus. Durch den extremen Marktanteil in vielen Bereichen entsteht quasi ein Monopol. Wer als Betreiber einer →Website nicht auf der 1. Seite der Suchergebnisse gelistet wird, hat mit seinem Unternehmen sehr oft existentielle Probleme. Dabei kann Google durch geschicktes Verschieben der Werbegewinne in Steueroasen wie Luxemburg, Niederlande oder Irland ein Bezahlen von Steuern weitgehend vermeiden.

http://sicherheitskultur.at/notizen_1_06.htm#google

Google+: Social Network (2011 bis 2019) das über die Funktion →circles eine leichtere Strukturierung der →Friends von →Benutzern ermöglichen wollte, damit der →context collapse der Vermischung unterschiedlicher Zielgruppen vermindert wird. →Facebook versuchte, mit ähnlichen Funktionalitäten nachzuziehen. Google Plus war auch ohne die große Zahl der aktiven Nutzer wie bei Facebook ein Vorteil für →Google da dort (mit Zustimmung der G+ →Account Nutzer) alle anderen Google →Daten zusammenflossen: die Suchanfragen, →Google Maps Anfragen, →Youtube-Aktivitäten, die Kontakte in →Gmail, und vor allem die Informationen über →Website-Besuche über das Google Ads-Network und vermutlich auch die →Android Aktivitäten

Google Analytics: sehr häufig eingesetzter kostenloser Service für →Website-Betreiber um detaillierte Benutzer-Statistiken zu erhalten. Dafür werden jedoch die Nutzungsdaten der Besucher an die →Google-Server gesendet und dort verarbeitet. Google verlangt, dass dies in den →Datenschutzerklärungen der Websites verkündet wird, dies ist jedoch zumeist nicht der Fall. Seit 2010 bietet Google eine Version, bei der die →IP-Adressen bereits auf der Website →anonymisiert werden können. Dies muss der Web-Programmierer aber bewusst aktivieren. Besser sind andere kostenlose Tools, die direkt auf der Website selbst ablaufen, bzw. Anbieter innerhalb der EU

Google Authenticator: →Authentisierungslösung die →HOTP und →TOTP unterstützt. Die entsprechende →App generiert ein →One-time password das von der →Software oder der →Website geprüft und bei Erfolg akzeptiert wird

Google Cloud Messaging: (GCM) Dienst für →Android →Smartphones damit ein →Server Nachrichten an eine →App schicken kann ohne dass diese im Foreground läuft (und die Batterie belastet). Entspricht →Apple Push Notification

Google Docs: Textverarbeitung in der →G Suite

Google Glass: problematisches Projekt bei der in eine Brille eine Kamera, Mikrofon und Display eingebaut wird. Dem Träger können auf diese Weise vor seinen Augen Informationen eingeblendet werden, z.B. könnten über →Face recognition die →Facebook Profile der Menschen um ihn herum eingeblendet werden (dies wird derzeit (noch) nicht implementiert). Der Überbegriff für das Einblenden von zusätzlichen Informationen in das Blickfeld von Menschen nennt man →Augmented Reality (AR). 2013 wird innerhalb und außerhalb von →Google bereits an Versionen auf der Basis von Kontaktlinsen gearbeitet, andere Geräte auf Basis einer Brille sind auch verfügbar.

Die eingebaute Kamera kann alles aufnehmen was um den Glass-Nutzer herum passiert und speichern. Dadurch werden Aufzeichnungen von Personen gemacht, die sich dagegen nicht wehren können. Dies führt dazu, dass Menschen ständig damit rechnen müssen, dass ihr Verhalten aufgezeichnet wird

Da diese →Daten auch in der →Cloud abgespeichert werden können sie dort auch mittels →speech zu text auswertbar gemacht werden. Siehe auch →Lifebits

Google Maps: Kartendienst von →Google. Siehe →Google Streetview

Google Meet: Videokommunikationsdienst, der 2020 als →Videokonferenzsystem angeboten wird. Vor allem interessant für Firmen, bei denen →G Suite im Einsatz ist

Google Now: Service auf →Android der Benutzern auf Grund von gesammelten →Daten persönliche Ratschläge für ihr Verhalten gibt (→personal assistant, →virtual assistant), Fragen beantwortet und einfache Aufgaben erledigt. Wird meist über Sprachsteuerung genutzt. Zur Problematik siehe →Contextual Computing

Google Pay: →NFC Zahlungsdienst auf →Android Geräten auf der Basis der →HCE Architektur (früher Google Wallet oder Android Pay). Erlaubt das Bezahlen mittels →Smartphone an →Bankomatkassen. Dabei wird die →2 Faktor Authentisierung mittels ‚Besitz des Smartphones" plus einem weiteren Faktor zum Entsperren des Geräts abgebildet (→PIN oder →Fingerprint). Benutzer können die selbe →Kreditkarte nutzen, die auch für →Google Play hinterlegt ist. Ähnlich wie bei →Apple Pay wird aber nicht die hinterlegte Kartennummer an den Händler übertragen sondern eine generierte virtuelle Nummer. D.h. der Händler erfährt nicht die Bankverbindung des Kunden. Im Gegensatz zu →Apple erlaubt Google auch anderen →App Entwicklern den →Zugriff auf die NFC Schnittstelle des Smartphones. Daher gibt es auch alternative Zahlungsapps wie z.B. Samsung Pay oder LG Pay die aber in Deutschland keine Rolle spielen. →WeChat Pay und →Alipay nutzen nicht NFC sondern →QR Codes

Google Play: →App Store für →Android-→Smartphones. Dort wird ein →Programm zum Aufspüren von bösartigen →Apps eingesetzt: →Bouncer. Seine Effektivität ist umstritten. Außerdem stehen für Android-Geräte Apps auch von vielen anderen (zum Teil dubiosen) →Markets zur Verfügung

Google Streetview: umstrittener Service, bei der zusätzlich zu den Karten und Satellitenfotos auf →Google Maps auch Fotos beider Straßenseiten gezeigt werden. Da auf diesen Fotos auch Personen, Autokennzeichen u.ä. zu sehen sind, entstehen →Datenschutzprobleme. Mittlerweile werden in vielen Ländern Gesichter und Autokennzeichen automatisiert verpixelt (→Pixelation).

Ähnliche Dienste stehen von vielen Anbietern zur Verfügung, zum Teil von innerhalb der EU, die jedoch fast nie Verpixelungen durchführen. Im Rahmen von der Foto-Aktivitäten wurden von Google auch die →SSIDs von →WLAN-Netzen aufgezeichnet. Diese sollen der → Standortbestimmung in →Android →Smartphones dienen. Dabei wurden aber auch andere private Daten aufgezeichnet, aus Versehen, wie Google erklärte

Google Workspace: (auch G Suite genannt) Kombination von Software die vor allem an Firmen vermarktet wird, Konkurrenz zu →O365 von →Microsoft vor allem bei kleineren Unternehmen. In beiden Fällen wird die gesammte →Software →cloud-basiert angeboten und genutzt, es sind keine eigenen →Server mehr notwendig um eine Firmen-IT aufzubauen

GoP: →Grundsätze ordnungsmäßiger Buchführung

GOPHERSET: Programm der →NSA zur Manipulation von →SIM-Karten

Governance: (lat. Steuerung) Prozesse und Mechanismen zur Steuerung und Kontrolle einer Organisation. IT-Governance ist der Teilbereich, der sich mit Informationsverarbeitung befasst. Instrumente sind z.B. →Basel II, →SOX, →COSO (siehe IT-Governance Institute, http://itgi.org)

GPL: (GNU General Public License) Schema zur Lizensierung von →Open Source Software, (weiter)entwickelt durch die →Open Software Foundation. Wichtiger Punkt ist, dass bei Verwendung dieses Programmcodes alle daraus entstandenen Programme (Derivate) ebenfalls unter diese Lizenz fallen. Siehe →Copyleft,→Lizenz

GPO: (Group Policy Object) →Group Policies

GPRS: (General Packet Radio Service) Verfahren für die Übertragung von Daten über Mobilfunkstrecken. Durch die gleichzeitige Nutzung mehrerer →GSM-Kanäle können höhere Datenraten erzielt werden. GPRS ist als „always-on" Mechanismus implementiert. Das Verfahren wird zur Anbindung von →PDAs und von →Laptops (über GPRS →Handies oder spezielle →GSM/GPRS-Karten in Laptops) verwendet. Dabei wird dem Endgerät über das →DHCP-Protocol eine →IP-Adresse zugewiesen. Diese Adresse ist in der Regel im →Internet sichtbar. Obwohl die Funkstrecke der Verbindung verschlüsselt ist, stellt die Sichtbarkeit im Internet ein Sicherheitsproblem dar, das durch den Einsatz einer Personal→Firewall reduziert werden kann. Eine zusätzliche Absicherung des Datenverkehrs ist mittels →VPN möglich. Siehe →2G

GPS: (global positioning system) System das mit Hilfe einer großen Zahl von Satelliten und entsprechenden Empfängern den geographischen Ort, Höhe und Geschwindigkeit bestimmen können. Diese Funktionalität wird in mehr und mehr Geräte (z.B. →Smartphones, →Autos, etc.) eingebaut und kann dort in Verbindung mit entsprechenden Anwendungen zu Verletzungen von →Vertraulichkeit führen. Siehe →Geolocation, →A-GPS

GPS Jammer: illegale Geräte, die den Empfang von GPS-Signalen verhindern und z.B. von LKW-Fahrern eingesetzt werden um GPS-basierte Fuhrparküberwachung auszuschalten.

Auf Grund der immer stärkeren Abhängigkeit von Systemen wie Antennen-Ausrichtung, Synchronisation der Handy-Masten zwecks Gesprächsweiterleitung, Synchronisierung der Elektrizitätsnetze, Navigation von Flugzeugen, Zügen und den PKWs der Rettungsdienste kann dies zu ernsthaften Folgen führen. Die nächste Stufe sind dann **GPS Spoofer**, die GPS-Daten empfangen, leicht verändern und mit höherer Feldstärke wieder aussenden und damit anderen Geräten falsche Standorte vorspielen. Als Gegenmaßnahme wird u.a. „Receiver autonomous Integrity Monitoring" eingesetzt

GPU: (Graphics processing unit) spezieller →Prozessor, in allen modernen →Graphikkarten, Spielkonsolen und →Smartphones, der sehr schnell Informationen über Bilder (auch z.B. in 3D) (oder Filme) in die flache 2-D Darstellungen umrechnen kann. Dabei finden viele parallele Rechenoperationen statt (sowohl →Gleitkomma- wie auch Festkomma-(→Integer-)Operationen). Daher können diese Prozessoren auch für andere rechenintensive Operationen verwendet werden, z.B. →Passwort-Cracking, im „→Mining" von →Cryptocurrencies oder in →Supercomputern. Dabei kommen zum Teil mehrere GPUs pro PC bis hin zu extrem hohen Zahlen von GPUs zum Einsatz. Siehe auch →Graphikkarte

Gramm-Leach-Bliley Act: (GLBA, Financial Services Modernization Act, 1999) US-Gesetz, das für Finanzinstitutionen (im weitesten Sinne) Maßnahmen zum Schutz von Daten bzgl. →Integrität und →Vertraulichkeit vorschreibt.
http://www.ffiec.gov/ffiecinfobase/resources/management/con-15usc_6801_6805-gramm_leach_bliley_act.pdf

Graphikkarte: Komponente eines →Rechners der die Bildschirmanbindung herstellt. Früher sehr einfache Komponenten, heute können diese Geräte mittels →GPU sehr schnell hoch aufgelöste 3D-Objekte auf die 2D-Bildschirme „mappen". Sie benötigen dafür eine sehr hohe spezialisierte Rechenleistung. Diese Rechenleistung kann durch entsprechende →Driver auch für andere Aufgaben, z.B. im Bereich der →Kryptographie genutzt werden. Beliebt ist die Nutzung von solchen →Graphikkarten für das „Knacken" von →Passwort-Hashes durch →Brute Force →Angriffe auf gestohlene Hashes oder das „Minen" von →Bitcoins

GRC: (→Governance, →risk & →Compliance) Zusammenfassung der Anforderungen von →SOX. Entsprechende Software-Module decken →Benutzermanagement, →Autorisierungsmanagement, →Zugriffsmanagement und →Logging ab

Greeting Cards: (engl. Grußkarten) oft kostenlose Möglichkeit, per →E-Mail (oft animierte) Bilder mit einem Grußtext zu versenden (bzw. einen →Link auf eine →Website, auf der die Karte dann eingesehen werden kann). Es mehren sich Berichte, dass das implizite Vertrauen des Empfängers in den ihm bekannten Absender für die Installation von →Malware auf dem Rechner des Empfängers genutzt wird. Wird seit dem Siegeszug von →Messaging Apps wie →Whatsapp kaum noch verwendet

Greylist: Konzept der automatisierten →Spam-Bekämpfung bei →E-Mails. Der Mailserver verweigert die Annahme des E-Mails von einer bisher unbekannten Kombination von Absender und Empfänger und wartet darauf, dass der Sender noch einen Versuch startet. Dieser wird dann akzeptiert. Erhöht den Datenverkehr weiter und blockiert Ressourcen beim Sender. Falls es sich durchsetzt, werden die Spammer ebenfalls zweimal senden

Grid Computing: modernes Konzept, bei der eine große Zahl von Rechnern, verbunden durch Datennetze wie z.B. das →Internet, gemeinsam an einer Aufgabe arbeiten. Beispiel ist z.B. SETI, die Suche nach Spuren von außerirdischer Intelligenz in Radiosignalen. Zum Teil wird dabei eine standardisierte Software eingesetzt, z.B. der →Globus Access Grid Toolkit der Global Alliance Organisation. In dieser Software wird nicht nur der Datenaustausch abgehandelt, sondern auch Sicherheitsaspekte wie →Authentisierung. Bisherige Entwicklungen benutzen z.B. XrML (Extensible Rights Markup Language), XACML (Extensible Access Control Markup Language) und →SAML (Security Assertion Markup Language). Siehe →Cloud Computing

Group Policies: Konzept, nach dem auf der Basis von →Active Directory an zentraler Stelle viele Einstellungen von Windows-Systemen, u.a. auch wichtige Sicherheitseinstellungen leicht geändert werden können

Group Pressure: (engl. Gruppenzwang) oft ein Grund, warum Nutzer bei Diensten wie →Social Networks mitmachen die zu einer Aufweichung ihrer →Privatsphäre führen. Kann auch zu Effekten wie →Cyber Bullying führen. Siehe auch →Gamification, →Reputation System

Grundsätze ordnungsmäßiger Buchführung: (GoB) teils geschriebene, teils ungeschriebene Regeln zur →Buchführung und Bilanzierung, die sich aus Wissenschaft und Praxis, der Rechtsprechung sowie Empfehlungen von Wirtschaftsverbänden ergeben. Heute, u.a. durch →SOX und die 8.EU-Richtlinie (→EuroSOX) eng verknüpft mit →IT-Sicherheit. Siehe →IFRS

Grundschutz: minimale Schutzmaßnahmen, die auf jeden Fall erfüllt sein müssen

Grundschutzhandbuch: (GSH) vom bundesdeutschen →BSI herausgegebenes umfangreiches Werk zur Beschreibung einer Vorgehensweise zur →Informationssicherheit für Systeme mittleren Schutzbedarfs ohne vorhe-

rige spezifische →Risikoanalyse. Der Name impliziert, dass die dargestellten →Maßnahmen als Minimum betrachtet werden. →Grundschutz. Siehe http://sicherheitskultur.at/best_practise.htm

Grußkarten: (→Greeting Cards)

GSM: →2G

GSM Jammer: Geräte, die den Betrieb von GSM-→Handys stören. Sie sind in Europa verboten (aber erhältlich), werden von Bankräubern eingesetzt um →Tracking durch GSM-Geräte zu verhindern, die in →Bankomaten einbaut werden

GSS: (Generic Security Services) →API zur Implementierung von starken →Authentisierungen im →Internet. Siehe →RFC 1508, 1509, 2078

G Suite: →Google Workspace

GTIM: (Global Trade Identification Number) im Rahmen von →EPC zur Identifizierung von Waren eingesetzt. Siehe →RFID

GUI: (Graphical User Interface) Bedienungsoberfläche bei der die Information auf einem graphischen Gerät dargestellt werden und bei der die Bedienung über Maus und Keyboard (Tastatur) erfolgt

H.323: Signalling Empfehlung der →ITU für audiovisuelle Kommunikation, z.B. →VoIP. Die Übertragung ist verschlüsselt. Es scheint sich jedoch außer für Videokonferenzen →SIP durchzusetzen

Habbo Hotel: eine von vielen →virtual worlds für Kinder, problematisch wegen der Versuche von Pädophilen, diese Plattform zur Anbahnung von Kontakten zu nutzen (→Cybergrooming)

HACCP: (Hazard Analysis and Critical Control Points) →Risikomanagement-Methode in der Lebensmittelindustrie, heute auch oft in Pharmazie und anderen Bereichen genutzt. Im Zentrum steht die Identifizierung der Punkte, in denen kontinuierliche Messungen die Sicherheit der Produktion sicherstellen

Hacker: ursprünglich war Hacker ein positiv besetzter Begriff der für Programmierer verwendet wurden, der beim Entwurf, Eingabe und Ausführung eines →Programms die größtmögliche Effizienz anstrebte. Hacker wird heute allgemein für Personen verwendet, die sich unberechtigt Zugang zu einem technischen Informationssystemverschaffen, heute oft im Dienst der →organisierten Kriminalität. Siehe auch →Cybercrime, →Cyberwar, →Cyberterrorismus, →Shell, →VX, →Black Hat= →Cracker, →White Hat = →Ethical Hacker, →L0pht

HackerOne: (auch The Internet Bug Bounty) Initiative von →Facebook und →Microsoft um →Bug Bountys für →Schwachstellen in →Programmen anzubieten, die nicht direkt 1 Hersteller zugeordnet sind, z.B. in →Open Source Software wie →php, Python, Ruby on Rails, Perl, →OpenSSL, Apache, aber auch in grundsätzlichen Konzepten wie →Sandboxes von →Browsern und →Betriebssystemen. Außerdem bietet die Platform für Hersteller eine Fehlersuche als →Crowdsourcing an, d.h. Firmen können eine Belohnung für →Bugs in ihrer Software ausloben. Im Rahmen von HackerOne wurde auch →Heartbleed entdeckt

Hacktivismus: Kunstwort aus →Hacker und Aktivismus. Nutzung von →Angriffen (Gesetzesverletzungen) im →Internet auf →Netze oder →Systeme durch Private für politische Zwecke. Dabei wird →DoS verglichen mit Sitzstreik, →Wesite-→Defacing mit Spraypainting. Auch Methoden der →Cyberspionage werden eingesetzt um z.B. an Informationen über die Gegner zu kommen oder etwas aufzudecken. Ethisch bedenklich wird es, wenn Unbeteiligte zu Schaden kommen, z.B. durch die Veröffentlichung ihrer →Passworte. Beispiele sind →anonymous, →4chan, →LULZSEC, →cult of the dead cow, →Chaos Computer Club. Siehe →Cyberwar, →Slacktivism

http://sicherheitskultur.at/Angreifer_im_Internet.htm#hacktivism

Hadoop: spezielle →Datenbank die für sehr große Mengen von von unstrukturierten Daten (Petabytes = 1000 Terabytes = 1 Mio Gigabytes) eingesetzt wird, genutzt für →Data Mining. Hadoop wurde 2012 durch Impala ergänzt, das →SQL-Abfragen gegen die unstrukturierten Daten erlaubt. Benutzt das spezielle →Dateisystem →HDFS und oft auch →PIG.

Hadopi: durch ein umstrittenes französisches Gesetz 2009 eingesetzte Behörde, die nach einem "→Three-strike-Verfahren" gegen →Urheberrechtsverletzungen im →Internet vorgehen soll. Der Verdächtigte wird zunächst zweimal verwarnt, beim 3. Mal wird ein vereinfachtes Gerichtsverfahren eingeleitet, bei dem Geldstrafen und die zeitweilige Sperrung des Internetzugangs ausgesprochen werden können. Ein ähnliches Verfahren wurde 2011 in den USA durch private Vereinbarung zwischen Musikindustrie und →ISPs etabliert

Haftung: komplexer juristischer Begriff, zum Teil synonym mit Schuld verwendet. Relevant über den zivilrechtlichen →Schadenersatz im Zusammenhang mit →Vorsatz oder →Fahrlässigkeit. Eine Haftung für IT-Manager gegenüber dem Unternehmen oder Kunden kann sich aus der Nicht-Einhaltung von Gesetzen, aber auch aus mangelnder Sorgfalt, z.B. durch Ignorieren des →Stand der Technik ergeben. Eine Haftung für Diensteanbieter leitet sich in Ö aus §3 →ECG her (z.B. auch für Betreiber einer privaten →Website). Es kann sich z.B. ein →Unterlassungsanspruch ergeben. Siehe →DPI

Hacking Team: italienisches Unternehmen

das Software zum →Abhören von →PCs an beliebige Regierungen verkauft, auch an Diktatoren die es zum Auffinden von Dissidenten verwenden. Wurde im Sommer 2015 gehackt und 400 GB Mails und Unterlagen veröffentlicht. Dadurch konnten Firmen im Bereich →Malware-Schutz ihre Produkte so verbessern, dass sie diese Schadsoftware erkennen, Vergleichbare Firmen sind → FinFisher, →Vupen. Siehe →Black hat

Hailstorm: Security Scanner für →Web-Applications. Siehe →Penentration Test, →AJAX

Hamming: Theoretiker, Entwickler des **Hamming Codes** zur Fehlerkorrektur

Hamming distance und **Hamming weight**: beim Vergleich von 2 gleich langen String- oder Bit-Folgen die Zahl der Korrekturen um aus dem einen Wert den anderen zu bekommen. Wird beim Knacken von →Verschlüsselungen genutzt, z.B. bei →side channel attacks oder bei der →Iriserkennung

HAN: (Home Area Network) Konzept der Vernetzung von →Haushaltsgeräten und →Haustechnik. Gedacht ist dabei an →Computer, →Fernseher, Video-Recorder, aber auch Haushaltsgeräte und Alarmanlagen. Dieses Netz wird i.d.R. mit dem →Internet verbunden sein so dass von einem →Smartphone von überall auf die Geräte zugegriffen werden kann. Teile des Netzes werden drahtlos aufgebaut werden, z.B. mit →WLAN oder →Zigbee. Siehe auch →M2M, →HNAP

Hancock: von AT&T 2002 patentierte →Programmiersprache für →Data Mining und zum Ausforschen von →Communities of Interest. Siehe →LI, →IIS

Handy: im Deutschen umgangssprachig für Mobiltelefon (engl: mobile). Durch die fortschreitende Integration mit der Funktionalität von →PDAs und der Möglichkeit der Nutzung von →WAP-, →GPRS- und →UMTS-Diensten werden Sicherheitsfragen immer relevanter. Systembedingt muss der Aufenthaltsort jedes eingeschalteten Geräts dem Netzprovider bekannt sein (→Geolocation). Als Teil der →Verkehrsdaten sind diese Informationen für →Überwachungsmaßnahmen sehr begehrt. Geräte mit →A-GPS unterstützen solche Funktionalitäten noch besser. Siehe →MDA, →Semacode, →IMEI, →IMSI, →MSISDN

Handy-Strahlung: Mögliche Gesundheitsschäden durch die elektromagnetische Strahlung die in unserer Umwelt mehr und mehr präsent ist (nicht nur durch die →Handys und ihre Funkmasten, sondern z.B. auch die →WLAN-Router in jedem Haushalt). Im Zusammenhang mit der Einführung von 5G-Technologie spricht die WHO von „potentiell gesundheitsgefährdend". Es gibt derzeit keine Hinweise dass für elektro-magnetische Strahlung im Gegensatz zu ionisierender Strahlen (Alpha-, Beta-, Gamma-Strahlung) kein Wirkmechanismus in Richtung →DNA-Veränderungen kennt. Grundsätzlich hat elektro-magnetische Strahlung bei ausreichender Leistung eine Wärmewirkung (siehe Mikrowelle). Fakt ist, dass elektromagnetische Strahlung mit dem Quadrat der Entfernung abnimmt. D.h. ein Handy am Ohr hat bei gleicher Leistung eine vielfach höhere Wirkung als Handymasten in einiger Entfernung. Schwierig bei der Bewertung ist, dass digitale Handynetze erst seit ca. 1991 im Einsatz sind (→2G) und dass bei neueren Technologien andere Effekte auftreten könnten, d.h. es liegen keine Langzeiterfahrungen vor.

Hardware: physische Implementierung eines IT-Geräts, die heute jedoch sehr oft in Form von →virtuellen Geräten implementiert werden, natürlich letztendlich auch wieder auf einer Hardware

Härten: bei einem →Betriebssystem das Entfernen aller nicht benötigten Dienste und Software

Hash-Funktion: generiert aus einer beliebigen Datenmenge einen kurzen Extrakt (ähnlich wie „checksum", **Hash-Wert**) und zwar derart, dass aus dem Extrakt die ursprüngliche Datei nicht rekonstruierbar und es zudem extrem aufwendig ist, eine Datei anderen Inhalts zu erzeugen, die denselben Hash-Wert liefert (→Kollision). Bei der digitalen Signatur wird der Hash-Wert einer Nachricht, z.B. einer →E-Mail, mit dem privaten Schlüssel des Absenders verschlüsselt, um die →E-Mail mit einer digitalen →Signatur zu versehen. Fortschritte der Kryptographie haben 2005 die Sicherheit der häufig eingesetzten Hash-Algorithmen →MD5 und →SHA-1 langfristig in Frage gestellt. Neuere Algorithmen werden gesucht: MD 160 (→RIPE). Siehe →MAC, →HMAC, →Salz, →Fuzzy Hashing

Hassposting: Äußerungen im →Internet, typischerweise in →Social Media, die zu zum Hass gegen andere Personen aufrufen, oft auf Grund von Rasse, Sexualität, Herkunft, oder wegen anderen politischen Positionen. Die juristische Bekämpfung ist oft schwierig, u.a. weil die →Identität des Posters in vielen Fällen nicht sicher festgestellt werden kann. Aber auch weil z.B. in Ö der Tatbestand der Beleidigung eine Äußerung in einer größeren „Öffentlichkeit" voraussetzt. Solche Äußerungen können bis zu Morddrohungen reichen und haben in anderen Ländern mittels →Facebook-Postings auch bereits Progrome ausgelöst (siehe z.B. die Rohingya in Myanmar). Von Politikern wird als Gegenmaßnahme oft ein →Klarnamenszwang gefordert, der aber ebenfalls problematisch ist. Siehe →Netzwerkdurchsetzungsgesetz, →Klarnamenszwang

Hauptspeicher: →Speicher, →Arbeitsspeicher

Haushaltsgeräte: im Rahmen von →M2M werden mehr und mehr vernetzte Haushalts-

geräte angeboten, die mittels →HAN miteinander verbunden sind, aber auch mit den →Smartphones auch über beliebige Entfernung gesteuert oder automatisiert werden können, z.B. Einschalten der Kaffeemaschine durch den Wecker oder aus der Ferne. Da in solchen einfachen Geräten →Authentisierungen fast nie sauber implementiert werden sind viele neue →Angriffsmöglichkeiten zu erwarten. Siehe auch →Haustechnik

Haustechnik: Zusätzlich zu den →Haushaltsgeräten werden auch Steuerungen wie Thermostate, Rauchmelder, Lampen über →HAN miteinander und mit dem →Internet vernetzt. →Google hat 2014 die Firma Nest übernommen, die auf Thermostate spezialisiert ist. Google erwartet sich aus den →Daten der Haustechnik noch viel mehr Informationen über die Menschen, die dann für gezielte Werbung eingesetzt werden kann. Zugpferd für diese intelligenten Automatisierungen ist die Bequemlichkeit der Steuerung über →Smartphone →Apps. Siehe auch →M2M

HBA: (Host Bus Adapter) Adapter-Karte in einem Server. Beispiele sind →Fibre Channel Adapter, →SCSI- oder →iSCSI-Karten. Siehe →Bus

HBCI: (Homebanking Computer Interface) in D. standardisiertes Interface, das ein sichereres →Homebanking mittels eines speziellen Clients erlaubt, bei dem z.B. die gegenseitige →Authentisierung durch →Smartcard abgesichert werden kann. Weiterentwickelt zu →FinTS. Könnte jetzt im Prinzip durch die Schnittstellen nach →PSD2 abgelöst werden, die (im Gegensatz zu FinTS oder HBCI) von allen Banken in Europa unterstützt werden müssen

HBGary Federal: US Sicherheitsfirma die u.a. für Regierungsbehörden arbeitete und auch vor unethischen bis illegalen Aktivitäten nicht zurückschreckte. Nach der Ankündigung des CEO Aaron Barr in 2010 dass er Mitglieder von →Anonymous enttarnen werde hat Anonymous die Server von HBGary mittels einer Kombination von →SQL-Injektion und →Social Engineering übernommen und alle →Daten und →E-Mails des Unternehmens veröffentlicht.
http://sicherheitskultur.at/notizen_1_11.htm#hbgary

HCE: →Host Card Emulation

HDCP: (High-bandwidth Digital Content Protection) →DRM-Verfahren für digitale Videoausgänge von →PCs, DVD-Spieler u.a. z.B. DVI- oder →HDMI-Ausgänge. Implementiert z.B. in neuen MacBooks und in →Vista. Content der von HDCP geschützt ist wird nur nach →Schlüsselaustausch und →Verschlüsselung zu einem entsprechenden Wiedergabegerät übertragen. Okt.2010: es wird berichtet, dass der Masterkey im Internet veröffentlicht wurde, 2013 wird berichtet, dass jemand einen Kabel-Adapter entwickelt hat, der gültige Schlüssel offen legt

HDFS: (Hadoop Distributed File System) spezielles →Dateisystem für sehr große unstrukturierte Daten die mittels →Hadoop analysiert werden sollen. Die Daten werden über viele Knoten verteilt

HDMI: (High-Definition Multimedia Interface) Standard (Hardware und Software) für die Verbindung digitaler Abspiel und Wiedergabegeräte für Filme in hoher Auflösung. Der Standard enthält High-bandwidth Digital Content Protection (→HDCP), ein Verfahren mit dem eine hochauflösende →DVD (Blueray oder HD DVD) das HDMI-Gerät mittels "image constraint token" (ICT) zum Downgrade der Auflösung veranlassen kann, wenn Geräte angeschlossen werden, die als „untrusted“ betrachtet werden. Dies soll die Nutzung von →Raubkopien einschränken (→DRM), da diese Geräte mit einem →Kopierschutz ausgestattet sein sollen. Da aber derzeit kaum HDMI-lizensierte Geräte zur Verfügung stehen hat sich die Industrie darauf geeinigt, dass die Content-Anbieter diese Feature frühestens 2010 aktivieren, siehe →AACS

Headset: Kombination aus Kopfhörer und Mikrophone, in 2020 stark nachgefragt wegen dem Boom an →Webkonferenzen da die Qualität eines Headsets deutlich über der von eingebauten Mikrophonen in →Laptops liegt. Die Geräte werden mit →USB-Kabel oder mit →Bluetooth-Anbindung angeboten. Eine weitere optionale Feature ist →ANC. Für →Apple-Geräte können auch →AirPods genutzt werden

Heap Overflow: Variation des →Buffer Overflows. Überlauf eines Speicherbereiches im Arbeitsspeicher eines →Computers, in →Malware genutzt für →Angriffe. Heap bezeichnet einen dynamischen Speicherbereich in →Programmen

Heartbleed: →Bug in →OpenSSL bei eine wenig genutzt Heartbeat-Funktionalität (im logische Sitzungen auch bei Inaktivität aufrecht zu erhalten) ausgenutzt werden konnte um 64KB Speicher von →Webservern auszulesen, in denen sich Dateninhalte der letzten Übertragungen und unter Umständen auch die privaten →SSL-Schlüssel befinden können. Damit waren auf 1 Schlag 2/3 aller Webserver verwundbar. Es musste nicht nur die Software aktualisiert werden (was unterschiedlich schnell umgesetzt wurde), sondern es mussten auch neu SSL-→Zertifikate bestellt und installiert werden, eine erhebliche Anforderung an die →CAs. Heartbleed wird als GAU des Internets betrachtet. Es betrifft auch viele andere Komponenten, wie z.b. →TOR, →VPN-Produkte und vieles andere mehr. In →Embedded Systems lässt sich so ein Fehler kaum beheben, viele Geräte werden für immer verwundbar bleiben. Der Fehler war seit 2

Jahren in der Software, es ist nicht ganz klar, ob er nicht in dieser Zeit auch heimlich ausgenutzt wurde

Heuristics: Verfahren der → Malware-Schutz, bei dem nicht wie sonst üblich nach Informationspattern (Mustern) gesucht wird, sondern durch Simulation der Programmausführung analysiert wird, ob das betreffende →Programm sich wie →Malware verhält

HFNetChk: Command Line Tool zum Scannen von →Client →PCs in Windows-Netzen, agentless, d.h. braucht keine Software auf dem Client

HFS: (Hierarchical File System) für →MacOS oder (Hi Performance FileSystem) für HP-UX. Siehe →File System

HFT: →High Frequency Trading

Hidden File: →Datei, die über ein Attribut „unsichtbar" gemacht wird, d.h. für den „normalen" Anwender nicht sichtbar ist. Auf diese Weise soll eine versehentliche Beschädigung vermieden werden. Wird jedoch auch von →Malware benutzt um der Entdeckung zu entgehen. Siehe →Obfuscation

Hidden Volume: unsichtbares →Dateisystem. Siehe →TrueCrypt, →Deniability

Higgins Trust Framework: →Open Source Initiative zu →federated identity. Siehe →SAML

High Availability (HA): →Hochverfügbarkeit

High Freqency Trading: (HFT) automatisierter Handel an Börsen. Dafür sind extrem direkte Anbindungen an die Rechner einer Börse notwendig, am besten im gleichen Gebäude oder mit einer direkten →Lichtleiter-Verbindung. Entscheidend ist nicht die Bandbreite, sondern die →Latency, d.h. die Verzögerung bis das erste Byte ankommt. Dabei werden Kauf- oder Verkaufsangebote nur für wenige Millisekunden angeboten und sofort wieder zurückgenommen. Ziel ist es, minimale Kursunterschiede die nur für kurze Zeit bestehen, auszunutzen. Dabei kommt es zu sog.flash crashes, bei denen für Zeitspannen im Sekundenbereich riesige Kurseinbrüche oder –sprünge passieren können, da andere Rechner ebenso schnell auf Kursveränderungen reagieren und sich so leicht hochschaukeln. Die Kurse stabilisieren sich entweder automatisch nach einiger Zeit oder die Börsenaufsicht unterbricht den Handel. Diese Handelsaktivitäten sind umstritten. Bereits 2010 machte High-Frequency Trading bereits 70% der Umsätze von US-Börsen aus. 2012 verlor ein High-Frequency Trader (Knight Capital) innerhalb von 40 Minuten 400 Mio. $, da es einen Fehler im Algorithmus gab und der Rechner aus unbekannten Gründen nicht gestoppt werden konnte. 2014 bekommt das Thema durch das Buch „Flash Boys" erhöhte Aufmerksamkeit. Es geht dabei auch um Aktivitäten von solchen Händlern, die „orders" von menschlichen Händlern zu „überholen" und vorher den Titel zu kaufen und dann zu einem veränderten Preis wieder anzubieten. Dabei lassen sich z.B. Gewinnspannen von 0,5% erzielen, was jedoch bei Milliardenumsätzen pro Tag sehr viele Millionen ergibt

HIPERLAN: Standard einer alternativen Technologie zum →WLAN-Standard, um Funknetze zwischen Rechnern aufzubauen. Die Standards haben sich auf dem Markt nicht durchsetzen können, obwohl sie technisch interessante Konzepte enthalten

HIPPA: (Health Insurance Portability and Accountability Act) US-Gesetz, das u.a. →Datenschutzregeln für den Umgang mit gesundheitsbezogenen Daten vorschreibt. Das Gesetz betrifft auch alle Firmen, die für ihre Mitarbeiter Krankenversicherungen anbieten. Siehe →eHealth, →PHI, →ePH, →ELGA, →eGK

HIPS: (Host Intrusion Prevention) neue Technik bei Windows Vista, die den Kern des →Betriebssystems (→kernel) vor →Angriffen schützen soll. Siehe →IPS, →NIPS

History: Datei eines →Webbrowsers eine Liste der besuchten →Websites gespeichert wird. Wenn →Vertraulichkeit gewünscht wird, muss sichergestellt werden, dass diese Datei regelmäßig gelöscht wird. Siehe →Private Browsing, →Forensics

HL7: (Health Level Seven) →EDI-Standard für das Gesundheitswesen

HLM: (→home location register)

HMAC: (keyed-**h**ash **m**essage **a**uthentication **c**ode) →Message Authentication Code der durch die Nutzung von kryptographischen Verfahren plus einem →Schlüssel erzeugt wird. Beispiele: HMAC-→SHA-1, HMAC-→MD5

HMI: (human machine interface) Schnittstelle für die Interaktion von Menschen mit Maschinen, z.B. →Computern und komplexen Systemen, z.B. →SCADA. Beinhaltet Input- und Output-Elemente und kann bei schlechtem Design (→Usability) Ursprung von Fehlbedienungen und Fehleinschätzungen sein

HNAP: →Home Network Administration Protocol

Hoax: (engl. Streich, blinder Alarm) Falschmeldung, häufig in Form einer Warnung vor einem angeblichen, aber nicht wirklich existierenden →Virus, häufig in Form einer Ketten-Mail verbreitet, in der vor bestimmten Programmen, Dateien, ja selbst vor →E-Mails gewarnt wird

Hochverfügbarkeit: (High Availability) Einsatz von →redundanten Systemen, die eine weitere Verfügbarkeit einer Anwendung, auch nach Ausfall eines Systembestandteils, ermöglicht. Beispiele sind →Clustersysteme, →Load Sharing, →RAID-Platten, →Enterprise Storage

Systeme und Stand-By Rechner)

HOIC: (High Orbit Ion Cannon) gefährlichere Variation des →LOIC, verwendet für →dDoSD-→Angriffe. Ein →open source Werkzeug, der Angreifer muss nur die →URL des Ziels eingeben

Home Automation: (Heimautomation, auch Smart Home) Umstellung von Haushaltsgeräten wie Licht, Heizung, Warnanlagen, Küchengeräten, →Fernseher auf Vernetzung und Automatisierung. Verwendet werden dabei u.a. →HAN mit Protokollen wie →Z-Wave oder →ZigBee. Dies ist Teil des →Internet of Things und hat alle die Probleme, die dort entstehen.

Es konnte 2014 gezeigt werden, dass ein solche Geräte extrem unsicher sind und sehr leicht angreifbar. Dies liegt u.a. daran, dass die Geräte sehr einfach bedienbar sein sollen, d.h. sich selbständig neue →Firmware-Updates aus dem →Internet nachladen, was leicht von →Angreifern ausgenutzt werden kann. Aber auch ohne direkte Angriffe entsteht auf der Grund der fast immer üblichen →Cloud-Implementierung (die „Intelligenz" ensteht weitgehend erst dadurch, dass die Messungen und Events des einzelnen Hauses zusammengeführt und zentral mittels →Big Data Techniken ausgewertet werden) immer eine Verletzungen der →Vertraulichkeit. „My Home is my Castle" kann für das Smart Home nicht gesagt werden. Wenn nur der Ex-Partner →Zugang zu diesen Geräten und dem →WLAN-Zugang hat weil z.B. nur er oder sie die →Passworte kennen, so stellt dies eine Form der →digitalen Gewalt dar, entweder über →Zugriffe auf →Kameras oder durch unautorisierte Manipulation von Licht oder Türschlössern

Homebanking: →e-Banking

Home location register: (HLR) →Datenbank die jeder →Handy-→Netzbetreiber haben muss, in der für jede →SIM-Karte 1 Eintrag liegt. Dort wird eingetragen, in welcher →Base station sich ein Handy gerade eingebucht hat, d.h. auch in welchem Land. Auf diese Weise wird Roaming ermöglicht, der Provider im Heimatland weiß, in welches andere Netz er eingehende Anrufe für dieses Gerät weiterleiten muss. Dort ist dann bekannt, in welcher Base Station das Handy gerade angemeldet ist

Home Network Administration Protocol: (HNAP) von Cisco gekauftes high-level →Protokoll für die →Identifikation, Konfiguration und Administration in einem Netzwerk. Beruht auf →SOAP und sendet →Daten zumeist in Klartext. Wird hauptsächlich für „home" →Router genutzt, d.h. →ISPs nutzen HNAP für die Administration der Geräte ihrer Kunden. Schwächen in der Implementierung haben 2010 und 2014 zahlreiche →Angriffe gegen „home" →Router vieler Hersteller ermöglicht

Home Office: Arbeiten „von zu Hause", kam 2020 zu einem Durchbruch als dies weitgehend „angeordnet" wurde. Dies führte zu einem Boom an →VPN-Implementierungen (damit sich →PCs und →Laptops) in die Firmennetze verbinden können und dort die üblichen →Anwendungen genutzt werden können. Die andere Alternative sind →Desktop-Sharing Lösungen wie →ICA, MS →Terminal Server oder →VNC. Bei beiden Technologien können bei der Implementierung zahlreiche Fehler gemadcht werden. Wichtig ist z.B. auf jeden Fall →2 Faktor Authentisierung. Ein weiteres Ergebnis war der Durchbruch bei →Webkonferenzsystemen, die die Bedeutung von →Videokonferenzen auf Hardwarebasis stark bedrängt haben.

Es wird spekuliert, dass dabei auch →Metcalfe's Law relevant sein könnte. Vor 2020 fanden Meetings nur ausnahmsweise über →Webkonferenzsysteme statt, jedes Arbeiten von zu Hause zwang alle anderen ebenfalls zur Nutzung des Systems und die remote Nutzer waren nicht voll integriert. In 2020 wurde „remote" zum Standard und dies machte es einfacher für den Einzelnen der zu Hause bleiben wollte.

Falls es nach der Pandemie bei einem Anstieg des Home Office-Anteils gegenüber 2019 bleiben würde so hätte das wohl zahlreiche Auswirkungen, z.B. bevorzugte Wohnorte, dadurch Miethöhen in den Städten vs. weiter entfernt. Ein Ausdünnen der Städte könnte zu einer Reduktion des öffentlichen Verkehrsangebots führen, etc.

Homomorphic Encryption: →Verschlüsselungsverfahren bei dem es möglich ist, mit den verschlüsselten Daten arithmetische Operationen auszuführen. Dies ist notwendig wenn z.B. Daten in der →Cloud gespeichert und verarbeitet werden, der Betreiber jedoch keinen →Zugriff zu den Daten haben soll. Fully homomorphic bedeutet dass sowohl Addition wie auch Multiplikation möglich sind, in diesem Fall sind auch alle anderen Operationen möglich. Ein Anwendungsbeispiel wären z.B. →Smart Meter, die den Verbrauch aufaddieren ohne ihn zu kennen. Siehe auch →searchable Encryption, →multi-party computation http://www.americanscientist.org/issues/pub/alice-and-bob-in-cipherspace/1

Homepage: private →Webseiten, die ab ca. 1995 populär wurden und ab ca. 2004 weitgehend durch →Profile auf →Social Networks abgelöst wurden. Siehe auch →Content

Honeypot: Testrechner im →Internet mit Standardprogrammen, dessen Sinn darin besteht, →Hackerattacken zu provozieren, zu erfassen und zu dokumentieren, um daraus Erfahrungen für Echtsysteme zu sammeln. Auch in der Form von Honey-Clients, d.h. spezielle →Webbrowser die auf →Websites

nach →Schadsoftware suchen (Capture, Monkey Spider). Wird auch im →ICS-Umfeld eingesetzt

Hop: in →IP-Netzen typischerweise ein →Router, der →Daten zum Ziel weiterleitet. Der Abstand in IP-Netzen wird oft in Hops angegeben, da jeder Hop eine geringe Verzögerung (→„latency“) in eine Datenverbindung einbringt (nicht zu verwechseln mit „Bandbreite“). Bei →Angriffen im →Internet wird der Ursprung des Angriffs oft verschleiert, indem Rechner unter der Kontrolle der Angreifer als zusätzliche „hop points“ genutzt werden, so dass deren IP-Adresse dann als Absender in den →Logs des Opfers auftaucht um auf diese Weise die →attribution des Angriffs, d.h. die →Identifizierung des Angreifers, zu erschweren

Host: alter Name für →Mainframe

Host Card Emulation: Software Architektur die es ermöglicht dass virtuelle Repräsentationen von →Identitätskarten, wie z.B. →Kreditkarten für die Nutzung in tragbaren Geräten wie →Smartphones ohne sicheren Hardwarespeicher (→TPM) z.B. für Zahlungsdienste über →NFC genutzt werden können. Eingesetzt bei →Google Pay. Bei →Apple Pay nicht notwendig, da alle →iOS Geräte auf einer einheitlichen Hardware beruhen die entsprechende Hardware-Elemente enthält

Hoster: →Webhoster

Hosting: Form des →Outsourcings bei der eine Anwendung auf fremder Hardware genutzt wird (oft verwendet für →Websites, auch in der Form →Virtual Host) oder als eine Form des →Cloud Computings, wie bei →EC2. Siehe →19-Zoll Rack

Hosts file: Datei in vielen Betriebssystemen, in dem eine Zuordnung zwischen Servern oder →Domainen und →IP-Adressen vorgenommen wird. Wenn eine Domaine hier eingetragen ist, so wird die IP-Adresse nicht über →DNS ermittelt. Eine Modifikation des hostsfiles erlaubt →Phishing Angriffe

HOTP: (HMAC-based One-time Password Algorithm) →Authentisierungsverfahren bei dem ein →Algorithmus auf der Basis von kryptografischen Elementen ein einmal zu nutzendes →Passwort generiert wird (→OTP). Bei jeder Nutzung wird ein Zähler um 1 erhöht und dadurch ein anderes →Passwort generiert. Es kann passieren, dass der Client-Zähler höher ist als der des →Servers (z.B. weil bei einem anderen Server genutzt), daher muss eine Resynchronisierung implementiert werden. Siehe auch →keyless system, →TOTP

Hot Site: →Rechnerraum für →Hot-Standby

Hotspot: Einwählpunkt/Einwählbereich in ein →WLAN (→Access Point), bei dem ein Nutzer einen drahtlosen Zugang zum Internet erhalten kann. Mit Hotspots in Hotels, Restaurants, auf öffentlichen Plätzen usw. kann man sich z.B. mit einem →Notebook oder →Smartphone mit Funkkarte ins →Internet einwählen. Wegen möglicher Gefährdungen sollte dies nur mit gut geschützten Rechnern geschehen (z.B. Virenschutz, →Firewall, aktualisierte Systemversionen, Sicherheitspatches, etc.). Siehe →Internetcafé

Hot-Standy: Verfahren der →Hochverfügbarkeit, bei dem nur einer von 2 Rechnern aktiv in Produktion ist, der andere jedoch jederzeit innerhalb einer sehr kurzen Umschaltzeit die Last übernehmen kann. Im Gegensatz dazu →Cold Standby, →Fail-over

Housing: Form des →Outsourcing bei der eigene oder fremde Hardware in einem fremden Rechenzentrum betrieben wird (Strom, Klima, räumliche Sicherheit werden vom Housing-Anbieter bezogen). Erlaubt nur sehr eingeschränkten →Zugang zu den Rechnern und erfordert →Fernwartungssoftware. Wurde weiterentwickelt zu →cloudbasierten Angeboten wie Amazon →EC2, bei der die Hardware nur „virtuell“ zur Verfügung steht und dadurch auch nur bei Bedarf angemietet wird

HPKP: (HTTP Public Key Pinning) Verfahren zur Vermeidung von →Man-in-the-Middle →Angriffen bei →HTTPS-Verbindungen zu →Webservern. Dabei übermittelt der Server an den →Webbrowser einmalig die Merkmale des Server-→Zertifikats, das zukünftig genutzt werden soll. Der Browser speichert dieses und erlaubt zukünftig nur noch Verbindungen zu dieser Website die mit diesem Zertifikat verbunden sind. Probleme entstehen wenn nach dieser ersten Übertragung der Administrator der Website dieses Zertifikat „verliert“ oder gestohlen bekommt. Dann ist keine Verbindung mehr möglich, der Fachbegriff ist „HPKP Suicide“. Dies könnte auch für Erpressung genutzt werden, wenn ein Angreifer das Zertifikat unter seine Kontrolle bringen kann („RansomPKP“). alternative Verfahren sind →Certifikate Transparency und →Certificate Authority Authorisation

HR: (Human Resource, engl. für Personalabteilung) muss in die →Informationssicherheit einbezogen werden, siehe entspr. Kapitel in →ISO 17799

HSCSD: (High Speed Circuit Switched Data) schnelleres Datenübertragungsverfahren auf der Basis von →GSM (ähnlich zu →GPRS). HSCSD wird zugunsten der paketorientierten Übertragung GPRS/→EDGE und →UMTS/ →HSDPA an Bedeutung verlieren

HSDPA: (High Speed Downlink Packet Access) Verfahren zur Beschleunigung des Datentransfers bei →UMTS (von 380 kbit/s bei UMTS auf die zehnfache Leistung)

HSM:
1) (High Security Modul) spezieller Hochsicherheitsspeicher, i.d.R. zur Aufbewahrung

von privaten →Schlüsseln von Banken oder →Zertifizierungsstellen. Zerstörung des Speicherinhaltes bei unberechtigtem Öffnen des Gerätes. Speicherinhalt sollte das Gerät nie verlassen, für →Disaster Recovery ist jedoch eine separate Aufbewahrung des Inhaltes notwendig. Entspricht von der Funktionalität her einer →SmartCard und wird nach →FIPS-140 bewertet

2) (Hierarchical Storage Management) Auslagerung von selten genutzten Daten auf billigere Speichermedien

HSPD: (Homeland Security Presidential Directive) US-Regierungsanweisungen im Rahmen von →DHS. HSPD)-5 richtet ein National →Incident Management System (NIMS), das von allen Bundesbehörden genutzt werden muss. HSPD-12 bestimmt, dass bei Bundesbehörden ab Aug.2006 →Smartcards mit →biometrischer Absicherung (nach dem Standard FIPS-201, Federal Identity Processing Standard) für die →Authentisierung von Mitarbeitern für den →Zugang zu Gebäuden und den →Zugriff zu →Daten genutzt werden müssen. Smartcards werden vor allem im Finanzbereich nach →FIPS-140 bewertet

HSTS: (HTTP Strict Transport Security) neuer Mechanismus mit dem eine →Website signalisieren kann, dass sie nur über →HTTPS kommuniziert. Ziel ist das Verhindern von →MITM-→Angriffen. Leider kann ein Angreifer diese Nachricht unterdrücken. Daher müssen die →Webbrowser bereits eine entsprechende Liste beinhalten von Websites die nur über HTTPS kommunizieren möchten

HTML: (Hypertext Markup Language) von →SGML abgeleitete Sprache, die verwendet wird, um den Inhalt von Webseiten zu kodieren. Eine der wichtigsten Features ist der →Hyperlink, mit dessen Hilfe von einer gegebenen Seite auf einer andere verknüpft werden kann. Siehe →DHTML, →WebDAV. Tutorial auf http://de.selfhtml.org/

HTML5: Nachfolgeversion von HMTL4. Sie unterstützt neue Formen des lokalen Speichers (→HMTL5 Storage statt →Cookies), dynamische 2D und 3D Graphiken und macht damit z.B. →Flash unnötig. HTML5 bietet auf Grund der erweiterten Funktionalitäten auch neue Möglichkeiten für →Schwachstellen, entweder in den →Browser-Implementierungen, durch neue Funktionalitäten wie z.B. neue Möglichkeiten, externe Quellen einzubinden (`poster`, `srcdoc`) oder →Web sockets oder Web Messaging. Probleme können aber auch entstehen wenn Entwickler von →Websites im lokalen HTML5-Speicher sensible Daten ablegen, die dann entweder durch →Schadsoftware auf dem →PC ausgelesen werden oder auf Grund von Implementierungsfehlern auch anderen Websites zur Verfügung stehen. HTML5 bietet auch neue Möglichkeiten für →XSS. Siehe auch → Cross-Origin Resource Sharing

HTML5 Storage: →DOM Storage, wird für →Tracking von →Benutzern verwendet

HTML-Injection: Einfügen von →HTML-code in fremde →Websites zum Zwecke eines → Angriffs, z.B. →Phishing. Kann über →MITM, →XSS oder auf dem →PC des Nutzers geschehen (→Schadsoftware)

HTTP: (Hypertext Transfer Protocol) auf dem →IP-Protokoll basierendes Verfahren mit dessen Hilfe ein →Web-Browser mit einem →Webserver kommunizieren kann - nicht zu verwechseln mit →HTML. Das http-Protokoll wird für beide Richtungen eingesetzt, vom →Webbrowser zur →Website und dann die Antwort von der Website zum Webbrowser. 2012 wird bekannt, dass einige Mobilfunkanbieter die →Identität der Nutzer (mittels →IMSI oder →MSISDN) in den http-Headern mitsenden. Zur Verschlüsselung von http-Verbindungen wird →https eingesetzt.

2015 kommt http 2.0 in Fahrt. Dabei geht es darum, dass moderne Website auch bei schnellen Anbindungen ans Internet langsam laden, die schon eine simple Website heute nach dem eigentlichen HTML-Object viele weitere, wie z.B. Style sheets (→CSS) oder →JavaScript Module nachlädt. In http 1 erfordert dies jeweils neue logische Verbindungen zum Webserver, deren Aufbau jeweils eine beträchtliche →Latency, d.h. Verzögerung bedeutet (und außerdem viele Netzwerkgerät die die Verbindung bearbeiten müssen, wie →Firewalls, Load Balancer, und den Webserver selbst, belasten. Daher werden in http 2 alle Datenobjecte die im Rahmen des Ladens 1 Page kommen von dem Webserver auf derselben logischen Verbindung übertragen. Für die Sicherheit sollte sich nichts ändern. Nach den Veröffentlichungen der →NSA-Leaks durch →Edward Snowden wurden nahezu alle Verbindungen vom unverschlüsselten http auf das verschlüsselte →https umgestellt. Geholfen hat dabei, dass →Google damit gedroht hatte, diese Websites nicht mehr zu listen und/oder als unsicher zu markieren. Siehe →QUIC

HTTPflood: →Angriff auf Rechner (→DoS) bei der durch das Anfordern einer sehr großen Zahl von Elementen einer →Website diese lahmgelegt wird. Siehe →Denial of Service

http referer: Tippfehler in der →HTTP-Dokumentation. Siehe →Referrer

https: Variante des →http-Protokolls, welches das Verschlüsselungsprotokoll →SSL, bzw. →TLS nutzt. Es wird für →E-Banking und bei E-Commerce eingesetzt, wenn vertrauliche Daten übertragen werden sollen. Erkennbar ist der Einsatz durch die Buchstaben „https://..“ in der →URL-Zeile des →Webbrowsers und am Vorhängeschloss-Symbol am Rande der Browseroberfläche. Benutzt →Zertifikate um

die Identität des →Webservers sicher zu dokumentieren. 2011 kam es zu zahlreichen Sicherheitsverletzungen bei →Certificate Authorities, daher wird 2012 ein neues Verfahren, →Sovereign Keys vorgeschlagen. Siehe auch →HSTS. http://sicherheitskultur.at/notizen_1_13.htm#https

Huawei: großes chinesisches Unternehmen im Bereich →Router, →Smartphones und Technologien für Unterseekabel. Die USA werfen der Firma Verbindungen zur →PLA vor und befürchtet, dass die Geräte →Backdoors enthalten. 2014 wird bekannt, dass die →NSA tief in die Netze von Huawei eingedrungen ist und wohl auch →Zugriff auf Quellcode und Technologien hat

Hub: Verkabelungstechnologie, bei der einzelne Geräte eines Datennetzes (→LAN) oder ganze Datennetze an einem →Port des Hubs angeschlossen sind. Im Gegensatz zum →Switch erscheint der gesamte Datenverkehr aller angeschlossenen Netze auf jedem der Ports

Hubzilla: sehr vielseitiger Dienst mit →Social network, →Blogging und →Micro blogging, →Wiki, Image gallery, File hosting der die →Protokolle →ActivityPub, →Diaspora und →OStatus unterstützt und dadurch →Daten mit vielen anderen Diensten austauschen kann. Siehe →Fediverse

Human-in-the-Loop: (man-in-the-loop) beschreibt Situationen, bei denen eine Sicherheitsentscheidung erst dann gefällt wird nachdem Menschen über →Alerts, →Status-Anzeigen o.ä. auf eine Situation aufmerksam gemacht wurden. Dies betrifft u.a. alle Warnungen, die von →Webbrowsern angezeigt werden. In der Praxis führt dies oft zu schlechten Sicherheitsentscheidungen, z.B. weil der Mensch die Kommunikation übersieht, missversteht oder aus anderen Gründen die falsche Entscheidung trifft. Daher sollte bei Sicherheitsdesign immer versucht werden, im →Programm selbst die bestmögliche Entscheidung zu treffen. Siehe →Fehler

Auch Schlagwort bei →autonomen Waffen, das besagt, dass die entgültige Entscheidung zum Töten immer einem Menschen überlassen sein muss. Dies ist die NATO-Doktrin in 2019. Es wird vermutet, dass diese Doktrin in dem Augenblick fällt, wenn das erste autonome Waffensystem eines Gegners zu einer ernsthaften Bedrohung für die NATO führt. Hintergrund ist, dass bei einem Man-in-the-Loop immer nennenswerte Reaktionsverzögerungen entstehen (im Sekundenbereich). Dies könnte z.B. bei einem Luftkampf mit einem autonom gesteurten feindlichen Flugzeug ein Nachteil sein. Die Doktrin wird aufgeweicht indem sie nicht gilt, wenn das feindliche System zuerst angegriffen hat, worunter auch Zielsuch-Radar verstanden wird

HVAC: (heating, ventilation, and air conditioning) Lieferanten für moderne Systeme der Haustechnik brauchen üblicherweise heute online →Zugriff auf "ihre" Geräte. Dafür wird ihnen oft →Zugang zum internen Netz gegeben. Dies ist ein Fehler, wie die Firma Target in den USA in 2014 bitter lernen musste: →Angreifer drangen in das Netz der Wartungsfirma ein und gelangten von dort in das Target-Netz und konnten ca. 700 000 →Kreditkarten „entführen"

Hyperlink: eine der wichtigsten Features von →HTML, erlaubt das direkte Verknüpfen von Textstellen in unterschiedlichen →Dokumenten auf unterschiedlichen →Servern mit Hilfe einer →URL. Da →Anwender oft nicht überschauen können, wohin ein Link wirklich führt, können diese über einen Link auf eine →Website mit → Malicious Code geschickt werden, die durch Vortäuschen des erwarteten Inhalts, z.B. der Bank des Anwenders (→Spoofing) zu einem →Phishing-Angriff ausgenutzt werden kann

Hypervisor: uneinheitlich genutzter Begriff aus dem Bereich →Betriebssystem-→Virtualisierung. Wichtig ist die Absicherung dieser → Accounts, da ein ‚böser" Administrator mit diesen Zugriffsrechten sehr viele Maschinen übernehmen und für seine Zwecke nutzen kann

I2P: (Invisible Internet Project) Projekt zur Entwicklung eines anonymen Kommunikationsnetzwerks auf der Basis von →P2P-Konzepten

IAM: (Identity and Access Management) →Prozesse, →Policies und Technologien zur Verwaltung von Benutzern (→Verzeichnisdienst) und deren →Authentifizierung zur Freigabe von →Zugriffen. Enthält i.d.R. nicht die →Autorisierung. Siehe →Identity Management

IBAN: (International Bank Account Number, ISO 13616) mit maximal 30 Stellen, enthält für die →Integrität 2 Stellen mit einer →Checksum und für D. und Ö die an sich durch die →BIC redundante Bankleitzahl und leider nicht ganz kompatiblen Ländercode (ISO 3166-1 alpha-2). Durch die Prüfsumme können Fehleingaben oder Tippfehler schon bei der Eingabe erkannt werden (wie auch bei →Kreditkarten) – alle kritischen nummerischen Identifikationen sollten solche Prüfungen enthalten. Verwaltet durch →SWIFT

IBE: (identity based encryption) →ID-based Cryptography

iBeacon: von →Apple entwickelte Technik für das →Tracking von Geräten in Räumen. Dafür werden kleine Geräte platziert, die mittels BLE (→Bluetooth Low Energy) Signale aussenden, die von entsprechenden →Apps erkannt werden. Auf diese Weise können z.B. Geschäfte Nachrichten an Personen senden,

die gerade das Geschäft betreten haben. Ebenso lassen sich aber auch Personen auf diese Weise innerhalb von entsprechend ausgerüsteten Gebäuden lokalisieren, z.B. Mitarbeiter über ihre Firmen-Smartphones

IBM: (International Business Machines Corporation) eine der wenigen noch existierenden Firmen aus der Frühzeit der IT, gegründet 1911 als Computing-Tabulating-Recording Company (CTR) und 1924 umbenannt in "International Business Machines". In den Anfängen entwickelte und verkaufte die Firma Lochkartenmaschinen, basierend auf den Patenten des Mitgründers Hollerith. Diese Lochkartensysteme wurden (über die IBM-Tochter Dehomag) im 3. Reich zur Vearbeitung der Volkszählungsdaten (mit dem Datenfeld Rasse) und zur Verwaltung der KZs eingesetzt.

Im 2. Weltkrieg wurden elektro-mechanische →Rechner gebaut und ab 1952 Rechner mit Vakuumröhren. IBM entwickelte sich in den 60iger Jahren zum dominierenden Anbieter von Rechnern für kommerzielle Zwecke (→Mainframes). Der Sager unter den Einkäufern für Groß-EDV war: "No one ever got fired for buying IBM."

Die Entwicklung des sog. IBM-PCs ermöglichte dem Unternehmen den Eintritt (und wohl auch das Überleben) in den Zeiten als Großrechner mehr und mehr durch kleinere System abgelöst wurden und die traditionellen Konkurrenten (BUNCH = Burroughs, UNIVAC, NCR, Control Data Corporation (CDC), Honeywell als Rechnerhersteller aus dem Markt verschwanden.

IBN: →Background Noise

ICA: (Intelligent Console Architecture, heute „Independent Computing Architecture") Protokoll zur effizienten Übertragung von Bildschirminhalten und Benutzereingaben. Erlaubt den Betrieb eines (meist) MS Windows-basierten Systems über entfernte Datenverbindungen. Von Firma →Citrix unter dem Schlagwort „Server Based Computing“ vermarktet. ICA ist auch mit Verschlüsselung verfügbar. Sicherheitsrelevant, da sich auf diese Weise Anwendungen leicht auch für externe Benutzer verfügbar machen lassen, ohne dass diese direkt in das Firmennetz müssen. Dies hat Vorteile, aber auch Risiken. Ähnlich zu anderen →Terminalserver-Implementationen, wie MS Terminal Server, →VNC und PC-Anywhere

ICANN: (Internet Corporation for Assigned Names and Numbers) Organisation zur Verwaltung der Adressen im →Internet. Siehe →UDRP, →DANE

ICAO: (International Civil Aviation Organization) Zivilflugbehörde, untersteht der UN. Ziel ist die Förderung des Zivilflugverkehrs. Macht auch Vorschläge zu Sicherheit, z.B. Einsatz von einheitlichen Passformaten, aktuell auf der Basis von →RFID und →Biometrie (→ePass). Siehe →PKD

ICAP: (intellectual capital) neues Schlagwort für das, was die →Informationssicherheit schützen muss: Die →Informationen in den Köpfen der Mitarbeiter plus die Geschäftsdaten auf jedem Speichermedium plus die Geschäftslogic, die in Skripten und Programmen implementiert ist

ICC: (International Chamber of Commerce, Internationale Handeskammer) eine Organisation zur Förderung des Handels. Kümmert sich auch um Fragen der →Wirtschaftskriminalität. http://www.icc-austria.org/

ICE: (In case of emergency) Vorschlag, im →Handy-→Adressbuch im Eintrag ICE (bzw. ICE1, ICE2, ….) die Nummer abzulegen, die im Falle eines →Notfalls zu verständigen ist

iCloud: Daten-Synchronisation und →Backup von Appe, genutzt auf →MaxOS und →iOS-Geräten. Die →Daten werden zwar verschlüsselt übertragen und gespeichert (außer den →E-Mails), die →Schlüssel sind jedoch unter Kontrolle von →Apple und stehen auch US-Behörden zur Verfügung

ICMP: (Internet Control Message Protocol) Teil der →IP-Protokollfamilie. Wird im Programm →Ping genutzt, um die Erreichbarkeit und Verfügbarkeit eines Rechners zu prüfen, bzw.→Traceroute, um zu prüfen, wie eine →Nachricht im Detail weitergeleitet wird. Kann auch zu Angriffen genutzt werden, („Ping of Death“)

ICMPv6: (Internet Control Message Protocol version 6) →Protocol mit dessen Hilfe ein →Rechner sich in einem →IPv6 Netz eine →IP-Adresse von einem →Router geben lassen kann. Dies fällt unter →SLAAC

ICQ: („I seek you“) - →Chat Programm für Kommunikation zu zweit oder in Gruppen. Kann auch für die Verteilung von →Malicious Content eingesetzt werden

ICS: (Industrial control system) Genereller Begriff für Industriesteuerungen, zu denen auch →SCADA-Systeme und →PLCs gehören. Solche Anlagen waren früher durch eine →Air gap von andere Firmennetzen getrennt, heute jedoch oft nicht mehr. Oft sind sie sogar im →Internet zu finden, und zwar entweder über normale →Suchmaschinen wie →Google oder über spezielle wie →Shodan. ICS sind ein wichtiges Ziel für →Cyberwar. Siehe auch →Stuxnet

ICS-CERT: spezialisierte →CERT für →ICS-Systeme

ICT: 1) Information and **C**ommunications **T**echnology, deutsch: IKT, die Gesamtheit von →Computer- und →Datenübertragungs-Technologien
2) (Image Constraint Token) →DRM-Verfahren bei →AACS, das die Auflösung des Outputs einer hochauflösenden DVD künstlich begrenzt, siehe → HDMI

ID3 Tag: Format für Zusatzinformationen (→Metadaten), die in Audiodateien des →MP3-Formats. Metadaten können ungewollt Informationen preisgeben

ID-based Cryptography: (Identity Based Cryptography, IBE) Verfahren im Rahmen von →Public Key Verschlüsselung, bei der der Public Key aus einem bekannten String, z.B. der E-Mail-Adresse geniert wird. Statt einer →CA als vertrauenswürdiger Erzeuger von Schlüsselpaaren haben wir eine Private Key Generator (PKG) genannte Stelle, die für jeden Nutzer einen zum bekannten public key passenden private key erzeugt

IDEA: (International Data Encryption Algorithm) 1990 in der Schweiz entwickeltes symmetrisches →Verschlüsselungsverfahren, gilt als sehr sicher. IDEA benutzt einen 128-bit Schlüssel und wurde in der ersten Version von →PGP verwendet

IDEF: (Intrusion Detection Exchange Format) Format für den Austausch von →Attack Pattern. → Intrusion Detection Working Group)

Identification: →Identifizierung

Identifizierung: Feststellung der Identität einer Person, z.B. durch Vorlage eines Ausweises oder Eingabe einer Benutzerkennung, d.h. einer vorher vergebenen Kennung. In der →Biometrie das Finden einer Person in einer Datenbank mit vielen Personen. Siehe →KYC

Identifizierung kann auch indirekt über die Identifizierung eines Geräts versucht werden, das mit dieser Person verbunden ist, z.B. die →IMEI des Telefons, dies ist jedoch keine wirklich sichere Identifizierung, da Geräte verloren oder gestohlen sein können, siehe →Fingerprinting. Siehe →FIDIS

Die →Verifizierung der Identität ist ein separater Vorgang, der →Authentifizierung genannt wird (z.B. durch Eingabe eines →Passworts, →PINs oder Nutzung eines privaten →Schlüssels einer Smartcard)

Auf Grund der Verlagerung vieler Dienste ins →Internet besteht ein sehr großer Bedarf an Identitätslösungen. So bietet z.B. Jumio 2014 die Verifizierung von 380 verschiedenen Ausweisen aus 105 Ländern an. Nutzer müssen die Ausweise mit einer →Smartphone Kamera fotografieren oder einscannen.

Identität: →Identifizierung

Identitätsmanagement: →Identity Management

Identity Fraud: →Identity Theft

Identity Management: (IDM) Verwaltung von Berechtigungen und →Authentifizierungsinformationen, heute oft auch als →IAM. Es wird zwischen enterprise-centric und user-centric unterschieden. Ersteres enhält User →Provisioning, aber auch den Approval Workflow zum Anlegen und Verwaltung der Accounts. →AAA, →Verzeichnisdienst. User-centric beschäftigt sich mit Authentisierungsmechanismen im →Internet. Ziel ist dabei, dass der Nutzer die Kontrolle über seine →Daten behält. Aktiv sind hier vor allem →PRIME und →Liberty Alliance. Federated IDM erlaubt dabei, dass Authentisierungen zwischen Systemen kommuniziert werden können, was →Single Sign-On erlaubt. Siehe →IGF, →CardSpace, →PEAP

Identity Theft: (engl. Identitätsdiebstahl) betrügerisches Auftreten als andere Person, real oder erfunden.

„New Account Creation“ ist speziell in den USA ein großes Problem mangels fehlender Personalausweise. Die →SSN wird dort oft als →Authentisierung, z.B. beim Beantragen eines Kredits, verwendet. Auch wenn die Bank in einem solchen Fall den direkten finanziellen Schaden trägt, so entstehen für die Opfer doch erhebliche Unannehmlichkeiten durch Verlust der →Kreditwürdigkeit (→Kreditschutz, →fraud alert, →credit freeze). 2014 gibt es Dienste, die gegen einige Hundert $ vollständige gefälschte Dokumentation anbieten, vom Führerschein, Geburtsurkunde bis zu einer Stromrechnung die für den Nachweis des festen Wohnsitzes gilt.

„Account Takover“ ist der zweite Fall: die Nutzung einer bestehenden →Kredit- oder →Bankomatkarte oder Bankkontos. Auch europäische Karten- und Account-Information (mit →Passwort oder →PIN), →eBay-Accounts mit Passworten u.ä. werden auf entsprechenden Webservern angeboten. Wenn es auch in Europa schwer ist, einen Bankkredit ohne Ausweis zu bekommen, so entstehen trotzdem für den Betroffenen erhebliche negative Auswirkungen. Siehe →Carding, →Phishing, →Data Leakage

Identity Provider: (IdP) Siehe →Federation Services

IdenTrus: weltweite Bankeninitiative zur Standardisierung von →PKI in der Bankenwelt. Hierbei geht es mehr um die Vereinheitlichung der rechtlichen Grundlagen, als um technische Fragen. Ziel ist, dass die Zertifikate der Partner-Banken untereinander frei anerkannt werden. Heute (2006) auch als →CA aktiv. http://www.identrus.com/

IDFA: (IDentifier for Advertisers, auch IFA) Ersatz für die →UDID die ab →iOS6 nicht mehr für Device-→Tracking genutzt werden darf. Auch IDFA ist eine Kennung die an das

Gerät gebunden ist und dadurch eine Wiedererkennung von Benutzers auch in unterschiedlichen →Apps erlaubt. Es wird ähnlich wie →Cookies implementiert, d.h. der Benutzer kann diese Funktionalität abschalten, Default ist jedoch aktiviert und die Option des Abschaltens ist gut versteckt und verwirrend bezeichnet. Die IDFA kann nicht nur von Apps ausgelesen werden, sondern wird auch vom →Browser gesendet. Das Äquivalent bei →Android ist →Android Advertising ID

IDL: (interface definition language) beschreibt in (computer-)sprach-unabhängiger Form, wie eine bestimmte Software aufgerufen werden kann. Ist relevant, wenn es um Aufrufe zwischen verschiedenen Sprachen und/oder Architekturen geht. IDL ist z.B. ein Teil von →CORBA und →SOAP

IDM: (Identity Management) Mechanismen der →Identifizierung von Personen, siehe →Authentisierung

IDN: (Internationalized Domain Names) →Domain Namen mit Zeichen, die nicht in →ASCII enthalten sind, z.B. chinesische, kyrillische oder arabische Zeichen. Wird zum Sicherheitsproblem, wenn gleich aussehende kyrillische Zeichen zum Darstellen einer →spoof →Website im Rahmen von →Phishing verwendet werden. Siehe →DNS

IdP: Identity Provider bei →SAML und →OpenID. Siehe →Federation Services

IDS: →Intrusion Detection System

IEEE: (Institute of Electrical and Electronics Engineers, gesprochen ai-triple-ii): 1884 gegründete US-amerikanische Organisation, die heute Standards für die Computer und elektronische Industrie erlässt. Am bekanntesten sind die IEEE 802 Standards für →LAN Technologien

IEEE 802 Standards: (siehe auch →IEEE).

Standards für →LAN Technologie, z.B.

801.1q →QoS

802.1x →NAC, Network Access Control

802.2, OSI-→Schichtenmodell für Netzwerke

802.3, die Basis für →Ethernet

802.5 →Token Ring

802.11, 15, 16 →Wireless Networks

IKE: (Internet →Key Exchange, RFC 2409), Teil des →IPsec Protokolls

IETF: (Internet Engineering Task Force) Standardisierungsgremium für →Internet-Technologien, beschäftigt sich mit Detailfragen der Implementierung und arbeitet durch Veröffentlichung von →RFCs

IFA: →IDFA

IFF: (Identification friend or foe) kryptografisches System zur positiven Identifizierung von zugehörigen Geräten, eingesetzt vor allem beim Militär. Verwendet werden →Challenge-Response Verfahren

iFrame: (InlineFrame) →HTML-Element, das Inhalte von anderen →Websites in eine →Webseite eingliedert. Wird z.B. für Werbung genutzt, aber auch für die Verbreitung von →Malware. Dafür wird eine Minimalgröße von 1x1 pixel genutzt (→Web Bug) und durch geeignete HTML-Anweisungen die Schadsoftware geladen (→Drive-by →Infektion). →JavaScript in einem eingebundenen iFrame kann Inhalte auf der Hauptseite, z.B. →Hyperlinks verändern

IFRS: (International Financial Reporting Standard) →Rechnungslegungvorschrift für Aktiengesellschaften, die sich international immer stärker gegen →US-GAAP durchsetzt nachdem sie jetzt auch von den US-Behörden akzeptiert wird. Im deutschspr.Raum →GoB

IGF: 1) (Identity →Governance Framework) von →Oracle vorgeschlagener Standard, um die Übertragung von persönlichen Daten wie Kreditkartennummern zwischen verschiedenen Systemen besser nachvollziehen lassen. Dies erleichtert →Compliance-Anforderungen wie →SOX, →Gramm-Leach-Bliley oder die →European Data Protection Initiative. Grundlage sind →Liberty Alliance und →OASIS. Siehe →Identity Management

2) (Internet →Governance Forum) Diskussionsplattform für →Internet-Themen, tagt einmal pro Jahr. Themen sind z.B. Internationalisierung der Kontrolle des Internets

IGIT: →Governance

IGL: (Intel loss-gain) in der Spionage-Community das Abwägen zwischen (Zer)stören eines „feindlichen" Geräts oder Aktivität versus dem Gewinnen von Informationen durch Abhören desselben. Ein ähnlicher Gain-loss Effekt tritt bei starker Verschlüsselung ein: die Verteidigung der Vertraulichkeit wird höher, aber die Geheimdienste können nicht mehr mithören. Siehe auch →Crypto wars

IKE: (Internet Key Exchange) →IPsec

IKS: (internes Kontrollsystem) systematische organisatorische →Maßnahmen (→controls) und Kontrollen (checks) zur Einhaltung von Richtlinien und zur Abwehr von Schäden, siehe →SOX

IKT: (Informations- und Kommunikationstechnologie) →ICT

IM: →Messaging Dienste

Image Tag: genutzt in →Social Network, in digitalen →Kameras und Photosharing →Websites. →Benutzer können Bildern Namen von Personen oder andere Attribute zuordnen. Über →Face Recognition kann heute bereits vielfach diese Person automatisiert in Sammlungen von Fotos erkannt und damit automatisch „getaggt" werden. Stand der Technik 2011 ist, dass diese Funktionalität in Fotosharing- und →Social Networking-→Websites,

angeboten wird, ebenso als integrierte Funktion in digitalen Kameras. Technologisch möglich wäre auch ein Fotografieren einer fremden Person und ein automatisiertes Durchsuchen von Foto-Sammlungen wie Social Network-→Profilen. Da dadurch ein personen-bezogenes Objekt außerhalb der Kontrolle des Betroffenen entsteht das die →Privatsphäre verletzen kann wird dies derzeit nicht angeboten

IMAP: (Internet Message Access Protocol) Verfahren mit dessen Hilfe ein Anwender auf seine →Mailbox zugreifen kann, um →E-Mails abzurufen. Dabei wird im Gegensatz zum →POP3-Protokoll zuerst nur die Header Information übertragen, so dass gezielt einzelne E-Mails abgerufen werden können

IMD: (implantable medical device) Medizinische Geräte wie Herzschrittmacher, Insulinpumpen, u.ä. die in den Körper des Patienten implantiert werden und dann über drahtlose Verbindungen justiert werden. Dabei wurde generell auf Sicherheitsmaßnahmen wie →Authentisierung verzichten, u.a. im schnelle Hilfe nicht zu behindern. Es konnten →Angriffe gegen diese Geräte demonstriert werden. Siehe →Medizinische Geräte

IMEI: (International Mobile Equipment Identity) eindeutige, interne Kennung jedes →Handys. Kann über die Sequenz *#06# auf jedem Handy angezeigt werden. Kann im Gegensatz zum →SIM von einem Dieb nicht ausgetauscht werden. Wird bei einem Telefonat zum Service-Provider übertragen und könnte daher zum Sperren von gestohlenen Handys benutzt werden. Diesen Dienst bieten jedoch leider nur wenige Provider an. Die IMEI kann, wie auch die →IMSI und →MSISDN zur →Identifizierung von Mobilfunknutzer eingesetzt werden. Siehe →Fingerprinting

Impact: in der →Informationssicherheit: Ausmaß der Auswirkungen eines Sicherheits-→vorfalls (→Incident)

Impersonation Attack: alle →Angriffe zur Erlangung von →Zugriffs-Legitimierungen, z.B. →Phishing, →Keylogger, u.ä.

Implant: 1) in der Medizin →IMD

2) Im Rahmen der Leaks von →Edward Snowden wird bekannt, dass die →NSA mit ihrer →TAO-Abteilung seit Beginn des Jahrtausends extrem fortgeschrittene →Malware entwickelt, die sie Implants nennen. Diese Implants stehen nicht nur für Endgeräte wie →PCs und →Smartphones zur Verfügung, sondern auch für Netzwerkkomponenten wie →Router die für ein flächendeckendes Abgreifen von Datenströmen geeignet sind.

Dabei werden als passive Implants solche bezeichnet die auf →Layer 1 und →Layer 2 des Netzwerks Datenströme mitschneiden, z.B. alles was über einen →Fibre-Strang fließt.

Active Implants sind in der Lage, eine Filterung auf Grundlage von Dateninhalten durchzühren und nur bestimmte Inhalte auszuleiten.

Auch für →Firmware, wie z.B. →BIOS und für →Magnetplatten stehen Implants zur Verfügung.

IMS: (→IP Multimedia Subsystem)

IMSI: (International Mobile Subscriber Identity) interne Kennung eines →SIM. Diese wird vom Mobilfunkprovider mit der →MSISDN, der eigentlichen Telefonnummer verknüpft. Diese beiden Werte und auch die →IMEI können zur →Identifizierung von Mobilfunknutzer eingesetzt werden

IMSI-Catcher: →Angriff auf →Handys, täuscht eine Handy-Funkzelle vor. Alle aktiven →GSM-Handys im Umkreis dieser Funkzelle melden sich dort an. Kann für einen →Lauschangriff oder →DoS genutzt werden. Siehe auch http://sicherheitskultur.at/abhoeren.htm

In-band: Übertragung von Kontroll-, Steuerungs- oder →Authentisierungsinformationen im Datenkanal, Gegensatz: →Out-of-band

Incident: (Vorfall)

1) nach →ITIL eine Störung, d.h. ein Ereignis, das nicht zum standardmäßigen Betrieb eines Services gehört und das tatsächlich oder potentiell eine Unterbrechung oder eine Minderung der Service-→Qualität verursacht. Incidents werden nach ITIL meist vom →Service Desk entgegengenommen. Grund kann sein:

- Anwendung nicht verfügbar oder in einem Fehlerzustand
- Hardware-Ausfall oder eingeschränkte Benutzung
- Service Request zur Information oder Bitte um Unterstützung

Incidents können aber auch auf Grund von →Systemüberwachungen initiiert werden.

2) **Security Incident:** ein schwerwiegender Sicherheitsvorfall der nach den Prozessen des „Security Incident Handbooks“ abgehandelt wird (evtl. →Forensics), mit einer möglichen Eskalation zum →Krisenstab

Incident Management: nach →ITIL die →Prozesse rund um den →Service Desk, wo Störungsmeldungen entgegen genommen werden. Im Rahmen des Incident Managements werden keine Fehler behoben, sondern bestenfalls Work-Arounds angeboten. Die Fehleranalyse findet im Rahmen des →Problem Managements statt. Siehe →CSIRT

INDECT: (Intelligent information system supporting observation, searching and detection for security of citizens in urban environment) von der EU finanziertes, sehr umstrittenes Projekt, das alle bestehenden Überwachungstechnologien zu einem universellen Überwachungsinstrument einer proaktiven Polizeiarbeit bündeln soll. Das Projekt wird von Datenschützern stark kritisiert

Indicator of Compromise: (IOC) im Rahmen einer →forensischen Untersuchung einer →Angriffs auf IT-Systeme die bei der Arbeit gefundenen Spuren. Sie bestimmen, ob als Ergebnis eine →Attribution des Angreifers vorgenommen werden kann. Solche IOCs fließen dann als Trigger in Systeme ein, die solche Angriffe (z.B. →APTs) erkennen können sollen.

Es werden atomic, behavioural und computed IOCs unterschieden. Atomic IOCs sind .z.B. externe →IP-Adressen mit denen gefundene Schadsoftware (z.B. ein RAT) kommuniziert hat (gefunden in einem →Log), deren →domain names oder →E-Mail-Adressen von →Phishing Mails. Computed IOCs sind z.B. →Hash-Werte von gefundener Schadsoftware. Behavioural IOCs sind z.B. die Angriffswege wie →Waterhole Attacks, Phishing Mails oder unauthorisierte Verbindungen von außen zu internen Systemen (gefunden in Logs)

Industriespionage: →Wirtschaftsspionage

IEController: →Sandbox-Technologie zur Absicherung von →Webbrowsern und anderen →Programmen. Siehe →Active Content

Industrie 4.0: Schlagwort, das auf die Forschungsunion der deutschen Bundesregierung und ein gleichnamiges Projekt in der Hightech-Strategie der Bundesregierung zurückgeht. Es geht dabei um die Erweiterung der computerunterstützten Produktion um → Internet of Things. D.h. jede technische Komponente ist vernetzt und kann mit jeder anderen kommunizieren. Dies wirft erhebliche Sicherheitsprobleme auf, da hierfür neue →Protokolle entwickelt werden müssen, die aber zumeist (auch auf Grund geringer Prozessorleistung) selten sichere →Authentisierung und →Verschlüsselung unterstützen. Eines der vorgeschlagenen →Protokolle für M2M ist →OPC UA

Infektion: in der IT: Installation von →Schadsoftware auf einem →Rechner. Infektionen sind ein Beispiel für →Externalität: der Gewinn für den Angreifer ist in der Regeln viel geringer als die Kosten die dem Nutzer für die Bereinigung der Infektion entstehen (bei resistenten →root kits mit →MBR-Infektion oft Kauf einer →Magnetplatte oder gar eines PCs, Nutzung externer Hilfe, Zeitaufwand > 8 Stunden). Denn die durchschnittliche Nutzungsdauer eines infizierten PCs für den Angreifer liegt meist nur bei wenigen Tagen, danach wird die Infektion i.d.Regel entdeckt. Siehe →Drive-by, →Hacker

InfoCard: →CardSpace

InfraGard: Programm des FBIs: US-Firmen und FBI tauschen Informationen aus. http://www.infragard.net/

InfoCard: →CardSpace

Information Custodian: →Informationstreuhänder

Informationelle Selbstbestimmung: durch das sog. Volkszählungsurteil des Bundesverfassungsgericht in D. 1983 etabliertes Recht der Kontrolle an den eigenen Daten. "Dies (Verlust der Privatsphäre) würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist." – Im Gegensatz dazu steht der (falsche) Satz: →Nothing to hide. https://de.wikipedia.org/wiki/Informationelle_Selbstbestimmung

Informationen: entstehen aus →Daten, wenn diese für eine Zielerreichung genutzt werden (können)

Information Owner: Informationsbesitzer oder Informationsverantwortlicher. Person, die für eine definierte Information oder ein System bezüglich ihrer Verwendung und ihres Schutzes in Bezug auf →Vertraulichkeit, →Integrität, →Verfügbarkeit, →Authentizität und →Verbindlichkeit die Verantwortung trägt. Gegenpart zum →Informationstreuhänder

Informationsaustausch: →Datenaustausch

Information Security Policy: Dokument, mit dem das Management Vorgaben und Richtlinien für die Implementierung von →Informationssicherheit gibt. Auch →Sicherheitskonzept oder →Sicherheitspolicy (Sicherheitspolitik) genannt. Zu unterscheiden von → IT Security Policy, die sich nur auf die IT-Systeme bezieht, d.h. z.B. Vertraulichkeitsverlust durch unachtsame Gespräche ausklammert

Informationssicherheit: lt. ISO 17799 die Sicherstellung von →Vertraulichkeit, →Integrität und →Verfügbarkeit von →Informationen. Ein Zustand, in dem die unberechtigte Ressourcennutzung erschwert und möglichst erkannt wird. Ziel ist, dass keine unautorisierte Informationsveränderung oder -gewinnung erfolgen kann. Zusätzlich ist auch Konformatität mit Gesetzen und Vorschriften notwendig. →IT-Sicherheit ist eine Untermenge der Informationssicherheit.

Information Security wird von Geheimdiensten oft als Titel verwendet um →Überwachungsmaßnahmen ihrer Bürger zu implementieren. Siehe →PESTEL

Informationssicherheitsbeauftragter: übernimmt die Gesamtverantwortung für die Entwicklung und Implementierung von →Informationssicherheit. Siehe →CISO

Informationssicherheits-Managementsystem: (ISMS) Teil des gesamten Managementsystems, der basierend auf einem Geschäftsrisikoansatz die →Informationssicherheit etabliert, implementiert, betreibt, überwacht, prüft, wartet und verbessert

Informationstechnik: alle technischen Mittel,

die der maschinellen oder maschinell unterstützten Erzeugung, Speicherung, Verarbeitung oder Übertragung von Informationen dienen; alle dazu erforderlichen Komponenten, einschließlich der Programme und der technischen Voraussetzungen für die Kommunikation. International und in der Bundesverwaltung gängige Bezeichnung für technikunterstützte Informationsverarbeitung. Synonym: Informations- und Kommunikationstechnik (IuK), technikunterstützte Informationsverarbeitung (TUI). Frühere Bezeichnungen: EDV, ADV, DV

Informationstreuhänder: (engl. information custodian) Durchführender der Datenverarbeitung (entweder als →Outsourcer oder als interne IT), verantwortlich für die Wahrung der →Vertraulichkeit, →Integrität, →Verfügbarkeit, →Authentizität und →Verbindlichkeit definierter Informationen, in der Regel durch den →Information Owner über →SLA beauftragt

Informationsweiterverwendungsgesetz: (→IWG)

Information Warfare: →Cyberwar

Ingress Filtering: das Filtern von Datenverkehr auf dem Weg nach innen um Angriffe von außen zu verhindern. Siehe →egress filtering

Impact: (engl. Auswirkung) Ergebnis, bzw. Ausmaß der Auswirkungen eines Security →Incidents

Instagram: →Social Network das ursprünglich auf Foto- und Videosharing fokusiert war aber wegen ihres großen Erfolgs speziell bei Jugendlichen bereits 2 Jahre nach Bestehen 2012 von →Facebook (jetzt →Meta) aufgekauft wurde. Es gehört zu den →Blogging-Diensten. Das Integrieren der →Daten und →Benutzer mit den anderen Facebook-Diensten wird als problematisch gesehen. Wird weiterhin als →walled garden betrieben, d.h. nicht mal die Nutzer von Facebook, Instagram und Whatsapp können miteinander kommunizieren

Instant Messaging: →Messaging

Instruction: in der IT: →Computerbefehl

Integer: Festkommazahl →Zahlendarstellung

Integrität: Sicherstellen der Vollständigkeit und Unversehrtheit der von →Daten und der verwendeten →Prozesse (Def. →ISO 17799). siehe auch →Authentizität, →Checksum, http://sicherheitskultur.at/Datenschrott.htm

Integrity Level: Sicherheitsattribute von →Prozessen in →Vista (und späteren Windows-Systemen) (auch Mandatory Integrity Control). Wird genutzt, damit der Internet Explorer auf niedrigerer Priorität läuft als durch den →DACL des →Benutzers vorgegeben

Intellectual property: (IP) Rechte eines Autors oder eines Unternehmens an einem nicht-materiellen Werk (Kunstwerk, Musikstück, Film, Buch, oder auch Computer→Programm). Solche Inhalte sind durch die Möglichkeit der digitalen Kopie ohne Qualitätsverluste nur sehr schwer zu schützen. Siehe →Copyright, →Urheberrecht, →Kopierschutz, →DRM, →Raubkopie, →ACTA, →PRO-IP, →DMCA. http://www.ip-watch.org/

Intelligence explosion: (auch →singularity) bei →artificial intelligence der Moment in dem die intelligenten Systeme sich (oder die Nachfolgegeneration) immer wieder selbst verbessern so dass es zu einer Hyper-Intelligenz kommt, deren Ergebnisse (z.B. in der Physik, z.B. auch der Waffentechnik, Finanzmarktoptimierung, etc.) kein Mensch mehr nachvollziehen kann (siehe Szenario des Filmes „Matrix“). Solche Szenarien sollen u.a. durch Forschungen zu Sicherheitsmaßnahmen ähnlich zu den (theoretischen) →Robotergesetzen verhindert werden. Die Wissenschaftswelt ist geteilt zwischen: „das kann eh nicht passieren“ und „das wird sehr bald passieren“. Siehe auch →Meme für die Weitergabe von „Ideen“ von Maschine zu Maschine in der Form vom Temes. Ausführlichste Diskussion in Nick Bostrom: Superintelligenz. Siehe auch https://en.wikipedia.org/wiki/Philosophy_of_artificial_intelligence

Internet: weltumspannendes Datennetz auf Basis des →IP Protokolls, in dem alle angeschlossenen Geräte durch eindeutige →IP-Adressen identifiziert sind. Die heutigen Probleme der IT- und →Informationssicherheit sind erst entstanden, seit das →Internet eine globale Verknüpfung und damit Erreichbarkeit aller angeschlossenen →Rechner für jeden potentiellen Angreifer ermöglicht. Weder Sicherheit noch →Privatsphäre waren Designanforderung, sondern nur Überlebensfähigkeit im Fall eines Kernwaffenangriffs. Diese wird erreicht durch flexibles →Routing über alternative (redundante) Wege und die Zerlegung einer Nachricht in viele Daten→pakete.

Internet und →Web werden oft synonmym genutzt, aber das Internet ist nur das Transportmedium für viele Dienste, eines davon ist Web, andere sind →E-Mail, →Messaging, →Telephonie wie →Skype, etc. →Suchmaschinen durchsuchen das Web, nicht das Internet. Siehe →Web 2.0, →net neutrality, →Internet of Things

Internet-Banking: →e-Banking

Internet im Koffer: Projekt, bei dem es Regierungsgegnern ermöglicht werden soll, unabhängig von den offiziellen Stellen →Zugang zum →Internet zu bekommen. Grundlagen sind z.B. →Mesh Routing zwischen →Handys und Satellitenlink aus dem Koffer. Wird u.a. von der US-Regierung unterstützt

Internetcafé: öffentliche Einrichtung, wo gegen Entgelt auf das →Internet zugegriffen werden kann (→surfen). Sicherheitsrelevant, da der Kunde nicht kontrollieren kann, ob nicht über →Keylogger und ähnliche →Malware

vertrauliche Informationen gesammelt werden. Ermöglicht auch Nutzern die keinen PC besitzen die Teilnahme am Internet, ebenso ermöglicht es eine anonymere Nutzung als der eigene →PC (oder →Smartphone), die über ihre →IP-Adresse sehr leicht zu identifizieren sind, siehe →Vorratsdatenspeicherung. Wird deswegen für legitime und für illegitime Zwecke verwendet. Siehe auch →Hotspot

Internet Governance Forum: →IGF

Internet of Things: (IoT) Schlagwort das bezeichnet, dass in der Zukunft fast alle Geräte, auch die mechanischen Haushaltsgeräte wie Waschmaschine und Kühlschrank, →Zugang zum →Internet haben werden. Dies wird entweder direkt mittels →IPv6 sein oder indirekt über eine →WLAN Verbindung zum →Router in der Wohnung. Die Nutzung der Geräte erfolgt dann z.B. mittels →Smartphone →Apps und kann aus der Ferne geschehen.

Problematisch in Bezug auf →Privatsphäre und digitale und physische Sicherheit. Die bisherige Erfahrung zeigt, dass die Entwickler von Geräten sehr schlecht darin sind, diese gegen unbefugte Nutzung zu sichern. Beispiele sind die Manipulation von →Autos, →medizinischen Geräten (→IMDs) wie Herzschrittmachern, Insulinpumpen, u.ä. bei denen gravierende Sicherheitslücken gezeigt wurden, ebenso →Smartmeter. Auch für Steuerungen von Heizungen, Beleuchtung, etc konnten unbefugte Zugriffe demonstriert werden.

Zusätzlich verraten natürlich alle diese Dinge über ihren Status Informationen über den Besitzer, oder dringen wie →Webcams direkt in die Privatsphäre ein wenn die Geräte öffentlich erreichbar sind.

Ein weiterer Effekt wird die vorzeitige Veralterung (→Obsoleszenz) die dann eintritt, wenn das Gerät zwar noch einwandfrei funktioniert (bei Waschmaschinen und Kühlschränken sollten das 10 Jahre sein), aber eine veraltete →Betriebssystemversion (→embedded System) enthält und daher keine Sicherheits→patches mehr bekommen kann und dadurch verwundbar wird und (an sich) ersetzt gehört (Beispiel 2014, →Windows XP erhält keine Sicherheitspatches mehr, aber deren Umstieg auf Windows 7 oft an der Nicht-Verfügbarkeit von Geräte-Treibern scheitert). Daher werden viele Geräte entweder vorzeitig entsorgt oder von den Netzen getrennt werden müssen, sofern dann weiterhin eine Nutzung möglich ist. Siehe auch →Home Automation

http://sicherheitskultur.at/notizen_1_14.htm#things

Internet Radio: Radiosender, der nicht über Funkwellen, sondern über das →Internet sendet. Die Nutzung durch Mitarbeiter kann für Unternehmen einen erheblichen Bandbreitenverlust darstellen. Siehe →Podcast

Internet Research Agency: (IRA) →Trollfabrik

Interpretation: das Ausführen von →Programmen in →Laufzeitumgebungen ohne dass vorher eine Umwandlung aus der →Programmiersprache in den Befehlsatz stattgefunden hat (z.B. →Python oder →JavaScript). Dies erlaubt hohe Flexibilität, z.B. bei den Datentypen, ist aber langsam. Eine Lösung kann dann ein →JIT-Compiler sein

Intranet: im Gegensatz zum →Internet ist dies ein internes Firmennetz, das ebenfalls auf Internet-Technologien (z.B. →TCP/IP, ein oder mehreren →Webservern) besteht und auf diese Weise interne Informationen oder Dienste anbietet

Intruder: Person, die unberechtigt Computer Services nutzt, bzw. in ein Netz eindringt. →Intrusion Detection System

Intrusion Detection System: (IDS) im Gegensatz zur →Firewall, die den Datenverkehr filtert, lauscht ein IDS im internen Netz oder auf Servern nach unerwarteten Ereignissen. Dies geschieht z.B. durch das Erkennen von →Attack Pattern, die auf einen bekannten Typ von →Hackerangriff hindeuten. Auch können diese Systeme mit Hilfe der →Firewall bei einem →dDoS-Angriff gezielt die angreifenden Systeme sperren. Siehe →Intrusion Prevention System, →NBAD, →IPS, →NIPS, →HIPS

Intrusion Detection Working Group: (IDWG) Industriegremium, erstellt u.a. Intrusion Detection Exchange Format (→IDEF) für den Austausch von →Attack Pattern

Intrusion Prevention System: (IPS) Weiterentwicklung des →IDS dahingehend, dass →Angriffe nicht nur erkannt, sondern auch aktiv verhindert werden (→Prävention), z.B. durch Ändern der →Firewall-Regeln zum Blocken eines gerade stattfindenden →Angriffs. Zumeist in der Form →NIPS oder →HIPS

Intrusion Prevention Management System: Weiterentwicklung des →IPS-Konzepts. Enthält ein →GUI zur Darstellung, Korrelation von Ereignissen aus verschiedenen Quellen, Integration mit →Vulnerability Management und Reporting

Intrusion Testing: →Penetration Testing

IOC: →Indicator of Compromise

IoT: (→Internet of Things)

iOS: →Betriebssystem des →iPhones und →iPads, beruhend auf →Mac OS X. Es werden zahlreiche Verwundbarkeiten gefunden, obwohl vergleichsweise gute Sicherheitskonzepte implementiert sind (→Sandbox für →Apps, →Verschlüsselung von →Daten, restriktiver →Market für Apps, etc.). Allerdings laufen, im Gegensatz zu →Android und Windows 8 →Metro alle →Apps unter demselben →User Account. Siehe auch →App Store, →IDFA

IP: 1) →intellectual property

3) →IP Protocol

iPad: sehr erfolgreicher Tablett-→PC von Apple, verwendet das →Betriebssystem →iOS und ist weitgehend kompatibel mit dem →iPhone

IP Adresse: Schema von 4 Zahlen, mit diesen Hilfe alle im →Internet sichtbaren Geräte eindeutig identifiziert sind. Über den →DNS-Service werden →Domain Namen in diese Adressen umgesetzt, z.B. 129.192.13.5. Auf Grund der Beschränkung auf die Zahlen von 1 bis 255 für jede der Stellen, ist die Zahl der Adressen heute nicht mehr ausreichend. Eine oft eingesetzte Lösung ist →NAT und die neue Protokollversion →IPv6. Siehe →Private Address Space

IP-Hijacking: →Angriff mittels →BGP, bei der der Angreifer „verkündet", dass er der beste Link zu einer bestimmten →Website ist. Alle anderen →ISPs schicken dann den Datenverkehr dort hin. Dort kann er verschwinden, oder abgehört werden und über einen anderen Weg doch zugestellt werden. Auf diese Weise lassen sich auch Verbindungen zu sehr entfernten Websites abhören

iPhone: seit 2007 sehr erfolgreiches →Smartphone von →Apple, verwendet das →Betriebssystems →iOS und ist weitgehend kompatibel mit dem →iPad und →iPod Touch. Durch die sehr stark abgeschottete Infrastruktur (→Apps nur vom iTunes →App Store, zwangsweise Installation von Sicherheits-→Patches) wird ein Sicherheitsvorteil gegenüber →Android Geräten erreicht. Die Nutzung von iTunes für die →Datensicherung wirft jedoch →Privatsphäre-Probleme auf, da große Teile der →Daten unverschlüsselt gespeichert werden

IPMI: (Intelligent Platform Management Interface) standardisiertes Interface, dessen Hardware (Baseboard Management Controller, BMC) direkt auf dem →Motherboad eines →Rechners sitzt und für Wartungszwecke eingesetzt wird. Hersteller können (zumeist sogar bei ausgeschaltetem Zustand) auf diese Weise auf alle Komponenten eines Rechners zugreifen, auch über Netzwerke. Kann daher auch zu Sicherheitsverletzungen führen, da in der Regel keinerlei Schutzmaßnahmen implementiert sind und die →Passworte oft sehr weit bekannt sind. 2015 werden →Verwundbarkeiten diskutiert und rund 2.400 IPMI-Management-Board sind in Österreich über das Internet erreichbar

IP Multimedia Subsystem: (IMS) Sammlung von Spezifikationen des 3rd Generation Partnership Project (3GPP) mit Ziel eines standardisierten →Zugriffs auf Dienste wie →VoIP, Teleconferencing, etc. von Drahtlosnetzen unterschiedlicher Technologien. Ein wichtiger Bestandteil ist →SIP und →Generic Access Network

iPod: →MP3-Player von Apple mit großem Marktanteil. Sicherheitsrelevant wenn im Businesscontext eingesetzt, da über die →USB-Schnittstelle auch →Dateien aus Firmennetzen gewollt oder ungewollt entfernt werden können. Der iPod wurde ab 2007 immer stärker durch den **iPod Touch** verdrängt, der im Gegensatz zum iPod mit dem →Betriebssystem →iOS läuft und dadurch quasi ein →Smartphone ohne Telefonschnittstelle und ohne →GPS-Modul ist. Über →WLAN oder →Bluetooth kann ein solches Gerät trotzdem fast alle →Internet-Funktionalitäten nutzen, z.B. →Apps ausführen

IP-Paket: Datenblock im →IP-Protocol, der die Grundlage des Datenverkehrs bei →IP-Verbindungen darstellt

IP Phone: erlaubt die Nutzung von →VoIP, entweder in der Form von Hardware mit geeigneter Funktionalität oder als →Softphone

IP Protocol: Übertragungsprotokoll auf dem das →Internet basiert. Anwendungen benutzen entweder →TCP/IP oder →UDP/IP. Datenpakete werden mit Hilfe von →Routern zwischen Sender und Empfänger transportiert. Siehe auch →Fragmentierung, →IP Traceback

IPR: Intellectual Property Right. Entspricht vom Konzept her dem →Urheberrecht, geht jedoch von einem anderen Ansatz aus

IPS: →Intrusion Prevention System

IPsec: (Internet Protocol Security) standardisiertes Protokoll für den Aufbau von →VPN-Verbindungen. Nur für →IP-basierte Protokolle nutzbar. Enthält die Standards RFC 2401–Sicherheitsarchitektur für das Internetprotokoll, RFC 2402 -Authentication Header, RFC 2406–Encapsulating Security Payload, RFC 2407-IPsec Domain of Interpretation (IPsec DoI), RFC 2408-Internet Security Association and Key Management Protocol (ISAKMP), RFC 2409-Internet →Key Exchange (IKE). Der Vorteil und Nachteil von IPsec gegenüber →SSL/VPN ist, dass beliebiger IP-Datenverkehr zwischen den verbundenen System oder Netze möglich ist, d.h. auch →Angriffe. Vermutlich 2014 für die →NSA nur durch Diebstahl von Schlüsseln knackbar, siehe →TAO.

IPsec-VPN: Virtual Privat Network (VPN) via →IPsec verbindet zwei →Netzwerke oder einen →Computer mit einem Netzwerk und ermöglicht sicheren Datenverkehr über öffentliche Verbindungen (beispielsweise →Internet). Mit Hilfe von Chiffrier- und Authentifizierungstechniken werden vertrauliche Daten abhör- und manipulationssicher ausgetauscht. Zum Schutz der Datenübertragung gibt es ein sogenanntes Tunneling-Protokoll (→VPN-Tunnel), das die Daten ver- bzw. entschlüsselt und die →Authentisierung sicherstellt. Siehe auch →VPN-Dienste

IP-Spoofing: →Address Spoofing

IP TRACEBACK: von →NSA und der chin. Regierung initiiertes Projekt um die Möglichkeiten der →Anomymität im →Internet weiter einzuschränken

iPad: erfolgreiche Version eines →Tablett-Computers von →Apple

IPv4: Traditionelle Version des →IP Protocols, das durch →IPv6 ergänzt oder schon lange abgelöst werden soll. Wird hauptsächlich in Regionen verwendet, in denen IPv4-Adressen knapp sind, z.B. Asien

IPv6: Neue Version des →IP Protocols, das eine ganze Reihe von Problemen der alten Implementierung behebt oder vermeidet, z.B. die Knappheit der Adressen (siehe →NAT) und der fehlende Quality of Service (→QoS) und eine ganze Reihe von neuen Sicherheitsproblemen einführt. Dazu gehört, dass →Computer, die innerhalb eines Firmennetzes stehen und bei denen IPv6 nicht gesperrt ist, oft an der Firmen-→Firewall vorbei ins →Internet kommunizieren können. →Websites die IPv6-Daten nicht selbst empfangen können sondern nur über Gateway/→Proxy verlieren die Informationen über die originäre IPv6-Adresse, bzw. müssen für →SSL-Verkehr ein eigenes SSL-→Zertifikat implementieren. Siehe →ISATAP, →Teredo, →ICMPv6, →DHCPv6, →NDP

IRC: (Internet Relay Chat) ursprüngliches →Chat-, bzw. →Messaging System. Benutzer treffen sich in Channels, meist organisiert nach Interessensgruppen oder in privaten Sessions. Auch in diesem System kann →Malicious Content verteilt werden. Sie werden auch sehr oft zum Steuern von →Botnets verwendet. →ICQ, →Messaging

IrDA: (Infrared Data Association) definiert ein Kommunikationsprotokoll für infrarote Schnittstellen, d.h. →Handys und →PDA. Siehe →OBEX

Iris-Erkennung: die Iris ist die äußere Regenbogenhaut auf dem Auge, d.h. der farbige Rand um die Linse (um die Pupille). Die Struktur der Iris kann für eine →biometrische →Identifizierung eingesetzt werden. Dafür wird das Muster mittels hochauflösender Kameras (auch auf einige Entfernung) in den sog. Iriscode umgewandelt und dann mittels geeigneter →Algorithmen mit den Iriscode in entsprechenden →Datenbanken verglichen. Dabei wird die →Hamming Distance bestimmt. Es wird von den meisten Personen als weniger eindringlich empfunden als der →Retina-Erkennung, bei der die Person direkt am Gerät stehen muss. Es konnte 2012 gezeigt werden, dass mit Hilfe von einem →genetic algorithm sich aus vorhandenem Iriscode die Muster einer Iris rückberechnen lassen, so dass sich bei einer Iriserkennung später wieder den gleichen Iriscode ergeben. Iriserkennungssysteme können oft durch ein Foto einer echten oder ‚künstlichen' Iris getäuscht werden

IRL: (in real live) nicht im →Internet, verwendet um zu sagen, dass etwas weder in einem →Social Network, noch in →virtual reality wie →Second Live stattfindet

IRR: (internal rate of return, Interner-Zinssatz-Methode) Methode der →Wirtschaftlichkeitsberechnung. Siehe →ROI, →NPV

ISAC: (Information Sharing and Analysis Centre) industrie-spezifische US-Gruppierungen zum Austausch von Informationen über IT-Security. Siehe →PISCE, →APACS

ISACA: (Information Systems Audit and Control Association) internationale Organisation der IT-Auditoren. Siehe →CobiT

ISAE 3420: International Standards for Assurance Engagements (ISAE) No. 3402, Nachfolger von →SAS 70 als Reporting Format für Audits von →Dienstleistern

ISAKMP: Internet Security Association and Key Management Protocol (RFC 2408). Teil des →IPsec Standards

ISATAP: (Intra-Site Automatic Tunnel Addressing Protocol) Methode um IPv4-Pakete in →IPv6-Paketen zu verpacken. Auf diese Weise können jedoch auch →Angriffe an einer →Firewall oder →IPS vorbei geführt werden. Siehe →Teredo

iSCSI: (Internet-SCSI) Protokollanbindung von →SCSI über das →TCP/IP Protokoll. Enthält Sicherheitsfeatures wie z.B. →Device- und LUN-→ACLs, Authentisierung der Geräte im →SAN mittels →CHAP und kann mit →IPsec implementiert werden

ISDN: (Integrated Services Digital Network) digitales Netz für Sprach-, Datenkommunikation. Die Geschwindigkeit der Datenverbindungen (2x 64 kbit) gilt heute als eher langsam, z.B. im Vergleich zu Kabel und →ADSL

ISEA 3402: (International Standard on Assurance Engagements) internationaler Auditierstandard, siehe auch →SAS 70, http://isae3402.com/

ISMS: →Informationssicherheits-Managementsystem

ISO: (International Standards Organisation) internationale Standardisierungsbehörde, entspricht →DIN oder →Önorm. www.iso.org

ISO/IEC 13335: Standard zu Fragen der →Informationssicherheit und →Risikomanagement im IT-Bereich

ISO/IEC 15504: Standard zu Fragen rund im Software→prozesse. Siehe →SPICE, →ISO/IEC 21827

ISO/TS 16949: →Qualitätsnorm im Automobilbau, basiert auf →ISO 9001:2000

ISO 17799: ein aus dem britischen →BS7799 Standard hervorgegangener →Information Security Standard, angenehm nicht-technisch, knapp gehalten. Es hat folgende Gliederung:

- Organisation der Sicherheit
- Einstufung und Kontrolle der Werte
- Personelle Sicherheit
- Physische und Umgebungssicherheit
- Management der Kommunikation und des Betriebes
- Zugangskontrolle
- Systementwicklung- und Wartung
- Management des kontinuierlichen Geschäftsbetriebes
- Kontrollen/Einhaltung der Verpflichtungen

Es wurde in 2005 als gründlich überarbeitete Version herausgegeben. →ISO 27000 Siehe http://sicherheitskultur.at/best_practise.htm

ISO 20000: Familie von Standards zu Service-→Qualität, in der die →ITIL-Konzepte aufgehen

ISO/IEC 21827: Systems Security Engineering Capability Maturity Model (SSE-CMM) entwickelt durch die International Systems Security Engineering Association (ISSEA). Norm zur Darstellung des →Reifegrads der Sicherheits-→Prozesse (und damit spezieller als →ISO/IEC 15504). Siehe →CMM, →SMM, →SSE-CMM

ISO 27000: Familie von Standards zur →Informationssicherheit, in der z.B. die →ISO 17799 als 27002 aufgeht (2006/07)

ISO 27001 geht aus der BS 7799-2 (→ISMS) hervor. ISO 27003 wird sich mit Hilfestellungen bei der Implementierung beschäftigen, ISO 27004 definiert →Metriken und Effektivitätsmessungen (→Kennzahlen, →KPI) und ISO 27005 wird aus →ISO 13335 hervorgehen

ISO 9001:2000: prozessorientierte Normierung zur Erhöhung der →Qualität von Arbeitsabläufen (und damit Arbeitsergebnissen)

ISO Model: schichten-orientierte Darstellung eines Datenaustauschs, z.B. der →TCP/IP →Protokolle. Dabei bezeichnet

→Layer 1: physical connectivity
Layer 2: Data Link (z.B. →ARP)
Layer 3: Network (z.B. →IP)
Layer 4: Transport (z.B. →TCP, →UDP)
Layer 5: Session (z.B. MSRPC)
Layer 6: Presentation (z.B. →ASCII)
Layer 7: Application (z.B. →http, →smtp)

ISP: (Internet Service Provider) Anbieter von → Internet-Anbindungen, in der Regel sowohl für private Nutzung (Einwahl über Modem, →ADSL oder Kabel) oder mit Hilfe von →Standleitungen für kommerzielle Nutzung. Manchmal werden dabei sicherheitsrelevante Dienste zur Verfügung gestellt. In den USA werden 2011 einige erwischt die Anfragen ihrer Kunden an →Suchmaschinen auf andere →Websites umleiten und dafür Kickback kassieren. Siehe →IXP, →NSP, →CNI, →ISPA

ISPA: (Internet Service Providers Austria) Vereinigung der →ISPs in Österreich. Verfolgen z.B. eine einheitliche Politik zu Fragen der Herausgabe von Kundeninformationen bei der Verfolgung von →Tauschbörsen-Teilnehmern und zu →Data Retention. http://www.ispa.at/

ISS: 1) (Intelligence Support Systems) Systeme mit deren Hilfe →Überwachungen (→LI) und deren Auswertungen (→Hancock) durchgeführt werden können

2) Anbieter von Sicherheitssoftware, jetzt Teil von IBM, prominent bei →IDS

iTAN: (indexTAN) Verfahren, bei dem die →TAN Nummern zur Absicherung von →e-Banking Transaktionen nicht beliebig verwendet werden können, sondern durchnummeriert sind und vom e-Banking-Server gezielt angefordert werden. Dies schützt gegen die derzeitige →Phishing Technologie, nicht jedoch gegen →Man-in-the-Middle Angriffe

ITIL: (Information Technology Infrastructure Library) Sammlung von →Best-Practise Methoden zum systematischen Organisieren aller Tätigkeiten im Bereich Service Management und Services Support für Informationssysteme. ITIL definiert Prozesse und die Interaktionen. ITIL- Prozesse sind.

→ Incident Management
→ Problem Management
→ Configuration Management
→ Change Management
→ Release Management
→ Service Level Management (→SLA)
→ Finance Management for IT Services
→ Capacity Management
→ Continuity Management
→ Availability Management

auch: →ISO 20 000, →itSMF, →remediation

http://sicherheitskultur.at/best_practise.htm

IT-Grundschutzhandbuch: →Grundschutzhandbuch

ITPIN: (IT Process Improfement Network) Referenzmodel für IT-Services. →ITIL

ITSEC: (Information Technique System Evaluation Criteria) 1991 veröffentlicht, ein Kriterienkatalog zur Beurteilung und Zertifizierung der Sicherheit von informationstechnischen Systemen im europäischen Bereich. Die Weiterentwicklung der →ITSEC und Vereinheitlichung mit diversen nationalen Kriterienkatalogen sind die →Common Criteria

IT Security Policy: →Information Security Policy

IT-Sicherheit: Sicherheit von IT-Systemen, →Anwendungen und Daten, enger als → Infor-

mationssicherheit

ITSM: IT Service Management. Siehe →itSMSF

***it*SMF:** (IT Service Management Forum, http://www.itsmfi.org/) internationale Organisation mit dem Ziel der Verbesserung und Weiterentwicklung von →ITIL. Sehr interessant die Arbeiten zu →Metric von Service Mgmt.

ITU: (International Telecommunication Union) 1865 gegründete Vereinigung der Telefongesellschaften, heute eine Agentur der UNO. →CCITT ist die Unterabteilung, die sich um Standards kümmert, auch: http://www.itu.int/

IWG: (Informationsweiterverwendungsgesetz) in Ö und D gültiges Gesetz, das die Weiterverwendung von Informationen regelt, die Behörden im Zuge ihrer Arbeit öffentlich zur Verfügung stellen, z.B. Katasterinformationen

IXP: (Internet Exchange Point) Endpunkte der direkten Verbindungen zwischen mehreren →Netzbetreibern für schnellen →Datentransfer zwischen großen Netzbetreibern ohne externe Fernverbindungsanbieter (→NSP, tier 1) zu nutzen (Details siehe →Peering) unter Nutzung von →BGP. Große IX sind: LINX (London), AMS-IX (Amsterdam), DE-CIX (Frankfurt), HKIX (Hong Kong). Dies sind Gebäude („Telecom Hotel“) in denen viele Glassfasterkabel enden (→Backbone).Siehe →Verfügbarkeitsproblematik

J2EE: (Java Platform, Enterprise Edition) transaktionsbasierte Software-Umgebung auf Java-basis, deren Komponenten auch als →Open Source zur Verfügung stehen, enthält zahlreiche sicherheitsrelevante Komponenten, z.B. →JMS, →JAAS. Konkurrenz zu →.NET

JAAS: (Java Authentication and Authorization Service) →Java→API für →Authentisierung und →Autorisierung. Die eigentliche Methode wird in einem Pluggable Authentication Module implementiert

Jail-break: Entfernen von Restriktionen bei einem →Apple iPhone oder iPad. Durch ein jail-break gewinnt der Benutzer volle Kontrolle über sein Gerät, die verwendete Software kann das Gerät jedoch auch anfälliger gegen →Angriffe machen. Siehe →rooting

Jamming: →Denial of Service →Angriff gegen drahtlose Kommunikation, z.B. →GSM, →UMTS oder →LTE

JAP: (Java Anon →Proxy) →Anonymisierer, entwickelt im Rahmen des Projektes →AN.ON der TU Dresden, der Uni Regensburg und des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein. Das →Client Programm JAP sendet die Internetanfragen verschlüsselt an eine „Kaskade“ von „Mix“-Server, die die Anfragen untereinander verschlüsselt weiterleiten, bis der jeweils letzte die Anfrage offen an den Zielserver versendet. Kann zum Umgehen von Zensur, aber auch für kriminelle Aktivitäten genutzt werden. Eine durch Gerichtsbeschluss erzwungene Protokollierungsfunktion für bestimmte Websiten kann deaktiviert werden. Die Software steht als →Open Source zur Verfügung

Java: Programmiersprache von Sun Microsystems. Konzipiert für „transportablen“ Code, d.h. Programme die auf unterschiedlichen Systemen ohne Veränderungen ausgeführt werden können. Leider haben sich seit ca. 2010 immer mehr →Verwundbarkeiten in Java gefunden, so dass es heute zu einer der größten →Schwachstellen auf vielen Systemen geworden ist. Dies liegt speziell auch daran, dass auch bei einer Aktualisierung ältere Versionen oft auch dem Rechner bleiben (oder bleiben müssen, weil bestehende Programme nicht mit den neuen Versionen arbeiten). Statistiken zeigen in 2013, dass 93% aller →Webbrowser mittels Java verwundbar sind, über die Hälfte der Installationen sind älter als 2 Jahre nicht aktualisiert. Siehe →J2EE

Java Card: →Java-Implementierung für →Embedded Devices, z.B. →SIMs. So lassen sich z.B. →OTPs oder →digitale Signaturen im →Handy realisieren

Java Runtime Environment: (JRE) →Laufzeitumgebung für →Java

JavaScript: Programmiersprache, die von → Netscape entwickelt wurde und nichts mit →Java zu tun hat (marketingtechnische Namensänderung). Sie wird hauptsächlich innerhalb von →Webseiten verwendet, kann aber auch beliebige →Datenübertragungen im →Internet durchführen. Mit ihrer Hilfe lassen sich lokale Aktionen, z.B. Feldüberprüfungen oder Interaktivität der Webseite, erreichen. Vom Konzept her sollten sich damit keine Schäden auf Rechnern erzeugen lassen, jedoch treten immer mal wieder Implementierungslücken zu Tage, die zu →Verwundbarkeiten führen können. Lässt sich auch für →Device Fingerprinting nutzen. Kann über →no-script Plugin abgeschaltet werden, aber dann funktionieren viele →Websites nicht mehr. Hat bei →single-page applications eine zentrale Bedeutung, dabei werden zumeist fertige Programmbibliothen wie →angularJS oder →jQuery eingesetzt. JavaScript wird heute aber auch oft in Servern für netznahe Programmierung eingesetzt, z.B. mit →Node.js

JbroFuzz: von → OWASP veröffentlichtes →Fuzzing Tool für Kommunikationsprotokolle

Jericho Forum: Vereinigung von Anwender- und Herstellerfirmen zum Thema Deperimeterisation, d.h. der schwindenden Bedeutung von starren und undurchdringlichen Grenzen zum Schutz des internen →Netzes z.B. wegen der Forderung nach Mobilität der Mitarbeiter und Integration von Partnernetzen. Dies bedeutet eine Verschiebung von →Trust Boundaries

JIT-Compiler: (Just-in-time-Kompilierung)

üblicherweise findet die Übersetzung aus einer →Programmiersprache in →Befehle in einem separaten Schritt VOR Beginn der Ausführung statt. Ein JIT-Compiler wird eingesetzt, wenn diese Übersetzung erst während der Laufzeit des →Programmes stattfindet, aber eine →Interpretation zu langsam ist. Typische Sprachen bei denen dies der Fall ist sind →Python oder →JavaScript

Jitsi: →Open-Source → Webkonferenzsystem das heute über →WebRTC arbeitet und daher von allen modernen →Webbrowsern genutzt werden kann. Die Server werden dezentral gehostet. Jitsi wurde 2020 für Online-Unterricht genutzt, es kann ohne Anmeldung bei Kenntnis einer Server-→URL (z.B. https://meet.jit.si/ sofort genutzt werden

JIT-Spraying: Technik zur Infektion von Rechnern die durch →ASLR geschützt sind. Dabei wird ausgenutzt, dass sog. JIT (just-in-time) →Compiler Script-code, z.B. →action script, erst zur Laufzeit erzeugen. Spraying bezieht sich auf die Technik einer →NOP-slide

JMS: (Java Messaging Service) Software in →J2EE für →Messaging

Journal: (transaction log) bei →Datenbanken: Liste der Änderungen seit einem definierten und gesicherten Stand, verwendet für →Wiederherstellung (→forward recovery). Man unterscheidet →„before images“ und →„after images“. Erstere werden verwendet, um fehlerhafte Änderungen rückgängig zu machen (→undo)

JobCard: →ELENA

JPEG (Joint Photographic Expert Group): Eines der zwei gebräuchlichsten Datenformate für Bilder im Internet, gut geeignet für Farbbilder (das andere ist →GIF). JPEG-codierte Bilder sind in der Regel kleiner als GIFs. In JPEG Dateien kann →Malicious Code versteckt sein. Mit Hilfe von →Steganographie können Nachrichten in Bildern versteckt werden. http://www.jpeg.org/

jQery: Programmbibliothek für →JavaScript für die →DOM-Manipulation zur Entwicklung von →single-page →Webseiten

JSON: (JavaScript Object Notation) text-basiertes lesbares Datenaustauschformat, alternativ zu →XML, oft genutzt in →Ajax. Kann genutzt werden für die Umgehung von →SOP

Juice jacking: →Angriff gegen ein tragbares Gerät, z.B. →Smartphone mittels Ladegerät.

Junk Mail: →Spam

Jurisdiction Shopping: Suche nach Staaten, die einen sicheren Hafen für internationale (oft kriminelle) Aktivitäten bieten

Kad: →P2Ü-Netz, wird seit 2010 für die Steuerung von →TDL-4 eingesetzt

Kaizen: (jap. Veränderung zum Besseren) ein japanisches Management-Konzept für kontinuierliche Verbesserung (→KVP) mit starker Mitarbeiterzentrierung. Siehe →TQM, →PDCA

Kamera: digitale Kameras enthalten heute eine Reihe von Funktionalitäten die die →Privatsphäre gefährden können, z.B. werden →GPS-Koordinaten oft automatisch in die →Meta-Tags der Fotos übernommen. Ebenso können viele Kameras →Image-Tags mit den Namen der Personen auf dem Bild erstellen. Bei einem Hochladen auf eine Photosharing- oder →Social Networking →Website stehen diese Informationen auch extern zur Verfügung und geben in Kombination mit dem Datum den Aufenthaltsort preis. Digitale Kameras die im Rahmen von →Home Automation eingesetzt werden (z.B. →Überwachung des Kinderzimmers oder des Eingangsbereiches, siehe →Doorbell) können nach einer Trennung für →digitale Gewalt genutzt werden. Daher ist nach einer Trennung ein Zurücksetzen aller →Passworte wichtig

Kartengeld: →e-Geld

Katastrophe, Katastrophenfall: (K-Fall) das Eintreten einer Situation, bei der der →Katastrophenplan aktiviert werden muss. Der Begriff ist mehr oder weniger synonym für →Krise

Katastrophenplan: Beschreibung der →Prozesse und Vorkehrungen die eine eingeschränkte, aber dem Notfall angemessene, IT-Versorgung sicherzustellen sollen. Teil ist immer ein →Alarmplan. Siehe →Disaster Recovery, →Business Continuity

KaZaA: Internet-Tauschbörse ab 2001. Der Originalclient enthielt →Spyware, KaZaA-lite hatte einen etwas besseren Ruf. →Skype verwendete Teile des KaZaA-Netzes für Telephonie. 2012 eingestellt. Siehe →P2P

KCM: (key continuity management) Vorschlag für ein vereinfachtes →Verschlüsselungskonzept für →E-mails, bei der jeder Benutzer selbst ein Schlüsselpaar erstellt, und seinen →Public Key aktiv mit seinen E-mails verteilt und das daher ohne →CA auskommt

KDC: →Key Distribution Centre

Kennzahlen: →KPI

Kerberos: (Höllenhund der griechischen Mythologie) vom MIT (Massachusetts Institut of Technologie) entwickeltes Verfahren zur →Authentisierung mittels →SSO durch Austausch von „tickets“. Das Konzept wird heute z.B. auch in MS Windows verwendet, wurde jedoch „kreativ“ verändert und ist damit nicht kompatibel zum MIT Kerberos, aber sehr weit verbreitet, da standard-mäßig in jedem windows-basierten Firmennetz unterstützt. Die Windows Implementierung erfordert „trust“ zwischen den beteiligten →AD-Systemen. AD kann heute aber auch mittels →AD FS →SAML unterstützen.

http://www.ietf.org/rfc/rfc1510.txt

Kerckhoff's Principle: Grundprinzip der →Verschlüsselung, dass Sicherheit nicht durch die Vertraulichkeit des →Verschlüsselungsalgorithmus entstehen sollte, sondern durch den Schlüssels, 1883 in *La Cryptographie militaire.* Siehe →Shannon, →Obscurity

Kernel: Kern eines →Betriebssystem. Basiskomponenten die für den grundlegenden Betrieb des Betriebssystems notwendig sind. Sie werden beim →Boot-Vorgang zuerst geladen. Kernel-Dienste stellen die Basis für die Sicherheitsfunktionen dar. Infektionen in diesen Kompomenten sind sehr schwer zu finden. Viele Sicherheitsfunktionen stützen sich auf Kernel-Dienste. Siehe →root kit, →HIPS

Kettenbriefe: kein primäres Sicherheitsproblem, soll jedoch vom →Facebook Immune System erkannt und in der Ausbreitung gestoppt werden weil durch die hohe →Konnektivität des →Social Graps schon in wenigen Minuten bis zu 5% aller Mitglieder erreicht werden können

Keyboard: (engl.→Tastatur). Siehe auch →visual keyboard

Key Distribution Centre: (KDC) Teil einer →PKI, die den öffentlichen →Schlüssel verteilt, in der Regel in Verbindung mit →CRL oder →OCSP

Key Escrow: →Key Recovery

Key Exchange: Verfahren zum sicheren Austausch von symmetrischen →Schlüsseln. Siehe →IKE, →Diffie-Hellman

Keyless System: (remote keyless system, RKS) →Authentisierungsverfahren das bei Autos und Gebäuden genutzt wird um berührungslos (mittels Radiofrequenzen) ein Schloss zu öffnen, kann als Gerät (Schlüssel oder „key fob") oder als →Software in Form einer →App implementiert werden. Dabei wird ähnlich wie bei →HOTP ein Zähler verwendet („rolling code") der bei jeder Nutzung hochgezählt wird. Dadurch ist eine Resynchronisierung notwendig wenn z.B. das Gerät wiederholt ohne Verbindung zum Auto aktiviert wird. Diese Resynchronisierung ermöglicht auch →Replay-→Angriffe. Erste Implementierungen waren bereits 1980. Vielfältige Angriffe sind möglich, fast alle diese Systeme sind stark verwundbar. Ein simpler Angriff ist das Unterdrücken des „Verschließkommandos" durch Störung der Übertragung des Kommandos („jamming"). Dadurch verbleibt das Auto offen. Moderne Systeme aktivieren sich oft selbständig über die Nähe zwischen „Schlüssel" und Fahrzeug (proximity). Dies hat den Vorteil dass der Besitzer kein Hand für das Öffnen braucht. Solche Technik wird manchmal auch verwendet um den Motor zu stoppen wenn der Schlüssel nicht mehr in der Nähe des Fahrzeugs ist („immobiliser"). Dies soll verhindern dass die Zündung kurz geschlossen wird, hat aber zu Problemen geführt wenn z.B. ein Kind den Schlüssel, der ja nicht in der Zündung steckt, aus dem Fenster wirft. Proxmity Systeme werden häufig angegriffen indem der Angreifer/Dieb einen Empfänger für das Signal des Schlüssels in die Nähe des Schlüssels bringt (zumeist einen →Laptop im Vorgarten des Besitzers) der dann ein verstärktes Signal an das Fahrzeug sendet, das sich dann öffnet und einen Motorstart erlaubt

Keylogger: spezielle Form von →Spyware, oft als →Trojaner auf einem Rechner installiert, die Tastenanschläge sammelt und überträgt, u.a. →Passworte. Oft auch als unbemerkt installiertes Gerät zwischen →Tastatur und → PCs, das Texteingaben Passworte aufzeichnet Siehe →Phishing, →Dropzone, →visual keyboard

Key management: (Schlüsselverwaltung) komplexes Aufgabengebiet im Rahmen von →Verschlüsselung und möglicher Angriffspunkt. Es geht z.B. um die sichere Aufbewahrung und Zugriff auf →Schlüssel die bei kryptographischen Verfahren benötigt werden, um (automatisierten) Austausch von Schlüsseln vor deren Ablauf und den Austausch von Schlüsseln mit Gegenstellen und auch →Key Recovery. Siehe auch →PFS

Key Recovery: (key escrow) Verfahren mit dessen Hilfe verschlüsselte →Daten ohne Kenntnis des eigentlichen →Schlüssels entschlüsselt werden können. Dies ist sinnvoll wenn es sich z.B. um Firmendaten handelt, die auch nach dem Ausscheiden eines Mitarbeiters noch lesbar sein sollen. Auf Grund der Möglichkeit des (staatlichen) Missbrauchs ein umstrittenes Thema. Bei den meisten →PKI-Produkten ist dies eine optionale Feature. Siehe →Escrow Encryption Standard, →CrashPlan

KI: künstliche Intelligenz, siehe AI, →artificial intelligence

Killbit: Mechanismus, der die Ausführung von →Active X im Internet Explorer verhindert. Dies verhindert jedoch auch die Benutzung von Active X zu Update-Zwecken

Kill chain: militärisches Konzept das besagt, dass ein →Angreifer um ein Ziel zu erreichen eine Reihe von Schritten ausführen muss und dass es für den Verteidiger ausreicht, eines davon zu vereiteln. Dies ist die Umkehr des Spruchs dass „der Angreifer nur 1 →Schwachstelle finden muss, der Verteidiger ALLE Schwachstellen stopfen muss". Wird in der IT-Sicherheit zur Abwehr von →targeted attacks durch →Breach Detection Systems verwendet

Kill Switch: (deutsch: Notaus) Einrichtung zum schnellen De-aktivieren von einem Gerät. In der Informationssicherheit unterschiedlich verwendet, z.B.

α) (angebliche) Hintertüren in Geräten (wie z.B. →Routern) die es einem Eingeweiten

erlauben die Geräte auf die Ferne die Deaktivieren, z.B. im Kriegsfall des eigenen Staates mit dem Kunden-Staat. In den USA geforderte Funktionalität zum Abschalten des →Internets bei Gefahr oder →Bedrohung

β) Vorgeschlagene Lösung zum Sperren von gestohlenen →Smartphones die über das jeweilige Betriebssystem und Hardware läuft und unabhängig ist von der weltweiten Kooperation von Mobilfunkprovidern (was beim Sperren mittels →IMEI notwendig ist, leider nirgendwo implementiert wird und durch Verkauf in andere Regionen ausgehebelt werden kann). In den USA ist Smartphone-Raub mittlerweile landesweit 30% aller Raubüberfälle, in großen Städten bis zu 70%, „Apple picking".

Klarnamenszwang: auch **Klarnamenspflicht**. In Ö und D immer wieder geforderte Regelung, dass bei Kommunikationen in →Internet zwar →Pseudonyme genutzt werden dürfen, diese aber an einer Stelle, entweder bei dem Betreiber der Website oder einer zentralen Stelle mit dem realen Namen verknüpft sein müssen. Die Befürworter einer solchen Regelung wollen dass es keine →Anonymität im Internet gibt, so wie dies in Ländern wie China, Nordkorea, Iran, … auch umgesetzt ist. So etwas klingt im Hinblick auf →Fake News, →Hasspostings, Morddrohungen, etc. durchaus logisch. Problematisch daran ist jedoch nicht nur die Einschränkung der „freien Meinungsäußerung" (weil kritische Äußerungen z.B. zu negativen Auswirkungen im Beruf führen könnten), sondern auch, dass es für Betreiber einer Website mit Kommentarmöglichkeiten sehr aufwendig ist, die wirkliche →Identität einer Person zu prüfen. Die heute übliche Angabe einer →E-Mail-Adresse bei der Registrierung stellt ja keine Identitätsprüfung dar

Klassifizierung: auf dem Gebiet der Informationssicherheit: Sicherstellung eines angemessenen Schutzniveaus für Informationswerte (→Daten, Anwendungen und Systeme) durch Einteilung nach →Vertraulichkeits-, →Integritäts- und →Verfügbarkeitsbedarf. Siehe →Datenklassifizierung

Klimatisierung: wichtiger Aspekt der Ausstattung eines →Rechnerraums. Ausfälle der Klimaanlage können zum Gesamtausfall und sogar zur Zerstörung von →Rechnern oder →Backup-Medien führen

KMU: (kleine und mittlere Unternehmen) konkrete Einstufung abhängig von Mitarbeiterzahl, Bilanzsumme oder Umsatz. Auf Grund von schwach besetztem IT-Personal oft nicht optimal gegen IT-Risiken abgesichert, engl. →SME oder →SMB. Siehe →UTM

Knowledge-Management: 'Wissensmanagement'; soll Orientierungskarten für den Informationsdschungel anlegen. Dazu wird das Wissen in einem Unternehmen systematisch gesammelt, analysiert, aufbereitet und anderen Mitarbeitern zur Verfügung gestellt. Wissensmanagement soll verhindern, dass in einer Abteilung eines Unternehmens über eine Problemlösung nachgedacht wird, die in einer anderen Abteilung schon gefunden wurde. Schwierigkeiten bereitet aber noch die Frage, wie man das Wissen aus den Köpfen der Mitarbeiter am besten ins Intranet bekommt - denn nicht alles lässt sich in Worten oder Bildern ausdrücken und ausdrucken

Kollision: bei digitalen →Signaturen und →Hash-Werten, wenn 2 unterschiedliche Texte den gleichen Hash-Wert ergeben. Dies passiert natürlich immer, wenn viele große Texte auf einen kleinen Wert reduziert werden. Eine Signatur gilt als „unsicher", wenn eine solche Kollision gezielt erzeugt werden kann, so dass ein Dokument nach einer Veränderung immer noch die gleiche Signatur hat

Konkurrenzspionage: →Wirtschaftsspionage

Konnektivität: Verbindung oder die Art und Weise einer Verbindung bzw. die Verbindungsdichte, z.B. in einem →Social Graph eines →Social Networks. Hohe Konnektivität bedeutet sehr schnell mögliche Verteilung von Informationen, hinter denen sich auch →Angriffe verbergen können oder Belästigungen wie →Kettenbriefe. Siehe auch →Kontakte, →friends

Kontakte: anderer Name für das →Adressbuch in einem →Computer oder →Smartphone. Wird gern „entwendet", weil diese →Daten Hinweise auf das soziale Netz eines Menschen geben, den „→Social Graph", der für Marketing-Zwecke wertvoll ist. Andere Hinweise auf den Social Graph sind die →friends in den →Social Networks, aber auch einfache Adresslisten im Rahmen von →E-Mail

Kontinuierlicher Verbesserungsprozess: (KVP) ständiger →Prozess zur Verbesserung der Leistungserbringung, der Kundenbetreuung, des Umfeldes, der Situation der Mitarbeiter oder anderer relevanter Faktoren des betrieblichen Geschehens. Dazu werden entsprechende Prozesse definiert, diese in festgelegten Perioden durchlaufen und dabei die Voraussetzungen für eine kontinuierliche Beteiligung der Mitarbeiter an Verbesserungen geschaffen. Wichtige Elemente sind die Messbarkeit von wichtigen Parametern und deren kontinuierliche Messung. KVP ist in wichtiges Element des umfassenden →Qualitätsmanagements (→TQM). Siehe →Kaizen

Kontinuitätsmanagement: Ziel ist es, Unterbrechungen der Geschäftstätigkeit entgegenzuwirken und die kritischen →Geschäftsprozesse vor den Auswirkungen wesentlicher Ausfälle oder →Katastrophen zu schützen; es soll Störungen durch Katastrophen und Sicher-

heitsversagen (z.B. als Folge von Naturkatastrophen, Unfällen, Geräteausfällen und mutwilligen Beschädigungen) durch eine Kombination aus präventiven und reaktiven Kontrollen auf ein akzeptables Maß reduzieren; →Notfallpläne sollen sicherstellen, dass Geschäftsprozesse in der erforderlichen Zeit wiederhergestellt werden können. Ziel kann auch sein, mit einem Verlust der Kontinuität anderweitig umgehen zu können. Siehe →Business Continuity

KonTraG: (Gesetz zur Kontrolle und Transparenz im Unternehmensbereich) deutsches Gesetz. Nach dem KonTraG sind Aktiengesellschaften (AG) in Deutschland gesetzlich zur Risikofrüherkennung, einem Teilbereich des →Risikomanagements, verpflichtet, um den Erhalt des Unternehmens sicherzustellen. International finden sich ähnliche rechtliche Anforderungen beispielsweise im →Sarbanes Oxley Act

Konzernprivileg: im →Datenschutz gibt es (im Gegensatz z.B. zum Kartellgesetz) kein Konzernprivileg, d.h. der Datentransfer zu einem Tochter- oder Schwester-Unternehmen wird genauso betrachtet wie zu jedem anderen Unternehmen

Kopierschutz: technologische Verfahren, die ein Kopieren von Produkten wie Musik, Büchern oder Filme verhindern sollen (oft unter Verwendung →kryptographischer →Schlüssel). Eingesetzte Verfahren werden zumeist entweder schnell „geknackt" und/oder sind auch für legitime Nutzer stark behindernd. Siehe →DRM, →CSS, →Copyright, →Reverse Engineering, →CGMS-A, →VEIL, →EME, →eBook

KPI: (key performance indicator) →Kennzahlen zur Messung, ob strategische Ziele erreicht werden, für die →Informationssicherheit in →itSMF, →ISO 27004, →OSSTMM. Siehe →Benchmark, →Mystery Activity

Kreditkarte: erfunden 1950 von Frank X. McNamara unter dem Namen Diners Club. Heute meistgenutztes Zahlungsmittel im →Internet. Durch Haftungsübernahme durch die Kreditkarten-Organisation für den Kunden relativ sicher, vgl. Haftung bei →Bankomatkarten. Wegen der Haftung verfügen die Kreditkartenorganisation heute über ausgefeilte →Fraud-Detection Systeme. Kunde kann jederzeit die Rückerstattung verlangen (→ Chargeback), der Händler muss dann die Transaktion nachweisen. Nutzung von Kreditkarten bedeutet Verlust der →Anonymität wie bei Nutzung einer Bankomat- oder →Kundenkarte.

Die Ökosystem für Kreditkarten sieht folgendermaßen aus: Der Kunde bezieht die Karte von Card Issuer (VISA, MasterCard, American Express, Diners Club, u.a.), oft „gebrandet" durch seine Hausbank oder ein anderes Unternehmen. Wenn die Karte bei einem Händler benutzt wird, so hat dieser eine Verbindung mit einem →Acquirer (heute oft elektronisch, d.h. online). Dabei wird je nach Vertragsgestaltung zumeist bereits →Fraud Detection durchgeführt, dies ist jedoch für den Händler teurer. Der Händler trägt ansonsten das Risiko einer gestohlenen Karte die vom eigentlichen Besitzer storniert wurde. Der Acquirer holt sich dann den Betrag minus eines Abschlags vom Endpreis minus seines Anteils vom Kartenaussteller wieder, der den Kunden mit dem vollen Betrag belastet. Das Risiko für Stornierungen durch den Kunden trägt größtenteils der Händler, abhängig von Details des Vertrags, speziell im Rahmen von →CNP Fraud. Für 2013 werden für die USA Schäden von 5 Milliarden Euro, für den Rest der Welt weitere 5 Milliarden.

Ein ähnliches Konzept sind →Pre-Paid Cards, dabei muss der Betrag vorher eingezahlt werden und stellt für die Herausgeber nur dann ein Risiko dar, wenn es den Angreifern gelingt, in das interne System einzudringen und die Karten unberechtigt aufzuladen und ohne Limit zu setzen (solche Angriffe sind seit 2011 bekannt). Pre-paid Karten können oft verwendet werden wo Kreditkarten verwendbar sind, z.B. im →Internet. Zum Teil sind sie aber auch für spezielle Zwecke vorbehalten, oft sind sie auch rein virtuell und bestehen dann nur aus einem Zahlen- und Buchstaben Code (→e-Geld). Siehe →AIS, →CISP, →SDP, →PCI, →PAN, →CVV, →3-D Secure, →CNP, →Track 2

Kreditkartennummer: 16-stellige Zahl zur Identifikation einer →Kreditkarte. Die ersten 6 Stellen sind die Issuer Identification Number (IIN). Eine der Stellen ist eine →Checksum nach dem →Luhn Algorithmus

Kreditrisiko: bei Banken Gefahr des Ausfalls oder der Bonitätsverschlechterung eines Schuldners. Siehe →Basel II

Kreditschutz: Firmen, die Aufzeichnungen über die →Kreditwürdigkeit von Personen und Firmen führen. Problematisch, wenn dort falsche Informationen abgelegt sind von denen der Betroffene, der in der EU theoretisch ein Auskunfts- und Korrekturrecht hat, nichts weiß. Siehe →Datenschutz, →fraud alert, →Schufa, →Scoring

Kreditwürdigkeit: spezielle Form des →Ratings von Personen um Abzuschätzen, mit welcher Wahrscheinlichkeit sie einen Kredit nicht zurückzahlen werden. Betrifft auch den Abschluss von Handy-Verträgen. Dabei geht der Trend dahin, dass auch →Daten aus →Social Networks eingesetzt werden (wenn die →friends einer Person nicht kreditwürdig sind, die trifft dies mit einer gewissen Wahrscheinlichkeit auch auf diese Person zu). Dies kann zu erheblichen sozialen Ungerechtigkeiten führen. →Scoring

Kriminalität: →organisierte Kriminalität, →Wirtschaftskriminalität

Krise: Wende in einer kontinuierlichen Entwicklung. Im Sicherheitsmanagement ein schwerer Vorfall, der Entscheidungen verlangt und vom →Krisenstab behandelt werden muss. Sehr analog zu →Katastrophenfall

Krisenmanagement: Bewältigung einer →Krise, beinhaltet auch interne und externe Kommunikation, setzt eine entsprechende Vorbereitung voraus

Krisenstab: üblicherweise im Rahmen des →Notfallsplans eingesetztes kleines Team, das über das Vorgehen im Not- oder →Katastrophenfall entscheidet. Oft in Form einer Überlagerung bestehender Managementstrukturen

Kritikalität: ursprünglich aus der Kernenergie (K. eines Reaktors), in der IT die Angabe wie wichtig die →Verfügbarkeit von Systemen und Anwendungen ist. Siehe →Business Continuity

Kryptographie: Lehre von der Verschlüsselung. →Daten oder Nachrichten werden mit Hilfe von Regeln in eine Form gebracht, das nur ein berechtigter Empfänger lesen kann. Heute in der Regel durch Verschlüsselungsverfahren, mit deren Hilfe Informationen durch mathematische Algorithmen unter Verwendung eines Schlüssels in eine unverständliche Form (Cipher Text) gebracht werden. Nur wer einen geeigneten Schlüssel besitzt kann die ursprüngliche Information wiederherstellen. Andere Anwendungen sind Hash-Funktionen und Schlüsselaustauschverfahren wie →Diffie-Hellman. Mehr Details unter →Verschlüsselungsverfahren, →Hash-Funktion, →Open Source

Kryptologie: Wissenschaft vom Ver- und Entschlüsseln. Weil die →Vertraulichkeit von →Daten im →Internet auch für den E-Commerce von großer Bedeutung ist, rechnen Experten damit, dass Kryptologie immer wichtiger wird. Gesucht sind sichere Verfahren zur Datenübermittlung. Siehe →Kryptographie

Kubernetes: →Open Source System zur automatisierten Bereitstellung, Skalierung und Verwaltung von Rechenleistungen in sog. Container-Anwendungen (→Containervirtualisierung). Kubernetes Implementierungen können im eigenen →Rechenzentrum genutzt werden (z.B. mit Red Hats OpenShift) oder extern in →Microsofts Azure, IBMs Bluemix, Amazons →AWS oder Oracles. Die Skalierung ist sehr flexibel: bei Bedarf können dynamisch zusätzliche Instanzen eines Containers aktiviert werden. Die Kompatibilität erlaubt es, dass eine Kunbernetes Implementierung lokal Rechenleistung dynamisch mit externen Leistungen kombiniert

Kunde: bzw. Customer. In der →Informationssicherheit die Organisationseinheit (intern oder extern), für die eine Dienstleistung erbracht wird. Wichtiger Begriff in der →ISO 17799-2005. Siehe →Information Owner

Kundenkarte: (auch Treue- oder Bonuskarte) nach einer Registrierung an Kunden ausgegebene Identifikationskarte, die günstigere Bedingungen ermöglicht, aber eine Offenlegung des Kaufverhaltens bedeutet, das über →data mining ausgewertet werden kann (→Consumer Profile), entweder durch das Unternehmen selbst oder nach Weitergabe auch in zentralen →Datenbanken von Datensammlern (→data aggregation). Der gleiche Effekt tritt natürlich auch bei Bezahlung mit →Bankomat- oder →Kreditkarte ein. Siehe →Privatsphäre, →Anonymität

Künstliche Intelligenz: →Artificial intelligence

Kursrisiko: im Handel die Gefahr, dass während der Dauer eines Geschäftsvorgangs, vom Angebot bis zur Zahlung Währungskurse sich nachteilig verändern, kann durch Finanzinstrumente abgefangen werden

KVM: (Keyboard, Video, Mouse) über einen KVM-Switch werden →Tastatur, →Bildschirm und →Maus wahlweise mit unterschiedlichen →Rechnern (zumeist →Servern) verbunden, kann auch über →IP-Verbindungen geführt werden

KVP: (→kontinuierlicher Verbesserungsprozess). Siehe →Kaizen

KYC: (know your customer) Forderung an alle Finanzdienstleister, dass sie die →Identität ihrer Kunden zweifelsfrei feststellen und dokumentieren müssen, z.B. durch Prüfung eines amtlichen Ausweises. Wenn dies nicht implementiert wird, wie z.B. bei anonymen →e-Geld, so ist →Geldwäsche möglich

L0pht: Legendäre →Hacker-Gruppe, wurde 1998 zu einem Hearing des US Senates eingeladen und weiß auf die konzeptionellen Sicherheitsprobleme des →Internets hin. Bekannt durch L0pht crack, ein Tool zum Cracken von →Passworten. Die Gruppe war bei den Pionieren von →Responsible Disclosure. L0pht ging 2000 in @stake auf, das später von Symantec gekauft wurde

L2TP: (→Layer 2 Tunneling Protocol) auf →PPP basierende Technologie um protokollneutrale →VPNs aufzubauen. Ältere Technologie, gilt nicht als sehr sicher, ist aber in China nur schwer zu blockieren und wird daher von VPN-Services angeboten um die Zensurmaßnahmen zu umgehen

LaGrande: Technologieansatz von Intel, um die Rechnersicherheit zu verbessern. Sie verwendet dabei →TPM und Virtualisierungstechniken

Lampertz-Zelle: Hoch-Sicherheitsraum für Server (→Rechnerraum) oder Backup-Medien. Ausgestattet mit →Brandschutz, →Klimatisierung und →Zutrittskontrolle

LAN: (Local Area Network) Infrastruktur zur

Vernetzung von Rechnern innerhalb einer Organisation und eines Gebäudes. Verschiedene LANs können über ein →WAN (wide area network) miteinander verbunden sein, oder über eine Internet-Anbindung im →Internet eingebunden sein

Laptop: (auch →Notebook) tragbarer →PC mit integriertem →Bildschirm, →Tastatur und →Maus der leicht entwendet wird, an vielen Stellen ins →Internet geht und daher ein Sicherheitsrisiko darstellt. Schutz der →Daten durch →Verschlüsselung der →Festplatte und →Passwortschutz im →BIOS. Im Gegensatz dazu →Desktop

LARP: (Live Action Role-Playing Game) Form des Role-Playing Games (→RPG) bei dem die Spieler ihre gewählten Rollen in der Realität (→IRL) einnehmen. Dies können historische Rollen sein, oder auch andere. Wird sogar für Unterrichtszwecke eingesetzt, z.B. für Sprachen-Lernen. Eine spezielle Form sind →ARGs. Eine andere Variante sind →Capture the Flag

Lastenheft: (oder Anforderungsspezifikation) beschreibt die unmittelbaren Anforderungen, Erwartungen und Wünsche an ein geplantes Produkt, z.B. Software, formuliert in natürlicher Sprache. Siehe →Wasserfallmethode

Lastschrift: Möglichkeit in D., Ö und →SEPA Geld von einem fremden Konto anzufordern. Erfordert keine Freigabe durch den Zahlenden. Die Sicherheit entsteht durch den Rücktransfer bei Widerspruch

Latency: (engl. Verzögerung) im →Internet meist die Verzögerung bei Datenverbindungen. Jedes Netzwerkgerät (z.B. →Router) muss ein Datenpaket empfangen, dann Untersuchen und geeignet Verarbeiten, z.B. Weiterleiten. Dabei entstehen Verzögerungen, die deutlich spürbar sind (Millisekunden-Bereich). Eine typische Internetverbindung besteht es 10 und mehr →Hops, die auf dem Rückweg der Antwort wieder genommen werden müssen. Gemessen wird diese Verzögerung z.B. mittels →Ping, gemessen wird, die Gesamtzeit wird als RTT bezeichnet (round trip time). Siehe →5G

Lateral Movements: Suche und Infektion der eigentlichen Zielrechner bei einem →APT-→Angriff. Erfolgt nachdem der Angreifer über Techniken wie →Social Engineering einen ersten (eigentlich unwichtigen) →Rechner übernehmen konnte

Lauschangriff: passiver →Angriff auf die →Vertraulichkeit von Informationen, entweder durch →Abhören von Gesprächen oder →Datenübertragungen. Auch über die Abstrahlung von Bildschirmen lassen sich Bildschirminhalte auslesen (→Tempest-Angriff). Siehe →Lawful Intercept, →SINA-Box

Laufzeitumgebung: (runtime environment) beschreibt und verwaltet die Resourcen, die einem →Programm zur Laufzeit (d.h. während der Ausführung) zur Verfügung stehen, z.B. Programmbibliotheken, aber auch Netzzugriffe, →Speicher, →Datenbanken, Laufzeitvariable mit benötigten →Informationen, etc. Beispiele sind →Java mit →JRE, →Flash mit →AIR, alle →Webbrowser, →.NET, …

Lawful Intercept: (LI) →Abhören von Kommunikation (Telefon, →E-mail und anderem →Datenverkehr) durch die dazu berechtigten Stellen. Ab 2012 behaupten die Behörden, dass es ein „Going dark"-Problem gäbe, d.h. durch die besser werdenden →Verschlüsselungen viele Kommunikationsdienste und das →Peer-to-peer Konzept wäre dieser →Zugriff oft technisch nicht mehr möglich. Diese Argumentation ist umstritten, denn anderseits stehen den Behörden z.B. über →Social Network heute Berge von →Daten für die Aufklärung von Straftaten zur Verfügung die es früher nicht gab. Siehe →Überwachung, →Wiretap, →Lauschangriff, →Messaging Dienste

Law Enforcement: (LE) Sammelbegriff für Polizei- und andere Sicherheitsbehörden

Law Enforcement Access: →Zugriff von Strafverfolgungsbehörden auf →Daten, entweder Kommunikationsdaten wie bei der →Vorratsdatenspeicherung und →Lawful Intercept, (bzw. →Bundestrojaner) oder auch auf Daten die bei einem Service-Anbieter „in the →cloud" vorliegen. Solche Zugriffe benötigen optimalerweise einen Richterbeschluss - liegen die Daten in einem anderen Land, so werden (optimalerweise) im Amtshilfeverfahren auch die Richter im Zielland gefragt. Es hat sich jedoch eingebürgert, dass US-Anbieter wie →Facebook und →Google auch direkte Auskünfte geben ohne Involvierung der US-Behörden (Google legt darüber regelmäßige Berichte vor).

Ein weiterer Aspekt betrifft die Beschlagnahme. In Fällen, wo der Service-Anbieter als möglicherweise beteiligt angesehen wird, werden Strafverfolgungsbehörden eine Beschlagnahmung durchführen und nicht darauf vertrauen, dass die Administratoren des Service-Anbieters die Daten korrekt und vollständig herausgeben. Wenn, wie bei →Cloud Lösungen üblich, Daten verschiedener Kunden aus verschiedenen Ländern im selben System verarbeitet werden, so muss im Rahmen der →Mandantentrennung eine saubere Trennung der Kundendaten dergestalt möglich sein, dass die Anforderungen an Beweisfestigkeit und trotzdem die Behörden nicht Zugriff auf Daten aus Ländern erhalten, auf die sie keine Zugriffsrechte haben. Dies kann z.B. durch → Verschlüsselung der Daten mit unterschiedlichen →Schlüsseln pro Land erreicht werden

Lavabit: →E-Mail-Service mit sicherer →Verschlüsselung von Ladar Levison der bekannt wurde, weil der 2014 geschlossen wurde, als

die US-Behörden von Levison die →Schlüssel zum Entschlüsseln der Mails von →Edward Snowden verlangt hatten. Siehe auch →DIME

Layer: (engl. Schicht) Konzept bei Design eines Netzes. Eine Schicht fasst verwandte Funktionalitäten zusammen, die Dienste für die darüber liegende Schicht liefern und solche von der darunterliegenden Schicht empfangen. Siehe →TCP/IP, →ISO-Modell

LDAP: (Lightweight Directory Access Protocol) Protokoll in dem beschrieben ist, wie mit Verzeichnisdiensten kommuniziert wird. Die gängigen Internet-Browser- und E-Mail-Programme unterstützen dieses Protokoll. Es ist auch für den Betrieb einer →PKI wichtig. Es ist eine Nachfolgetechnologie für das umfangreichere →X.500. http://www.ietf.org/rfc/rfc2559.txt

LE: Law enforcement = Polizeibehörden und ähnliche Dienste

LEAP: (Lightweight Extensible Authentication Protocol) von CISCO genutzte Implementierung von →EAP zur Verwendung für →WLAN. Verwendet →MS-CHAP und gilt daher als zu schwach

Leased Line: →Standleitung

Least Privilege: Design-Prinzip für Software, die besagt, dass jede →Anwendung oder jeder →Benutzer nur das Minimum an Rechten haben sollte die für den jeweiligen Zweck notwendig sind. Wird verletzt, wenn wie unter MS Windows sehr oft anzutreffen, alle Benutzer mit →Admin-Rechten arbeiten oder wenn unter →Unix/Linux Arbeiten als „root“ ausgeführt werden, ohne dass diese Rechte notwendig sind. Siehe →Admin Approval Mode in →Vista

Leet: (auch Leetspeak, Leetspeek, 1137) Netzjargon von (selbsternannten) →Internet-Profis. Basis ist das Ersetzen von Buchstaben durch Zahlen oder Sonderzeichen bzw. durch andere Veränderungen, Beispiel: →pwned. Viele Beispiele siehe https://de.wikipedia.org/wiki/Leetspeak und https://en.wikipedia.org/wiki/Leet

Legal Technology: (LT) →Software und Online-Dienste die juristische Arbeitsschritte unterstützt oder automatisiert. LT 1.0 beschreibt Dienste der Büroorganisation, z.B. Ablage, Recherche, Webkonferenzen und Dienste wie →e-Discovery ein.

LT 2.0 beschreibt zukünftige automatische juristische Dienstleistungen und LT 3.0 Automatisierungen wie →Smart Contracts und →AI-Einsatz

Let’s Encrypt: (LE) non-profit Organisation die seit 2016 →Zertifikate für die Nutzung von verschlüsselten →Websites (→TLS) automatisiert und kostenlos erstellt und auch automatisiert in die Website integrieren und aktualisieren lassen. Dies hat dazu geführt, dass die alte Forderung dass ALLE Websites nur noch verschlüsselt erreichbar sein sollten (siehe Reaktion auf →Edward Snowden), seit ca. 2019 weitestgehend erreicht wurde. LE hat damit den Markt der traditionellen →certificate authorities sehr stark umgekrempelt. Okt. 2019 hatte LE →837 Mio Zertifikate erstellt

LexisNexis: US →Daten-Aggregator, bekannt geworden u.a. durch "Verluste" von persönlichen Daten. http://sicherheitskultur.at/privacy_loss.htm#privat

LI: →Lawful Intercept

Liberty Alliance: Industrie-Allianz für →Federated Identity Systems. Entwickelte das ID-FF-Protocol, das heute in →SAML aufgegangen ist

Libra: von →Facebook ab 2018 geplante digitale Währung, eine Form von →Stablecoin. Einige Zentralbanken finden das nicht gut wenn eine große Internetfirma die Kontrolle über die internationalen Finanzflüsse konktrolliert und sind deswegen dabei, eigene →CBDC einzuführen

Lichtleiter: →Lichtwellenleiter

Lichtwellenleiter: →Fibre Optics

Liechtenstein-CD: Fall von →Datendiebstahl bei dem Steuerbehörden in D. 2002 Daten von Bankkunden in Liechtenstein gekauft haben. Ähnliche Fälle sind danach noch öfter passiert. Problematisch, da auf diese Weise →Cybercrime-Aktivitäten staatlich „sanktioniert“ werden und →Administratoren zu illegalen Tätigkeiten (Bruch das →Bankgeheimnisses und des →Datenschutzes) verleitet werden. http://sicherheitskultur.at/notizen_1_10.htm#diebstahl

Likes: Inbegriff des Belohnungssystems das die →Stickyness von erfolgreichen →Social Networking →Websites ausmacht. Dabei wird mit Tricks aus dem Bereich des Glücksspiels z.B. auf abwechselnde Belohnung und fehlende Belohnung gesetzt. Likes, retweets u.ä. stellen dabei die Belohnungen dar die der Nutzer nicht verpassen will

Like-Button: (Gefällt mir) Konzept beim →Social Networking dass Benutzer einer „regulären“ Content-→Website mittels dieses Buttons eine Zustimmung ausdrücken können, die dann automatisch allen ihren „→friends“ kommuniziert wird. Bei →Facebook bewirkt aber bereits die blose Anwesenheit des Buttons auf einer besuchten Seite dass ein →Tracking dieses Benutzers durchgeführt wird, auch wenn er nicht FB-Benutzer ist. Facebook hat dieses Konzept 2011 durch →Open Graph auf beliebige Beziehungen erweitert. Verben können jetzt definiert werden wie hört, sieht, kauft, besucht, etc. zusammen mit entsprechenden Objekten wie Orten oder Musikstücken. Alle Daten die so anfallen sind Teil des →Social Graphs

Like-Jacking: →Schadsoftware, z.B. in Form eines Video-Aufrufs, die bei Aktivierung das

Drücken des →Like-Buttons simuliert und sich damit an alle „→friends“ weiterverbreitet

Link: →Hyperlink

LinkedIn: größtes →Social Network für berufliche Vernetzung, > 200 Mio Benutzer in 200 Ländern. Da es hauptsächlich beruflich genutzt wird und viele Job-Histories enthält sehr gut geeignet für →Open Source Research und →Social Engineering. Oft enthalten die Profile Angaben über Inhalte, die der Verschwiegenheitspflicht unterliegen. So listen viele →NSA-Mitarbeiter die Codenamen der geheimen Programme in ihrem öffentlichen Lebenslauf auf. →Angriffe über das Übernehmen von bestehenden Accounts oder über das Anlegen von Fake Accounts. Wurde 2016 von →Microsoft gekauft, ist jedoch z.B. von der Benutzerverwaltung (noch) nicht in andere Microsoft-Dienste wie →Outlook integriert

Link Key: wird bei der Herstellung eines →Pairings zwischen zwei →Bluetooth-Geräten verwendet. Entsteht durch Eingabe eines gemeinsamen →Pass Keys auf beiden Geräten. Als →Unit Keys oder →Combination Keys möglich

LinkNYC: Projekt von →Sidewalk Labs in New York. Details siehe Sidewalk Labs

Linux: weit verbreitetes →UNIX →Betriebssystem, erstellt auf der Basis von →Open Source und verteilt unter GNU/Linux →Lizenz als →Freeware. Siehe auch →LSM, →Tails

Lifebits: Konzept bei der das ganze Leben eines Menschen aufgezeichnet wird, z.B. durch →Google Glass oder andere →wearable computing Projekte. Problematisch, da ja auch große Teile des Lebens seiner Mitmenschen ungefragt aufgezeichnet (und immer häufiger auch auswertbar) werden. Zu unterscheiden von →Quantified Self

Lifelogging: wird bisher nur von wenigen Menschen durchgeführt. Dabei werden alle Daten aus der Umgebung des Betroffenen z.B. mittels Fotos, Video und Sprache aufgezeichnet. Dies soll ein perfektes Gedächtnis erzeugen und kann verbunden werden mit →frictionless sharing. Dadurch wird natürlich auch in die →Privatsphäre der Menschen in der Umgebung eingegriffen

LifeStyle: Marke des österreichischen →Data Aggregators Schober, bekommt seine detaillierten Informationen u.a. durch Fragebogen-Aktionen mit amtlichem Aussehen, bzw. möglicherweise auch über →Kundenkarten

Lizenz: generell die Erlaubnis, etwas zu tun. Im →Urheberrecht entweder eine einfache oder exklusive Lizenz zur Nutzung eines Werkes, z.B. eines Textes oder einer Software. Normalerweise ein Vertrag zwischen zwei Vertragspartnern, kann aber auch generell gewährt werden, z.B. beim Einstellen ins →Internet. Nach →Creative Commons werden dabei 3 Fragen definiert:
a) Nutzung ohne Nennung des Autors erlaubt?
b) kommerzielle Nutzung erlaubt?
c) sind Veränderungen (Derivate) erlaubt und muss dafür die gleiche Lizenzform verwendet werden?
Daraus ergibt sich z.B. „freie Software“ und public domain-Werke, bei denen pauschale Nutzungsrechte eingeräumt werden. Siehe →Urheberrecht, →GPL, →EULA, →Freeware

LSM: (Linux Security Modules) Framework für Sicherheitserweiterungen im →Linux Kernel auf der Basis von →Mandatory Access Control. Implementiert durch →SELinux und →AppArmor

Load Sharing: Lastverteilung. Wenn mehrere Rechner (oft in der Form eines →Clusters jeweils einen Teil der Last übernehmen. Mit Hilfe dieser Technologie wird →Hochverfügbarkeit mit einer Erweiterung der Rechnerkapazität kombiniert

Local adversary: →global adversary

Localization: Schlagwort im Rahmen von →Cloud Computing (mehr Details auch dort), bei dem es darum geht, in welchen Ländern →Daten gespeichert werden. Dies kann juristisch einen Unterschied machen, z.B. wenn es um Zugriffe von →Law Enforcement Behörden geht. Anderseits hat 2013 in Mgr von →Microsoft erklärt, dass der →Zugriff durch die →NSA auch auf Daten in Europa möglich ist. Trotzdem arbeitet 2014 Microsoft in diese Richtung, →Google erklärt sich ausdrücklich dagegen

Local Shared Object: (→LSO)

Lochkarte: Alter →Datenträger, entstanden noch vor der Erfindung des →Computers, verwendet anfangs für Dateneingabe für Webstühle, dann ab 1890 durch Hollerith für die Auswertung der amerikanischen →Volkszählung weiterentwickelt, zusammen mit den dafür nötigen Stanz-, Lese- und Sortiermaschinen (Tabelliermaschinen), die über sog. Stecktafeln programmiert wurden

Log: →Logging

Logfile, Logdaten: Daten, die beim →Logging entstehen. Sicherheitsrelevante Logfiles sollten vor Modifikationen geschützt sein und regelmäßig ausgewertet werden. Oft enthalten sie →personenbezogene Daten und können daher unter das →Datenschutzgesetz fallen. Siehe →Data Retention, →Monitoring

Logging: Schreiben von →Protokollen von Aktivitäten, Events und Zugriffen durch →Benutzer, →Systeme und Geräte. Die Auswertung der Logfiles ist ein wichtiger Aspekt der Informationssicherheit. Das →DSG fordert z.B., dass →Zugriffe auf und die Veränderung von →sensiblen Daten so protokolliert werden müssen, dass Verursacher festgestellt werden können. Logs spielen auch im Rahmen eines →SIEM eine große Rolle. Siehe →syslog

Log-in: →Authentisierung in einem →Netz, →Betriebssystem oder →Anwendung. Siehe →SSO

Logische Sicherheit: zusammen mit →physischer und →personeller Sicherheit wichtige Bausteine von →IT und →Informationssicherheit. Bezeichnet Software-Schutz der Systeme, z.B. Identifizierung, Kennwörter, Auskunftsrechte, Berechtigung und die dafür notwendigen →Prozesse

GotoMeeting: Software für →Webkonferenzsysteme von Firma →LogMeIn (LogMeIn wurde unter anderem Namen in Budapest gegründet und nahm 2006 diesen Namen an, 2016 übernahmen sie die GoTo-Sparte von →Citrix). GotoMeeting ist sehr ähnlich zu GotoTraining, GotoWebinar, GotoAssist (→Fernwartung), etc.). So wie ähnliche Dienste nutzen sie verschlüsselte Datenübertragung zu zentralen Servern, auf denen die Inhalte in Klartext vorliegen

LOIC: (Low Orbit Ion Cannon) fiktionale Waffe aus dem Spiel Command&Conquer). →Programm das für →DoS-Angriffe genutzt warden kann. Wird oft für →Hacktivismus genutzt, Aktivisten können damit einem freiwilligen →Botnetz betreten. Es wurde z.B. bei Aktivitäten von →4chan oder →Anonymous eingesetzt. Siehe auch →HOIC

LoRaWAN: (Long Range Wide Area Network) Funkverbindungen mit kleiner Reichweite werden zu Weitverkehrsnetzen mit geringer Bandbreite zusammengeschlossen. →Amazon setzt diese Technik (in Verbindung mit BLE (→Bluetooth Low Energy) bei →Amazon Echo und →Amazon Ring ein damit diese Geräte auch im Bedarsfall eine Verbindung zum →Internet über fremde Geräte dieses Typs aufbauen können, z.B. die Geräte des Nachbarn. Die Sicherheit dieser Feature ist noch nicht unabhängig getestet worden

LOVINT: Analogie zu →SIGINT, beschreibt wenn Geheimdienstmitarbeiter die →Überwachungstechnologien zur Kontrolle von Partnern oder anderen „love interests“ nutzen

LSASS: (Local Security Authority Subsystem) Dienst in MS Windows für die Überprüfung von Benutzeranmeldungen und →Zugriffsrechten

LSO: (Local Shared Object) →Flash Cookie

LTE: (3GPP Long Term Evolution) Nachfolgekonzept zu →UMTS. 2012 wurde gezeigt, dass es sehr anfällig gegen →Jamming ist, da dafür lediglich bestimmte Steuerkanäle gestört werden müssen. Siehe →4G

Luftschnittstelle: bei der Nutzung einer drahtlosen Übertragungstechnik der Anteil der Datenübertragung der drahtlos erfolgt. Im Fall von Handytechnologien wie →GSM, →GPRS und →UMTS ist dieser Teil immer verschlüsselt (zwischen dem Endgerät und der Relaisstation), im Fall von →Wireless kann die Übertragung, speziell im öffentlichen Bereich, auch unverschlüsselt sein (zwischen dem Endgerät und dem →Access Point)

Luhn Algorithmus: →Checksum, die z.B. für →Kreditkartennummern eingesetzt wird, enthält Schutz gegen das Vertauschen von Nachbarziffern

LULZ: „for the LULZ“ bezeichnet die Motivation eines →Angriffs gegen Netze oder Systeme der weder aus finanziellen Motiven geschieht, noch →Hacktivismus ist, sondern nur im Spaß zu haben. Ethisch bedenklich wird es, wenn Unbeteiligte zu Schaden kommen, z.B. durch die Veröffentlichung ihrer →Passworte. LULZ wird zumeist interpretiert als Plural-Substantiv von LOL (laughing out loud).

LULZSEC: →Hacker-Gruppe die 2011 einige spektakuläre Aktionen hatte, z.B. gegen → Sony. →Hacktivismus. Siehe http://sicherheitskultur.at/notizen_1_11.htm#rant

LUN: (Logical Unit Number) im →SCSI-Protokoll und Ablegern wie →Fibre Channel Protokoll (FCP) werden Komponenten eines Geräts (zumeist →Festplatten) mittels LUN adressiert. Beispiele für LUNs sind von einem Disksubsystem exportierte physikalische oder virtuelle Festplatten, sowie die Bandlaufwerke und Roboter und Bandbibliothek. Siehe →SAN

LUN Masking: schränkt die Sichtbarkeit von Festplatten ein, die ein Disksubsystem im Rahmen von →Enterprise Storage Systemen exportiert. Jeder Rechner „sieht“ nur die Festplatten, die ihm zugewiesen sind

Lustre: →File system für verteilte Speicherumgebungen, wird meist im Zusammenhang mit →UNIX (→Linux) für Hochleistungsanforderungen eingesetzt

M2M: Schlagwort, analog zu P2P (peer-to-peer), das dafür steht, dass in Zukunft zusätzlich zu der Tatsache, dass (fast) jeder Mensch jederzeit direkt vernetzt ist, auch (alle?) Dinge an dieser Vernetzung teilhaben werden. Ende 2012 wird die Zahl der vernetzten Dinge bereits auf 50 Milliarden geschätzt (→Webcams, Steuerungen im Industriebereich (→ ICS), →RFID-Chips in der Logistic). M2M ist auch die Basis von →Industrie 4.0

In Zukunft werden auch privat genutzte Geräte wie →Autos oder Haushaltsgeräte (→HAN), z.B. Thermostaten, aber auch Kühlschränke, Waschmaschinen, Kaffeemaschinen, etc. vernetzt sein und mit anderen Geräten, z.B. unseren →Smartphones kommunizieren. → Verwundbarkeiten in Autos, →Smartmetern und →medizinischen Geräten haben bereits aufgezeigt, dass z.B. →Authentisierungen fast nie sauber implementiert werden und daher viele neue →Angriffsmöglichkeiten entstehen. M2M wird nicht ohne Übergang zu →IPv6 möglich sein, das seine eigenen Probleme

aufwirft. Eines der vorgeschlagenen →Protokolle für M2M ist →OPC UA

MAC:

1) **MAC address:** (Media Access Control Address) Hardwareaedresse, die weltweit zentral vergeben wird und ein Gerät in einem lokalen IP-Netz eindeutig identifiziert. Diese Information wird z.T. zur Identifizierung und Autorisierung von Geräten genutzt, z.B. bei einigen →Wireless Networks. Sie kann aber leicht gefälscht werden, was bei Kabelmodems routinemäßig eingesetzt wird.

2) →**Mandatory Access Control**

3) →**Message Authentication Code**

4) **MAC-Times** - **M**odify, **A**ccess, **C**reation – im Bereich der IT-→Forensics bezeichnen MAC-Times die zu sichernden Zugriffszeiten zu allen Dateien. Diese sind zu sichern, bevor irgendwelche anderen Aktivitäten auf den Rechnern diese verfälschen könnten

Machine Learning: →Algorithmen, die aus →Daten mehr oder weniger selbständig lernen können. Genutzt z.B. für Mustererkennung. Verwandt mit →Neural Networks und ein Teilgebiet von →Artificial Intelligence und →Data Mining. Ein →OpenSource Projekt in diesem Umfeld ist TORCH. Siehe auch →Explainability, →DeepMind

Mac OS X: →Betriebssystem von Apple. Mac OS X (basierend auf →Unix) ist für PowerPC- und Intel-basierte Rechner. Es hat sich in den letzten Jahren leider als nicht resistent gegen →Schadsoftware herausgestellt und muss genauso regelmäßig aktualisiert werden wie →Windows Systeme. Viele der Sicherheitsfeatures von Windows →Vista und →Win 7 kommen erst 2011 in Mac OS X. Eine Variante von Mac OS wird als →iOS auf den →iPhones und →iPad verwendet. Siehe →Gatekeeper

Macro: aus →Programmiersprachen übernommener Begriff. Ein Script, das in einer „scriptable" →Anwendung für erweiterte Funktionalität sorgt. Unter Windows können solche Makros beliebigen Code ausführen, d.h. sie können großen Schaden anrichten. Beispiele für „scriptable" Anwendungen sind MS Word, MS Excel, MS Outlook, Adobe Acrobat. Siehe →Macrovirus

Macrovirus: →Virus, das die Makrofähigkeit von vielen Programmen (MS Word, MS Excel, Adobe, Outlook, etc.) ausnutzt. Mit Hilfe eines solchen →Makros lässt sich meist beliebiger Code auf einem System ausführen. Entsprechende Programme sollten so eingestellt sein, dass sie nur nach Rückfrage bei dem Anwender Makros ausführen

Magnetband: →Datenträger in Form eines Bandes, bei dem eine oder mehrere magnetisierbare Schichten auf einem nichtmagnetisierbaren Träger aufgebracht sind und bei dem die Information durch Magnetisierung aufgezeichnet wird

Magnetplatte: (auch Festplatte) →Datenträger in Form einer oder mehrerer Platten, bei denen magnetisierbare Schichten beidseitig auf einem nichtmagnetisierbaren Träger (oft Aluminium) aufgebracht sind und bei denen die Information durch Magnetisierung aufgezeichnet wird. Oft auch Festplatte genannt (im Gegensatz zu Floppy), Größe heute von 500 GB bis >2TB (Terabyte). Alternativ werden heute sehr oft →SSD eingesetzt. Siehe →S.M.A.R.T.

Magnetstreifen: Kurzes Stück →Magnetband auf einer →Kredit- oder →Bankomatkarte, auf dem →Daten gespeichert sind. Solche Daten sind sehr leicht fälschbar und daher sehr unsicher

Mail spoofing: Versenden von Nachrichten mit falschen Absenderangaben mit dem Ziel, unerkannt zu bleiben, oder vorzugeben jemand anders zu sein, wird bei →Spam und →Phishing oft verwendet. Siehe →spoofing

Mainframe: traditioneller Großrechner mit proprietären →Betriebssystem und monolithischer Architektur. Genutzt bis 1970 hauptsächlich im sog. Batch-Modus (d.h. Programme die mittels →Lochkarten oder andere Mechanismen gestartet wurden und keinen interaktiven Input von Menschen bekamen), bzw. ab dieser Zeit dann auch interaktiv, meist über sog. →Terminals, d.h. text-orientierte →Bildschirme. Der Hersteller mit einem dominierenden Marktanteil war IBM, andere Firmen wurden als BUNCH zusammengefasst: Burroughs, Univac, NCR, Control Data, Honeywell – alle diese Firmen sind heute nicht mehr im IT-Geschäft tätig, Ergebnis der Revolution durch →PCs und ab 1970 immer stärker werdender →Minicomputer wie die von DEC, Perkin Elmer, Silicon Graphics (SGI), Data General, Wang (die Größe typischerweise bis zu heutiger 19-Zoll Rack-Größe). Die meisten dieser Firmen existieren heute zwar nicht mehr, die Nachfolger dieser Rechner sind es aber, die heute als →Server bezeichnet werden

Maker: Technoslang für →3D Drucker, MakerBot ist eine Herstellerfirma

Malicious Code: (malicious, engl. bösartig) →Schadsoftware. Siehe → Malware-Schutz

MALINTENT: umstrittenes Projekt des →DHS um auf Grund von kontaktlos gemessenen Daten wie Körpertemperatur, Puls, Atemrhythmus und unwillkürliche Aktivitäten der Gesichtsmuskeln böse Absichten eines Menschen zu erkennen. Erinnert an die →"Precrime Detection" des Films →Minority Report. Siehe →Präventionsstaat

Malvertising: Kunstwort, das die Verteilung von →Schadsoftware (Malware) mittels Werbeeinblendungen auf reputablen →Websites beschreibt. Dafür wird Werbenetzwerken wie →Google's DoubleClick eine Anzeige „untergeschoben", deren Inhalt nachträglich

dynamisch durch die Malware ersetzt wird

Malware: →Schadsoftware, siehe →Malware-Schutz

Malware-Schutz: →Programme, die entweder auf einem →PC, einem →Server oder in Verbindung mit →Firewalls oder →Proxies Dateninhalte auf →Malware untersuchen. Die Kommunikation zwischen Firewalls und Scannern findet über das →CVP Protokoll statt. Herkömmliche Verfahren suchen in →Dateien nach Bit-→Pattern von bekannten „bösen" →Programmen (ergänzt durch →Heuristics), können damit jedoch neue →Schadsoftware und stoßen jedoch auf Grund von →Code Obfuscation mehr und mehr an ihre Grenzen (→UPX) und bei gezielten Angriffen (→targeted attacks) fast immer wirkungslos. Neue Methoden sind das Ausführen der Programme in →Sandboxes um zu sehen, was die Programme wirklich tun, bzw. das Überwachen der Geräte auf ungewöhnliche Aktivitäten wie Verbindungsaufbau zu →Botnets oder anderen →IP-Adressen die im Rahmen von Schadsoftware aufgefallen waren. Dazu gehört auch das Simulieren von →Browser-Verhalten bei der Ausführung von →JavaScript. Siehe, →Virus, →Decompression Bomb

Managed Service Provider: (MSP) übernehmen für kleinere Firmen alles dass, was IT-Administratoren tun würden, wenn sich das Unternehmen eine eigene IT-Abteilung leisten könnte. D.h. die Qualität dieser Firmen ist für die Sicherheit einer Firma ganz wichtig. Der Supply Chain Attack gegen Kaseya (einem Anbieter für Administrations-Software für MSPs) in 2021 hat gezeigt, dass solche Firmen schlimmstenfalls auch Einfallstore für Schadsoftware sein können.

Man-in-the-Browser: Spezialfall des →Man-in-the-Middle Angriffs bei dem sich die →Schadsoftware z.B. als Browser-Plugin (→BHO) im →Web-browser selbst installiert und damit Zugriff auf die Inhalte hat die im Browser angezeigt werden, auch dann, wenn die Sitzung über eine →HTTPS-Verbindung abgesichert war. Auf diese Weise können leicht →Passworte und andere vertrauliche Inhalte abgehört und an Angreifer übertragen werden

Man-in-the-Cloud: (MITC) Schlagwort der Sicherheitsfirma Minerva für eine neue Angriffsoption: Angreifer können durch Veränderungen in der Windows Registry bestehende Verbindungen zu →Cloud-Speicherdiensten wie →Dropbox, →Google Drive, OneDrive, etc. so umleiten, dass die Daten auf einen →Account unter der Kontrolle des Angreifers fließen. Ebenso können sie durch Übernahme des Accounts des Opfers Software auf dessen →PC übertragen. Dies ist möglich, da für diese →Zugriffe typischerweise kein →Passwort benötigt wird, sondern nur ein Langzeit →OAuth-→Token, der auf jedem anderen Gerät genutzt werden kann. D.h. das Transportieren dieses Tokens ermöglicht die unberechtigten Zugriffe

Man-in-the-Loop: →Human-in-the-Loop

Man-in-the-Mailbox: Schlagwort für Angriffe bei denen das natürliche Vertrauen von Benutzern gegenüber den Inhalten ihrer Mailbox, speziell von Kollegen oder guten Bekannten ausgenutzt wird. Im Gegensatz zu e-mail-basierten →Social Engineering →Angriffen wird hier der Inhalt von legitimen →E-Mails verändert, z.B. durch Einfügen von →URLs zu →Malware oder infizierte Anhänge

Man-in-the-Middle Angriff: (MITM) Angriff, bei dem ein Computer logisch zwischen zwei Kommunikationspartnern steht und auf diese Weise Daten mitlesen oder verändern kann, der Begriff wird seit 1995 genutzt. Der Angriff kann auch dann erreicht werden, wenn der Angreifer nicht physikalisch den Datenverkehr unterbrochen hat. Dies gelingt z.B. durch Veränderung der →DNS-Konfiguration für diese →Domain. Auf diese Weise können Informationen mitgelesen, abgefangen und verfälscht werden. Eine weitere Möglichkeit ist, wenn der Angreifer „auf" dem Gerät selbst sitzt und dort den Datenverkehr kontrolliert und verändert, z.B. durch einen →Trojaner (→Man-in-the-Browser) oder Nutzung von →PAC. In 2011 wurden die Internetsitzungen von 300 000 Benutzern im Iran über Veränderung der DNS-Einträge plus gefälschte →SSL-→Zertifikate umgeleitet und geknackt, d.h. ihre Passworte wurden bekannt.

Verhindert werden solche Angriffe über eine sichere →Authentisierung der Kommunikationspartner, z.B. mittels →SSL-Zertifikat. Dabei ist es wichtig, dass der Benutzer das Zertifikat der Website selbst überprüft. Da dies bei →Smartphone →Apps nicht möglich ist fällt diese Aufgabe der App selbst zu, wird aber sehr oft nicht korrekt erledigt und erlaubt damit solche MITM-Angriffe. Eine Methode um dies sicher zu implementieren ist →Certificate Pinning in der →Smartphone →App. Vorgeschlagene Verfahren gegen unautorisierte Zertifikate sind →OCSP, →HPKP, →Certificate Authority Authentication und →Certificate Transparency Siehe →ARP, →Phishing, →Man-on-the-Side http://sicherheitskultur.at/man_in_the-middle.htm

Man-in-the-Mobile: →Schadsoftware im → Smartphone die versucht, den →Datenverkehr zu überwachen oder zu ändern, bzw. die →mTAN-→SMS umzuleiten. Bei konsequenter Implementierung des →Sandbox-Konzept und Abwesenheit von →Jailbreak oder →Rooting ist der Zugriff auf den Datenverkehr nur schwer möglich, bei Jailbreak sehr wohl. Das Umleiten der SMS ist jedoch sehr leicht und wird von 2011 bereits eingesetzt

http://sicherheitskultur.at/man_in_the-middle.htm#mitmo

Mandantentrennung: (engl. Multi Tenancy)

Separierung von Daten unterschiedlicher juristischer Einheiten die auf einem gemeinsamen System verarbeitet werden, z.B. wie bei →Cloud Computing üblich, so dass ausgeschlossen ist, dass eine juristische Einheit, auch bei Programmfehlern, →Zugriff auf Daten von möglichen Mitbewerbern bekommt. Dies wird zwar heute noch zumeist über Filterung auf Grund eines Datenfeldes (z.B. Kunden-ID) durchgeführt, was aber nicht unter allen Umständen ausreichend ist, speziell wenn Daten aus unterschiedlichen Ländern verarbeitet werden und dabei →Law Enforcment Access berücksichtigt werden muss

Mandatory Access Control: (MAC) für den Level B1 des →ITSEC gefordertes Verfahren, bei dem Objekte (Daten, Bildschirme Datenspeicher, Drucker und Personen), sowohl nach Zugriffsleveln, als auch Zugriffskategorien eingestuft werden. Nur wenn alle diese Kriterien erfüllt sind, kann die gewünschte Aktion ausgeführt werden. Siehe →TCSEC, →MLS, →MULTICS

Man-on-the-Side: Variante zum →Man-in-the-Middle Angriff der u.a. von der →NSA eingesetzt wird um →Rechner zu infizieren. Dabei wird der Datenverkehr vom →Webbrowser zum →Webserver zusätzlich zu einem weiteren Webserver umgeleitet, der in die Antwort des korrekten Webserver zusätzliche Datenpakete einfügt, z.B. ein →Javascript, oder eine Verlinkung auf einen weiteren Webserver, von dem aus dann ein →Exploit zum Webbrowser gesendet wird

MAPI: (Messaging Application Programming Interface) ursprünglich von →Microsoft entwickelte Schnittstelle, über die ein Client Programm →E-Mail-orientierte Kommandos an einen „Message Store“, d.h. einen Mailserver absetzen kann. War bis MS Exchange 5.5 die Hauptzugriffsmethode für Microsoft

MapReduce: Programmierkonzept für die Auswertung sehr großer unstrukturierter Daten (→Big Data), ursprünglich von →Google für ihre →Suchmaschine entwickelt. Eine Implementierung ist →Pig

Marion: (Méthode d´Analyse des Risques Informatiques et d´Optimisation par Niveau) 1986 in Frankreich entwickelt und in dem Buch “La sécurité des réseaux; Méthodes et techniques” 1989 publiziert. Marion ist eine Applikation zur Beurteilung der →Informationssicherheit und basiert auf der gleichnamigen Methode, welche sich hauptsächlich in „frankophonen“ Gebieten etabliert und in vielen französischen Unternehmen bis heute im praktischen Einsatz bewährt hat

Market: Begriff für eine →Website, von der sog. →Apps für mobile Geräte wie → Smartphones heruntergeladen und auf den Geräten installiert werden können. Offizielle Markets implementieren einen begrenzten Schutz gegen →mobile Malware, „alternate markets“ wie sie für →iPhones nach einem →Jailbreak zur Verfügung stehen oder für →Android-Geräte grundsätzlich sind eine optimale Verteilmöglichkeit für →Schadsoftware für diese Geräte. Die Schadsoftware besteht ganz oft aus populären Apps, wie z.b. Spiele (→Games) die mittels →Re-engineering mit zusätzlichen Schadfunktionen versehen wurden. 2011 wird für Android von 50000 neuen Schadsoftware Apps pro Tag berichtet

Marktrisiko: für Banken die Gefahr der Wertverringerung eingegangener Positionen infolge adverser Marktbewegungen. Siehe →Basel II

Mashup: Kombination von Daten und/oder Anwendungen, zumeist mittels →Web 2.0 Technologien wie z.B. →AJAX. Beispiel ist das Anzeigen von Hotels von einer Reisewebsite in Google Earth, Verlinkung mit Flickr-Fotos oder →YouTube Videos. Durch die dadurch entstehende Komplexität können neue Sicherheitslücken entstehen

Maßnahmen: (engl. Measures & →Controls) Aktivitäten und Einrichtungen, die zum Schutz gegen Verletzungen der →Informationssicherheit genutzt werden.

Masquerade: →Spoofing

Massive Open Online Courses: (MOOC) Trend seit 2013/14 – sehr renomierte Universitäten, z.B. MIT und Harvard bieten Studiengänge online für einen weltweiten Studentenkreis, zum Teil kostenlos, bzw. nur die Prüfungen kosten Geld. Dies fällt unter das Stichwort →Disruption („disruptive innovation“)

Mastodon: Software für eine →Micro-Blogging-Implementierung auf der Basis des →ActivityPub →Protokolls, das dadurch →Daten mit vielen anderen Diensten austauschen kann, siehe →Fediverse

Match on Card: →MOC

Matrix:

1. (Multistate Anti-→Terrorism Information Exchange) US Überwachungsprojekt das eine große Zahl unterschiedlicher Quellen von personenbezogenen →Daten kombiniert. http://sicherheitskultur.at/privacy_loss.htm#privat
2. Als Matrix-Protokoll ein offener Standard für →Messaging in föderierten Umgebungen. D.h. nicht alle Nutzer müssen auf derselben Instanz angemeldet sein. Die Nutzer auf verschiedenen Matrix Servern können sich alle miteinander vernetzen (Federation). (Außer mit den separaten Netzen auf Matrix-Basis, wie das Bundeswehr-Netz, das Netz der französischen Behörden, etc.) Die Benutzernamen bestehen aus einer Kombination eines Namens mit dem Server auf dem dieser Account angelegt

wurde, z.B. StefanXYZ:matrix.org. Eine Telefonnummer ist im Gegensatz zu den meisten anderen Diensten nicht notwendig, d.h. es wird ein höherer Grad an →Anonymität erreicht. Die Software (siehe matrix.org) unterstützt →Chat, →voice over und Videotelephonie. Als Client wird vor allem →Element (https://element.io/) oder →Fractal eingesetzt. Es gibt bridges zu iMessage, →E-Mail, →Facebook Messenger, →Mastodon, →RSS, →Skype, →Telegram, →SMS, →Whatsapp, →WeChat, →IRC, →Slack, →XMPP

Maturity: (Reifegrad) es gibt eine Reihe von Modellen zur Darstellung des Reifegrads von Sicherheitsprozessen: →ISO/IEC 21827, →CMM, →SMM

Maus: Eingabegerät für Bildschirmpositionen, alternativ dazu Trackpad, Touch Screen, o.ä. Heute oft auch drahtlos, bei →Servern oft über →KVM-Switches. Es gibt →Angriffe bei denen ein externes Programm, z.B. auf einem →USB-Stick, Maus- und Tastatur-Eingaben simuliert und auf diese Weise →Zugriff zum Rechner bekommt

MBR: (Master Boot Record) erster Datenblock eines partitionierten Speichermediums, genutzt für den Start des →Rechners, wird oft von →Schadsoftware genutzt um sich zu verstecken und sicher gestartet zu werden. Siehe →root kit, →Mebroot, →secure boot

MBS: (Multi Bank Standard) standardisiertes Protokoll, bei dem (hauptsächlich kommerzielle) Bankkunden mittels eines →Client-Programms auf ihrem Rechner mit mehr als einer Bank Daten austauschen können, meist direkt aus den jeweiligen Buchhaltungsprogrammen (FIBU) heraus, auch →Telebanking genannt. Gilt als sicherer als →E-Banking übers →Internet

MBSA: (→Microsoft Baseline Security Analyzer) analysiert den →Patch-Zustand von Windows-Systemen und Konfigurationsfehler. Benutzt →HFNetChk

MCP: (Mobile Contactless Payment) Anwendung auf →UICC-Karten, die über →NFC kommunizieren soll und →Kredit- und →Bankomatkarten ersetzen soll. Dabei hält der Benutzer sein →Handy in die Nähe des Lesegeräts und gibt über einen Dialog auf dem Handy die Zahlung frei. Technisch wird dafür eine Application auf der UICC installiert, die über ein →SIM-Toolkit mit Software auf dem Handy kommunizieren kann. Außerdem wird vermutlich noch ein Benutzer-Interface auf dem Handy installiert. Installation und Aktualisierungen sollen auch OTA (over the air) möglich sein. Sicherheit soll über die →tamper-resistance der UICC entstehen, allerdings ist noch nicht klar, wie das bei einem Handy mit →Jail-break erreicht werden kann

MD5: →Hash-Funktion, wie sie bei der digitalen →Signatur eingesetzt wird. Mit einer Hash-Funktion wird aus einem langen Dokument ein kurzer Wert berechnet, der sich auch bei sehr geringen Änderungen im Dokument sehr stark verändert. Dadurch kann die →Integrität, die Unversehrtheit eines Dokumentes, festgestellt werden. Die Sicherheit von MD5 wurde 2005 in Frage gestellt und Ende 2008 geknackt, es wird leider immer noch in →SSL-Zertifikaten verwendet

MDA: (Mobile Digital Assistant) bis ca. 2010 ein →PDA mit der zusätzlichen Funktionalität eines →Mobiltelefons

MDM: →Mobile Device Management

Meat Puppet: Gegensatz zu →Sock puppet (d.h. 1 Person spielt mehrere digitale Identitäten bei Online-Diskussionen). Bei Meat Puppet wird eine Person dafür bezahlt wird, Meinungen online zu vertreten, z.B. in →Social Networks (z.B. Beträge auf Firmenseiten) oder in Diskussionsforen (→Chat Room). Wird vom US-Militär unter dem Begriff „Digital Engagement“ eingesetzt

Mebroot: generische Software-Plattform für die →Infektion von →Rechnern auf der Ebene von →MBRs. Erlaubt das Installieren, De-Installieren und Aktivieren beliebigen von →Schadsoftware-Modulen

Mechanical Turk: Service von →Amazon, bei der nicht-automatisierbare Arbeiten weltweit Vergeben werden können, oft gegen extreme geringe Bezahlung. Dadurch stehen in Ländern und Städten mit guter →Internet-Anbindung billige Arbeitskräfte für Arbeiten zur Verfügung, die im →Web implementierbar sind. Dieses Geschäftsmodell wird heute von vielen anderen Firmen ebenfalls implementiert (→Crowdsourcing). So haben die Social Networks wie →Facebook und →Youtube das Bewerten und Löschen von →Hasspostings sehr oft in Länder ausgelagert in denen Arbeitskräfte billiger sind. Solche Geschäftsmodelle werden zum Teil auch für →Angriffe, z.B. das Knacken von →CAPTCHAs und →Spamverteilung in → Social Networks und →Blogs genutzt, siehe auch Crowdsourcing und →Astroturfing. Der Name bezieht sich auf einen angeblichen Schachroboter aus dem 18.Jhdt. http://de.wikipedia.org/wiki/Schacht%C3%BCrke

Media Gateway: bei →VoIP Systemen die Umsetzung von inkompatiblen Formaten, z.B. →SIP- oder →H.323-Signalling nach →SS7 und den elektronischen Sprachdaten, z.B in →PSTN- oder mobile Formate wie →GSM oder →NGN. →Schwachstellen in VoIP-Systemen können so auch traditionelle Telefonnetze (→PSTN) bedrohen, anderseits können diese Gateways auch Angriffspunkt sein. Siehe →MGCP

Medienbruch: Wechsel eines informationstragenden Medium bei einem Datenaustausch oder Datenverarbeitung, z.B. eine Neueingabe

von →Daten, bei der es zu Verletzungen der →Integrität kommen kann. Sicherheitstechnisch manchmal erwünscht, z.B. →TAN-Versand via →SMS oder beim Konzept des →Terminalservers oder →SSL/VPN, da durch den Bruch ein automatisierter →Angriff sehr erschwert wird

Medieninhaber: Personen die Inhalte kommunizieren. Sie sind für diese Inhalte verantwortlich. Von Medien im juristischen Sinne versteht man jedes Mittel zur Verbreitung von Mitteilungen oder Darbietungen mit gedanklichem Inhalt in Wort, Schrift, Ton oder Bild an einen größeren Personenkreis (dies kann bereits ab 10 Personen greifen). Dies kann Newsletter, →Webseiten und →Social Network Präsenzen betreffen. Wenn andere Personen dort illegale Inhalte verbreiten so reicht auf Basis des →Medienprivilegs ein zeitnahes Entfernen nach Kenntnisnahme

Medienprivileg: um die Pressefreiheit zu schützen werden einige Punkte des →Datenschutzes nicht auf sog. Medien angewandt. Darunter wird auch verstanden, dass es Medienbetreiber nur dann für Inhalte haften die auf ihrer →Website veröffentlicht werden, wenn sie nach einer Information über illegale Inhalte diese nicht zeitnah entfernt haben. Dies betrifft z.B. auch Personen, auf deren →Social Network Präsenz andere Personen Inhalte posten

Medizinische Geräte: Solche Geräte sind heute zumeist →Computer, die sehr oft vernetzt sind und allen Gefahren ausgesetzt sind, die für Computer gelten. Sie enthalten oft sehr viele →Verwundbarkeiten, da die Entwickler oft auf Sicherheit keinen Wert legen und die Software auf sehr veralteten Systemen beruht, die sehr oft niemals mit Sicherheits-→Patches aktualisiert werden. Ein spezielles Problem sind →IMDs (implanted medical devices) die über drahtlose Schnittstellen angegriffen werden können. Siehe →Internet of Things

Mehrwertnummern: Möglichkeit zum Ausnutzen von Infektionen auf →Smartphones durch Anruf oder SMS an solche Nummern, bei denen jeder Anruf oder jedes SMS einen hohen Betrag kosten kann. Der Benutzer erkennt diesen →Angriff oft erst an der hohen Handyrechnung

Meldestelle: in der Informationssicherheit Stelle bei der unerwünschte Inhalte und kriminelle Aktivitäten im →Internet wie z.B. Kinderpornographie gemeldet werden können: http://sicherheitskultur.at/hilfe_im_internet.htm

Meme: ursprünglich geprägt von Richard Dawkins in seinem Buch „The Selfish Gene“ um (analog zur Weitergabe von biologischen Eigenschaften durch Gene), wie Weitergabe von Ideen, Konzepten, Kunst, Modeerscheinungen und Erfindungen im Rahmen von „Kultur“ zu beschreiben. Wie bei den Genen findet eine Veränderung bei der Weitergabe statt. Im 21.Jhdt. vor allem als Web-Meme verstanden. Dies sind Postings, die eine hohe Popularität erreichen. Beispiel sind z.B. die LOLcats die von →4chan populär gemacht wurden. Andere Beispiele sind Gangnam Style Videos, Doge, Starwars Kid, Tron Guy, Obama Rage Face. Wenn Ihnen diese Begriffe nichts sagen, dann liegt es daran, dass Web-Memes hauptsächlich in-side Jokes sind, mit denen der Re-Poster sagt, dass er den Witz versteht und „dazu gehört“.

Im Rahmen der →Intelligence Explosion Diskussion sind Meme ein „2nd replicator“. So wie nach der Selfish Gene Theorie die Gene 1st replicator sind (sie „benutzen“ Organismen um weitergegeben zu werden), so „nutzen“ Meme die Menschen für ihre Weitergabe und Mutation. Als 3rd replicator werden Teme bezeichnet (technological meme). Dies sind technologische Weiterentwicklungen, die im Rahmen von →artificial intelligence von Maschine zu Maschine übertragen werden.

Memory: →Speicher

Menstruationsapp: siehe →Gesundheitsapp

Mental Security Model: Repräsentation des (vermuteten) Sicherheitskonzepts im Kopf des →Benutzers. Je genauer dies mit der Realität übereinstimmt, desto besser „funktioniert“ das Sicherheitskonzept. Und je genauer dieses Bild des Laien mit dem des Experten übereinstimmt, desto besser kann dieser mit dem Laien über diese Fragen kommunizieren. Die für diese Kommunikation genutzten Metaphern sind physische Sicherheit (→Schlüssel, →Firewall, →Intrusion Prevention), Medizin (→Infektion, →Virus, →Wurm), Kriminalität (→Malicious Code), Krieg (→DMZ)

Mesh Routing / Mesh Networking: dynamisches Routing mit dessen Hilfe ein →IP-Netz ohne zentrale Komponenten aufgebaut werden kann, z.B. durch Verwendung von →OLSR zwischen →Handys. Wird zum Teil eingesetzt um alternative Netze zu implementieren, die nicht von Regierung und anderen kontrolliert werden. Siehe auch →Internet im Koffer

In Österreich wird solche Technik durch den Verein →FunkFeuer eingesetzt um in mehreren Städten eine Internet-Anbindung für Bürger zu implementieren. In Berlin und anderen Städten gibt es Implementierungen der Freifunk-Gemeinschaft

Message Authentication Code: (MAC) kryptogrphascher →Algorithmus, der aus einem geheimen →Schlüssel und einer Informationseinheit beliebiger Länge eine kurze Informationseinheit erstellt, die die →Integrität der Übertragung und durch den Schlüssel auch die →Authentizität (d.h. die Korrektheit des Absenders) verfiziiert. Verwandt zu →Hash Funktion, die allerdings keinen Schlüssel verwendet und dadurch nur die Integrität bestätigen können.

Siehe →HMAC

Messaging:

1) Überbegriff für →Programme, wie →ICQ, →IRC, →Pidgin, Yahoo! Messenger, AOL Instant Messenger iMessage, →Blackberry Messenger, →Skype und MSN Messenger, aber auch →Smartphone →Apps wie →WhatsApp, →Signal, →Riot, →Telegram, →WeChat, eBuddy XMS, WowTalk, Tango, →Snapchat mit deren Hilfe zwei oder mehre Personen miteinander durch Eintippen von Texten →Chatten oder Texte auszutauschen (und oft auch Sprache, Videoströme oder beliebige →Dateien austauschen können). Im Gegensatz zu →Chat Rooms kennen sich die beteiligten Personen in den meisten Fällen bereits.

Für den Nutzen solcher System gilt →Metcalfe's Law, d.h. der Nutzen (und Wert) des Systems steigt mit dem Quadrat der Nutzerzahl. Dies führt dazu, dass es neue Anwendungen gegen zahlreich genutzte recht schwer haben.

Alle diese Systeme erlauben auch den Austausch von Dateien und stellen daher bei falscher Nutzung ein Sicherheitsrisiko dar. Würmer oder auch →SPIM (SPAM over IM) verbreiten sich, indem sie einen →Link an alle Personen in der „Buddy List" des Rechners versenden. Dies erfordert das Klicken des Anwenders auf den so empfangenen Link, dies geschieht aber oft, weil der Link anscheinend von einem Bekannten kommt.

Eine andere Angriffstechnik verwendet Dateitransfer. Messaging Dienste werden zunehmend auch im geschäftlichen Bereich und auch sehr oft zum Steuern von →Botnets verwendet.

Schwierig ist bei den Smartphone Apps zumeist die sichere →Identifizierung und →Authentisierung der Benutzer. Mittels →Enumeration können viele Teilnehmer gefunden werden. Dadurch ist es leicht andere Benutzer zu simulieren (und z.B. →Spam zu versenden) oder deren Botschaften zu empfangen.

Strafverfolgungsbehörden fordern den →Zugang zu diesen Dialogen (zumindest nach einem entsprechenden Richterbeschluss, → lawful intercept). Dies ist aber technisch nicht möglich, wenn sie bei Skype oder der Firmenlösung von Blackberry der Datenaustausch direkt zwischen den Geräten passiert (→peer-to-peer) und mit einem nicht-zentralen verschlüsselt ist. Siehe →Zombie, →XMPP

2) Austausch von →Daten zwischen IT-Systemen mittels spezialisierter Software zumeist in lokalen Netzen, die für die →Vertraulichkeit, →Integrität (keine Veränderung, keine Duplizierung, kein Verlust), →Authentizität und andere Sicherheitsanforderungen sorgt. Beispiele sind →MQ-Series, →Tibco, →JMS, →ESB. Diese Systeme arbeiten zumeist asynchron, d.h. verfügen über iterne Zwischenspeicher und unterstützen z.T. auch Formatumwandlungen. Konzepte sind point-to-point, broadcast und →publish-subscribe. Verwandte Schlagworte sind →MOM und →EAM. Abgegrenzt zu →EDI zum Austausch zwischen entfernten und heterogenen Systemen und →Client-Server Kommunikation

Messenger: →Messaging Dienst

Meta: neuer Name von →Facebook. Hergeleitet von Metaverse, einer fiktiven, heute oft virtuellen, ‚Welt' wie z.B. →Second Life

Metadaten: →Informationen, die die eigentlichen →Daten beschreiben. Beispiel ist →ID3 in →MP3 oder →EXIF in →JPEG- und →TIFF-Bildern, aber auch die „Eigenschaften" in allen MS-Office Dateien oder auch →Image Tags. Metadaten können ungewollt Informationen preisgeben, z.B. Serien-Nr. der Kamera, Datum und Ort der Aufnahme, Namen der fotografierten Personen. Siehe auch →Mujahedeen Secrets. Ebenfalls zu Metadaten gehören die →Verbindungsdaten von →Messaging Diensten oder Telefonaten, die Auskunft über das soziale Netz einer Person, d.h. seinen →Social Graph geben können

Metasploit: →Open-Source Projekt rund um →Penetrationtest, →IDS und →Schwachstellenmanagement

Meta Tags: für den Benutzer nicht direkt sichtbare Informationen einer →Webseite im →HTML-Format, die von →Webbrowsern und vor allem von →Suchmaschinen interpretiert wird. Kann für →Traffic Diversion genutzt werden

Metcalfe's law: Faustregel über das Kosten-Nutzenverhältnis von Kommunikationssystemen (z.B. Telefonnetz, →Social Network oder →Messaging App. Die Regel besagt, dass der Nutzen eines Kommunikationssystems proportional zur Anzahl der möglichen Verbindungen zwischen den Teilnehmern (also etwa dem Quadrat der Teilnehmerzahl). Dies führt dazu, dass es neue Anwendungen gegen zahlreich genutzte recht schwer haben.

Es wird spekuliert, dass auch beim Thema →Home Office relevant sein könnte. Vor 2020 fanden Meetings nur ausnahmsweise über →Webkonferenzsysteme statt, jedes Arbeiten von zu Hause zwang alle anderen ebenfalls zur Nutzung des Systems und die remote Nutzer waren nicht voll integriert. In 2020 wurde „remote" zum Standard und dies machte es einfacher für den Einzelnen.

Metrik: mathematische Verfahren zum bestimmen von Abständen. In →IP-Netzen z.B. Angabe des Abstandes in Zahl der „→hops", d.h. der →Router zwischen Quelle und Ziel, nicht der räumlichen Entfernung. Bei →Fuzzy Hashing Bestimmung der Ähnlichkeit von 2 digitalen Objekten. In der Informationssicher-

heit: quantitatives Messen von Sicherheitsaspekten. Siehe →KPI, →itSMF, →ISO 27004, →OSSTMM

Metro: Bezeichnung für die Oberfläche von WP7 und Windows 8. Es enthält auch weitere Sicherheitsfeatures über →VISTA hinaus, z.B. werden native Metro →Apps (wie bei → Android) in einem eigenen Benutzer →Account ausgeführt und haben dadurch unabhängig von der →Sandbox keinen →Zugriff auf die Objekte der anderen Apps. Verbunden mit Einschränkungen des App →Stores ergibt sich dadurch ein Sicherheitsniveau vergleichbar wie →iOS

MFA: →Multi-Faktor Authentication

MFD: (multi-functional device) →Multifunktionsprinter)

MGCP: (Media Gateway Control Protocol) Kommunikationsprotokoll, eingesetzt bei →VoIP zur Steuerung von →Media Gateways

MIC: (Mandatory Integrity Control) →Integrity Level

Micro-blogging: →Blogging von sehr kurzen Texten, z.B. bei →Twitter 140 Zeichen, →Mastodon 420 Zeichen, Hubzilla, →Weibo, →Xing. Durch die Nutzung von →URL-Shortening können trotzdem lange →URLs versendet werden, die auf „gefährliche" →Websites verweisen. Dieses Problem lösen einige Dienste, indem URLs immer als eine konstante Länge gezählt werden. Die einzelnen Postings sind entweder privat oder öffentlich zugänglich und werden wie chronologisch dargestellt. Blogging und Mikroblogging sind beide eine Form von →Social Networking. Im Gegensatz dazu →Messaging, bei dem immer eine feste Adressatengruppe (einzeln oder als Gruppe adressiert wird)

Microsoft: (MS) In der Vergangenheit wegen der Sicherheit seiner Software oft gescholtener Monopolist, der seit ca. 2000 viele Sicherheits-Initiativen gestartet hat (z.B. Schulungen für ALLE Entwickler), die sich seit ca. 2004 mit Windows XP SP2 in seinen Produkten niederschlagen. Mit →Vista wurden →UAC, →ASLR und →DEP eingeführt. Mittlerweile liegen →Adobe mit →Flash und dem →PDF-Reader, aber auch →Apple bei den Unsicherheitsstatistiken vor MS. Mit Windows 8 und →Metro werden weitere Sicherheitsfeatures eingeführt, die besser sind als vergleichbare bei →iOS.

Microsoft ist sehr aktiv bei der aktiven Bekämpfung von -→Botnets auf juristischen und technischen Wegen. Sie setzen dabei auf verschiedene Gesetze, u.a. auf →RICO. Siehe auch →SDL, →Threat Modelling, →OneCare, →MSRT, →MBSA, →MMC, →MOF, →SCOM, →SCCM, →NGSCB, →Patch Tuesday, →NEAT, →Xbox, →LinkedIn.

Microsoft ist über Microsoft Azure auch im →Cloud Hosting sehr aktiv, siehe z.B. →Kubernetes. In den letzten Jahren versucht Microsoft vom Verkauf ihrer Office Software zur Nutzung von Office 365 als monatlich zahlbarer Cloud-Dienst zu kommen

MIDlet: →Java-Programme für →Embedded Systems wie →Smartphones, basierend auf J2ME (Micro Edition). Oft sind dies Spiele und solche Programme können ein Sicherheitsrisiko darstellen, wenn sie aus ihrer →Sandbox herauskommen und die Kommunikationsfähigkeiten der Geräte ansprechen

Middleware: bei der Programmierung von →Computern genutzte Softwarekomponenten, oft in der Form eines →APIs, das zwischen dem →Kernel und den Anwendungsroutinen sitzt. Diese Komponenten erleichtern dem Entwickler die Arbeit, da komplexe Funktionen wie Voice Recognition oder das Ansprechen von komplexen Geräten auf einfache Schnittstellen reduziert werden. Auch Kommunikation mit anderen Geräten im Netz kann auf diese Weise für den Programmierer vereinfacht werden. Auch viele Sicherheitsfunktionen, wie z.B. →Authentisierung werden meist über entsprechende Middleware implementiert

MiFID: (Markets in Financial Instruments Directive 2004/39/EC) Harmonisierung der Finanzmärkte im europäischen Binnenmarkt. Sie stellt auch Anforderungen an die Dokumentation von Finanzmarktgeschäften und daraus können sich auch Anforderungen an die Nachvollziehbarkeit der IT ergeben

MIME: (Multipurpose Internet Mail Extension) Erweiterung des ursprünglichen →SMTP →E-Mail Formates, so dass auch die Verwendung von Umlauten und nichtenglischen Inhalten, sowie binäre Attachments unterstützt werden. Dabei werden diese Inhalte durch entsprechende Kodierung in eine Form gebracht, bei der in jedem Byte nur die ersten 7-bit genutzt werden. Durch die Erweiterung zu →S/MIME können Sicherheitsaspekte berücksichtigt werden. 1992 von der →IETF standardisiert

Minimalprinzip: →Sicherheitskonzept, dass →Anwendungen mit den geringsten notwendigen Rechten ausgestattet sein sollten (principle of least privilege)

Minicomputer: Klasse von →Computern die ab ca. 1970 die →Mainframes in vielen Bereichen abgelöst hatten. Wurden dann ihrerseits durch die →PCs abgelöst. Anbieter waren DEC, Perkin Elmer, Silicon Graphics, Data General, Wang (die Größe typischerweise bis zu heutiger 19-Zoll Rack-Größe).

Minority Report: Film von Spielberg nach einer Geschichte von P.K.Dick bei der es um →Precrime Detection geht, d.h. das Vereiteln eines Verbrechens bevor es begangen wird. 2008 wird dies vom →DHS-Programm →MALINTENT oder → EDVIRSP versucht umzusetzen

MINT: Schlagwort und Abkürzung für die

Fächer Mathematik, Informatik, Naturwissenschaft, Technik. Wird i.d.Regel verwendet wenn es um darum geht, dass dies zu wenig in den Schulen gefördert wird, oder um den geringen Frauenanteil in diesem Fächern

Mirror, Mirroring: (disk mirroring, engl. Plattenspiegelung) Methode, bei der durch geeignete Technologie auf Hard- oder Software-Ebene alle Daten auf mindestens 2 →Magnetplatten geschrieben werden. Dies kann synchron oder asynchron (mit Zeitverzögerung) geschehen. Siehe →split, →Hochverfügbarkeit, →Disaster Recovery, →Synchronisation

Mission Creep: wenn sich der Umfang eines Projektes oder einer Aufgabe nachträglich verändert, als Beispiele werden oft militärische Einsätze genannt, die sich langsam immer mehr ausgeweitet haben. Auch sich langsam aber stetig erweiternde Aufgaben oder Befugnisse einer Organisation gehören zu diesem Effekt (z.B. Abhörbefugnisse von Sicherheitsbehörden). Sehr verwandt ist Scope Creep im Projektmanagement: einem laufenden Projekt werden nachträglich zusätzliche Aufgaben gegeben

In der IT auch sehr häufiger Effekt: →Daten die für einen begrenzten Zweck gesammelt wurden, werden später auch für andere Zwecke genutzt Dies führt z.B. zu einer Aushöhlung des →Datenschutzes und ist in den europäischen →Datenschutzgesetzen ausdrücklich verboten („Zweckbindung der Daten“)

MITB: →Man-in-the-Browser Angriff

MITM: →Man-in-the-Middle Angriff

MITRE: non-profit US-Organiation (Abspaltung von MIT) im Dienst von US-Behörden, auch in D. aktiv, spezialisiert auf IT-Sicherheit, bekannt für die →CVE-Liste

MITRE ATT&CK Matrix: pflegt sehr systematische Konzepte von IT-→Angriffen gegen Unternehmen, Netze und →Smartphones mit sehr detaillierten Details zu den Angriffen und den jeweils genutzten Angriffswerkzeugen und –techniken, gegliedert nach Reconnaissance, Resource Development, Initial →Access, Execution, →Persistence, →Privilege Escalation. https://attack.mitre.org/versions/v8/

Mix: 1981 entwickeltes Konzept für die →Anonymisierung von →Nachrichten in Netzen in zentralen Servern, die durch Mischung von Nachrichtenteile unterschiedlichen Ursprungs den Bezug zur Quelle der Nachricht verwischen, siehe →JAP

MHP: (Multimedia Home Platform) vorgeschlagener Standard für Übertragung und Darstellung interaktiver Inhalte im digitalen Fernsehen auf Basis von →Java. Dabei werden auch Features wie das Sperren der Fernbedienung während Werbeblöcken diskutiert. →DVP

MLS: (Multi-Level Security) →TCSEC

MMC: (→Microsoft Management Console) →Programm in Windows 2000 (und höher). Gibt eine einheitliche Sicht zu Management-Diensten auf dem →PC selbst, bei Nutzung von →ADS auch auf die davon verwalteten Rechner

MMORPG: (Massively Multiplayer Online Role-Playing →Game (→RPG), auch MMOG oder MMO) über das →Internet sehr weit vernetzte Spiele (→World of Warcraft mit 4,5 Mio. Benutzern), die wegen der wachsenden monetären Möglichkeiten Ziel von →Malware werden. Zum einen können das interne →DoS-Angriffe sein (auf Grund der wachsenden Gestaltungsmöglichkeiten durch die Benutzer), aber auch der Diebstahl von Accounts oder Betrug bei dem Verkauf von →Avataren oder ihren Ausstattungen. Außerdem berichtet →Edward Snowden, dass auch die Geheimdienste in MMORPGs aktiv sind, wenn sie dort Kommunikationskanäle ihrer Zielpersonen vermuten

MMS:
1) (Multimedia Messaging Service) Nachfolger von →SMS für den Austausch von Nachrichten zwischen →Handys, der die Limitierung auf 160 Zeichen nicht hat. Ein MMS darf aus beliebig vielen Anhängen beliebigen Typs bestehen. Damit ist es möglich, auch Bilder oder Videosequenzen, aber auch ausführbare Programme an einen oder mehrere Empfänger zu verschicken. Eine prinzipielle Größenbeschränkung gibt es nicht. Dies kann, speziell bei entsprechenden →Schwachstellen der jeweiligen →Handys, oder auch →Social Engineering, zu Angriffen genutzt werden
2) (Managed Security Services) Dienstleistungen wie →IDS/IPS oder →dDoS Prevention und/oder Mitigation, die von externen Anbietern erbracht werden

Mobile Horizon:→Virtualisierungslösungen für →Smartphones von →VMware. Auf →Android wird dabei ein virtuelles Android-System als ‚guest‘ unter einem regulären (benutzer-kontrollierten) →Android von Hersteller/ Mobilfunkanbieter. Problem ist dabei →Jail-breaking. Auf →iOS ist dies aus juristischen Gründen nicht möglich, daher wird →App Wrapping verwendet. Konkurenten sind dabei Good Technologies und Touchdown von NitroDesk

Mobile IP: RFC2002, standardisiert die Möglichkeit, dass ein mobiles Gerät, z.B. →Smartphone oder →PDA, das mit einem lokalen Netz verbunden ist, seine Verbindung und seine →IP-Adresse behalten kann, während der Benutzer sich aus der Reichweite des ersten Netzes entfernt. Diese Funktionalität war bisher nur bei →GSM- und →UMTS-Netzen implementiert

Mobiler Code: neu aufgenommen in die →ISO 17799-2005. Dort ist mit diesem Begriff nicht →Java, →ActiveX o.ä. gemeint, das vom Benutzer erst geladen werden muss, sondern

ein Programmcode, der sich selbstständig bewegt, z.B. mobile Agenten

Mobile Device Management: (MDM) Software zum Verwalten einer großen Zahl von mobilen Geräten, zumeist →Smartphones. Die Features sind: Support von

- Verwaltung der Geräte und Status-Übersicht (OS-Level, etc.)
- Verteilung und Kontrolle von lokalen Einstellungen
- Erzwingung von Security Policies
- Löschen von Daten, Verteilung von Security Zertifikaten (→SCEP)
- Kontrolle über die Active Sync Settings, Möglichkeit der Löschung der Firmen-Mails
- Kontrolle der Security Settings und rules, z.B. jailbreak Erkennung, etc.
- Begrenzte Kontrolle über die installierten Apps
- Unterstützung von Remote Support durch Bildschirmübernahme

Mobile Malware: →Schadsoftware die für mobile Geräte, d.h. →Smartphone, →Tabletts, etc. konzipiert ist.

Mobilgerät: meist ist ein →Mobiltelefon gemeint, aber streng genommen fallen darunter auch die früheren →PDAs und ähnliche mobile Geräte

Mobiltelefon: im deutschsprachigen Raum →Handy, d.h. entweder ein →Smartphone oder ein sog. →Feature Phone

MOC: (Match on Card) Technologie in einigen →COS (Smartcard Operating Systems), bei der im Smartcard Leser ein →Fingerprint Leser integriert ist, der die Eingabe eines →PINs zum „Öffnen“ der Smartcard ersetzt

Modem: (Modulator-Demodulator) Geräte um über eine analoge Verbindung, z.B. Telefonleitung (→POT), digitale Daten zu übertragen. Für besonders sichere Übertragungen ist auch der Einsatz von verschlüsselnden Modems möglich. Bei diesen wird der gesamte Datenverkehr automatisch und für den →Benutzer und die →Systeme transparent verschlüsselt. Siehe →Callback, →BBS, →Terminal

MOF: (→Microsoft Operations Framework) Microsoft Implementierung von →ITIL

MOICE: (Microsoft Office Isolated Conversion Environment) →Sandbox-Technology das seit 2010 auch von Adobe eingesetzt wird

MOM: 1) (→Microsoft Operations Monitor) System-Überwachungstool, heute →SCOM

2) (Message-oriented →Middleware) →Messaging

Money Mule: oft unschuldige, d.h. naive Helfer bei →Cybercrime, die die eigentliche Geldüberweisung zum Täter im Ausland vornehmen. Beliebt sind Bargeldüberweisungen, z.B. durch →Western Union oder →ACH Transfers. Money Mules werden über Annoncen auf Job-Plattformen und →Spam-Mails rekrutiert (“Earn Thousands Working at Home!”). Sie haben nur eine kurze Kariere, weil ihr Konto für die Opfer klar erkennbar ist und sie daher eine Anklage wg. Beihilfe zum Betrug erwarten sowie eine Schadenersatzforderung. Sog. Mule Control Panel sind →Websites auf denen die Daten der angeworbenen Personen verwaltet werden und auf die die →Schadsoftware des infizierten →PCs (heute zumeist →Man-in-the-Browser) zugreift wenn sich die Gelegenheit für eine betrügerische Überweisung bietet

Monitoring: Überwachung von sicherheitsrelevanten Aspekten eines Betriebs und soll zu →Alarmen und dann →Vorfallsbehandlung führen. Solche Events können über →SNMP gemeldet werden, durch Software wie →Tripwire, →vulnerability scans, Software→Agents oder durch automatisierte Auswertung von →Logfiles. Problematisch sind →False Positives

MONKEYCALENDER: Programm der →NSA zur Manipulation von →SIM-Karten

MOOC: →Massive Open Online Courses

MOS: (Mean opinion score) numerische Angabe (1-5) für die →Qualität von Ton- und Video-Übertragungen, z.B. →VoIP. Kann subjektiv bestimmt werden oder über technische Messungen von packet delay, packet loss and jitter (unregelmäßige Verzögerungen). Siehe →RTCP

MOSS: (Microsoft Office SharePoint Server) Web-Anwendung, die unterschiedliche Services aus dem Office-Bereich über →https auch firmenübergreifend Verfügbar macht

Motherboard: Hauptplatine eines →Computers (oder anderen softwaregesteuerten Gerätes), auf dem die einzelnen Komponenten wie →CPU, →Speicher, Interfaces zu Erweiterungskarten, z.B. Netzwerkkarten, etc. angeschlossen sind, oft über Sockel die ein Auswechseln erlauben. Auch das →BIOS-Programm ist auf einem →EPROM Chip auf dem Motherboard. Verbindung zu anderen Geräten zumeist über einen →Bus

Mpack: 2007 sehr fortgeschrittenes →Angriffstool russischen Ursprungs zur Erzeugung von →bots, bei dem der Autor eine 45-50% Erfolgsgarantie gibt. Verwendet eine umfangreiche Palette von →Schwachstellen. Preis ca. 1000$

M-PESA: mobiles Zahlungssystem in Kenia (und anderen Ländern) das auf dem →SIM Application Toolkit (STK) Erweiterungen beruht. Es wird seit 2007 von Vodaphone sehr erfolgreich betrieben. Es beruht darauf, dass mittels →PIN-gesicherten verschlüsselten → SMS ein Guthaben (Airtime genannt) innerhalb der →SIM-Karte des →Handys gespeichert wird und zu anderen SIM-Karten übertragen werden kann. Barauszahlungen sind bei Tankstellen, Supermärkten, Straßenkiosken,

Internetcafés und Handyläden möglich. Vorteil ist, dass dies auch Menschen ohne Bankkonto eine einfache Teilnahme am bargeldlosen Geschäftsleben ermöglicht, kritisiert wird, dass speziell in Ländern in denen keine Konkurrenz besteht die Gebühren sehr hoch sein können

MPLS: (Multiprotocol Label Switching) Protokoll für verbindungsorientierte Vermittlung in verbindungslosen →WANs (→Layer 3). Es entsteht eine Form von →VPN, allerdings ohne →Verschlüsselung. Es wird →VRF eingesetzt

MRTD: (machine readable travel document) Ausweise und Reisepässe, deren Inhalt maschinell ausgelesen werden kann. Meist verwendet für die neuen →biometrischen Reisepässe, allerdings sind die europäischen Pässe durch den Einsatz der →MRZ schon sehr lang maschinell lesbar. Siehe →ePass, →FIDIS

MRZ: (Machine Readable Zone) Bereich in Pässen, der mittels →OCR gelesen werden kann. Er enthält u.a. Namen, Passnummer, Geschlecht und Ablaufdatum. Dieser Bereich wird, wenn bei →RFID-Pässen →BAS eingesetzt wird, als →Schlüssel zur →Verschlüsselung der auf dem Chip gespeicherten Daten eingesetzt

MP3: (MPEG-1 Audio →Layer-3) Verfahren zur Kodierung und Komprimierung von Musik und Sprache in digitaler Form. Durch die Möglichkeit des legalen und illegalen Austausches solcher Dateien mit Musik ist ein erheblicher Datenverkehr entstanden. Viele Firmen blockieren dieses Datenformat in ihrem Internetzugang und verbieten →P2P-Daten. In MP3-Dateien kann heute auch →Malicious Code versteckt werden, zusätzlich gibt es Abspielprogramme, die innerhalb dieses Formates als Erweiterung auch Scripten erlauben, was zu einem Sicherheitsproblem werden kann

MP3-Player: Geräte zum Abspielen von Musik und/oder Videos. Einer der Marktführer ist/war dabei der →iPod, später variiert zum iPod Touch von Apple. Sicherheitsrelevant, da diese Geräte über →USB leicht an Firmenrechner angeschlossen werden können und über ihre Speicher →Daten ein- und ausschleusen können

MPC: (→multi-party computation)

M-Pesa: (mobile pesa=swahili f. Geld) 2013 fortgeschrittenstes Zahlungssystem für →Handys. Nach →Authentifizierung durch National ID kann damit auf Bargeld zugegriffen werden oder gezahlt werden. Siehe →e-Geld

MPLS: (Multiple Protocol Label Switching) Methode die verbindungsorientierte Datenübertragung mit paketbasierten Internet Routing Protokollen verbindet. Es ist eine Methode um →Layer 2 und Layer 3 Protokolle zu kapseln, ähnlich zu →PPP. Hierdurch wird die Möglichkeit gegeben, vielfältige Arten von Daten wie Telefonverkehr oder IP-Pakete zu übertragen

mPOS: →POS

MQ-Series: →Messaging Software von IBM

MQTT: MQ Telemetry Transport or Message Queue Telemetry Transport. Auf →TCP/IP basierendes →Protokoll zum Austausch von Datenblöcken (Nachrichten). Wird vor allem im →IoT Bereich zum Datenaustausch zwischen Geräten genutzt. Es basiert auf dem →Publish-Subscribe Prinzip

MS-CHAP: →Authentisierungsprotokoll auf der Basis von →CHAP, gilt als unsicher bzgl. →Brute Force →Dictionary Attacks

MSI: Windows Installer (vormals Microsoft Installer), eine Installationsumgebung für Windows Systeme, die von vielen Installationspaketen genutzt wird. →Softwareverteilung

MSISDN: Telefonnummer in einem Mobilfunknetz, verknüpft mit der →IMSI der →SIM-Karte

MSP: →Managed Service Provider

MSRT: (Malicious Software Removal Tool) kostenlose Software von Microsoft zum Entfernen von →Schadsoftware, geringere Abdeckung als kommerzielle Alternativen

MSUS: (Microsoft Software Update Service) →SUS

MTA: (Mail Transfer Agent) abstrakter Begriff für das →Programm, das →E-Mails von einem E-Mail-Client-Programm empfängt und (normalerweise) über das →Internet an einen MDA (Mail Delivery Agent) weiterleitet, der die E-Mails in die Empfänger-Mailboxen verteilt von denen sie über →POP3 oder →IMAP abgerufen werden

mTAN: Verfahren, bei dem →TAN Nummern zur Absicherung von →e-Banking-Transaktionen vom e-Banking-Server per →SMS zum Benutzer übertragen werden. Durch die Verwendung eines 2. Kommunikationskanals (→ „out-of-band“) erhöht dies die Sicherheit gegen →Phishing. Es schützt jedoch nicht gegen →Man-in-the-Middle Angriffe (MITM) und verliert seine Schutzfunktion weitgehend wenn das e-Banking ebenfalls auf einem →Smartphone durchgeführt wird. Ebenso ist es angreifbar über die →SS7 →Verwundbarkeiten. Daher wird an neuen Verfahren gearbeitet, z.B. →CAP

MTLS: (Multiplexed Transport →Layer Security) Unterstützung von mehreren Datenströmen über eine →TLS-Verbindung

Mujahedeen Secrets: →Verschlüsselungsprogram, das on Al-Qaeda empfohlen wird/wurde. Seine Nutzung ist ein sicherer Web, die Aufmerksamkeit der →NSA auf sich zu ziehen, die diese Übertragung mittels →XKeyscore selektiert. Trotz der Verschlüsselung der →Daten (d.h. der Message) sind die →Metadaten wie von welcher →IP-Adresse zu wel-

cher Zeit und an welchen Adressaten natürlich für die NSA von großem Interesse um die entsprechenden Netzwerke zu identifizieren. Auf die gleiche Weise werden natürlich auch →PGP-Nutzer selektiert, ziehen aber bei weitem nicht die gleiche Aufmerksamkeit auf sich

Mule: →Money Mule

Multicast: Bandbreite sparendes Datenübertragungsverfahren das aber nur da eingesetzt werden kann, wo alle Empfänger zu einem Zeitpunkt die selben →Daten empfangen. Was bei →Streaming-Diensten nicht der Fall ist. Dort muss daher →Unicast eingesetzt werden

MULTICS: (Multiplexed Information and Computing Service) interaktives →Betriebssystem (1974), bei dem viele Sicherheitsfeatures, z.B. →ACLs, →DAC und →MAC erstmalig genutzt wurden, heute schon lange nicht mehr im Einsatz

Multi-Faktor-Authentication: (MFA) Verbesserung von →2 Faktor Authentisierung (Authentisierung= Authentifizierung =Authentication)

Multifunktionsprinter: (MFD, multi-functional device) moderne Drucker, die Scannen, Fax und andere Funktionalitäten kombinieren und oft über ein allgemeines →Betriebssystem mit →Festplatten verfügen. Sicherheitsrelevant, wenn sie über das interne Netz (oder sogar das →Internet) ansprechbar sind und über ihre Scanner-Funktion die Versendung von Scans von Papierdokumenten auch ins Internet ermöglichen.

Fotokopien werden durch Einscannen, Abspeichern des Images auf der internen Festplatte und dann Ausdrucken erzeugt. Grundsätzlich verbleiben (möglicherweise vertrauliche) → Druckausgaben auch später noch auf der internen Magnetplatte zu finden (oder zu „recovern“ sind, →Datenrettung).

Viele der Geräte kommunizieren ihren Funktionsstatus, den Zustand der Patronen und ähnliches regelmäßig mittels Internetverbindung an den Hersteller, so dass automatisch Patronen geliefert werden können.

Drucker können über zusätzliche Sicherheitsfunktionen verfügen, so z.B. verschlüselte Übertragungen, oder dass z.B. vertrauliche Druckausgaben nur lokal abrufbar sind, wenn der →Benutzer sich →authentifiziert, bzw. verschlüsselte Übertragungen ermöglichen. Siehe →PJL

Multihome: Verfahren zur Steigerung der →Verfügbarkeit von →Systemen in →IP-Netzen durch Unterstützung mehrerer Netzanschlüsse. Siehe →SCTP

Multi-Party Computation: (MPC) Konzept der →Kryptographie, bei dem mehrere Teilnehmer gemeinsam an einem Problem rechnen (z.B. Größenvergleich), ohne dass der andere Teilnehmer die →Daten selbst sieht. 2015 wird gezeigt, dass es sich mittels der Mathematik hinter →Bticoin mit einer geringeren Rechenaufwand lösen lässt, als mit →homomorphic encryption. Verwand mit →Zero knowledge proof

Multi Tenancy: →Mandantentrennung

Mumble: Sprachkonferenzsoftware, →Open Source und wegen guter Audioqualität und vor allem niedrigen Latenz sehr geschätzt bei online →Games (als Hintergrundkanal zwischen Spielern eines Teams). Als klassisches →Client-Server Konzept implementiert, die →Server „Murmur“ können leicht selbst betrieben werden. Hohe →Verschlüsselungs-Sicherheit durch →Perfect Forward Secrecy

Murphys Law: „alles was schief gehen kann, wird auch schief gehen“. Wichtiger Aspekt im Bereich →Safety, bei →Security aber ebenfalls zu berücksichtigen

MUSCULAR: Aktivität der →NSA um den Datenverkehrs zwischen den →Rechenzentren von →Cloud-Diensten abzuhören

Must not: (engl. darf nicht) kommt in Standards und →RFCs vor, wird leicht missverstanden

Mystery Activity: Verfahren zur →Qualitätskontrolle durch normierte Testaktivitäten, z.B. Testanrufe zur Aktivierung eines Geschäftsprozesses, kann auch für →Informationssicherheit verwendet werden (historisch: Mystery Shopping als Marketingaktivität). Siehe →Benchmark, →KPI

NAC:

1) (Network Admission Control) Konzept von Cisco um →Zugriff zu einem Netz nur nach Prüfung des Sicherheitsstatus eines Endgerätes (→PC oder →PDA) zu erlauben auf der Basis von Agents auf den Geräten. →Endpoint Security

2) (Network Access Control, IEEE 802.1x) Freigabe des Netzzugangs an einem → Port eines →Switches nur auf Grund einer Prüfung der Identität des Gerätes und/oder Benutzers. →Authentisierung über →Radius und →EAP-TLS, bzw. →PEAP, sehr oft gegen →ADS. →Fallback ist die Prüfung der →MAC-Adresse eines Gerätes. Erfordert auf dem Gerät einen →Supplicant

Nacktscanner: Darstellung von Menschen ohne Kleidung, wird immer öfter in Flughäfen genutzt. Problematisch in Bezug auf →Privatsphäre. Siehe →Terahertz Imaging, →Backscatter X-ray

Nachhaltigkeit: Begriff der u.a. ein ethisches Verhalten im Geschäftsbetrieb bezeichnet. Es bezieht sich nicht nur auf Umweltschutz (wie ISO 14001), sondern eine Berücksichtigung aller →Stakeholder. Siehe →Corporate Social Responsibility

Nachricht: geordnete Folge von Zeichen für die Weitergabe von Information. [ISO 2382/16], →ASCII

NaCL: (→Native Client)

NAND Lock: Bei →Android Geräten von HTC eine Einrichtung, die Verhindern soll dass das →Betriebssystem überschrieben wird, d.h. Verhinderung von →Rooting. Kann aber leider auch ausgehebelt werden

Nannycam: →Webcam

NAP:
1) (Network Access Protection) Konzept von →Microsoft, um Zugriff nur nach Prüfung des Sicherheitsstatus eines Endgerätes zu erlauben und in Vista und XP SP2 enthalten sein wird. Grundlage ist ein Windows Quarantine Agent (QA) auf dem Endgerät. Siehe →Endpoint Security

2) (Network Access Point) →Bluetooth-Gerät, das →Routing oder →Bridging eines Bluetooth Gerätes zu einem anderen Netzwerk erlaubt

Napster: erste →Tauschbörse für Musik im →Internet (1998). Auf Grund des dabei genutzten zentralen Servers juristisch angreifbar durch die →RIAA und 2001 eingestellt. 2002 aufgekauft durch Bertelsmann und als kostenpflichtiger Dienst neu gestartet, konnte aber gegen iTunes nicht konkurrieren. Siehe →P2P, →Raubkopie, →KaZaA, →eDonkey, →Tauschbörse

NAPT: (Network Address Port Translation) ähnlich zu →NAT: →private →IP-Adressen in Firmennetzen werden in eine oder mehrere öffentliche, d.h. offiziell zugeordnete IP-Adressen übersetzt. Bei NAPT werden jedoch auch die →Port-Nummern verändert um zu verhindern, dass es Konflikte gibt, wenn sich mehrere interne Rechner zufällig mit derselben Portnummer zu 1 externen Rechner verbinden, z.B. bei →WebRTC-basierten →Videokonferenzsystemen. Das wird mit Hilfe von externen →STUN-Servern gelöst

Narus: US-Unternehmen, führend bei Geräten zur Analyse von großen Datenmengen während der Übetragung im →Internet (→E-Mail, →VoIP-Verkehr, →Messenging, etc.). Ein Gerät ist Narus Semantic Traffic Analyzer 64000). Dies wird als →Deep packet inspection bezeichnet. Wird für legale richterlich angeordnete Überwachungen (→LI), aber auch für heimliche Überwachungen in vielen Ländern eingesetzt. Die flächendeckenden Überwachungen in den USA wurden 2006 durch einen →Whistleblower öffentlich bekannt. Siehe →Semantic Traffic Analysis. Siehe →NSA

National Security Letter: (NSL) im US-→Patriot Act eingeführtes Verfahren, bei dem das FBI →Daten ohne Gerichtsbeschluss einfordern kann. Der Betreiber wird zu vollkommenen Stillschweigen über diesen Vorgang verpflichtet, eine Überprüfung durch Gericht ist nicht möglich. In manchen Jahren wurden NSL bis zu 50 000 mal genutzt. Dies ist auch für uns relevant, denn bei →Cloud Computing unterliegen US-Firmen diesem Gesetz sogar dann, wenn die Daten in Europa gespeichert werden

NAT: (Network Address Translation) Umsetzung von einer oder mehrerer sog. →privater →IP-Adressen in eine oder mehrere öffentliche, d.h. offiziell zugeordnete IP-Adressen. Dieses Verfahren wird vor allem in →Firewalls eingesetzt und umgeht die Probleme, die sich aus der Knappheit der IP-Adressen ergeben und bietet gleichzeitig eine gewisse →Anonymisierung der →Zugriffe aus einem Unternehmen nach außen. Siehe auch →NAPT und →STUN

Native Client: (NaCL) →Sandbox von →Google mit der unabhängig von →Betriebssystem und →Webbrowser →Programme für →x86-Prozessoren in einer abgesicherten Umgebung innerhalb des Browsers ausgeführt werden können (sicherer Ersatz für →ActiveX). Dabei wird die Speicher-Segmentierung des Chips verwendet und alle Aufrufe an das Betriebssystem durch innerhalb des Browser-Plugins kontrolliert

Navigationsgerät: (Navi) Gerät für →Geolocation, zumeist in ein Auto eingebaut. Stellt mittels →GPS den Standort fest und kann diesen auf integrierten Straßenkarten anzeigen und Wegempfehlungen abgeben. Kann eine Verletzung der Privatsphäre darstellen wenn erweiterte Funktionen eine Geschwindigkeitsüberwachung und –aufzeichnung oder Weitermeldung des Standorts durchführen, oft als Schutz bei Fahrzeugdiebstählen

NBAD: (Network behavior anomaly detection) automatisierte Analyse des Verkehrs in einem Datennetz, z.B. bzgl. Bandbreitenbedarf, →Port-Nutzung und Datenvolumen um Anomalien zu entdecken, die auf →Angriffe hindeuten könnten. Es geht damit über den →Patternmatching eines →IPS oder →IDS hinaus

NCSD: (National Cyber Security Division) Teil vom →DHS und verantwortlich für den Schutz der USA gegen →Internet-basierende →Angriffe. →US-CERT ist Teil dieser Behörde

NDA: (Non Disclosure Agreement) „Nicht-Freigabevereinbarung“, ein rechtsverbindliches Dokument, das die →Vertraulichkeit von Ideen, Designs, Plänen, Konzepten oder anderem kommerziellen Material schützt. Häufig werden NDAs von Verkäufern, Fremdfirmen, Beratern und anderen Nichtangestellten unterzeichnet, die in **Kontakt** mit solchem Material kommen (könnten)

NDEF: (NFC Data Exchange Format) für →NFC verwendetes unverschlüsseltes Datenaustauschprotokoll

NDP: (Neighbor Discovery Protocol) Protokoll

unter →IPv6 bei dem mittels →ICMPv6 Messages Rechner in einem Netz →IP Adressen beziehen können und andere Netzwerkinformationen wie Default Gateway. Es ersetzt →ARP, →DHCP und →ICMP

NDS: (Novell Directory Services) jetzt unter dem Namen eDirectory, ein →Verzeichnisdienst von Novell

NEAT: Akronym von →Microsoft in einer Anleitung für Entwickler in Bezug auf →Security Usability. Es geht darum, unter welchen Umständen Benutzer ein Fenster sehen sollen, indem sie sicherheitsrelevante Entscheidungen treffen müssen.

N(essary): es muss etwas sein, bei der es absolut notwendig ist, den Benutzer zu fragen

E(xplained): die Erklärung muss alles enthalten was ein Benutzer braucht, um die geforderte Entscheidung zu treffen

A(ctionable): Eine solche Frage an den Benutzer ist nur erlaubt wenn der Benutzer wirklich in der Lage ist, diese Entscheidung zu treffen

T(ested): Die Implementierung muss getestet werden.

Der Aspekt „Explained" wird weiter erkärt durch SPRUCE:

S(ource): erklären wer oder was die Frage stellt

P(rocess): die Schritte aufzeigen, die der Benutzer befolgen muss

R(isk): das →Risiko, bzw. korrekterweise die →Bedrohung aufzeigen, die bei einer falschen Entscheidung eintreffen könnte

U(nique knowledge of user): erklären, welche →Informationen des Benutzers zu einer korrekten Entscheidung betragen können

C(hoices): erklären, welche Optionen der Benutzer hat

E(vidence): auf Informationen hinweisen, die dem Benutzer bei der Entscheidung helfen können

Need-to-Know: Sicherheitskonzept, ursprünglich aus dem militärischen Bereich, das besagt, dass jeder Nutzer nur →Zugang zu den →Informationen oder →Anwendungen haben sollte, die er für die Erfüllung seiner Aufgaben braucht

Nessus: →open-source →Programm zum Auffinden von bekannten →Schwachstellen in IT-Systemen. Wird bei →Angriffen und für →Penetration Tests genutzt

Nest: siehe →Doorbells

.NET: von →Microsoft entwickelte Softwareplattform mit →Laufzeitumgebung (→RTE) für die Zielrechner, Entwicklungsumgebung (→API) und weitere Dienstprogramme (Services). Unterstützt werden mehrere →Programmiersprachen, ersetzt COM und ist Konkurrenz zu →J2EE. Siehe →Silverlight, →FxCop

NetBEUI: (NetBIOS Enhanced User Interface) verbesserte Version des →NetBIOS Protokolls, das besonders in älteren MS Windows Netzen zum Sharen von Dateien verwendet wurde. Dieses Protokoll stellt heute oft ein Sicherheitsproblem dar

Netflix: US-Unternehmen, bereits 1997 gegründet, seit 2007 mit kostenpflichtigen →Streaming für Filme. 2019 die dominierende Streaming-Firma und zusammen mit einigen anderen Anbietern (z.B. →Amazon Prime) eine ernsthafte Bedrohung für traditionelles (lineares) Fernsehen mit festen Sendezeiten. Bei den Streaming Angeboten wie Netflix kann der Nutzer jede Sendung zu jeder Zeit sehen und ist nicht feste Sendezeiten gebunden. Netflix ist 2019 auch einer der großen Produzenten exklusive für Eigenproduktionen, speziell Serien (die nur dort zu konsumieren sind). Netflix und →Spotify sind Beispiele die die oft behauptete These widerlegen, dass im →Internet alles kostenlos (d.h. über →Werbung und →Überwachung der Nutzer finanziert) sein muss. Siehe auch →Social Viewing

NetFlow: Technik zur Verkehrsanalyse in → Datennetzen, genutzt für Kapazitätsplanung oder zur →QoS-Analyse. Dabei sendet ein →Router oder →Layer-3→Switch →Verkehrsdaten an einen speziellen Server. In →Backbone-Netzen mit hohem Datenverkehr wird nur ein statistisch ausgewählter Teil des Verkehrs betrachtet, bis zu einer „sampling rate" von 1:10000. Wird u.a. zum Erkennen von →dDoS-Angriffen verwendet. Zum Ändern des Datenflusses wird dann oft →RSVP eingesetzt**.** Netflow ist sehr wichtig bei der Abwehr von →dDoS-→Angriffen

Net Nanny: Filterprogramm zum Schutz vor jugendgefährdenden Seiten im →Internet

Net neutrality: Forderung, dass auch in Zukunft alle Datenströme im →Internet mit gleicher Prioritität übertragen werden und durch die →ISP nicht reglementiert werden. Diese Gleichberechtigung aller Anwendungen war eine der grundlegenden Konzepte der ursprünglichen Internet-Entwickler (im Gegensatz zu den bis dahin üblichen Konzepten der Telekomfirmen die die zentrale Kontrolle über ihr jeweiliges Netz und damit auch deren Anwendungen hatten). Dieses Konzept wird aber seit ca. 2018 immer stärker bedroht, z.B. indem Telekom-Anbieter (→ISPs) eigene →Streaming-Dienste (z.B. für TV-Inhalte) anbieten und diese oft aus den Datenlimits der Nutzer ausnehmen. Ein anderer Aspekt ist die Entwicklung dass Anbieter wie →Google eigene Glasfasernetze implementieren (speziell in den Weltmeeren) und auf diesen Netzen die Prioritäten frei bestimmen können, z.B. nur eigene und „befreudete" Dienste bzw. die Daten ihrer →Cloud-Kunden übertragen. Dies hebelt die Idee aus, dass die zentrale

Infrastruktur des Internets allen gleich zur Verfügung steht

Netscape: fast vergessene Firma, die 1995 einen der ersten graphischen Web-→Browser entwickelt hat und auch →SSL und →Javascript entwickelte. Siehe →Crypto Wars, →Bug Bounty

Netstumbler: →open-source Tool zum Auffinden von →WLAN-Netzen, cracken von →WEP-→Passworten. Wird für →Angriffe und →Penetration Tests genutzt

Net reconnaissance: Nutzung des →Webs zur Informationssammlung über Personen oder Unternehmen mittels →Suchmaschinen und →Social Networking. →Industriespionage, →targeted attack, →spear fishing

Network Access Control: (→NAC)

Network Admission Control: (→NAC)

Network Management: Nutzung von →Systemen, mit deren Hilfe der Gesamtzustand eines komplexen →Netzwerks leicht bez. →Sicherheit, →Verfügbarkeit und Performance überwacht werden kann. Dabei wird meist →SNMP eingesetzt. →IDS können in dieses System integriert sein

Network Security: Konzept der Absicherung einer IT-Umgebung durch Überwachung des →Netzes, z.B. durch →Firewall, →Proxy, →Intrusion Dection und Prevention. Allgemeine Vernetzung hat Netze jedoch heute weitgehend löchrig gemacht, daher muss Network Security durch →Application Security ergänzt werden. Siehe →NIPS, →Desktop Security

Netz: kurz für →Netzwerk, oft auch für →www

Netzbetreiber: Entweder Anbieter eines Mobilfunknetzes. Dann betreibt er →Base Station und →Home Location Register. Oder auch Anbieter von Kabelnetzen, →Leased Lines, bzw. den Backbones zwischen den →IXPs

NetzDG: →Netzwerkdurchsetzungsgesetz

Netze-von-Netzen: (networks of networks) Konzept mit dem versucht wird, sich der Komplexität der realen Welt anzunähern. Dabei ist Netz weit definiert: →Datennetz, →Social Network, Versorgungsnetze, aber auch Verknüpfungen in der Biologie, in den Abläufen innerhalb von Zellen und Verknüpfungen die zu Wetter und Klima führen. Die mathematische Betrachtung dieser Netze von Netzen führt zu Erkenntnissen bzgl. →Resilience unter kritischen Umständen. So ist diese geringer wenn eines der Netze „assortativity“ aufweißt, d.h. stark vernetzte Knoten sind hauptsächlich untereinander vernetzt, schwach vernetzte Knoten ebenfalls nur untereinander. Dies steht im Gegensatz z.B. zum „small world network“ (→6-degree of segregation) bei dem es zwar viele eng verknüpfte Cluster von Knoten gibt, aber auch Verbindungen zwischen den Clustern. Erkenntnisse aus diesen Forschungen sollen zu Konzepten führen wie reale Netze wie die Stromversorgung weniger anfällig für Effekte wie Kaskadenausfälle gemacht werden können

Netzgeld: →e-Geld

Netzneutralität: →Net Neutrality

Netzwerk: (network)

1) Übertragungssystem für Nachrichten (→Daten) in einer bestimmten Umgebung. Ein →Computer-Netzwerk besteht meist aus →Servern, →PCs, →Routern und →Switches. Dabei kann jeder →PC unabhängig arbeiten, zugleich aber über das Netz mit anderen Rechnern, z.B. Servern, kommunizieren, mit diesen Informationen austauschen und ggf. auf andere Ressourcen im Netz oder andere Netzen zurückgreifen. Ein Netz erfordert entsprechende Hard- (Router, Switches) und Software. Es gibt offene Netze, insbesondere das →Internet und geschlossene Netze, z.B. →LAN oder →WLAN. Siehe →Datennetze, →Computernetze, →VLAN

2) im Bereich →Social Networking das Netz das durch alle Kontakte (→friends) der Teilnehmer entsteht. Dieses kann zu Zwecken des →Data Minings ausgewertet werden und durch die damit verbundenen →Zugriffsrechte für →Datendiebstahl missbraucht werden

Netzwerkadapter: Teil eines →Computers, über den auf →Datennetze zugegriffen wird, entweder auf dem →Motherboard oder als separate Steckkarte. Kann bei →Betriebssystem→Virtualisierung gemeinsam von mehreren Betriebssystemen genutzt werden

Netzwerkdurchsetzungsgesetz: (NetzDG) Gesetz in D das für Anbieter von →social networks nach Kenntnis und Prüfung von rechtswidrigen Inhalten, z.B. →Hasspostings, eine Löschung oder Sperrung vorschreibt. Es gibt Opfern von Persönlichkeitsverletzungen im →Internet einen Anspruch auf Auskunft über →Daten des Verletzers aufgrund gerichtlicher Anordnung. Das Gesetz wird kritisiert und teilweise als Zensurinfrastruktur bezeichnet. Ebenso wird der Trend kritisiert, immer mehr Rechtsentscheidungen an private Betreiber zu delegieren, siehe auch →Upload-Filter. In beiden Fällen können die hohen Bußgelddrohungen dazu führen, dass die Betreiber zur Sicherheit Inhalte im Zweifelsfall löschen werden

Netzwerkprotokolle: Verfahren, mit denen Daten in einem Datennetz übertragen werden. Beispiele sind →TCP/IP, →NetBEUI, →PPP, →IPSec

Netzüberwachung: →Network Management

Neuronale Netze: →Neural Network

Neural Network: in Hardware oder Software implementierte →Algorithmen die vom neuralen Netz im Nervensystem von Lebewesen inspiriert sind. Sie wurden in den 80igern

entwickelt und heute im Bereich →Deep Learning / →Machine Learning für Mustererkennung, speziell Bild- und Spracherkennung, verwendet. Spracherkennung wird z.B. für →personal assistants immer wichtiger wird. Auch automatische Übersetzer beruhen auf so einem Algorithmus. Problematisch ist an diesem Konzept, dass neuronale Netze „sich" nicht erklären können (fehlende →explainability). Neuronale Netze machen z.B. bei Bilderkennung oft für Menschen absolut verblüffende Fehler. Speziell bei mehrstufigen Netzen ist eine Rekonstruktion einer Fehlentscheidung, z.B. nach einem Unfall eines →autonomen Fahrzeugs, nicht möglich, was ein Problem darstellt. Neuronale Netze werden manchmal als Überwindung von →Turing Maschinen gesehen, was jedoch nicht der Fall ist. D.h. auch und speziell neuronale Netze sind nicht geeignet die Basis für starke →artificial intelligence zu bilden

Neuroprothese: Schnittstelle zwischen dem Nervensystem und Geräten, z.B. für Cochlear Implants oder Anschlüsse an Sehnerven. Diese Aktivitäten sind ähnlich zu →brain-computer interface (BCI). Ziel ist bei beiden Aktivitäten (derzeit) vor allem die Hilfe für Kranke, aber natürlich ist auch das Militär an solchen Entwicklungen sehr interessiert um die Fähigkeiten der Soldaten zu erweitern. Es gibt darüber hinaus auch Zielsetzungen die in Richtung →Transhumanismus gehen. Die EU unterstützt das Forschungsprojekt VERE (virtual embodiment and robotic re-embodidment) bei dem die Grenzen zwischen Mensch und Maschine aufgehoben werden sollen

Neustart: gängiges Verfahren zur Behebung von →Software-Problemen, speziell bei →Absturz. Dabei wird oft das betroffene →System aus- und wieder eingeschaltet

Newsgroup: Diskussionsforen in den frühen Zeit des →Internets, implementiert mit Hilfe des Network News Transfer Protocol (NNTP). Die Foren waren Teil des Usenets auf der Basis der UUCP dial-up Infrastruktur. Teilnehmer wählten sich typischweise über →Modems ein

Next Generation Identification: Programm des FBIs bei der eine →Datenbank mit →biometrischen Merkmalen für „Person of Interest" eingerichtet werden, für die zuerst nur die Gesichter gespeichert werden, für später ist →Iris-Erkennung, →DNA und →Stimm-Erkennung geplant.Die Gesichter sollen automatisiert mit Fotos im →Internet verglichen werden und mit den Aufnahmen von Überwachungskameras. Die Nutzung ist geplant für Polizei, Grenzbehörden und auch Firmen. Dabei wird es große Probleme mit →False Positives geben, d.h. fälschlich erkannten Personen die dann (regelmäßig) „aufgegriffen" werden

Next Generation Network: (NGN) Schlagwort für eine Integration von Daten, Sprache und Video über →IP-basierte Netze jeglicher Art, inkl. →WLAN, mobile Netze (→UMTS, →Bluetooth)

NFC: (Near Field Communication) drahtlose Techniken im Abstandsbereich von Zentimetern nach ISO 18092. Diese Technik ist gedacht, um z.B. →SmartPhones für Zahlungen zu benutzen (→ApplePay, →GooglePay) oder mittels →Kreditkarten kontaktlos, d.h. schneller bezahlen oder Geld abheben zu können. Dabei gelten die Smartphones als „aktive" NFC-Implementierung, die über die Batterie des Geräts versorgt werden, in →Smartcards gibt es „passive" NFC-Chips, z.B. in →Bankomat- oder →Kreditkarten, die ihren Strom aus dem Lesegerät beziehen müssen und außer der NFC-Schnittstelle keine Datenein- oder –Ausgabe haben. Diese Geräte können ihre Geräte-ID kommunizieren und damit entsprechende Datensätze in einer →Datenbank indizieren. Drahtlose Bankomat- und Kreditkarten speichern ab 2013 jedoch auch vertrauliche Informationen wie Name, Konto-, bzw. Kreditkartennummer und die letzten Zahlungen. Es können geringwertige Zahlungen (weil ohne Interaktionsmöglichkeit) oder der Zutritt zu Räumen oder Events freigegeben werden. Angreifer können jedoch auch drahtlos an sensible Daten kommen.

Zahlreiche Sicherheitsprobleme werden berichtet, so ist z.B. der Datenaustausch mittels →NDEF unverschlüsselt und ‚bösartige' NFC-Etiketten (NFC tag) können die Handys auf →URLs schicken, ohne dass der Anwender das sieht. NFC Tags sind teilweise überschreibbar und damit für →Angriffe verwendbar. Auf Grund der räumlichen Nähe und dem Ablauf der Handshakes ist ein →Man-in-the-Middle Angriff nicht möglich, ein →Abhören der Verbindungen aber sehr wohl, speziell im sog. Active-active mode (beide Geräte haben eigene Stromversorgung). D.h. ohne zusätzlich implementierte →Verschlüsselung können vertrauliche Daten offengelegt werden. In Verbindung mit →Zertifikaten in der →UICC sind mobile Zahlungslösungen geplant (→MCP)

NFS: (Network File System) Zugriffsmethode auf →Dateien über ein →Netzwerk. Enthält wenig Sicherheitsfeatures und ist z.B. nicht geschützt gegen →Spoofing von Geräten, besser ist →AFS. Siehe →File system

NGFW: (Next Generation Firewall) Schlagwort mit dem ein →Firewall betitelt wird der „tiefer" in den Datenverkehr einsieht und z.B. →IPS mit enthält. Hintergrund ist, dass heute ein sehr großer Teil des →Datenverkehrs durch Firewalls über →http oder →https abgehandelt wird und sich dadurch der Kontrolle entzieht (z.B. →Skype). Dies machen sich auch die

Entwickler von →Schadsoftware zu nutze, speziell wenn sie nach einer →Infektion in einem Firmennetz Verbindungen zu einem →Command and Control Server aufbauen wollen. NGFW ist ähnlich zum Schlagwort →UTM (→Unified Threat Management)

NGI: (→Next Generation Identification)

NGSCB: (Next Generation Secure Computing Base, ausgesprochen „enscub“) Von →Microsoft propagiertes Sicherheitskonzept, das auf der →TCG Hardware beruht. Dabei geht es um eine eindeutige Identifizierung eines Rechners über einen Identitätschip auf dem →Motherboard. Alternativ dazu gibt es →EMSCB mit →Turaya

Nickname: spezielle Form einer →Benutzerkennung. Spitzname/Phantasiename bei der Kommunikation im Internet, den sich die Teilnehmer i.d.R. selbst geben. Bietet eine gewisse Form der Anonymisierung, die jedoch durch Rückverfolgung, z.B. auf die →IP-Adressen von der sie genutzt wurde, aufgehoben werden kann

NGN: →Next Generation Network

NIMD: (Novel Intelligence from Massive Data) US-Forschungsprogramm zur Nutzung sehr großer Datenmengen (z.B. Internetaktivitäten und Telefondaten) zur Informationsgewinnung für Nachrichtendienste. Finanziert durch →ARDA und →NAS, wird als Nachfolger von →TIA betrachtet

NIPS: (network intrusion prevention system) Überwachung eines Netzes zum Schutz gegen →Angriffe. Im Gegensatz zum →IDS setzt ein NIPS geeignete Maßnahmen zur Blockierung des Angriffs. Durch Tricks auf der →IP-Ebene können Angriffe jeder auch am NIPS vorbei geführt werden, →Fragmentierung (frag router). Siehe →HIPS

NIST: (National Institute for Standards and Technology) US-amerikanische Standardisierungsbehörde, kümmert sich auch um Sicherheitsstandards, z.B. für →Verschlüsselung, Risikoanalyse, u.ä.

Nitrokey: →USB-basierte →Authentisierungslösung auf →open source Basis. Kann zum Authentisierung gegen →Windows, →Linux oder →MacOS genutzt werden. Die Geräte werden über einen →PIN geschützt und unterstützen →HOTP und →TOTP, sind kompatibel mit →Google Authenticator. Siehe auch →Yubikey

nmap: →open-source →Programm zum Finden und Auflisten von Rechnern und offenen →TCP- oder →UDP-→Ports in Netzen. Wird bei →Angriffen und für →Penetration Tests genutzt

Node.js: →JavaScript →Laufzeitumgebung für die Programmierung auf Servern

No Fly List: US-Programm zum →Screening von Flugpassagieren. Sehr fehlerhaft (doppelte Namen, Namensgleichheiten, Namensähnlichkeiten). Angeblich 2019 eingestellt. Siehe →CAPPS II, →Secure Flight

Non-captive outsourcing: →Outsourcing

Nonce: (number used once) zumeist eine →Zufallszahl, die z.B. im Ablauf eines →Authentifizierungsverfahren genutzt wird und durch die Einmalnutzung gegen →Replay-Angriffe schützen soll

Non Disclosure Agreement: →NDA

Non-Repudiation: (deutsch: Verbindlichkeit) bezieht sich auf die Sicherstellung, dass die Aktionen einer Instanz (Benutzer, Prozesse, Systeme, Informationen, etc.) ausschließlich dieser Instanz zugeordnet werden können und dass die Kommunikationsbeziehung bzw. der Informationsaustausch nicht geleugnet werden kann. Siehe →Authentizität, →EDI. Gegenteil: →Deniability

NOP-Slide: →Programmier-Technik bei der eine anzuspringende Adressstelle nicht exakt bekannt ist. Daher werden vor der gesuchten Stelle NOP (no-operation) Instruktionen eingefügt, die sofort durchlaufen werden bis die gesuchte Stelle kommt. Kann genutzt werden um →ASLR auszuhebeln

Normen: in der IT äquivalent zu →Standard

No-Script: Plugin in →Browsern zum selektiven Abschalten von →Javascript zur Vermeidung von →Schadsoftware und →Tracking. Reduziert jedoch die Verwendbarkeit von vielen →Websites

NoSQL: (auch „Not only SQL“) Sammelbegriff für Datenbanktypen die andere Zugriffsmethoden als SQL-Kommandos unterstützen. Werden hauptsächlich rund um →Data Mining (→Big Data) eingesetzt und unterstützen z.B. Datenstrukturen wie „key-value pairs“ oder große unstrukturierte Datensammlungen wie →Websites in den großen Suchmaschinen. Typischerweise fehlen dann alle Sicherheitsfeatures wie →Authentisierung von Nutzern, →Logging, →Mandantentrennung, etc. Dies ist besonders problematisch, wenn diese Datenbanken direkt im Internet erreichbar sind, was 2015 im Fall von MongoDB und anderen dramatisch gezeigt wurde

Notebook: Siehe →Laptop

Notfall: Eintritt eines Problems, z.B. IT-Ausfall, mit einer begrenzten Auswirkung/ Impact und begrenzter (erwarteter) Dauer, Steigerungsstufe zu →Incident. Bei längerer Dauer oder größeren Auswirkungen spricht man von einem →Katastrophenfall oder eine Krise. Initiiert werden Notfälle oft über einen →Incident

Notfallplan: Beschreibung der notwendigen Prozesse, die bei Eintritt eines →Notfalls aktiviert werden müssen. Wichtiger Aspekt ist der →Alarmplan. Untermenge eines →Katastrophenplans, der für größere und längerfristig

andauernde Katastrophen gilt

„**Nothing to Hide“:** Schlagwort mit dem →Angriffe auf die →Privatsphäre legitimiert werden sollen: z.B. in einem Roman von Upton Sinclair 1918: "If you have nothing to hide you have nothing to fear." Widerlegt wurde das Argument in D. durch das sog. Volkszählungsurteil des Bundesverfassungsgericht 1983 durch Etablierung des Rechts auf „→informationelle Selbstbestimmung“

NPV: (net present value, Kapitalwertmethode) Verfahren für → Wirtschaftlichkeitsberechnungen). Durch Abzinsung auf den Beginn der Investition werden Zahlungen, die zu späteren Zeitpunkten anfallen, vergleichbar gemacht. →ROI, →IRR

NSA: (National Security Agency / Central Security Service) US-Behörde, Teil des Verteidigungsministeriums, die für das →Abhören und Entschlüsseln von elektronischen →Nachrichten zuständig ist (→SIGINT). Sie beschäftigt u.a.eine große Zahl von Mathematikern, die auf →Kryptographie spezialisiert sind („Knacken“ von →Verschlüsselungen wie auch Erstellen von sicheren Verfahren für die Nutzung von US-Stellen), aber auch Sicherheitserweiterungen für →Betriebssysteme und Geräte erstellen, z.B. → SELinux.

2013 wurde veröffentlicht, dass die NSA mit Hilfe des britischen →GCHQ einen großen Teil des →Internet-→Datenverkehrs abfangen, entschlüsseln und auswerten und im Rahmen von Programmen wie →PRISM, Daten von Webmail-Anbietern und →Social Networking Anbietern überwachen und mit Programmen wie → Tempora, →XKeyscore anderen Datenverkehr analysieren. →MUSCULAR ist das Codewort für das Abhören des Datenverkehrs zwischen den →Rechenzentren vieler → Cloud-Dienste. Mit Hilfe von →QUANTUM kann die NSA auch gezielt einzelne →Rechner infizieren und damit übernehmen. Erste Hinweise hatte es bereits 2006 gegeben: Mark Klein verriet, dass die NSA in AT&T Räumlichkeiten Datenleitungen anzapft. Siehe →Echelon als älterer Vorläufer.

Mit →CO-TRAVELLER sammelt die NSA die täglich Milliarden von →Handy →Standortdaten, wertet sie mit →HAPPYFOOT aus und gewinnt daraus Erkenntnisse über Verbindungen und Aktivitäten. Eine wichtige Abteilung ist →TAO (Tailored Access Operations), die gezielt, aber auch „auf Vorrat“, in fremde Systeme eindringt.

2015 wird bekannt, dass es auch seit vielen Jahren Offensive-Planungen bei der NSA gibt, mit dem Ziel sog. D Weapons im Krieg einzusetzen um durch großflächiges Zerstören der IT-Infrastruktur des Gegners ein Land zu lähmen und auch →Schadsoftware im →BIOS einzusetzen.

Siehe auch →DISHFIRE, →GILGAMESH, →VICTORYDANCE, →MONKEYCALENDER, →GOPHERSET, →Semantic Archive

NSL: (→National Security Letter)

NSO: israelisches Unternehmen das auf die Entwicklung von →Staatstrojanern spezialisiert ist. Wurde 2021 bekannt durch einen →Zero-Click Exploit auf →iOS-Geräte von →Apple. Kritisiert wurde vor allen Dingen, dass die Firma ziemlich wahllos auch in Diktaturen verkauft und die Software sehr stark zur →Überwachung kritischer Journalisten, Oppositioneller, aber auch europäischer Politiker eingesetzt wurde. Mehrere Regierungen haben juristische Schritte gegen das Unternehmen unternommen

NSP: (Network Service Provider) Anbieter von Fernverbindung für →Internet-Datenverkehr (Details siehe →Peering), im Gegensatz zu →ISP. Siehe →IXP, →CNI

NTFS: (New Technology File System) →File System, das ab MS Windows NT verwendet wird, sicherer →gegen Datenverluste. Neuere Versionen auch mit →Verschlüsselungsoptionen, z.B. →Bitlocker. →EFS

NTLM: (NT LAN Manager) →Authentisierungsprotokoll v. →Microsoft auf Challenge/Response-Basis, ähnlich wie →MS-CHAP. NTLM über →HTTP erlaubt ein →Single Sign-On auf →Webservern oder →Proxys auf Basis der Windows-Benutzeranmeldung. NTLM 1.0 (LAN Manager) gilt als unsicher, Kompatibilität muss disabled werden

NTP: (Network Time Protocol) Verfahren zur Abfrage der aktuellen Zeit von einem →Time Server. →Zugriff über dieses Protokoll muss im →Firewall erlaubt werden. RFCs 778, 891, 956, 958 und 1305. Wird seite 2013 verstärkt für →dDoS-→Angriffe genutzt, da es eine kaum genutzte Funktionalität gibt, wo zu Debugging Zwecken, der →Server auf eine kurze Anfrage eine lange Liste seiner letzten Aufrufe sendet (→amplification). Diese Liste kann mittels →Adress Spoofing an das Opfer gesendet werden, diesen Vorgang nennt man →Reflection

Nudge: Theorie im Bereich Behavioral Science das beschreibt, wie durch Manipulation der →Choice Archtitecture Menschen zu bestimmten Verhaltensweisen gebracht werden können ohne dass ihnen die Manipulation bewusst ist. Dies ist eine Gefahr beim →Contextual Computing, wo →Smartphone →Apps wie →Google Now benutzerbezogene Ratschläge geben

Null Log-on: (null sessions) im Domain-Konzept von Windows die Möglichkeit, dass eine Anwendung anonym auf →Shares oder →Accounts zugreift. Seit Windows 2000 kontrollierbar, aber als Default erlaubt. Mit Windows 2003 besser kontrollierbar

Nummernschilderkennung: →ANPR

NXDOMAIN: Non-Existent Domain bezeichnet eine →Internet-→Domain die vom →DNS nicht aufgelöst werden kann, z.B. weil sie (noch)

nicht registriert ist oder der Benutzer sich vertippt hat. Domainbetreiber, z.B. →ISPs versuchen zum Teil Geld damit zu verdienen indem sie diese Anfragen auf andere →Websites umleiten und dort →Werbung schalten (DNS Error Monetization). Siehe → Domain-Squatting, →Typosquatting

O365: Angebot von →Microsoft für Unternehmen und Private die MS Office Programme als →Cloud-Lösung zu nutzen (die entsprechende Lösung von →Google heißt →Google Workspace). Dabei können Firmen separate →Domainen einrichten lassen und gegen Aufpreis eine ganze Reihe von sicherheitsrelevanten Optionen aktivieren, z.B. Mandantentrennung innerhalb der „Firmenwolke“, →Authentisierung gegen das interne →AD mittels →AD FS, →DLP und →CASB zum Verhindern vom →Phishing →Angriffen gegen die →Accounts der Mitarbeiter im →Internet. Da die gesammte →Software →cloud-basiert angeboten und genutzt wird sind keine eigenen →Server mehr notwendig um eine Firmen-IT aufzubauen

OASIS: (Organization for the Advancement of Structured Information Standards) US-amerikanische Organisation die die Schaffung und Verbreitung von →XML-basierenden Standards fördert. Sie hat 2002 eine Untergruppierung →SSJC gegründet, die sich um Standards kümmert, die bei Sicherheitstechnologien hilfreich sind

OAuth: →Autorisierungsprotokoll mit dem ein Benutzer (user) einer Anwendung/→Website/ →Smartphone →App (Consumer) →Zugriff auf seine →Daten erlaubt die von einer anderen Anwendung/→Website (Service) verwaltet werden, ohne dass er sein →Passwort preisgeben muss. Wird von Flickr, →DropBox, Yahoo! →Google, →Facebook, MySpace, →Microsoft, →Netflix, →Twitter und anderen unterstützt (die zum Teil eigene Protokolle für diesen Zweck angeboten hatten). Konzept beruht auf dem Austausch eines limited access OAuth →Token (valet key). Diese sind jedoch nicht signiert, für die →Vertraulichkeit und →Authentisierung der beteiligten →Server müssen die Mechanismen von →SSL genutzt werden, was auf Grund der vielen Schwächen (z.B. fehlende gegenseitige Authentisierung, speziell bei →Smartphone →Apps) problematisch ist. →Google, das OAuth intensiv einsetzt, z.B. in →Google Docs, konzipiert daher ein Verfahren, bei dem bei der ersten Authentisierung des Benutzers auf einem Gerät die →App oder der →Chrome-Browser ein SSL-client Zertifikat erzeugt und damit dieses Gerät fest an diesen Kanal bindet („channel binding“).

OAuth ist kein →Authentisierungsprotokoll wie z.B. →SAML oder →OpenID, die jedoch mit OAuth kombiniert werden können. Siehe auch →WS FS

OBD: →On-Board-Diagnose

OBEX: (OBject Exchange Protocol) Protokoll zum Austausch von binären Objekten zwischen Geräten, z.B. über Infrarot (→IrDA) oder →Bluetooth, z.B. zum Austausch von Kontakten und Terminen (vCard und vCalender) und anderen Dateien zwischen →PC, →Handy und →PDA. Solche Transfers können natürlich zum Austausch von →Schadsoftware verwendet werden

Obfuscation: Erschweren der Analyse des Inhalts eines →Programmes, einer →Kommunikation oder →Nachricht, ohne dass dabei wirkliche Verschlüsselung eingesetzt wird, z.B. wenn ein Datenelement gescrambelt wird (z.B. mit XOR oder Vertauschung der Bitpositionen). →Code Obfuscation wird z.B. bei →Malware eingesetzt, um eine Erkennung zu vermeiden. Kann auch zum Schutz eingesetzt werden, da es „die Latte für den Angreifer höher legt“

Obscurity: (engl. Dunkelheit) „practical obscurity“ = etwas ist schwer zu finden, heute durch →Suchmaschinen und andere Internetfunktionen nicht mehr in dem früheren Maße gegeben. Neue Suchfunktionalitäten, wie z.B. →Facebook Graph oder die Timeline, stellen zwar technisch keine Sicherheitsverletzungen dar, da sie nur →Daten anzeigen, auf die bisher auch schon zugegriffen werden konnte, anderseits reduzieren sie jedoch trotzdem die →Privatsphäre von Personen. Ähnlich kann man in Bezug auf →Face Recognition argumentieren. Gesichter in der Öffentlichkeit sind sicher nicht →vertraulich, anderseits ergibt die technische Möglichkeit, ein Gesicht mit allen Fotos auf Facebook zu vergleichen sehr wohl eine Reduzierung der Privatsphäre. Das Konzept: “→’Security through obscurity’ does not work” = geheim halten eines →Algorithmus oder Speicherorts stellt keine Sicherheit her, ist zwar korrrekt, aber in vielen Fällen entsteht Privatsphäre nicht erst durch Geheimhaltung, sondern auch die Obscurity, dadurch, dass Informationen zwar nicht sicher verborgen sind, aber sehr schwer aufzufinden. Siehe auch →Shannon, →Kerckhoffs’ principle, →Scrambling

Obsoleszenz: Überalterung von Geräten aus anderen Gründen als der Ausfall der Geräte. In der IT sehr üblich, z.B. wenn wie bei →Windows XP keine Sicherheits→patches mehr erstellt werden und die Geräte dadurch verwundbar werden. Im Rahmen des →Internet of Things wird dies aber alle Geräte betreffen, die mittels →Embedded Systems software-gesteuert sind, z.B. →Autos, → medizinische Geräten (→IMDs) wie Herzschrittmacher, Insulinpumpen, u.ä., in Zukunft aber auch Haushaltsgeräte wie Waschmaschine und Kühlschrank. Bereits heute ein großes Problem bei →Android →Smartphones, für ca die Hälfte von ihnen gibt es keine Sicherheitsupdates, da die Android-

Anbieter Landschaft so zerklüftet ist, dass für die geringen Stückzahlen pro Gerät die Bereitstellung von Patches sehr teuer wäre

OCR: (optical character recognition) automatische Umwandlung von gedruckten Texten in leicht weiter zu verarbeitende elektronische Textdarstellung. Siehe →MRZ

OCS: (Office Communication Server) →Microsoft Product im Bereich →VoIP und →Messaging

OCSP: (Online Certifcation Status Protocol) Verfahren für →Certificate Authority um zu kommunizieren, welche →Zertifikate kompromittiert sind. Im Gegensatz zum →CRL-Verfahren wird dabei nicht die gesamte Liste aller abgelaufenen →Zertifikate, sondern nur der Status des nachgefragten Zertifikats übertragen. Das Verfahren gilt als gescheitert, da bei Nichterreichbarkeit des jeweiligen OCSP-Servers die →Webbrowser zur Sicherheit trotzdem den →Zugriff erlauben. Alternative Verfahren sind →HPKP, →Certificate Authority Authentication und →Certificate Transparency http://www.ietf.org/rfc/rfc2560.txt

OCSSP: (online content sharing service provider) die Zielgruppe des geplanten EU-Urheberrechts. Dies sind Plattformen bei denen die Nutzer Daten hochladen können, d.h. vor allem →Google mit →Youtube, aber auch Fotosharing und →Websites bei denen Texte hochgeladen werden können. Das Gesetz will durch Größenbeschränkungen die Lasten für kleinere (junge) Anbieter reduzieren. Siehe →Upload-Filter

Octave: (Operationally Critical Threat, Asset, and Vulnerability Evaluation) Risikomanagement-Methode, die von →CERT empfohlen und durch Tools unterstützt wird. http://www.cert.org/octave/

Oculus Rift: spezielle Brille (ähnlich einer Skibrille) mit integrierten Bildschirmen und Bewegungs→sensoren die für →virtual reality Nutzung gedacht ist. 2014 von →Facebook gekauft. Auf diese Weise soll ein „immersives" Erlebnis erreicht werden

Öffentlicher Schlüssel: →Verschlüsselung

Off-the-Record Messaging: (OTR) neues Prinzip der Nachrichten-→Verschlüsselung von →Instant Messaging (als Produkt verfügbar von http://www.cypherpunks.ca/otr/). Es bietet Vertraulichkeit, Authentisierung der Gegenstelle und es kann später nicht mal festgestellt werden, ob ein bestimmter → Schlüssel von einer bestimmten Person genutzt wurde (→deniability) und auch →PFS. Gilt als eines der wenigen Messaging Protokolle die auch 2014 nicht durch die →NSA zu entschlüsseln sind. Nutzt →AES, →Diffie-Hellmann und →SHA-1

Office of Personel Management (OPM): US-Behörde die alle Regierungsangestellten betreut, inkl. Geheimdienst und Militär. OPM wurde 2015 Opfer eines großen →Angriffs (China zugeschrieben) bei dem große Mengen an extrem sensiblen →Daten entwendet wurden (→Data breach). Es soll zu schweren Konsequenzen für Mitarbeiter des CIA, etc geführt haben

OIO: (Offensive Operations Information) neuer Begriff für →Information Warfare

OK: →organisierte Kriminalität

OLPC: (one laptop per child) Initiative für einen Laptop unter 100 $ für →computer literacy in Entwicklungsländern. 100 $ ist letztendlich nicht gelungen, es wurden jedoch bis 2011 2,4 Mio Geräte an Kinder verteilt. Das Projekt hat als Nebeneffekt zur kommerziellen Einführung der sog. Netbooks geführt, die zum halben Preis von →Laptops erhältlich sind. Benutzt neues Sicherheitskonzept →Bitfrost

OLSR: (Optimized Link State Routing Protocol) →IP-protocol für den Aufbau von drahtlosen ad-hoc Netzen, z.B. zwischen Mobilfunkgeräten

On-Board-Diagnose: (OBD) eine physische Schnittstelle (Stecker) im →Auto über den ein →Laptop →Zugriff auf die Elektronik, d.h. die vielen →Computer im Auto bekommt. Dies dient, wie der Name sagt, hauptsächlich zum Auslesen von Fehlerprotokollen (→Logs), bzw. um die Elektronik auf einem definierten Ausgangszustand zurückzusetzen („reset"). Unabhängige Werkstätten und Pannendienste bemängeln, dass sie oft keinen →Zugang zu dieser Schnittstelle bekommen (oder mittels sehr mühsamen Anfragen), anderseits wurden diese Zugänge auch benutzt, um Fahrzeuge zu „übernehmen". Die Fahrzeugdaten können im Falle eines Unfalls sehr wichtig sein, bzw. können nach dem Verkauf des Fahrzeugs eine →Privatsphäre-Verletzung darstellen, da dort zum Teil auch die früheren Routen verzeichnet sind

OneCare: früherer Sicherheitsdienst von → Microsoft für Privatkunden. Enthielt →Virenschutz, Spywareschutz u. ä. Funktionalitäten. Immer noch kostenlos verfügbar ist →MSRT, für Firmen gibt es kostenpflichtig →ForeFront. Ab 2009 durch Microsoft Security Essentials abgelöst

One-time-Password: →OTP

Onion: (.onion) spezielle →Domain-Endung (statt z.b. .com) für →Websites, die nur im TOR-Netzwerk erreichbar sind. Mehr Information unter →TOR

Onion-Routing: siehe →TOR

Online-Durchsicht: einmalige Momentaufnahme bei →RFS-Einsatz

Online Durchsuchung: →Online Durchsicht und →Online-Überwachung

Online-Überwachung: →RFS-Einsatz über einen Zeitraum, inkl. →Keylogger

ÖNORM: (Österreichisches Normeninstitut)

Normungsbehörde, hat auch zahlreiche sicherheitsrelevante →Standards erlassen. Siehe →DIN, →ANSI, →ISO, →NIST

ONR 17700: wichtige Önorm zum Thema →Web Application Security, liegt in engl. vor und wird vermutlich international genormt

ONS: (Object Naming Service) zentraler Service, der nach dem Auslesen des →EPC (Electronic Product Code) eines →RFID-Tags auf einen oder mehrere Rechner verweist, auf welchen Produktinformationen zu finden sind (Hersteller, Großhändler, Einzelhändler). Der Aufbau ist ähnlich wie der →DNS-Service für →Domain-Adressen im →Internet (root ONS, local ONS). Der ONS Service verweist auf andere Rechner auf denen die Produktinformationen (authoritative product manufacturer information) im →PML-Format [Physical Markup Language, eine Untermenge von →XML] abgelegt sind und für alle Mitglieder der Business Organisation abrufbar sind. Dadurch ist ein Nachverfolgen eines Produktes vom Hersteller bis zum Kunden möglich. Zugriff zu den über EPC erschließbaren Informationen wird reguliert über eine Authentifizierung mittels →Zertifikaten (ausgestellt von speziellen →CAs) und →ACLs, gesetzt durch den „Owner" des jeweiligen EPCs für seine Trading Partner

OPC UA: (OPC Unified Architecture) ein industrielles →M2M-→Protokoll, vorgeschlagen bereits 2006 von der OPC Foundation das eine wichtige Rolle bei →Industrie 4.0 spielen soll. Das →BSI hat die Sicherheit geprüft und keine systematischen Sicherheitslücken identifiziert. Diese können aber typischerweise auch durch Implementierungsfehler entstehen

Open Banking: →PSD2

OpenBazaar: open source Projekt für eine dezentrale Handelsplatform auf der Basis von →Bitcoin und →TOR. Nachdem das FBI 2013 die Silk Road website geschlossen hatte begann 2014 die Entwicklung an einer dezentralen Architektur, die nicht zentral geschlossen werden kann, da die Angebote weltweit verteilt sind. Das wäre eine ideale Platform für illegale Handelsaktivitäten, siehe →Darknet Market

Open Data: →Daten die von jedermann zu jedem Zweck genutzt, weiterverbreitet und weiterverwendet werden dürfen. Wenn die Daten von Behörden zur Verfügung gestellt werden, so wird dies auch als →Open Government bezeichnet. Dabei geht es darum, dass diese Daten (leicht) maschinenlesbar und entgeltsfrei sein sollen. Die Daten sollten (auch) in maschinell auswertbaren Formaten vorliegen, z.B. nicht →PDF, sondern →XML oder →JSON damit eine digitale Weiterverarbeitung leicht möglich ist. Da geht es entweder für neue Dienste, z.B. →Apps die diese Daten visualisieren, z.B. die Positionen von Bussen oder Zügen oder auch für Barrierefreiheit für Vorlese-Programme für Sehbehinderte.

Open Government: Bereitstellen von →Open Data durch Behörden (Exekutive, Legislative, Judikative). Ein Beispiel kann das Veröffentlichen von Sitzungsprotokollen oder Urteilen in leicht auswertbarer Form sein (so dass z.B. (historische) statistische Auswertungen und Analysen leicht möglich sind) oder andere Daten wie Verkehrsflüsse die durch die →Sensoren der Dienstleister anfallen

OpenID: dezentrales →Identitätsmanagementsystem (d.h. →Federated Identity Framework wie →CardSpace und →Geneva) für →Web-Anwendungen, bei dem der →Webserver mit einem →Identity Provider Kontakt aufnimmt, demgegenüber der →Benutzer sich authentifiziert. Die Sicherheit hängt von der Art dieser →Authentifizierung ab. Der Austausch erfolgt mittels →Protokollen wie →WS-FS und →SAML. Siehe auch →OAuth, →BrowserID

Open Government: Forderung nach Transparenz in Politik und öffentlicher Verwaltung. Dazu gehören auch Forderungen nach Kollaborations- und Partizipationsmöglichkeiten für einzelne Bürger oder Organisationen. Dies sollte nicht nur technisch/digital implementiert werden, sondern auch durch Workshops, Barcamps, Interviews und andere Formen des direkten Kontakts

Open Graph: 2011 von →Facebook angebotene →API mit deren Hilfe das Konzept des →Like-Buttons auf beliebige Beziehungen erweitert. Verben können jetzt definiert werden wie hört, sieht, kauft, besucht, etc. zusammen mit entsprechenden Objekten wie Orten oder Musikstücken. Alle Daten die so anfallen sind Teil des →Social Graphs

Open Redirect: →Schwachstelle bei →Websites, wenn diese die Funktionalität anbietet, dass eine →URL dieser Website konstruiert werden kann, die auf beliebige andere (böse) Websites weiterleitet

Open Relay: Mailserver, der schlecht konfiguriert ist und deswegen eine anonyme Weiterleitung von →E-Mails von →Spam-Versendern erlaubt, heute weitgehend durch →Botnets ersetzt. OpenRelays kommen auf eine →Blacklist (→DNSBL). E-Mails von diesen Mailservern werden dann von vielen anderen Mailservern nicht mehr angenommen

Open Social: von →Google 2007 (als Nachzügler in diesem Geschäftsbereich) entwickeltes →Protokoll (→API) für den Transport persönlicher →Daten zwischen →Social Network →Websites. Ziel ist es, dass Benutzer eines →Netzwerks mit Benutzern oder Funktionen anderer Netzwerke interagieren können, bzw. dass Daten zwischen Netzwerken ausgetauscht werden können. Könnte eine weitere →Bedrohung für die →Privatsphäre der Teilnehmer darstellen

Open Software Foundation: Organisation, die die →GPL (weiter)entwickelt. Siehe →Open Source

Open Source: →Software, die im offenen Austausch von →Quellcode weiterentwickelt wird. Regeln sind: alle haben Zugriff auf den Quellcode und dürfen ihn frei verwenden. Wenn dabei Weiterentwicklungen entstehen, so unterliegen diese auch diesen Regeln. Dies ist vor allem wichtig bei →kryptographischer Software, da nur so die Gefahr von →Backdoors reduziert werden kann. Leider hat sich im konkreten Fall von →OpenSSL und dem →Heartbleed bug dies als Fehleinschätzung herausgestellt. So bekommen einige Open Source Aktivitäten sehr hohe Aufmerksamkeit und Unterstützung auch durch Firmen (z.B. →Linux), andere werden von nur wenigen Freiwilligen in ihrer Freizeit betrieben und können daher nur schwer die notwendige Qualitätssicherung erreichen. Eine wichtige Unterstützung die Firmen welche Open Source Produkte einsetzen, liefern können sind z.B. →Pentests und Programm-Audits, deren Ergebnisse den Entwicklern zurück gemeldet werden. Siehe →Open Software Foundation, →GPL, →HackerOne, →fork

Open Source Intelligence: Methode die von Polizei und Geheimdiensten genutzt wird. Dabei werden Informationen aus öffentlich zugänglichen Quellen wie z.B. →Suchmaschinen im Internet genutzt. Siehe auch →ENLETS

Open Source Research: Vorgangsweise bei der Angreifer oder Spionagebehörden öffentlich zugängliche Quellen nutzen um an Informationen zu kommen, die dann für einen weiteren →Angriff genutzt werden können. Wichtig vor allem bei →Social Engineering

OpenSSL: vermutlich meistgenutzte Bibliothek für →Verschlüsselungsroutinen, verfügbar als →Open Source. OpenSSL wird in vielen kommerziellen und nicht-kommerziellen Produkten eingesetzt. Es kam zu trauriger Berühmtheit, als 2014 der →Heartbleed Bug entdeckt wurde und damit 2/3 der →Webserver im →Internet verwundbar waren. Trotzdem gilt Open Source immer noch als sichere Alternative zu kommerzieller Software. OpenSSL unterstützt auch das Protokoll TLS

OpenStack: Framework zur Erstellung und Administration von öffentlichen oder privaten →Cloud-Lösungen. AT&T, AMD, Brocade Communications Systems, Cisco, Dell, EMC, Ericsson, F5, Go Daddy, Groupe Bull, Hewlett-Packard, IBM, Inktank, Intel, NEC, NetApp, Nexenta, Rackspace Hosting, Red Hat, SUSE Linux, PLUMgrid, VMware, Oracle and Yahoo! sind beteiligt. Die Software (APIs) sind kompatibel mit Amazon →EC2 und S3

OpenVZ: neues Virtualisierungskonzept, bei dem ohne Virtualisierungslayer gearbeitet wird, sondern mit sog. Container die alle einen gemeinsamen Kernel nutzen. Dadurch gibt es nur sehr geringe Trennung zwischen den „guest“ Systemen. Dies ist von den Resourcen her effizient, aber bietet nicht die Sicherheit einer wirklichen Virtualisierung wie z.B. →VMware

Operating System: (OS) →Betriebssystem

Operationelles Risiko: (OpRisk) (oft auch operationales R.) Gefahr von Verlusten als Folge unzulänglicher oder fehlgeschlagener interner →Prozesse (z.B. nicht entdeckter Betrug), Menschen und →Systeme oder von externen Ereignissen. Nach →Basel II gibt es 7 „event types“: internal fraud, external fraud, employement practise & workplace safety (enthält auch Diskriminierung), clients, products & business practise (Marktmanipulation, Antitrust, Bilanzfälschung), damage to physical assets, business disruption & systems failure (Stromausfall, Hardware- und Software-Fehler), Execution, Delivery & Process Management (Dateneingabefehler, Buchhaltungsfehler). Siehe auch →AMA

Operatives Risiko: das komplexen →Systemen und →Prozessen inhärente Fehlerrisiko, eine Untermenge des →operationellen Risikos (OpRisk)

Opportunistic Encryption: neues Schlagwort, das nach →Edward Snowden geprägt wurde. Es beschreibt verschlüsselte Verbindungen, bei denen sich jedoch nicht zuerst die beiden Gegenstellen ihrer →Identität versichern, so wie es nötig ist um Man-in-the-Middle →Angriffe zu verhindern (was den Einsatz von →Zertifikaten auf beiden Seiten erfordern würde), sondern eine Verschlüsselung ohne Absicherung der Identität der Gegenstelle aufbauen. Diese Verbindungen sind dann zwar immer noch mittels Man-in-the-Middle angreifbar, jedoch erfordert dies deutlich mehr Aufwand als ein einfaches Kopieren der Daten auf der Leitung

OpRisk: →operationelles Risiko

OpSec: (operational security) →Hacker-Terminologie für Vorsichtsmaßnahmen die die Sicherheit und →Anonymität im →Internet erhöhen. Die vielen →Data Leakage Fälle seit 2014 führen dazu, dass mehr und mehr Menschen OpSec lernen sollten, z.B. dass man unterschiedliche →Passworte für unterschiedliche Zwecke nutzt, peinliche Dinge nicht vom Arbeitsplatz aus tut (da gibt es einen →Proxy der alles mitschreibt), dass man sich für solche Dinge einen falschen E-Mail-Account anlegt, etc.

Opt-In: Konzept, bei dem ein Benutzer eine explizite Zustimmung zu etwas geben muss. Z.B. Zusenden von → E-Mail erst nachdem der Empfänger die Erlaubnis gegeben hat (→Permission Marketing). Ziel ist die Vermeidung von →Spam. Die Erlaubnis kann durch Anklicken auf einem Anmeldeformular geschehen, erweitert auch durch verified- oder

confirmed-Opt-In, d.h. der Kunde muss auf ein Bestätigungs-E-Mmail antworten, bevor er registriert wird. Das gleiche gilt für andere Aspekte wie Speicherung von →Cookies (geplante EU-Forderung), oder →Tracking von Benutzerverhalten. →Datenschützer favorisieren Opt-In-Verfahren. Siehe auch →Opt-out, →Choice Architecture

Opt-Out: Konzept, bei dem ein Benutzer keine explizite Zustimmung geben muss, sondern lediglich die Möglichkeit hat, nachträglich etwas zu verhindern oder zu blockieren. Opt-Out wird von Marketing- und Werbefirmen gegen über Opt-In bevorzugt, auch →Facebook ist bekannt dafürm maximal Opt-Out anzubieten. Z.B. die Möglichkeit der Stornierung von unangeforderten →E-Mails (→UBE, →UCE, →Spam). Unter gewissen Umständen legal, wenn der Kunde die Möglichkeit hat, über eine → Website oder ein Antwort-E-Mail zukünftige Zusendungen zu verhindern. Bei Mailversand sollte auf jeden Fall die →Robinson Liste respektiert werden. Unterschiedliche Regeln in jedem Land.

Opt-Out wird auch bei →Behavioural Advertising angeboten. Dabei findet jedoch weiterhin ein →Tracking der Benutzer statt, lediglich werden die Werbeeinschaltungen nicht auf der Basis der trotzdem gesammelten →Informationen über den →Benutzer (→PII) geschaltet. Siehe auch →Choice Architecture

Oracle:

α) US-Unternehmen das durch seine → Datenbanksoftware bekannt wurde. Ua.a. durch Übernahme von anderen Softwareprodukten wie →Java führt Oracle 2011-2013 oft die Liste der häufigsten →Verwundbarkeiten an

β) Klasse von →Angriffen gegen →Verschlüsselungen

Orange Book: →TCSEC, →Common Criteria/ ISO 15408

Organisierte Kriminalität: (OK) Kriminalität unter Verwendung gewerblicher oder geschäftsähnlicher Strukturen. Seit ca. Mitte 2004 auch stark im →Internet aktiv, z.B. durch Finanzierung von →Hackern, →Erpressung über →dDoS-Angriffe, Durchführung der Geldtransfer und →Geldwäsche nach →Phishing-Angriffen. Siehe →Hacker, →VX, →Botnetz http://sicherheitskultur.at/spam.htm#OK

ORIMOR: (Open Risk Model Repository) Open Source-Projekt für die Entwicklung eines IT-→ Risiko-Modells, Tools und Handbücher. http://www.somap.org/repository/default.html

OS: (operating system) →Betriebssystem

OSI Schichtenmodell: von →IEEE standardisierte Konzeption für Netzwerke, beruhend auf 7 Schichten (→Layer) mit unterschiedlichen Aufgaben und definierten Schnittstellen, erlaubt die Entwicklung und den leichteren Austausch von Komponenten im Kommunikations-→Stack. →TCP/IP nutzt statt 7 nur 4 Schichten. Siehe →Segment

OSOR: (Open Source Observatory and Repository) EU-Organisation, die die Nutzung von Open Source Software für →öffentliche Verwaltungen unterstützt

OSS: (Open Source Software) Software, die im →Quellcode und unter →Open Source Lizens-Schemata verfügbar ist. Siehe →GPL, →Copyleft, →Lizenz

OSSTMM: (Open-Source Security Testing Methodology Manual) Zusammenstellung von →Best Practise Regeln für das systematische Testen von IT-Umgebungen im Hinblick auf →Risiken und →Schwachstellen. Es enthält →Penetration Testing als einen Aspekt. http://www.osstmm.org/

OStatus: offener Standard für →Micro-Blogging zum Aufbau eines föderativen →Social Networks. Das →Protokoll OStatus wird implementiert von GNU social, →Friendica, →Mastodon, Pleroma, Hubzilla, und weiteren. Siehe →Fediverse

Österreichisches Informationssicherheitshandbuch: Sammlung von Regeln und Best-Practise Vorgaben. https://www.sicherheitshandbuch.gv.at/

osTriage: flexible →Forensic-Software, typischerweise auf einem →USB-Stick, die eine Kurzanalyse eines →PCs durchführt und dabei →Dateien, aber auch Logs u.ä. untersucht. Kann über →Hash-Codes 500 000 Dateien erkennen und nach über 300 Schlüsselworten suchen

OSVDB: (Open Source Vulnerability Database) öffentliche Datensammlung zu →Verwundbarkeiten auf der Basis von →CVEs

OTA: (→over-the-air), z.B. OTA-Update

OTP:

1) (One-time-Password) Einmalpasswort, ein Verfahren um eine Authentifizierung einer Person gegen das Abhören und →„Replay" sicher zu machen. Früher waren die Haupttechnologien vorgedruckte →TAN-Listen, besser sind →Token, d.h. Geräte die sich ständig ändernde →Passworte generieren und anzeigen. Diese Variante ist auch als →App auf →Smartphones verfügbar. Auch OTPs schützen (so wie →2-Faktor-Authentifizierung) nicht 100% gegen →Phishing →Angriffe, machen aber den Angriff für die Angreifer schwieriger. Bei Risk-based-Authentication wird automatisiert entschieden, ob der 2. Faktor angefordert wird, dies lässt sich austricksen. Siehe auch →FIDO, →HOTP und →TOTP

2) (Online Transaction Processing) spezielles Datenbankverfahren, das sehr schnellen →Zugriff auf meist kurze Datensätze erlaubt

OTR: (→Off-the-Record Messaging)

OTS: (over-the-shoulder) Konzept in →Vista bei der der → Benutzer mit Standard-Rechten arbeitet, aber für bestimmte Aufgaben das lokale Administrator-Passwort eingeben muss. Dies kann auch über →Remote Assistance geschehen

Outlook Web Access: (OWA) →Web-Anwendung, die ein →Zugriff auf →E-Mails im →Microsoft Exchange Server mittels →Web-Browser erlaubt. Siehe →WebReady Document Viewing

Out-of-Band: (OOB) Sicherheitskonzept, bei mehrere Datenkanäle genutzt werden, die nicht gleichzeitig überwacht oder kontrolliert werden können. Z.B. wenn sensible Informationen erst dann entschlüsselt oder verarbeitbar gemacht werden können, wenn eine zusätzliche Information über einen anderen Datenkanal übertragen wurde. Beispiel ist auch die Versendung eines →PIN-Codes auf Papier oder per →SMS

Out-of-band Autorisierung: →Autorisierung z.B. einer →e-Banking Transaktion mit Hilfe eines 2. Kanals, z.B. →SMS (→mTAN). Setzt aber getrennte Geräte voraus, d.h. verliert die Schutzfunktion wenn sowohl e-Banking wie SMS-Empfang auf demselben Gerät passieren

Outsourcing: (Outside Resource Using) Rückgriff auf Quellen/Ressourcen außerhalb (des Verantwortungsbereiches) des Unternehmens. (Als „Nearshoring“ bezeichnet wenn die Dienstleister in regional nahen Ländern sitzen) Dabei müssen durch →SLAs die jeweiligen Sicherheits- und Verfügbarkeitsanforderungen festgelegt werden, einschließlich der Aspekte eines →Katastrophen-Falls. Oft wird angenommen, dass auf diese Weise auch Verantwortungen übertragen werden können, dies ist jedoch nicht der Fall. Es wird zwischen captive und non-captive outsourcing unterschieden. Dabei bezeichnet captive outsourcing einen Dienstleister der Teil des Konzerns ist (oder verbleibt). Non-captive sind alle anderen Nicht-Konzern Dienstleister, z.B. die vielen →cloud computing Anbieter, die oft nur für einzelne Funktionen genutzt werden, z.B. →O365 für Office-Funktionen oder SAP (→SaaS), bzw. →hosting oder →housing.

Weitestgehende Möglichkeit: Auslagern der gesamten eigenen IT-Abteilung zu einem externen Anbieter, oft einschließlich Übernahme der existierenden Hardware, Räumlichkeiten und Personal. Dabei verbleibt typischerweise eine →Retained Organisation im Unternehmen, oft einige der ursprünglich in der IT arbeitenden Kollegen

OVAL: Standard für den Austausch von sicherheitsrelevanten Informationen, z.B. Sicherheitswarnmeldungen auf der Basis von →XML. In OVAL geschriebene Inhalte findet man beispielsweise in dem von der MITRE Corporation betreuten OVAL-Repository. Siehe →CVE, →CME

Overnet: Protokoll für →P2P, z.B. in →eDonkey genutzt, aber auch von →Storm Worm

Over-the-Air: (OTA) Over-the-Air Provisioning (OTAP), Over-the-Air Update oder Over-the-Air Programming. Methode zur Installation oder Aktualisierung von entfernten Geräten, z.B. bei →IoT, aber auch bei →Smartphones. Bei Smartphones gibt es dafür standardisierte Verfahren bei denen mittels →SMS Aktualisierungen in →SIM-Karten oder →Handys durchgeführt werden können. 2019 wurden →Schwachstellen in diesem Protokoll gefunden. Generell stellen solche OTA Aktualisierungen Herausforderungen dar, da z.B. bei einem Abbruch der Verbindung (z.B. bei Verbindungsunterbrechung durch Stromausfall) ein Gerät (z.B. ein modernes Auto) funktionslos werden kann (→“brick“). Dies ist bei modernen Autos ein großes Thema, da heute das Verhalten eines Fahrzeugs weitgehend durch →Software bestimmt wird. Dies bedeutet, dass es fehleranfällig ist, und dass für die Behebung ein Software-Update notwendig ist (→Patchen). Wenn dies nur im Rahmen einer Rückrufaktion in die Werkstatt möglich ist, so ist dies mit hohen Kosten für den Hersteller verbunden. Anderseits besteht das Risiko des „bricks“

OWA: →Outlook Web Access

OWASP: (Open Web Application Security Project) gemeinnütziges Projekt für sicherere →Web-Anwendungen. Siehe →Application Security, →Sprajax, →WAP, →ONR 17700

OWASP Top Ten: aktualisierte Liste der wichtigsten →Verwundbarkeiten von →Web-Anwendungen

OWL: (Web Ontology Language) formale Sprache zur Darstellung von Beziehungen zwischen Objekten, in diesem Fall Informationen im →Web. Siehe →Semantic Web, →FOAF

Oxy Reduct: Anbieter einer Lösung zur →Brandvermeidung, der Begriff wird jedoch oft auch generisch genutzt. Ein anderer Anbieter ist Permatec. Siehe →Brandschutz

P2P: (Peer-to-Peer Networking) Technologie bei der →Rechner direkt miteinander kommunizieren ohne über zentrale →Server zu gehen. So findet die Sprach- und Video-Kommunikation bei →Skype ohne den zentralen Server statt, der z.B. die Anmeldung durchführt oder Teile der Text-→Chats.

P2P wird seit 2012 auch eingesetzt, um →Botnets weniger anfällig für das Ausschalten der zentralen Server (→C&C Server) zu machen. Siehe →sinkholing
P2P steckt auch hinter modernen →Tauschbörsen (→Filesharing), mit deren Hilfe mehr oder weniger legal, →Dateien (Musik, Filme, Programme, Bilder) zwischen beliebigen

Rechnern direkt, d.h. diskret, ausgetauscht werden können. Eine der ersten P2P-Implementierungen war →Napster. 2005 machte auch →KaZaA Schlagzeilen, oft negativ im Sinne einer Sicherheitsbedrohung. Moderne Systeme (2010) wie →BitTorrent arbeiten sehr dezentral und sind sehr schwer zu überwachen. Aus diesem Grund werden P2P-Techniken verstärkt bei der Steuerung von →Botnets eingesetzt. Siehe jedoch →Deep Packet Inspection zur Identifizierung Protokollen trotz →Verschlüsselung, z.B. durch Ausnutzung von spezifischen Sequenzen beim Aushandeln der Schlüssel oder durch typische Blockgrößen oder Timings.

P2P-Netze können durch →Sybil Attacks (Sybil nodes) angegriffen werden

P300: bei einem EEG (Elektroenzephalogramm) Signal eine Welle die 300 ms nach einem Ereignis auftritt das die Aufmerksamkeit der Versuchsperson erregt. Wird für →Brain Computer Interfaces (BCI) verwendet, u.a. um bei Behinderungen. Problematisch, wenn es bei der Befragung von Verdächtigen genutzt wird um festzustellen, ob bestimmte Bilder die nur der Täter kennen sollte, bei den Befragten dieses Signal auslösen (guilty knowledge). Wissenschaftlich nicht ganz geklärt

P3P: (Platform for Privacy Preferences) Verfahren, damit →Websites auf einfache Weise ihre →Privacy Policy in →XML ausdrücken können, sodass diese vom Nutzerrechner automatisiert ausgewertet werden kann. Der Nutzer entscheidet dann, ob er die Website unter den gegebenen Bedingungen besuchen möchte oder nicht. P3P als universeller, technischer Standard erlaubt es, weltweit im ganzen →Internet →Datenschutz-Policies für die Nutzer transparent zu machen. Die Nutzer hätten damit eine größere Kontrolle darüber, was mit ihren persönlichen Daten geschieht. Siehe →Privatsphäre

PAA: (Protect America Act) Erlaubnis für die US-Behörden zum →Abhören von Kommunikation innerhalb der USA ohne Richterbeschluss, solange die Annahme besteht, dass mindestens 1 Partei außerhalb der USA ist. Siehe →Patriot Act

PAC: (proxy auto-configuration) Protokoll zur automatischen Konfiguration eines →Webbrowser zur Nutzung eines Reverse →Proxys. Kann für Umleitung des Datenverkehrs eines →Webbrowser und somit für →Man-in-the-Middle →Angriffe genutzt werden

PACE: (→Password →Authentication Connection Establishment) vom deutschen BSI entwickeltes →Protokoll für den Aufbau eines sicheren Kommunikationskanals zwischen einem →Chip und einem Lesegerät, verwendet für den elektronischen Personalausweis (→ ePerso), soll →BAC im →ePass ersetzen

Packet: (engl. für Paket) in der →IP Paket, ein Datenblock, der an eine bestimmte Empfangsadresse übertragen werden soll. Kann aus →Integritätsgründen eine →Checksum enthalten oder aus →Vertraulichkeitsgründen verschlüsselt sein

Packetfilter: Software, die bestimmte →IP-→Pakete analysiert und bei bestimmten Inhalten Aktionen unternimmt. Teil z.B. eines →Firewalls

Packet Sniffer: →Programm oder Gerät, das Daten→pakete in →Netzen aufzeichnet, kann für die Fehlersuche oder als Angriffstool verwendet werden. Siehe →Paketfilter

Page: (engl. Seite)

1) Struktur von →Websites durch einzeln aufrufbare Dateien, i.d.R. im →HTML-Format

2) logische Struktur von →Hauptspeicher bei →Betriebssystemen mit virtueller Speicherverwaltung (→virtual memory). Für einzelne Pages können zumeist Sicherheitsattribute gesetzt werden, z.B. →DEP

Pairing: bei →Bluetooth der Vorgang, mit dem eine Vertrauensbeziehung zwischen zwei Geräten hergestellt wird. Wenn diese Beziehung, wie bei →Unit Keys, permanent erhalten bleibt, so kann dies ein Sicherheitsrisiko darstellen. Siehe →Bluesnarfing

Paket: →Packet

Palladium: von →Microsoft entwickeltes Sicherheitskonzept, heute →NGSCB genannt.

Palm OS: Betriebssystem für →PDAs und →Smartphones

PAM: (process assessment model) →SPICE

PAN:

1) (Personal Area Network) Netz aus →Bluetooth-Geräten (PAN User = PANU). Dabei kommt manchmal →UWB zum Einsatz

2) (Primary Account Number) →Kreditkartennummer. Muss nach den →PCI-DSS-Regeln gut geschützt werden, durch z.B. nur teilweise angezeigt werden

Pandemie: länder- und kontinentübergreifende Ausbreitung einer Krankheit (Epidemie ist lokal begrenzt). Wird durch Nicht-Verfügbarkeit von Personal (entweder durch die Krankheit selbst oder durch Quarantäne-Maßnahmen) und dadurch bedingte Knappheit aller Ressourcen schnell sicherheitsrelevant. →Notfallpläne und →BCM sollten daher darauf eingehen. Siehe →2020

Parler: →Social Network. Eigenbeschreibung: „→Twitter ohne Zensur“, viele „rechte“ Inhalte, auch Antisemitismus, →QAnon-Inhalte), starkes Wachstum Ende 2020 (10 Mio registrierte Nutzer, 4 Mio aktive). Jan. 2021 aus den →App-Stores und von →AWS entfernt und damit vorläufig beendet (gerade als viele „Konservative“ dorthin umziehen wollten)

Partial adversary: anderes Wort für →local adversary

Partition: Technik, bei der eine →Festplatte (oder ein anderes Speichermedium wie →SSD oder →Flash-Speicher) in mehrere logische Teile aufgeteilt wird. Jede Partition kann möglicherweise ein anderes →Betriebssystem enthalten von dem wahlweise gestartet werden kann. Eine solche Aufteilung kann auch aus Sicherheitsgründen durchgeführt werden, z.B. um die Daten getrennt vom Betriebssystem sichern zu können

Passkey: wird bei der Herstellung eines →Pairings zwischen zwei →Bluetooth-Geräten auf beiden Geräten eingegeben und dient der Erstellung des →Link Keys

Passphrase: Längere und daher sicherere Version des →Passworts, in der Regel aus mehreren Worten bestehend

Passport: Versuch von →Microsoft, eine zentrale Stelle für die →Authentisierung von →Webanwendungen unterschiedlicher Art zu schaffen. Umstritten wegen der zentralen Kontrolle aller Daten durch 1 Hersteller. Genutzt u.a. für hotmail und andere Microsoft-Dienste. Siehe →federated identity. →CardSpace

Pass-the-Hash: →Angriffstechnik, bei der ein „gefundener" →NTLM-→Passwort →Hash verwendet wird, um sich bei einem anderen System anzumelden ohne das eigentliche Passwort zu kennen, wird bei →APTs oft verwendet um sich weiter im Netz des Unternehmens zu verbreiten

Passwort: (in Kombination mit dem →Benutzernamen oft →Credential) geheime Zeichenfolge, die zusammen mit der →Benutzerkennung des Nutzers zur →Authentisierung des Benutzers dient und den Zugriff auf geschützte Rechner, →Websites oder Dateien erlaubt. Ein „starkes" Passwort hat eine hohe →Entropy, d.h. ist nicht zu kurz, alphanumerisch mit Sonderzeichen. Die Stärke eines Passworts wird oft als →Zero-order Entropy gemessen. Dies ist aber problematisch, da viele Aspekte wie die Nutzung der Listen von häufig genutzten Passworten (→Passwort Leaks) durch „Cracker" (siehe →Passwort-Recovery, →Credential Stuffing) nicht berücksichtigt werden. Daher ist die Einmaligkeit von Passworten ein noch wichtigerer Faktor für die →Sicherheit als die Stärke. Einmaligkeit bedeutet dass diese Zeichenfolge auf keiner anderen Website genutzt wird. Dies erfordert vom Benutzer die Nutzung eines →Passwort-Safes http://sicherheitskultur.at/Passworte.htm#tricks

Durch Authentisierung sollen unberechtigte Personen von Diensten ausgeschlossen werden (→Authorisierung). Besser sind →Einmalpassworte (OTP), entweder in Form von →TAN Listen oder über →Token, bzw. Authentisierungen über →Smartcards. →Biometrie ist eine weitere Alternative.

2 wichtige Angriffe sind → Passwort Stuffing und →Passwort Spraying.

Siehe →ZKPP, →PStore, →Passwort Ablauf, →Passwort Hashing

Passwort Ablauf: Zwang zum Ändern eines Passworts nach Ablauf einer Periode, zumeist 1 Monat. Umstritten, da gute Passworte länger sicher sind, und in falschen Händen viel schneller als in 1 Monat „geknackt" sind. Siehe →Brute Force, →Rainbow Table

Passwort Hashing: Methode zum Schutz gegen →Brute Force Angriffe gegen Passworte. Dabei wird jedes Passwort vor dem Hashen mit einem Zufallsstring verlängt, der →Salz genannt wird. Danach wird ein extra langsamer →Hash-Algorithmus eingesetzt, z.B. →PBKDF2, →Bcrypt, →Scrypt. Zumeist wird der Algorithmus noch für eine große Zahl von „rounds" immer wieder auf das Ergebnis des Algorithmus angewendet. Ziel ist, den Resourcenaufwand für Brute Force Angriffe möglichst hoch zu machen

Passwort Leak: Sammlungen von →Passworten die öffentlich bekannt geworden sind. Typischerweise gelingt dies durch Ausnutzen von →Verwundbarkeiten in →Websites oder über →Phishing. Diese Sammlungen werden von Kriminellen weiterverkauft und dann für illegalen →Zugang zu anderen Konten genutzt. Sicherheitsforscher bieten auch Zugang für alle zu solchen Sammlungen damit man z.B. sehen kann, ob der eigene →Account in einem Leak enthalten ist oder um zu sehen, ob eigene Passworte von Kriminellen genutzt werden. 2 prominente Sammlungen für die Nutzung durch jedermann sind (dort kann geprüft werden ob ein eigenes Passwort auf einer Website kompromiert, d.h. leaked wurde: https://sec.hpi.de/ilc/ und https://haveibeenpwned.com/

Password Recovery:

1) (=Password Cracking) Programme, die durch Methoden wie →Brute Force und →Dictionary Attack →Passworte „knacken". Sehr leicht durchzuführen, wenn Zugriff zum angegriffenen System besteht, z.B. nach Verlust eines →Laptops. Diese Programme sind auch kommerziell erhältlich und können gegen Windows, aber auch →Zip-Dateien und verschlüsselte Office-Dokumente eingesetzt werden
2) →Passwort Reset

Password Renewal: anderes Wort für →Passwort Reset.

Passwort Reset: Das automatisierte Zurücksetzen eines →Passworts wenn der →Benutzer einer →Website auf „Passwort vergessen" geklickt hat. Dabei wird zumeist ein neues Einmal-Passwort an eine andere Mail-Adresse gesendet. Dies ist bei den heutigen Webdiensten eine große Schwachstelle da durch die Übernahme nur 1 Mail-Accounts oft alle weitere Accounts dieses Benutzers

übernommen werden können (weitere E-Mail-Dienste, →Social Networking, Filespeicherdienste wie →iCloud, →Webshops wie Amazon und →Netflix, Bezahldienste wie →PayPal. Dadurch entstehen für die Opfer zum Teil erhebliche Schäden, z.B. Verlust aller E-Mails, direkte finanzielle Schäden durch betrügerische Überweisungen, bis hin zu →Remote →Wipe von Geräten

Passwort Safe: Software auf einem IT-Gerät zur sicheren Speicherung von →Passworten / Credentials (verfügbar für alle →Betriebssysteme, inkl. →Smartphones). Kann zumindest teilweise durch Speicherung der Passworte im →Web-Browser ersetzt werden (falls dort mit Master-Passwort gesichert). Dies ermöglicht die Nutzung von komplexen Passworten die jeweils nur auf 1 →Website genutzt werden und schützt dadurch gegen →Angriffe wie →Passwort Stuffing

Passwort Spraying: →Angriffstechnik gegen →Websites bei der häufig verwendete →Passworte (z.B. 123456 oder 12345678) gegen sehr viele Benutzerkonten durchprobiert werden. Durch das „Probieren" von wenigen Passworten gegen viele Konten wird ein Blockieren der Konten wegen zu vielen Versuchen vermieden und da diese Passworte sehr häufig verwendet werden, können immer einige (zufällige) Benutzerkonten „geknackt" werden. Sehr erfolgreich wenn es nicht um 1 bestimmtes Benutzer-Konto geht. Die dabei verwendeten Passworte stammen aus →Passwort Leaks

Passwort Unblocking Key: (PUK) Schlüssel zum Entsperren eines nach mehrmaliger Falscheingabe eines →Passwortes gesperrten Gerätes. Meist in Verbindung mit einem →Handy

PAT: (Port Address Translation) ähnliche Methode wie →NAT um nichtoffizielle in offizielle →IP-Adressen umzuwandeln. Wie bei NAT werden dabei →Port-Nummern des →TCP-Protokolls verwendet

Patch: →Software-Aktualisierung zur Behebung von →Schwachstellen, zumeist über das →Internet (oft automatisch) verteilt. Eignet sich über eine Analyse von „vorher" und „nachher" auch zur automatisierten Erzeugung von →Exploits. Siehe →Window of Exposure

PatchGuard: Konzept in den x64 editions von →Windows zum Verhindern von →Root kits und anderer →Malware, von einigen Anti-Viren-Herstellern kritisiert

Patch Management: →Prozesse die notwendig sind um sicherzustellen, dass Informationen über vorhandene →Patches bekannt sind und dass bei der Korrektur der →Software keine neuen Probleme entstehen, beinhaltet auch die Entscheidung, ob ein Patch installiert werden soll. Siehe →Change Management

Patch Tuesday: von →Microsoft eingeführter fester Tag, an dem monatlich →Patches zur Verfügung gestellt werden. Der feste Patch Cycle hat zu einem gekoppelten Zyklus von →zero day exploits geführt

Path Traversal: →Angriff auf eine →Website durch Verändern, i.d.R. Verkürzen der →URL die dem Benutzer angezeigt wird, kann zum →Zugriff auf Bereiche führen, die für externe nicht zugänglich sein sollten

Patriot Act: →USA Patriot-Act

Pattern: (engl.Muster) in der IT ein Muster in Computer-→Malware nach dem ein Anti-Viren-Programm checkt oder von Angriffssequenzen auf die ein →IDS oder →IPS achtet. Siehe →Dynamic Code Obfuscation, →Targeted Attacks, →Polymorphismus

Pawned: (oder pwn3) →Leet für den „Verlust" meines →Passworts (üblicherweise) durch eine unsichere →Website. Siehe →Passwort Leak

Payload: →Malicious Code eines →Virus oder →Wurms, der den Schaden anrichtet, bzw. die vom Schreiber gewünschte Aktion ausführt

Paysafecard: elektronisches anonymes Preaid-Zahlungsmittel, gern genutzt im Internet-Untergrund. Durch die Weitergabe eines →PIN-codes kann der Empfänger auf das Geld zugreifen. Siehe →e-Crime, →Bezahldienste

PayPal: sehr erfolgreicher Bezahldienst im →Internet, gegründet ca. 2000, von 2002 – 2015 Teil von →eBay (dabei gewann Elon Musk einen großen Teil seines Startvermögens), seitdem als Aktiengesellschaft selbstständig. Zeichnet sich durch bequeme Nutzung aus, auch für Privatleute die z.B. Geld für Zimmervermietung einnehmen wollen. 100 Währungen werden unterstützt und automatisch konvertiert. Ab 2019 unterstützen sie Online Casinos nicht mehr. Es gibt Hinweise dass PayPal Konten sperrt, wenn sie vom US-Heimschutz-Ministerium Hinweise auf Terrorverdacht bekommen, dagegen gibt es nur schwierige Rechtsmittel

Pay-per-click: (PPC) Bezahlmethode für Werbung im →Internet. Dabei zahlt derWird genutzt bei →Domainnamen-Piraterie und → Traffic Diversion. Wird mittels →Click-fraud ausgenutzt indem automatisiert auf bestimmte Anzeigen „geklickt", z.B. über PCs in →Botnets oder →Webserver unter Kontrolle der Betrüger. →Microsoft schätzt, dass 20% aller Klicks auf Werbung betrügerisch sind

Pay-per-Install: Geschäftsmodell von legitimen und kriminellen Organisationen. Darunter fällt, wenn →Freeware dadurch finanziert wird, indem beim Download und Installieren weitere →Software inkludiert wird (oft z.B. →Google →Chrome) die der Kunde aktiv desektieren muss.

Im kriminellen Bereich wird bei diesem Geschäftsmodell für jede Infektion eines

Rechners gezahlt. Die Preise hängen davon ab, in welchem Land das Opfer sitzt und ob es sich um einen Privat-Rechner oder einen Firmenrechner handelt, letztere bringen mehr Geld ein, da dort die Chance besteht, an brisante Daten zu kommen

Pay-per-view: Bezahlmethode für Werbung im →Internet, bei der bereits bei der Präsentatoin der Werbung im →Browser („Impression“) der Werbende zahlen muss. Häufiger ist →Pay-per-click, bei der die Bezahlung nur dann fällig ist, wenn der Benutzer auf die Werbung klickt und auf die entsprechende →Website weitergeleitet wird

Pay-TV: Fernsehen, das nicht durch Werbung sondern durch Zahlungen der Zuschauer finanziert wird. Erfordert zum Verhindern von kostenlosen Nutzern oft →Verschlüsselung, die jedoch sehr oft nach kurzer Zeit „geknackt“ ist. Pay-TV ist auf der Basis von digitalen Technologien (→DVB) einfacher zu implementieren als analog. Eine spezielle Form ist PPV (**Pay-per-view**), so für jede Übertragung separat gezahlt werden muss. Eine weitere Form seit ca. 2017 ist →Streaming Dienste wie →Netflix, →Amazon Prime, Disney+

PBA: (Pre-Boot Authentication) Technik für die →Festplattenverschlüsselung. Dabei wird, bevor irgendeines der auf der Festplatte installierten →OS geladen wird, zuerst von einer separaten →Partition ein →Programm gestartet, das den Benutzer authentisiert

PBKDF2: (Password-Based Key Derivation Function) Teil der →PKCS-Serie von Cryptographie Standards, wird genutzt um einen →Schlüssel aus Benutzer-→Passworten und →Salt zu generieren, indem →Hash-Funktionen mehrfach (>1000-fach) angewendet werden. Siehe auch →Bcrypt, →Scrypt

PBX: (Private branch exchange) traditionelle Telefonanlage, heute oft ersetzt durch →VoIP-Systeme. Siehe →POT, →PSTN

PC: (Personal Computer) ursprünglich genereller Begriff für einen Rechner, der von einer einzelnen Person genutzt wurde (im Gegensatz zu Mainframes und Minis, die von vielen Personen gleichzeitig genutzt wurden). Heute wird damit meist eine spezielle Rechner-Architektur gemeint, die von →IBM 1980 entwickelt und zum Quasi-Standard wurde („IBM-PC“). Eine sehr wichtige CPU-Architektur ist war dabei →x86

PCAOB: (Public Company Accounting Oversight Board) US-Behörde, deren Buchhaltungsregeln “Audit Standard 2” Teil von →SOX sind

PCI: 1) (Payment Card Industry) PCI-DSS Data Security Standard. Sicherheitsprogramm der PCI-→Kreditkarten-Organisation. Inhaltlich nur ein Grundschutz, jedoch mit jährlichen →Audits für Händler, die viele →Kreditkarten verarbeiten und mit hohen Geldstrafen bei Verletzungen

2) (Peripheral Component Interconnect) Standard Interface für den Anschluss von Zusatzkarten auf dem →Motherboard von →Rechnern, erlaubt wie →Firewire den Zugriff auf den gesammten Speicherinhalt des Geräts

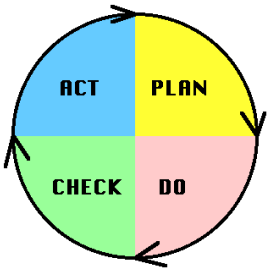
PCMCIA: (***P**ersonal **C**omputer **M**emory **C**ard **I**nternational **A**ssociation)* Standard für externe Einschübe in Laptop-→PCs. Wurde früher oft für Netzwerkanschlüsse genutzt, ist heute z.B. für Kartenleser für →Smartcards in Einsatz. Die Einschübe gibt es in drei Größen, z.T. sind dann Kombinationen mehrer Einschübe möglich. PCMCIA unterstützt →DMA und kann genutzt werden um sensible Inhalte wie →Passworte aus dem →Hauptspeicher auszulesen

PC/SC: (Personal Computer/Smartcard) Spezifikationen für den Anschluss von →Smartcards an →PCs (Hardware-Abstraktion)

PDA: (Personal Digital Assistant) →Rechner in Taschenrechnergröße, der über entsprechende Schnittstellen auch in Datennetze eingebunden werden kann und daher mehr und mehr sicherheitsrelevant wird. Beispiel Palm oder iPAC von Compaq, Weiterentwicklung zum →Smartphone. Standard-Sicherheitsvorkehrung sollte Power-On-Schutz sein, d.h. nach dem Einschalten muss der Anwender erst ein →Passwort oder →PIN eingeben

PDC: (Primary Domain Controller) Server in einer pre-Windows 2000 NT-Umgebung, zum Zwecke der Benutzer-→Authentifizierung. Aus →Verfügbarkeitsgründen durch einen Backup Controller (BDC) unterstützt. Heute mit Zugriff zu →Active Directory implementiert

PDCA-Zyklus: (plan-do-check-act) von Willliam Deming entwickeltes Konzept des →Qualitätsmanagements zur Implementierung einer kontinuierlichen Erhöhung der Qualität (→Deming Cycle). Siehe →KVP, →TQM



PDF: (Portable Document Format) von Adobe entwickeltes transportables Datenformat, heute in →ISO standardisiert. Dokumente werden mit einem geeigneten →Programm in PDF-Format umgewandelt und können dann mit Hilfe eines PDF-Readers dargestellt und gedruckt werden. Vorteil ist, dass das Format der Darstellung auf diese Weise vom Autor fest vorgegeben werden kann und dass der Autor auch diverse Sicherheitseinstellungen festlegen kann, z.B. kein Drucken, kein Sichern, kein Entfernen des Textes durch Kopieren/Einfügen. Diese Funktionalität wird durch ein →Passwort geschützt, kann jedoch durch →Brute Force Angriffe relativ leicht umgangen werden. PDF-Doku-

mente können →Schadsoftware enthalten, u.a. weil in neuen Versionen auch →JavaScript enthalten sein kann, die beim Öffnen des Dokuments automatisch ausgeführt wird. Adobe hat daher in der letzten Reader-Version →Sandboxing eingeführt

PEAP: (Protected Extensible Authentication Protocol) von →Microsoft, RSA Security und Cisco Systems entwickeltes Protokoll für die →Authentifizierung auf der Basis von →Passworten und Server-→Zertifikaten für →SSL/TLS, wird genutzt in Verbindung mit →WPA und WPA2. Gilt als sicherer als →LEAP und hat gute →Windows Unterstützung. Eine Variante verwendet →MS-CHAP

Peering: eine der Grundlagen des Internets, beschreibt die finanziellen Regeln für den Datentransfer im →Internet. →ISPs, d.h. die Firmen die End-user und Firmen mit dem Internet verbinden werden als Tier 3 bezeichnet. Sie kaufen Bandbreite von Tier 2 Anbietern, die gegenseitige Peering-Verträge mit anderen Tier 2 Anbietern haben (um lokalen Traffic kostengünstig transportieren zu können) und von mindestens einem Tier 1 Anbieter Bandbreite kaufen (um die ganze Welt erreichen zu können). Tier 1 Anbieter (es gibt ca. 12) kaufen keine Bandbreite sondern haben Peering Verträge mit anderen Tier 1 Anbietern und verkaufen Bandbreite an Tier 2. Viele der Netzanbindungen finden in sog. →IXP statt

Peer-to-Peer: →P2P

Peertube: →open source Implementierung einer föderierten Video-Hosting Platform (siehe →Fediverse). Instanzen von Peertube können über →ActivityPub oder →WebTorrent angesprochen werden. Dies ist eine Alternative zu den traditonellen zentralen Diensten wie →Youtube, →Vimeo oder →Dailymotion. Durch die Nutzung der →P2P Technologie WebTorrent wird jeder →Browser der ein Video betrachtet auch wieder zu einer Quelle des Videos, das spart Bandbreite auf dem →Server

Penetration: in der IT das Eindringen in einen fremden Rechner durch Ausnutzung von →Schwachstellen oder Konfigurationsfehlern. Siehe →Computer Crime

Penetration Test: (Pentest) Test, bei dem ein →Angriff auf ein Rechnersystem simuliert wird, um mögliche →Schwachstellen/ →Verwundbarkeiten oder Konfigurationsfehler zu finden. Dabei können die gleichen Tools zum Einsatz kommen, wie sie auch von den →Hackern eingesetzt werden. Diese Tests werden durch die Eigentümer oder Betreiber der Systeme in Auftrag gegeben. Um eine klare rechtliche Situation zu schaffen muss derjenige der den Test durchführt sicherstellen, dass er eine →„Permission to Attack“ hat, und dass mögliche Betroffene, z.B. andere Nutzer des gleichen Systems ebenfalls zugestimmt haben oder zumindest informiert sind. Ansonsten könnte es zu einer Gesetzesverletzung auf Grundlage der →Cybercrime Convention kommen („Eindringen in fremde Computer-Systeme“). Bzgl. der Tools, siehe →nmap, →Nessus, →Cain, →Ethereal, →Netstumbler

Pentest: →Penetration Test

PEP: (politically exposed person) Politiker oder Personen aus ihrem Umfeld. Wird im Zusammenhang mit →Geldwäsche und Terrorismusfinanzierung verwendet. Siehe →World-Check

PEPP-PT: (Pan-European Privacy-Preserving Proximity Tracing) →Protokoll-Vorschlag für eine von Frankreich und Deutschland vorgeschlagene →Corona App die auf zentraler Datenspeicherung beruht hätte. Wurde mit Unterstützung von →Google und →Apple durch →DP-3T ersetzt

Perimeter: die Grenzen eines Grundstückes, Gebäudes, aber auch eines Netzwerkes

Perimeter Security: Verteidigung gegen →Angriffe, die darin besteht, dass die Grenzen so sicher wie möglich gemacht werden (Konzept der Burg). Dafür werden →Firewall, →Malware-Schutz, →Content Scanning, →Proxies u.ä. eingesetzt. Heute weitgehend als nicht ausreichend betrachtet, da Angriffe auch von innen erfolgen können, →Schadsoftware durch Laptops eingeschleust wird, die außerhalb im Internet waren und weil Firmennetze selbst mehr und mehr Verbindungen zum Internet haben. Moderneres Konzept: →de-perimeterisation, →Security in Depth, →Jericho Forum

Perfect Forward Secrecy: (PFS) durch die →Snowden-Veröffentlichung der Langzeitspeicherung von verschlüsseltem Datenverkehr durch US-Behörden entstand die Forderung, dass solch historischer Datenverkehr auch dann noch sicher sein soll wenn später bessere Methoden zum Knacken der →Verschlüsselung zur Verfügung stehen oder die Master-Schlüssel bekannt werden. Das Ziel von PFS wird erreicht, indem bei jeder „Sitzung“ (z.B. in einem →Messaging Dialog) mittels entsprechendem →Key Handling der symmetrische →Schlüssel mittels Verfahren wie elliptic curve →Diffie–Hellman so bestimmt und ausgetauscht werden, dass der Datenverkehr auch bei späterem bekannt werden eines der asymetrischen Schlüssels nicht entschlüsselt werden kann. Implementiert wird dieses Prinzip immer öfter, z.B. in →TLS seit TLS 1.2 (wenn aktiviert), im →Signal Encryption Protocol, das auch im →Facebook Messenger, →Google →Android Messaging →App, →Mumble und anderen Diensten genutzt wird. PFS schützt aber nicht bei physischem →Zugriff auf das Endgerät (z.B. →Smartphone) wenn dort die Nachrichten nicht gelöscht wurden

Permissioned data: Begriff den →Data Aggregatoren verwenden um zu erklären, dass

die Benutzer bei der Installation einer App oder bei der Nutzung eines →Cloud Dienstes wie →Facebook der Datensammlung und der Nutzung ihrer persönlichen →Daten wie ihres →Addressbuchs oder ihrer Aufenthaltsort (→Geolocation) zugestimmt haben

Permission Marketing: Versenden von →E-Mail, nachdem der Kunde die Erlaubnis dazu gegeben hat, Ziel ist die Vermeidung von →Spam. Siehe →Opt-In, →Double-Opt-In, →Opt-Out

Permission to Attack: →Penetration Test

Persistence: im Rahmen eines IT-→Angriffs die Fähigkeit des →Angreifers sich im Netz und den Systemen des Opfers so festzusetzen, dass auch Neustarts, Ändern der →Zugriffsberechtigungen und Umkonfigurationen die Angreifer weiter Zugriff auf die Systeme und Zugang zu den Netzen behalten, siehe →MITRE ATT&CK Matrix

Personal Firewall: (PFW) Programm, das auf einem Rechner installiert wird und das durch die Überwachung des Datenverkehrs zum Netz den Rechner schützen soll. Wie eine →Firewall in einem größeren Netzwerk soll diese persönliche Brandschutzmauer einen einzelnen →Computer vor Angriffen von außen schützen. Für alle Rechner, die mit dem →Internet kommunizieren auf jeden Fall notwendig

Personelle Sicherheit: zusammen mit →logischer und →physischer Sicherheit wichtige Bausteine von →IT und →Informationssicherheit. Bezeichnet Kontrollen die verhindern sollen, dass ungeeignete Mitarbeiter in Vertrauenspositionen bekommen, die es ihnen ermöglichen, leicht →Angriffe durchführen. Dazu gehört z.B. Überprüfung von Lebensläufen, Vorstrafenregister, u.ä. Siehe →Personensicherheit

personenbezogene Daten: (personal data) Begriff aus dem →Datenschutzgesetz: alle →Daten, die auf natürliche Personen bezogen sind oder bezogen werden können (verlinkt oder verlinkbar sind), z.B. Name, Anschrift, Alter, Geschlecht. Der Name muss nicht unbedingt enthalten sein, es bit auch „indirekt personenbezogene Daten“ wie →Facebook-ID, Telefonnummer, Autokennzeichen oder →IP-Adresse, die erst über Rückfragen bei anderen Stellen einer Person zugeordnet werden können. Auch diese fallen unter den Schutz des Datenschutzgesetzes. Verletzungen des Datenschutzes können nicht nur durch Firmen passieren. So ist das häufig durchgeführte Exportieren von →Adressbüchern im Rahmen von →Social Networks durch die Nutzer i.d.Regel Datenschutzverletzungen.

Besonders geschützt sind sog. →sensible Daten

Personensicherheit: nicht zu verwechseln mit →personeller Sicherheit. Hierbei geht es um den Schutz von Leib und Leben von Menschen, dies ist nicht Teil von →Informationssicherheit

Persönlichkeitsprofil: Zusammenstellung von Daten, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt. Ein solches Profil ist heute über die bei →Internetnutzung anfallenden Daten technisch leicht zu erstellen, stellt üblicherweise eine Verletzung der →Vertraulichkeit dar. Siehe →Datenschutz, →Consumer Profiling. Siehe →P3P

Pervasive Computing: Schlagwort bei dem es darum geht, dass →Computer immer mehr in Alltagsgegenstände eingebaut werden und diese langfristig über →Bluetooth, →RFID und andere Technologien untereinander und mit dem →Internet vernetzt werden. Dies wirft neue Probleme für die Informationssicherheit auf

PESTEL: (Political, Economic, Social, Technical, Environment and Legislative) beschreibt die externen Faktoren, die ein Unternehmen Einfluss nehmen, auch auf die →IT- und →Informationssicherheit

PET: (Privacy Enhancing Technologies) Sammelbegriff für Techniken zum Schutz personenbezogener →Daten. Ziel ist es, Gefährdungen der →Privatsphäre zu minimieren

Pflichtenheft: (auch Sollkonzept oder fachliche Spezifikation) vertraglich bindende, detaillierte Beschreibung einer zu erfüllenden Leistung, zum Beispiel der Erstellung eines Computerprogramms. Im Gegensatz zum →Lastenheft sind die Inhalte präzise, vollständig und nachvollziehbar sowie mit technischen Festlegungen der Betriebs- und Wartungsumgebung verknüpft. Während das Lastenheft vom ursprünglichen Auftraggeber angefertigt wurde, wird das Pflichtenheft vom Auftragnehmer (Entwicklungsabteilung/-firma) formuliert und vom Auftraggeber bestätigt

PFS: →Perfect Forward Secrecy

PGP: 1) →Pretty Good Privacy

2) (Personal Genom Project) Veröffentlichung der →DNA von 46 Freiwilligen zusammen mit ihren medizinischen Akten zu Forschungszwecken. Mit fallenden Preisen für DNA-Sequenzierung kann dies für viele Menschen möglich werden. Problematisch frü →Privatsphäre. Siehe →23andMe

PGPfone: Älteres Programm (1995) des →PGP-Entwicklers →Phil Zimmermann zum →Verschlüsseln von →VOIP-Verbindungen. Heute ersetzt durch →Zfone

Pharming: hat sich als Oberbegriff für verschiedene Arten von →DNS-Angriffen etabliert, z.B. durch Manipulation der „hosts“ Datei eines Rechners oder durch DNS Cache Poisoning

PHI: (Electronic Protected Health Information) schützenswerte Gesundheitsdaten in jeglicher

Form. Siehe →ePHI, →eHealth, →HIPPA

Phil Zimmermann: Entwickler von →PGP, 1991 als →open source im →Internet veröffentlicht. Weitere Produkte sind →PGPfone, →ZRTP, →DIME, →Zfone, 2012 →Silent Circle

Phishing: Kunstwort aus password fishing. Das Erschleichen von →Passworten, z.B. durch das Versenden von →E-Mails die zu einer Passworteingabe auf einer gefälschten →Website auffordern. Typischerweise mit Irreführung des Benutzers verbunden (→Social Engineering). Heute auch über →Man-in-the-Middle-→Angriffe, →Keylogger oder →Formgrabbing →Trojaner. Mehr oder weniger wirksame Schutzmechanismen sind z.B. →iTAN, →mTAN und →smartcard-basierte →Zertifikate. Angriff auch über →SMS möglich, dann →SmiShing. Herausforderung für den Angreifer ist, den Angriff →skalierbar zu machen. Siehe →Spear Phishing, →Geldwäsche, →„Finanzmanager", →APWG. http://sicherheitskultur.at/spam.htm#bankraub

Phishing Kit: fertige Software für einen →Phishing→Angriff. Siehe →RockPhish

Phone Flood: Form des →Denial of Service →Angriffs bei dem ein Telefon mit einer großen Zahl von automatisierten Anrufen belästigt wird, so dass keine legitimen Anrufe mehr möglich sind. Solche Angriffe sind kommerziell günstig zu haben: 1 Tag 1 Nummer blockieren für 20 $. Wird z.B. genutzt um in Verbindung mit einem anderen →Angriff zu verhindern, dass z.B. eine Beschwerdestelle oder Helpdesk erreichbar sind

Phorm: Unternehmen das Nutzungsdaten im →Internet durch Abfangen der →Daten beim →ISP (derzeit nur in UK) sammelt. Ziel ist Werbung, die auf die Interessen der Nutzer abgestimmt ist. Siehe →Consumer Profiling, →Nutzerprofil.
http://sicherheitskultur.at/notizen_2_08.htm#phorm

PhotoDNA: Technik um Fotos anhand eines robusten Fingerabdrucks zu identifizieren, der die Fotos auch nach Veränderungen, z.B. in der Größe weiter erkennt. Wird eingesetzt um Darstellungen von sexueller Gewalt gegen Kinder beim Austausch im →Internet zu idenfitizieren. Dies setzt jedoch voraus, dass zumindest in der zentralen Plattform des Austauschs das Bild in unverschlüsselter Form vorliegt. Dies ist bei →End-to-end →Verschlüsselung nicht der Fall, warum →LE-Behörden diese verbieten wollen (→Crypto Wars

php: (rekursives Akronym: PHP Hypertext Preprocessor) Skriptsprache mit einer an C bzw. Perl angelehnten Syntax, die hauptsächlich zur Erstellung dynamischer Webseiten verwendet wird. Bei PHP handelt es sich um →Open Source-Software. Die Sprache gilt als Fehleranfällig da sie „schlampiges" Programmieren erlaubt. Fehler bei der Programmierung und fehlendes Entfernen von Beispielscripten sind häufige Sicherheitslücken. 2014 stellt →Facebook eine sicherere Variante namens Hack vor. Siehe →Web Applikationen

Phreaking: kostenlos, oder auf Kosten anderer, telefonieren (oder surfen), heute nicht mehr so relevant. →Caller ID Spoofing

Physische Sicherheit: zusammen mit →logischer und →personeller Sicherheit wichtige Bausteine von →IT und →Informationssicherheit. Bezeichnet die Kontrolle des räumlichen →Zutritts zu kritischen Ressourcen

PIA: (Privacy Impact Assessment Framework) freiwillige Selbstverpflichtung von Firmen über den Schutz von →Privatsphäre beim Einsatz von →RFID-Technologien

Piconet: →Bluetooth-Netz, das aus einem Master und bis zu 7 anderen Geräten besteht. Die Masterrolle wandert zwischen den Geräten

Pidgin: →Instant Messaging System das mit einer sehr großen Zahl von anderen Systemen kommunizieren kann und durch Einbindung von →OTR auch verschlüsselte Kommunikation bietet

Pig: Programmiertool für sehr große Datenmengen (→Big Data), eingesetzt zusammen mit →Hadoop. Implementiert das → MapReduce Konzept

PII: (personal identifiable information) beim →Datenschutz die Datenelemente, die direkt oder indirekt zu einer Person führen, z.B. voller Name, SVN, Wohnadresse, E-mail-Adresse, Führerscheinnummer, →IP-Adresse u.ä. Nicht dazu gehören Geschlecht, Alter, Gehaltsklasse, Schulbildung. Diese Daten können auch dann einer Person zuordenbar sein, wenn Name oder eindeutige Informationen wie Sozialversicherungsnummer nicht dabei sind. Durch die Kombination verschiedener Datenelemente von verschiedenen Quellen lassen sich sehr oft auch →anonyme Informationen nachträglich zuordnen, z.B. in dem die gleichen →Daten auch auf einer →Social Networking Website gefunden werden, bei der der Benutzer unter vollem Namen auftritt (→Deanonymisierung). Siehe →Privatsphäre, →Identity Theft, →Data Breach, →Social Graph

PIN: (Personal Identification Number) dem →Passwort entsprechende Ziffernfolge, in der Regel rein numerisch. Wird u.a. auch für die →Bildschirmsperre bei →Smartphones verwendet, leider i.d.Regel in Form von „Trivialcocdes" wie 0000 und 1234. Dadurch lassen sich in allen Fällen bei denen die Benutzer die Codes selbst wählen können mit 5-7 Versuchen ca 20% aller PINs erraten. Bei → Android werden zumeist →Swipe für die Bildschirmsperre eingesetzt. Siehe →Bankomatkarte

Pineapple: winziger Computer, vergleichbar

mit → Raspberry Pi, aber ausgestattet mit → WLAN und →Bluetooth, der viel für →Pentests eingesetzt wird, z.B. →Man-in-the-Middle →Angriffe

Ping: kleines Hilfsprogramm zur Diagnose von Netzwerkproblemen in →TCP/IP-Netzen. Versendet ein Datenpaket (→ICMP-Paket) an eine →IP-Adresse, der Empfänger schickt eine Antwort. Bei Erhalten der Antwort weiß der Versender, dass das andere Gerät unter dieser Adresse existiert und aktiv ist. Aus der Laufzeit lässt sich auf die →Qualität der Verbindung schließen, z.B. die →Latency. Ping wird auch bei und für →Angriffe eingesetzt („Ping of Death“)

Pinning: →Certificate Pinning

PISCE: (Partnership for ICT Security Incident and Consumer Confidence Information Exchange Exchange) von →ENISA initierte Organisation für den Informationsaustausch zu IT-Sicherheit, gibt Studien in Auftrag. (→ISAC) http://wiki.enisa.europa.eu/

PitBull: Secure Program Launcher. Spezielles Programm, das es ermöglicht, eine gefährdete Anwendung, z.B. ein →Webserver-Programm in einer →Sandbox ablaufen zu lassen. Dies bedeutet, dass auch nach Übernahme der Kontrolle über diese Anwendung ein →Hacker keinen Systemzugriff hätte

Pixelation: (engl. verpixelt) Verfahren um auf Photos im →Internet die →Privatsphäre zu wahren in dem das Gesicht mit sehr groben Pixeln (elementaren Bildelementen) dargestellt wird. Siehe →Google Streetview

PixelFed: föderierter Dienst für Photosharing (analog zu →Instagram oder Flickr) der das Protokoll →ActivityPub unterstützt und dadurch →Daten mit vielen anderen Diensten austauschen kann

PJL: (Printer Job Language) Methode zur Kontrolle und Konfiguration von Druckern ohne physischen → Zugriff auf das Gerät. Nutzung dieser Sprache durch Unbefugte stellt ein Sicherheitsproblem dar. Siehe →Multifunktionsdrucker

PKCS: (Public Key Cryptographic Standard) Sammlung von Standards zu unterschiedlichen Aspekten, z.B. Algorithmen, Formaten von →Smartcards, etc. Durchnummeriert von #1 bis #15. →PBKDF2

PKD: (→Public Key →Directory) spezielle →PKI der →ICAO um die →Authentizität eines →ePass kontrollieren zu können. 2008 noch wenig eingesetzt

PKG: (Private Key Generator) →ID-based Cryptography

PKI: →Public Key Infrastructure

PLA: (People’s Liberation Army) Volksbefreiungsarmee, die Armee der Volksrepublik China. Recht aktiv im Bereich →Cyberspionage, siehe →APT1

Plakat: wird in Zukunft „intelligent“ sein („digital signage“), d.h. mit Kamera versehen, mit deren Hilfe Alter und Geschlecht von den Personen im Umfeld erkannt und die Werbung entsprechend gesteuert werden kann (→targeted advertising). Dies wird manchmal auch als →Face Recognition bezeichnet. Die Technologie wird bereits vereinzelt eingesetzt, kann weiterentwickelt werden so dass einzelne Personen erkannt werden und direkt angesprochen.bzw. über aus seinem Verhalten im →Internet bekannte Vorlieben zugeschnitten werden. Dies erfordert in Europa die Zustimmung des Betroffenen, in den USA wird diskutiert, ob ein Hinweisschild reicht

Plattform: in der →IT eine technische Grundlage, auf der →Programme ausgeführt werden können. Die Plattform liegt zwischen dem Programm und der darunter liegenden Ebene, z.B. einem →Betriebssystem, →Laufzeitumgebung wie →JRE oder →Webbrowser, bzw. →Hardware wie einer →CPU-Architektur

Plausible Deniability: Feature in einigen Datei→verschlüsselungsprogrammen, bei der es darum geht, gegenüber Behörden plausibel erklären zu können, dass man keine verschlüsselten Daten besitze, um so die Erzwingung der Herausgabe von →Schlüsseln, z.B. durch Erzwingungshaft (→RIPA) zu verhindern. Dabei wird z.B. in einem verschlüsselten Datencontainer ein weiterer verschlüsselter Datencontainer versteckt, der ohne Kenntnis des 2. Schlüssels nicht sichtbar ist, d.h. der erste Container erscheint leer. Plausible Deniability ist auch ein Problem bei der →Attribution von →Angriffen im →Internet

PLC: (Programmable logic controller, speicherprogrammierbare Steuerung) elektronische Baugruppe oder Computer, die zur Regelung einer Maschine oder Anlage eingesetzt werden, wichtiger Bestandteil von →SCADA Systemen. Ein PLC empfängt →Daten von →Sensoren (z.B. Druck oder Temperatur), verarbeitet diese und kommuniziert dann mit Steuerungen, z.B. Relays oder Motoren. Bekannt wurden PLCs durch →Stuxnet. PLCs werden programmiert mittels Programmiersprachen wie Ladder Logic. Verwendete Kommunikationsprotokolle sind z.B. Modbus, BACnet oder DF1. Siehe auch →Auto

Pleroma: →Micro blogging und →Social Networking Dienst der die →Protokolle →ActivityPub und →OStatus unterstützt und dadurch →Daten mit vielen anderen Diensten austauschen kann. Siehe →Fediverse

Plug-in: Hardware- oder Software Modul, mit dessen Hilfe die Funktionalität eines Systems erweitert wird. Oft verwendet im Zusammenhang mit Web →Browsern, wo es z.B. dazu dienen kann, zusätzliche Datenformate, wie z.B. →Streaming Media unterstützen. Meist werden solche Plug-ins direkt aus dem Internet

installiert, was bei einem bösartigen Plug-in zu großen Sicherheitsproblemen führen kann

PML: (Physical Markup Language) →ONS

PNG: (Portable Network Graphics) Datenformat mit verlustfreier Bildkompression, häufig genutzt auf →Websites (alternativ zu →JPEG [Qualitätsverlust] oder →GIF, ebenfalls verlustfrei). Wie die anderen Formate können auch PNG-images für →Schadsoftware ausgenutzt werden

PnP: (plug and play) Konzept, nach dem Peripherie-Geräte in Rechnern installiert werden, ohne dass eine manuelle Konfiguration (und idealerweise auch kein Neustart) benötigt wird. Dies erfordert geeignete Hardware- und Betriebssystemunterstützung. Der Begriff wurde populär durch Windows95, andere Systeme hatten eine solche Funktionalität jedoch zum Teil schon vorher. In der Windows-Implementierung gibt es leider eine Reihe von →Schwachstellen, die PnP zu einem →Risiko machen. Siehe →UPnP

P-NP-Problem: ungelöstes Problem der Mathematik und theoretischen →Informatik. Es geht um die sog. Komplexitätsklassen P und NP. Dabei steht P für alle Probleme, die von einer →Turing Maschine in Polynomalzeit lösbar sind. D.h. die Maschine braucht eine vorhersagbare maximale Zahl von Rechenschritten, Beispiel Sortieren). Bei NP Problemen ist eine maximale Zahl von Rechenschritten nicht bekannt. Leider fallen eine ganze Reihe von praktischen Problemen in die NP-Klasse. D.h. es ist unklar, ob sie je mit einer Turing Maschine in endlicher Zeit bearbeitet werden können

PNR: (Passenger Name Record) →Daten, die alle Fluggesellschaften speichern und seit 2004 im Fall von USA-Flügen auch an die US-Regierungsbehörden versenden, die diese 15 Jahre speichern. In der EU werden diese Daten vor dem Flug an die jeweilige Fluggastdatenzentralstelle gemeldet um so Personen zu finden, die im Verdacht stehen, an terroristischen Straftaten oder schwerer Kriminalität beteiligt zu sein. Es besteht jedoch Interesse der →LE-Behörden, dies auf andere Straftaten zu erweitern.

Enthält neben Name, Flugnummer, Datum auch Informationen wie z.B. spezielle Essenswünsche

PNRP: (Peer Name Resolution Protocol) neues Protokoll von →Microsoft (Teil von Vista), es ermöglicht dynamische →DNS Namensveröffentlichung und -auflösung und ersetzt das DNS Konzept, nutzbar unter →IPv6

Pocket PC: →PDA, Begriff meist für solche mit Windows CE Betriebssystem

Podcasting: Kunstwort aus →iPod und Broadcasting. Musik, Sprache oder Videos werden im →Internet zum Download angeboten. Die Wiedergabe findet zumeist zeitversetzt in Multimediaprogrammen oder tragbaren Geräten wie →MP3-Playern statt. Podcasts können auch ohne Clilent über einen Link auf einer →Website aufgerufen werden. In Verbindung mit →RSS und einem →Podcatcher ist eine Nutzung als Abonnement-Service möglich. Podcasting durch die Mitarbeiter kann für Unternehmen einen Bandbreitenverlust darstellen und über Sicherheitslücken in der verwendeten Software zu zusätzlichen Risiken führen

Podcatcher: →Software zum automatischen Download von →Podcasts

POE: (power over ethernet) Endgeräte, die ihre Energie über das →Ethernet-Kabel beziehen. Sicherheitsrelevant, wenn →Verfügbarkeit im →Katastrophenfall benötigt wird

Point-of-Sales: (→POS)

Polymorphismus: (Vielgestaltigkeit) Methode von →Schadsoftware, →Spam u.ä. durch automatisierte Veränderung des →Programmcodes (z.B. zufälliges Einfügen von Instruktionen die den Ablauf nicht verändern) oder Mailinhalts der Erkennung durch →Pattern-Matching zu entgehen. Siehe →Dynamic Code Obfuscation

Polymorphic Virus: →Virus (oder andere →Malware, z.B. →Trojaner), das seinen →Befehlscode so verändert, dass ein →Malware-Schutz, der nach festem Muster vorgeht, die Schadsoftware nicht erkennen kann

Poodle: (Padding Oracle On Downgraded Legacy Encryption) 2014 entdeckter Fehler im Design von →SSL 3.0. Daher sollte (z.B. für →HTTPS-traffic) nur noch →TLS in der letzten Version eingesetzt werden

POP: (Post Office Protocol) eigentl: POP3. Verfahren mit dessen Hilfe ein Anwender auf seine →Mailbox zugreifen kann, um →E-Mails abzurufen. Dabei findet eine →Authentifizierung durch →Passwort statt, dieses wird jedoch meist im E-Mail Client fest eingespeichert. Ein anderes Verfahren für diesen Zweck ist →IMAP. Beide werden seit den Veröffentlichungen von →Edward Snowden fast immer verschlüsselt implementiert

POP3: →POP

Pop-up: Technik, mit deren Hilfe →Adware durch Öffnen eines zusätzlichen Bildschirmfensters Werbung auf einem Rechner präsentiert. Pop-under ist eine Spezialform, bei der das neue Fenster unter den anderen Fenstern vorborgen ist und nur nach deren Schließung gesehen wird. Siehe →Adware, →PUP

Port:
1) der Eingang in ein Gerät, z.B. →Switch im →LAN
2) Komponente des →TCP Protokolls, mit dessen Hilfe einzelne Anwendungen auf einem Zielrechner adressiert werden können, siehe

→IP-Protokoll

Port Knocking: (engl. anklopfen am →Port) Technik von →Hackern um zu verbergen, dass ein eingeschleustes →Programm (z.B. →Spyware) auf einem bestimmten →Port „hört". Wenn ein externer →Port Scan diesen Port testet, so antwortet das Programm nicht, sondern wartet, ob nach einem festgelegten Zeitpunkt eine weitere Anfrage bei einem bestimmten anderen Port kommt. Erst nach Abwarten einer bestimmten Sequenz von Portnummern und zeitlichen Abständen reagiert das Programm auf die Anfrage von außen

Port Scans: systematisches Absuchen des →Internets (oder eines anderen Netzes) mit dem Ziel, verwundbare Rechner mit →Schwachstellen zu finden

Port Security: Verfahren, das sicherstellen soll, dass nur bestimmte →MAC-Adressen sich zum →Port eines →Switches im →LAN verbinden können. Zu den Implementierungsoptionen siehe →NAC

Portal: →Web-Portal

POS: (→point-of-sales) Geräte an einer Ladenkasse, die für die Bezahlung, inkl. Verarbeitung von →Kredit- und →Bankomatkarten geeignet sind. Bei allen Geräten mit →PIN-Eingabe ist →tamper-proof wichtig, aber schwer zu realisieren. →Infektionen der POS-Hardware haben 2013 und 2014 zum Verlust der Zahlungsdaten von Millionen US-Bürgern geführt. In Europa wird (i.d.Regel) das sichere weil chip-basierte →EMV-Protokoll eingesetzt (→Secure Element). →POS-Zahlungen sollen in Zukunft kontaktlos über →MCP und →NFC ablaufen. 2014 wird immer öfters mPOS genutzt (mobile POS). Das sind →smartphone-basierte Implementierungen die es einem Händler erlauben, →Kreditkarten mit einem Smartphone zu akzeptieren. 2014 wurden zahlreiche →Schwachstellen in diesem Implementierungen gefunden

POST: eine der 2 Formen der →Datenübertragung mittels →http beim Aufruf einer →Webseite mittels →URL. (Solche Datenübertrangen sind notwendig, wenn der Nutzer z.B. ein Formular ausfüllt). Bei POST werden die Daten nicht wie beim GET-request in der URL mitgeliefert sondern im Rahmen der http-Syntax separat übertragen, ist auch geeignet für große Datenmengen, z.B. Bilder. Wird meistens durch →Web-Browser implementiert, geht aber auch mittels →cURL. Wird bei modernen Website (→single-page application) durch Datenübertragungen „im Hintergrund" mittels →Javascript ersetzt, siehe →REST und →SOAP

Postel Law: „be conservative in what you do, be liberal in what you accept from others", d.h. strenge Einhaltung der (Standard-)Vorgaben, aber liberales Akzeptieren von Abweichungen. Dies kann zu →Schwachstellen führen, z.B. wenn ein →Downgrading von →SSL3 auf SSL2 erlaubt wird

Postkästen: in Firmen oft ein Sicherheitsrisiko, z.B. wenn vertrauliche Informationen unkontrolliert zugänglich sind. Siehe →Fax, →Druckausgaben

Post Privcay: gefährliche Strömung im Netz die sagt dass in Zukunft keine →Privatsphäre benötigt würde. "Wir sind hoffnungslose Idealisten und wünschen uns eine diskriminierungsfreie Welt, in der es nicht notwendig ist, sich ins Privatleben zurückzuziehen." http://sicherheitskultur.at/privacy.htm#post

POT: (Plain old Telephone) Technikerbezeichnung mit leicht ironischem Beiklang für die herkömmliche Telephonverbindung, die trotz moderner Kommunikationstechnologien ihre Bedeutung für Datenübertragungen bis heute nicht ganz verloren hat, aber von →VoIP bedroht ist. Auch gegen traditionelle Telefondienste werden 2013 →DoS-Services angeboten. Siehe →PSTN

Power Analysis: →Side Channel Angriff gegen →Verschlüsselungsgeräte, z.B. → Smartcards, der intern gespeicherte Schlüssel ausspäht, indem der leicht unterschiedliche Stromverbrauch während der Ausführung verschiedener →Befehle des →Programmcodes

PPC: →Pay-per-click

PPP: (Point-to-Point Protocol) Softwaretechnologie, die es ermöglicht, über einfache Telefonleitung das →TCP/IP Protokoll zu nutzen. Wird für alle →modem-basierenden Internetanbindungen genutzt

PPTP: (Point-to-Point Tunneling Protocol) Protokoll, das für →VPN-Verbindungen eingesetzt wird. Ältere Technologie, vermutlich 2014 durch die →NSA emtschlüsselbar, ist aber in China nur schwer zu blockieren und wird daher von VPN-Services angeboten um die Zensurmaßnahmen zu umgehen

PPV: (Pay-per-view) →Pay-TV

Prävention: eine der 3 Aufgaben des Sicherheitsmanagements: der Versuch, Vorfälle und damit Schäden zu verhindern. Die anderen Aufgaben sind →Entdeckung und →Reaktion. Siehe →IPS

Präventionsstaat: nächste Stufe nach →Polizeistaat. Die durch →Überwachung der Bürger gewonnenen →Informationen sollen zur Verhinderung von Straftaten oder Störungen der öffentlichen Ordnung eingesetzt werden. Beispiele dazu: → EDVIRSP, → MALINTENT

Pre-Boot Authentication: →PBA

Precrime Detection: siehe →MALINTENT, →Minority Report

Premium SMS: eingehende oder ausgehende →SMS die mit erhöhten Gebühren verbunden sind und zur Bezahlung von Klingeltönen für →Handys oder ähnliches verwendet werden können. Sie werden auch für kriminelle Zwecke wie →Ransomware genutzt werden.

Dies wird auch als →Toll Fraud bezeichnet. Schutz dagegen entsteht erstmal dadurch, dass der Benutzer eine weitere Interaktion mit dem Dienst durchführen muss um den Vertragsabschluss zu bestätigen (double →opt-in). Dies lässt sich jedoch durch eine entsprechende App leicht aushebeln. Mit Hilfe dieses Betrugs können Betrüger Millionen pro Monat einnehmen. Dies geht jedoch nur in Ländern in denen der Einrichter der Premium Nummer das Geld sofort ausbezahlt bekommt. In Westeuropa werden die Gelder mit 1-2 Monaten Verspätung gezahlt, d.h. die Benutzer haben Zeit, sich nach dem Erhalt der Rechnung noch zu beschweren

Presence Server: bei →Unified Messaging und →VoIP die Instanz, die für jeden Teilnehmer anzeigt, ob, wie und wo er erreichbar ist, in Zukunft auch mit →Geolocation-Funktionalität, kann die Kommunikation vereinfachen, hat aber →Privacy-Aspekte

Pre-paid Karten: können oft wie Kreditkarten verwendet werden, z.B. im →Internet. Zum Teil sind sie aber auch für spezielle Zwecke vorbehalten, oft sind sie auch rein virtuell und bestehen dann nur aus einem Zahlen- und Buchstaben Code (→e-Geld). Da der Geldwert bereits bezahlt ist besteht für den Händler kein Risiko mehr. Da diese „Karten“ anonym sind werden sie auch oft für die Bezahlung illegaler Aktionen oder bei kleineren Erpressungen verwendet, z.B. →RansomWare

Pre-shared key: (→PSK)

Pretty Good Privacy: (PGP) populäres unentgeltliches Programm (für Privatnutzung) zur Verschlüsselung von Daten mit Hilfe eines →Public Key Verfahrens. Die Sicherstellung der →Identität der Besitzer der Public Keys wird durch ein sog. →Web-of-Trust erreicht. Dabei bescheinigen sich Personen gegenseitig ihre Identität. GnuPG ist eine alternative Verschlüsselungssoftware in der public Domain die mit PGP kompatibel ist (→RFC 2440 (OpenPGP)). Ihre Entwicklung wurde durch das bundesdeutsche →BSI unterstützt. http://www.gnupg.org/ Siehe auch →Mujahe deen Secrets

Previous Versions: Funktionalität in →Vista analog zu →Volume Shadow Copy

Primary Effect: psychologischer Effekt. Wenn Menschen zeitlich nacheinander Informationen über eine Situation bekommen, so wird die erste Information am stärksten bewertet. Siehe →Automation Bias, →vigilance decrement

PRIME: (Privacy and Identity Management in Europe) von der EU-Kommission gefördertes Projekt, das Vorschläge für →Identitätsmanagement im →Internet mit möglichst geringen Eingriffen in die →Privatsphäre machen soll (minimale Offenlegung persönlicher Daten). Siehe →Liberty Alliance, →P3P

PRINCE2: (Projects in Controlled Environments) Methodologie für systematisches Projektmanagement, auch für →Software-Entwicklung zur Erzielung einer höheren →Qualität

PRISM: Programm der →NSA das ihren Mitarbeitern →Zugriff auf einige →Daten von Webdiensten wie →Google, →Facebook u.a. gibt, die nach Prüfung durch den geheimen →FISA-Gerichtshof auf eine Filterliste von zu selektierenden Daten gesetzt wurden. Die Existenz dieses Programmes wurde veröffentlicht durch →Edward Snowden. Nach Veröffentlichung anderer Aktivitäten wie →MUSCULAR, bei dem der Datenverkehr zwischen den →Rechenzentren von →Cloud-Diensten direkt abgehört wurde gibt es die Theorie, dass PRISM nur eine Aktivität sein könnte um die wirkliche Herkunft der Daten zu verschleiern. Siehe auch →Tempora

Privacy: →Privatsphäre, →Datenschutz

Privacy by Default: in Verbindung mit Privacy by Design wichtige Aspekte die in Art.23 der 2012 vorgeschlagenen neue EU Data Protection →Regulation gefordert werden. Darunter wird verstanden, dass die eine Minimierung der Nutzung von personenbezogenen →Daten von vorn herein in der Technologie und den organisatorischen Prozessen beinhaltet sein muss. „by Default“ bedeutet, dass zu Beginn der Nutzung die Einstellungen auf „restriktiv“ gesetzt werden müssen und der Benutzer dann selbst großzügigeres „Teilen“ seiner Daten einstellen kann

Privacy Enhancing Technologies: →PET

Privacy Shield: Nachfolge-Vertrag zu →Safe Harbor (das 2015 gekippt wurde, „Schrems-I Urteil“) und dann durch Privacy Shield ersetzt wurde und dann 2020 im Schrems-II Urteil ebenfalls für untauglich als Rechtsgrundlage für Datentransfer in die USA erklärt wurde. Das Problem waren in beiden Fällen die uneingeschränkten →Zugriffe der Geheimdienste zu den persönlichen →Daten der EU-Bürger. Details siehe Safe Harbor

Privacy Statement: →Datenschutzerklärung

Private Address Space: Reservierte Adressbereiche bei →IP-Adressen. Für IPv4 sind in RFC 1918 definiert:

10.0.0 – 10.255.255.255 (10/8 prefix)
172.16.0.0 – 172.31.255.255 (172.16/12prefix)
192.168.0.0. – 192.168.255.255 (192.168/16 prefix)

Für →IPv6 definiert RFC 4193 den Block fd00::/8 für 48-bit große private Blöcke. Im Gegensatz zu IPv4 enthält IPv6 eine 40-bit →Zufallszahl im Kollisionen zu vermeiden, da diese privaten IP-Adressen global verwendet werden können

Private Browsing: (auch InPrivate Browsing) ist ein Modus bei modernen →Web-Browsern der auf dem lokalen →Rechner des →Be-

nutzers viele Spuren wie →Cookies, History, →Cache Einträge löscht. Dieser Modus bietet KEINE →Anonymität im →Internet, wie Laien manchmal vermuten. D.h. →Tracking der Benutzer findet weiterhin statt

Private Cloud: Implementierung von →Cloud Technologien im Unternehmensnetz. Unterscheidet sich von →Server-→Virtualisierung dadurch, dass Technologien wie Self-Deployment eingesetzt werden, wie sie z.B. bei Amazons →EC2 eingesetzt werden. Dies erlaubt ein schnelleres zur Verfügung stellen von Rechenleistung und Services. →OpenStack will solche Deployment- und Administrations-Lösungen als →Open Source zur Verfügung stellen

Privater Schlüssel: →Verschlüsselung

Privatkopie: Kopie eines →urheberrechtlich geschützten Werkes für nichtgewerbliche und nichtöffentliche Nutzung. Siehe →DRM, →Streamripper, →Raubkopie, →Webradio-Recorder

Privatsphäre: (engl.privacy) komplexes Konzept mit vielen Aspekten. Im angelsächsischen Recht seit 1890 definiert als ‚right to be let alone'. Seit ca. 1980 werden mehrere Dimensionen beschrieben: psychologische P. (Intimsphäre), physische P. (z.B. die Wohnung), interaktionelle P. (Kontrolle über Interaktionen und Kommunikation) und informationelle P. (→Vertraulichkeit von Informationen über eine Person). Mehrere der Dimensionen der P. sind von vielerlei Entwicklungen, u.a. neuen Technologien. Siehe auch →PII, http://sicherheitskultur.at/privacy.htm

Privileged Account: →Accounts, die sehr mächtig sind, zumeist nur 1x existieren, z.B. →root und oft von mehreren →Benutzern geteilt oder von →Anwendungen, z.B. technische →Accounts für →Datenbankzugriffe. Dies erzeugt Probleme mit der →Accountability und sollte auf jeden Fall vermieden werden. Siehe →PUPM (privileged account and password management)

Privilege Escalation: Sehr oft eines →Angriffs im →Internet (speziell bei →targeted attacks). Der Angreifer beginnt damit, dass er auf einem →Rechner, z.B. mittels →Spear phishing die Kontrolle bekommt. Dabei muss er, falls der Benutzer nicht mit erhöhten Rechten ausgestattet ist, diese erlangen, z.B. durch Ausnützen einer entsprechenden →Verwundbarkeit im →Betriebssystem oder einer andere Software, siehe →MITRE ATT&CK Matrix

PRNG: →Pseudo Random Number Generator

Problem Management: →Prozess in →ITIL, durch den die nachteiligen Auswirkungen eines →Incidents minimiert werden. Es analysiert die Störungen, entwickelt →Work-Arounds und leitet im Rahmen des →Change Managements über ein →RfC die Störungsbehebung ein

Process: (engl. →Prozess)

Process injection: →Angriffstechnik, bei der man →Programmcode im Adressraum eines anderen Prozesses zur Ausführung bringt, in dem man diesen Prozess zwingt, eine programmfremde Dynamic Link Library (DLL) zu laden, daher auch DLL-Injection

Processor: Bezeichnung für den Teil eines →Rechners, in dem die primäre Abarbeitung der →Programme abläuft, heute zumeist implementiert in Form eines einzigen →Chips

Profil: Repräsentanz eines →Benutzer auf einer →Social Networking →Website. Profile werden über →friend-requests miteinander verbunden und haben dann erweiterte →Zugriffsrecht auf vertrauliche Informationen, bzw. werden automatisiert über Änderungen in anderen Profilen informiert. Siehe auch →Benutzerprofil, →Bewegungsprofil, →Persönlichkeitsprofil

Profiling: →Consumer Profiling

Programm: Folge von →Anweisungen (→instructions), die in einem Rechner ausgeführt werden, um eine bestimmte Aufgabe zu erledigen. Während der Ausführung nimmt es meist die Form eines →Prozesses an. Siehe →Algorithmus

Programmabsturz: durch →Programmierfehler hervorgerufenes Ende der Ausführung eines →Programmes (besser: eines →Prozesses). Siehe →Absturz, →Abort

Programmbefehle, Programmcode: Sequenz von logischen →Befehlen (instructions) an die →CPU des Rechners. Eine logische Gruppierung solcher Befehle ist meist ein →Programm. In Programmen kann es durch →Programmierfehler zu einem →Absturz kommen, bzw. zu →Verwundbarkeiten, die →Schwachstellen darstellen können

Programmieren: Nutzung einer →Programmiersprache für die Erstellung eines →Programmes, siehe →Programmierfehler

Programmierfehler: häufiger Anlass von →Programmabstürzen und →Verwundbarkeiten von IT-Systemen. Siehe →Buffer Overflow, →Race condition

Programmiersprache: künstliche Sprache für die Programmierung von →Rechnern. Heute zumeist nicht mehr auf der Ebene der →Programmbefehle des Rechners

Progressive Web App: (PWA) spezielle Form einer →Website auf der Basis von →HTML, →CSS und →JavaScript, mit deren Hilfe auch lokale →Dateien bearbeitet werden können ohne dass eine →Internetverbindung besteht. Solche Implementierungen können →Smartphone →Apps ersetzten. 2019 will →Microsoft das Mailprogramm Outlook auch in dieser Form anbieten.

PRO-IP: US-Gesetz (Prioritizing Resources and Organization for Intellectual Property Act of 2008) zum Vorgehen gegen →Raubkopien.

Sollte 2012 durch →SOPA verschärft werden. Siehe auch →ACTA, →DMCA

Promiscuous Mode: Einstelllung einer Netzwerkkarte, so dass alle Daten die in einem Kabel übertragen werden, von dieser empfangen werden können, nicht nur die für diesen Rechner bestimmten Daten. Wird in →Packet Sniffern verwendet

Proof-of-Work: Sicherheitsmaßnahme mit der →DoS, →Spam und anderer Missbrauch verhindert werden soll. Die „Arbeit" (Rechenoperationen) wird in der Regel durch einen →Computer geleistet (im Gegensatz zum →CAPTCHA) und muss für den Ausführenden aufwendig sein, für den Empfänger aber leicht zu überprüfen. Ein Bespiel dieses Konzepts ist Client Puzzle Protocol (CPP). Siehe auch →Blockchain, →Bitcoin

Protect America Act: →PAA

Protected Storage: (Pstore) Technologie in →Windows zum Speichern von Benutzername und →Passwort für automatisiertes Login zu →Websites. Gilt als unsicher, wird von vielen →Keyloggern ausgelesen. Daher sollten Anwendungen das sicherere →DPAPI (Data Protection Application Programming Interface) nutzen (Internet Explorer ab V.7)

Protocol Analyzer: (→Sniffer) Hardware- oder Software Werkzeug zur Aufzeichnung und Auswertung von →Datenverkehr auf Netzen. Siehe →Ethereal, →Switch

Protokollierung: in der IT: chronologische Aufzeichnung von Ereignissen in →Logs

Provider: →ISP

Provisioning: in der IT:

1) Server Provisioning: das Einrichten eines Servers durch Installation und Konfiguration von Software

2) User Provisioning: das Einrichten, Verändern oder Löschen eines Benutzer-→Accounts, einschließlich sinnvoller →Auditierungsprozesse. Dies ist, für die IT-Systeme im Finanzbereich, in wichtiger Teil von →SOX. Siehe →Identity Management

Proxy: (engl. (Rechts)vertreter) jemand der im Namen oder Auftrag eines anderen aktiv ist

Proxy Server: Rechner oder Software zwischen einem →Client Rechner und einem Server, z.B. →Webbrowser und →Webserver. Dabei kann entweder eine →Caching-Funktion zur Beschleunigung des Verkehrs oder Entlastung des Servers oder eine Filterfunktion (→Content Filtering) genutzt werden oder auch eine →Kontrolle der Benutzerzugriffe (→UAM) oder auch eine →Anonymisierung der Zugriffe stattfinden. Proxy Server sind applikationsspezifisch, d.h. sie behandeln jeweils nur einen Dienst (nur ein oder mehrere →Protokolle), z.B. entweder Mail, Webseiten oder DNS Verkehr, etc. Anders ist das beim →Socks-Proxy.

Reverse Proxys sitzen zwischen einem Rechner und dem Internet und leiten den Internetanfragen nach außen weiter und verteilen die „Antworten" dann intern. Sie können mit Hilfe des →PAC (proxy auto-configuration) automatisch im →Webbrowser eingestellt werden. PAC wird auch von Schadsoftware genutzt um den Datenverkehr des Opfers umzuleiten und so →Man-in-the-Middle →Angriffe durchzuführen. Siehe →Application level gateway.

Prozess: in der IT

1) →Computer→Programm während der Ausführung, einschließlich der →Daten im →Hauptspeicher und der ausführbaren Version des →Programmcodes

2) schematische Darstellung von Abläufen. Wichtig in der →Informationssicherheit zur Sicherstellung von korrekten und sicheren Arbeitsabläufen. Beispiel sind die →ITIL-Prozesse. Gartner definiert die 4 wichtigsten Sicherheitsprozess als: Network access control (→NAC), Identity and Access Management (→IAM), →vulnerability management und → intrusion prevention. Zusätzlich fordern sie einen →Datensicherheits- Prozess. Wichtig ist für sie nicht nur die Existenz dieser Prozesse sondern deren Integration. Siehe →Geschäftsprozess, →Kontinuierlicher Verbesserungsprozess

Prozessor: Einheit in einem elektronischen Gerät das auf Grund eines →Programmes digitale Operationen ausführen kann. Bei einem →Computer zumeist in Form einer →CPU, bei anderen Geräten oft in anderer Form, z.B. →DSP oder →GPU einer →Graphikkarte

Prüfsumme: schwache Methode zur Entdeckung von Fehlern in →Datenübertragungen oder Dateneingaben, z.B. →CRC oder in den →Kreditkartennummern

PSD2: (Payment Service Directive 2) Zahlungsdiensterichtlinie, gilt ab 2019 und hat im Wesentlichen 2 neue Elemente: die sog. →SCA (strong customer authentication) besagt, dass alle kritischen Vorgänge beim →e-Banking (Login, Überweisungen) über 2 Faktor →Authentifizierung (→2FA) abgesichert werden müssen. Dafür haben eine Reihe von Banken spezielle →Smartphone →Apps im Einsatz, andererseits ist aber auch →mTAN ausreichend, nicht jedoch →iTAN. Das ist eigentliche eine gute Idee, die mehr Sicherheit verspricht. Nach meiner Einschätzung hat dies jedoch zu einer Professionalisierung der →Angriffe geführt, denn einfache →Phishing-Angriffe oder →Credential Stuffing führen jetzt nicht mehr zum Erfolg. Die →Websites hinter den Phishing-Angriffen müssen jetzt automatisiert sein und sofort bei der Zielbank die Anforderung des 2. Faktors triggern, damit der Kunde den auch noch preisgibt. Dies wird

durch entsprechende Automatisierung erreicht.

Das 2. Element ist *Open Banking*. Dies ist eine Trennung zwischen sog. ASPSPs (Account Servicing Payment Service Providern - die traditionellen Banken) die Konten ihrer Kunden führen und neuen Diensten Account Information Service Provider (AISPs), die Information aus den Konten mehrerer Banken in 1 Interface anzeigen und Payment Initiation Services Provider (PISPs) – Zahlungsauslösedienste, die in Shopping Websites eingebunden werden und eine direkte Zahlung vom Konto des Kunden zum Händler auslösen. Als problematisch kann sich herausstellen, dass damit jedes Unternehmen mit entsprechenden Lizenzen mit Zustimmung des Kunden auf die Bankdaten des Kunden zugreifen darf. Dies könnte die Datensammlungen von Konzernen wie Google, Facebook, etc. deutlich erhöhen. Siehe https://sicherheitskultur.at/Internet_politik.htm#psd2

Pseudonymisierung: Ersetzen der →Identifizierungsmerkmale in personenbezogenen → Daten durch einen anderen eindeutigen Code, z.B. damit Finanz- oder Gesundheitsdaten für Forschungs- oder Testzwecke verwenden zu können ohne den →Datenschutz zu verletzen. Der Vorgang der →Anonymisierung genannt wird ist häufig in Wirklichkeit eine Pseudonymisierung. Anonymisierungen und Pseudonymisierungen lassen sich leider zumeist rückgängig machen, siehe →De-Anonymisierung

Pseudonymität: im Gegensatz zur →Anonymität, bei der gar nichts über eine handelnde Person bekannt ist, wird hierbei ein (evtl. permanentes) Pseudonym („Nickname“) verwendet, das eine Zuordnung zu früheren Handlungen dieser Person ermöglicht. Pseudonymität wurde 2011 zu einem Thema weil →Social Networks wie →Facebook Pseudonyme nicht nur in den Benutzungsbedingungen verbieten, sondern solche Accounts auch recht willkürlich löschen. Das Verbot kann zu erheblichen Gefahren in totalitären Gesellschaften führen. Mehr unter http://sicherheitskultur.at/anonymity.htm

Pseudo Random Number Generator: (PRNG) wichtiger →Algorithmus bei Simulationen und auch in Sicherheits→programmen. Mit gleichem Startwert („→seed“) liefern sie typischerweise eine vorgegegene Zahlenfolge (für Simulationen zumeist als →Gleitkommazahlen zwischen 0 und 1). Ihre Qualität wird durch ihre Periodizität bestimmt und ob durch →Abhören der Folge auf zukünftige Zahlen geschlossen werden kann. Zu Angriffen siehe →Random

PSK: (pre-shared key) bei symmetrischen →Verschlüsselung das manuelle Eintragen der Schlüssel in beiden Endpunkten der Kommunikation, alternativ dazu z.B. →Diffie Hellman

Pstore: (Windows →Protected Storage)

PSTN: (Public Switched Telephone Network) traditionelles Telefonnetz. Siehe →POT, →PBX, →SS7, →SCTP

Psychologie: traditinell bei der Informationssicherheit viel zu sehr ignoriert. Siehe →Benutzerpsychologie, →Risikopsychologie

Public Domain: →Programme (oder andere geistige Werke), die frei verwendet, kopiert und weitergegeben werden dürfen, weil der Autor sich damit einverstanden erklärt hat. Oft sind Bedingungen daran geknüpft, z. B. →GPL, →Urheberrecht, →GNU project

Public Key Verfahren: Verfahren, bei dem ein Schlüsselpaar erzeugt wird. Dabei wird der Private Key geheimgehalten (z.B. Speichern auf →Smartcard), der Public Key (meist in Form eines →Zertifikates) öffentlich zur Verfügung gestellt.

Das Prinzip des Public Key Verfahrens besteht darin, dass beim Verschlüsseln die Daten, mit dem Public Key des Empfängers, verschlüsselt werden. Der Empfänger kann die Daten dann mit seinem eigenen Private Key entschlüsseln (die technische Implementierung ist i.d.R. etwas komplizierter).

Für die →digitale Signatur wird ein →Hash (Prüfsumme) über die Daten erzeugt und mit dem Private Key des Unterzeichners verschlüsselt. Jeder Empfänger kann mit Hilfe des Public Keys des Unterzeichners die →Integrität verifizieren

Public Key Infrastructure: (PKI) beschreibt die Infrastruktur, die für die sichere Erzeugung und das Management von digitalen →Zertifikaten für →Public Key basierende Verfahren nötig ist.

Eine allgemeine PKI besteht aus:

1. →Certificate Authority (CA), die die öffentlichen →Schlüssel der Kunden oder Teilnehmer signiert. Die Regeln für den Betrieb einer Certificate Authority werden in einem →Certification Practice Statement (CPS) im Detail beschrieben

2. →Registration Authority (RA), die Anträge für die Austeilung der Digitalbescheinigungen validiert, d.h. die Identität der Person oder Behörde überprüft. Die Ausrichtungsberechtigung autorisiert die Signierung der öffentlichen Schlüssel der Kunden

3. →Verzeichnisdienst, der →Zertifikate im →X.509 Format öffentlich zur Verfügung stellt. Dies kann in der Form eines →LDAP- oder →X.500 Directory geschehen. Stornierungen von Zertifikaten werden als →CRL (certificate revocation list) veröffentlicht, oder über einen →OCSP-Server

Public Key Server: Server, auf dem ausgestellte Zertifikate durch die →Certificate Authority der Allgemeinheit zugänglich ge-

macht werden, Teil einer →PKI

Publish-Subscribe: Implementierung von →Messaging bei der der Sender nicht auf eine Antwort des oder der Empfänger wartet, sondern die Daten unter einem bestimmten Identifier zur Verfügung stellt. Der Empfänger wird automatisch über die Verfügbarkeit informiert und kann die Nachricht(en) abrufen. Bespiele sind →MQ-Series von IBM, Tibco oder →MQTT

PUK: →Passwort Unblocking Key

Pump-and-dump: mittlerweile häufigste Form der →Spam-E-mails. →Aktienbetrug durch massenweises Bewerben von „penny stocks", d.h. von Aktien die im Cent-Bereich gehandelt werden. Der Betrüger kauft eine große Zahl der billigen Aktion, die er nach Anstieg des Kurses verkauft, während die anderen, die auch verdienen wollen, noch am Kaufen sind

PUP: (Potentially Unwanted Program) Umschreibung für unerwünschte Software, wie →Spyware oder →Adware. Der Begriff rührt daher, dass →Anti-Virus-Software Firmen die Media-Firmen die →Pop-Ups installieren, nicht mit Firmen in einen Topf werfen wollen, die →Keylogger u.ä. installieren und daher die meiste AV-Software Spyware ignoriert. Andererseits sind für die meisten Benutzer alle Programme unerwünschte, die sie nicht ausdrücklich installiert haben und/oder die sie bei der Arbeit behindern. PUP umfasst alle diese Programme

PUPM: (→privileged account and password management)

PUS: (Potentially Unwanted Software) auch PUSSware (Potentially Unwanted Software Services), →PUP

PXE: (Preboot Execution Environment) Feature von Intel-Chips das mittels →DHCP und →TFTP ein →Boot über ein Netz erlaubt. Kann für →Angriffe genutzt werden

Python: →Programmiersprache die meist interpretiert (und nicht compiliert) wird. Es liegen aber auch →JIT-Compiler vor. Python wurde ca. 1990 für die Lehre entwickelt mit dem Ziel Einfachheit und Übersichtlichkeit

QA: (Quality Assurance) →TQM

QAnon: Gruppe die seit 2017 Verschwörungstheorien mit teilweise rechtsextremem Hintergrund im →Internet verbreitet. Zentrale These ist eine einflussreiche, weltweit agierende, satanistische Elite entführe Kinder, halte sie gefangen, foltere und ermorde sie, um aus ihrem Blut eine Verjüngungsdroge zu gewinnen. US-Präsident Trump bekämpfe diese Elite und einen angeblichen „Deep State". Gegründet in den USA, aber die Gruppe hat auch in D. und Ö. Anhänger. Die Gruppe wurde 2018 wegen →Doxing und ‚Aufruf zu Gewalt' aus →Reddit entfernt, unterwanderte dann #SaveTheChildren auf →Facebook und →Instagram und spielt weiter eine sehr aktive Rolle in „rechten" Kreisen

QHSE: (Quality, Health, →Safety, Environment) Abteilung oder Verantwortlicher für alle diese Themen, die Vorschriften und Reglementierungen unterliegen. Manchmal auch noch zuständig für →Security. Siehe →Compliance

QKD: (Quantum Key Distribution) Generierung und Verteilung eines →Schlüssels auf Grund quantenmechanischer Prozesse auf der Basis von „verschränkten Teilchen". Das besondere daran ist, dass ein →Abhören der Schlüsselübertragung zu einer Störung führt, die entdeckt wird (da bei der Quantenmechanik eine Beobachtung immer zu einer Veränderung führt). Daher theoretisch vom Konzept her abhörsicher. Die Problematik liegt aber in der physischen Umsetzung, bei der Schwachstellen entstehen können die ein Angreifer ausnutzen kann (→side channel attacks).

http://arstechnica.com/security/2012/09/quantum-cryptography-yesterday-today-and-tomorrow/

QM: (Qualitätsmanagement) →TQM, →Six Sigma

QR-Code: →2D-Barcode, in der Werbung gern verwendet um mittels →Smartphone-Kamera eine →URL zu kommunizieren. Wird 2011 für →Angriffe genutzt, indem auf eine →Website mit →Schadcode verlinkt wird. Neues Schlagwort: →Attagging. Gefährlichere Angriffe lassen sich vermutlich über →USSD-Codes an →Handys schicken. Es gibt auch Verfahren zur Standardisierung der Abbildung von Zahlungsinformationen in QR-Codes. Auch hier besteht das Risiko darin, dass diese (z.B. durch Aufkleber) gefälscht sein könnten.

QR-codes werden ansatzweise auch für Absicherungen (Ersatz 2. Kanal, →out-of-band Kanal) verwendet, da es jedoch von sich aus keine →Verschlüsselung enthält ist es zwar schwieriger zu knacken, aber ohne zusätzliche kryptographische Absicherung nicht wirklich sicher.

In China werden QR Codes in den Zahlungssystemen →Alipay und →WeChat Pay genutzt (die ab 2019 auch noch Europa kommen). Händler und Käufer identfizieren sich dabei über temporäre QR Codes, die in den internen Systemen dann verknüpft werden. Ein ähnliches System auf Basis des →EAN

In Europa kam der QR-Code 2021 zu einer gewissen Prominenz, da er die Basis für die europäischen Corona-Impfbescheinigungen darstellt, eine sehr datensparende Lösung

QoS: (Quality of Service) meist über →SLA vereinbartes Serviceniveau, z.B. bzgl. Verfügbarkeit, Übertragungsleistung, etc. In Netzwerken bezieht sich QoS auf die Wahrscheinlichkeitenn für Dropped Packets, zu lange Verzögerungen bei der Zustellung eines Datenpaketes, Zustellungen in der falschen

Reihenfolge, die Reservierung von Bandbreite (→RSVP) oder Zustellung fehlerhafter Pakete

Quadplay: neues Schlagwort von CISCO das besagt, dass die gleiche Netzinfrastruktur für Daten, Sprache, Video und mobile Kommunikation genutzt wird. Es ist nicht klar, ob sich die Sicherheit dadurch erhöht oder erniedrigt

Qualität, Qualitätsmanagement: synergistisch mit Informationssicherheit. Siehe →TQM

Quantencomputer: Theoretische Implementierung auf der Basis von Quantentheorie, bisher nur als Proof-of-Concept verfügbar. Dabei werden ganz andere →Algorithmen eingesetzt, mit deren Hilfe Qubits manipuliert werden. Diese können nur 0 oder 1, sondern beliebige Zwischenwerte annehmen, die Wahrscheinlichkeiten entsprechen. Damit sollen die meisten der bisherigen Verschlüsselungsalgorithmen knackbar sein (mit Ausnahme z.B. von Lattice-based Cryptography),→Shor-Algorithmus
http://arstechnica.com/security/2012/09/quantum-cryptography-yesterday-today-and-tomorrow/

Quantified Self: (auch self-tracking, self-hacking, body hacking) Aktivitisten dieser Bewegung versuchen, durch viele →Sensoren (→wearable computing) möglichst viele →Daten über sich selbst, ihren Körper und ihre Aktivitäten zu sammeln und diese dann mittels →Data Mining auszuwerten. Dabei werden die Daten in der Regel auf zentrale Server geladen, wo sie auch mit den Daten anderer Teilnehmer verglichen werden können und öffentlich werden. Solange dies freiwillig geschieht, könnte man dies als unproblematisch betrachten, aber auf Grund des großen (wirtschaftlichen) Interesses z.B. durch Versicherungen die für Teilnehmer gezielt Rabatte anbieten wird oder durch Arbeitgeber, die durch →Gesundheitsapps eine gesundere Belegschaft fördern möchten wird vermutlich bald ein Druck entstehen bei so etwas mitzumachen und die Daten zu teilen. Siehe →P300, →Datenschutz, →Privatsphäre

Dies muss unterschieden werden von →life-logging (→Lifebits). Dabei werden alle Daten aus der Umgebung des Betroffenen z.B. mittels Fotos, Video und Sprache aufgezeichnet. Dies soll ein perfektes Gedächtnis erzeugen und kann verbunden werden mit →frictionless sharing. Dadurch wird natürlich auch in die Privatsphäre der Menschen in der Umgebung eingegriffen

QUANTUM: Aktivität der →NSA, bei der durch einen Man-on-the-Side →Angriff der Datenverkehr vom →Webbrowser zum →Webserver zusätzlich zu einem weiteren Webserver umgeleitet wird, der in die Antwort des korrekten Webserver zusätzliche Datenpakete einfügt, z.B. ein →Javascript, oder eine Verlinkung auf einen weiteren Webserver, von dem aus dann ein →Exploit zum Webbrowser gesendet wird. Dadurch ist die gezielte Übernahme von →Rechnern möglich

Quarantäne: 1)im Zusammenhang mit →Endpoint Security: wenn der Status des externen Gerätes (→PC oder →PDA) überprüft und als unzureichend empfunden wurde (z.B. veralteter →Virenschutz oder →Patch-Zustand) und das Gerät in einem speziellen Netzwerksegment zuerst aktualisiert wird

2) Aspekt von →BCM wenn bei einer →Pandemie Mitarbeiter zu Hause bleiben müssen. Firmen sollten für solche Fälle planen und zum Beispiel entsprechende →Zugänge aus dem →Internet vorsehen

Quellcode: (engl. Source code) Version eines Computer-→Programmes vor der Übersetzung (Umwandlung) in ausführbare Form. Nur die Quellcode-Version erlaubt die Änderung von Programmen und die Inspektion auf mögliche Sicherheitslücken. Zum Verhindern des Einbaus von Trojanern in den Quellcode sollte eine unabhängige Verwaltung des Quellcodes stattfinden. Quellcode sollte aus Sicherheitsgründen in Quellcode-Verwaltungssystemen verwaltet werden. Siehe →Open Source, →OSS

Quellcode-Verwaltung: ein wichtiger Aspekt einer sicheren Software-Entwicklung. Diese Systeme unterstützen Aspekte wie Protokollierung aller Änderungen, Wiederherstellen früherer Zustände, Änderungen nur durch spezielle Personen, etc. Produkte sind z.B. →GitHub, CVS, PVCS, SCCS, →RCS,.... Siehe auch →SCM – Software Configuration Management

Quellen-TKÜ: Telekommunikations→überwachung) auf dem Endgerät selbst, d.h. Abhören von →Messaging Apps, →VoIP oder →E-Mail vor der →Verschlüsselung für die Übertragung im →Internet. Dies setzt in aller Regel den Einsatz eines →Bundestrojaners voraus und ist daher politisch sehr umstritten. Siehe →RFS

QUIC: neues Transportprotokoll für das →Internet das gegenüber seinen Vorgängern insbesondere eine höhere Geschwindigkeit sowie konsequente →Verschlüsselung auch von Metadaten bietet, wird bei →HTTP/3 verwendet

Quick-Karte: frühere, angeblich anonyme Speicherkarte für die österreichischen →Bankomatkarten (→Geldkarte). Nach der Bezahlung erfolgt ein Abgleich mit einer Verrechnungsstelle (Evidenzzentrale), damit bei einer Zerstörung des Chips der Kontostand wiederhergestellt werden kann. Die Bezahlung erfolgt ohne Eingabe von →PIN. Siehe →e-Geld

Qwant: französische →Suchmaschine als einzige EU-basierte Alternative zu →Google. Da die Anfragen der Benutzer nicht registriert werden bietet sie auch keine personallisierten Ergebnisse. Dies vermeidet auch die →Filter Bubble. Sie verwenden ihren eigenen

→Crawler

RA: →Registration Authority

Race condition: (auch race hazard) →Schwachstelle in →Programmen, bei der der zeitliche Ablauf von meist mehreren parallelen Vorgängen eine entscheidende Rolle spielt

Rack: →19-Zoll Rack

Radio Frequency Analysis: →Side Channel Angriff, z.B. gegen kontaktlose →Smartcards durch Analyse der Veränderungen im elektromagnetischen Feld während der Ausführung von →Computerbefehlen

RADIUS: (Remote Access Dial-In User Service) älteres Protokoll für →Authentisierungsinformationen. Wird heute noch oft eingesetzt, auch z.B. in Verbindung mit →Token für →OTP. http://www.ietf.org/rfc/rfc2865.txt

RAID: (Redundant Array of Independent Disks) Verfahren bei dem mehrere → Magnetplatten so zusammengefasst werden, dass sie wie eine logische Platte erscheinen. Erlaubt in einer spez. Ausprägung, dass die Daten und eine Prüfsumme so auf mehrere Magnetplatten verteilt werden, dass auch bei Ausfall einer Platte der Betrieb aufrechterhalten werden kann. Wird für →Hochverfügbarkeit eingesetzt

Rainbow Table: sehr große Tabellen (> 100 GB) mit vorberechneten →Passwort-→Hashes, die für ein schnelles „Cracken" von Passworten genutzt werden. Auf diese Weise wird das „Knacken" von Passworten sehr beschleunigt, als Schutz gegen diese Angriffe wird →Salz eingesetzt, bzw. Passworte die länger sind als 8 Zeichen. Wird 2013 kaum noch genutzt, da →GPU-basierte →Brute Force und →Dictionary Attacks schneller sind

RAM: 1) (random access memory) →Speicher 2) (**R**eliability, **A**vailabilty, **M**aintainability) Schlagwort rund um →Hochverfügbarkeit. Es geht um hohe Verfügbarkeit durch Ausfallsicherheit und vereinfachte und dadurch schnelle Reparatur (vereinfachte Fehlersuche, gute Diagnostic Tools, schneller Komponentenaustausch)

Random: (engl. zufällig, zufallsbedingt) bei Zufallszahlengeneratoren (random number generator) wird unterschieden zwischen →pseudorandom number generator) PRG oder PRNG die auf Grundlage eines Startwerts („seed") eine vorgegebene Zahlenfolge produzieren und →random number generator (RNG).

Bei Sicherheitsanwendungen, z.B. bei der Erzeugung von →Schlüsseln, z.B. beim Starten einer →HTTPS-Verbindung, ist es wichtig, dass ein Angreifer der die Verbindung abhören will, nicht in der Lage ist, die Zufallszahl zu erraten oder über →brute force →Angriffe zu bekommen. Schwächen bei den Zufallszahlen sind daher sehr oft ein Angriffspunkt auf die →Verschlüsselungsalgorithmen. Noch problematischer ist allerdings, dass Programmierer die Zufallszahlen benötigen oft glauben, dies sei einfach und selbstgeschriebene Algorithmen nutzen, bei der die Zahlenfolge sich schnell wiederholt oder leicht vorherzusagen ist. Schwächung von Zufallszahlengeneratoren ist einer der Angriffe der →NSA. 2014 wurde bekannt, dass die NSA die →RSA (mehr oder weniger direkt) dafür bezahlt hat, dass ein →pseudorandom number generator mit einer →Backdoor in einer RSA-Software als Default eingesetzt wird (Dual_EC_DRBG)

Random Number Generator: (RNG) Generator für Zufallszahlen, wichtiger →Algorithmus in Sicherheits→programmen. Kann in →Software nur schwer implementiert werden (wirklich zufällig sind nur Ereignisse wie z.B. Kernzerfall oder Rauschen). Dies wird bei RNGs in →Rechnern zumeist simuliert, indem sog. →Entropie aus der Hardware bezogen wird (z.B. Plattenzugriffe oder Tastaturtimings). Wichtige →Algorithmen sind Yarrow in →MacOs, →iOS und FreeBSD und Fortuna in →Windows. Oft werden in RNGs kryptographische Funktionen wie →Hash-Algorithmen und PRNGs genutzt

RansomWare: →Schadsoftware, die z.B. durch →Verschlüsselung von →Dateien den →Rechner unbenutzbar macht und dann Lösegeld für die Entschlüsselung einfordert. Zuerst gesichtet ca. 2013, aber seit Ende 2015 zum dominierenden →Angriff im →Internet geworden, sowohl gegen Private wie Firmen. 2021 ist es zu einem der wichtigsten Zweige der Cyberkriminialität geworden, da die Gewinne erheblich sind und die Risiken für die Angreifer gering.

Hauptschutz ist Aktualisieren aller →Programme aller IT-Systeme, Vermeiden des Ausführens von →Schadsoftware durch entsprechende Schutzprogramme (aber →Malware-Schutz kann auf neue Varianten oft nicht sofort reagieren), das Erschweren von →Phishing-→Angriffen (z.B. durch →2 Faktor Authentisierung auf allen Verbindungen von außen ins Firmennetz und ausgelagerte →Datensicherung.

Zum Teil können Programme von →Antivirenfirmen Dateien auch entschlüsseln. Hilfe gibt es auf den →Websites der Antivirenfirmen. Herausforderung für die Angreifer ist das Inkasso, hier riskieren sie, dass man ihnen auf die Spur kommt. Dabei kamen früher Services wie →Western Union oder →Bezahldienste wie →paysafecard, heute vor allem →Bitcoin zum Einsatz (→e-Geld). Auf Grund der recht einfachen Umsetzung zumeist über per →E-Mail versendete Schadsoftware und die relativ sicheren Bezahlmöglichkeiten immer dominierender. Wird auch für Firmen immer mehr zum Problem, so es ist bereits zahlreiche Kliniken 2016 in zahlreichen Kliniken zu Betriebsausfällen gekommen. 2021 ist über einige sehr

spektakuläre Fälle mit großen Kollateralschäden und hohen Forderungen (die sehr oft bezahlt wurden) zu einer deutlichen Eskalation der Situation gekommen. Die Tatsache, dass sog. Cyberversicherungen die Lösegeldzahlungen oft übernehmen kurbelt wohl die Situation weiter an. Siehe auch http://sicherheitskultur.at/spam.htm#ransom

Ransomware-as-a-Service: (RaaS) ein Schlagwort, das die Tatsache beschreibt, dass durch den großen Erfolg bei dieser Form von Kriminalität eine sehr hohe Arbeitsteilung entstanden ist. Eine Gruppe erstellt den Zugang zum Netz des Opfers („access dealer“) und verkauft den dann weiter an andere, die die Verschlüsselung und oft auch das Entwenden von Daten vornehmen (Zwecks weiteren Erpressungsoptionen für den Fall, dass das Opfer die Daten aus einer Sicherung wiederherstellt). Andere wiederum sind für die Verhandlungen zuständig und wiederum andere kümmern sich um die finanziellen Geldflüsse

RaaS: →Ransomware-as-a-Service

rar-Format: Komprimierungsformat für Daten, siehe auch →Decompression Bombs

RAS: (Remote Access Service) Dienst der einen Zugang zum internen LAN / Local Area Network/ internes Netzwerk erlaubt. Über →call-back kann dabei die Zugangssicherheit erhöht werden

Raspberry Pi: (Himbeerkuchen) kreditkartengroßer Einplatinen-→Computer, entwickelt 2012 von Privatleuten für Schulungsszwecke, erhältlich für < 50 €. Es stehen mehrere → open-source →Betriebssysteme und mittlerweile jede Menge Software zur Verfügung. Siehe auch →Pineapple

Rasterfahndung: (engl. Dragnet) frühe (1970) Form von →data mining für polizeiliche Zwecke, in D. geregelt durch Landes- und Bundesgesetze, in Ö zwar theoretisch möglich, aber angeblich nie eingesetzt. Erstmals genutzt bei der Fahndung nach RAF-Mitgliedern. Es ging damals darum, z.B. durch Auswertung aller Rechnungsdaten für Elektrizitätsunternehmen Wohnungen zu finden, deren Stromrechnung bar bezahlt wurde und nicht über eine Bankverbindung. Es wurden Gesetze geschaffen die dies unter bestimmten Bedingungen ermöglichen.

Heute gibt es auf Grund der umfassenden Datenbestände dafür viel mehr technische Möglichkeiten, z.B. über die Daten die bei der →Vorratsdatenspeicherung anfallen. Diese technischen Möglichkeiten sind jedoch durch die Gesetze in D. und Ö eingeschränkt, d.h. es darf auf diese Daten immer nur einzeln zugegriffen werden, ein Durchsuchen der Datenbestände ist nur unter sehr eingeschränkten Umständen erlaubt. In anderen Ländern bestehen diese Einschränkungen oft nicht, so plant das FBI im Rahmen von →NGI einen automatisierten Abgleich ihrer Foto-Datenbank mit öffentlichen zugänglichen Fotos und den Bildern von Überwachungskameras. Ähnliche Rasterfahndungen sind mittels →Stimm-Erkennung gegen großflächig überwachte Telefonsysteme möglich.

Problematisch ist, dass bei der Durchführung kaum eine Diskriminierung vermeiden lässt und die Vorgehensweise mit dem Konzept der Unschuldsvermutung nicht kompatibel ist.

RAT: (Remote Access Trojan) Begriff, der ursprünglich nur ein spezielles Schadprogramm bezeichnete, jetzt aber oft für die Klasse von Programmen benutzt die sich als →Trojaner auf einem Rechner einnisten und dann eine Fernsteuerung dieses Rechners, z.B. für → dDoS-Angriffe oder im Rahmen von →APT-→Angriffen, erlauben. Beispiele sind Poison Ivy RAT, Xtreme RAT, Gh0st RAT. RATs sind eine Form von →Backdoors. Rechner mit solchen Backdoors werden manchmal auch →Zombies oder →Drohnen genannt

Rating: 1) Ratings sind Zeugnisse, in denen z.B. die →Kreditwürdigkeit von Menschen benotet wird. Diese sind ein wichtiges Instrument für die Festlegung der Konditionen bei Finanzierungen. Problematisch ist dabei, dass zunehmend auch Informationen aus →Social Networks und anderen Quellen einbezogen werden, was zu sozialen Ungerechtigkeiten und falschen Ablehnungen führen kann (z.B. wenn solche Ratings von Personalabteilungen genutzt werden um zu entscheiden wer zu einem Vorstellungsgespräch eingeladen wird. In China wird an einem umfassenden System gearbeitet, mit dem Menschen und Firmen über ihr Verhalten im →Internet (inkl. Konsumverhalten) ein Rating bekommen, das dann von allen anderen Menschen, Firmen und Behörden eingesehen werden kann

2) im Rahmen von →e-Commerce gibt es Ratings bezüglich →Vertrauenswürdigkeit von Händlern im Internet. Hierfür gibt es Organisationen, wie z.B. Cybertrust

3) im Rahmen von →eBay werden Ratings für Käufer und Verkäufer interaktiv, auf Grund von Feedback der Teilnehmer, automatisch errechnet

Rational Unified Process: (→RUP)

Raubkopie: (Slangbetriff Warez) illegale Version kommerzieller Software oder →anderer geschützter Inhalte (Musik, Filme), wobei zumeist der →Kopierschutz „geknackt“ wurde (→cracking). Viele der im →Internet erhältlichen Raubkopien sind mit →Trojanern oder →Spyware-Programmen gekoppelt. Auf diese Weise kann der Raubkopierer durch die dabei anfallenden Daten oder durch Nutzung des Rechners als Teil eines →Botnets Geld verdienen. Bei →Smartphone →Apps werden oft zusätzliche Funktionalitäten eingebaut (→Re-Engineering), z.B. für den Diebstahl per-

sönlicher →Daten oder Nutzung des Handys für Anrufe oder SMS auf →Mehrwertnummern. Siehe →Urheberrecht, →Copyright, →ACTA, →PRO-IP, →SOPA

RAV: (Risk Assessment Value) Teil von →OSSTMM zur Quantifizierung von Sicherheitsrisiken

RBA: →Risk-based-Authentication

RBAC: (Role-based access control) modernes →Sicherheitskonzept in IT-Systemen, bei dem die Rechte eines Benutzers im System variabel von seiner jeweiligen Rolle abhängen, damit eine Erweiterung von →Mandatory Access Control und →Discretionary Access Control. Implementiert z.B. in →Active Directory, →SELinux, FreeBSD, Solaris, →Oracle, SAP. Siehe →Authentisierung, →Autorisierung

RBN: →Russian Business Network

RC4: meistgenutze →Stromverschlüsselung, obwohl sie als geknackt gilt (angeblich kann die →NSA sie „in-realtime" entschlüsseln) und es Patentstreitigkeiten zu RC4 gibt. Sie ist sehr schnell und wird in allen →Webbrowsern untersützt. Problematisch ist dies, da ein →Man-in-the-Middle die Verbindung zum →Webserver auf jeden →Algorithmus heruntersetzen kann, der von beiden Seiten unterstützt wird

RC5: (Rivest Cipher) →Blockverschlüsselung mit geringem Ressourcenverbrauch, bei Schlüssellängen von 72-bit auch 2011 noch sicher

RCE: (remote command execution) eine der gefährlicheren →Schwachstellen – erlaubt das Ausführen von →Befehlen ohne direkten →Zugriff auf das Gerät, z.B. über das →Internet (z.B. nachdem das Opfer eine präparierte →Webseite besucht hat)

RCS:

1. (Rich Communication Services) Kommunikations→protokoll für Nachrichten zwischen →Mobilgeräten als Ablöse von →SMS. In 2019 wird diskutiert dass RCS zwar mehr Funktionen enthält aber aus Sicherheitssicht kein so großer Fortschritt ist, da im RCS-Protokoll zahlreiche → Schwachstellen gefunden wurden, so dass es nicht viel besser als das unverschlüsselte →SMS ist, das über das ebenfalls problematische Protokoll →SS7 versendet wird. Wird zum Teil auch als SMS+ bezeichnet. Die Einführung hängt davon ab, ab wann der jeweilige Telefonprovider seinen SMS-Versand auf dieses Protokoll umstellt. Genutzt wird RCS über die Messaging →App des →Smartphones, →Apple denkt 2019 noch über die Unterstützung nach
2. (Revision Control System) ältere →Software zur →Quellcode-Verwaltung von →Programmen

RDF: (Resource Description Framework) Spezifikation für ein Modell zur Repräsentation von Metadaten (Informationen über Webseiten und andere Objekte). Dies wird auch als →Semantic Web bezeichnet. Dies wird sicherheitsrelevant, da dadurch eine automatisierte Auswertung und Zusammenführung von →Websites unterschiedlicher Inhalte möglich wird, was die Möglichkeiten zu Überwachung durch →Data Mining in →Social Network Sites sehr vereinfacht. RDF wird u.a. in →RSS verwendet

rDNS: (→reverse DNS Lookup)

RDP: 1) (Remote Desktop Protocol) Grundlage für den Windows →Terminalserver Dienst. Erlaubt nicht nur die Präsentation eines Bildschirminhalts auf einem anderen (Client)-Rechner, sondern unterstützt auch den Zugriff auf Drucker und Peripherie des Clientgerätes. Wird, ebenso wie →Citrix, für eine Absicherung des Fernzugriffs auf Firmennetze genutzt, da eine solche Vorgehensweise keinen direkten Durchgriff zum Firmennetz wie bei einem →VPN-Tunnel erlaubt

4) (→Right to Data Portability)

Reaktion: eine der 3 Aufgaben des Sicherheitsmanagements: →Vorfallsbehandlung. Die anderen Aufgaben sind →Prävention und →Entdeckung

REAL ID: umstrittenes US-Gesetz zur Einführung eines Minimum-Standards für State-Identification cards für US-Bürger, vergleichbar mit einem Personalausweis. 2009 weigerten sich alle 50 Staaten, es zu implementieren. Mittlerweile (2019) ist es für alle Staaten der USA verpflichtend

Real-time Bidding: (RTB) die Technik mit der entschieden wird, welche Werbung auf einer →Website platziert wird. Dabei bieten Dienste wie DoubleClick (von →Google) oder DSP (von →Amazon) in dem Augenblick in dem ein Nutzer eine Website aufruft die Charakteristik dieses Nutzers an ihre Werbekunden an. Diese können auf der Basis dieser Daten (oder ergänzt durch Daten die der Werber selbst über diese Person hat) innerhalb von Millisekunden entscheiden, wie viel dem Werber eine Werbungsschaltung für diesen Nutzer wert ist. Auf diese Weise können auch Werber die nicht zum Zug kommen zusätzliche Daten über diese Person gewinnen. Alle diese Aktionen kommen ohne den realen Namen des Nutzers aus, es werden Pseudonyme wie →Advertising ID oder spezifische →Cookie-IDs genutzt

Real-time Protection: Funktionalität in →Virenschutz-Software und Anti-→Spyware Software bei der ein Starten des inkriminierten →Programmes verhindert wird

ReCAPTCHA: von →Google angebotener →Captcha Dienst zum Erkennen von →Bots. Dabei mussten früher kleine Fotos erkannt, bzw. interpretiert werden, in Version 3 wird dies

durch eine Analyse der Interaktion des Nutzers mit der →Website unter Einbeziehung der Daten die Google bereits über jeden Nutzer gespeichert hat versucht. Dies führt zu einer weiteren Anreicherung der Nutzerdaten bei Google

Rechenzentrum: →Rechnerraum

Rechner: (engl.: →Computer)

Rechnerraum: zumeist speziell ausgestatteter Raum für den Betrieb von Rechnern. Enthält Klimaanlage, oft eine separate Stromversorgung, →USV, →Brandschutz und Doppelboden für eine bequeme Kabelführung und vielen Reihen von →19-Zoll Racks. Siehe →Blitzschutz, →Data Center

Rechnungslegungsvorschrift: Regeln für die ordnungsgemäße Durchführung der Buchhaltungsaktivitäten. Durch die Nutzung von IT ist →Informationssicherheit eine Voraussetzung. Siehe →Compliance, →US-GAAP, →IFRS, →GoB

ReCoB: (Remote-Controlled Browsers System) von der deutschen →BSI favorisiertes Konzept für die Darstellung von →AJAX-basierten →Webseiten. Grundlage ist das separate Hosten des →Webbrowsers in einer →DMZ und Präsentation durch →Terminalserverkonzepte

Recorded Future: kommerzielles Unternehmen, finanziert von →Google und In-Q-Tel (Investmentarm der US-Intellegenzbehörden) das auf Grund von Auswertungen des → Internets Aussagen über den Zeitraum von 1 Woche anbietet (→Data Mining). Die einfachste Variante kostet 2011 149$ pro Monat

Recovery: Wiederherstellen eines ursprünglichen Zustandes, z.B. nach einem Schadensfall, oft durch Zurückladen von →Datensicherungsmedien. Siehe →Disaster Recovery

Recovery CD: →Datenträger, der eine Wiederherstellung des →Betriebssystems nach einer Beschädigung von Systemdateien erlaubt. Kann aber auch als →Angriffswerkzeug eingesetzt werden, z.B. um neue Administrator-→Accounts auf gestohlenen →Laptops einzurichten. Schutz dagegen bietet nur →Festplattenverschlüsselung

Reddit: seit 2008 ein →Social Network in dem Inhalte der ca. 430 Mio Nutzer in sog. Subreddits angeordnet werden, d.h. nicht wie z.B. bei →Facebook nach →Algorithmen aktiv verteilt werden. Umstritten, da sehr wenig Beschränkungen bzgl. der Inhalte bestehen. Verboten sind →Doxing, Aufruf zu Gewalt und Bedrohung. Wegen dieser Punkte wurde 2018 →QAnon aus Reddit entfernt, dies bedeutet nach Reddit-Regeln, dass zu den QAnon-Themen nie wieder ein Subreddit angelegt werden kann und die Nutzer permanent gesperrt sind (anders als bei den anderen Netzwerken wo diese Themen immer wieder neu eingebracht werden können). 2021 hat ein Subreddit aktiv Aktien des kleinen Unternehmens GameStop gepusht und damit Hedgefonds die auf einen starken Absturz der Aktien „gewettet" hatten (shorten) in große Bedrängnis gebracht

Red Flag Rules: Sections 114 und 315 aus →FATCA, das Finanzunternehmen zu mehr Vorsicht in Bezug auf →Identity Theft zwingt

red team: aus dem militärischen Sprachgebrauch: Gruppe, die den Feind spielt, in der IT z.B. im Rahmen eines →Penetrationstests. Siehe →tiger team

Redundanz: mehrfache Auslegung einer Ressource um →Hochverfügbarkeit zu erreichen. Siehe →common mode failure

Re-Engineering: Analyse von (zumeist fremden) →Programmen mit dem Ziel, ihre Funktion zu verstehen, bzw. sehr oft zusätzliche Funktionen (→Schadcode) zu implementieren. Dies geschieht z.B. bei →Smartphones um in beliebte →Apps Funktionen zum Diebstahl persönlicher →Daten oder Anruf zu →Mehrwertnummern einzubauen. Für diesen Zweck steht, abhängig von der eingesetzten →Programmiersprache und →Betriebssystem, spezielle →Software zur Verfügung, die diese Analyse erleichtert

Referrer: (in ‚http referer header' fehlt das ‚r') Wenn ein Objekt von einem →Webserver angefordert wird, z.B. ein Image, so übermittelt der →Webbrowser die ursprüngliche →URL, z.B. die →Webpage indem der Link zum Objekt enthalten war. So entstehen mittels →Web beacon oder →Web bug →Nutzerprofile für Werbezwecke

Reflection: (auch Reflected attack oder Reflective →Amplification Attack) →dDoS-→Angriff im →Internet. Der Angreifer trägt im →IP-Paket die →IP-Adresse des Opfers als Quelle ein (→spoofing) und sendet dies an Reflectors, d.h.→Hosts, die eine erheblich größere Datenmenge an den vermeintlichen Absender „zurück"senden (z.B. kurze Anfrage mit langer Antwort, bis →Amplification Faktor 1000)

Reflexion: in der Programmierung die Fähigkeit eines →Programms, sich selbst während der Ausführung zu analysieren und verändern. Dies verlangt nach Meta-Informationen wie Datentypen und ermöglicht Sicherheitsfunktionen wie Typenüberprüfung. Unterstützt, z.B. bei →Java, C#, VB.NET oder IronPython

regedit: →Registry

Registar: zumeist Registrierungsstelle für →Domains im →Internet. Spielt eine wichtige Rolle vom →Domain-Squatting und beim →Brand-Protection

Registration Authority (RA): →PKI

Registry: in der IT:

1) spezielle →Datenbank auf MS Windows

Rechnern, in denen das →Betriebssystem und →Anwendungen vor allem Programmparameter ablegen. Die Informationen sind für den Anwender nur über ein spezielles Programm (→regedit) zugänglich, auch →Malware nutzt dies aus und benutzt Registry Einträge für ihre Zwecke

2) Registrierungsstelle, z.B. im Rahmen des →DNS-Systems

3) Krankenaktenindex bei →ELGA

Regression Testing: bei →Software Tests die Wiederholung aller früheren Tests nach jeder Änderung der Software. Ziel ist es, zu vermeiden, dass frühere Fehler durch neue Änderungen wieder auftauchen oder bestehende Funktionalitäten verloren gehen. Siehe →Capture& Replay, →SCM

Regulation: EU-Regulation. Eine EU-Verordnung wird sofort geltendes Recht in den Mitgliedsländern. Der Nachfolger zur →Data Protection →Directive ist/war als Regulation geplant, d.h. diese Verordnung würde nationales Recht sofort außer Kraft setzen. Da diese Regulation strengere Vorschriften enthält ist sie 2013 (vorerst) am Widerstand von Irland und Großbritannen gescheitert. Siehe →EU

Reifegrad: (engl.maturity) Qualität einer Implementierung. Kann zertifiziert werden, z.B. nach →CMM oder →SSE-CMM

Release Management: Prozesse, die es ermlichen, Veränderungen an Hardware oder Software in geordneter Weise in eine Produktionsumgebung einzuführen. Teil des →ITIL-Prozesses und verwandt mit →Change Management und →Configuration Management

Remailer: →Anonymer Remailer

Remanence: das nur langsame „Verfallen" der Speicherinhalte von (an sich flüchtigen) Halbleiter-→Speichern (→DRAM), lässt sich für →Angriffe ausnutzen in dem die Speicherinhalte auch nach dem Ausschalten eines Geräts manchmal noch lesbar sind

Remediation: Beheben eines Problems oder einer →Schwachstelle, Teil des →Incident Managements. Siehe →ITIL

Remote Access: → Zugriff auf Rechner über eine größere Entfernung, in der Regel von außerhalb des Firmennetzes. Siehe →VPN, →RAS, →ICA, →RDP

Remote Access Service: →RAS

Remote Assistance: Konzept bei dem →Administratoren sich mit →Desktops verbinden können um dort Administrationsaufgaben, auch mit ihren erweiterten Rechten, durchzuführen. Unter Windows seit Windows XP. →VNC

Remote Forensic Software: (→RFS)

Remote Wipe: Löschen von →Daten auf einem →Smartphone oder anderem Gerät (z.B. unter →MacOS) mittels Fernzugriff, z.B. bei Diebstahl des Geräts. Der Dieb kann dies verhindern indem er die →SIM-Karte entfernt, womit das Gerät seine „Identität" gegenüber dem Remote-→Zugriff verliert. Anderseits ist diese Technik auch schon genutzt worden um bei Übernahme eines entsprechenden →Accounts im →Internet (z.B. →iCloud-Account) alle Daten auf dem Gerät des Opfers zu löschen. Remote Wipe wird bei Firmen oft im Rahmen von →MDM eingesetzt. Siehe auch →Wipe von →Festplatten

Rendering: (bzw. Rendern) Übersetzung in eine graphische Darstellung, auch bei 3D Darstellungen mittels →GPU). Meist jedoch verwendet zur Beschreibung der Übersetzung von →HTML Code einer →Webseite in die Darstellung im →Browser. Dies ist eine der zentralen Komponenten im Web-Browser und ist zum Teil separierbar. So werden bei fast allen Browsern in 2020 entweder Chromium (von →Google Blink – enhalten in →Chrome) oder die Rendering Engine von →Firefox genutzt

Replay-Angriff: →Angriff durch →Abhören eines →Datenverkehrs während des Austausches von →Authentisierungsinformationen und das Wiederholen dieser Informationen zu einem späteren Zeitpunkt um unbefugt in ein System eindringen zu können. Gegenmaßnahmen sind →OTP, →rolling code oder →Challenge Response

Replikator: →3D-Drucker, der sich selbst herstellen kann

Reputation Repair: Dienste die den „guten Ruf" im →Internet wiederherstellen sollen, z.B. wenn auf →Websites verleumderische Informationen verbreitet werden. Dazu gehören z.B. juristische Schritte (oder der Kontakt mit dem Diensteanbieter wie →Youtube oder → Facebook) um die Inhalte zu entfernen. Andererseits können übereilte Aktivitäten zum Entfernen von unerwünschten Inhalten, z.B. von Youtube schnell zum Vorwurf der Zensur führen (und zur weiten Verbreitung auf vielen anderen →Websites), was aus einer kleinen Krise leicht eine große Krise für das Unternehmen machen kann. Wenn ein Entfernen nicht möglich ist oder nicht ratsam, so beraten diese Firmen dabei, wie ein eigener Webauftritt so genutzt werden kann, dass bei Suchanfragen die unerwünschten Inhalte auf den hinteren Seiten erscheinen (→SEO). Siehe auch →Sexting, →Revenche-Porn, →Cyber Bullying

Reputation System: Konzept zur Herstellung von →Trust in →Web-Communities. Ein gutes Beispiel ist →eBay, bei dem Käufer und Verkäufer sich gegenseitig bewerten und auf diese Weise ein Rating entsteht, das reflektieren soll, ob der (virtuellen) Person vertraut werden kann. Der Erfolg ist gemischt, da auch dieses System manipuliert werden kann, z.B. durch →Sybil Attacks (Sybil nodes). Siehe auch →Gamification

Resilience: Die Fähigkeit von Systemen (jeglicher Art) mit unerwarteten Situationen fertig zu werden, z.B. auch mit Ausfällen von Komponenten oder mit →Angriffen. Biologische Systeme zeichnen sich typischerweise durch einen hohen Grad von Resilience aus. Siehe auch →Netze-von-Netzen

Resource Provider: → Federation Services

Responsible Disclosure: Form der Veröffentlichung von →Schwachstellen (zum Teil zusammen mit →Exploits), bei der der Hersteller zuerst eine Frist für die Erstellung eines →Patches erhält. Siehe auch →Bug Bounty, →ethical hacker, →L0pht

REST: (Representational State Transfer) →Programmierkonzept für den Austausch von →Daten zwischen →Rechnern. Wird heute auch sehr oft zwischen →Browser und →Webserver eingesetzt um →single-page applications zu implementieren (ähnlich wie →WSDL und →SOAP). Es werden dafür auf →Javascript basierende →Programmierbibliotheken angeboten die solche Entwicklungen stark vereinfachen

Restore: Zurückladen von →Daten aus →Datensicherungen, oft Teil eines →Recovery Vorganges

Restrisiko: →Risiken können nie 100% vermieden werden (selbst Untätigkeit birgt Risiken). Als Restrisiko wird bezeichnet, was nach einer →Risikoanalyse und –bewertung von der Person oder dem Unternehmen als akzeptables Risiko akzeptiert wird. Dazu kommen allerdings auch noch alle die Risiken, die bei der Analyse nicht erkannt wurden

Retained Organisation: →Outsourcing

Retargeting: Variante des →Trackings von →Website-Besuchern für die Platzierung von Werbung. Dabei wird beim Besuch einer bestimmten Website, z.B. des Werbenden oder auf einer Website zu einem bestimmten Thema, ein →Cookie gesetzt so dass dieser Benutzer beim Besuch anderer (themenneutraler) Websites wiedererkannt wird und durch Werbung zu einer Handlung (Kauf o.ä.) aufgefordert wird. Auch im US-Wahlkampf eingesetzt, dadurch werden →Internet-Nutzer auch auf Grund ihrer politischer Ausrichtung getrackt

Retina-Erkennung: →Identifizierung von Personen durch Analyse der Struktur der Retina am Augenhintergrund. Erfordert eine große Nähe zum Gerät und wird daher als stärkerer Eingriff empfunden als andere →biometrische Erkennung, wie z.B. →Iris-Erkennung oder →Face Recognition. Wird z.B. für den →Zugang zu einem →Rechnerraum eingesetzt

Revenche-Porn: (Rache-Porno) Versenden von pornographischen (oder freizügigen) Darstellungen um einer anderen Person zu schaden, oft trifft dies eine Ex-Partnerin. Dafür gibt es spezielle →Websites, die zum Teil Geld damit verdienen, gegen Geld diese Darstellungen wieder zu löschen. Natürlich ist dies illegal, aber leider durchaus verbreitet (auf Facebook allein wurden 2018 monatlich 54.000 Racheporno-Fälle geprüft). Dafür können z.B. Bilder verwendet werden, die als →Sexting entstanden sind. Manchmal wird empfohlen, bei solchen Fotos sicherzustellen, dass Identifikationsmerkmale, wie z.B. das Gesicht nicht mit drauf sind. Gegenmaßnahmen sind begrenzt. Man kann den Täter anzeigen, aber oft kann nicht sicher bewiesen werden, wir das Foto veröffentlicht hat. Man kann jedoch auch von der Website und →Suchmaschinen eine Löschung verlangen (Recht auf Vergessenwerden), oft wird man dafür jedoch einen spezialisierten Anwalt brauchen. Dies fällt auch unter →Reputation Repair

Reverse DNS Lookup: (rDNS) Feststellen eines hostnames und → Domäne bei gegebener →IP-Adresse, genutzt als Anti-→Spam Technik. Siehe →DNS

Reverse Engineering: Analyse von →Programmcode z.B. zum „Knacken“ von →Kopierschutz zum Erstellen von →Raubkopien. Siehe →Code Obfuscation

Reverse Proxy: →Proxy

Revision: unabhängiger, neutraler Vergleich zwischen dem tatsächlichen und dem vorgegebenen Zustand (Soll/Ist-Vergleich) eines Regelwerkes hinsichtlich seiner Zweckeignung und/oder Einhaltung. Siehe →Audit

Revocation: (engl. Rückruf) Prozess der bei Kompromittierung eines →Authentisierungselementes, z.B. →Smartcard, digitales →Zertifikat, abläuft um eine weitere Nutzung zu verhindern (→CRL, →OCSP). Bei →Biometrie nicht möglich

RFC:
1. Request for Comment: Mechanismus der →IETF Organisation zur Schaffung von de-facto Standards für Internet-Anwendungen. Oft sicherheitsrelevant, z.B. RFC 1244 Site Security-Handbook.
http://www.ietf.org/rfc/rfc1244.txt

2. Request for Change: auch “Change Request”. Im Rahmen von →ITIL der Vorgang, der ein Problem vom →Problem Management an das →Change Management übergibt

RFID: (Radio Frequency Identification) generell jede Technologie, bei der Identifikationsdaten drahtlos ausgetauscht werden. Dies reicht von älteren kontaktlosen →Smartcards für →Zutrittssysteme bis zu den kleinen preiswerten Chips, die eingesetzt werden, um Produkte und anderes zu identifizieren. In beiden Fällen ist eine Kennung enthalten, die über ein Funksignal aktiviert wird. Der Chip wird bei passivem Betrieb mittels Funk auch mit Energie versorgt. In der Form von →EPC

(Electronic Product Code) (oder →UPC) als Ersatz für die →Barcodes des →EAN eingesetzt. Wichtigster →Angriff ist →Cloning, erschwert durch →Verschlüsselung und →Authentifizierung. Mit geeigneten Antennen sind RFID Übertragungen über Entfernungen bis zu mehreren 100 Metern möglich. 2006 gibt es erste →RFID-Pässe, →ePass, die sich als angreifbar erwiesen haben. Aspekte der →Privatsphäre weden in →PIA behandelt

RFIDIOt: →open source Tools zur Nutzung von →RFID-Geräten, auch zum Lesen und →Clonen von →ePassports. http://rfidiot.org/

RFID Pass: umstrittene moderne Reisepässe, die drahtlos lesbare persönliche Informationen, einschließlich →biometrischer Daten (derzeit ein Foto des Gesichts) enthalten. Dabei wird eine →Verschlüsselung verwendet. Siehe →MRZ, →ePass

RFS: (remote forensic software) Software für die →Überwachung von „informationstechnischen Systemen" über das →Internet. Installation entweder nach Eindringen in die Wohnung oder analog zu sonstiger →Schadsoftware. Funktionen können sein:

a) →Quellen-→TKÜ (Telekommunikationsüberwachung), d.h. Abhören von →VoIP vor der →Verschlüsselung oder →E-Mail, bzw.

b) →Online Durchsuchung, d.h. →Online-Durchsicht (einmalige Momentaufnahme) oder →Online-Überwachung (über einen Zeitraum, inkl. →Keylogger) Umgangssprachlich auch →Bundestrojaner. Siehe →Forensic

RIAA: (Recording Industry Association of America) Interessenvertretung der US Musikindustrie, die →Digital Right Management (DRM) fordert und derzeit mit Hilfe von Prozessen versucht, →Filesharing über →P2P-Netze zu verhindern, siehe →Copyright

RICO Act: (Racketeer Influenced and Corrupt Organisations Act) US-Gesetz gegen organisierte Kriminalität, wird von →Microsoft zur Bekämpfung von →Botnets genutzt.

RID:

a. (Real-time Inter-network Defense) Draft IETF Standard zum Austausch von Informationen über →Angriffe wie →Würmer oder →DoS zwischen →ISPs

b. (**Recorder Identification Code**). Seriennummer eines CD- oder DVD-Brenners, wird auf jedes Medium gebrannt. Siehe →Fingerprinting

Ring: siehe →Doorbells

Right to Data Portability: (RDP) Article 18 in der Draft Data Protection Regulation der EU. Der →data subject muss "without hindrance" seine →Daten von einem Service Provider zu einem anderen transportieren können, z.B. von einem →Social Network zu einem anderen. Die Details sind derzeit noch unklar, es könnten auch mögliche neue Risiken dadurch entstehen. Diese Regel klingt wie eine gute Idee, könnte aber auch negative Effekte für den Wettbewerb haben: so wäre (so wie im Draft formuliert) auch ein Start-Up bereits in der ersten Version gezwungen, Datenkompalitibilität mit dem Marktführer anzubieten. →Facebook hat bereits eine Datenexport-Funktionalität implementiert

Rijndael: symmetrischer →Verschlüsselungsalgorithmus, der 2002 das ursprüngliche Standard Verfahren →DES als →AES (Advanced Enrcyption Standard) des amerikanischen NIST ersetzt hat. Es kann Schlüssellängen von 128, 196 und 256-bit verwenden und gilt als sehr sicher. http://www.esat.kuleuven.ac.be/~rijmen/rijndael/

RIM: (Research in Motion) eigentlich der Name der Firma, die das →Blackberry →E-Mail Gerät entwickelt hat. Wird jedoch auch für das Protokoll verwendet, das ein Blackberry benutzt, um mit dem entsprechenden Server zu kommunizieren

RIPA: (RIP Act, Regulation of Investigatory Powers Act, 2000) englisches Gesetz, regelt Überwachungsaktionen. Wird z.T. auch von Gemeinden bei „anti-social behavior" eingesetzt, z.B. Lärm, Grafiti, u.ä. Enthält auch Erzwingungshaft für die Herausgabe von →Schlüsseln, z.B. für →Festplattenverschlüsselung, vorsieht. Gegenmaßnahme ist z.B. →Plausible →Deniability

RIPE: (Reseaux IP Européens) Vereinigung der europäischen Organisation zur Vergabe von →IP-Adressen und →Domänen, auch aktiv in Sicherheitsfragen, z.B. bzgl. →DNS. Hat das →Hash-Verfahren MD 160 entwickelt. www.ripe.net. Andere regionale Organisationen sind APIN, APNIC, LACNIC, AfriNIC

RISC: (Reduced instruction set computer) CPU-Architektur bei der die Komplexität der (im Gegensatz zu →CISC) die →Befehle zugunsten einfacherer Implementierung und damit zumeist auch Stromverbrauch reduziert werden. Fehlende Befehle, z.B. für ‚editierende Speichertransfer in →Cobol) müssen dann vom →Compiler in eine Folge von Befehlen umgesetzt werden. Dabei werden typischerweise die Befehle weggelassen, die von Compilern selten benutzt werden. Ein heutiges Beispiel einer solchen Architektur ist z.B. →ARM

Risk-based-Authentication: (RBA) →Authentisierungsverfahren bei dem ein →Algorithmus im →Webserver dynamisch entscheidet, ob zusätzlich zum →Passwort noch ein 2. Faktor angefordert werden soll (z.B. ein →PIN der mittels →SMS übertragen wird). Dies soll die Sicherheit erhöhen ohne die Bequemlichkeit einzuschränken. Die Entscheidung basiert auf Faktoren wie der →IP-Adresse oder Eigenschaften des Geräts (→Device-Fingerprint oder →Browser-Fingerprint). 2021 können →Angreifer aber auch diese Systeme

durch vorherige Infektion des Geräts austricksen

Risiko: Nach →NIST SP800-30: die →Wahrscheinlichkeit, dass eine bestimmte →Bedrohungsquelle (→threat) unter Ausnutzung einer Verwundbarkeit (→vulnerability) ein Ergebnis (→impact) produziert das abträglich für das Unternehmen ist. D.h. es geht um Gefahrensituationen, in denen nachteilige Folgen eintreten können, aber nicht müssen. Risiko ist an sich nicht negativ, so lange das Risiko erkannt und verstanden ist und durch die Möglichkeit von ausreichenden Vorteilen belohnt wird. D.h. Risiko muss nicht unbedingt minimiert werden, sondern erkannt, bewertet und kontrolliert. Keine Geschäftstätigkeit ist ohne R. Siehe →operationelles R., →operatives R. →Restrisiko, →Marktrisiko, →Kreditrisiko, →Kursrisiko, →Risikoakzeptanz, →Risikoanalyse, →VaR, →ALE http://sicherheitskultur.at/Eisberg_risk.htm

Risikoanalyse: methodische Ermittlung aller Risiken eines Systems durch Abschätzung der Eintritts→wahrscheinlichkeit eines schädigenden Ereignisses und des damit verbundenen Schadensausmaßes (unter Einbeziehung von Bedrohungsanalyse und Verwundbarkeiten). Formale Vorgehensweisen sind u.a. beschrieben in →NIST SP800-39, →OCTAVE, →ISO 27005, →Black Swan

Risikoakzeptanz: Dokumentieren der Nicht-Behandlung von aufgezeigten Risiken, z.B. weil die erwarteten Schäden geringer sind als die Kosten für die Vermeidung oder weil sich durch das Akzeptieren der Risiken Vorteile ergeben, die das Akzeptieren der möglichen Schäden akzeptabel erscheinen lassen

Risikomanagement: (Risk Management) Verfahren zur Identifizierung, Kontrolle, Minimierung oder Vermeidung von Sicherheitsrisiken unter Aufwendung von akzeptablen Kosten (Def. ISO 17799) Dazu gehören →Prozesse wie →Datenklassifizierung, →Change Management, →Event →Monitoring, Architekturfragen wie →Netzwerk-Struktur, →Trust-Strukturen, z.B. zwischen →Windows →Domains und die →Auditierung von →Maßnahmen. Siehe →ISO13335, →Octave

Risikopsychologie: menschliche Fehleinschätzungen von →Risiko. Menschen konzentrieren sich auf Risiken die in der Presse berichtet werden, die sehr selten aber bizarr sind und schätzen alltägliche Risiken (wie Autounfälle), Probleme die sie nicht ändern können oder wo sie sich selbst in Kontrolle glauben, zu niedrig ein. Auch werden Schäden die erst in Zukunft realisiert werden (z.B. verminderte Gesundheit durch Rauchen), durch „→discounting“ mental abgewertet

RKE: (remote keyless entry) →RFID- oder →Infrarot-Systeme zum Öffnen von Türen, z.B. auch Autos. Anfällig gegen →Angriffe, z.B. →side channel attacks, trotz der Nutzung von →**rolling code** (**code hopping**), z.B. in KeyLoq

RL: (real live, wirkliches Leben) in der Internet-Szene, z.B. bei Gamern (→MMORPG) oft genutzte Abkürzung zur Abgrenzung der Aktiviäten im →Internet zu Aktitäten ohne →Computer und →Smartphone. Wird manchmal verwendet um zu sagen, dass die ethischen Regeln des RL auch in Internet-Kommunikationen gelten sollen. Es gibt Soziologen die von einer zunehmenden Verschmelzung der Identitäten von RL und im Internet ausgehen

rlogin: Applikation, die es dem Nutzer erlaubt, auf einem entfernten →UNIX-Rechner zu arbeiten. Sehr ähnlich zu →telnet. Auf Grund der geringen Sicherheitsimplementierung stellt diese Anwendung ein Sicherheitsrisiko dar

RMAN: (Oracle Recovery Manager) Tool zur →Datensicherung von →Oracle →Datenbanken. Erkennt auch Datenkorruption auf Blockebene und wird von vielen kommerziellen Tools intern genutzt

RMI: (remote method invocation) Kommunikationsprotokoll und Programmierschnittstelle in →Java (sehr ähnlich zu →RPC), sehr oft genutzt zwischen →Clients und →Servern. Nutzt →Ports 1098 und 1099 und arbeitet ohne →Verschlüsselung

Road Pricing: Sicherheitsrelevant, da bei allen bargeldlosen automatischen Verfahren Bewegungsdaten von den Fahrzeugen anfallen. Siehe →Data Mining

Robinson Liste: Liste von Personen oder Firmen, die keine unangeforderten Zusendungen (Brief oder →E-Mail) erhalten möchten. Siehe →Spam, →Opt-Out. In Ö: http://www.fachverbandwerbung.at/de/faq/faq_5.shtml#59, werbung@wko.at

Roboter: Maschine die auf Grund von →artificial intelligence selbständig (d.h. autonom) handelt. Dadurch entstehen eine ganze Reihe von Herausforderungen, z.B. die Absicherung solcher Systeme gegen →Angriffe die das System missbrauchen könnten (analog zu Angriffen auf →SCADA), aber auch im Bereich →Ethik, z.B. bei selbstfahrenden →Autos (→autonomous car) und →Drohnen, bzw. allgemein bei →autonomen Waffensystemen

Robotergesetze: von Isaac Asimov in 1942 (!!) im Rahmen einer Science Fiction Kurzgeschichte entwickelte Regeln die in der →Firmware von autonomen Geräten als →Ethik dienen sollen.

1. Ein Roboter darf kein menschliches Wesen (wissentlich) verletzen oder durch Untätigkeit gestatten, dass einem menschlichen Wesen (wissentlich) Schaden zugefügt wird.
2. Ein Roboter muss den ihm von einem Menschen gegebenen Befehlen

gehorchen – es sei denn, ein solcher Befehl würde mit Regel eins kollidieren.

3. Ein Roboter muss seine Existenz beschützen, solange dieser Schutz nicht mit Regel eins oder zwei kollidiert.

Es wurde zwischenzeitlich gezeigt, dass diese Regeln nicht ausreichend sind. http://philipps-welt.info/robots.htm#asimovlaws

Aber bei derzeit eingesetzten Robotern sind solche oder ähnliche Regeln sowieso nicht implementiert, es gelten die üblichen Sicherheitsnormen der physischen Sicherheit. Bei →autonomen Waffen, z.B. →Drohnen würden diese Gesetze den Einsatz des Geräts verhindern. Es gibt jedoch im Forschungsbereich →AI sehr wohl Aktivitäten dazu, wie die Menschheit vor autonomen Geräten oder Intelligenzen geschützt werden könnte (autonome Intelligenzen könnten auch ohne Körper Menschen erheblichen Schaden zufügen, wenn sie z.B. in die Steuerungen von Geräten (→Autos, Industrieanlagen) eingreifen können

robots.txt: →Datei auf einem →Webserver, die den →Bots der →Suchmaschinen mitteilt, welche der →Webseiten und/oder Images für eine Suche indiziert werden sollen. Wichtiges Mittel um Inhalte aus den Suchmaschinen fern zu halten. Soll durch →ACAP erweitert werden

RockPhish Gang: →Hackerorganisation, der die →Angriffssoftware →Neosploit und ca. 50% aller →Phishing-Angriffe zugeschrieben werden. Hat angeblich 2008 das moderne →Fast-Flux →Botnet →Asprox übernommen

Rogue Call Center: illegale Dienstleistung, bei der gegen entsprechende Zahlung →Social Engineering Angriffe (in vielen Sprachen) durchgeführt werden, z.B. das Erschleichen von Zugangs-→Passworten oder →TANs

ROI: (return on investment) Verfahren der →Wirtschaftlichkeitsberechnung. Gewinn, der durch eine Investition verursacht wird. Problematisch für Sicherheitsprojekte, da sich hier nur eine Vermeidung oder Verminderung von Schäden erwarten lässt (Reduzierung des →ALE). Siehe →ROSI, →NPV, →IRR

Rolling code: (auch code hopping) Konzept zum Verhindern von →Replay Attacks. Verwendet z.B. in →RKE-Systemen wie KeeLoq

root: in der IT:

1) unter →Unix oder →Linux der →Benutzername, der →Zugriff auf alle Teile des Systems hat und keinerlei Einschränkungen unterliegt. Die Nutzung dieses Benutzernamens sollte so weit wie möglich eingeschränkt werden und das zugeordnete →Passwort sollte so wenig wie möglich bekannt sein. Entspricht dem „administrator“ auf anderen Systemen. Siehe →sudo

2) in hierarchisch aufgebauten Ordnungssystemen, z.B. →Verzeichnisdienst oder File System, das „tiefste“ (bzw. „höchste“) Element, von dem aus alle anderen Elemente verzweigen

Rooting: Entfernen von Restriktionen bei einem →Android →Smartphone. Dadurch gewinnt der Benutzer volle Kontrolle über sein Gerät, die verwendete Software kann das Gerät jedoch auch anfälliger gegen →Angriffe machen. Siehe auch →jail-break bei →iOS, →NAND lock

Root jail: unter →Unix oder →Linux das Konzept, dass ein →Programm, das für seine Ausführung „root-Rechte“ braucht, trotzdem in seinen Auswirkungen eingeschränkt ist. Siehe →Pittbull, →DropMyRights

Rootkit: Software, die von →Hackern nach einem Eindringen in ein IT-Gerät genutzt wird, um Spuren (z.B. Einträge in →Logfiles) zu zerstören und die →Schadsoftware für den Anwender unsichtbar zu machen (diese Dateien werden dann nicht angezeigt). Oft wird dabei die Schadsoftware auch in den →MBR eingetragen und ist dann nur sehr schwer zu entfernen. Siehe →Bootkit

RosettaNet: Initiative zur Standardisierung der Formate von Geschäftsdokumenten und allgemeinen Informationen auf der Basis der →XML Technologien. Wird von vielen als Zukunft von →EDI gesehen. Arbeitet zusammen mit →OASIS

ROSI: (return on security investment) Ansatz, der eine Monetarisierung der →Informationssicherheit versucht. Siehe →ROI

Router: Geräte, die die Verbindung zwischen zwei Netzen herstellen. Router können auch von →Hackern missbraucht werden, z.B. durch Ausnützen und Manipulation der →Protokolle mit denen Router sich gegenseitig automatisiert über ihre Verbindungen informieren. Über →Port-Nummern und →IP-Adressbereiche kann ein begrenzter →Zugriffsschutz implementiert werden.

Der Begriff wird seit ca.2010 auch für integrierte Geräte verwendet, die in Privatwohnungen den →Internet-→Zugang herstellen und Router, Kabelmodem, →Firewall und →WLAN-→Access Point enthalten. Diese Massengeräte die nicht von geschultem Personal betreut werden, sind oft über das Internet angreifbar und werden dann manchmal für →Angriffe auf die Rechner im Haushalt oder auch zum Aufbau eines →Botnets verwendet. Sie verwenden oft eine Firmware namens →DD-WRT. Fast alle Anbieter wie Linksys, Netgear, Fritzbox, ASUS, D-Link, Cisco. 2014 wird bekannt, dass die →NSA mit ihrer →TAO Group weltweit sehr viele Router übernimmt, um damit den gesamten Datenverkehr abhören zu können. Siehe auch →MPLS, →VRF, →HNAP

Routing: Weiterleiten von →Daten→paketen

in →Netzen, z.B. mittels →Routern. Kann für →DoS manipuliert werden (route hijacking). Siehe →Cyberwar

RPC: (remote procedure call) Protokoll, das es einem Rechner erlaubt, →Programme auf einem anderen Rechner aufzurufen, ähnlich zu →RMI. Die Daten werden unverschlüsselt übertragen. Wird bei →Microsoft Systemen oft als Angriffspunkt für eine →Penetration genutzt (port 135/TCP)

RPG: 1) (Role Playing →Game). Spiel, bei dem die Spieler Rollen verkörpern. RPGs können IRL (in real live) gespielt werden (entweder als →LARP oder auf Papier als „tabletop RPG“) oder elektronisch. Wenn elektronisch dann entweder allein (z.B. *Dungeons & Dragons*) oder als →MMORPG (z.B. → World of Warcraft)

RPO: (Recovery Point Objective) maximaler zeitlicher Abstand zwischen letzter gesicherter →Transaktion vor einem Ausfall und dem Ausfall, siehe →RTO, →Desaster Recovery

RSA: 1) Verschlüsselungsverfahren. Die Abkürzung RSA steht für die drei Entwickler des Algorithmus: Ron Rivest, Adi Shamir und Len Adleman. Der RSA Algorithmus wird für asymmetrische →Verschlüsselungsverfahren verwendet. Seine Sicherheit basiert darauf, dass es zwar einfach ist, zwei große Primzahlen miteinander zu multiplizieren, umgekehrt aber schwer, ohne Kenntnis dieser Primzahlen das Produkt in seine Faktoren zu zerlegen.
http://arstechnica.com/security/2013/10/a-relatively-easy-to-understand-primer-on-elliptic-curve-cryptography/

2) RSA Data Security Inc., US-amerikanische Firma, die Sicherheitsprodukte anbietet. Gegründet von den RSA-Entwicklern Rivest, Shamir und Adleman. 2011 wird bei einem →Angriff auf das RSA-Netz der Algorithmus und wichtige Elemente der →2-Faktor-Authentifizierungs-→Token von RSA entführt. Diese Informationen werden später für ein Eindrucken bei Lockheed genutzt. 2013 wird bekannt, dass die →NSA die RSA (mehr oder weniger direkt) dafür bezahlt hat, dass ein →Zufallszahlengenerator mit einer →Backdoor in einer RSA-Software als Default eingesetzt wird (Dual_EC_DRBG)

RSS: (Really Simple Syndication oder auch Rich Site Summary) beruht auf →XML und wird verwendet, um Kurzbeschreibungen von Artikeln auf →Websites (insbesondere Zeitungsartikel) zu speichern und in maschinenlesbarer Form bereitzustellen. Ein spezieller RSS-Browser ruft diese Überschriften nach Kategorien ab und zeigt Headline, kurze Zusammenfassung und Link zum Artikel

RSVP: (Resource ReSerVation Protocol) Reservierung von Bandbreite zwischen →Routern. Wird für →QoS und zur Abwehr von →Denial of Service →Angriffen eingesetzt. Die beiden wichtigesten Konzepte sind Flowspec für die Reservierung von Resourcen und Filterspec für die Definition der Datenpakete für die die Flowspec Regeln gelten sollen

RTE: (run-time environment) hardware- und betriebsssystem-unabhängige →Laufzeitumgebung wie →Java-JVM (virtual machine) oder →.NET, die Systemfunktionalitäten für eine oder mehrere →Programmiersprachen anbietet. Aus Kompatibilitätsgründen werden bei JVM ältere verwundbare Versionen nicht gelöscht

RTO: (Recovery Time Objective) maximale Zeit vom Eintritt des Ausfalls bis zur Wiederaufnahme des Betriebs. Siehe →RPO, →Disaster Recovery

RTB: →Real-time bidding

RTCP: (RTP Control Protocol) in Verbindung mit →RTP eingesetztes Protocol für →out-of-band Informationen zu einem RTP-Datenfluss, eingesetzt z.B. in für die Überwachung der →Qualität von →VoIP. Siehe →MOS

RTP: →SRTP, →ZRTP, →RTCP

RTU: (Remote Terminal Unit, Fernbedienungsterminal) bei →SCADA Systemen die Regelelemente die eine Fernsteuerung, z.B. von einem Leitstand aus, erlauben

RUP: (Rational Unified Process) objektorientiertes Vorgehensmodell zur Softwareentwicklung und kommerzielles Produkt von Rational Software, seit 2002 Teil von IBM. Siehe →UML

Russian Business Network: (RBN) →ISP in Russland, das angeblich für die →organisierte Kriminalität im →Internet arbeitet

SaaS:

1) (Software as a Service) spezielle Form des →Cloud Computing. Nutzung von Anwendungen die im →Web zur Verfügung stehen, wie z.B. →Webmail. Mittels Technologien wie →AJAX können heute auch andere Anwendung sinnvoll angeboten werden, Beispiele sind salesforce.com oder die Office Anwendungen, die Google zur Verfügung stellt. Da zumeist die Anwenderdaten bei dem Serviceanbieter gespeichert werden, kann dies eine Gefährdung der →Vertraulichkeit darstellen und zwar mit →skalierbaren →Angriffen. Siehe →Outsourcing

2) (Security as a Service) Schlagwort für Security Dienstleistungen, z.B. Services wie das Untersuchen des Mailverkehrs auf →Spam oder zentral angebotenes →Vulnerability Scanning

Safari: Web-Browser von →Apple. Siehe →Browser

Safeguard: Begriff der Informationssicherheit. Verfahren, mit dem einem →Risiko begegnet wird. deutsch →Schutzmaßnahme

Safe Harbor: im →Datenschutz von 2000 -

2015 die Vereinbarung zwischen der EU und USA, die es europäischen Unternehmen ermöglichte, personenbezogene Daten legal in die USA zu übertragen. Wurde 2015 im sog. Schrems-I Urteil gekippt und durch →Privacy Shield ersetzt, das 2020 in Schrems-II ebenfalls für untauglich erklärt wurde. Die EU-Datenschutzrichtlinie verbietet es grundsätzlich, personenbezogene Daten in Staaten zu übertragen, die über kein dem EU-Recht vergleichbares Datenschutzniveau verfügen. Dies trifft auf die USA zu. US-Unternehmen konnten dem Safe Harbor beitreten und sich auf der entsprechenden Liste des US-Handelsministeriums eintragen lassen, wenn sie sich verpflichteten, die so genannten Safe Harbor Principles zu beachten. Problematisch ist Safe Harbor weil US-Unternehmen jederzeit die Teilnahme an Safe Harbor einstellen konnten und andererseits die Sicherheit nur über Selbst-Assessment bescheinigt wurde. Das Problem waren in beiden Fällen die uneingeschränkten →Zugriffe der Geheimdienste zu den persönlichen →Daten der EU-Bürger. Speziell im Zusammenhang mit den Entüllungen zur NSA durch →Edward Snowden gab es viele Stimmen für eine Aussetzung oder Abschaffung des Abkommens, was dann aber erst durch das Urteil Schrems-I gelungen ist

Safer: →API unter Windows, das es Anwendungen wie →E-Mail erlaubt, sicherheitsrelevante Informationen abzurufen, bevor ein →externes Programm oder →Scripts ausgeführt wird. Siehe →DropMyRights

Safety: → Security

Salami-Angriff: Hacker-Attacke (→Hacker), aus vielen kleinen, schwer zu entdeckenden Angriffen - sozusagen scheibchenweise. Auf diese Weise kann der Hacker vermeiden, von einem →IDS aufgespürt zu werden

Salt, Salz: zusätzliche Zufalls-Bits die bei einer →Hash-Funktion verwendet werden um einen →Angriff über vorberechnete Hash-Tabellen zu erschweren. Angeblich hat die NSA von Firmen wie Google eine Tabelle der verwendeten Salts für jeden Benutzer angefordert. Siehe auch →PBKDF2, →Bcrypt, →Scrypt, →Passwort

Samba: →Unix und →Linux Implementierung des Dateizugriffs zu →SMB/→CIFS angebundenen Magnetplattensystemen (→Shares)

Same Origin Policy: 1) (SOP) Sicherheitskonzept in →Browsern. →JavaScript und →ActionScript sollen nur dann auf Objekte wie →Cookies, →XML- oder →HTML-Dateien zugreifen können, wenn diese in →Domain, →Protokoll und →Portnummer übereinstimmen, gilt jedoch nicht für GET-requests. Soll →XSS und →CSRF verhindern, ist jedoch nicht wirklich effektiv. Wird in →HTML5 durch →Cross-Origin Resource Sharing ersetzt, was neue Risiken bietet. Siehe →CSP

2) (Standard Operating Procedure) schriftlich fixierte Arbeitsanweisungen, wichtig zur Einhaltung von →Qualität und Sicherheit

SAML: (Security Assertion Markup Language) auf →XML basierender Standard der →OASIS Organisation, mit dessen Hilfe →Authentisierungs- und →Autorisierungsinformationen ausgetauscht werden können, eine Implementierung von →Federation Services. Implementierungen sind Shibboleth, →AD FS, →WS FS. SAML unterstützt auch targeted IDs, d.h. Pseudonyme, d.h. der Service Provider (SP) muss vom →Identity Provider (IdP) nicht unbedingt Informationen über die wahre Identität bekommen, es kann auch ausreichen, dass eine Behauptung des Benutzers (z.B. bzgl. seines Alters) bestätigt wird (→claims-based authentication). SAML definiert Assertions, d.h. Aussagen über Personen, Protocols, die den Austausch von Fragen und Antworten zwischen IdP und SP definieren, Bindings die definieren wie diese Nachrichten physisch übertragen werden (z.B. →http) und Profile, z.B. das Webbrowser SSO Profil. Kann sinnvoll mit →OAuth für die →Autorisierung von →Zugriffen zwischen Benutzerprofilen auf unterschiedlichen →Websites kombiniert werden

Samurai: →Hacker, der angeheuert wird, um legal ein Firmensystem auf interne Sicherheitslücken zu testen

SAN: (Storage Area Network) Netz zum Anschluss von →Enterprise Storage Systemen, wird häufig mit →Fibre Channel Technologie gleichgesetzt. Es kann aber auch über andere Technologien, z.B. →iSCSI realisiert werden und verwendet spezielle →Switches. Siehe →Virtualisierung

Sandbox: Konzept, bei dem ein Programm in einer kontrollierten Umgebung ausgeführt wird, damit verhindert werden kann, dass dieses Programm Schaden anrichtet. Java→Applets laufen normalerweise in einer Sandbox ab. Über das Signieren von solchen Applets lassen sich Anwendungen entwickeln, die auch über die →Festplatte u.ä. zugreifen können. Andere Beispiele von Sandbox-Implementierungen sind die →Apps auf vielen →Smartphones, Adobe Reader X und PC-Programme wie →Sandboxie oder →NaCL. Auch mit Hilfe von virtuellen Maschinen (→VM) lassen sich Sandboxes implementieren. Dies wird von Firmen eingesetzt, die →Programme zum Schutz gegen →Malware entwickeln eingesetzt, um in dieser virtuellen Umgebung das Verhalten von unbekannten Programmen besser und automatisiert beobachten zu können. Die Entwickler der Malware setzen dahe sog. Sandbox-Evasion Techniken ein und der Entdeckung zu entgehen. Siehe →PitBull, →IEController, →chroot

Sandbox-Evasion: Techniken von →Malware-Entwicklern um der Entdeckung innerhalb einer virtuellen Testumgebung zu entgehen, z.B. das Erkennen, dass es sich nicht um einen orginären →PC sondern eine simulierte Umgebung handelt

Sandboxie: Software für →Windows, das es erlaubt, →Programme, z.b. →Web brwoser, so auszuführen, dass sie nicht direkt auf die →Festplatte oder die →Registry zugreifen können

Sarbanes-Oxley Act: (SOX) (Public Company Accounting Reform and Investor Protection Act, 2002) US-Rechnungslegungsvorschrift für Unternehmen, die an US-Börsen gelistet sind, Reaktion des Gesetzgebers auf den Enron-Skandal. Ziel ist eine stärkere Verankerung der Verantwortung des Managements durch Sicherstellen, dass die finanziellen Statements korrekt sind und vom Management abgezeichnet werden. Section 404 verlangt einen jährlichen Report über alle internen →Controls für IT-Systeme, die im Finanzreporting genutzt werden. Section 302 verlangt eine Offenlegung von →Schwachstellen jedes Quartal. Konkretisiert werden die Regeln durch →PCAOB Audit Standard 2, der ein internes Kontrollsystem (→IKS) ähnlich zu →COSO verlangt. →EuroSOX, →KontrAG http://www.law.uc.edu/CCL/SOact/soact.pdf

SAS: (Statements on Auditing Standards) US-Regeln für →Audits, herausgegeben durch das "Auditing Standards Board" des "American Institute of Certified Public Accountants" (AICPA). Einzelne der Regeln sind durchaus relevant für die →Informationssicherheit, z.B. SAS 70 (www.sas70.com), die den Umfang eines standardisierten Audits beschreibt, oder SAS No.99 (Consideration of Fraud in a Financial Statement Audit). Auch durch den →Sarbanes-Oxley Act, Section 404, gewinnt z.B. SAS 70 immer mehr Bedeutung, 2012 jedoch ersetzt durch →ISEA 3402 und/oder →SSAE 16

SAS 70: →SAS

SASL: (Simple Authentication and Security Layer) genereller Standard für die →Authentisierung von →IP-Verbindungen. Dabei können unterschiedliche Verfahren eingesetzt werden, z.B. →Kerberos, →NTLM

SATAN: (Security Administrator Tool for Analyzing Networks) eines der ersten →Freeware Programme zur Suche von →Schwachstellen in Netzwerken und Rechnern. Siehe →nessus

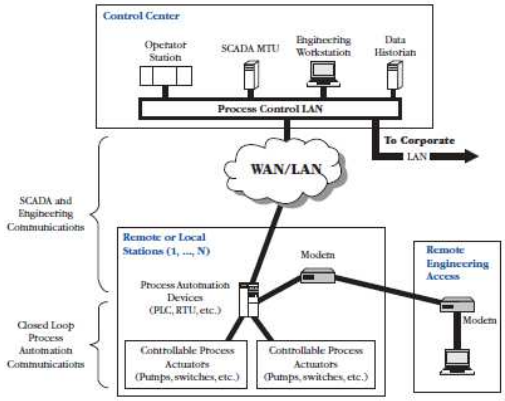
SB 1386 (California): →Datenschutzgesetz in Kalifornien, das eine Veröffentlichung von Sicherheitsvorfällen mit personenbezogenen Daten erzwingt

SCA: (strong customer authentication), siehe →PSD2

SCADA: (Supervisory Control and Data Aquisition) Verfahren um Netze von →Sensoren und Reglern mittels →PLCs zu überwachen und zu steuern, d.h. das das Überwachen und Steuern technischer Prozesse mittels eines Computer-Systems. Wird z.B. bei der Wasser- und Energieversorgung eingesetzt, heute oft verbunden mit dem „Office-Netz" und zum Teil mit →Internetzugang.

Dies ist eine →Schwachstelle die bei →terroristischen →Angriffen ausgenutzt werden kann. Jedoch auch ohne eine solche Verbindung können SCADA-Systeme erfolgreich angegriffen werden, wie →Stuxnet gezeigt hat. Dabei werden oft →USB-Sticks als Transportmedium für den →Schadcode eingesetzt (bewusst durch einen Saboteur oder unbewusst, weil ein Mitarbeiter nicht weiß, dass sein USB-Stick Schadcode enthält). Dies ist dann notwendig, wenn die Systeme mittels →Airgap geschützt sind.

Mittlerweile wurden →Schwachstellen in vielen Steuerungssystemen gefunden und dokumentiert. SCADA ist eine Untermenge von →ICS.



Siehe →HMI, →RTU

Scareware: neue Klasse von →Schadsoftware, die nach einer →Infektion des →PCs behauptet, der →PC sei infiziert und müsste durch eine kommerziell erhältliche Software bereinigt werden. Nach der Bezahlung wird eine Software zum Download angeboten, die in der Regel zu einer weiteren →Infektion des Geräts führt

Scatternet: bei →Bluetooth die Möglichkeit, dass mehrere →Piconets zu einem Netz mit mehr als 8 Teilnehmern verbunden werden

SCCM: (System Center Configuration Manager) System Management Tool von →Microsoft, enthält auch →Patch-Management. Nachfolger von →SMS, siehe SCE

SCE: (System Center Essentials) System-Überwachungs- und –Konfigurations-Tool von →Microsoft für →KMUs, enthält →WSUS

SCEP: →Simple Certificate Enrollment Protocol

Schadcode: →Programme oder Programmteile, die bei ihrer Ausführung Schäden verursa-

chen. Beispiele sind →Viren, →Würmer, etc. Dies können entweder Programmteile sein, die in andere reguläre Programme (oft Systemprogramme) eingeschleust werden um dort eine Schadfunktion auszuüben oder selbstständige Programme. Siehe →Re-Engineering

Schadsoftware: (auch Malware oder →Malicious Code genannt) Sammelbezeichnung für Software, deren Sinn und Zweck es ist, den Betriebsablauf eines →Computers oder →IT-Netzes zu stören. Implementierungen sind →Viren, →Würmer, bösartige Java→Applets, bösartige →ActiveX Programme, bösartige →Javascripts, →Trojaner, →Ransomware, →Scareware. Wird seit 2004 verstärkt und systematisch für kriminelle Zwecke eingesetzt (→organisierte Kriminalität). Siehe → Malware-Schutz, →Obfuscation, →Drive-by-→Infektion, →Mebroot, →TDL-4, →Polymorphismus, →mobile Malware, →crypting

Schengen-Informationssystem (SIS) II: umstrittene →biometrische Datenbank, die eine große Zahl von Informationen über EU-Bürger und Visa-Antragsteller enthält, einschließlich ihrer biometrischen Daten. Siehe →ePass

Schichtenmodell: →IEEE 802.2

Schleppnetzfahndung: (eng. drift net) Einsatz von →Data Mining, um aus einer großen Zahl von (personenbezogenen) Daten, z.B. Telefon- oder →Kreditkartenrechnungen, Bewegungsdaten aus dem →Road Pricing oder →Handy-→standortdaten Hinweise auf gesuchte Personen zu finden. Siehe →NIMD

Schlüssel (digital): →Verschlüsselung

Schüsselverwaltung: →Key Handling

Schredder: Gerät zum sicheren Entsorgen von →Altpapier zum Schutz von →Vertraulichkeit. Schreddern nur in Längsrichtung kann von professionellen Organisationen durch geeignete Software nach Einscannen der Schnippsel wieder rekonstruiert werden, ist jedoch für mittlere Vertraulichkeitsanforderungen ausreichend

Schufa: wichtigste →Kreditschutz-Organisation in D. Erstellt Bewertungen auf Grund der ihnen verfügbaren (oft unvollständigen) →Daten. Daher wird kritisiert, dass auf Grundlage dieses →Scorings oft Menschen benachteiligt werden

Schutzmaßnahme: Verfahren, mit dem einer →Bedrohung begegnet wird. Siehe →control, →safeguard

Schwache AI: →artificial intelligence

Schwache KI: →artificial intelligence

Schwachstelle: →Vulnerability, →Verwundbarkeit

SCM: (Software Configuration Management). →Quellcode-Verwaltung

SCOM: (System Center Operations Manager) System Überwachungstool von →Microsoft, Konfiguration auf der Basis von →SML. Nachfolger von MOM, siehe →SCE

Scoring: Bewertung von Menschen, Geräten oder Firmen. Heute entweder durch anderen Menschen (z.B. Bewertung von Lehrern, Firmen, Hotels, Restaurants) mittels entsprechender →Apps oder →Websites oder →Algorithmen, die eine Bewertung auf Grund von →Tracking-Daten durchführen. Wird eingesetzt bei vielen automatisierten Entscheidungen kann recht problematisch sein. Bei der Bewertung durch Algorithemen und →Artificial Intelligence (AI) werden alle Vorurteile die in den →Daten stecken in den Algorithmus übernommen. Fast keiner der AI-Systeme kann seine Entscheidungen begründen. Damit werden diese Entscheidungen nicht verifizierbar. Rating durch Menschen bietet viele Möglichkeiten der Manipulation und Erpressung. Siehe auch →Social Credit System, →Artificial Intelligence Act

SCP: 1) (secure copy) →Protokoll und →Programm für verschlüsselte Dateiübertragung über →SSH. Siehe →FTP, →SFTP

2) →Situational Crime Prevention

Scrambling: systematisches Verändern eines Textes oder →Programmcodes aus Sicherheitsgründen ohne Verwendung eines →Schlüssels, d.h. von →Verschlüsselung zu trennen. Bietet daher nur wenig Sicherheit sondern nur →Security through Obscurity

Screening: in der → Biometrie die Suche nach Personen (mit einer gewissen Eigenschaft) in einer Datenbank mit noch mehr Personen (N:M, N in M). Ziel kann sein, bestimmte Personengruppen in der Bevölkerung zu identifizieren, z.B. „Terroristen“ oder anfällige für eine bestimmte Krankheit. Sehr schwer zu realisieren

Screenlock: →Bildschirmsperre

Script: →Programmiersprache, die vor allem für kleine überschaubaure Probleme genutzt wird, oft als Teil von fertigen Software-→Anwendungen. Siehe →JavaScript

Script Kiddy: unerfahrener, junger →Hacker, der versucht, mit einfachen Programmen (= 'scripts') ein Computersystem zu stören oder gar zum Absturz zu bringen, oder in ein Computersystem einzudringen. Wird heute (2004/05) immer mehr durch professionelle Angreifer ergänzt

Scrubbing: (engl. Schruppen) das “Reinigen” von →Daten, z.B. durch Löschen von Daten auf temporär belegten Speichermedien, Bereinigung von Daten in Datenbanken oder auch das Filtern von unerwünschten Datenpaketen zur Abwehr eines →dDoS-Angriffs

Scrypt: →Password Hashing Funktion die bewusst auf großen Resourcenverbrauch programmiert wurde um →Brute Force Angriffe zu erschweren. Siehe auch →PBKDF2, →Bcrypt

SCS: →Social Credit System in China

SCSI: (Small Computer System Interface) wichtige Technik für IO-Busse mit parallelem Interface. Das SCSI-Protokoll wird heute jedoch auch über alternative Techniken, wie z.B. →iSCSI, genutzt

SCTP: (Stream Control Transmission Protocol) →Layer-3 Protocol (analog zu →TCP), wird verwendet in →PSTN. Im Gegensatz zu TCP wird →Multihome und Multistream unterstützt

SDK: (software development kit) hilfreiche Sammlung von →Programmteilen für abgegrenzte Funktionalität. Hat in der Programmierung on →Smartphone →Apps, aber auch modernen →Websites eine sehr große Bedeutung. Teilweise problematisch aus 2 Gründen: 1. werden sehr oft veraltete (unsichere) Versionen verwendet da es dem Entwickler zu mühsam ist, ständig neue Versionen seiner Software zu veröffentlichen wann immer eine der von ihm genutzten SDKs eine neue Version herausbringt. Zum anderen senden viele dieser Programmteile →Daten an die Anbieter dieser (meist kostenlosen) SDKs. Auf diese Weise bekommen z.B. →Facebook und →Google eine große Menge zusätzlicher Nutzerdaten geliefert (was für sie das kostenlose Anbieten der SDKs lukrativ macht). Siehe →Gesundheitsapp

SDL: 1) (Security Development Lifecycle) Software-Entwicklungsmethode von →Microsoft

2) (Specification and Description Language) von der →ITU definierter Standard zum Beschreiben von →State-Machine Systemen, kann für die automatische Codegenerierung verwendet werden

SDM: (System Definition Model) heute →SML

SDN: (→Software-defined networking)

SDP:

1) (Site Data Protection) Sicherheitsprogramm der Mastercard-→Kreditkarten-Organisation. Inhaltlich ein minimaler Grundschutz
2) (Session Description Protocol) bei →VoIP häufig genutztes Verfahren zur Übertragung der Metadaten. Die Audiosignale werden dann meist mittels →RTP übertragen. Siehe →SIP

SDR: →Software-defined Radio

SE: (→Secure Element)

Searchable Encryption: um →Daten sicher in der →Cloud verarbeiten zu können, wäre es wichtig, dass die Daten vor dem Transfer in die Cloud veschlüsselt werden. Dann kann aber bei herkömmlicher →Verschlüsselung in den Daten nicht mehr gesucht werden. Eine teilweise Lösung liegt darin, die Daten blockweise oder wortweise zu verschlüsseln, dadurch kann bei einer identitischen Verschlüsselung der Suchbegriffe auch in den verschlüsselten Daten gesucht werden. Wenn dies für →E-Mails angewendet wird so sind dadurch dass der Beginn und das Ende der E-Mails stark standardisiert sind, plain-text →Angriffe leicht möglich. Siehe auch →homomorphic encryption

Search Arbitrage: Technik zur Nutzung von →Websites im Rahmen von →Domain Parking. Ausnutzen, dass Anzeigen für gewisse Suchbegriffe, z.B. über Google →Adwords, sehr teuer sind, die Interessenten jedoch zum Teil günstiger gelockt werden können

Search Engine Optimization: →SEO

Second Life: (SL) seit 2003 →virtual world in der Personen durch →Avatare repräsentiert werden. Da die interne Währung (Linden $, →virtual currency) konvertierbar ist, auch ein Ziel von Betrügern Ort von →Cyber Bullying und Übergriffe auf Minderjährige. Siehe Problem der →Altersverifikation, →Cybergrooming. Seit 2017 lag die Zahl nur noch bei 800 000 Nutzern, angeblich wird an einer Nachfolge gearbeitet

Section Control: Überwachung von Fahrzeugen durch automatische Erkennung der Nummernschilder (→ANPR), hauptsächlich auf Autobahnen. Dient der Geschwindigkeitsüberwachung. Die Nummernschilderkennung kann natürlich auch für →Tracking eingesetzt werden

Sector: grundlegende Datenstruktur auf einer →Magnetplatte, die bereits von Hersteller vorgegeben ist. Wird bei der Formatierung neu geschrieben. →Cluster geben eine weitere Datenstruktur innerhalb der Sektoren hinzu

Secure Boot: Prozess der bei Windows 8 zwischen →UEFI (Nachfolger von →BIOS) und dem →Betriebssystem geteilt wird und →Rootkits verhindern soll. Bei Secure Boot können nur digital signierte Installationsmaterialien verwendet werden können, was z.B. auch ältere Versionen von MS →Windows verhindern würde

Secure by Default: →Sicherheitskonzept bei dem die Grundeinstellungen einer →Software oder eines →Rechners nach der Installation bereits sicher sind. D.h. keine voreingestellten allgemeinen →Passworte, →Firewalls sicher aktiviert und restriktiv eingestellt. Kann sich mit Benutzerfreundlichkeit beißen

Secure by Design: →Sicherheitskonzept bei dem bereits beim Entwurf der Software →Bedrohungen und die potentielle Böswilligkeit der Nutzer einkalkuliert werden. Ein solches Design hat es nicht nötig, „geheim“ zu sein, da die Sicherheit bereits im Design enthalten ist (keine →Security through Obscurity)

Secure Desktop Mode: verhindert in →Vista, dass andere →Tasks mit dem offenen →UAC-Fenster interagieren können

Secure Electronic Transaction: →SET

Secure Element: (SE) Gerät oder Komponente, die mittels →kryptographischen Techniken gegen Manipulation gehärtet ist („tamper resistant“) und geeignet ist, sensible Daten sicher zu speichern und zu verarbeiten. Beispiele sind →TPM, →HSM, →Chipkarten Chips zB. In Bankomatkarten, →SIM-Karten (→UICC). Leider enthalten heutige (2014) →Smartphones nur in Ausnahmefällen solche Elemente die für eine sichere Programmierung von →Apps, z.B. im Bankenbereich genutzt werden könnten (auf die SIM-Karten haben →Apps aus Sicherheitsgründen keinen Zugriff). Problematisch bleibt aber immer noch die Sicherung des Zugriffs auf das Secure Element. Dafür müssen Device Driver des Betriebssystems genutzt werden und falls dieser kompromitiert ist, können die Daten trotzdem manipuliert werden. Beispiel für ähnliche →Angriffe sind die kompromitierten →POS-Terminals, die trotz des Secure Elements in einer Bankomatkarte Zahlungen manipulieren können. Apple hat 2014 erstmals im A7 Prozessor „Secure Enclave“ eingebaut

Secure Flight: Nachfolgeprogramm in den USA zum wegen Widerstand eingestellten →CAPPS II-Programm. Ziel ist das →Screening von Flugpassagieren. Streitpunkt ist zusätzlich zum Abgleich gegen eine Watch-List die von der →TSA gewünschte Profilierung aller Passagiere auf der Basis von kommerziellen Datensammlungen, z.B. →Acxiom. Siehe →No Fly List

Secure Multipurpose Mail Extension: (S/MIME) Erweiterung des MIME-Formates, das die →Verschlüsselung und digitale →Signatur von →E-Mails unterstützt

Secure Remote Password Protocol: (SRP) in →SSL/TLS, →EAP, →SAML implementierte Methode zur →Authentifizierung mittels →Zero-knowledge password proof, d.h. mit sehr eingeschränkten Möglichkeiten zum →Abhören

Secure Shell: →SSH

Secure Socket Layer: →SSL

Secure Viewer: Konzept“You sign what you see”, d.h. das Programm mit dem eine digitale Unterschrift getätigt wird, zeigt den Inhalt, der signiert wird, an. Siehe →Signatur

Security: zusammen mit →Safety einer der beiden Aspekte, die im deutschen mit →Sicherheit zusammengefasst werden. Security ist auf theoretischer Ebene nur sehr schwer von Safety abzugrenzen. Safty schütz vor →„Murphys Law“, Security schützt auch gegen →Angriffe. In der Praxis spricht man von IT-Security, National Security, Computer Security, wohingegen Safety als Material Safety, Road Safety, Workplace Safety genutzt wird, siehe →QHSE

Security Breach Disclosure: aus den USA stammende Gesetzesinitiativen wie →California Security Breach Information Act, die eine Offenlegung erfordern, wenn Kundendaten „verloren“ gehen. Siehe →Identity Theft

Security Envelopes: →Sicherheitskonzept von →DHS, bei dem zwischen →Trusted Systems (und Personen) und Untrusted Systems unterschieden wird. Die Eingruppierung geschieht auf der Grundlage von →Authentisierungen

Security in Depth: →Sicherheitskonzept, wobei unterschiedliche, eigentlich redundante Sicherheitsmaßnahmen dafür sorgen sollen, dass auch →Angriffe abgewehrt werden können, die bereits einige Verteidigungen überwunden, oder umgangen haben. Beispiele sind →IDS, Malware-Schutz auf Arbeitsplätzen, Netztrennung durch →VLAN, etc. Gegensatz zu →Perimeter Security

Security information and event management: (SIEM) Realtime analyse aller Logs, ink. Netzwerkhardware wie →Router und →Firewall und allen Anwendungen. Weiterhin können auch die →Audit-Logs von →Zugangssystemen inkludiert werden. Ziel ist es, durch Techniken aus dem Bereich →Data Mining, wie Korrelation zwischen den Events →Angriffe und vor allem auch Datenabflüsse bei →APTs zu entdecken

Security Policy: →Information Security Policy

Security through Obscurity: falsches →Sicherheitskonzept das davon ausgeht, dass →Sicherheit dadurch entsteht, dass die Details dem Implementierung nicht bekannt sind. Richtiger ist →Secure by Design, d.h. die Sicherheitskonzepte sind bekannt und geprüft worden. In der →Kryptographie wird das Vermeiden von S.t.O. durch das →Kerckhoff Principle beschrieben. Siehe →Obscurity

Security Usability: Konzepte die es dem →Benutzer ermöglichen sollen, sicherheitsrelevante Entscheidungen zu treffen. Beispiel ist →NEAT

Seed: →Pseudo Random Number Generator

Segment:

1) Struktur in →Daten-→Netzen, unterschiedlich pro →OSI Schicht

2) Form der Organisation von →Hauptspeicher in →Computern zur →Sicherheits-Implementierung, nicht unterstützt in MS→Windows, und nur rudimentär in →Linux

Segregation of duties: →4-Augen-Prinzip

Selbstbestimmung, informationelle: (engl. Informational self-determination) nach dem →Volkszählungsurteil in D definiertes Recht, über die Preisgabe und Verwendung seiner →personenbezogenen Daten selbst zu bestimmen. Siehe →Datenschutz

Self-XSS: spezielle Variante von →XSS die →Verwundbarkeiten im →Webbrowser ausnutzt

SELinux: →RBAC-basierte Sicherheitserwei-

terungen für →Linux, implementiert von der →NSA mittels →LSM

Semacode, Semapedia: Bezeichnung für ein 2D-→Barcodesymbol, in dem eine URL kodiert ist, das von Foto- →Handys erkannt wird und ein Öffnen einer →Webseite bewirken kann. Diese Verlinkung kann genutzt werden, um auf dem Handy →Schadsoftware zu installieren

Semantic Archive: russische Software, mit deren Hilfe der vom russischen Geheimdienst FSB (dem Nachfolger des KGB) gesammelte →Internet-→Datenverkehr analog zu den entsprechenden methoden der →NSA mittels →Big-Data Methoden analysiert wird

Semantic Forest: Technologie die von der →NSA genutzt wird, um (abgehörte) →Dokumente (zum Teil durch →Speech to Text erzeugt) nach dem Inhalt zu klassifizieren. Geht über die Erkennung von Keywords hinaus

Semantic Traffic Analysis: →Narus

Semantic Web: →Web 3.0, →RDF

Sender ID: von →Microsoft vorgeschlagenes Verfahren zur Lösung des →Spam- und →Phishing Problems. Es enthält 3 Komponenten: Sender Policy Framework (→SPF), Caller ID for E-Mail und Submitter Optimization. Dabei werden im →DNS SPF-Datensätze für alle Domainen gehalten. Wenn ein Mailserver ein E-Mail empfängt, so vergleicht er die →IP-Adresse von der das E-Mail kommt, mit der der Absender Domaine. Nur bei Übereinstimmung wird akzeptiert

Sendmail: →SMTP

sensible Daten: nach dem österreichischen →Datenschutzgesetz: →Daten natürlicher Personen über ihre rassische und ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugung, Gesundheit oder ihr Sexualleben. Siehe →Datenschutz, →personenbezogene Daten

Sensor: Messeinheit, heute fast immer an digitale →Prozessoren angeschlossen, ursprünglich hauptsächlich im Bereich →SCADA und Industriesteuerungen (→ICS) genutzt. Heute sind Sensoren zusätzlich in vielen Geräte, vor allem in →Smartphones und → wearable computing zu finden. Dies reicht von Bewegungssensoren bis zu Sensoren für Blutdruck und andere Gesundheitswerte. Da diese Sensoren ihren →Daten letztendlich alle ins →Internet schicken, ist dies ein erhebliches →Privatsphäreproblem. Extrem wichtig sind Sensoren auch bei →autonomen Fahrzeugen und →autonomen Waffen

Sentiment Analysis: (Stimmungsanalyse) Spezialgebiet von →Big Data. Die Auswertung von Kommunikation in →E-Mails, →Social Network Postings, →Tweets, die Stimmung in Teilen der Nutzer analysiert wird. Problematisch wird dies, wenn diese Analyse zu Folgen für den Einzelnen führen, so wird 2014 versucht, potentielle Selbstmörder auf diese Weise zu finden und einer Behandlung zuzuführen. Dabei kommt es aber zu einer großen Zahl von falschen Diagnosen, die zu konkreten Nachteilen für die Betroffenen führen können. Diese Auswertungen von Social Network Postings werden 2014 sogar auf eine Analyse von Persönlichkeitsstrukturen einzelner Personen (Myers-Briggs Test) genutzt

SEO: (search engine optimization) (legale oder illegale) Bemühungen in →Suchmaschinen auf den vorderen Seiten gelistet zu werden, z.B. in dem wichtige Suchbegriffe im Text deutlich hervorgeheben werden oder über sog. Meta-Tags angezeigt oder auch über sog. Link-Farmen. Eine Suchmaschinen-Listung auf der ersten Seite der Ergebnisliste ist für viele Unternehmen existentiell. Illegale Methoden werden auch als ‚black SEO' bezeichnet. Sie verwenden z.B. sog. Doorway-Sites, die auf der Basis der Ergebnisse von Google Trends automatisiert erstellt werden, indem Texte legitimer Sites wie →Wikipedia geplündert und neu arrangiert werden, verbunden mit einem →Link auf den zu bewerbenden Webshop. Eine weitere Technik fügt automatisiert Links in Gästebücher und Diskussionsforen ein

SEPA: (Single Euro Payment Area) Vereinheitlichung des bargeldlosen Zahlens (Überweisung, →Lastschrift, Kartenzahlungen) über Ländergrenzen. Schließt neben den EU-Ländern auch andere ein. Sicherheitsrelevant da solche Überweisungen im Rahmen von →Phishing leicht über Ländergrenzen hinweg möglich sind und per Gesetz sehr schnell ausgeführt werden muss. D.h. die Angreifer haben eine Chance das Geld zu bekommen bevor das Zielkonto gesperrt ist. Der SEPA Raum ist größer als die →EEA, die wiederum größer als die EU ist. Die →PSD2 Richtlinie der EU gilt für den SEPA Raum. Im SEPA-Raum werden nach und nach neue innovative Dienste eingeführt. Nach der SEPA Lastschrift gibt es →SCT Inst, eine Überweisung (SEPA Credit Transfer) die innerhalb von 15 Sek abgeschlossen sein muss und in Zukunft eine Abbuchung in ähnlicher Geschwindigkeit, was besonderns für →eCommerce sehr interessant sein sollte. Siehe auch →IBAN, →BIC

Separation of Duty: Sicherheitsprinzip mit 2 möglichen Ausprägungen: →4-Augen-Prinzip (dual control) und →Funktionstrennung (functional separation). Beides ist z.B. in Banken- und Buchhaltungssystemen realisiert

Server: Variante eines →Rechners zumeist im Geschäftsumfeld, der mehr als einem Nutzer zur Verfügung steht, zumeist in ein →Rack eingebaut ohne eigenen →Bildschirm oder →Tastatur. Server bezeichnet aber heute zumeist einen virtuellen Server (siehe →virtual machine), bei dem durch geeignete Software

mehrere Betriebssysteme auf einem physischen Server implementiert sind. Beispiele für beide Typen von Servern: →Webserver, →Datenbankserver

Serverraum: Raum in dem viele physische →Server betrieben werden. Es muss →physische Sicherheit gegeben sein. Siehe →Data Center, →Colocation

Server-Side Request Forgery: (SSRF) →Angriff, bei dem Funktionalität eines →Servers ausgenutzt wird um Teile des Servers zu erreichen, die normalerweise nicht zugänglich sein sollten, verwandt mit →CSRF

Service Desk: nach →ITIL die zentrale Stelle, die alle Störungsmeldungen entgegennimmt. Aufgaben des Service Desks werden im →Incident Management beschrieben

Service Level Agreement: →SLA

Service Level Management: (SLM) nach →ITIL stellt das SLM sicher, dass die Service-Ziele in Service Level Agreements (→SLAs) dokumentiert und geregelt werden, außerdem überwacht und überprüft es den tatsächlich erbrachten Service auf Einhaltung der Vorgaben

Session: Kommunikationsverbindung, die zu einem bestimmten Zeitpunkt gestartet wurde und (zumeist) definiert beendet wird. Dies kann z.B. eine →Authentifizierung am Beginn und ein Logout am Ende sein. Es gibt session-orientierte →Protokolle wie →TCP und sessionlose wie →UDP

Session Cookie: →Session Management

Session Management: Sicherstellen, dass der zu Beginn hergestellte Kontext einer →Session erhalten bleibt, kann z.B. im →Web oft durch →Cookies mit geeigneten Inhalten erreicht werden (session cookies). →Angriffe gegen das Session Management können bei Anwendungen wie →e-Banking schwerwiegende Folgen haben

SET: (Secure Electronic Transaction) Spezifikation eines Protokolls für den gesicherten Austausch von Kreditkartendaten bei einem Kauf im →Internet. SET wurde von VISA und Mastercard mit IT- und Kryptographie-Unternehmen entwickelt. Die Sicherheitsmechanismen bestehen aus einer Kombination symmetrischer und asymmetrischer →Kryptographie, sowie →Authentifizierung der Beteiligten durch digitale →Zertifikate. Im Gegensatz zu →SSL beschränkt sich die Anwendbarkeit von SET auf den reinen Zahlungsverkehr. Ein Vorteil von SET ist die klare Identifikation des Kunden und die Tatsache, dass die Kreditkarteninformation nicht dem Händler zur Verfügung steht. Auf Grund der Notwendigkeit von Software-Installation und der Verfügbarkeit und Einfachheit von SSL hat sich dieses Verfahren nicht durchsetzen können

Sexting: Variation von →Texting (engl. für →SMS - d.h. Versenden von kurzen Nachrichten). Sexting bezeichnet das Versenden von Texten und Bildern sexuellen Inhalten. Solche Nachrichten haben in den USA bereits oft die Karriere von Politikern beendet. Daher wird gern →SnapChat verwendet, ein Dienst, bei dem die Nachrichten nach einer festgesetzten Zahl von Sekunden gelöscht wird (indem ein →Schlüssel zerstört wird).

Sexting kann problematisch sein wenn die Bilder Minderjährige darstellen (siehe →Cybergrooming). Dann kann dies unter Kinderpornographie, d.h. Herstellen, Besitz oder Verbreitung von pornografischen Darstellungen Minderjähriger, fallen. „Kann“ weil in D. und Ö. pornografische Darstellungen Jugendlicher (14–17 Jahre) mit Einwilligung (d.h. typischerweise zwischen 2 Partnern) OK sind. Absolut nicht OK ist das Versenden an andere Menschen (oder das „Rumzeigen“), dies kann unter →Revenche-Porn, →Cyber Bullying oder Cyber Mobbing fallen, bzw. sehr wohl unter Verbreitung von Kinderpornographie. Aber auch unter Erwachsenen können explizite Darstellungen bei Weiterbreitung zu Problemen sorgen (z.B. Erpressungsversuche wie bei Bezos, bzw. Karriereende wie bei US-Politikern). Daher wird manchmal empfohlen, bei der Aufnahme solcher Fotos sicherzustellen, dass Identifikationsmerkmale, wie z.B. das Gesicht nicht zu sehen sind. Gegenmaßnahmen siehe →Revenche-Porn

SFTP: (secure →FTP) nicht ganz klar definierter Begriff für sichereren Dateiaustausch, entweder auf der Basis von →SCP oder FTP über →SSL

SGML: (Standard Generalized Markup Language) Kodierungsstandard, der für die Textverarbeitung entwickelt wurde, um Formatierungen in einer standardisierten Form wiedergeben zu können. Eine stark vereinfachte Variante wurde zur ersten Version von →HTML. →XML ist ebenfalls aus SGML hervorgegangen

SHA: (Secure →Hash Algorithm) Mehrere Verfahren, um aus großen Dateien eine vergleichsweise kurze „checksum“ zu erzeugen,so dass auch geringe Änderungen in den →Daten ein ganz anderes Ergebnis erzeugen. Wird heute in den Familien SHA-1, SHA-2, SHA-3 eingesetzt. Für SHA-1 wurde Anfang 2005 bereits ein Verfahren zum Erzeugen einer →Collision aufgezeigt (Erzeugung einer anderen Datei mit dem gleichen Hash-Wert). Durch das neue Verfahren hat sich die Zeit für die Berechnung der Kollision verkürzt. Damit sind die SHA-1 Algorithmen nicht viel sicherer als →MD5. Besser sind die SHA-2 Versionen SHA-256 und SHA-512. SHA-3 ist noch in Entwicklung

Shadow IT: Begriff der beschreibt, dass heute (214) IT-Abteilungen mehr und mehr die Kontrolle über die Firmen-IT verlieren. Gründe sind z.B. die →ByoD-Welle, wo Mitarbeiter und

Vorstände mit neuen →Smartphones oder →Tabletts kommen und ihre →E-Mails auf diesen Geräten bearbeiten wollen, bzw. überhaupt auf Tabletts ihre Arbeit erledigen. Dies wirft ganz neue Herausforderungen für die IT-Abteilungen in Bezug auf Sicherheit und Benutzer-Support auf. Dazu gehört aber auch, dasss Fachabteilungen an der Firmen-IT vorbei Verträge mit →Cloud Diensten (→SaaS) wie z.B. salesforce.com abschließen ohne sich an die internen Sicherheits- oder andere Regeln zu halten, z.B. separate →Authentisierungsimplementierungen in das Unternehmen einbringen. Es kann sogar so weit gehen, dass Fachabteilungen mit technischem Know-how ganze →Server bei Diensten wie →AWS anmieten. Ebenfalls gehört dazu, dass Mitarbeiter ohne Rücksprache Firmendaten auf Cloudspeicher-Dienste wie →Dropbox auslagern

shall: (engl. muss) wichtiges Wort in →Standards und →Best Practise Dokumenten. Es bezeichnet eine Vorschrift. Siehe →should, →must not

Shannon: 2001 verstorbener Informationstheoretiker, Begründer der information theory und information entropy. Sicherheitsrelevant ist Shannon's Maxim: „the enemy knows the system", siehe →Obscurity, →Kerckhoffs' principle

Share:

1) Datenbereiche auf zentralen Magnetplattensystemen, auf die mehrere →Benutzer zugreifen können, unter Windows mittels →SMB, unter →Unix und →Linux mittels →Samba. Bei falscher Rechtevergabe oder Eindringen in das Netzwerk ein Sicherheitsprobleme. Mit Windows 7 und Windows Server 2012 können solche →Zugriffe mittels SMB 3 auch verschlüsselt erfolgen
2) Ereignis in einem Social Network: Ein Benutzer klickt auf einer anderen →Website auf einen „Share"-Button und „teilt" dieses Ereignis mit seinen „friends". Im Roman „The Circle" auf die Spitze getrieben mit Slogans wie „sharing is caring" und „everything that happens must be known". Siehe auch →Zuckerberg's Law

Shareware: →Programm(e), die zunächst kostenlos getestet werden können, für deren Benutzung der Autor dann aber einen Kostenbeitrag verlangt, ohne den die weitere Benutzung eine Verletzung des →Urheberrechts darstellt. Z.T. mit eingeschränkter Funktion (erst nach Zahlung des Kostenbeitrages wird die Vollversion zur Verfügung gestellt und ggf. Unterstützung bei Problemen angeboten). Siehe →Public Domain, →Freeware, →GPL

Shell: in der IT eine Form des Computer-→Zugriffs, typischerweise mittels Texteingaben („command line interface", CLI), das in aller Regel Zugriff auf Funktionalitäten des →Betriebssystems ermöglicht. Der Name rührt daher, dass damit die Schale um das Betriebssystem gemeint ist. „getting shell" bedeutet unter →Hackern, dass er/sie Betriebssystemzugriff erlangt hat

Shell account: →Account auf einem Rechner, der ein Arbeiten auf diesem Rechner ermöglicht, entweder durch einen →GUI oder durch ein Fenster, in dem Kommandos als Text eingegeben werden können. →Hacker versuchen, auch über Zugriff vom →Internet aus eine solche Shell zu eröffnen, um dann auf dem fremden Rechner Kommandos ausführen zu können

Shield Icon: Anzeige in →Vista und Windows 7, dass eine Funktion →Admin-Rechte benötigt, Teil von →UAC

Shockwave: Datenformat von Macromedia (jetzt Adobe) mit dessen Hilfe Inhalte (Sound, Bilder) komprimiert und im →Webbrowser dargestellt werden können. Director-Shockwave Dateien haben die Dateiendung ".dcr". →Schwachstellen in älteren Versionen lassen sich für →Angriffe ausnutzen

Shodan: spezielle →Suchmaschine zum Auffinden von →ICS-Anlagen, d.h. Industriesteuerung, die wenn sie →Verwundbarkeiten enthalten (was sie fast immer tun) für →Angriffe gegen Infrastrukturen wie Wasserversorgung, Stromgewinnung, und alle Arten von →IoT-Geräten missbraucht werden können

Shor-Algorithmus: →Algorithmus für →Quanten-Computer für die Berechnung der Faktoren von Primzahlen. Würde, wenn realisiert, asymetrische →Verschlüsselungen auf der Basis von Primfaktoren „knacken" können. 2013 erst bis zur Zahl 15 (=5x3) möglich

should: (engl. sollte) wichtiges Wort in →Standards und →Best Practise Dokumenten. Es bezeichnet eine Empfehlung, die nicht zwingend ist. Siehe →shall, →must not. http://www.kan.de/pdf/brief/deu/1999-1-sprachen.pdf

Sicherheit: im Deutschen unklar definierter Begriff, der →Security (Sach- und Informationsschutz, auch gegen vorsätzliche →Angriffe) und →Safety (Schutz von Leben und Gesundheit, z.B. durch Unfälle) beinhaltet

Sicherheitskonzept: Grundlegende Vorgehensweisen und Annahmen zur Erreichung von →Sicherheit, z.B. →4-Augen-Prinzip, → Defense in Depth, →Kerckhoff's Principle, → Compartmentalization, →Fail-safe, →Minimalprinzip, →Need-to-know, →Out-of-band, →Secure by Default, →Secure by Design, →Privacy by Default, →Privacy by Design, nicht →Security through Obscurity. Siehe →Information Security Policy

Sicherheitslöcher: →Verwundbarkeiten

Sicherheitspolicy, Sicherheitspolitik: →Information Security Policy

Side Channel Angriff: →Angriff über die Analyse von Nebeneffekten des Betriebs von IT-Systemen, z.B. gegen →Smartcards über Stromverbrauch (→Power Analysis, differential power analysis, DPA) oder elektronische Abstrahlungen (→Electromagnetic Analysis, →Radio Frequency Analysis) oder →Van Eck Strahlung. Auch möglich durch Ausnutzen von shared Komponenten wie →Cache. So wurde 2012 gezeigt, dass es möglich ist aus dem Cache einer virtuellen Maschine einen →Schlüssel einer anderen virtuellen Maschine auszulesen. Siehe →Hamming

Sidewalk Labs: Tochterfirma von →Google (d.h. →Alphabet) mit dem Fokus auf ‚urban innovation organization'. Sie wollen städtische Infrastruktur durch technische Lösungen verbessern um damit die Kosten und den Energieverbrauch zu reduzieren und den Komfort zu erhöhen. Das größte Projekt ist in Toronto, wo die Stadt der Firma 2017 ein Erneuerungsprojekt für ein Stadtviertel überlassen hat. Aus der Zivilgesellschaft gibt es Widerstand dazu, es wird eine Übertechnisierung und Datensammelwut vorgeworfen. Eine Tochtergesellschaft Intersections hat in New York 7500 Telefonzellen auf kostenloses →WLAN und andere →Internetdienste (wie z.B. öffentliches Websurfing an Bildschirmen der Telefonzellen) umgerüstet (→LinkNYC). Dagegen gibt es viele Bürgerproteste denn es werden nicht nur die →Daten aller Nutzer dieser Kioske gesammelt, sondern aller Menschen die an den Kiosken mit ihren Smartphones vorbeigehen (→Tracking), zur Erklärung siehe unter →Access Point

SIDF: (Sender ID Framework) von →Microsoft vorgeschlagenes Verfahren zur Vermeidung von →Spam. Enthält das →SPF-Verfahren

SIEM: →Security information and event management

SigG: →Signaturgesetz

SIGINT: (Signals Intelligence) Spionage durch Auswertung von Kommunikation, heute zumeist durch →Überwachung von →Internet-Datenverkehr. Früher durch Überwachung von →Telex, →Fax, Telefon, Sprechfunk, Morsesignalen, etc. Im Gegensatz dazu HUMINT, human intelligence, der Einsatz von Spionen und Informanten im jeweiligen Land. Siehe auch →ECHELON, →Edward Snowden, →NSA, →LOVINT, →ENLETS

Signal: →Open-Source →Messaging →Client der für seine Datensparsamkeit und gute →Verschlüsselung (→PFS) bekannt ist (→Signal Encryption Protocol), das nun auch von →Whatsapp eingesetzt wird. Nachrichten, aber auch Nutzerprofile u.ä. sind auch für die (dezentralen) Betreiber eines solchen Dienstes nicht einsehbar. Die →Daten werden über →RTP übertragen und können auch Sprache und Video sein. Gegründet vom Verschlüsselungsexperten Moxie Marlinspike und →WhatsApp-Gründer Brian Acton (letzterer 'regiert' als Alleinherrscher über das Projekt). Signal hat den Ruf, "der gute Messenger". Im Gegensatz zu →Matrix und →Telegram wird aber nicht nur eine Telefonnummer beim Anlegen eines Benutzeraccountss verlangt, sondern auch allen Kommunikationsteilnehmern in jedem Gespräch angezeigt, d.h. für hoch-vertrauliche Kommunikation (z.B. →Whistleblowing) nicht geeignet.

Signal Encryption Protocol: →Verschlüsselungs-Protokoll das von Signal genutzt wird, aber mittlerweile auch von →Facebook Messenger, →Google →Android Messaging →App, →Mumble und anderen Diensten. Sehr gute Implementierung von →End-to-end →Perfect Forward Secrecy

Signator gem: § 2/2 →SigG: "Signator: eine natürliche Person, der Signaturerstellungsdaten und die entsprechenden Signaturprüfdaten zugeordnet sind und die entweder im eigenen oder im fremden Namen eine elektronische →Signatur erstellt, oder ein Zertifizierungsdiensteanbieter (→CA), der Zertifikate für die Erbringung von Zertifizierungsdiensten verwendet."

Der Signator ist demnach eine natürliche Person. Die einzige Ausnahme im österreichischen SigG stellen die qualifizierten Zertifikate von Trust Centern dar, die diese im Rahmen ihrer Leistungserbringung einsetzen

Signatur, digitale: →digitale Signatur

Signaturgesetz (SigG): Gesetz in D. und Ö, das die rechtlichen Grundlagen für die Nutzung von →digitalen Signaturen schafft

Signaturkarte: → Smartcard, die mittels eines Lesegerätes für die Erzeugung einer →digitalen Signatur und damit auch zur →Identifizierung einer Person geeignet ist. →Bürgerkarte

Silent Circle: neue Firmengründung von →Phil Zimmermann mit dem Ziel sicherer Kommunikation auf →Smartphones. Silent Phone bietet end-to-end verschlüsseltes Telefonieren und Silent Text bietet verschlüsselte →SMS. Die Software ist als →open source verifizierbar. Die Software bildet auch die Basis des Blackphones, einer sicheren →Android Variante

Silent Commerce: (SC) Transaktion von Rechner zu Rechner, ohne Eingriff des Menschen. So könnte z. B. der Computer des Herstellers beim Zulieferer automatisch den benötigten Nachschub bestellen, Auftragsabwicklung, Rechnungsstellung, selbst die Bezahlung ließen sich automatisieren. Ein anderes häufig genanntes Beispiel für Silent Commerce ist der Kühlschrank, der selbstständig nachbestellt, wenn ein Lebensmittel zur Neige geht. Entsprechende Systeme werden z.B. im Einzelhandel für Nach-

bestellungen bereits eingesetzt

Silent SMS: spezielles →SMS, das vom →Handy nicht angezeigt wird und der Ortsbestimmung des Handys dient, z.B. bei →Überwachung. Kann in Notsituationen gerechtfertigt sein. Siehe →Geolocation

Silverlight: Konkurrenzprodukt von →Microsoft gegen →Adobe Flash, Adobe →Shockwave, Apple Quicktime zur Darstellung von 2-D Graphiken und Multimedia. Basiert auf →XAML und ist damit für →Suchmaschinen besser indizierbar. Unterstützt →MP3, wma- und wmv-Format. Der Silverlight Code hat keinen →Zugriff außerhalb „local stores", z.B. auf Peripherie oder lokale →APIs. Allerdings ist dieser Plattenbereich nicht geschützt. Silverlight enthält eine reduzierte Version das →.NET-Runtime und ist keine Implementierung des →SVG-Standards

SIM: 1) (Subscriber Identity Module) ein kleiner Computer mit einem Prozessor, RAM und ROM in Form einer kleinen →Smart Card (→UICC) die in ein →Handy gesteckt wird und dort u.a. die →IMSI verwaltet die mit der Telefonnummer des Geräts verknüpft ist. Die SIM wird vom Mobilfunkprovider bei Vertragsabschluss ausgegeben und die IMSI wird einer Telefonnummer zuordnet so dass sie eine sichere →Identifizierung und →Authentisierung der Karte (und damit des Geräts) ermöglicht. Die IMSI und zugehörige kryptographische →Schlüssel werden im →Chip der Karte (→Secure Element) gespeichert. Durch Austausch einer SIM-Karte wandert die Telefonnummer in ein anderes Handy. Vergleiche mit →IMEI. Eine SIM wird in der Regel über 1 oder 2 →PINs geschützt, denen wiederum PUKs zugeordnet sind. Siehe →Java Card, →IMSI, →USIM. 2013 werden →Angriffe bekannt, bei denen mittels →SMS →Schadsoftware in einer SIM-Karte installiert wird. SIM sind ein Beispiel für ein →secure element. 2014 wird bekannt, dass die →NSA Software hat, mit deren Hilfe sie die SIM-Karten manipulieren kann, so dass sie an die Daten der Nutzer kommen (→GOPHERSET, →MONKEYCALENDER).

Neue Entwicklungen sind embedded SIM die aus einem Gerät nicht entfernt werden können (z.B. Apple SIM) und z.B. in →Autos für →eCall, Verkaufs-oder Fahrkartenautomaten oder für einige eReader eingesetzt werden. Ein anderes Konzept sind remote provisioning SIM, d.h. ein oder mehrere Mobilfunkanbieter können ihre Authentisierungsinformationen in der Karte ablegen. Das würde z.B. ermöglichen, dass →Tablets oder Autos in jedem Land einen lokalen Mobilfunkanbieter nutzen können.

Eine SIM unterstützt noch viele weitere Software-Elemente, z.B. einen S@T-Browser und Java-Programme, die in einer Java-VM ablaufen. Durch →SMS kann der Mobilfunkprovider (oder →Angreifer) Aktionen im Handy triggern. Deutschland, Österreich und die Schweiz sollen von diesem Simjacker Angriff nicht betroffen sein

2) (Security Information Management) Sammeln, Auswerten, Korrelieren und Analysieren von Sicherheitsinformationen und Events, zumeist gesammelt aus →Logfiles,→IPS, →IDS, aber auch in Bezug auf →Zugriffe, →IAM Systeme, →Audit trails, →Vulnerability Mgmt., →Change Mgmt., Verbrauch von System Resourcen (→Capacity Mgmt.). Ziel kann eine Verbesserung bei →Compliance Anforderungen sein, z.B. →PCI-DSS, →HIPAA oder im Rahmen von →DLP

SIM Application Toolkit: (STK) →API das einer Anwendung auf einer →SIM-Karte ermöglicht, Dienste der Handy-Software oder das Mobilfunknetz anzusprechen. STK ist auf in den meisten SIM-Karten installiert. In Kenia baut das mobile Zahlungssystem →M-PESA auf dem SIM Toolkit auf

Simple Certificate Enrollment Protocol: (SCEP) Methode zum großflächigen Ausrollen von →digitalen →Zertifikaten auf eine große Zahl von Geräten, z.B →Smartphones. Dies sollte daher in →MDM Software unterstützt werden um automatisiert alle Geräte die z.B. auf das Firmen-E-Mail zugreifen wollen, an Hand dieser Zertifikate automatisch zu →authentisieren

Simple Object Access Protocol: →SOAP

SIM-Swapping: →Angriff gegen Sicherheitssysteme, z.B. →2FA, bei denen →SMS die an ein →Handy gesendet werden, indem über →Social Engineering eine neue SIM-Karte für die Telefonnummer des Opfers beantragt wird. Danach gehen alle SMS für das Opfer an den Angreifer, z.B. →mTANs

SINA-Box: (sichere Inter-Netzwerk-Architektur) entwickelt vom →BSI zur Verarbeitung von sensiblen →Daten in unsicheren →Netzen. Sie dienen bei Behörden in D. der sicheren →Datenübertragung mittels →VPN, auch für Daten, die beim →Abhören entstehen. Sie müssen für diesen Zweck bei jedem →ISP mit über 10000 →E-Mail Konten installiert sein

Single Point of Failure: Ressource, deren Ausfall zum Gesamtausfall führt. Siehe →Common Mode Failure, →Choke Point, →Hochverfügbarkeit

Single Sign-On: (SSO) →Authentisierungsverfahren, bei dem ein →Benutzer →Zugriff auf mehrere Computersysteme oder Applikationen bekommt ohne sich jeweils neu anzumelden. Diese erhöht die →Benutzerfreundlichkeit deutlich, erleichtert den Verwaltungsaufwand und vermeidet eine große Zahl an →Passworten. Hauptverfahren sind die Speicherung der jeweiligen →Credentials im Benutzer-PC oder zentrale Authentisierung mittels Software-→Token wie bei →Kerberos,

→SAML, →AD FS

Single-page Application: spezielle Form einer →Webseite bei der mittels →Javascript-Aufrufen alle Inhalte dynamisch auf Grund von Benutzerinteraktionen nachgeladen werden. Dies führt zu einer Interaktion mit dem Nutzer Dies ermöglicht Interaktionen die ähnlich zu konventionellen PC-→Programmen z.B.Text-Editieren oder →Smartphone →Apps ist. Wird oft bei modernem e-Banking genutzt. Bei der Implementierung werden →Protokolle wie →REST oder →SOAP genutzt, für die vielfältige fertige Javascript Bibliotheken wie z.B. →angularJS und →jQuery angeboten werden

Single-page Webseite: →single-page application

Singularity: siehe →intelligence explosion

Sinkholing: Trick um ein →Peer-to-peer →Botnetz zu deaktivieren. Dabei wird die Liste von anderen infizierten Systemen die jeder Teilnehmer am Botnetz vorhält nach und nach durch →IP-Adressen ersetzt, die von durch diejenigen kontrolliert werden, die das Netz lahmlegen wollen (optimalerweise die Sicherheitsprofis, möglicherweise auch die „Konkurrenz“)

Sinowal: (alias Torpig) Banken→Trojaner, der für eine große Zahl von kompromittierten Bankkonten und →Kreditkarten verantwortlich gemacht wird. Er wird aktiv, wenn ein Nutzer eine von 2700 Banken→websites aufruft und fragt dann innerhalb dieser Webseite →Daten ab. Er zeichnet sich dadurch aus, dass er kaum entdeckt wird (er schreibt sich in den →MBR) und seit 3 Jahren (Stand 2008) sehr erfolgreich aktiv ist. Siehe →Fast Flux

SIP: (Session Initiation Protocol) häufig verwendet für den Aufbau von →VoIP-Sitzungen (→Signalling), nicht nutzbar hinter →NAT-→Firewalls. Für die Datenübertragung wird dann →SDP oder →RTF verwendet. Siehe →H.323, →SS7

Siri: Service unter →iOS der Benutzern auf Grund von gesammelten →Daten persönliche Ratschläge für ihr Verhalten gibt (→personal assistant), Fragen beantwortet und einfache Aufgaben erledigt. Wird meist über Sprachsteuerung genutzt. Zur Problematik siehe →Contextual Computing

SIS: (Schengen Information System) seit 1995 aktive →Datenbank der EU-Staaten, die ab 2004 auf SIS II erweitert wird und Hinweise auf gesuchte Personen und Gegenstände oder vormals in der EU abgewiese Personen enthält.
http://www.statewatch.org/news/2005/may/sisII-analysis-may05.pdf

Situational Crime Prevention: (SCP) das Implementieren von Technologie dergestalt, dass unerwünschtes Verhalten technisch verhindert wird, Beispiel ist →DRM. Solche Lösungen werden heute immer öfter implementiert, speziell auch bei Software-Lösungen (ist aber auch in Hardware möglich, z.B. Zugangssschranken die „schwarz-fahren“ sicher verhindern). SCP wird heute oft als „große Lösung“ gesehen da es (vermutlich) viel unerwünschtes Verhalten verhindert, wirft aber anderseits auch Probleme auf, z.B. wer definiert was unerwünscht ist? Zum anderen spricht viel dafür, dass wenn Bürger nicht hin und wieder ethisch-moralische Entscheidungen treffen müssen, diese Fähigkeit verkümmert. Relevant wird dies z.B. bei →autonomen Fahrzeugen, die so programmiert sein könnten, dass Geschwindigkeitsübertretungen u.ä. gar nicht möglich sind

Six Sigma: (6σ) Begriff aus dem →Qualitätsmanagement, basierend auf statistischen Arbeiten von Joseph Juran. Sigma bezeichnet die Abweichung vom Zustand der Perfektion. Sechs Sigma bedeutet 3,4 Defekte in 1 Million. Durch Messung der Defekte wird ein systematisches Reduzieren und Eliminieren möglich. Siehe →TQM, →FMEA

skalierbar: (engl. scalable) bei dem Thema →Verfügbarkeit die Möglichkeit, das System für höhere Anforderungen leicht zu erweitern. Bei →Angriffen auf Systeme oder Rechner die Möglichkeit des gleichzeitigen Angriffs auf viele Systeme, z.B. beim →Phishing. Ein Angriff der nicht skaliert ist z.B. →Abhören über →IMSI-Catcher, dies geht nur für →targeted attacks

Skimming: Abfangen der Daten auf dem Magnetstreifen der →Bankomatkarten (der sog. →Track 2) durch ein geeignetes Lesegerät das von den Betrügern im oder am →Bankomaten eingebaut wird plus Ausspähen der →PIN-Eingabe entweder über gefälschte Tastatur oder optisch. Deswegen in Europa nur noch Nutzung des →EMV-Protokoll auf der Basis einer →Chipkarte. Betrüger weichen daher für die Nutzung der gewonnenen →Daten auf andere Regionen aus, in denen nur Magnetstreifen genutzt werden. Um dies zu verhindern wurde 2015 →Geoblocking eingeführt, d.h. die Karten sind für alle nicht-europäischen Länder gesperrt und müssen vor einem Urlaub durch den Kunden freigeschaltet werden

Skype: unentgeltliche →VoIP-Software von →Microsoft die Telefonieren und Videochat zwischen Rechnern, aber auch mit Festnetzgeräten erlaubt. Wurde 2020 auch als →Webkonferenzsystem eingesetzt. Sicherheitsrelevant, da kein →Quellcode verfügbar ist, nicht ganz klar ist, welche möglicherweise unerwünschte Zusatzfunktionalität enthalten ist und weil das →P2P-Konzept eine Kontrolle z.B. in Hinblick auf verborgene Kommunikation erschwert. Verwendet nicht das →SIP-Protokoll und funktioniert auch hinter →NAT-→Firewalls (→UDP hole punching). Es wird eine

→Verschlüsselung eingesetzt, die Polizei klagt über Probleme bei der →Überwachung da es keinen zentralen Server gibt, bei dem Sprach- und Video-Kommunikation zentral abgehört werden könnte. Daher muss eigentlich eine solche Überwachung am Endgerät selbst stattfinden und erfordert so etwas wie den →Bundestrojaner. Es gibt jedoch Versionen, z.B. für China, bei denen Teile der Chat-Daten an zentrale Server geliefert werden. 2014 wurde bekannt, dass auf Wunsch der →NSA eine →Backdoor eingebaut wurde, deren genaue Funktionalität noch nicht bekannt ist. Anderseits liegen wie bei fast allen dieser Systeme auch bei Nutzung von →Verschlüsselung für die Datenübertragung trotzdem am zentralen →Server zumindest die Verbindungsdaten, meist aber auch die vollständigen Daten vor (Ausnahme z.B. →Messaging Dienst →Signal)

Sog. →Skype Resolver liefern zu jedem Skype-Benutzernamen die →IP-Adresse. Solche Dienste werden gemeinsam mit →Denial of Service Diensten angeboten, d.h. sie bieten an, den Skype-Zugang einer Person oder einer Firma zu stören. Die IP-Adresse lässt sich mittels →Geolocation auch zu einem Ort zurückverfolgen. Siehe auch →Neural Network

Skype Resolver: →Skype

SL: (→Second Life)

SLA: (Service Level Agreement) Vertrag zwischen einem →Information Owner (Fachabteilung) und einem →Informationstreuhänder (Information Custodian, IT-Dienstleister), die sich zu bestimmten Services und →Qualitäten verpflichten, Teil des →IITL-Konzepts. Siehe auch http://sicherheitskultur.at/SLA_Checklist.htm

SLAAC: (Stateless address autoconfiguration) automatisierte Adressevergabe bei →IPv6, implementiert über →ICMPv6; im Gegensatz zu →DHCPv6 = stateful

Slack:

1. als File Slack der nicht für die Datenspeicherung verwendete Teil eines →Clusters auf einer →Magnetplatte
2. →Messaging →Software für Team-Communication, analog zu →Teams von →Microsoft

Slacktivism: Schlagwort zum Thema politische Aktivierung durch das →Internet. Untersuchungen zeigen, dass starke Unterstützung einer Aktion auf →Social Networking Websites wie →Facebook sehr oft geringe Aktivitäten im „richtigen Leben“ bedeuten. Die Nutzung des →Like-Buttons kann dazu führen, dass ein mögliches schlechtes Gewissen wegen Inaktivität zu politischen Fragestellungen. Ein Beispiel ist →Bank run 2010

SLAX: modulare Software für →Penetrationstest auf →Linux-Basis. Weiterentwicklungen: →BackTrack, TeaM-TL, SLAMP, Wolvix, Planktum

Small world network: →6-degree of freedom

S.M.A.R.T.: (Self-Monitoring, Analysis, and Reporting Technology) Technologie zur automatisierten Überwachung von →Magnetplatten

Smart: siehe →Smart Devices

Smartcard: standardisierte Plastikkarten (ISO/IEC 7816, ISO/IEC 7810-kontaktbehaftet, ISO/IEC 14443-kontaktlos, →NFC) die entweder nur über →Speicher oder über einen Prozessorchip verfügen. Damit können Daten direkt auf der Karte verarbeitet, z.B. verschlüsselt werden. Erfunden 1982 durch Bull in Frankreich. Smartcards werden u.a. als →Signaturkarten für →Authentisierungszwecke und bei →PKI-Projekten, sowie zur verschlüsselten Aufbewahrung digitaler →Schlüssel eingesetzt. Angriffe auf Smartcards können auch →Side Channel Angriffe sein. Siehe →Bürgerkarte, →e-Card, →eGK →EMV, →Geldkarte, →Quick, →edu-card, →HSM, →COS

Smart Contract: Computerprotokolle, die Verträge abbilden und sogar deren Einhaltung verifzieren können. Die Idee ist, dass solche Verträge eine erhebliche Automatisierung ermöglichen könnten und dadurch die sog. Transaktionskosten von Verträgen (und damit des Handels) drastisch senken, z.B. elektronische Zahlungen unter bestimmten Bedingungen auszulösen. Ein Projekt der Implementierung ist →Ethereum, als bereits bestehende Beispiele werden →DRM und →Crypto currencies genannt. Siehe auch →Legal Technology

Smart Devices: Geräte, z.B. Haushaltsgeräte (→IoT) oder persönliche Geräte wie Uhren oder Sensoren, die über eine →Vernetzung verfügen und dadurch von der Ferne (z.B. über →Smartphone) gesteuert werden können. Dazu gehören auch →Smart TV, →Smart Trainer, Smart →Doorbells und →Smart Speaker. Stellen auf Grund von →Verwundbarkeiten sehr oft Bedrohungen für die →Sicherheit und/oder →Privatsphäre dar

Smart Grid: Konzept einer weiteren Automatisierung der Stromnetze bei dem auch →Daten von Verbrauchern (siehe →Smart Meter) bei der Steuerung der Netze berücksichtigt werden. Dies wird vor allem notwendig, da immer mehr Stromerzeugung dezentral geschieht, z.B. durch privat aufgestellte Sonnenkollektoren oder Windräder. Dadurch ist die Steuerung des Stromflusses deutlich komplexer geworden und es kann, speziell auf Grund der schlechten Vorhersagbarkeit vieler Quellen für umweltfreundlichen Strom leicht zu Instabilitäten im Netz und dadurch maximal zu einem →Blackout kommen

Smart Home: →Home Automation

Smart Meter: Umstrittenes Konzept von digitalen Stromzählern die angeblich helfen, den Stromverbrauch zu reduzieren in dem sie den Verbrauch der Haushalte sofort anzeigen und auch an die Netzbetreiber und Elektrizitätsversorger zurückliefern. Dies soll Tarife ermöglichen bei denen lastabhängig unterschiedliche Tarife berechnet werden, z.B. billiger Strom wenn ein großes Angebot vorliegt. Diese Rückmeldung des Stromverbrauchs ermöglicht jedoch auch viele Einblicke in die Haushalte und verletzt damit die →Privatsphäre. Anderseits enthalten diese Zähler fast immer Mechanismen für den Umgang mit säumigen Zahlern, z.B. Abstellen des Stroms aus der Ferne oder Begrenzung der abrufbaren Leistung. Smart Meter sind Teil des →Smart Grids. Durch Manipulation dieser Netze bieten sich zahlreiche neue →Angriffe. Smart meter sind 1 Aspekt von →M2M. Siehe auch →AMR, →IoT, →CPS

Smartphone: →Handy mit erweiterten Funktionalitäten. Zu Beginn waren dies nur Funktionen eines →PDAs, d.h. →E-Mail, Kontakte, Notizen, Kalender, Web-Surfing und Synchronisieren mit Desktop-Rechnern. Geprägt wurde der Begriff bereits 2000 durch Firma Ericsson. Ab ca. 2007 (→iPhone) wurden aber nahezu alle Funktionalitäten eines herkömmlichen →Rechners wie unter →Windows oder →MacOS angeboten. Diese Funktionalitäten machen die Geräte auch anfällig gegenüber →Angriffen. Diese finden über →E-Mail oder →Social Networking Nachrichten statt, aber auch über →SMS, →WLAN, →MMS oder (seltener) →Bluetooth und erfordern zumeist (noch) die Mithilfe des Benutzers (mittels →Social Engineering). Verwendete Betriebssysteme bei Smartphone sind →iOS, →Android, Windows Mobile - heute ersetzt durch →Windows Phone 7 (8), →Blackberry, →WinCE, →Palm OS und →Symbian OS (die letzten 4 stark abnehmend, bzw. 2015 kaum noch im Einsatz).Smartphones mit →Tabletts. Geräte mit (und auch ohne) →A-GPS ausgestattet können mittels entsprechender Anwendungen (wie alle Handys) zu vielfältigen Verletzungen der →Privatsphäre führen.

Wenn Smartphones Firmendaten enthalten sollten sie über →Mobile Device Management verwaltet werden. Die modernen Versionen dieser Geräte sind vom Konzept her im Vergleich zum →PC oder →MacOS-Gerät vergleichsweise sicher, hervorzuheben sind →Sandbox-Konzept für die →Apps und weit verbreitete Speicher→-Verschlüsselung.

Größte Sicherheitsschwäche ist, dass diese Geräte immer in Verbindung mit →Cloud-Diensten genutzt werden und dass diese notorisch unsicher sind. Verschlüsselung der auf den →Servern im →Internet gespeicherten Daten ist extreme selten. Maximal wird die Datenübertragung über →HTTPS abgesichert. Außerdem werden diese Geräte unsicher weil eine sehr große Zahl von Apps installiert wird, die zwar in einer Sandbox laufen, aber →Zugriff auf fast alle Gerätefunktionen haben, wie z.B. →Kontakte, →E-Mails, →SMS, →GPS und darüber nicht nur →Privatsphäre-Verletzungen auslösen, sondern auch finanzielle Schäden anrichten können.

Ebenfalls problematisch ist, dass unklar ist, welche Komponenten in einem Gerät, das ausgeschaltet ist, immer noch aktiv ist. Gerüchte besagen, dass die →NSA auch abgeschaltete Geräte orten kann. Sicher ist, dass nur ein Entfernen der Batterie wirklich sicherstellen kann, dass das Gerät „tot“ ist. Dies ist bei einem →iPhone aber nicht möglich, daher hat →Edward Snowden die Smartphones während vertraulicher Sitzungen in den Kühlschrank getan.

Siehe auch →GeoLocation, →Markets, →Kill Switch, →Contextual Computing

Smart Speaker: →Virtual Assistants die als Hardware verfügbar sind und nicht nur auf →Smartphone. Zu ihrer Problematik mehr unter Virtual Assistant und →Smart TV. Siehe auch →Amazon Echo. Das BSI macht Vorschläge für eine sichere Konfiguration: https://www.youtube.com/watch?v=oRA18JUyXGc

Smart Trainer: Trainingsgerät das an das →Internet angebunden ist und mittels Datenaustausch mit zentralen Plattformen Funktionalitäten bietet, die lokal nicht zur erbringen sind. Siehe z.B. →Zwift

Smart TV: Moderne Fernseher, die typischerweise mit dem →Internet vernetzt sind und über Sprachsteuerung gesteuert werden können. Die Sprachsteuerung muss IMMER auf die Sprache im Zimmer hören und stellt dadurch eine potentielle Verletzung von →Privatsphäre dar. Da die Geräte üblicherweise auch für →Streaming-Dienste Wie →Netflix eingesetzt werden sollen haben sie uneingeschränkten →Zugang zum Internet und senden meist auch Nutzungsdaten ihrer Besitzer, die auch sensibel sein können

SMB:

1) (Server Message Block) Zugriffsprotokoll auf →Shares in Windows-Netzen (ursprünglich von IBM entwickelt). Wurde auf Windows Systemen früher über →NetBIOS genutzt, heute über →TCP/IP. Heute zu →CIFS weiterentwickelt. SMB 3.0 kann auch verschlüsselte Verbindungen nutzen. Siehe →Samba

2) (Small and Medium-sized Businesses) →KMU

SME: (Small and Medium-sized Enterprises) →KMU

S/MIME: →Secure Multipurpose Mail Extension

SMiShing: in Anlehung an →Phishing, →SMS

mit betrügerischer Absicht, oft mit Link zu →Website mit →Malware, Spezialform des →Social Engineering

SML: (Service Modeling Language) auf →XML basierender Standard für maschinell lesbare (IT)-Systembeschreibungen für die Nutzung in System-Management-Werkzeugen, z.B. →SCOM. Vormals →SDM

SMM: (security maturity model) vom Frauenhofer-Institut entwickeltes Modell, das den Reifegrad eines Unternehmens in Bezug auf →Informationssicherheit angibt. Stufe 0: Vertrauen in den jeweiligen Hersteller, Stufe 1: kurzfristige Lösungen, keine Strategie, reaktiv, Stufe 2: Sicherheitspolitik, Stufe 3: Sicherheitsprozesse durchgehend im Unternehmen verankert. →ISO/IEC 21827 http://www.isst.fraunhofer.de/englisch/download/32195_sec-model-pb-engl.pdf

SMS:

1) (**Short Message Service**) (engl. text) Verfahren, bei dem mittels →Handy Textnachrichten bis 160 Zeichen versendet werden. Kann auch zum Versenden von →OTPs im →e-Banking eingesetzt werden und als „2. Kanal" („out-of-band") eine bessere Sicherheit bieten (→mTAN). Diese Sicherheit geht jedoch verloren seit →Smartphones für e-Banking eingesetzt werden und dadurch die →Infektionen eines Gerätes sowohl den Datenverkehr wie auch den 2.Kanal des SMS beeinflussen kann.

Kann für Betrugsversuche genutzt werden →SmiShing, 2008 wird auch →Spam durch die Nutzung von SMS-Gateways zu einem Problem. In der Form von →Premium SMS auch für kriminelle Aktivitäten wie →Ransomware eingesetzt. Siehe auch →Twitter, →Sexting, →Mehrwertnummern.

Wird von der →NSA großflächig abgefangen und ausgewertet (→DISHFIRE program). Interessant sind vor allem SMS wie „entgangene Anrufe", „roaming Hinweise", Benachrichtigungen über Kreditkartenrechnungen und andere Banknachrichtungen, z.B. Zahlungen und auch die →mTAN SMS die Hinweise auf Zahlungen und damit Vernetzungen bieten

2) (**Systems Management Server**) kostenpflichtiges Software Management und Software-Verteilungsprogramm für Windows Systeme. Kann in neueren Versionen auch für die Verteilung von →Patches und Virenschutz-Updates verwendet werden. Abgelöst durch →SCCM. Siehe auch →WSUS

SMS-Flood: Form des →Denial of Service →Angriffs bei dem an ein →Handy eine so große Zahl von →SMS gesendet werden, dass die legitimen SMS darin untergehen. Solche Angriffe sind kommerziell günstig zu haben: 1000 SMS für 15 $

SMS-TAN: →mTAN

SMTP: (Simple Mail Transfer Protocol) Übertragungsprotokoll für →E-Mails zwischen E-Mail Servern im →Internet. Wird auch von E-Mail Clients für das Senden von E-Mails verwendet. Für den Abruf von E-Mails aus →Mailboxen verwenden die E-Mail Clients hingegen →POP oder →IMAP. Sicherheitsrelevant ist SMTP, erstens auf Grund von →Schwachstellen (d.h. Programmierfehlern) in der Implementierung, zweitens durch fehlende →Verschlüsselung und →Authentifizierung des Senders und drittens durch die Tatsache, dass es für den Austausch von →Malicious Code über E-Mail genutzt wird. Daher wird der SMTP-Verkehr heute oft durch →Content Scanning bzgl. →Malicious Code überwacht. Verschlüsselung von Server zu Server kann sehr leicht durch aktivieren der →TLS Feature erreicht werden. →ESMTP ist eine Erweiterung, die u.a. auch →Verschlüsselung unterstützt. SMTP wird oft durch das →Public Domain Produkt →Sendmail implementiert

Snapchat: →Messaging App, die speziell für den Austausch von Bildern gedacht ist und bei denen sich die Bilder nach wenigen Sekunden automatisch löschen. Sehr beliebt, da es (mehr oder weniger) sicherstellt, dass diese Fotos nicht weitergeleitet werden. Wenn der Empfänger einen Screenshot macht, so wird der Sender darüber informiert. Wird für →Sexting verwendet. 2014 lehnen die Gründer einer Übernahme durch →Facebook ab. Problematisch an Snapchat ist, dass zwar ein Schutz gegen →Privatsphäre-Verletzung durch den Empfänger besteht, aber die meisten Nutzer nicht realisieren, dass der Betreiber natürlich sehr wohl die Möglichkeit hat/hätte, die Daten oder Bilder zu analysieren und/oder zu speichern, bzw. dass Regierungsbehörden die Betreiber dazu zwingen können

Snapshot: ältere Kopie eines aktuellen Datenbestandes, z.B. einer →Magnetplatte, verwendet für →Datensicherung oder schnelle →Wiederherstellung. Siehe →Volume Shadow Copy. Bei der →Betriebssystem→Virtualisierung die Möglichkeit eines →Hauptspeicherabzugs des laufenden Betriebssystems auf →Magnetplatte für →Forensic oder schnelle Wiederherstellung

Sniffer: ('Schnüffler') Programme, die an der Netzwerkkarte sitzen und alle Datenpakete auswerten. Sie sind für Netzwerkadministratoren wichtig. Manchmal werden sie aber auch von →Hackern eingesetzt, weil die Sniffer auch unverschlüsselt übertragene Passwörter darstellen können. (→Protocol Analyzer)

SNMP: (Simple Network Management Protocol) Technologie zum Austausch von Zustandsinformationen in komplexen →Netzwerken. Auf diese Weise können Geräte und Systeme ihren Zustand an Netzwerk Management Systeme kommunizieren. Die Geräte (agents) speichern dafür die Zustandsinformationen in einer MIB (Management Infor-

mation Base) und können sie auf Anfrage abgeben. Diese Technologie ist sicherheitsrelevant, da sie Verfügbarkeitsüberwachungen ermöglicht. Siehe →Monitoring

Snooping: unerlaubtes „Mithören“ von Daten in Datennetzen. →Abhören

Snort: →Open Source Variante eines →Intrusion Prevention Systems. Überwacht den →Datenverkehr und vergleicht ihn mit Pattern von bekannten →Angriffen

Snowden: →Edward Snowden

SOA: (Service Oriented Architecture) Management- und Systemarchitektur-Konzept, das auf →Geschäftsprozessen und deren Abbildung in Services beruht. Kann über Web Services auf der Basis von Standards wie →SOAP, →WSDL und →UDDI eingesetzt, doch kann eine SOA prinzipiell auf jeder dienstbasierten Technologie wie zum Beispiel →CORBA, DCOM oder Enterprise Java Beans (EJB) implementiert werden. Sicherheitsrelevant, da sich auch über diese Schnittstellen Angriffe realisieren werden lassen. Siehe →ESB

SOAP: (Simple Object Access Protocol) auf →XML basierendes Verfahren, das erlaubt, strukturierte →Daten zwischen Anwendungen zu übertragen, z.B. auch zwischen →Browser und →Webserver (zur Implementierung einer →single-page application). Ein →W3C-Standard, wird z.B. auch für →ebXML eingesetzt. Sicherheit kann mittels →WSS implementiert werden

Social Adertising: Werbung bei der mittels der durch →Data Mining gewonnenen →Daten und den →Informationen des →Social Graphs Werbebotschaften mit dem Foto von →Friends des Betroffenen versehen werden, bzw. mit der Information, wie viele der Kontakte dies ebenfalls gekauft haben oder →“like“n. Auf diese Weise wird ein stärkerer Werbe-Effekt erreicht, da sich Menschen leicht über ihr Umfeld beeinflussen lassen. Diese Technik könnte unter Verwendung von →Social Bots auch zu →Social Engineering im ursprünglichen Sinne verwendet werden

Social Bot: Schlagwort für →Software mit deren Hilfe Angreifer versuchen in →Social Networks viele →Friends zu sammeln. Die Software beginnt mit →Friend-requests an Zufallspersonen und hat dabei eine Erfolgsquote von ca. 20%. Dann sendet sie Friend-request an friends-of-friends (→FOAF) und bekommt damit eine erheblich höhere Erfolgsquote. Wegen den mit dem Friend-Status verbundenen →Zugriffsrechten und dem Vertrauensstatus können diese →Bots dann →Malware verteilen oder private →Daten auslesen und verkaufen. Die Beziehungen könnten auch für →Social Advertising genutzt werden.

Seit ca. 2017 werden Social Bots auch im Rahmen von →Trollfabriken zur Beeinflussung von Meinungen und/oder Verhalten z.B. durch den Einsatz von automatisierter Software auf →Twitter oder →Facebook genutzt. http://www.webecologyproject.org/

Social Circle: Funktion in der Google →Suchmaschine bei der die Suchergebnisse auf Grund der Inhalte der →Social Networking →Profile seiner Kontakte optimiert werden. Microsoft hat eine ähnliche Funktion in seiner Suchmaschine Bing

Social Credit System: (SCS) In China eingeführtes System, das alle Bürger nach einheitlichen Kriterien bewerten will (→Scoring) um ein sozial angepasstes positives Verhalten zu erzwingen. Dabei werden die →Daten die bei den Behörden über die Bürger anfallen mit den →Tracking-Daten der Betreiber der großen Internetplatformen (vor allem →Alibaba und →Tencent) kombiniert. Diese Bewertung wird dann für viele Aspekte des realen Lebens verwendet, z.B. Jobsuche, Wohnungssuche, Zugang zu Verkehrsmitteln, Krediten, etc. Mittels →Gesichtserkennung und flächendeckenden Kameras werden dann Reiseverbote u.ä. konsequent und recht effektiv durchgesetzt.

Was ist der Unterschied zu der →Überwachung im Westen? In China hat der Staat auch →Zugriff auf die gesammelten →Daten. Dies war in den USA nur bis zu den Veröffentlichungen von →Edward Snowden der Fall. Bis dahin hat die →NSA z.B. die Datentransfer von →Google zwiwschen ihren →Datacentren systematisch mitgeschnitten und auch den meisten Datenverkehr zwischen →Web-Browsern und →Web-Servern. Nach der Veröffentlichung hat Google alle internen Datenströme verschlüsselt und auch die Webseiten dazu gezwungen, auf →HTTPS umzustellen. Stark geholfen hat bei Letzterem, dass mit →Let’s Encrypt eine kostenlose automatische Implementierung zur Verfügung steht. Natürlich gibt es weiterhin Bestrebungen von staatlichen Behören, Zugriff auf mehr Datenströme zu bekommen, z.B. durch sog. →Staatstrojaner oder →Bundestrojaner. Siehe https://sicherheitskultur.at/china_social_credit_score

Social Engineering: ursprünglich sozialpolitischer Begriff für die Idee, Menschen mit Ingenieursmethoden zu “formen” (siehe auch →Choice Architecture). Heute zumeist eine spezielle Form des →Angriffs, bei dem nicht die Software oder elektronische Systeme direkt angegriffen werden, sondern die sog. →„*Wetware*“, also der Mensch mit seinen Stärken und Schwächen. Der Angreifer versucht, vertrauliche →Informationen zu erlangen, indem er seine "Social Skills", also sozialen Fähigkeiten einsetzt (human-based social engineering). Diese Angriffe nutzen oft Neugier, Hilfsbereitschaft oder Respekt vor Autoritäten aus, z.B. über das Telefon, indem sich der Angreifer

als Kollege des Opfers ausgibt und versucht, an die gewünschten Informationen (z.B. Passwörter) zu kommen. Eine Unterform des Social Engineering ist „computer based social engineering“. Damit werden Angriffe bezeichnet, die den →Anwender zur Ausführung oder Download von →Malware verleitet. →Phishing fällt auch unter diese Form. Die Informationen in →Social Networks sind oft eine Grundlage für solche Angriffe. Siehe: Kevin Mitnick, The Art of Deception, →Open Source Research, http://sicherheitskultur.at/social_engineering

Social Graph: logisches Netzwerk zwischen Menschen die in irgendeiner Verbindung zueinander stehen, aber auch zwischen Menschen und Objekten. Die erste Variante entsteht, wenn Aktivitäten wie Telefonate oder →Chat →Kontakte oder Friend-Listen und die →Konnektivität des Netzes mathematisch ausgewertet werden. Ziel sind dabei nicht nur die direkt zugreifbaren →PII sondern auch die Struktur der Verbindungen zwischen den Personen. Der zweite Fall bezieht sich auf Beziehungen die Benutzer entweder aktiv kundtun (Like-Button, →Facebook →Open Graph) oder die bei einer Auswertung ihrer Aktivitäten im →Internet entstehen (→Tracking). Siehe →Social Networks, →Data Mining, →Metadaten, →Verbindungsdaten

Social Media: →Social Network, aber auch (kommerzielle) →Websites wie →amazon auf denen →Benutzer Produkte, Dienste, Filme, Musik, Spiele oder ähnliches kommentieren und diskutieren. Auch dazu gezählt werden →virtual worlds wie →Second Life und social games wie Farmville oder CityVille

Social Network: Dienst zur Kontaktaufnahme und/oder dem Austausch zwischen Personen (→Web 2.0) (z.B. →Facebook, →TikTok, Myspace (mittlerweile obsolet), →Xing, →LinkedIn, aber auch Dienste wie Flickr, →Youtube, Yelp und alle →Blogs bei denen Nutzer sich registrieren können und dann z.B. durch das Kommentieren von Äußerungen der anderen Nutzer mit diesen interagieren) und die damit dem Aufbau von Web-Communities dienen. Die meisten solcher →Plattformen werden kommerziell betrieben und optimieren die Verweildauer der Nutzer mittels →Algorithmen die stark emotionalisierende und radikalisierende Postings bevorzugen. Es gibt, z.B. im →Fediverse auch nicht-kommerziell betriebene Plattformen die diesen Vermarktungsdruck nicht haben.

Für den Nutzen solcher System gilt →Metcalfe’s Law, d.h. der Nutzen (und Wert) des Systems steigt mit dem Quadrat der Nutzerzahl. Dies führt dazu, dass es neue Anwendungen gegen zahlreich genutzte recht schwer haben.

Das Geschäftsmodell der kommerziell betriebenen Netzwerke beruht auf dem Verkauf von Werbung auf der Basis von Benutzerprofilen. Die von Benutzer-→Daten (→Profil) oder ihre Äußerungen berühren i.d.Regel Aspekte der →Privatsphäre.

Die expliziten Äußerungen der Nutzer (Postings) sind für Zielgruppen einsehbar (public, →friends, friends-of-friends {→FOAF}), die durch den Betreiber vordefiniert (und begrenzt durch den Benutzer steuerbar) sind. Da Friends zumeist nicht nur „reale“ Freunde sondern auch Arbeitskollegen, Familienmitglieder oder gänzlich unbekannte Personen (oder →Socialbots) sind (siehe →Friend-request) kommt es zu einem Effekt, der als →context collapse bezeichnet wird: unterschiedliche Zielgruppen wie Freunde, Kollegen und Familie bekommen dabei →Zugriff auf dieselben Informationen. Social Networks dienen auch als →Chat room. Wenn es sich um Auftritte von Firmen handelt („fan pages“) so sind viele der Einträge von den Unternehmen selbst beautragt, →meat puppet.

Die von den Nutzern erstellten Inhalte (Daten) stellen für die Betreiber einen großen Wert dar, da diese heute mittels →data mining sehr genau ausgewertet werden können um auf diese Weise →targeted advertising durchführen zu können. Die Geschäftsmodelle sehen entweder so aus, dass die Daten direkt verkauft werden, oder dass andere Unternehmen zielgruppen-orientierte Werbung im Social Network platzieren können.

Social Networks lösen spätestens seit 2011 in der Kommunikation der Jugendlichen →E-Mail stark ab.

Bedrohungen können entstehen, wenn Angreifer (die sich zum Teil als Friends einschleichen) mittels dieser Funktionen auf →Malware verlinken oder direkt einstellen, z.B. über →HTML- oder andere Inhalte (z.B. MP3). Auch →SPAM, →Phishing und →Malware werden über Social Networks verteilt. Eine weitere →Angriffsmöglichkeit sind Social Network →Apps, d.h. in diese Netzwerke eingebundene →Programme die mehr oder weniger vollen →Zugriff auf alle Profildaten der Benutzer haben.

Solche zentralen Anbieter von Social Networks werden auch als →walled garden bezeichnet. Mittlerweile gibt es auch alternative Implementierungen von verteilten Social Networks ohne zentrale Kontrolle, zB. auf →Fediverse oder →ActivityPub. Beispiele sind z.B. für ActivityPub →Mastodon, →Nextcloud (file hosting), →Peertube (video upload und streaming), →Friendica, →PixelFed (Photo sharing) und WriteFreely (→Blogging).

Justische Probleme können für die Nutzer entstehen, denn sie sind als →Medieninhaber für die von ihnen erstellten oder weiterverbreiteten Inhalte verantwortlich.

Siehe →Drive-by-Infektion, →RDF, →Open Social, →Contact Scraping, →Apps, →sock puppet, →Astroturfing, →Social Graph,

→COPPA, →FoMo, →Dunbar Number, →fake news, →fake accounts

http://philipps-welt.info/social networks.htm

http://www.webecologyproject.org/

Social Reading: automatisiertes Überwachen von Leseauswahl, Lesegeschwindigkeit und anderen Parametern zur Weitergabe („sharing“) in einem →Social Network, zur Bewertung des Bildungseifers im Fall von Online-Kursen oder einfach zu Marketingzwecken

Social Viewing: Wurde →2020 populär, erlaubt es, dass mehrere Zuschauer gleichzeitig einen Film sehen und parallel kommentieren können (als wären sie in 1 Raum). Kann bei Disney+, →Amazon Prime und bei →Netflix genutzt werden

Sock-puppeting: Nutzung einer falschen Online-Identität um sich selbst positiv zu kommentieren oder Werbung für sich und seine Firma zu machen. In jedem Fall unethisch, illegal wenn z.B. gegen Regeln der Börsenaufsicht oder andere Gesetze verstoßen wird

Sock puppet: (engl. Sockenpuppe) bei →Social Networks wenn jemand mehrere →Accounts anlegt (→Fake Account) und sich damit an Diskussionen beteiligt, damit es so aussieht, als gäbe es andere Personen die mit ihm/ihr übereinstimmen. Solche Dienste werden kommerziell angeboten. Dabei bedient ein Angestellter i.d.Regel 20 solcher falschen Identitäten gleichzeitig. Der Begriff wurde bereits 1993 in →Usenet geprägt. Ein anderer Begriff dafür ist →Astroturfing. Siehe →Meat puppet

SOCKS: Protokoll um →TCP Datenverkehr durch einen →Proxy Server zu schleusen. Socks Proxys zeichnen sich dadurch aus, dass sie viele →Protokolle weiterleiten können. Dabei können, ähnlich wie bei einem →Firewall, die →IP-Adressen verborgen werden

Socks bot: bei →Malware ein Software-Prozess im infizierten Rechner der als „driver“ Datenverkehr an der →Firewall vorbei transportieren kann

SoD: →segregation of duties

Softphone: →Programm, das die Nutzung von → VoIP-Diensten ermöglicht

Soft SIM: noch nicht implementiertes Konzept das ein →SIM-Karte im Betriebssystem simuliert und ohne →secure element arbeitet. Dies würde die SIM Informationen sehr leicht angreifbar machen

Software: →Programmcode, der in einem IT-Gerät (im weitesten Sinne, einschließlich →Embedded Systems in Gebrauchsgeräten) ausgeführt wird. Enthält als Untermenge →Betriebssystem und Anwendungsprogramme. Software ist i.d.R. komplex und daher fehlerbehaftet, was leider immer →Schwachstellen bedingt. Siehe →Software Test

Software-Agenten: Konzept von Programmen, die selbständig im Auftrag des Benutzers Aktionen durchführen. Dabei ist der rechtliche Status dieser Aktionen noch unklar. Siehe →bots

Software Configuration Management (SCM): →Quellcode-Verwaltung

Software-defined Networking: (SDN) Konzept bei dem die beiden logischen Ebenen eines →Routers („control plane“ für die Verwaltung der Routing Tables, Neighbor Tables, Link State Database) vom „data plane“ das die →Pakete weiterleitet) getrennt werden. Dabei wird das Control Plane in einen separaten Rechner ausgelagert, und kommuniziert mit dem Data Plane. Ein Beispiel für diese Kommunikation ist OpenFlow. Die Sicherheitsaspekte dieses Konzepts sind noch umstritten

Software-defined Radio: (SDR) Hardware und Software mit deren Hilfe sehr unterschiedliche drahtlose Techniken implementiert werden können. Dabei wird z.B. Software wie →GNU Radio und Hardware wie →DSP eingesetzt. Eine Implementierung ist →USRP.

Mit Hilfe von von Software-defined Radio verwischt sich die Unterscheidung zwischen Sender und Empfänger. Die gleiche Hardware, z.B. im →Smartphone, kann durch entsprechende Änderung in der →Software oder →Firmware zum Empfangen oder Senden verwendet werden und zwar auf einem nur von der Geometrie der Antenne angeschränkten relativ großem Frequenzbereich.

Software-defined Radio wird oft zur Demonstration von →Verwundbarkeiten bei drahtlosen Übertragungen jeglicher Art verwendet, z.B. →RFID, →LTE, usw. Könnte aber natürlich auch für →Angriffe, d.h. →Abhören oder Stören (→DoS) verwendet werden. Siehe ADS-B

Softwareentwicklung: Erstellen von →Programmen für →Computer. Mangelnde →Qualität und Programmierdisziplin führen dazu, dass viele →Schwachstellen in den Programmen zu Angriffsmöglichkeiten für →Schadsoftware führen. Siehe →CMM, →SPICE, →V-Modell, →RUP

Software Test: →Qualität von Software kann nur durch systematische und strukturierte Tests gesichert werden. Tools dafür z.B. Eclipse TPTP, Mercury QuickTest, Rational Functional Tester, Compuware TestPartner. Siehe →Capture&Replay

Software-Verteilung: automatisiertes Installieren von Software (Betriebssystemkomponenten oder Anwendungen) oder →Patches auf einer großen Zahl von Rechnern. Bei der sog. Paketierung werden die Installationsmaterialien des Softwareherstellers in ein geeignetes Format für das jeweilige Verteilungstool umge-

wandelt. Siehe →MSI, →SMS

Solarwinds: in 2020 kam es zu einem der umfangreichsten →Data breaches in US-Behörden. In die IT-Security- und Netzwerk-Software Orion des US-Anbieters Solarwinds war mindestens 1 →Backdoor eingebaut worden. Dies öffnete dann die Netze von über 250 US-Behörden die Orion einsetzen für die ausländischen Angreifer (plus einige andere, z.B. →Microsoft). Peinlich für die US-Behörden ist weiterhin, dass dieser Angriff erst durch die Sicherheitsfirma FireEye und nicht durch die zuständigen US-Behörden entdeckt wurde (z.B. Cyber Command des Militärs, der National Security Agency (NSA) oder dem Department of Homeland Security)

Solid state disk: (SSD) heute oft eingesetzte Alternative zu →Magnetplatten, die einen schnelleren →Zugriff zu →Daten liefert und weniger Strom verbraucht. Wird vor allem in →Laptops eingesetzt, aber auch zur Beschleunigung des →Betriebssystems von →Desktops. Aus Sicherheitssicht gilt für alle diese Speicher, dass ein wirklich permanentes Löschen deutlich schwieriger ist als bei Magnetplatten, Details unter →Flash-Speicher

Sony: Unterhaltungs- und Elektronic Konzern mit einer sehr gemischten Geschichte zu Informationssicherheit. 2005 kam heraus, dass seit einiger Zeit über Sony Musik-CDs →rootkits auf Rechnern installiert werden, die Sony-CDs abspielen, die ein Weiterkopieren verhindern sollen. Nach der Entdeckung wurde eine angebliche Lösch-Software veröffentlicht, die weitere Software installiert. Später wurde auf solchen CDs eine andere Form von →Kopierschutz eingesetzt, pikanterweise unter Verletzung des →Copyrights von →Open Source Projekten.

Positiv ist zu vermerken, dass Playstation 3 zu Beginn mit der Möglichkeit kam, andere →Betriebssysteme darauf zu nutzen, dies wurde jedoch 2010 durch →Firmware-Upgrade gesperrt. Ein →Hacker/→Hacktivist wurde juristisch verfolgt (eine außergerichtliche Einigung wurde erreicht).

2011 muss Sony verkünden, dass aus dem PSN (Playstation Network) 77 Mio. Kundendaten gestohlen wurden und von SOE (Sony Online Entertainment) 24 Mio. Von Sony Pictures wurden 1 Mio Benutzerdaten und →Passworte kopiert, ebenso 3,5 Mio Gutscheincodes. →LULZSEC bekennt sich dazu.

Ende 2014 drangen Hacker bei Sony Pictures ein, stahlen alle Daten und löschten dann die Computer-Platten vollständig. Die Wiederherstellung des Betriebs wird auf ca. 10 Wochen geschätzt. Die →Attribution des →Angriffs ist umstritten, die US-Behörden beschuldigen Nordkorea (die wegen eines satirischen Films sauer auf Sony Pictures waren). Kurz danach fiel die →Internet-Anbindung von Nordkorea für einige Tage aus. Ein wirklicher Nachweis der Täterschaft ist aber sehr schwierig und die Anschludigungen sind umstritten

SOP: 1) (Standard Operating Procedure, ursprünglich aus dem Militär) schriftlich definierte Regeln für den Betrieb der IT. Wichtig, wenn es darum geht, →Qualität und Sicherheit zu gewährleisten

2) →Same Origin Policy

SOPA: (Stop Online Piracy Act) Versuch eines US-Gesetzes das strengeres Vorgehen gegen →Raubkopien erreichen sollte. Wurde nach weltweiten Protesten zurückgezogen. Die Inhalte sind jedoch weitgehend bereits in →PRO-IP Act, →ACTA, →DMCA die z.B. ausreichten um gegen Megaupload vorzugehen

Source code: →Quellcode

Source Code Management: →Quellcode-Verwaltung

Sousveillance: Kunstwort, das die Überwachung nicht durch den Staat (→Surveillance), sondern durch die Mitbürger bezeichnet

Sovereign Keys: 2012 Vorschlag für eine bessere Absicherung von →Websites als dies derzeit über →SSL möglich ist. Die Absicherung der →Webbrowser beruht darauf, dass diese die →Zertifikate der →Websites überprüfen. 2011 ist es jedoch zu zahlreichen Sicherheitsverletzungen bei →Certificate Authorities gekommen. Wenn ein Browser Verdacht auf eine Fälschung hat, so wird eine Warnung angezeigt, die jedoch sehr oft ignoriert wird. Das neue Verfahren verifiziert Websites über Erweiterungen im →DNSSEC Protokoll

SOX: →Sarbanes-Oxley Act

Spam: ursprünglich unerwünschte Zusendung von Werbung mittels Massen-→E-Mails, oft mit gefälschtem Absender (→Spoofing). Heute werden für Spam auch →Blogs und →Social Networks verwendet. Dies wird auch als →Spamvertising bezeichnet. Dafür muss der Spammer →Zugang zu →Accounts von registrierten Personen haben oder neue Accounts anlegen, z.B. in →Wikis. Accounts stehen auch zum Kauf, sortiert nach Thema: Dating, Jobsuche, oder andere.

E-Mail-Spam kann direkt über den Verbrauch von Bandbreite, oder indirekt, z.B. über Sperrung des gefälschten Absenders für diesen zu einem Sicherheitsproblem werden. Der Schutz geschieht über Ausfiltern der E-Mails, entweder über Listen von Versendern oder über den Inhalt der Mails. Der Name bezieht sich auf eine Szene von „Monty Pyton“ und ist englisches Kunstwort, das sich aus den

Anfangsbuchstaben der Wörter „spices, pork and ham“ ableitet.

Woher bekommen die Spammer Ihre Adresse?

- Ernte von →Websites (postings, etc.), →Spambot
- Ernte von korrumpierten Websites (Registrierungs-E-Mail-Adressen)
- →Dictionary Attack gegen große →ISPs oder →Free-mailer
- korrumpierte Privatrechner (→Würmer, →Spyware, →Trojaner, →Hackerangriff), deren →Adressbuch ausgelesen wird
- Verkauf durch Firmen, die die Adresse legitim erfahren haben (z.B. Registrierungen, Mailing Lists oder Shopping im Internet, Kunde hat vergessen, das Häkchen von "meine Adresse darf an Partnerfirmen weitergegeben werden" zu entfernen)
- Kauf aus der Konkursmasse von →E-Commerce-Firmen, in diesem Augenblick gelten die Privacy Regeln der Originalfirma nicht mehr, der Konkursverwalter macht alles zu Geld

2009 und 2010 oft in Form von →Stock-Pump-and-Dump-Spam. Messungen zeigen für Werbe-Spam nur Erfolgsraten von 0,00001%, die durch massenhaften Versand ausgeglichen werden. Zum Schutz siehe auch →SIPF, Sender Policy Framework (→SPF), →Sender ID, DomainKeys Identified Mail (→DKIM), →Blacklist, →Whitelist, →Greylist, →SURBL. Ab 2010 word Spam auch immer öfter in →Social Networks und →Blogs eingestellt. Dies soll durch Verfahren wie →CAPTCHAs verhindert werden, darum wird dann zum Teil Handarbeit wie der →Mechanical Turk eingesetzt. Siehe auch →Crowdturfing http://sicherheitskultur.at/spam.htm

SPAM: (Switched Port Analyzer) Funktionalität von Cisco-→Switches um →Protocoll Analyzer zu unterstützen (RSPAN=Remote SPAN)

Spambot: automatisierte →Programme die →Websites nach →E-Mail-Adressen durchsuchen oder falsche →Webmailer-→Accounts anlegen um dann Spam-Mails zu versenden

Spanning tree protocol: →STP

Spamvertising: Kunstwort aus →Spam und Advertising (d.h. Werbung). Der Begriff wird speziell dann verwendet wenn nicht →E-Mail genutzt wird, sondern z.B. Links die in →Blogs oder →Wikis eingebaut werden. Beworben wird zu einem großen Teil für →3P (pills, porn and poker), d.h. Medikamente die übers →Internet bestellt werden können wie z.B. Viagra, Pornographie und Glückspiel-Websites. Oft wird dabei oft das Geschäftsmodell →Affiliate Network verwendet

SPD: (surge protective device) Überspannungsschutz, wichtig für elektronische Geräte, sowohl in der Stromversorgung wie auch in Datenleitungen, auch →TVSS genannt. Diese „surge“ entstehen durch Entladungen, Induktion, z.B. bei Blitz oder beim Einschalten von großen Verbrauchern

Spear Phishing: (engl. Speer(p)fischen) Variante des → Phishing Angriffs, bei der gezielt einzelne Personen oder eine Gruppe →E-Mails mit entsprechender →Spyware (z.B. →Keylogger) erhält. (targeted email trojans). Ziel ist dabei oft →Industriespionage. Siehe →targeted attack

Speech to Text: automatische Erkennung von gesprochenem Text. Wird von der →NSA zum →Abhören von Telefonaten eingesetzt. Wird vor allem in Verbindung mit →Google Glass oder →Lifebits sehr problematisch wenn Aussagen anderer Menschen auf diese Weise maschinell verarbeitbar werden. Siehe →Semantic Forest

Speicher: 1) (Memory, auch Hauptspeicher oder →Arbeitsspeicher) Datenspeicher, in dem binäre Informationen gespeichert werden. Diese Informationen sind entweder →Computerbefehle (d.h. →Programme) oder →Daten. Aus diesem Speicher „liest“ die →CPU die Informationen (bits) aus und führt die Verarbeitung durch. Speicher können auf verschiedenen Technologien beruhen, z.B. Halbleiterspeicher, wie auf dem →Motherboard, bei Heimrechnern gemessen in Megabyte (1 Mio. Byte), im Vergleich dazu Plattenspeicher, gemessen in Gigabyte (10^9, deutsch 1 Millliarde, engl. 1 billion), Terabyte (10^{12}, deutsch 1 Billion, engl. trillion) und heute oft bereits Petabyte (10^{15}, deutsch 1 Billiarde, engl quadrillion). Umgangssprachlich ist mit Speicher / Memory heute meist der Halbleiterspeicher auf dem Motherboard gemeint, der auch Hauptspeicher oder →DRAM genannt wird. Diese Speicher sind flüchtig und bleiben typischerweise nur erhalten solange der Speicher mit Strom versorgt wird. D.h. beim Starten eines →PCs oder →Smartphones werden diese Daten aus dem permanenten Speicher (→Festplatte oder →SSD) geladen (→boot). Smartphones werden daher typischerweise fast nie ausgeschaltet, daher sind die Geräte beim Einschalten sofort aktiv. Durch Kühlung lässt sich die flüchtige Information eines Speichers jedoch auch länger konservieren (→Remanence), dies lässt sich für →Angriffe, z.B. die →Schlüssel einer →Festplattenverschlüsselungen nutzen. Siehe →Virtual Memory, →Page, →Segment

2) Jedes Gerät, auf dem binäre →Daten aufbewahrt werden können. Siehe →Speichersystem

Speichersystem: Gerät, in dem →Daten abgelegt werden, auf die dann später wieder zugegriffen werden kann, z.B. →Magnetplatten oder Magnetbänder

Spiele: →Games

SpyEye: →Schadsoftware, Konkurrenz zu →Zeus, genutzt um Rechner zu infizieren und zu manipulieren und →Botnetze aufzubauen und zu betreiben, vor allem gegen →e-Banking eingesetzt. Enthält u.a. →Keylogging Features, kann aber als →Man-in-the-Browser auch konfiguriert werden um dynamisch mit →2-Faktor-Authentisierungen wie →SMS-TAN umzugehen und Geld zu überweisen

SPICE: (Software Process Improvement and Capability Determination), →ISO 15504. Ein Modell für das zur Beurteilung von Unternehmensprozessen rund im Software (→PAM), verwandt mit →CMM, allerdings mit 6 Reifegraden. Ebefalls relevant ist ISO 12207-Prozesse im Software-Lebenszyklus

SpiderOak: →Cloud service, siehe →Dropbox

Spieltheorie: mathematische Disziplin die sich mit menschlichem Verhalten in Entscheidungssituationen beschäftigt. Dabei wird von kooperativen und nicht-kooperativen Modellen ausgegangen, ein wichtiges Beispiel ist das sog. „Gefangenendilemma". Solche →Algorithmen spielen bei dem Übergang von →Überwachung zum Vorhersagen von persönlichem Verhalten durch →Big Data Analysen eine wichtige Rolle. Durch die Möglichkeit, Verhalten vorherzusagen entsteht auch die Möglichkeit, bestimmte Optionen (wie z.B. Kredite, →Kreditschutz oder Informationen) gar nicht erst anzubieten (weil die „virtuelle Persönlichkeit", die sich aus den →Daten ergibt entweder kein Interesse haben wird oder die Option missbrauchen könnte (→Pre-crime), falsch wie die virtuelle Persönlichkeit sein mag)

SPIM: (SPAM over IM) Versand von →SPAM mittels →Messaging Dienst

SPIT: (SPAM over Telephone) bei der Nutzung eines →VoIP-Systems das automatisierte Senden von großen Mengen von telefonischen Sprachnachrichten in die →Voicemail-Inbox des Nutzers. SPIT ist noch schwerer zu filtern als →SPAM

Split: Konzept der →Datensicherung von →Datenbanken, bei der die Datenbank kurz gestoppt wird, dann eine Auftrennung der gespiegelten Magnetplatten (→Mirror) durchgeführt wird (→BCV) und danach das 2. Volume gesichert wird, während die Datenbank weiter in Produktion ist

Split traffic: wenn ein →VPN-Client bei Verbindung zur VPN-Gegenstelle jeglichen anderen externen Datenverkehr verhindert. Sehr zu empfehlen

SPF: (Sender Policy Framework) Erweiterung zur Vermeidung von →Spam und →Phishing. Dabei wird im →DNS Record jeder →Domaine ein Datensatz abgelegt, der alle legitimen →IP-Adressen der →SMTP-Server dieser Domaine beschreibt. So wird →Spoofing erschwert. Soll 2012 durch →DMARC erweitert werden

Spontane Vernetzung: automatische Integration von IT-Geräten und darauf eingerichteten Diensten in ein lokales Netz, dass die Nutzung dieser Dienste, oder den Zugriff auf weitere Ressourcen im Netz ermöglicht. Ein →Notebook, ein Drucker, usw. werden in einem Raum automatisch in das Netz integriert, das die übrigen IT-Komponenten verbindet, ohne dass eine Installation erforderlich ist. Dies ist speziell bei →Bluetooth der Fall und kann dann eine →Verwundbarkeit darstellen

Spoofing: (engl.Spoof = Parodie) Technik der Vortäuschung einer falschen Identität oder Absenderadresse, oft mit der Absicht, durch die gefälschten Daten authentifiziert zu werden. Ziel ist zumeist die Erlangung von Informationen durch Benutzer oder System-Instanzen (→Address-Spoofing, →DNS-Spoofing, →Caller ID Spoofing, →Mail-Spoofing), manchmal Masquerade genannt. Siehe →Fake, →Accountability, →Hacker, →SPF, →Twitter

Spotify: seite 2006 →Streamingdienst für Musik, Konkurrenz zu →Apple mit mittleweile 2020 größtem Marktanteil und damit stark bestimmend für die Finanzierung von Musikereinnahmen. →Netflix, →Amazon Prime und Spotify sind Beispiele die die oft behauptete These widerlegen, dass im →Internet alles kostenlos (d.h. über →Werbung und →Überwachung der Nutzer finanziert) sein muss (wobei Spotify auch ein eingeschränktes kostenloses Angebot mit Werbung anbietet)

Sprachanalyse: automatische Auswertung von Sprachsignalen, z.B. bei →VoIP wie →Skype. Damit kann z.B. bei bestimmten Begriffen oder bei emotionaler Erregung im Gespräch mit einem Call-Center ein Alarm ausgelöst werden. Siehe auch →Stimm-Erkennung

Sprajax: → Open-Source Security Scanner für →Ajax-basierte →Web-Applications von der →OWASP, eine Alternative zu →Hailstorm

SPRUCE: siehe →NEAT

Spy-App: →Software auf →Smartphone die zur →Überwachung von Kindern oder (Ex-) Partnern eingesetzt wird (→digitale Gewalt). Dafür ist es lediglich notwendig, dass der →Angreifer →Zugriff auf das entsperrte Gerät hat, dann kann er oder sie eine solche App installieren. Diese Apps werden NICHT angezeigt und senden typischerweise Standort, alle Kommunikationen (wie →Whatsapp, etc.) und Fotos an ein anderes Smartphone. Wenn Frauen in ein Frauenhaus kommen so

ist sehr oft ein solchermaßen infiziertes Handy dabei. Solche infizierten Smartphones können durch →Factory Reset auf den Kaufzustand zurückgesetzt werden, die Opfer verlieren dabei typischerweise alle ihre →Daten und Kontakte. Das heimliche Installieren einer solchen App ist bei Erwachsenen sicher verboten, bei Kindern hängt es vom Alter des Kindes ab, ob dies noch zulässig ist. Bei älteren Kindern sollte das Kind zumindest darüber informiert sein. Eine Verurteilung wegen Installation der Software bei einem Partner ist extrem selten, die die Anwesenheit der App auf dem Gerät kein Beweis ist, dass der (Ex-)Partner die App installiert hat. Siehe https://sicherheitskultur.at/spyware

SpyNet: Online-Community von →Microsoft zum Austausch von Informationen zu →Spyware

Spyware: Software, die oft in der Form eines →Trojaners, oder unter Ausnutzung von →Schwachstellen, auf dem Rechner des Benutzers installiert wird und die dann dort, z.B. →Passworte, das →Surf-Verhalten des Anwenders oder →E-Mail-Adressen ausspioniert und an den Autor der Spyware sendet. Eine spezielle Form sind →Key Logger. Auf diese Weise finanzieren sich z.B. manche →Raubkopierer oder →P2P-Programme. Die Abgrenzung zu →Adware ist umstritten. Hersteller dieser Software wehren sich gegen den Begriff Spyware, obwohl ihre Programme zwecks Optimierung der in Form von →Pop-ups dargestellten Anzeigen oft das Surfverhalten der Benutzer weiterleiten. Spyware beschreibt (normalerweise) ungezielte Infektionen, im Gegensatz zu →APT, bei der es sich um zielgerichtete →Angriffe handelt. Um solche handelt es sich bei →Federal Spyware (→CIPAV) und dem →Bundestrojaner, die damit eigentlich zur Klasse APT gehören. Siehe auch →Spy-App

SQL: (Structured Query Language) ursprünglich nur verwendet als Bezeichnung für eine Datenbankabfragesprache, 1986 von →ANSI standardisiert. Heute oft verwendet im Zusammenhang mit →Microsoft SQL Server oder →SQL Server-→Port (1433), bzw. dem →Open Source Tool MySQL. In letzterem Zusammenhang sicherheitsrelevant, siehe →SQL Injection

SQL-Injection: →Angriffsmethode gegen →Websites bei der →Datenbankbefehle in Eingabefelder auf →Webseiten eingegeben werden, in der Hoffnung dass Programmierfehler einen direkten Zugriff auf die →Datenbank des →Webservers ermöglichen. Eine spezielle Variante ist SQL-Injection mit Conversion Error. Diese wird angewendet, wenn zwar SQL-Kommandas von der Datenbank ausgeführt werden, aber der →Angreifer die Ergebnisse nicht sieht. In diesem Fall versucht der Angreifer, die Textdaten in eine Zahl umzuwandeln, was zu einem Conversion Error führt, der bei falscher Einstellung der Datenbank im →Web-Browser ausgegeben wird. Eine weitere Variante ist „blind SQL-Injection“. Diese kommt zum Einsatz wenn der Angreifer keine Daten im →Browser angezeigt bekommt. Trotzdem kann über eine Auswertung der Antwortzeiten erkannt werden, ob im Hintergrund ein SQL-Kommando ausgeführt wurde. Der →Angriff (in der einen oder anderen Form) gelingt leider viel zu oft, auch in prominenten Fällen wie →HBGary und →Sony

SQO-OSS: (Software Quality Observatory for Open Source Software) Initiative der EU zur Beurteilung und Verbesserung der Software-→Qualität von →Open Source Software

SRP: (Secure Remote Password Protocol) kryptographisches Protokoll mit dessen Hilfe ein geheimer →Schlüssel ausgehandelt werden kann ohne dass eine zentrale vertrauenswürdige Stelle benötigt wird, vergleichbar mit →Diffie-Hellman

SRST: (Survivable Remote Site Telephony) Feature von Cisco →IP-Phones, damit auch ohne CallManager eine Verbindung hergestellt warden kann

SRTP: (Secure Realtime Transport Protocol, RFC 3711) sichere Version von RTP, genutzt von →Unicast und →Multicast Anwendungen, z.B. Videoconferencing und →VoIP. Setzt auf →UTP auf

SS7: (Signalling System No. 7) 1975 von AT&T entwickeltes und von der →ITU-T standardisiertes System zum Austausch von Kontrollinformationen in Telekommunikationsnetzen (→PSTN) (als Ersatz für frühere →In-band Signalisierung). Wichtig sind dabei Verfahren zur schnellstmöglichen Fehlerbehebung und zum Finden von alternativen Pfaden in Millisekunden. In 2014 wird bekannt, dass mittels SS7 Regierungsbehörden (z.B. die →NSA) und auch zivile „Dienstleister“ die →Zugriff auf die Netze von Telefongesellschaften in einem Land der Welt haben, weltweit Telefongespräche umleiten und damit abhören können und den Ort von beliebigen →Handys feststellen. Durch die fehlende Sicherheit im Konzept von SS7 werden auch alle handy-basierten Verfahren wie →mTAN unsicher. Telefonanbieter haben zusätzliche Sicherheitsmaßnahmen implementiert so dass in Europa Angriffe gegen Telefone üblicherweise nicht über SS7 sondern mittels Übernahme der →SIM-Karte durch →Social Engineering stattfinden (→SIM-Swapping). In →VoIP-Systeme ersetzt durch →SIP oder →H.323. Siehe →Media Gateway

SSAE 16: (Statements on Standards for Attestation Engagements) ist ein Nachfolger von →SAS 70 bei der Auditierung von Service-Organisationen. Siehe http://ssae16.com/

SSD: (→solid state disk)

SSE: (server-side encryption) →Verschlüsselungsimplementierung bei →Cloud Computing bei der die Schlüssel jedoch unter Kontrolle der Betreiber stehen (→SSE, z.B. Amazon Webservice S3, im Gegensatz zum AWS JDK for Java, das client-seitige Verschlüsselung erlaubt). Für die →Benutzer zwar bequem, da keine eigenen Schlüsselverwaltung, aber auch →Compliance-Gründen sehr oft nicht akzeptabel

SSE-CMM: (System Security Engineering - Capability Maturity Model) Dokument der ISSEA (International Systems Security Engineering Association) zum Reifegrad von Sicherheitsprozessen. Sehr ähnlich zu →ISO/IEC 21827. Siehe →CMM

SSH: (Secure Shell) auf dem →IP-Protokoll basiertes Protokoll zum interaktiven Arbeiten auf einem Rechner mit Hilfe eines Textinterfaces. Auf Grund von →Verschlüsselung und → Authentisierung sicherer als →Telnet. 2012 schreibt die NSA, dass sie solche Verbindungen manchmal entschlüsseln können

SSID: Kennung eines →Access Points im →FunkLAN. Sie sollte aus Sicherheitsgründen keine unnötigen Informationen, z.B. Firmenname oder Abteilung enthalten. Ihre Aussendung kann z.T. auch ganz unterdrückt werden

SSJC: →OASIS

SSL: (Secure Socket →Layer) →Protokoll, das ursprünglich 1993 von →Netscape entwickelt wurde, aber bald als de-facto Standard anerkannt war. Es dient zur →Authentisierung von →Webservern mittels →Zertifikaten und der →Verschlüsselung von Daten die über HTTP versendet werden (das dann zu →HTTPS wird). Theoretisch ist auch die Authentisierung von →Browsern möglich, entsprechende Zertifikate haben sich jedoch (leider) nicht durchgesetzt. Seit 2006 ergänzt durch die Alternative →TLS. Seit 2014 (u.a. durch →Heartbleed und →Poodle) gilt selbst die letzte Version (3.0) als zu unsicher und es sollte nur noch TLS verwendet werden. 2015 erklärt die Organisation hinter →PCI-DSS SSL offiziell als nicht geeignet für die Zertifizierung, da keine sichere Implementierung mehr bereit bereit steht.

→Google konzipiert ein Verfahren, bei der ersten Authentisierung des Benutzers auf einem Gerät die →App oder der →Chrome-Browser ein SSL/TLS-client Zertifikat erzeugt und damit dieses Gerät fest an diesen Kanal bindet („channel binding“).

SSL und TLS verwenden →Zertifikate nach →X.509 (wenn dabei →MD5 als →Hash verwendet wird, so ist das Zertifikat seit Ende 2008 fälschbar, besser ist →SHA-1). Das SSL-Protokoll wird vom Browser dadurch initiiert, dass dem bekannten http ein „s“ angehängt wird (https://www.firma.at). Es wird ein anderer →Port des →IP-Protokolles verwendet, meist 443. Das ist für den Browser der Anlass, vom angesprochenen Server zur Authentisierung ein Zertifikat und seinen öffentlichen Schlüssel (Public Key) anzufordern. Dieser Schlüssel wird zusammen mit einer Prüfsumme (→ Fingerprint) und einer ID an den Browser zurückgemeldet. Wegen der fehlenden Authentisierung der →Client-→PCs ist das Verfahren anfällig gegen →Man-in-the-Middle Angriffe. Seit 2009 erweitert durch →EV Certificate. Siehe auch →HSTS

Auf Grund der immer stärkeren Nutzung von →Smartphone →Apps stellt die Wirksamkeit von SSL (oder →TLS) gegen →Man-in-the-Middle Angriffe kaum noch gegeben, da der Benutzer keine Möglichkeit hat, das Zertifikat des →Webservers zu überprüfen, mit dem die App kommuniziert. Diese Überprüfung muss in der App selbst durchgeführt werden, was zumeist unterbleibt.

2010 und 2011 werden zahlreiche Schwächen im Protokoll veröffentlicht, aber die eigentliche Schwäche liegt in der Anfälligkeit von Zertifikatsherausgebern (→CAs) gegen →Angriffe bei denen gefälschte Zertifikate erstellt werden, denen die Browser automatisch vertrauen, da dort eine Liste von über 600 angeblich vertrauenswürdigen CAs hinterlegt ist. 2011 werden zahlreiche CAs erfolgreich angegriffen, offenbar zum Teil um politische Dissidenten mit Man-in-the-Middle Angriffe abzuhören. Siehe →TLS, →Sovereign Keys http://sicherheitskultur.at/notizen_1_11.htm#iran

SSL/VPN: Implementierung eines →VPN zum →Zugriff mittels →Webbrowser. Im Gegensatz zu →IPsec kommt es dabei zu einem „Medienbruch“ ähnlich wie bei einem →Terminalserver, d.h. es werden nicht 2 Netze verbunden, sondern eine Benutzeroberfläche wird präsentiert

SSN: (Social Security Number) US-Version der →SVN. Mangels anderer lebenslanger Identifikation und fehlenden Personalausweise wird die Kenntnis der SSN in den USA sehr häufig als →Authentifizierung, z.B. beim Beantragen eines Kredits, verwendet. Sie ist daher Hauptangriffspunkt bei →Phishing für →Identity Theft

SSO: →Single Sign-On

SSRF: →Server-Side Request Forgery

Staatstrojaner: (umgangssprachlich in D und Ö als Bundestrojaner bezeichnet) →Spyware, die für eine heimliche Durchsuchung und /oder Überwachung der →Rechner von Verdächtigen eingesetzt wurde. In den USA als →CIPAV im Einsatz. Oft ist es ein jeweils maßgeschneidertes Programm "Remote Forensic Software" (→RFS). Der Einsatz solcher Software zu Überwachungszwecken wird immer stärker gefordert seit die →End-toend →Verschlüsselung immer stärker eingesetzt wird und dadurch eine →Überwachung auf zentralen →Servern

verhindert. Siehe →Federal Spyware, →NSO, →FinFischer/Finspy
http://sicherheitskultur.at/notizen_1_07.htm#bundestrojaner

Stablecoin: eine →Cryptocurrency die an eine oder mehrere Währungen gebunden ist und daher geringeren Kursschwankungen unterliegen sollte als traditionelle Cryptocurrencies, wie →Bitcoin. Da würden z.B. "Central Bank Digital Currencies" (→CBDC) gehören, aber auch die von →Facebook geplante Währung →Libra.

Stack: 1) alle Schichten (→Layer) die für eine Datenkommunikation genutzt werden. Siehe →OSI Schichtenmodell

2) spezifische Datenorganisation, oft hardware-unterstützt. Dabei wird das zuletzt gespeicherte Datenelement als erstes wieder entnommen (Last In – First Out)

Stakeholder: Begriff aus der →Businessethik, der im Gegensatz zu den Shareholdern alle von Handlungen eines Unternehmens Betroffenen, inkl. der Natur und Umwelt, bezeichnet

Stalking: (deutsch: Nachstellung) willentliches und wiederholtes (beharrliches) Verfolgen oder Belästigen einer Person, heute oft auch im →Internet

Stammdaten: →Daten zumeist Personen betreffend, die für Abrechnungszwecke im Rahmen von Geschäftsverbindungen gesammelt werden, z.B. durch →Handy→netzbetreiber. Deren Herausgabe ist unter bestimmten Umständen gesetztlich vorgeschrieben. →Verkehrsdaten

Standard: (auch →Normen) Regeln technischer und organisatorischer Art, die mehr oder weniger verbindlich sein können. Siehe →ANSI, →DIN, →ISO, →ÖNORM, →NIST, →RFC, →IEEE, →Best Practise, Stand der Technik (state of the art), →shall, →should

Stand der Technik: →Best Practise Regeln, wie etwas implementiert oder durchgeführt werden soll. Das Nicht-Einhalten kann eine Verletzung der erforderlichen Sorgfalt darstellen und dadurch eine →Haftung nach sich ziehen. 2006 ergibt sich in Ö. eine Pflicht zum Einhalten des „Stands der Technik“ nur durch →SOX, →Basel II oder andere Corporate →Governance Regeln (z.B. GmbH-Gesetz, Aktiengesetz), in D. aus dem →KonTraG

Standleitung: heute sehr selten genutzte dedizierte Kommunikationsanbindung im Nahbereich, bei der ein einzelner Kommunikationsstrang (4-Draht Telefon, →Lichtleiter oder Coax) für einen einzelne Verbindung genutzt wird. Gilt als sicherer als z.B. Wahlleitungen und bietet einen festen →QoS. Im Fernbereich sehr teuer, daher wird dort meist →ATM oder →Frame Relay eingesetzt, bzw. Datentransfer über →Internet

Standortdaten: →Daten die notwendigerweise beim Betrieb eines Mobilfunknetzes anfallen da der Betreiber den Standort (d.h. die nächste „Zelle“ kennen muss um eingehende Gespräche zum nächsten Handymasten [=→base station]) zustellen zu können (→home location register). Diese Daten sind u.a. Ziel der →Vorratsdatenspeicherung. Standortdaten entstehen auch in jedem →Smartphone, da typischerweise dort ein →GPS-Modul eingebaut ist, bzw. der Standort über Datenbanken von →WLAN-Netzen bestimmt werden (→Google war in diesem Zusammenhang in die Schlagzeilen gekommen als die WLAN-Sammlung im Rahmen von →Google Streetview publik wurde, aber andere Dienste bieten ähnliche Datenbanken an).

Viele →Apps greifen auf diese Standortdaten zu und machen diese dann zu Geld. Standortdaten sind begehrt, da sie sehr viel über das Verhalten der Menschen aussagen. Länger andauernde Bewegungsprofile einer Person sind die wirklich →anonym, da sich aus dem Aufenthaltsort am Tag (Arbeitsplatz) und in der Nacht (Wohnort) in den meisten Fällen die Person bestimmen lässt. Die →NSA sammelt täglich weltweit Milliarden entsprechender Datensätze

Starke AI: →artificial intelligence

Starke KI: →artificial intelligence

Stateless Tracking: Methoden um →Benutzer im →Internet wiederzuerkennen ohne →Daten auf dem →PC oder →Smartphone des Nutzers abzulegen (z.B.→Cookies). Wird z.B. mittels →Device Fingerprinting erreicht. → Tracking ist whichtig für gezielte Werbung, aber auch für →Surveillance

State-Machine: Konzept der Computerwissenschaft. Dabei werden die Details des über eine Zeiteinheit erhaltenen Inputs auf Veränderungen einer begrenzten Anzahl von Zuständen (States) reduziert. Dies vereinfacht die Programmierung von Systemen, bei denen der Output nicht nur vom direkten Input, sondern auch früheren Ereignissen abhängt. Wird z.B. in →Firewalls verwendet. Siehe →SDL

State-of-the-Art: deutsch →Stand der Technik

Status-Anzeigen: Implementierung von →Human-in-the-Loop. Das →Programm zeigt an mehr oder weniger prominenter Stelle Hinweise an, die Der →Benutzer als Basis für eine Sicherheitsentscheidung nehmen sollte, z.B. das Fehlen des →SSL-Indikators im →Webbrowser. Dies führt sehr oft zu suboptimalen Sicherheitsentscheidung

Steam: →Internet →Vertriebsplattform für Spiele (→Games). Über diese →Plattform wird nicht nur der Verkauf, sondern auch die Verwaltung der Kunden / Gamer, die Verteilung der →Software sowie die Überwachung von Lizensen (→DRM) durchgeführt. D.h. andere Spieleanbieter wie Valve nutzen diese Plattform auch

Steganographie: Verstecken von Daten, z.B. in großen Datenmengen. Dabei geht es um →Verschlüsselungsverfahren, bei dem so kommuniziert wird, dass die Kommunikation selbst für Uneingeweihte nicht erkennbar ist. Zu diesem Zweck wird eine (möglicherweise verschlüsselte) Nachricht in einer anderen Nachricht, oder in Daten, z.B. einem digitalisierten Bild versteckt. Ähnlich wie bei einem digitalen Wasserzeichen werden zusätzliche Informationen in eine Datei codiert, die nur mit einem speziellen Programm oder Tool wieder lesbar gemacht werden können. So kann ein digitalisierter Text, z. B. in einer Bilddatei, verschwinden und nur vom Inhaber des Decodier-→Schlüssels wieder ausgelesen werden. Eine andere Anwendung von steganographischen Verfahren wird bei →TOR versucht, indem der Datenverkehr mittels „bridges“ und „pluggable transports“ so verändert wird, dass er nicht als TOR-Datenverkehr erkannt werden soll (z.B. in einem Land in dem TOR verboten ist). Siehe →Deniability

Stickyness: häufige Forderung der Betreiber von →Social Networking →Websites oder ähnlichen →Apps. Sie beschreibt den →Suchtcharakter den diese Anbieter für ihre Angebote erreichen wollen damit die Nutzer möglichst viel ihrer Lebenszeit auf dieser Plattform verbringen und während dieser Zeit personalisiterte →Werbung geschaltet werden kann. Dabei werden zum Teil Erkenntnisse aus der Optimierung von Spielautomaten eingesetzt, wie das Wechseln zwischen Gewinn und Verlust, zwischen Up und Down, z.B. durch abwechselnd negatives Feedback und positives, z.B. →Likes. Ein dafür manchmal gebräuchlicher Begriff ist →dark pattern. Auch bei Computerspielen (→Games), z.B. Pokémon ist ein Suchtelement Teil des Designs. Ein anderer Aspekt ist →FOMO (fear of missing out). Diese Techniken stehen im Kern des →Überwachungskapitalismus

Stimme: →Stimm-Erkennung

Stimm-Erkennung: automatische Analyse von Stimmen zum Zwecke der →Identifizierung von Personen oder deren Gefühlszustand, z.B. ob sie ärgerlich sind oder verliebt. Technisch werden dabei →DSP eingesetzt. Wenn Zugang zu vielen Telefonverbindungen besteht kann damit auch eine großflächige Fahnung (→Rasterfandung) durchgeführt werden. Siehe →Sprachanalyse, →Überwachung, →NGI

STK: →SIM Application Toolkit

Stock-Pump-and-Dump-Spam: →Pump-and-dump

Storage Area Network: →SAN

Storm Worm: →Botnet auf →P2P-Basis mit verteilten Control Center, daher schwer angreifbar. →Overnet http://www.heise.de/security/artikel/106686

STP: (spanning tree protocol, IEEE Standard 802.1D) Verfahren für →Redundanz in →Layer-2 → IP-Netzen, das es erlaubt, alternative Pfade zwischen →Switchen vordefiniert und verkabelt zu haben. Siehe →Hochverfügbarkeit

Streaming: Streaming bezeichnet die Übertragung von Tönen und Videos über →Computer-Netze und in „nicht-linearer“ Form (d.h. Nutzer können im Gegensatz zu Rundfunk und Fernsehen selbst den Zeitpunkt und die Inhalte auswählen – eine Ausnahme stellt →Webradio dar). Ein wichtiger Aspekt ist, dass bei Streaming (im Gegensatz zum Kauf einer DVD) kein Erwerb der Inhalte entsteht, sondern nur ein Nutzungsrecht. →Social Viewing bezeichnet Systeme mit deren Hilfe mehrere Zuschauer gleichzeitig einen Film sehen und parallel kommentieren können, wurde 2020 populär.

Genutzt werden →Streaming Media, bekannte Beispiele solcher Dienste für Filme sind →Netflix, →Amazon Prime, Disney+ und →Spotify. Diese Anbieter produzieren seit ca. 2016 eigene Inhalte und sind eine ernsthafte Bedrohung für die traditionelle Film-Industrie und ihre traditionellen Vermarktungswege. Im Bereich Videostreaming dominert →Google →Youtube, Dailymotion und → Vimeo, als alternative gibt es →Peertube. Bei Musik streiten sich →Spotify und →Apple um Marktanteile. Da Streaming hohe Anforderungen an die Bandbreite stellt gab es erste Dienste erst ca. 2000. →2020 gab einen erheblichen Schub für Streaming. Streaming Dienste sind einer der Streitpunktpunkte bei →Net Neutrality da oft gewünscht wird dass die großen Datenmengen priorisiert und/oder für die Nutzer kostenfrei übertragen werden (außerhalb der Datenlimits). Die Nicht-Linearität bedeutet, dass Inhalte als →Unicast übertragen werden müssen, d.h. wenn 1000 Personen dasselbe Video schauen, so muss der →Server trotzdem die Inhalte 1000x über die Leitungen senden. Deswegen werden die Inhalte möglichst nahe bei dem Empfängern auf →CDN-Servern gespeichert. Trotzdem stellen Videodaten mittlerweile ca. 80% des →Internet-Verkehrs dar.

Seit ca. 2013 gibt es Streaming von Videospielen (→Games). Führend ist dabei die Plattform Twitch (Teil von →Amazon) auf der Zuschauer anderen beim Spielen zusehen können. Dies ist überraschend populär. Es finden dort jedoch auf andere Auftritte statt. Eine weitere Form des Streamens von Spielen bezeichnet Spiele die rein im →Web-Browser genutzt werden und daher nicht an Gaming-PCs gebunden sind (z.B. Dienste wie →Google Stadia, →Microsoft xCloud, →Amazon Luna, Onlive oder Gaikai). Dies wird auch Cloud-Gaming genannt

Streaming Media: Technologie die es ermöglicht, auf Töne und Bilder die auf →Websites

angeboten werden, kontinuierlich zuzugreifen und ohne Abspeichern auf der eigenen →Festplatte direkt darzubieten. Wird z.B. für Internet Radio benutzt. Für Audio wurde zu Beginn Realaudio von Progressive Media oder auch MP3 oder Vorbis eingesetzt. Verwendete →Protokolle sind RTSP (Real-time Streaming Protocol), →RTP (Real-time Transport Protocol), →RTCP (Real-time Control Protocol). Inhalte können in →Smartphone →Apps, →Web-Browsern oder →Smart TVs abgespielt werden. Siehe →Streamripper

Streamripper: →Software, die es erlaubt, die kontinuierlichen Audio-Ströme von →Webradio in →Dateien im →MP3-Format umzuwandeln. Dabei wird im Fall von Privatkopien in Ö das →Urheberrecht nicht verletzt. Siehe →Webradio-Recorder

Streetview: →Google Streetview

Stresser: dDoS-as-a-service Dienst um →IP-Adressen für eine begrenzte Zeit nicht erreichbar zu machen. Details siehe →Denial of Service

Stromverschlüsselung: (engl. stream cipher) →Verschlüsselung eines kontinuierlichen Datenstroms. Siehe →A5

STUN: (simple traversal of →UDP through →NATs) Technik um eine Verbindung zwischen 2 Rechnern hinter →NAT-, bzw. →NAPT - →Firewalls oder →Routern zu ermöglichen (RFC3489). Es wird bei einem externen STUN-Server angefragt, was die eigene externe →IP-Adresse und →Port-Nummer ist. Mit deren Hilfe kann eine →Peer-to-peer Verbindung hinter →Firewalls aufgebaut werden, z.B. wichtig bei →WebRTC →Webvideokonferenzen. Siehe →UDP hole punching

Stuxnet: Name der Software für einen →Angriff auf die Kernwaffenanreichung und ein Kernkraftwerk im Iran mittels Manipulation der →PLC Software mit dem Ziel der Zerstörung von Anlagenkomponenten. Dieses Ziel wurde offensichtlich erreicht. Verwendet wurden Techniken des →APT, inkl. mehrere →Zero Day Exploits, gestohlene →X.509 →Zertifikate zum →Signieren von Code und →Rootkit-Technologien. Eingeschleust wurde der →Schadcode über →USB-Stick zur Überwindung des →Air gaps.

Neu war die konkrete Umsetzung eines bis dahin theoretischen Angriffs auf Hardware-Komponenten durch Manipulation ihrer elektronischen Steuerungen. Der Angriff war sehr aufwendig, ziemlich sicher wurden Teile der Anlage mit Originalkomponenten nachgestellt um die Software zu testen. Verdächtigt wird eine Allianz aus USA und Israel, aus den USA gibt es eine inoffizielle Bestätigung.

2013 wird herausgefunden, dass bereits seit 2007 eine noch komplexere Variante in der Natanz im Einsatz war, die den Druck in den Zentrifugen so erhöhte, dass die Lebensdauer der Zentrifugen reduziert wurde. Diese Variante war direkt vor Ort installiert worden. Ab 2009 wird dann die 2. Variante eingesetzt, die die Frequenz der Zentrifugen erhöht und mittels USB-Stick übertragen wurde.

Stuxnet wird als Beispiel für →Cyberwar gesehen, aber Cyber Sabotage ist vermutlich treffender. Siehe http://sicherheitskultur.at/notizen_1_10.htm#stux

Sub-Domain: Namenselement vor dem →Domain-Name einer →URL. Z.B. books.google.com (books ist die Sub-Domain von google.com). →Websites auf einer Sub-Domain können auf →Cookies zugreifen, die von der übergeordneten Domain geschrieben wurden

Suchmaschinen: Webdienste, die mit Hilfe von →bots ein Verzeichnis des →World Wide Webs erstellen. Dabei wird jedoch auf Grund der Größe des Webs nur ein kleiner Teil katalogisiert, das sog. Surface Web, geschätzt als ca. 16%. Das →Deep Web ist noch bis zu 500 mal größer, da es viele Seiten gibt, die von Suchmaschinen nie erreicht werden können, entweder weil dies ein Passwort voraussetzt oder weil dies Datenbankanfragen sind oder weil sie nicht mittels →http erreichbar sind. Suchmaschinen verlieren an Relevanz wenn mehr und mehr Inhalte, die für Benutzer wichtig sind, nicht erreichbar sind, z.B. weil sie in den →Facebook Profilen nicht-öffentlich sind. →Google versuchte daher, die Inhalte von →Google+ (jetzt obsolet) auch in den Suchergebnissen zu liefern, konnte dies jedoch für andere →Social Networks nicht tun. Da Suchmaschinen keinen →Zugriff auf den →Social Graph der Nutzer hat, endet jede Suche nach einem persönlichen Bekannten bei irgendwelchen Prominenten im Web.

Suchmaschinen sind problematisch durch ihr →Data Mining der Suchanfragen, die sensible →Daten enthalten und (speziell bei Weitergabe) zu Verletzungen der →Privatsphäre führen können, siehe →Spear fishing, →targeted attack, →Google, →Swoogle, →SEO, →Social Circle, →contextual discovery. Alternative Optionen sind z.B. →DuckduckGo oder das französische →qwant. Bei solchen Suchmaschinen werden oft die Anfragen nach Google weitergeleitet, aber dadurch auch anonymisiert

Suchtcharakter: sehr erfolgreichen →Websites vor allem in Bereich →Social Networking, wie →Facebook, aber auch →Youtube wird Suchtcharakter nachgesagt, auch →stickyness genannt. Zweck des Designs und der Konzepte ist es, die Nutzer möglichst lange auf der jeweiligen Website oder →App zu halten um einen möglichst großen Anteil an den Werbeeinnahmen zu erhalten. Die Methoden werden oft als →Dark Pattern bezeichnet. Siehe →Werbung

sudo: →Programm auf →Unix Systemen, das

es erlaubt, dass bestimmte Benutzer Programme ausführen können, die normalerweise als „superuser“ (su) ausgeführt werden müssen, ohne dass diese Anwender diese Rechte „haben“. http://www.courtesan.com/sudo/

Super-App: →WeChat

Supercomputer: ein →Computer, der erheblich schneller ist als die zu einer gewissen Zeit üblichen Computer. Die Geschwindigkeit wird in der Regel in FLOPS (→floating point operations per second) gemessen, da solche Geräte fast immer für →Gleitkommaoperationen wie z.B. große Simulationen (z.B. Wettervorhersage, Kernenergie und Kernwaffenforschung) genutzt werden. In den 60igern gebaut von Control Data oder Cray Research in der Form von Vektorrechnern, Leistungen einige 100 MFLOPS), heute durch extreme Parallelisierungen Leistungen im Peta FLOPS Bereich

Supplicant: Software auf einem Gerät, das über →NAC (IEEE 802.1x) authentisiert werden soll

SURBL: (Spam URI Realtime Block Lists) Liste von →Domains, die früher in →Spam referenziert wurden

Surfen: auch Web Surfing. Die Nutzung eines Web →Browsers um Informationen im →Internet abzurufen. Ein wichtiger Aspekt ist das Verfolgen von →Hyperlinks von einer Webseite zur nächsten. Sicherheitsrelevant, weil über →Verwundbarkeiten der verwendeten Software und →Malware auf Websites →Angriffe erfolgen können

Surveillance: (engl. →Überwachung) →Big Brother, →Sousveillance

survival time: durchschnittliche Zeit bis zu einer Infektion durch →Würmer im →Internet. Ein nicht geschütztes System (ohne →Firewall und mit nicht-aktueller Software, →Patch) wäre nach dieser Zeit infiziert. Die Messungen schwanken zwischen 5 und 10 Minuten

SUS: (Software Update Services) kostenloses →Programm für die Verwaltung von →Patches in Windows-Netzen. Verwendet →MSUS als Server-Komponente und →„Automatic Update“ als Client-Software. Soll von →WSUS abgelöst werden

SVG: (Scalable Vector Graphics) Standard der →W3C-Organisation für die Präsentation von 2-D Graphiken im →Webbrowser auf →XML-Basis. Alternative zu →Flash und →Silverlight, aber derzeit (2008) nicht sehr gut unterstützt

SVN: (Sozialversicherungsnummer) in D., Ö, CH verwendete lebenslange Identifizierungsnummer für Zwecke der Sozialversicherung. Die in den USA verwendete →SSN wird auch für viele andere Zwecke eingesetzt

SVP: (Spectralink Voice Priority) spezielles Protokoll für →VoWLAN

SWATting: vor allem in den USA verbreitete extreme Form des →Cyber Bullying (Cyber Mobbing): Anruf bei der Polizei dass in einem Haus ein bewaffnetes Verbrechen passiert mit dem Ziel, dass die Polizei mit einem Großeinsatz das Haus umstellt. Wird oft als Racheakt verwendet, zum Teil angewendet gegen →Cybercrime-Journalisten, wie z.B. Brian Krebs. Wird jedoch auch gegen beliebige Personen eingesetzt, oft in der Gamer-Szene und sehr oft gegen Frauen. Sehr schwer zu verfolgen, da bestehende Gesetze auf körperliche Gewalt abzielen und die Täter oft mehrere →Anonymisierungsdienste verwenden um den Anruf bei der Polizei mittels →VoIP abzusetzen.

SWIFT: (Society for Worldwide Interbank Financial Telecommunication) internationale Genossenschaft der Geldinstitute, die ein Telekommunikationsnetz (SWIFT-Netz) für den Nachrichtenaustausch und Geldtransfer zwischen diesen unterhält, gegründet 1973. Ziel des Netzes ist ein Bank-zu-Bank Nachrichtenaustausch mit Sicherheit in Bezug auf →Non-repudiation und →Authentisierung. Dies wird durch →Hash und mehrfaches →Logging errreicht. →Vertraulichkeit wird über Hardware-→Verschlüsselung der Verbindungen erreicht. Die heutige Version setzt digitale →Signaturen ein. Siehe →BIC

Die eigentliche Sicherheit, auch gegen Betrug, entsteht durch doppelte →Buchführung (entwickelt bereits 1494). 2006 wird bekannt, dass SWIFT seit 2001 alle Daten über internationale Geldtransfer an den CIA liefert, die europäischen Behörden haben jetzt auch Interesse an den Daten geäußert.

2016 finden eine Reihe von →Angriffe statt bei denen das Geld mittels SWIFT-transfer auf Konten der Angreifer überwiesen wird. Durch geschicktes Weitertransferieren, z.B. zu Casinos können die Gelder zum Teil nicht verfoglt und zurückgeholt werden. Die Zentralbank von Bangladesh hat dabei 81 Mio USD verloren. Die Angriffe sind nicht gegen das Netz selbst sondern die Angreifer dringen in die Banksysteme ein und verwenden diese illegalerweise

Swipe: genutzt für das Entsperren einer →Bildschirmsperre, zuerst bei →Android → Smartphones. Dabei wird ein Code durch das Abfahren von quadratisch angeordneten Punkten auf einem Bildschirm eingegeben. Es entstehen in der Regel längere Sequenzen als die üblichen 4-stelligen →PINs. Jedoch hinterlässt die „Figur“ deutliche Schmierspuren auf dem Glas, wodurch diese Technik wieder sehr unsicher wird

Switch: Verkabelungstechnologie, bei der jedes einzelne Gerät eines Datennetzes (→LAN oder →SAN) an einem eigenen →Port des Switches angeschlossen ist. Ursprünglich entwickelt um den Durchsatz von →Ethernet-

Netzen zu erhöhen (im Gegensatz zum →Hub). Dies erschwert jedoch den Einsatz von →Protocol Analyzern, siehe →SPAN. Wird in Verbindung mit der →VLAN Technologie oft zu Sicherheitszwecken eingesetzt. →Virtuelle Server (→Vmware) enhalten oft virtuelle Switches in Verbindung mit virtuellen →Netzwerkadaptern (→Ports). Siehe →Port Security

Swoogle: →Suchmaschine für das →semantische Web

Sybil: Sybil Nodes sind Knoten in →Social Networks, →P2P-Systemen und reputationsbasierten Systemen künstliche Knoten (Mitglieder) die für Angriffe (Sybil Attacks) genutzt warden können

Synchronisation: automatischer Abgleich von Speicherbereichen, zum Teil für →Datensicherung verwendet. Siehe →Mirror

Symbian: →Betriebssystem für →Smartphones und →PDAs, das von der Firma Symbian angeboten wird und eine Alternative zu →WinCE und →PalmOS ist. Kam auf Nokia-→Smartphones zum Einsatz. Anfang 2005 gab es eine Reihe von →Schwachstellen, die zu Angriffen genutzt werden können, Symbian spielt seit ca. 2012 keine Rolle mehr

Synflood: →Angriff auf Rechner (→DoS) bei der durch das Senden einer sehr große Zahl von syn-Paketen zur Eröffnung einer →TCP-Verbindung ein Rechner lahmgelegt wird. Siehe →Denial of Service

Syslog: Standard-Verfahren zur Weiterleitung von →Logging-Daten in →IP-Netzen. Der Syslog-Server (syslogd) empfängt die Daten via →TCP oder →UDP, es kann mittels →SSL/TLS verschlüsselt werden. Logs die auf diese Weise auf separate Server gespiegelt werden können für →Audit-Zwecke oder Sicherheitsmonitoring verwendet werde

System: komplexes Gebilde aus Einzelkomponenten, die auf Grund ihrer Komplexität kaum zu durchschauen sind und dadurch →Bugs, d.h. unterwünschtes Verhalten, und damit →Schwachstellen für →Angriffe zeigen. Beispiel: IT-Netze, →Computer, →Betriebssystem

Systemüberwachung: Verfahren zur kontinuierlichen Überwachung des Zustands aller Komponenten der (IT-) Infrastruktur (Hardware und Software). Bei Fehlern werden →Incidentmeldungen generiert. Teil der Systemüberwachung ist die →Netzüberwachung

Tablett: mobiler →Computer der im Gegensatz zum →Laptop keinen aufklappbaren →Bildschirm hat sonder nur aus den Bildschirm besteht (ein großes →Smartphone). Es werden auch Lösungen angeboten die wie ein Laptop aufgeklappt werden können, aber Bildschirm und Tastatur separiert werden können, zumeist mit MS Windows. Erste Geräte gab es bereits in den 90igern, zum Erfolg kam diese Form erst durch das →iPad von Apple, später auch mit →Android verfügbar. Von den →Bedrohungen her gelten die gleichen Regeln wie für mobile Geräte und andere Computer, im Detail abhängig vom genutzten Betriebssystem (das von Handy-Systemen bis zur vollen →Desktop-Software reichen kann). Siehe auch →Shadow-IT

Tag: einem Objekt eine Beschreibung oder einen Namen zuordnen. Siehe →Image Tagging, →Meta Tags

Tails: (The Amnesic Incognito Live System) spezielles →Betriebssystem auf →Linux-Basis mit dem Ziel →Privatsphäre und →Anonymität besser zu schützen. Es wird von einer →DVD oder einem schreibgestützten →USB-Stick gestartet, nutzt keine →Festplatte und kann daher keine Ergebnisse und Verlaufsprotokolle abspeichern. Alle Verbindungen nach außen werden über →TOR geleitet. Gewinnt Popularität durch die Enthüllungen von →Edward Snowden, bei denen es zum Einsatz kam (und kommt). Leider konnten Forscher zeigen, dass auch dieses System durch Angriffe über die Schwachstellen im →BIOS angegriffen werden kann

Take-down: wichtigste Verteidigungsmaßnahme gegen eine aktive →Phishing-→Website (oder andere kriminelle Aktivitäten). Das angegriffene (imitierte) Unternehmen kontaktiert den →Hoster der falschen Website oder den →Registrar der →Domaine und verlangt die Stillegung („vom Netz nehmen“). Die Kontaktstelle ist oft der →Compliance-Officer. Kommerzielle Services bieten diese Dienstleistung an, oft als im Rahmen von →Brand-Protection

Tampering: →Tamper-proof

Tamper-proof, tamper resistance: Schutz vor Veränderung an Geräten oder →Software. Ein Manipulieren des Geräts oder der Software soll entweder sehr schwierig sein oder deutlich sichtbare Spuren hinterlassen. →UICC-Karten (z.B. →SIM) gelten als tamper resistant

TAN: (Transaktionsnummer) hauptsächlich in Europa eingesetztes Verfahren von One-time-passwords (→OTP) zur →Authentisierung von Finanztransaktionen. Die TANs werden von der Bank erzeugt und per Brief versandt. Mittlerweile (2005) auch einzeln im Bedarfsfall per →SMS verschickt oder an Hand einer Nummerierung gezielt angefordert. Siehe →iTAN, →mTAN, →Phishing

TAO: (Tailored Access Operations) Einheit innerhalb der →NSA die für →Angriffe auf Endgeräte (→PCs, →Server, →Router, etc.) zuständig sind. Sie verwenden dafür →Exploits (→implants) um →Zero-Day →Verwundbarkeiten ausnutzen zu können (→Targeted Attacks). Mit Hilfe der →TURBINE Aktivität können 2013 solche „Implants“ auch automatisiert auf vielen Millionen →Rechnern installiert und verwaltet werden. TAO wird z.B. dafür eingesetzt, um →Schlüssel zu stehlen, die für das Entschüsseln von IPsec oder TLS-

Verbindungen verwendet werden.

Ähnliche Einheiten wie TAO gibt es auch in anderen Ländern, dokumentiert ist →APT1 in China. Ein wichtiger Punkt dabei ist, dass solche Einheiten deutlich billiger sind als andere militärische Einheiten und daher auch von Ländern eingesetzt werden, die nicht für High-Tech bekannt sind, z.B. Nordkorea oder Iran

Targeted Advertising: Fähigkeit, Werbung an eine identifizierte Zielgruppe oder Person zu richten, z.B. durch Auswertung des Kauf- oder Surfverhaltens (→data mining). Kann im →Internet, aber auch bereits „im richtigen Leben" eingesetzt werden, z.b. mittels intelligenter →Plakate. Siehe auch →retargeting, →tracking

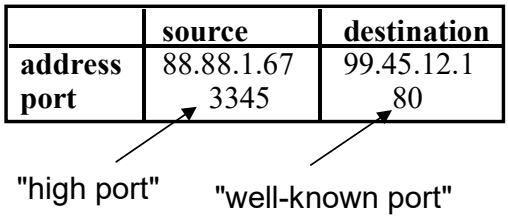
Targeted Attack: wichtige →Angriffsform u.a. für →Industriespionage. →Malware wird genau für 1 Unternehmen oder 1 Person programmiert und getestet, so dass sie dort als legitim akzeptiert wird und vom →Malwareschutz nicht erkannt wird, oft mittels Informationen in →Social Networking →Websites oder über →Suchmaschinen. Oft werden dabei →Zero-Day →Verwundbarkeiten eingesetzt. Siehe →Spear fishing, →TAO, →Breach Detection System, →Kill chain

Tastatur: (engl.Keyboard) Standardeingabegerät für →Rechner für Texte, bei Laptops integriert, bei →Servern über einen →KVM-Switch angeschlossen. →Keyboard-Logger zeichnen die Texteingaben, z.B. →Passworte illegal auf. Außerdem können elektromagn. Abstrahlungen bis 20 m Entfernung aufgefangen werden

Tauschbörse: Vernetzungen von →Internet-Benutzern um Musik, Filme oder Software untereinander austauschen. Sicherheitsaspekte unter →Filesharing, mehr technische Details unter →P2P. Siehe auch →Napster, →KaZaa, →eDonkey, →BitTorrent

TCG: (Trusted Computing Group) Konsortium von Computerfirmen (u.a. Intel, AMD, HP, IBM, Microsoft und Sun). Es geht um einen Hardwarestandard, der eine eindeutige Identifizierung eines Rechners und eine kryptographische Absicherung seiner Komponenten erlaubt. Implementiert durch einen →TPM (Trusted Platform Module) Chip auf dem →Motherboard. TCG standardisierte auch eine Festplattenverschlüsselung, die bereits in der Hardware aller zukünftigen Festplatten integriert ist. Siehe auch →NGSCB, →EMSCB, →Palladium, →ESS, →Trusted Storage

TCP: (Transmission Control Protocol) neben →UDP das wichtigste Kommunikationsprotokoll im → Internet, dessen Datenpakete mit dem →IP-Protokoll transportiert werden. Daher wird in der Umgangssprache oft fälschlicherweise der Begriff TPC/IP verwendet. Applikationen werden in TCP über →Port-Nummern adressiert, z.B. Port 80 an einen →Webserver



TCPA: (Trusted Computing Platform Alliance) früherer Name der →TCG.

TCP Wrapper: →open-source →Software zur Kontrolle von →IP-basierenden Netzzugriffen von Programmen auf dem Rechner selbst

TCSEC: (Trusted Computer System Evaluation Criteria) auch →Orange Book genannt. 1985 von der amerikanischen Regierung veröffentlichter Zertifizierungsstandard, der Kriterien für unterschiedliche Sicherheit für Computer vorgibt (→MLS). Die heute üblichen Systeme fallen in die unterste Klasse D (minimal Security), in der Klasse A (highly secure) finden sich nur einige Spezialsysteme. Von einer Reihe von Systemen, wie z.B. MS Windows oder Sun Solaris sind Spezialversionen verfügbar, die entweder der C2 oder der B1 Sicherheitsklasse entsprechen. In diesen Systemen wird die sog. →MAC (→Mandatory Access Control) implementiert, d.h. alle Objekte im System haben Autorisierungslevel, ebenso alle Benutzer. Eine weitere Feature is Discretionary access control (→DAC). Diese Systeme liegen aber bezüglich Features normalerweise mehrere Jahre hinter den Standardversionen zurück. Heute ersetzt durch →Common Criteria und →FIPS-140. Siehe →Bell-LaPadula

TDDSG: (Teledienstedatenschutzgesetz) deutsches Gesetz, 1997, das den →Datenschutz für Informations- und Kommunikationsdienste regelt, z.B. →Vertraulichkeit von Daten auf →Webservern und Aufbewahrungsvorschriften für →Logdaten. Es soll durch ein Telemediengesetz ersetzt werden. http://bundesrecht.juris.de/tddsg/index.html

TDE: (Transparent Data Encryption) →Oracle-Funktionalität zum automatischen →Ver- und Entschlüsseln von Spalten einer →Datenbank. Setzt dafür →Wallets ein. Vorteil ist, dass auf diese Weise vertrauliche Daten in →Datensicherungen nicht lesbar sind

TDL-4: 2011 Variante einer →Malware, die seit 2008 weiterentwickelt wurde. Die ältere Version TDL-3 wird seit Mitte 2010 konkurrierenden Cyberkriminellen zur Verfügung gestellt. Die neue Variante infiziert ebenfalls über den →MBR, wird jedoch über ein öffentliches →P2P-Netz →Kad gesteuert und zwar über →verschlüsselten Datenverkehr. Die Software installiert bis zu 30 Payload-Programme, u.a. eine →Proxy Software, so dass die Betreiber gegen Gebühr anonymes Surfen anbieten

Teams: →Webkonferenzsystem von →Microsoft primär für Firmen. Der große Durchbruch kam 2020 mit dem Einsatz für →Home Office. In vielen Firmen im Einsatz, weil damit auf die →Daten und →Anwendung von →O365 sehr gut zugegriffen werden kann (im Gegensatz zu reinen Webkonferenzlösungen wie →Zoom). Wurde aber auch bei Hochschulen eingeführt da dadurch die →Internet-Anbindung der Hochschulen entlastet wird (direkte Kommunikation zu den →Cloud-Servern)

Telebanking: →MBS, →e-Banking

Telecom Hotel: Siehe →IXP

Telegram: →Open-Source-Projekt, als →Messaging-App genutzt für Einzelkommunikation, aber durch die Option großer Gruppen geeignet für Massenkommunikation (fast) ohne Zensur wie ein →Social Network. Daher finden sich dort Regierungsgegner vieler Länder ebenso wie Rechtsextreme und Angebote für Drogen. Gegründet von Pawel Durow, dem Gründer des russischen Facebook-Klon VKontakte. Telegram hat, um dem Druck der russischen Regierung auszuweichen den offiziellen Sitz in Dubai und keine Adresse bei denen Behörden z.B. Löschaufforderungen oder Ersuchen um Auskünfte oder Sperrwünsche richten können. Der Ruf ist daher ähnlich gemischt wie →TOR.

Telegram ist nicht standardmäßig Ende-zu-Ende-verschlüsselt. Das bedeutet: Telegram könnte in Kommunikationsinhalte hineinschauen. Nur bei Zweier-Kommunikation lässt sich ein „geheimer Chat“ mit Verschlüsselung einstellen. Eine Telefonnummer wird beim Anlegen eines Benutzers verlangt, aber anderen Teilnehmern (im Gegensatz zu →Signal) nicht angezeigt. Telegram ist auf der Suche nach Einnahmequellen.

Telemedizin: Konzepte wie das Fern-Monitoring der Vitalwerte von Patienten im eigenen Haus, zum Teil kombiniert mit Gesprächen über →Videokonfernzsysteme. Bekam →2020 einen guten Anschub, problematisch da es um besonders schützenswerte →Daten geht die zum Teil über Dienste durchgeführt wurden die dafür nicht zugelassen sind. Siehe →e-Health

Telex: Kommunikationsmethode für berufliche Zwecke, ca. 1930 -1980, dann abgelöst durch →Fax. Basierte auf speziellen Geräten, sog. Fernschreiber. Dies waren Schreibmaschinen mit einem Anschluss an ein spezielles Telex-Netz, in dem Buchstaben mit 5 →Bit zu einem anderen Fernschreiber übertragen wurden, 5 bit erlauben nur Großbuchstaben

Telnet: auf dem →IP-Protokoll basierendes Protokoll für interaktives Arbeiten mit Hilfe eines textbasierenden User Interfaces. Da dieses Programm keine Verschlüsselung enthält und auch das Passwort in Klartext überträgt, ist es nicht sehr sicher und seit ca 2010 kaum noch genutzt. →SSH ist eine sichere Alternative

TEMPORA: Programm des britischen Geheimdienst →GCHQ bei dem ein sehr großer Teil der internationalen Glasfaserverbindungen auf denen die Datenverkehr im →Internet beruht, abgehört und ausgewertet werden. Dabei gibt es intensive Zusammenarbeit mit der →NSA, die speziell für das Knacken der →Verschlüsselungen zuständig ist. Siehe auch →PRISM, →Edward Snowden

Tempest: →Lauschangriff auf Informationen unter Ausnutzung der Abstrahlung von elektrischen oder elektronischen Geräten, z.B. →Bildschirmen, →Tastaturen u.ä. oder von Kabeln. Tempest (Transient Electromagnetic Pulse Emanation Standard) bezeichnet eigentlich den Schutz gegen solche →Angriffe. 2015 konnte gezeigt werden, dass selbst aus niedrigfrequenten Abstrahlungen im MHz Bereich →PGP →Schlüssel entziffert werden konnten. Die Geräte lassen sich heute mittels fertiger Komponenten wie →SDR extrem kostengünstig herstellen

Template: (engl. Vorlage) in der →Biometrie die Umwandlung des analogen →biometrischen Merkmales in eine digitale Form. Dabei wird z.B. statt des Images eines →Fingerprints die geometrische Anordnung der Verzweigungen und Unterbrechungen der Linien (ridges) gespeichert

Tencent: Riesiger Internetkonzern in China der (so wie →Alibaba) umfassende Services im Web und vor allem auf →Smartphones anbietet. Ihr Dienst →WeChat umfasst dabei Dienste wie →Social Networks, →Messaging und auch Zahlungsdienste. Ihr Dienst →Weibo ist einer der 2 größten Micro-Blogs in China. Die dabei anfallenden Daten der Nutzer müssen auch mit der Regierung geteilt werden, siehe →Social Credit System

Terahertz Imaging: Nutzung von elektromagnetischer Strahlung mit Wellenlängen im Milimeterbereich, die Kleidung durchdringt und deswegen auch als →Nacktscanner bezeichnet wird. Solche Darstellungen werden zahlreiche →Privatsphäre-Probleme auf, werden vor allem an Flughäfen eingesetzt. Dabei können sowohl aktive Methoden (Abtasten durch einen Strahl und Messung der Reflektion) wie auch passive Methoden (Darstellung der natürlichen Infrarot-Strahlung) genutzt werden

Teredo: Tunneling-Protokoll, mit dem →IPv6-Pakete mit →UDP über IPv4 gekapselt werden. Im Gegensatz von →6to4 kann Teredo auch mit nicht-öffentlichen IP-Adressen arbeiten, kann also mit Geräten hinter einem →NAT kommunizieren. Auf diese Weise können jedoch auch →Angriffe an einer →Firewall oder →IPS vorbei geführt werden. Benutzt Port 3544. Siehe →ISATAP, →TSP, →AYIYA

Terminal: alter Begriff für →Bildschirm. Gemeint waren damit zumeist text-orientierte

Bildschirme die zumeist über →Modem mit einem →Mainframe →Computer verbunden wurden. Berühmt war z.B. das Modell VT100, dessen Schnittstellen und Funktionen sich zu einem Industriestandard entwickelten und von vielen anderen Geräten emuliert wurden, bzw. 3270 für die Geräte die mit IBM-Mainframes verbunden waren. Der Begriff lebt heute in →Terminalserver weiter. Siehe auch →BBS

Terminal wird in der Technik auch als Endpunkt einer Leitung verstanden, z.B. einer Pipeline zur Beladung von Schiffen. In diesem Sinne ist auch das Terminal als Teil eines Flughafens zu verstehen, dort wo statt der Schiffe die Flugzeuge „andocken"

Terminalserver: Konzept um Bildschirminhalte eines →Rechners auf einem anderen Rechner betrachten und nutzen zu können. Implementiert z.B. in Windows Terminal Server (→RDP), →Citrix, Tarantella, GraphOn GO-Global und →VNC. Es wird oft für →Fernwartung und –diagnose genutzt. Stark eingesetzt in 2020 für →Home Office. Ein ähnliches Konzept ist mit dem →VMware Server möglich

Terrorismus: „das öffentliche Töten von vielen Zivilisten mit dem Ziel, Schrecken in der Bevölkerung zu erzielen", von der Statistik her weit überschätzt (verglichen mit realen Bedrohungen wie Autounfall). Wird als Vorwand für viele →Überwachungsmaßnahmen verwendet. Siehe http://sicherheitskultur.at/notizen_2_06.htm#fliegen

Text:

1) Nachrichten auf der Grundlage von Buchstaben, Zahlen und Sonderzeichen. Sehr komprimierte Form der Darstellung. Kann in strukturierter Form (z.B. im → XML-, CSV-Format oder →Datenbank) oder in unstrukturierter Form (als „Fließtext") vorliegen. Die strukturierten Texte sind beser maschinell auswertbar. Darstellung auf der Basis von Codierungen, z.B. →ASCII, →UTF-8
2) Englisch fürb →SMS

Texting: Versenden von kurzen Nachrichten entweder per →SMS, oder über →Chat- oder →Messaging Protokolle wie →WhatsApp und →Twitter, aber in der Variation →Sexting vor allem über →SnapChat

TFTP: (Trivial File Transfer Protocol) sehr einfaches Programm für Dateiübertragung auf der Basis von →UDP, sehr oft genutzt in → embedded systems für Konfigurationsdateien

Thin Client: Konzept, bei der Anwendungen mittels eines standardisierten Clients (Hardware oder Software) dargeboten werden, statt über eine →Client-Server Implementierung (→fat-client), die für jede Anwendung ein spezielles Client-Programm benötigt. Implementierungen auf Basis von →Citrix oder →Webbrowsern. Vorteil des Konzeptes ist die leichtere Wartbarkeit der Anwendungen und das Vermeiden von →VPN für →remote access, siehe auch →ICA. Auch ein →Webbrowser ist ein Thin Client

Threat: →Bedrohung

Threat Modelling: Methode die von →Microsoft propagiert wird um Bedrohung von Software, z.B. Websites, systematisch zu erkennen. →Risikomanagement. http://msdn.microsoft.com/security/securecode/threatmodeling/default.aspx

Three-strike-Verfahren: (three strikes out) →Hadopi

Thumb Drive: (engl. für →USB-Stick)

TIA: (→Terrorism Information Awareness) 2002 gestartetes US-Programm zur Sammlung von personenbezogenen Daten und Erstellung von Personenprofilen mittels →Datamining in (auch kommerziellen) Datenbanken, z.B. →Axciom, 2003 vom Congress gestoppt. Lebt heute weiter als →Matrix, bzw. Tangram, bzw. die vielen anderen Aktivitäten der →NSA. Siehe http://www.cio.com/archive/080104/cold.html

Tibco: Anbieter von →Messaging Software

TIFF: Format für →Dateien mit grafischen Inhalten. Kann wie fast alle grafischen Formate →Schadsoftware enthalten. Siehe →JPEG, →GIF

tiger team: *n. [U.S. military jargon]*

1. ursprünglich ein Team, das durch Eindringen in militärische Einrichtungen deren Sicherheit testet. Siehe →red team

2. heute auch oft gebraucht für ein Team, das eine Inspektion jeglicher Art durchführt oder eingesetzt wird, um eine schwierige Situation zu lösen

TikTok: →Social Network Dienst der vor allem von jungen Nutzer genutzt wird. Primäres Merkmal sind kurze Videos die oft für Karaoke-Darstellungen genutzt werden. Seit 2016 in China aktiv, ab 2017 unter dem neuen Namen weltweit angeboten. Unter jungen Leute weltweit in 2019 extrem populär

Timeout: in der IT: wenn nach einer vorgegebenen Wartezeit ein Ereignis ausgelöst wird, z.B. das Sperren eines →Bildschirms

Time Server: zentrale Rechner im →Internet, die von einer offiziellen Referenzuhr die Zeit erhalten, z.B. über Langwelle und von dem andere Geräte die aktuelle Zeit abfragen können. Diese Abfrage geschieht in der Regel über →NTP. Solche Server stehen im →Internet kostenlos zur Verfügung. Wichtig z.B. für die Synchronisierung von →Log-Informationen

Time stamp: →Zeitstempel

Tinfoil hat: (engl. Aluminiumhütchen) abwertender Begriff für Personen mit extremer Paranoia, basiert darauf, dass der

Aluminiumhut vor fremden Strahlungen schützen soll

TKIP: (Temporal Key Integrity Protocol) in →Wireless Networks in den Standards IEEE 802.1x, 802.11i und →WPA für die →Authentifizierung verwendet werden. Es schließt einige Sicherheitslücken in →WEP, wurde jedoch 2008 geknackt. In WPA sollte stattdessen →CCMP

TKÜ: Telekommunikationsüberwachung. →Abhören von →Telefon oder →E-Mail

TLP: (traffic light protocol) in der IT-Security übliches Schema um die →Vertraulichkeit von Security Informationen zu bezeichnen:

RED – nur für namentlich genannte Empfänger

AMBER – für andere in derselben Organisation die für diese Inkformation einen „→need to know" haben

GREEN – innerhalb einer beschriebenen Community, nicht für Veröffentlichung oder anderweite Verbreitung

WHITE – unterliegt nur den →Copyright, bzw. Urheberrechten

TLS: (Transport →Layer Security) →Protokoll zur Absicherung von →Internetverbindungen durch Verschlüsselung. Nachfolge und Erweiterung von →SSL seit 2006 (SSL und TLS sind sehr ähnlich, aber nicht kompatibel). Moderne →Webbrowser unterstützen beides, ebenso die meisten Mailserver die das →SMTP-Protokoll unterstützen (siehe →MTLS). Zu den Schwachstellen bei der Nutzung von TLS siehe →SSL). TLS enthält Compression, was für den sog. CRIME-Angriff genutzt wird. Siehe →Sovereign Keys, →HSTS

TLS state: seit 2018 sind fast alle →Websites mit TLS verschlüsselt und nun werden TLS session IDs und session tickets für das →Tracken von Personen im →Web verwendet

TNC: (Trusted Network Connect) standardbasiertes Konzept der →TCG mit dem Ziel →Endpoint Security, d.h. Überprüfung des Sicherheitsstatus von Endgeräten bevor diese in ein Firmennetz gelassen werden. Bisher sind diese Standards jedoch erst teilweise definiert und erfordern den Sicherheitschip →TPM

TOE: (Target of Evaluation) Konzept der →Common Criteria. Bei einer Sicherheitsbewertung muss das Gesamtsystem betrachtet werden, nicht nur die Einzelkomponenten

TOGAF: (The Open Group Architecture Framework) Rahmenvorgaben für eine IT-Architektur für Unternehmen. Die 4 Hauptbereiche sind: Business, Application, Data, Technology

Token: (engl. Zeichen, Gutschein, Spielmarke). oft verwendet im Zusammenhang mit →Authentisierungsverfahren.

1) Token-basierte Authentisierung nutzt ein Gerät, das auf elektronischem Wege ein →Einmalpasswort (→OTP) zur Verfügung stellt. Beispiel: →RSA SecureID oder Geräte von Vasco, Kobil, Gemalto

2) Datenobjekt das ausgetauscht wird, z.B. verwendet für →Authentisierung, siehe →SAML, →OAuth, →Kerberos

Tokenization:

a) Technik, bei der z.B. bei einer →Kreditkartentransaktion nach der →Authentisierung durch den Herausgeber der Karte die Kreditkartennummer durch eine 16-stellige Zufallszahl ersetzt wird. Der Händler kann für spätere Referenzen diese Zahl statt der Kreditkartennummer speichern ohne →PCI-DSS zu verletzen

b) Bei der Analyse von natürlicher Sprache das Zerlegen von Text in einzelne Elemente, die dann z.B. einer lexikalischen Analyse zugeführt werden können

Token Ring: ältere Netzwerktechnologie (ab 1980), →IEEE 802.5, heute von →TCP/IP fast vollständig abgelöst

Toll fraud: →Angriff vor allem bei Telefonie (auch →VoIP) oder durch →Premium SMS bei dem das Opfer die Gebühren für Dienste für andere übernimmt

Toolbar: zusätzliche Zeile unterhalb der Menüleiste in Bildschirmfenstern, die zusätzliche Funktionalitäten anbieten, z.B. leichter erreichbare Such-Funktionalitäten. Das Angebot solcher Toolbars wird zum Teil für die Installation von →Malicious Code benutzt

Toolkit: (engl. Werkzeugkasten) in der IT-Security oft eine Sammlung von →Angriffswerkzeugen. Beispiele sind Mpack, NeoSploit, IcePack, WebAttacker, WebAttacker2, Multi-Exploit, random.js, vipcrypt, makemelaugh, dycrypt

TOR: (The Onion Router) →Anonymisierer, der auf dem →Proxy-Prinzip beruht und verhindern soll, dass ein Benutzer, der z.B. eine →Website besucht, über seine →IP-Adresse identifiziert werden kann. Dies ist zum Schutz von bedrohten Personen wichtig, z.B. Oppositionelle in Polizeistaaten, aber z.B. auch Menschen (speziell Frauen), die bedroht werden. Die Tatsache, dass TOR die IP-Adresse verschleiert, wird auch als unlinkability bezeichnet.

Um dies zu erreichen wird der Datenverkehr zwischen mehreren, zufälllig ausgewählten Rechnern (TOR-Knoten), die alle die TOR-Software enthalten, verschlüsselt weiter übertragen, so dass der Datenverkehr dann an einer anderen, nicht nachvollziehbaren Stelle im Internet (unverschlüsselt) wieder auftaucht.

Dadurch wird die →IP-Adresse des Senders verschleiert. Zusätzliche →Verschlüsselung der Daten vom Browser des Benutzers zum Zielrechner (→End-to-end) ist notwendig, um →Vertraulichkeit zu erreichen. Die Entwicklung von TOR als →Open Source wird ca.60%

durch die US-Regierung gefördert, um damit freie Meinungsäußerung in Diktaturen zu fördern.

TOR ist nicht zum Schutz gegen →Global Adversary ausgelegt. Es ist angreifbar, z.B. durch die →NSA, der diese Anonymität durch eine umfassende Analyse der Datentransfers unter zeitlichen Aspekten „knacken" kann. Wenn der Datenverkehr an vielen Stellen im Netz gesammelt und ausgewertet wird, so lässt sich ein sehr großer Teil der Daten zuordnen. Identifzierung der Nutzer ist aber auch über →Device Fingerprinting möglich, speziell weil die Tatsache der TOR-Nutzung bereits eine weitgehende Einengung der Nutzerzahl darstellt. →Anonymität im Internet ist nicht wirklich möglich. Für →Whistleblower-Aktivitäten ist TOR empfehlenswert

Eine Verwendung für illegitime Zwecke sind TOR-basierte →Botnets. Siehe →WikiLeaks, →TOR Hidden Service

TOR Hidden Service: →Website, die über eine spezielle →Onion-→Domain-Adresse erreichbar ist (xxxx.onion statt xxxx.com). Dadurch kann der Datenverkehr vom TOR-Netz direkt zum →Webserver fließen und dieser Webserver ist im „richtigen" →Internet unter Umständen gar nicht sichtbar. 2013 gelang es dem FBI trotzdem, die Handelsplatform Silk Road „vom Netz zu nehmen" und die Betreiber zu verhaften. Die Summe der Websites mit .onion Domain-Adressen wird auch oft als „→DarkNet" bezeichnet. Die Suchmaschine Grams will seit 2014 diese Services ähnlich zu →Google indizieren, die Ergebnisse beruhen jedoch auf Selbst-Meldungen der Betreiber. Auf vielen dieser Websites werden illegale Produkte angeboten, daher werden sie immer wieder von Strafverfolgungsbehörden geschlossen (→ darknet market, →OpenBazaar). →Freenet verfolgt eine andere Intention.

TOTP: (Time-based One-time Password algorithm) Erweiterung von →HOTP, benutzt in vielen →2 Faktor Authentisierungen. Dabei wird auf der Basis der Uhrzeit und einem eindeutigen Wert für dieses Gerät ein →Passwort berechnet, das sich in regelmäßigen Intervallen, z.B. 30 Sekunden, verändert. Um Zeitungenauigkeiten zur berücksichtigen verwenden manche Implementierungen ein längeres Zeitfenster, was aber die Gefahr von →Replay-Attacken erhöht. Siehe auch →keyless system das für Autos und Gebäude verwendet wird aber anders funktioniert

Touch ID: Feature von moderneren →iPhones bei der ein integrierter →Fingerprint-Leser für das Entsperren des Geräts genutzt werden kann. Der →Chaos Computer Club konnte bereits mehrfach zeigen, dass Fingerabdrücke keine sichere →Authenisierungsmethode sind, da Fingerabdrücke nicht vertraulich sind. Sie sollten nur als zusätzliches Element eingesetzt werden. Mittels Touch ID können 2014 auch die Zahlungen von Apple Pay autorisiert werden. Die Fingerprint-Daten werden in einem →Secure Element gespeichert und sind daher nicht direkt auslesbar.

TPM: (Trusted Platform Module) Chip zur kryptographischen Absicherung von Rechnern mittels Sicherheitsoperationen wie digitale →Signatur geeignet ist (→Secure Element). Dazu gehört die Generierung von →Schlüsselpaaren, das Erstellen von →Hashes und deren Signatur. Kritisiert wird an TPM-Implementierungen, dass solche Techniken auch verwendet werden können, um alternative →Betriebssysteme wie z.B. →Linux, von Rechnern fern zu halten indem im UEFI nur die →Signaturen eines oder mehrerer Hersteller implementiert sind. Das System würde dann jedes andere Betriebssystem als „→Infektion" betrachten. Zum Thema wird TPM da Windows 11 TPM 2.0 als Voraussetzung haben wird. Siehe →TCG, →TXT

TPMS: (Tire Pressure Monitoring Systems) System zur drahtlosen Übertragung des Reifendrucks zu einem Computer im →Auto. Erfordert →Pairing der 4 →Sensoren mit dem TPM-controller (ECU). Die ID des Sensors lässt sich für →Überwachungszwecke nutzen. Mittels →GNU-Radio und →USRP lassen sich unautorisierte Kommandos zu dem System übertragen. In den USA für neue Fahrzeuge bereits Pflicht, in der EU geplant

TQM: (Total Quality Management) umfassendes →Qualitätsmanagement. Das Konzept von Qualitätsmanagement wurde in den 40iger Jahren in den USA entwickelt (William Edward →Deming), jedoch erst in den 50igern in Japan stark eingesetzt. Sicherheitsrelevant, da Qualität und Sicherheit stark miteinander verzahnt sind. Siehe →Six Sigma, →FMEA

Traceroute: Diagnostic Programm für →TCP/IP Verbindungen. Zeigt, auf welchem Weg von →Router zu Router die Daten in einem konkreten Fall durch das →Internet transportiert wurden. Sendet →UDP-Datagramme mit manipulierten IP-Time-to-live-(TTL)-Header-Feldern und sucht nach →ICMP-Meldungen „Time to live exceeded in transit" und „Destination unreachable" in den Antworten

Track 2: Bei →Bankomatkarten und →Kreditkarten eine der beiden Spuren auf dem Magnetstreifen. Beim →Skimming wird diese Spur ausgelesen. Sie enthält alles was benötigt wird, um eine gefälsche Karte irgendwo auf der Welt zu erstellen und dort einzusetzen, wo →EMV noch nicht im Einsatz ist

Tracking:

a) Tracken physischer Bewegungen durch Peilsender, z.B. auf →GSM-basis (→Handys) oder auf Grund der →Standort-Daten die bei Telefonbetreibern routinemäßig

anfallen und durch die →Vorratsdaten-speicherung erfasst werden. Ab ca. 2016 weitgehend durch das Anbieten von kostenlosen WLANs, bei denen sich Handys mit ihrer →MAC-Adresse anzmelden versuchen

b) Tracken von Benutzer-Aktivitäten im →Internet durch →Advertising Networks, z.B. durch das Setzen von →Cookies, →Flash Cookies, →HTML 5 Storage oder web-bugs beim →Webbrowsen. Ziel ist →behavioural advertising. Es können Benutzer oder Geräte getrackt werden. Technische Details unter →web bug. Einige Internetnutzer versuchen Tracking zu verhindern durch →Opt-Out, →DNT-Header oder →Blocking Tools. Siehe auch →data mining, →Private browsing, → UDID, →IDFA, →Retargeting, →stateless tracking, →device fingerprint, →Canvas Fingerprinting, →Advertising ID, →Tracking Pixel, →Access Point, http://sicherheitskultur.at/spuren_im_internet.htm

Tracking Pixel: (→Web bug)

Traffic Diversion: Nutzung von fremden Brandnames in Text (auch unsichtbar), Titel, →Meta-Tags einer →Website um durch →Suchmaschinen höher als der eigentliche Brand eingestuft zu werden, ähnlich zu →Cybersquatting und damit Verkehr zu dieser Website umzuleiten

Transaction log: Protokoll der Änderungen in einer →Datenbank. Verwendet für die →Wiederherstellung.Siehe auch →Journal

Transaktionsdaten: generell →Daten über Transaktionen, z.B. Verkäufe oder →Kommunikationen. Dies können die eigentlichen Inhaltsdaten der Transaktion sein, z.B. bei einem Verkauf, oder →Metadaten. wie bei einer Kommunikationsverbindung. Auswertungen beider Arten von Daten können leicht die →Privatsphäre beeinträchtigen. Siehe →Data Retention, →Vorratsdatenspeicherung

Transhumanismus: Denkrichtung die die Grenzen menschlicher Möglichkeiten durch den Einsatz technischer Mittel erweitern will. Diese Denkrichtung ist sehr aktiv rund um die IT-Firmen in Silicon Valley. Dabei werden je nach Forschungsreichtung Aspekte der AI-Forschung (z.B. „starke AI“) mit →brain-computer interface Forschungen und →Neuroprothesen kombiniert und über Konzepte wie das „Hochladen“ von menschlichem Bewusstsein in Maschinen zum Zwecke der Unsterblichkeit nachgedacht. Es gibt aber grundlegenede Zweife daran, dass so etwas ja funktionieren könnte: https://www.newscientist.com/article/mg24532652-900-uploading-your-brain-will-leave-you-exposed-to-software-glitches/

Die EU unterstützt ein Forschungsprojekt VERE (virtual embodiment and robotic re-embodidment) bei dem die Grenzen zwischen Mensch und Maschine aufgehoben werden sollen, das ähnliche Aspekte zu behandeln scheint

Trello: Projektmanagement →Software für gemeinsames Arbeiten in Arbeitsgruppen

Tripwire: Programm, das durch kontinuierliche Überwachen eines Rechners sicherstellen soll, dass keine unautorisierten Veränderungen vorgenommen werden. Ist als kommerzielles Produkt und als →Open Source verfügbar. Siehe →Change Management, →Monitoring

Trojaner: bzw. besser Trojanisches Pferd, (historisch das Holzpferd, mit dem es Odysseus gelang, sich →Zutritt zur stark befestigten Stadt Troja zu erschleichen). In der modernen Fassung ein →Programm, das vordergründig eine definierte Aufgabe erfüllt, aber zusätzliche verborgene Funktionen enthalten. So werden bei der Installation von →Freeware sehr oft zusätzliche Programme installiert, oft wird sogar korrekt im →EULA darauf hingewiesen. Im harmlosesten Fall ist dies →Adware, aber es kann auch →Spyware oder →Backdoor-Software sein. Im Finanzbereich gegen →e-Banking werden vor allem →Zeus und →SpyEye eingesetzt. Siehe →Form-grabbing, →Webinject, →CIPAV, →Bundestrojaner

Troll: (nord. Sagenwesen, Unhold) im →Internet jemand, der in Diskussionsforen, per →E-Mail oder ähnlichem andere Personen oder Gruppen gezielt provoziert, bis hin zu Todesdrohungen und →Cyberbullying. Sicher sehr oft unethisch, nur in Ausnahmefällen derzeit strafbar. Trolls wird mit den Persönlichkeitsmerkmalen Narzissmus, Psychopathie und vor allem Sadismus in Verbindung gebracht

Trollfabriken: Firmen die eine große Zahl von Menschen damit beschäftigen, auf →Social Networks und anderen Plattformen Stimmung für oder gegen etwas zu tun. Dabei können zur Verstärkung der Wirkung auch →Social Bots zum Einsatz kommen. Eine bekannte Trollfabrik ist die Internet Research Agency (IRA) in Petersburg

TrueCrypt: kostenloses →Open Source →Verschlüsselungsprogramm für Datenspeicher. Wurde 2014 überraschend von den Entwicklern als unsicher zurückgezogen, Gerüchte besagen, dies wäre evtl. auf Druck von Regierungsbehörden geschehen- ist daher zum Teil noch im Einsatz. Legt verschüsselte Container an in denen ein →Dateisystem „versteckt“ ist, das über eigenen Laufwerksbuchstaben verfügbar ist. Kann daher auch mit →Cloud-Speichern genutzt werden, die ein „mappen“ auf Laufwerksbuchstaben erlauben. Unterstützt auch →Hidden Volumes, d.h. ein →Deniable File System, Version 6 unterstützte ein →Deniable Operating System. Als Nachfolgeprogramm positioniert sich das ebenfalls Open Source Program VeraCrypt

Trust: wichtiges Konzept der Informationssicherheit: welchen Personen, →Systemen oder →Stellen darf vertraut werden, darf man sich verlassen. Ohne Trust in irgendwas ist keine Sicherheitsimplementierung möglich. Siehe →Certificate Authority, →Reputation System, →SAML, →virtual currency, →Web-of-Trust

Trust Boundary: →Sicherheitskonzept, dass nur solche Teile einer →Client-Server Anwendung (d.h. auch →web-browser-basiert) außerhalb sicherer Umgebungen liegen dürfen, deren Manipulation keine Sicherheitsverletzungen darstellen kann. D.h. sicherheits-relevante Daten oder Programmteile dürfen nicht im Benutzerzugriff sein, z.B. in der Form von →JavaScript. Siehe →Jericho Forum

Trust Center: →Certificate Authority

Trusted Computing Platform: →TCG

Trusted Execution Technology: Sicherheitskonzept von Intel für zukünftige Prozessoren. Beinhaltet spezielle Instruktionen, →Virtualisierungen und →TPM. AMD arbeitet an einem ähnlichen Konzept

Trusted Storage: Spezifikation der →TCG zur Verwendung von →TCM in Verbindung mit →Verschlüsselung oder →Zugriffsschutz z.B. für →Festplatten

Trusted System: 1) im Security Engineering ein System, dem vertraut werden MUSS, weil eine Verletzung die Gesamtsicherheit gefährden würde. D.h. es müssen besondere Sicherheitskriterien angelegt werden, z.B. was die →Authentisierung der →Benutzer betrifft. Ebenso sind → Risikoanalysen notwendig. Siehe →Security Envelopes

2) ein System, das über einen →TPM authentisiert ist

TSA: (Transportation Security Organisation) US-Behörde für die Zivilluftfahrt. Siehe →CAPPS II

TSP: (Tunnel Setup Protocol) eine der Möglichkeiten, →IPv6 Datenverkehr durch →IPv4 Netze zu tunneln, benutzt →Port 3653. Siehe →Teredo, →AYIYA

Turaya: →open-source Software zur Unterstützung von →TPM als Alternative zu →NGSCB, erstellt durch →EMSCB. Turaya-Crypt erlaubt z.B. die →Verschlüsselung von Daten oder Geräten und Turaya-VPN verschlüsselt Verbindungen

TURBINE: →NSA Aktivität mit deren Hilfe seit ca 2013 →TAO →Implants automatisiert auf vielen Millionen →Rechnern installieren und verwalten kann

Turing Complete: in der Informatik ein System zur Manipulation von →Daten (Instruktionssatz eines →Computers, Programmiersprache oder manuelles Regelwerk), mit dem eine →Turing Machine implementiert werden kann

Turing Machine: theoretische (mathematische) „Konstruktion“, die Symbole auf einem Speicherstreifen manipulieren kann, die Grundlage für alle unsere heutigen digitalen →Computer. Turing hat mathematisch gezeigt, dass eine solche Maschine jede andere Maschine emulieren kann (sofern sie über geeignete maschinelle Peripherie verfügt), was wir bei den heutigen Computern immer deutlicher sehen: Jeder Computer kann alle Aufgaben lösen, die von einem Computer lösbar sind (Beschränkungen liegen lediglich in der benötigten Rechenzeit, d.h. es gibt neben der Geschwindigkeit und Speichergröße keine grundsätzlichen Unterschiede zwischen →Smartphone und →Supercomputer). Siehe →Turing Complete, →P-NP-Problem

Turing Test: vom britischen Mathematiker Alan Turing in den frühen fünfziger Jahren entwickeltes Konzept, mit dessen Hilfe entschieden werden soll, ob ein Rechner als intelligent zu bezeichnen ist. Dabei geht es darum, dass ein Mensch nicht mehr erkennen können soll, ob er mit einem anderen Menschen oder dem Rechner kommuniziert. Wird seit einigen Jahren in der Form von →Captchas von Anbietern wie yahoo oder hotmail gegen →Spammer eingesetzt. Siehe →AI,
http://philipps-welt.info/Turing Test.htm

TVSS: (transient voltage surge suppressor) Siehe →SPD

Tweet: eine Kurznachricht in →Twitter

Twitter: →Social Network (ähnlich zu →Blog), bei dem Nachrichten von früher max. 140 Zeichen, jetzt 280, an alle „Follower“ versendet werden (→Micro-Blogging). →Socialbots auf Twitter werden eingesetzt um Meinungen und/oder Verhalten von Followern zu beeinflussen. 1% der Twitter-User erzeugen 30% der →Tweets, d.h. auch dieses Medium wird von wenigen Benutzern dominiert und lässt sich für Manipulationen nutzen (z.B. →Twitter Bombe). So wurde in 2012 in Indien eine Panik ausgelöst und falsche Tweets zur Lage in Syrien wurden erfolgreich genutzt um den Ölpreis zu beeinflussen. Außerdem ist es in prominenten Kreisen üblich, sich über entsprechende Services falsche Follower zu kaufen, ähnlich zu →sock-puppets. Die automatisierte Auswertung von Tweet verrät leider sehr viel über die Persönlichkeit von Personen, siehe →Big Five. 2014 gab Twitter zu, dass 23 Mio, d.h. 8,5% seomer 270 Mio account „fake“ sind. Siehe auch →Click farm. 2019 gehört Twitter (noch) zu den →walled garden Diensten, man erwägt aber, sich für ein föderatives Netzwerk zu öffnen, z.B. →Fediverse (siehe auch → Direct Market Act). Seit verstärkt rechtsradikale oder rassistische Inhalte zu Sperrungen führen weichen diese Nutzer auf Gab oder →Parler aus

Twitter Bombe: das Absetzen von Botschaf-

ten („→tweets“) mit dem gleichen Hashtag (#) um eine bestimmte Idee oder Information (Falschinformation) zu verbreiten, z.B. im Rahmen von Wahlen. Dabei kommen u.a. →Fake Accounts oder →Sock Puppets zum Einsatz. Bei einem Vorfall erzeugten 9 Fake Accounts 929 →Tweets in 138 Minuten, über Re-Tweets wurden 60 000 Benutzer erreicht bevor Twitter diese Bombe stoppte

TXT: (→Trusted Execution Technology)

Typosquatting: Registrieren von →Domain Namen mit Variationen der Namen anderer →Websites (z.B. einzelne Buchstaben ausgelassen, ‚wwwname' statt ‚www.name', ‚.cm' statt ‚.com' u.ä.). Ziel ist es, Besucher auf → Websites zu locken auf denen i.d.R. Werbung angeboten wird. Mittels →Pay-per-Click kann dann Geld verdient werden. Siehe →Domain Squatting, →NXDOMAIN

U2F: (→Universal 2nd Factor)

UAC: (→user account control)

UAF: →Universal Authentication Framework protocol

UAM: (User Access Management) Verwaltung der →Zugriffsrechte der Anwender zu Systemen, Anwendungen und Netzen, auch zum →Internet (→Proxy)

UAV: (unmanned areal vehicle) (deutsch: →Drohne, drone) unbemanntes Fluggerät, genutzt für visuelle →Überwachung, aber mittels Funktionalitäten wie →GILGAMESH auch für →Handy-Ortung und →VICTORY-DANCE für →WLAN-Ortung. Können zum Teil mittels →GPS autonom fliegen, werden aber zumeist aus der Ferne gesteuert, was eine hohe Bandbreite erfordert. Ab 2009 stellen in den USA die UAV-Piloten die Mehrheit aller Militärpiloten. UAVs werden in Nicht-Kriegsgebieten auch für Tötungen eingesetzt, oft lediglich auf Grundlage von →SIGINT, d.h. Auswertung von →Metadaten mit hoher Fehlerrate

UBE: (Unsolicited Bulk E-Mail) vornehmer Ausdruck für →Spam

Uber: US-Unternehmen, das 2015 auch in Europa aktiv wird. Mittels einer Smartphone App können Benutzer eine Taxifahrt bestellen, die jedoch sehr oft von nicht-lizensierten Privatleuten angeboten wird. Problematisch ist u.a. dass sowohl Fahrer wie Mitfahrer bewertet werden und diese Bewertungen anderen Benutzern der App zur Verfügung stehen, so dass sie sich entscheiden können, ob sie die Fahrt annehmen. Taxiunternehmen wehren sich gegen diese Konkurrenz. Die Preise für Fahrten mit Uber hängen von Angebot und Nachfrage ab und werden frei ausgehandelt

Überwachung: Beobachtung von Personen oder Orten, entweder durch direkte Beobachtung (→Videoüberwachung, →Webcam, →CCTV) oder durch Auswertung seines Verhaltens, z.B. durch →Abhören der Kommunikation, Auswertung von elektronischen Fahrscheinen, der Spuren im →Internet (→Data Mining) oder der Sprachkommunikation (→Data Retention), heute zumeist durch den Einsatz von →IKT. Führt zu einem Verlust an →Privatsphäre. Früher ein Privileg des Staates (→Surveillance), heute auch durch Private und Firmen (→Suchmaschinen, Speicherung des Kaufverhaltens auf →Website, etc., →Sousveillance), →Lawful Intercept, → Quellen-TKÜ, →Überwachungskapitalismus, →Überwachungssoftware, →Spyware, →Spy-App

Überwachungskapitalismus: Schlagwort geprägt von Shoshana Zuboff in ihrem Buch ‚Das Zeitalter des Überwachungskapitalismus' mit dem sie beschreibt, dass die großen Datensammler (→Google, →Amazon, →Facebook, →Microsoft, u.a.) ausreichend Daten über jeden Nutzer des →Internets sammeln um eine Persönlichkeitsanalyse und →Emotionserkennung durchzuführen, sehr gezielte Werbung zu platzieren (→behavioural advertising) und sogar in gewissem Maße eine Steuerung der Menschen zu erreichen. Dies ist ein äußerst lukratives Geschäftsmodell das seit ca. 2010 alle anderen Bereiche der Wirtschaft zu dominieren beginnt. Für China siehe →Social Credit System

Überwachungssoftware: →Spy-App

Überwachungsstaat: ein Staat der seine Bürger mit allen zur Verfügung stehenden und staatlich legalisierten Mitteln überwacht. So sollen Gesetzesverstöße besser und schneller erkannt und verfolgt werden. Befürworter führen die Verhinderung von Straftaten, →organisierter Kriminalität und →Terrorismus an. Nächste Stufe ist dann der →Präventionsstaat. Siehe →Big Brother

UCE: (Unsolicited Commercial E-Mail) vornehmer Ausdruck für →Spam

UCS: (Universal Character Set) Implementierungsoption(en) von →Unicode. Sie unterscheiden sich durch die Zahl der bits pro Einheit. Beispiele: UCS-4, UCS-2. UCS-2 benutzt bei Bedarf eine weitere Speichereinheit

UDDI: (Universal Description, Discovery and Integration) auf →SOAP basierendes Verfahren, mit dessen Hilfe eine Anwendung selbstständig erkennen kann, auf welche Weise Dienste auf einer anderen →Website genutzt werden können

UDID: (Unique Device Identifier) eindeutige Identifizierung der →iOS-Geräte von →Apple. Die UDID war vor iOS 6 für →Apps verfügbar und wurde daher gern für →Tracking von Benutzern über mehrere Apps hinweg eingesetzt. Das soll mit iOS 6 nicht mehr gehen, jede App wird eine spezifische ID dafür haben. Zusätzlich wird die →IDFA eingeführt, die wieder Geräte-Tracking erlaubt

UDP: (User Datagram Protocol) Mitglied der

→IP-Protokoll-Familie. Es ist „verbindungslos“ und wird zusammen mit →TCP/IP im Internet eingesetzt. UDP wird z.B. verwendet für DNS, Multimedia-Streaming und für einige Multi-Player Spiele (→MMORPG)

UDP hole punching: u.a. von →Skype verwendetes Verfahren zum Aufbau von Sitzungen zwischen Rechnern hinter →NAT-→Firewalls. Dabei verbinden sich beide Teilnehmer zuerst mit einem „supernode“ der nicht hinter NAT ist. Dieser teilt dann beiden Teilnehmern die Verbindungsdaten des anderen Teilnehmers mit und ermöglicht damit ein Durchdringen des Firewalls. Siehe →STUN

UDRP: (Uniform Domain Name Dispute Resolution Policy) Vorgehensweise der →ICANN bei Disputen zu →Domain Name Fragen, z.B. →Domain Parking

UEFI: (Unified Extensible Firmware Interface) Nachfolge der →BIOS-→Firmware die zum Starten eines Intel-→PCs verwendet wird. Durch ein Verhindern des →Bootens von „untrusted“ →Betriebssystemen wird manchmal der Boot von →Linux, auch von CD, verhindert. Wenn UEFI auf „→secure boot“ eingestellt ist, so können nur digital signierte Installationsmaterialien verwendet werden können, was z.B. auch ältere Versionen von MS →Windows verhindern würde. Details unter →TPM

UICC: (Universal Integrated Circuit Card) von der →ETSI standardisierter Typ von →Smartcard zu der auch →SIM-Karten von →GSM-→Handys gehört und die →USIM für →UMTS-Netze gehören. Beispiel für ein →secure element. Soll als sicherer →Speicher für →MCP-Lösungen genutzt werden. Leider fehlen 2014 in →Smartphones secure elements, die von →Apps genutzt werden könnten. Siehe auch →eUICC

Ultra-Wideband: (UWB) Funktechnik die z.B. bei →Apple →Airtags eingesetzt wird. Dabei kommen sehr geringe Energiemengen zum Einsatz, das Verfahren ist für Ortungen oder zum Aufbau von →PANs

UM: (→Unified Messaging)

UMA: (→Unlicensed Mobile Access)

UMTS: (Universal Mobile Telecommunications System) 3. Generation von Mobilfunktechnologie. Ermöglicht höhere Datenübertragungsraten und hat eine deutlich bessere Sicherheit gegenüber Abhören und anderen →Angriffen auf Datenübertragungen als →GSM und →GPRS. Siehe →HSDPA, →3G

Undo: Operation um einen früheren Stand zu erreichen, z.B. nach einem Fehler. Siehe →after image

Unicast: das im Internet üblicher Verfahren für das →Streamen von Musik und Videos. Die Nicht-Linearität bedeutet, dass Inhalte als Unicast übertragen werden müssen, d.h. wenn 1000 Personen dasselbe Video schauen, so muss der →Server trotzdem die Inhalte 1000x über die Leitungen senden. Deswegen werden die Inhalte möglichst nahe bei dem Empfängern auf →CDN-Servern gespeichert. Trotzdem stellen Videodaten mittlerweile ca. 80% des →Internet-Verkehrs dar

Unicode: Verfahren der Textdarstellung, das ca. eine Million Zeichen unterstützt, d.h. auch asiatische Alphabete und die vielen neuen Smileys. Nachfolger von →ASCII (nur 7 bit, US-Zeichensatz), verschiedenen ISO 8859 Variationen, die jeweils länder-, region- oder sprachspezifische Zeichensätze definieren, z.B. ISO8859-1 für Westeuropa. Auf technischer Ebene sind viele unterschiedliche Implementierungen vorhanden, z.B. (→UTF (Unicode Transformation Format) und →UCS (Universal Character Set). Sie unterscheiden sich in der Zahl der bits pro Zeichen. Beispiele sind UTF-32, UTF-16, UTF-8, UTF-EBCDIC. →URLs, die in Unicode sind, können für →Phishing-Angriffe verwendet werden, da auf diese Weise →Domain-Namen verschleiert, bzw. imitiert werden können (z.B. kyrillisches a statt westliches a, gleiche Darstellung, aber andere Web-→Domain, d.h. andere →Website). Eine gute Erklärung findet sich neben der Wikipedia auf https://www.golem.de/news/drei-jahrzehnte-unicode-alles-ausser-klingonisch-2203-163340.html

UNCID: (Uniform Rules of Conduct for the Interchange of Trade Data by Teletransmission) einheitliche Durchführungsregeln für den Handelsdatenaustausch via Telekommunikation, entwickelt durch die Internationale Handelskammer (→ ICC)

Unified Messaging: Zusammenfassung von →E-Mail, →Instant Messaging, →Fax, Videoconferencing, →Voicemail und →VoIP in einer Anwendung. Siehe →OCS, →Presence Server

Unit Key: Möglichkeit des →Link Keys bei der Herstellung eines →Pairings zwischen zwei →Bluetooth-Geräten. Unit Keys bleiben permanent gespeichert und können ein Sicherheitsrisiko darstellen

Universal 2nd Factor: (U2F) von →Google vorgeschlagener (und im Google Authenticator implementierter) Standard für →2-Faktor-Authentisierung, 2014 übernommen von →FIDO Alliance. Es sollen →USB oder →NFC Geräte genutzt werden, und kryptografisch ähnlich zu →Smartcards sein. Bei Google ist dies für →PCs und →Laptops über →USB-Stick und für →Smartphones über →Bluetooth implementiert.

Universal Authentication Framework: eine der von der →FIDO Alliance vorgeschlagene →Authentisierungsmethode, die →Passworte ersetzen soll

UNIX: Betriebssystem, das bereits 1969 von Bell Labs entwickelt wurde. Im Laufe seiner bewegten Geschichte wurde der →Quellcode speziell an Universitäten stark weiterentwickelt.

Heutige Implementierungen sind Solaris von Sun, AIX von IBM, HP/UX von HP und →Linux, das von einer →Open Source Community ehrenamtlich gepflegt und weiterentwickelt wird. Auf Grund der Beliebtheit, besonders in der akademischen Welt, wurden auf UNIX viele Sicherheitstechnologien entwickelt

Unlicensed Mobile Access: (UMA) Roaming zwischen →Bluetooth, →GSM, →UMTS und →WLAN-Netzen. Heute meist →Generic Access Network (GAN). In Verbindung mit anonymen →SIMs ermöglicht dies anonyme →Angriffe auf →VoIP-Systeme

Unterlassungsanspruch: →Haftung eines →Diensteanbieters (z.B. Betreiber einer →Website) für das Entfernen von unerlaubten Inhalten (auch z.B. Beleidigungen in Benutzerkommentaren oder im Gästebuch) oder bei Verletzungen des →Urheberrechts

Unternehmenskultur: umfasst das gesamte gewachsene Meinungs-, Norm- und Wertgefüge, welches das Verhalten der Führungskräfte und Mitarbeiter prägt. Positive Unternehmenskultur ist wichtig für Produktiviät, aber auch sicherheitsbewusstes Verhalten. Siehe →Nachhaltigkeit, →Businessethik, →CSR
http://sicherheitskultur.at/business_ethik.htm

UPC: (Universal Product Code) amerikanisches →Barcode System. Als EAN·UCC mit dem europäischen →EAN verschmolzen. Wird jetzt durch →EPC ersetzt

Upload-Filter: →Software um das Hochladen von →Daten zu verhindern, die unter dem →Copyright eines Rechteinhabers stehen (→Lizenz-, →Urheberrecht), zumeist ist damit Musik gemeint. Deren Einsatz im Rahmen der Diskussionen rund um die neue EU-Urheberrechtsreform (implizit). Kritiker sehen das Risiko dass es dadurch zu einem Overblocking kommt, d.h. dass die Betreiber der Systeme (→OCSSP) zur Risikovermeidung im Zweifel zu viel blockieren würden.

UpnP: (Universal Plug and Play) auf →TCP/IP, UDP, →HTTP und →XML beruhendes →Protokoll um eine automatische Konfigurierung von Geräten in Heim- oder Firmennetzen zu ermöglichen. 2013 wird veröffentlicht, dass im →Internet 6900 verschiedene Gerätetypen unter 81 Mio →IP-Adressen extern erreichbar sind. Dazu gehören Drucker, Heim-→Router von →ISPs für den →Zugang zum Internet, →Firewalls, Webcams und viele Überwachungskameras. UPnP-Geräte lassen sich leicht erkennen und sehr oft auch manipulieren. So lassen sich oft die Videostreams ansehen, bzw. →Daten abrufen oder auf den Druckern ausdrucken. Das UPnP-Protokoll war für Windows XP entwickelt worden um es einfach zu machen, externe Geräte an →PCs anzuschließen. Dabei wurden Themen wie →Authentisierung vollkommen ignoriert

UPS: (Uninterruptable Power Supply) nicht-unterbrechbare Stromversorgung, in der Regel durch Batteriebetrieb, jedoch oft auch Dieselgenerator. Deutsch: USV. Wichtige Maßzahl für die Auslegung ist →VA. Siehe →SPD, →TVSS

UPX: (Ultimate Packer for eXecutables) →Freeware Tool zum Kompromieren von →Programmen, oft eingesetzt zum Codieren von →Schadsoftware, so dass sie von →Virenschutzprogrammen nicht erkannt wird

Urheberrecht: bezeichnet das ausschließliche Recht eines Urhebers an seinem Werk. Es dient dem Schutz von Geistesschöpfungen. Es schützt den Urheber in seinem Persönlichkeitsrecht und seinen wirtschaftlichen Interessen. Urheberrecht ist „vertragsfest“ und kann in D, Ö und CH auch in einem Vertrag nicht abgegeben werden (auch nicht durch Arbeits- oder Werksvertrag). Teilweise wird auch von geistigen Eigentum (englisch: →IPR) gesprochen. Siehe →Copyright, →Creative Commons, →Public Domain, →Haftung, →fair use

URI: (Uniform Resource Identifier) Name oder Adresse einer Ressource im →Internet. Spezialformen sind →URL und →URN

URL: (Uniform Resource Locator) kompakte Beschreibung von Ressourcen, die als Zeichenkette dargestellt und über Internet abgerufen werden können. URLs werden in erster Linie zum Abrufen von Dokumenten und Informationen im →WWW verwendet. Syntax und Semantik ist in RFC 1738 definiert. Meistens enthält eine URL Informationen über das Zugriffsprotokoll (http://), die Adresse des Servers und weitere Details, wie z.B. einen Pfad oder Filenamen, oder sogar →Passworte für →Websites. Eine der Formen ist →URI.

Nach der ursprünglichen Definition konnten in URLs nur →ASCII-Zeichen abgebildet werden, d.h. keine Umlaute oder Zeichen aus anderen Alphabeten. Um dies zu ermöglichen wurde →PunyCode entwickelt. So wird dann z.B. „österreich-testet“ zu „xn--sterreich-testet-lwb.at“. Der →Webbrowser zeigt jedoch in der URL-Zeile nicht diesen String, sondern „österreich…“ an. Dies wird zu einem Sicherheitsproblem, da auf diese Weise Fake-URLs erzeugt werden können, die optisch nicht von den korrekten zu unterscheiden sind (z.B. wenn ein „a“ durch die gleich aussehende kyrillische Variante von „a“ ausgetauscht wird. Dies bietet gute Möglichkeiten für echt aussehende →Phsing-Mails

URL-Blocking: wichtiger Aspekt des →Content Filtering. Dadurch soll verhindert werden, dass Angestellte oder Kinder auf unerwünschte Webseiten zugreifen. Diese reichen von Pornographie bis →Freemailern. Zwei Haupttechniken sind a) Datenbanken von unerwünschten Adressen und b) Aufspüren unerwünschter Schlüsselworte. Ersteres produziert viele False Negatives, d.h. unerwünschte Seiten kommen durch, letzteres produziert

False Positives, d.h. Aufklärungsseiten und Seiten über „breast cancer“ werden als Porno identifiziert. Neuere Lösungen verwenden die statistische Methode der Cluster-Analyse oder →Bayesian Analysis zur genaueren Klassifizierung

URL-Shortening: Dienste wie tinyURL.com oder bit.ly, mit deren Hilfe eine lange →URL in eine kurze URL umgewandelt werden kann (z.B. http://tinyurl.com/ngIfC). Dies kann für →Angriffe genutzt werden, da der Benutzer auf diese Weise nicht sieht, auf welche „böse“ →Website er weitergeleitet wird. Auch →URL-Blocking wird auf diese Weise evtl. ausgehebelt und →Phishing-Angriffe werden erleichtert

URN: (Uniform Resource Name) Format für die einheitliche Bezeichnung von Ressourcen, z.B. "urn:isbn:0451450523" für Bücher. Spezialform einer →URI

Usability: (engl. Benutzbarkeit) Aspekt des → HMI (human machine interface). Eine einfache, verständliche Benutzbarkeit verringert die Wahrscheinlichkeit von Bedienfehlern. Siehe auch →Clickstream

USA Patriot-Act: 2001 (Providing Appropriate Tools Required to Intercept and Obstruct Terrorism) Grundlage für eine ganze Reihe von Aufhebungen der →Privatsphäre und anderer Rechte in den USA. U.a. kann das FBI (nach einem Hearing vor dem geheimen FISA (Foreign Intelligence Surveillance Act) court die Daten aller "american-based" Firmen einsehen, auch bzgl. Geschäftsvorgängen mit ausländischen Kunden (SEC. 215) Dies kann auch die Daten von europäischen Personen oder Firmen betreffen die US-→Cloud Dienste nutzen. Zusätzlich verlagert die US-Regierung diese Aktivitäten weitgehend auf private Datenbanken, siehe →Acxiom Corp, →ChoicePoint, →LexisNexis. →PAA. Alle US-Gesetze: http://thomas.loc.gov/

USB: (Universal Serial Bus) Standard (1996) zum Anschluss von Geräten (Computer-Peripherie, aber auch Fotoapparate, MP3-Spieler, etc.) an →Rechner. Erlaubt Übertragungsraten bis 12 Mbps und bis zu 127 Geräte. Wird mehr und mehr auch für Speicher (→USB-Sticks oder USB Festplatten) oder als Ersatz für →Smartcards verwendet. Über die USB-Schnittstelle kann →Schadsoftware in das Unternehmen und können →Daten aus dem Unternehmen übertragen werden. USB 3 unterstützt →DMA und kann genutzt werden um sensible Inhalte wie →Passworte aus dem →Hauptspeicher auszulesen. Siehe →Firewire, →Bus

US-CERT: (US Computer Emergency Readiness Team) hervor gegangen aus dem →CERT der Carnegie Mellon University, jezt Teil vom →DHS

USB-Stick: (USB-Speicherchips, engl. thumb drive) →Flash-basierter Datenspeicher der über die →USB-Schnittstelle an geeignete →Rechner angeschlossen werden kann. Durch die USB-Sticks (auch in der Form der integrierten Flashspeicher in →Handys, Fotoapparate und MP3-Spieler) kann auch →Malicious Code übertragen und →Daten aus Unternehmen entfernt werden. Auf diese Weise wurde z.B. →Schadcode im Fall von →Stuxnet in den vom übrigen Firmennetz getrennten Netzbereich eingeschleust. Auch von US-Kraftwerken werden solche Fälle berichtet, Stichwort: →SCADA.

Da USB-Sticks auch einen →Prozessor enthalten der beliebige Daten senden kann, d.h. auch selbständig erkennen, wo er jetzt eingesteckt wurde und welche →Schwachstellen dort ausgenutzt werden können. Wegen diesen zahlreichen Angriffsmöglichkeiten werden in einigen Organisationen USB-Sticks ganz verboten (im US Pentagon seit 2008), bzw. mittels →DLP überwacht, bzw. zwangsweise verschlüsselt. Siehe →Datendiebstahl

Usenet: frühe Form von →Social networking und →chat room

User: →Benutzer

User account control: (UAC) →Sicherheitskonzept in Windows →Vista. →Benutzer, die ohne →Admin-Rechte arbeiten und privilegierte Funktionen aufrufen (→shield icon) werden aufgefordert, eine separate →Autorisierung einzugeben, um diese Funktionen nutzen zu können. Benutzer, die →Admin-Rechte haben, arbeiten trotzdem erst mal im Standard Modus. Wenn für sie der → Administrator Approval Mode aktiviert ist, öffnet sich bei privilegierten Funktionen ein Fenster, in dem sie bestätigen müssen, dass sie jetzt administrative Funktionen ausführen. Gleichzeitig wird der →Secure Desktop Mode aktiviert, der verhindert, dass andere →Tasks mit dem offenen Fenster interagieren können

User permission fatigue: beschreibt die Problematik, dass →Benutzer sehr oft überfordert sind, wenn sie z.B. bei einer →Smartphone →App entscheiden sollen, welche →Zugriffsrechte diese App haben darf. Ähnliche Effekte treten auch auf wenn Benutzer, wie bei →Vista oder Windows 7, sehr häufig um Freigaben befragt werden

Username: →Benutzerkennung

User tracking: →Tracking

US-GAAP: (United States Generally Accepted Accounting Principles) →Rechnungslegungsvorschriften der USA. Relevant für die Informationssicherheit durch den Zusammenhang mit →Compliance-Vorschriften wie →SOX

USIM: (Subscriber Identiy Module) Anwendung auf einer →UICC, entspricht bei →UMTS-Geräten der →SIM-Karte bei →GSM. Moderne Versionen können mehr als nur die →Identität eines →Handys zu bestätigen (durch sichere

Speicherung einer →IMSI und zugehöriger →Schlüssel -→Secure Element). Dies kann bis zu →NFC-Chips und integrierten →Webserver und →Webbrowser gehen

USRP: (Universal Software Radio Peripheral) mittels →GNU Radio programmierbares Gerät mit dem sich sehr leicht drahtlose Geräte entwickeln lassen. Dies ist eine Implementierung eines →Software-defined Radios. Ermöglicht →Angriffe auf Geräte mit drahtlosen Verbindungen, wie z.B. →RFID, kontaktlose →Smartcards, →ePässe in Frequenzbereichen bis 2,9 GHz

USSD: (unstructured supplementary service data) Zeichenfolgen wie *#06#, die von →Handys automatisch interpretiert werden und Schäden anrichten können, z.B. →SIM sperren. Solche Codes können auch in →QR-Codes versteckt sein (z.B. in Form tel:<USSD>, die abhängig vom System und der verwendeten Software, evtl. sofort ausgeführt werden

USV: →UPS

UTF: (Unicode Transformation Format) Implementierungsoption(en) von →Unicode. Sie unterscheiden sich durch die Zahl der bits pro Einheit. Beispiele: UTF-32, UTF-16, UTF-8, UTF-EBCDIC und UTF-7. Alle außer UTF-32 benutzen bei Bedarf eine weitere Speichereinheit

UTM: (Unified Threat Management) neues Schlagwort für eine Lösung, die eine →Firewall-Funktionalität mit Anti-→Malware, →URL-Filtering, →Intrusion Prevention und u.a. Schutzfunktionalitäten vereint, jeder i.d.R. mit eingeschränkten Funktionalitäten gegenüber spezialisierten Lösungen. Zielgruppe sind →KMU. Für größere Unternehmen spricht die Industrie von →Next Generation Firewall (→NGFW)

UTMA: (Unified Threat Management Appliance) Hardwareimplementierung von →UTM

UUID: (Universally Unique Identifier) 16-Byte Zahl zur Benennung von Objekten, bei der sichergestellt ist, dass sie auch ohne Koordinierung nie von jemand anders verwendet wird. Dokumentiert in ISO/IEC 11578:1996, ISO/IEC 9834-8:2005 und RFC 4122. Frühere Versionen wurden kritisiert, da sie Informationen über den Erzeuger preisgaben

UWB: →Ultra-Wideband

V2I: →C-ITS

V2V: →C-ITS

VA: (Volt-Amp, elektrische Scheinleistung) wichtige Maßzahl für die Dimensionierung von →UPS, Verkabelungen und Sicherungen. Ergibt sich als Produkt von Volt und Ampère und liegt immer gleich oder höher als die →Watt-Zahl. Der Faktor Watt zu VA heißt Power Factor. Er ist für Heizgeräte 1, für viele elektronische Geräte auf Grund von Phasenverschiebungen z.B. 0,7. Servernetzteile haben heute oft einen Faktor von 1

VAN: (Value Added Network) Begriff der meist in Verbindung mit →EDI-Datenverkehr genutzt wird. Traditionell wurde EDI-Datenaustausch über eine Verbindung (permanent oder temporär) zu einem VAN durchgeführt. Der VAN hat dabei eine Transport- und →Mailbox-Funktion

Van Eck Strahlung: →Side Channel Angriff auf →Bildschirme, ursprünglich nur über Ausnutzung der elektromagnetischen Abstrahlung von Bildschirmablenkungen. Flachbildschirme haben dieses Problem nicht mehr, aber mittels Richtantenne und spezielle Hardware lassen sich →Graphikkarten, Kabel, →Tastaturen u.ä. weiterhin Abhören. Schutz durch Abschirmung, notfalls des gesammten Arbeitsraumes (→Tempest)

VaR: (Value at Risk) Methode im Bereich →Risk Management, bei der der erwartete Schaden oder Wertverlust abgeschätzt wird, bei →operationellem Risiko mangels Normalverteilung kaum anzuwenden. Alternative Methoden: Conditional VaR (tail-VaR), Extremwerttheorie, Peaks over Threshhold-Methode (POT), Fuzzy Logic, →Bayes'sche Netzwerke

VbVG: (Verbandsverantwortungsgesetz, 2005) ö. Gesetz, dass die Strafbarkeit auch auf juristische Personen, d.h. Firmen und Verbände ausdehnt. Bis dahin waren Strafverfahren, im Gegensatz zu Zivilklagen, nur gegen natürliche Personen, z.B. die Geschäftsführer eines Unternehmens möglich. Voraussetzung ist eine Straftat zugunsten der Firma oder eine Pflichtverletzung durch die Firma, wenn der Täter Entscheidungsträger ist oder wenn es keine Kontrollmaßnahmen gab, um die Tat eines Mitarbeiters zu entdecken oder zu verhindern

VCL: (Virus Construction Lab) Softwaretool, das auch einem sog. →Script Kiddy erlaubt, →Viren und →Würmer zu bauen. Dabei werden die Viren aus vorgefertigten Bausteinen für Angriffe, Schadwirkung, usw. zusammengesetzt

Vehicle to infrastructure: (V2I), siehe →C-ITS

Vehicle to vehicle: (V2V), siehe →C-ITS

VEIL: (Video Encoded Invisible Light) →Kopierschutz für analoge Videosignale, verwendet in vielen Geräten, kann mit →CGMS-A kombiniert werden. Kodiert eine Bitfolge in den analogen Datenstrom, ähnlich zu →Steganographie

VEP: →Vulnerabilities Equities Process

Veracrypt: →Open Source Nachfolgeprogramm zu →Truecrypt, dessen Entwicklung 2014 überraschend eingestellt wurde. Legt verschüsselte Container an in denen ein →Dateisystem „versteckt" ist, das über eigenen Laufwerksbuchstaben verfügbar ist.

Kann daher auch mit →Cloud-Speichern genutzt werden, die ein „mappen“ auf Laufwerksbuchstaben erlauben. Unterstützt auch →Hidden Volumes, d.h. ein →Deniable File System

Verbindlichkeit: →Non-Repudiation

Verbindungsdaten: →Daten bez. eines Kommunikationsvorganges, der i.d.Regel Datum, Uhrzeit und die beiden Teilnehmer enthält. Im Fall einer Handykommunikation enthalten die Daten auch den Aufenthaltsort der Teilnehmer. Umstritten ist die Länge der Aufbewahrung dieser Informationen und die Weitergabe ein Behörden, z.B. zwecks Aufklärung von Verbrechen oder prophylaktischer →Terrorismusbekämpfung. →Data Retention. Studien haben gezeigt, dass eine systematische Auswertung (→data mining) von Verbindungsdaten, z.B. in einem Unternehmen oder privat, tiefe Einsichten, z.B. in informelle Strukturen und das soziale Netz einer Person, d.h. ihren →Social Graph, geben können. Daran sieht man nicht nur ob eine Person eine zentrale oder Randrolle im Kommunikationsnetz spielt, interessant ist auch ob eine Person typischerweise Initiator oder Ziel einer Kommunikationsanfrage ist, ob auf ihre Anfragen reagiert wird oder nicht und

Siehe →Stammdaten, →Metadaten

Verfügbarkeit: Sicherstellen, dass autorisierte Nutzer zum jeweils notwendigen Zeitpunkt Zugriff zu Information und zugeordneten Systemen haben. (Def. →ISO 17799)

Verifzierung: an die →Identifizierung anschließender Vorgang, bei dem die mutmaßliche →Identität durch →Authentisierungsverfahren verifiziert wird

Verkehrsdaten: →Verbindungsdaten

Verschlüsselung: Transformation von →Daten mittels Verschlüsselungsalgorithmen, so dass nur berechtigte Empfänger diese verwenden können.

Man unterscheidet symmetrische und asymmetrische Verfahren. Bei einem symmetrischen Verfahren werden die Daten mit dem gleichen →Schlüssel ver- und entschlüsselt. Das heißt, der gleiche Schlüssel muss Sender und Empfänger bekannt sein. D.h. auch, dass die Schlüssel sicher ausgetauscht werden müssen.

Bei asymmetrischen Verfahren werden Daten mit dem öffentlichen Schlüssel des Empfängers verschlüsselt. Die Nachricht wird mit dem zugehörigen privaten Schlüssel entschlüsselt. Daher ist eine Übertragung des Schlüssels zwischen Sender und Empfänger nicht notwendig. Weil asymmetrische Verfahren sehr langsam arbeiten (da sie lange Schlüssel benötigen) wird fast immer ein 2-stufiges Verfahren genutzt: die Daten werden mit einem zufälligen Zufallsschlüssel verschlüsselt, dann wird dieser Schlüssel mit dem public key des Empfängers verschlüselt und mit den Daten übertragen. Asymmetrische Verfahren beruhen auf mathematischen Techniken, die in einer Richtung sehr schnell gehen, in der umgekehrten Richtung sehr langasam (z.B. Multiplikation von 2 Primzahlen geht schnell, die Zerlegung ist sehr langwierig, diese Zerlegung muss für ein Knacken des Schlüssels erfolgen). Alternatives Verfahren ist →Elliptic Curve Cryptography (ECC)

Angegriffen werden Verschlüsselungen durch →Brute Force, d.h. ausprobieren vieler Schlüssel (z.B. über →Graphikkarten), oder durch Auffinden von Schwächen in den Algorithmen, oder durch Fehler beim Generieren der immer notwendigen →Zufallszahlen. Andere Angriffe sind →side channel attacks.

In der Zukunft wird erwartet, dass →Quantencomputer viele der jetzigen Algorithmen knacken können. Neue Algorithmen wie Lattice-based Cryptography sollten immun dagegen sein.

Siehe auch →Stromverschlüsselung, →Blockverschlüsselung, →Festplattenverschlüsselung, →Quantencomputer, →QKD, →Diffie-Hellman, →AES, →DES, →Rijndael, →CSP, →Cryptochip, →Opportunistic Encryption, →Homomorphic Encryption, →Multi-Party Computation, →Zero knowledge proof, →Searchable Encryption, →Perfect Forward Security

http://sicherheitskultur.at/Eisbergprinzip.htm#schluesssel

Vertrauen: Gewissheit einer erwünschten Zukunft. Beruht auf der Kontinuität des regelhaften und erwünschten/erwarteten Verhaltens der Umgebung/ Person oder der eigenen Kenntnis und Beherrschung der Lage (einschließlich Ihrer Unwägbarkeiten). Als →*Trust* wichtiges Konzept der →Informationssicherheit

Vertraulichkeit: gegeben, wenn sichergestellt werden kann, dass Informationen nicht durch unautorisierte Personen, Instanzen oder Prozesse eingesehen werden können (Def. →ISO 17799)

Verwundbarkeit: →Programmfehler oder Konfigurationsfehler, die es einem Angreifer ermöglichen, ein Programm oder einen Rechner zu Zwecken zu missbrauchen, die vom Benutzer nicht erwünscht sind. Siehe →Vulnerability, →Schwachstelle

Verzeichnisdienst: deutsch, (engl. →Directory). Eine hierarchisch aufgebaute Datenorganisation, die speziell für Organisationen, Personen, ihre Zugriffsberechtigungen konzipiert ist. Der Standard für solche Verzeichnisse ist →X.500. Als Zugriffsmethode hat sich →LDAP durchgesetzt. Verzeichnisdienste werden vor allem für →Zugriffsberechtigungen und im Rahmen von →PKI eingesetzt

vhost: (→virtual host)

VICTORYDANCE: Aktivität der →NSA, bei der ein →UAV so ausgerüstet wird, dass noch aus 4 Meilen Höhe die →WLANs erkannt werden, erlaubt →Geolocation von Zielpersonen

Videokonferenz: Synchroner Austausch von Bild- und Ton über Datennetze, typischerweise über spezielle →Hardware und →Software. In 2020 wurde dies weitgehend durch →Webkonferenzsysteme abgelöst, da im →Home-Office ja nur reguläre →PCs und/oder →Smartphones zur Verfügung stehen

Videoüberwachung: →Überwachung von Personen oder Orten durch Kameras (engl. →CCTV). Früher durch Aufzeichnung auf →Magnetband, heute über →IP-Netze, oft offen bis zum →Web (→Webcam). Die Effektivität zum Verhindern von Verbrechen ist stark umstritten. Zu diesem Zwecke werden PTZ-Kameras eingesetzt (Pan/Tilt/Zoom) die manuell gesteuert werden. Wenn das Ziel die Aufklärung ist, so sind feste Kameras mit hoher Auflösung, deren Aufnahmen nur im Bedarfsfall ausgewertet werden, effektiver. Der Einsatz durch Private oder Firmen unterliegt dem →Datenschutzgesetz. In Firmen ist der Einsatz zustimmungspflichtig für den →Betriebsrat

Vier-Augen-Prinzip: (engl. Dual Control) →4-Augen-Prinzip

Vigilance decrement: psychologischer Effekt, dass die Wachsamkeit beim Warten auf seltene Ereignisse stark abnimmt. Problematisch z.B. bei →Videoüberwachung durch Menschen. Siehe →Primary Effect, →Automation Bias

Viren: in der IT →Malware

Virenschutz: in der IT →Malware-Schutz

Virtual Assistant: →Service auf →Smartphones der Benutzern auf Grund von gesammelten →Daten und Anfragen die oft verbal gestellt werden persönliche Ratschläge für ihr Verhalten gibt, Fragen beantwortet und einfache Aufgaben erledigt. Solche →Programme bieten wenn die Nutzer den Vorschlägen folgen, Manipulationsmöglichkeiten für die Firmen, die sie kontrollieren. Die Programme haben meist eine weibliche Stimme und Namen. Beispiele sind Cortana, Alexa, Siri. Solche Dienste werden ab ca. 2018 auch als Hardwaregeräte angeboten, dann oft →Smart Speaker genannt (Alexa mit →Amazon Echo, →Google Home, →Apple Homepod. Problematisch ist u.a. dass für die Spracheingabe die Geräte ALLEN Gesprächen im Haushalt zuhören und die Geräte wenn sie im selben Heim-Netzwerk liegen auch auf die anderen Geräte dort zugreifen können. Dies ist z.B. bei smarten Haushaltsgeräten (→IoT) evt. gewünscht, aber könnte auch zu Verletzungen der Privatsphäre führen.

Zur Problematik siehe auch →Contextual Computing

Virtual Host: Implementierung eines →Webservers, bei der viele →Websites mit unterschiedlichen Internet→Domänen auf einem Rechner „gehostet“ werden (→Hosting). →Angriffe gegen eine dieser Domänen können alle anderen in Mitleidenschaft ziehen, solche Installationen werden aus Gründen der Admnistrierbarkeit fast immer ohne →Firewall betrieben und es sind zahlreiche riskante Protokolle für das gesamte →Internet offen

Virtualisierung: Schlagwort, das die Trennung von logischer Realisierung und physischer Realität beschreibt. Sie findet auf allen Ebenen statt: →Server auf Hardware- oder Betriebssystemebene, →PC und →Desktop, →Magnetplatten, →Switches und andere Netzwerkdevices wie z.B. →Firewall. Generelle Sicherheitsfragen dazu sind: Wie sicher ist die Trennung der gemeinsamen Resourcen? Sicherheit der →Administration? Möglichkeiten und Gefahren durch →forensische Funktionaliltäten? Erfüllen von →Auditanforderungen, inkl. →Mandantentrennung in Logs?

1) Server-Hardware-Virtualisierung beschreibt eine mehr oder weniger dynamische Aufteilung eines Rechners mit einer großen Zahl von →CPUs (oder →Cores) in kleinere mit mehr oder weniger dedizierten Resourcen (lPar, nPar)

2) Betriebssystem-Virtualisierung. Dabei werden auf einem Rechner gleichzeitig mehrere →Betriebssysteme genutzt, alle Ressourcen werden entsprechend aufgeteilt. Vorteil ist, dass die bei modernen Servern oft sehr schlecht ausgelasteten →CPUs viel besser ausgelastet werden können, →Hauptspeicher-Anteile müssen jedem Betriebssystem (temporär) fix zugeordnet werden. Viele Implementierungen bieten Sicherheitsfeatures wie →Snapshots für eine schnelle →Wiederherstellung. Es erfordert ein entsprechendes „Betriebssystem“ „unterhalb“ der Host-Systemen (→Hypervisor). Es werden dabei auch die →Netzwerkadapter virtualisiert und innerhalb des Servers virtuelle →Switches realisiert. Für die Sicherheit ist es wichtig, dass die Systeme sich nicht beeinflussen können und nicht auf die →Daten (Hauptspeicher, Magnetplatten oder Datenverkehr über gemeinsam genutzte virtuelle Netzwerkadapter) der anderen Gast-Systeme zugreifen können. Siehe auch →VMware, →OpenVZ

3) PC- und Desktop Virtualisierung. Dafür kann u.a. die gleiche Software wie für Server genutzt werden, oder andere Konzepte wie →Terminalserver oder →Citrix

4) Bei Magnetplatten-Virtualisierung (Speicher-Virtualisierung) wird eine große Zahl von Magnetplatten in logische →LUNs zerteilt, die über ein →SAN angeschlossen vielen →Servern gleichzeitig zur Verfügung stehen. Es muss dabei verhindert werden, dass Server auf andere als „ihre“ Platten zugreifen können.

Siehe →VSAN

5) Netzwerkdevice-Virtualisierung. Mittels →VLAN-Technologie (→Layer 2-→Switch) oder →MPLS (Layer 3-→Router) und →VRF

6) Siehe →App wrapping

Virtual Machine: (VM) logische Instanz eines →Rechners, die bei einer Betriebssystem- oder Desktop-Virtualisierung entsteht wird und virtueller Server genannt. Siehe Punkte 2) und 3) von →Virtualisierung. Siehe auch →OpenVZ

Virtual Memory: Feature in →Betriebssystemen, bei der mehr →Hauptspeicher adressiert werden kann, als im →Rechner eingebaut ist, indem einzelne →Pages auf eine →Festplatte ausgelagert werden. Siehe →Segment

Virtual Currencies: Form von →e-Geld die sich nicht auf real-existierende Währungen bezieht sondern eine eigene Währung etabliert. Wird oft in →Games eingeführt. Beispiele sind →Bitcoin, →Facebook Credits, Nintendo Points oder Linden Dollar in →Second Life. Unterschieden werden Währungen vom Typ 1 (geschlossene in-game Währungen), Typ 2 (nur einseitige Konvertierbarkeit), Typ 3 (Konvertierbarkeit in beiden Richtungen). Im Gegensatz zu diesen Währungen steht „fiat currency“, das sind die von Nationalbanken (o.ä.) herausgegebenen Währungen, deren Akzeptanz durch gesetzliche Vorschriften entsteht. Es ist „aus dem Nichts“ dessen Wert auf dem Vertrauen (→trust) beruht, dass der Herausgeber (Emittent) für den Wert des Geldes „einsteht“. Da es keine Deckung durch Gold o.ä. gibt besteht bei einer zu hohen Geldmenge Inflationsrisiko. Virtuelle Währungen auf der Basis von kryptographischen Verfahren (→cryptocurrencies) und Blockchain Technologie sind →Bitcoin, Ripple, →Ethereum, Litecoin, PeerCoin, Namecoin, Feathercoin, Megacoin, Infinitecoin, u.a.

Regulierungsbehörden und Polizei haben u.a. die Herausforderung, dass unklar ist, welche Gesetze bei der Nutzung von Dingen wie Bitcoin überhaupt anwendbar sind. Ob Entwendung von Bitcoins aus einer →Wallet (auf einem →Computer) Diebstahl ist, ist fraglich, da kein Gegenstand entwendet wurde sondern nur →Datensätze. Konsumentenschutz bezieht sich oft auf „Geld“, und das ist oft gebunden an „von Regierungen oder Zentralbanken gegebene Zahlungsversprechen‘. Auch →Pump-and-Dump Schemes fallen evt. nicht unter die Börsegesetze

Virtual Private Network: (VPN) sichere verschlüsselte Verbindung zu einem privaten Netz oder einem →Server über eine unsichere Verbindung, meist das →Internet. Dabei wird mit Hilfe von Tunneling, d.h. Verschlüsseln des Datenverkehrs, sowohl →Integrität, wie auch →Vertraulichkeit der Daten gewährleistet.

Spezielle →**VPN-Dienste** werden im →Internet als →Anonymisierungdienste angeboten. Diese ermöglichen, dass der Kunde eine verschlüsselte Verbindung zu diesem Service aufbaut (entweder über HTTPS oder über andere Protokolle wie →IPsec. →L2TP, →PPTP), so dass die Dateninhalte von Überwachungsmaßnahmen nicht erkannt werden kann. Wird in Diktaturen von Oppositionellen genutzt, aber auch von Kriminellen. Die Sicherheit die ein solcher Dienst bietet hängt jedoch von der Ehrlichkeit des Anbieters ab, d.h. kann fraglich sein. Bessere Alternative ist zumeist →TOR. Siehe →Split traffic, →SSL/VPN, →MPLS, →SWATting

Virtual Reality: (VR) umfasst neben →virtual worlds die hauptsächlich auf Spiele konzentriert sind auch andere Anwendungen wie Simulationen, z.B. für Ausbildung und Training. Ein wichtiger Aspekt sind „immersive“ Interfaces, z.B. →Oculus Rift (2014 gekauft von →Facebook)

Virtual World: (VW) in Rechnern simulierte künstliche Umgebungen im →Internet in denen Personen durch →Avatare repräsentiert werden und dort interagieren können. Dazu gehören „civic world“ wie →Second Life, →Habbo Hotel oder Project Entopia und →MMORPGs wie →World of Warcraft**.** Siehe auch →Social Media

Virtuel: in der IT jegliche Implementierung von IT-Komponenten bei denen mehrere logische Geräte oder Dienste auf 1 physischen →Hardware implementiert sind. Viele Beispiele finden sich unter →Virtualisierung

Virus: in der IT: spezielle Form der Schadsoftware (→Malware), Computervirus, eine Form von →Malicious Code. Ein Programm, das sich vervielfältigen kann, indem es seinen →Programmcode in andere Programme einbaut. Früher war der Zweck, den Betriebsablauf eines Computers zu stören, ab 2004 werden Viren und Würmer auch für kriminelle Aktivitäten eingesetzt (→Zombies). Viren und →Würmer können mit Hilfe eines →VCL leicht erstellt werden. Siehe →Polymorphic Virus, →Obfuscation, →Assembler, →VirusTotal

VirusTotal: →Website die kostenlos →Dateien auf →Malware überprüft indem die Datei gegen 51 unterschiedliche Anti-Malware Produkte testet und aufzeigt, welche der System fündig geworden sind. 2012 von →Google gekauft

Vista: (Windows Vista) Erstes Betriebssystem von Microsoft mit stark verbesserten Sicherheitsaspekten, z.B. bei der Rechteverwaltung und zum Arbeiten ohne →Admin-Rechte. Dies geschieht u.a. dadurch, dass →Programme, die schreibenden Zugriff auf die →Registry benötigen, unter Vista in eine lokale Kopie schreiben können, die Teil des Benutzerprofils ist. Siehe →UAC, →ASLR, →MIC, →DAC, →DEP, →Admin Approval Mode, →OTS, →Windows, →BitLocker

Visual Keyboard: Verfahren zur →PIN-

Eingabe, bei der die Zahlen statt mittels →Tastatur über →Mouse-Clicks auf dem →Bildschirm selektiert werden. Fortgeschrittene →Keylogger sammeln daher für entsprechende →Website 50x50 Pixel um die Mouse-Clicks

VLAN: (Virtual LAN) Technologie zur flexiblen Implementierung von lokalen Netzen (→LAN). Dabei werden in einem →Switch einzelne →Ports zu einem Subnetz auf →Layer-2 zusammengefasst. Geräte, die in verschiedenen Subnetzen liegen, können nur kommunizieren, wenn entsprechende Routingregeln (auf →Layer-3, mit Filterfunktion) definiert sind. Auf diese Weise kann in einem Unternehmen eine Trennung zwischen verschiedenen Netzbereichen implementiert werden, was zu einer Verbesserung der Sicherheit führt. Siehe →IEEE 802.1q

VM: →virtual machine

V-Modell: abstrakte, umfassende Projektmanagement-Struktur für die →Softwareentwicklung

VMWare: Firma die Virtualisierungstechniken anbietet. Dabei laufen i.d.Regel mehrere →virtuelle →Rechner auf einer Hardware. Eine „Konsole“ auf VMware-Ebene steuert die Parameter der Virtualisierung, hat aber auch →Zugriff auf diese Gast-Systeme. Außer der Flexibilität solcher Virtualisierungen indem viele virtuelle Systeme 1 Hardware teilen können hat dieses Konzept auch Vorteile bei der →Hochverfügbarkeit, indem bei Ausfall einer Hardware ein System schnell auf ein anderes verschoben werden kann.Auch bei der Forensic können virtuelle Systeme von Vorteil sein. Ein neues Angebot von VMware ist →Mobile Horizon, ein Angebot für →Smartphones und ThinApp für Windows

VNC: (Virtual Network Computing) Methode zur Darstellung des Bildschirminhaltes eines →Rechners auf einem anderen (Client)-Rechner. Wird für Wartungszwecke oder für →Überwachung eingesetzt. VNC ist im Gegensatz zu Teamviewer und →Citrix GotoAssist →Open Source und geräteunabhängig. VNC stellt keine sichere Verbindung her und sollte nur in Verbindung mit einem →VPN-Tunnel oder →SSH eingesetzt werden. Das genutzte Protokoll heißt →RFB (remote frame buffer). 2013 wird VNC (wie auch Teamviewer) auch von Angreifern verwendet, um nach Installation des entsprechenden Servers auf dem infizierten PC des Opfers von dessen PC aus die Konten des Opfers leer zu räumen

Voicemail: Aufnahme von telefonischen Sprachnachrichten in die Inbox des →E-Mail-Systems, zumeist als Teil eines →VoIP- und →Unified Messaging Systems. Es entsteht dann die →Bedrohung →SPIT. Eine zu Voicemail äquivalente Funktionalität gibt es auch in Messaging Systemen wie →Whatsapp. Siehe auch →e-Discovery

Voice Analysis: →Sprachanalyse

Voice Recognition: →Stimm-Erkennung

VoIP: (Voice over IP) Übertragung von Sprachdaten über →IP-Netze, meist aus Kostengründen. Implementierung als Client am PC (z.B. →Skype) oder als Ersatz für einen traditionellen →PBX. Mit steigender Popularität mehren sich auch Berichte über →Schwachstellen und Sicherheitslücken. Entsprechende Software dafür ist im Internet verfügbar (→vomit). Da oft →Verschlüsselung eingesetzt wird, klagt die Polizei über Probleme beim →Abhören und wünscht den →Bundestrojaner. →Bedrohungen bei VoIP sind mangelnde →Verfügbarkeit, →toll fraud, Verletzung der →Vertraulichkeit, →Spoofing und Impersonation, →SPIT, session hijacking, →MITM. Spezielle Herausforderungen stellt Voice over WLAN (→VoWLAN). Siehe →SIP, →H.323, →MGCP, →SDP, →RTP, →SRST, →SRTP, →OCS, →Unified Messaging, →IP Phones, →SPIT, →Softphones, →MOS, →RTCP

Volatilität: beim →Risikomanagement die erwartete Schwankungsbreite von zukünftigen Ereignissen. Hauptsächlich im Bereich Finanzen verwendet, z.B. für die Schwankungsbreite von Kursen, siehe →VaR

Volkszählung: seit biblischen Zeiten beliebte →Überwachungsmethode. 1576 in Frankreich um menschliche „Parasiten“ loszuwerden, in der Habsburgermonarchie zur Ausgrenzung von Juden und Protestanten. Seit 1900 mittels elektronischer →Datenverarbeitung auf →Lochkarten. 1938 effizient bei der Erfassung der Juden in Deutschland und besetzten Gebieten. Siehe →Volkszählungsurteil

Volkszählungsurteil: zu der in D 1983 geplanten →Volkszählung gab es heftige Proteste. Im sog. Volkszählungsurteil des Verfassungsgerichts wurde das „Grundrecht auf informationelle →Selbstbestimmung“ festgeschrieben. Siehe auch →Datenschutz

Volume: logischer Teil einer →Festplatte, →USB-Stick oder →SSD die 1 →file system enhtält. Siehe auch →Festplattenverschlüsselung

Volume Shadow Copy: →VSS

vomit: (voice over misconfigured Internet telephones) Programm, das es ermöglicht, Gespräche über Cisco IP phone in Wav-Format zu konvertieren und damit leicht abzuhören, sofern Zugriff auf die Leitung besteht

Vorfall: →Incident

Vorfallsbehandlung: →Reaktion auf einen sicherheitsrelevanten Vorfall.. Siehe →Alarm

Vorratsdatenspeicherung: seit 2007 umstrittene Richtlinie der EU zu →Data Retention, die eine verdachtsunabhängige Speicherung von →Verkehrs- und/oder →Standortdaten von →Telefon und →Internetkommunikation

(→Transaktionsdaten) zum Zwecke der Polizeiarbeit und Rechtsverfolgung erzwingen will. Die Aufbewahungsfristen sollen dabei länger sein als dies z.B. für die Abrechnung der Telekomanbieter notwendig wäre. Dies ist zu trennen von der →Quellen-TKU (→Bundestrojaner). Umstritten ist bei der Vorratsdatenspeicherung u.a. bei welchen Gesetzesverletzungen (nur schwere Verbrechen oder auch Zivilrecht, z.B. →Urheberrechtsverletzungen) auf solche Daten zugegriffen werden kann. 2020 war (mal wieder) eine Entscheidung auf EU-Ebene: der EUGH-Anwalt hat in einem Gutachten die Grenzen für eine solche Speicherung sehr eng gesetzt. https://www.derstandard.at/story/2000113323491/eugh-anwalt-staerkt-verbot-weitreichender-vorratsdatenspeicherung

Vorsatz: wissentliches und/oder gewolltes Handeln, siehe →Fahrlässigkeit. Jeder →Angriff setzt Vorsatz voraus, der Grund für vorsätzliches falsches Verhalten kann auch Bequemlichkeit sein

VoWLAN: (Voice over WLAN) Problematisch ist die Garantie der nötigen Bandbreite und die Übergabe zwischen →APs. →SVP Server kommen zum Einsatz. Siehe →VoIP, →DECT

VPN: →Virtual Private Network

VPN-Dienste: traditionelle →Virtual Private Networks werden hauptsächlich zur Verbindung innerhalb und zwischen Firmen eingesetzt. VPN-Dienste sind kommerzielle Angebote an Privatpersonen, die es ermöglichen, die eigene IP-Adresse zu verschleiern. Dies ist eine ähnliche Funktionalität wie sie →TOR bietet, jedoch mit möglicherweise besserem Durchsatz. Das Problem ist dabei, dass jedoch KEINE →Anonymität erreicht und die Sicherheit vollständig von der Qualität und der Vertrauenswürdigkeit des Dienstanbieters abhängt. Dies mag für Funktionalitäten wie das Umgehen des →Geoblockings von → Streaming Diensten wie →Netflix ausreichend sein, nicht jedoch wenn jemand durch die Behörden eines Landes bedroht ist. Die Liste von unsicheren Diensten ist sehr lang

VPN-Tunnel: typischerweise eine Verbindung die mittels des →IPsec →Protokolls im →Internet hergestellt wird. Ziel ist dabei entweder eine abhörsichere Übertragung (z.B. Vermeidung von Zensur) oder aber die Umgehung von →Geoblocking um z.B. →Streaming-Dienste zu erreichen die in einem bestimmten Land nicht verfügbar sind. Wenn solche VPN-Tunnel vom eigenen Unternehmen angeboten und implementiert wird, so ist dieses (typischerweise) recht sicher. Problematisch sind die VPN-Tunnel, die für Privatleute angeboten werden weil deren Nutzung angeblich eine gesteigerte Privatsphäre bedeutet. Dies setzt jedoch voraus, dass dieser Betreiber rein ehrenwerte Motive hat. Speziell wenn der Dienst kostenlos oder sehr günstig ist, so fragt man sich natürlich, wie das Geschäftsmodell aussieht.

Wie unter →VPN-Dienste beschrieben wird dabei jedoch KEINE →Anonymität erreicht und die Qualität und Sicherheit ist sehr unterschiedlich. Wirkliche →Anonmyität wird nur mittels korrekter und vorsichtiger Nutzung von →TOR erreicht

VR: (→virtual reality)

VRF: (Virtual Routing and Forwarding) implementiert mehrere unabhängige Routing-Tabellen in einem →Router und erlaubt damit →MPLS

VSAN (Virtual SAN): logische Strukturierung in einem →SAN. Funktioniert ähnlich wie eine →Zone, arbeitet aber auf einer anderen Schicht des →Fibre Channel Protokolls

VSS: (Volume Shadow Service, Volume Shadow Copy) Funktionalität des Windows 2003 Dateisystems, bei dem automatisch Schattenkopien von Dateien angelegt werden, die einen Rückstieg auf ältere Versionen auch dann ermöglichen, wenn der Anwender die Datei selbst überschrieben hat. Auch in Verbindung mit →SAN-Systemen oder dem Data Protection Server (DPS) von Microsoft ergeben sich verbesserte Datensicherungsmöglichkeiten. Siehe →Previous Versions

VTL: (virtual tape library) Verfahren zur Beschleunigung von →Datensicherungen. Dabei werden langsame →Magnetbänder durch →Magnetplatten simuliert (→Cache). Oft findet später eine Auslagerung auf Magnetbänder statt. Dies verkürzt das →Backup-Fenster. Auch Backup-to-Disk genannt

Vulnerability: (engl. Verwundbarkeit). →Schwachstelle im System oder der Konfiguration, die dazu führt, dass ein →Angreifer mitels →Exploit auf einem System Schaden anrichten kann, Gegenwehr durch Installation eines →Patches. Wie werden nach dem →CVSS System bewertet. Wichtige Typen haben eigene Abkürzungen wie →RCE, XSS, →CSRF. →CERT und andere veröffentlichen regelmäßig Listen mit entdeckten Vulnerabilities. Siehe →Vulnerability Scanner, →CVE

Vulnerabilities Equities Process: (VEP) die Vorgehensweise, wie die →NSA entscheidet, ob sie eine gefundene →Vulnerability an den Hersteller weitermeldet oder für eigene Zwecke, d.h. →Angriffe auf Systeme einsetzt. Leider gewinnt dann zumeist der Angriff gegenüber dem Schutz der eigenen zivilen Infrastruktur, was sich dann z.B. im erfolgreichen Angriffen der Nord-Koreaner, Chinesen und Russen auf Regierungssysteme wie das →Office of Personel Management (OPM) niederschlägt

Vulnerability Management: systematische Behandlung von →Schwachstellen in →Software und →Systemen. Siehe →Patch Management

Vulnerability Scanner: Softwaretool, das ein Computersystem oder Netzwerk gegen eine Liste von bekannten →Vulnerabilities testet. Als kommerzielles Produkt und als →Freeware verfügbar (→Nessus) und auch als Service

Vupen: franz.Firma die sich auf →Zero-Day →Vulnerabilities und andere →Surveillance Software spezialisiert hat. Kunden sind vor allem Regierungen in aller Welt. Siehe auch →FinFisher, →Hacking Team, →Black Hat

VW: (→virtual world)

VX: (virus exchange) →Website für den Handel mit →Malware. Siehe →organisierte Kriminalität, →Hacker

W3C: (World Wide Web Consortium) Standardisierungsorganisation für →Internet-Technologien, z.B. im Sicherheitsbereich. Siehe →SVG, →HTML, →WAI

WAF: →Web Application Firewall, erforderlich z.B. für →PCI-DSS 1.1, auch →WSF genannt

Wahlmaschinen: →e-Voting

Wahrscheinlichkeit: wichtiger Aspekt bei →Risikoanalysen. Wird aus psychologischen Gründen von Menschen nur sehr fehlerhaft abgeschätzt.
http://sicherheitskultur.at/notizen_2_06.htm#risks

WAI: (Web Accessibility Initiative) Aktivität der →W3C zur Definition von Anforderungen an →Websites, die auch für Behinderte zugänglich sind. →Compliance wird durch W3C-A, W3C-AA oder W3C-AAA ausgedrückt
http://www.w3.org/TR/WAI-WEBCONTENT/full-checklist.html

Walkthrough: Methode des Software→Audits. Systematisches Durchdenken der →Programm-Logik, oft in Verbindung mit einer 2. Person. Siehe →Code Audit

Walled Garden: Bezeichnung für die leider typischen Implementierungen von →Internet-Diensten wie →Social Networks durch zentrale Anbieter. Nur wer auf genau dieser Plattform ist kann mit Nutzern dieser Platform kommunizieren. →E-Mail zeigt, dass offene Standards möglich sind (hier →SMTP, bzw. →Websites mit dem Standard →HTML) so dass jede mit jedem kommunizieren kann. Alternative Plattformen die solche Kompatibilität für Social Networking implementieren wollen basieren z.B. auf →Fediverse und →Protokollen wie →ActivityPub. Die europäische Politik sollte große Anbieter wie →Facebook oder →Twitter zur Unterstützung dieser Standards zwingen, was deren Geschäftsmodell bedrohen könnte

Wallet: (engl. Geldbörse)

1) Digital wallets, e-wallets oder cyberwallets: Kombination aus Software und →Daten für sicheres Bezahlen im →Internet. Die Software händelt →Verschlüsselung und den Daten-Transfer, sehr oft in Form von Electronic Commerce Modelling Language (ECML). Die Daten enthalten Name, Anschrift, →Kreditkarteninformationen. Eine Version die Ende der 90er von den Kreditkartenfirmen gestartet wurde hat sich nicht durchgesetzt. 2011 gibt es eine Wallet von →Bitcoin und →Google Wallet. Der Begriff wird im Zusammenhang mit den Bezahlformen rund um →NFC genutzt. Verlust der →Passworte zu Wallets für ein virtuelle Währungen, →Cryptocurrencies, z.B. →Bitcoin, führt zum Verlust des Geldes. Siehe →Wallet Recovery

2) Oracle Wallet: Behälter für →X.509 basierte →Schlüssel. Kann genutzt werden um einer Anwendung →Zugriff zu ermöglichen ohne dass im →Programmcode das →Passwort enthalten sein muss. Abgelegt wird das Wallet entweder in der Datenbank oder der Windows Registry, geschützt mit einem →Passwort. Für →Programme ist Auto-Login möglich, Schutz dann nur über File-Permission

Wallet Recovery: spezielle Dienste, die versuchen, die →Passworte mit denen →Cryptocurrencies wie →Bitcoin verwaltet werden wiederzuerlangen. Dies ist schwierig, da aus Sicherheitsgründen die Anzahl der Versuche begrenzt sein sollte. Bei sehr frühen Investoren deren frühe Einlagen viel-tausendfach gestiegen sind, kann es sich um sehr große Vermögen handeln

WAN: (Wide Area Network) Verbindung zwischen Rechnersystemen über eine größere Entfernung auf der Basis von Telekommunikationstechniken (→POT [plain old telephone], →ATM [asynchronous transmission mode], →Frame-Relay, u.ä. Virtualisierbar mittels →MPLS

WAP: 1) (Wireless Access Protocol) Verfahren für die Darstellung von Informationen auf →Handys. Es benutzt ein auf →XML basierendes Darstellungsformat →WML. Die Übertragungen sind in einem zu →SSL ähnlichen Verfahren verschlüsselt. Hat sich nicht durchsetzen können

2) (Wireless Access Point) →Access Point

3) (Web Application Firewall) Absicherung des externen Kontakts einer Web-Anwendung durch Filterung des Datenverkehrs

War chalking: →Markieren von „offenen“ →WLANs durch Markierungen Kreidesymbole

War driving: Suche nach „offenen“ →WLANs vom Auto aus. Auch in Verbindung mit →war chalking. Wird 2013 von der →NSA auch von →UAVs ausgeführt (Codename → VICTORYDANCE) und kann auf diese Weise →WLANs und auch Geräte die WLAN-Verbindungen aufbauen wollen, großflächig identifizieren

Warez: Slangausdruck für →Raubkopie

Warm Site: Kompromiss zwischen →Hot Site und →Cold Site für →Recovery Zwecke

Wassenaar: das Wassenaar Arrangement ist

eine internationale Überkeinkunft, initiiert durch die USA, das den Verkauf von Waffen oder „dual use goods“ (die eine militärische und zivile Nutzun haben) unter Strafe stellen. 2015 wird vorgeschlagen, dass →Vulnerabilities und vor allem →Exploits (die als Proof-of-Concept) zumeist mitgeliefert werden, z.B. im Rahmen eines →Bug Bounty Programmes, unter das Abkommen fallen könnten. Dann müsste der Researcher eine Lizenz im Heimatstaat beantragen, der aber selbst an diesem →Zero-Day interessiert sein könnte. Dies ist ein Versuch, den Markt für →Black Hats zu regulieren, aber kann auch auf →White hats angewendet werden

Wasser: dritthäufigster Grund für →Katastrophen in →Rechnerräumen. Vorbeugung durch Wartung der →Klimaanlage und Schutz durch Wassermelder

Wasserfallmodell: Vorgehensmodell in der Softwareentwicklung, bei dem der Softwareentwicklungsprozess in Phasen organisiert wird, die wohldefinierte und -dokumentierte Übergänge und Endprodukte haben (z.B. →Pflichtenheft und →Lastenheft)

Wasserzeichen/Watermark: →elektronisches Wasserzeichen zur Markierung digitaler Inhalte, z.B. Musik oder Videos. Soll →Copyright-Verletzungen nachweisbar machen

Watering Hole Attack: →Angriff auf eine Firma oder eine bestimmte Branche indem eine →Website übernommen wird, so dass die Besucher dieser Website sich über einen →Zero-Day ihre PCs infizieren. „Watering Hole“, da eine Website ausgesucht wird, die branchen-spezfische Inhalte darstellt so dass viele Mitarbeiter des gewünschten Industriezweigs sie regelmäßig aufsuchen

Watt: Maß für die wirklich aufgenommene Energie eines Gerätes, im Unterschied zu →VA

WCF: (Windows Communication Foundation) Teil von →.NET, unterstützt die →Kommunikation zwischen →Anwendungen, z.B. →Client und →Server. Sicherheit kann durch die Nutzung von →WSS implementiert werden. Siehe →SOA, →WSDL

Wearable Computing: IT-Geräte die direkt am Körper getragen werden, z.B. in Form einer Datenbrille (→Google Glass, →Oculus Rift), siehe auch →augmented reality, →quantified self, →Lifebits, →virtual reallity

Web: Kurzform von →World Wide Web, www

Web 2.0: ungenau verwendeter Begriff für neuere Aspekte des →world wide webs, z.B. die Veränderung von →Websites zu Plattformen zum Informationsaustausch, die Tatsache, dass Schätzungen davon ausgehen, dass nur 40% der Inhalte des Webs von Firmen erstellt werden und neue Formen wie →Blogs, →Wikis, →Social Network Sites und neue Techniken wie →Web Services oder →AJAX. Auch verwendet für die Verknüpfung von Services und Anwendungen auf verschiedenen →Websites, wie Hausanzeigen mit Google-Earth. Technologien sind →AJAX und →SOAP. Experten befürchten neue Sicherheitsprobleme, da diese Anwendungen nicht mehr hinter zentraler IT, wie →Firewalls versteckt sind und viele Entwickler wenig Ahnung von sicherer Web-Programmierung haben. Siehe →iFrame

Web 3.0: neues Schlagwort für die Idee, dass eine genügend intelligente Verknüpfung aller Inhalte im →Web (→Semantic Web) Bedeutungen erkennt und intelligentere Antworten gibt als jetzige →Suchmaschinen

Web-Anwendung: →Web-Application

Web-Application: Anwendung im →Web, oft mittels Programmiersprachen wie →php, →Phyton oder →AJAX, die Interaktionen der →Benutzer erlaubt und oft anfällig für →Angriffe (z.B. →XSS, →CSRF, →Path Traversal, →SQL-Injection, →Buffer Overflow) sind. Siehe →OWASP, →Firebug, →Application Security, →ONR 17700, →WAF, →WSF

Web Application Firewall: (WAF) →Appliance vor einem →Webserver, der die Anfrage filtert und auf diese Weise →Angriffe wie →SQL-Injection, →Buffer Overflow und andere verhindern soll, wird auch →WSF genannt. Siehe →Application Level Gateway

Webauftritt: Präsenz einer Firma, Privatperson oder Organisation im →Internet, in der Regel in Form einer →Website. Realisiert entweder eigenen →Webserver oder bei einem →Webhoster

Web beacon: (engl. beacon = Leuchtfeuer) →Web bug

Webbrowser: →Browser

Web Bug: Technik zum Nachverfolgen, wann ein →E-Mail oder Office Dokument gelesen wurde, ob es weitergeleitet wurde und wohin. Meist wird dafür ein →HTML-Link zu einer Graphik (1x1 pixel) eingefügt. Wenn das E-Mail oder Dokument geöffnet wird, so wird die Graphik vom →Webserver geladen und dies hinterlässt im →Log des Servers entsprechende Spuren, die ausgewertet werden können. Dies wird zur systematischen Datensammlung genutzt und kann eine →Bedrohung der →Privatsphäre darstellen. Web Bugs werden vor allem verwendet seit die →Web browser immer bessere Möglichkeiten bieten um →3rd-party-cookies zu verhindern

Andere Namen dafür sind →web bug, web beacon, tracking pixel, tracking bug, pixel tag, und clear gif. Bei dem Abruf dieser winzigen Graphik können beliebige Daten über den Benutzer mitgeliefert werden, z.B. die eingestellte Sprache des Rechners, das →Betriebssystem, alle →Cookies und auch die Inhalte von Eingabefeldern. Wenn die Graphik zurückgesendet wird können dabei auch 3rd

party cookies gesetzt werden, sofern die Browsereinstellungen dies erlauben. Siehe →Referrer

Webcam: Videokamera deren Inhalte im →Web zur Verfügung gestellt werden, i.d.R. zur →Überwachung genutzt. Wenn dies (speziell im öffentlichen Raum) ohne Zustimmung der Betroffenen geschieht ist dies eine Verletzung der →Privatsphäre. Oft installieen die Betroffenen die Geräte selbst, z.B. sog. Nannycams (z.B. Teddybären) zur Überwachung von Babysittern, die ihren Zweck nur erfüllen, wenn auf sie auch von der Ferne zugegriffen werden kann. Siehe →CCTV, →M2M, →Internet of Things

WebTorrent: eine →P2P Technologie die es erlaubt, dass Videos zwischen →Browsern ausgetauscht werden. Wird z.B. bei →Peertube verwendet. Dies ist analog zu →BitTorrent, aber auf Browser-basis

WeChat: Messaging App von →Tencent, die aber auch Zahlungsdienste und viele weitere Funktionen integriert hat und deutlich umfassender ist als ähnliche Dienste von anderen Anbietern. Sie wird auch als →Super-App bezeichnet. Die App bietet eine →API für sog. Mini-Programs, die über die WeChat App Zahlungsdienste (→WeChat Pay), Bestellungen, Reservierungen, Kommunikation mit Kunden, usw. leicht implementieren können. Viele (auch kleinere) Unternehmen oder Geschäfte, aber auch Behörden, nutzen dies als einfache Kommunikation und Bestell- und Zahlungsabwicklung mit ihren Kunden (> 1 Mio Mini-Programs). Da alle diese Mini-Programms →Zugriff auf die WeChat ID der Kunden haben entfällt auch die Notwendigkeit von Kundenanmeldung. Das ist bequem für Nutzer und Firmen, aber totale Transparenz für alle Aktivitäten von Firmen und Nutzern. Alle →Daten können auch in das →Social Credit System einfließen. Siehe auch https://sicherheitskultur.at/Internet_politik.htm#china

WeChat Pay: in →WeChat integrierte Bezahlfunktion als Ersatz für →Bargeld, konkurriert in China mit →Alipay

WebDAV: (Web-based Distributed Authoring and Versioning) Erweiterungen von →HTML zum Austausch und bearbeiten von →Dateien mittels →http. →Schwachstellen in der Implementierung führen zu →Verwundbarkeiten

Webex: →Software für →Webkonferenzsysteme und →Fernwartung die von →Cisco übernommen wurde. Wie viele solche Dienste wird die Datenübertragung verschlüsselt, die Inhalte liegen auf den zentralen Servern in Klartext vor

Webhoster: Service der →Webserver für andere betreibt. Diese Webserver können entweder nur für einen Kunden dediziert sein, oder unter einer großen Zahl von Kunden geteilt werden (virtual hosting). Webhoster haben Aufgaben bei →Take-down

Webinject: Technik bei Schadsoftware vor allem im Bankenbereich, bei der falsche Website-Inhalte im →Browser des Benutzers angezeigt werden, so dass seine Login-Daten an die →Angreifer übermittelt werden können. Wird in sog. →Trojanern wie →Zeus und →SpyEye eingesetzt

WebInspect: Security Scanner für →Web-Applications. →Penetration Test

Webkonferenzsystem: →Software mit deren Hilfe →Videokonferenzen ohne spezielle →Hardware und →Software durchgeführt werden können, wurde 2020 durch →Home-Office zum Durchbruch verholfen. Beispiele sind →BigBlueButton, →Teams, →WebEx, →Google Meet, →GotoMeeting, →Skype, →Jitsi, →Zoom und viele andere. Bei fast allen dieser Systeme liegen auch bei Nutzung von →Verschlüsselung für die Datenübertragung trotzdem am zentralen →Server zumindest die Verbindungsdaten, meist aber auch die vollständigen Daten vor (Ausnahme z.B. →Messaging Dienst →Signal). Sonst wären Features wie zentrale Aufzeichnung der Konferenz ja nicht möglich

Die →Zugangs-Sicherheit von Webkonferenzen liegt typsicherweise zum einen in der Notwendigkeit, sich beim Anlegen und Starten eines Events vorher zu →Authentisieren. Dies gilt auch für alle Teilnehmer von geschlossen Konferenzen, z.B. innerhalb 1 Firma. Anderseits wurden 2020 viele öffentliche Konferenzen durchgeführt. Der Zugang zu dem Events besteht meist in der Kenntnis einer →URL mit einem Zufalls-String (die mittels →E-Mail versendet oder auf einer →Webseite publiziert werden). Typischerweise können beim Anlegen eines Events weitere Schranken für die externen Teilnehmer definiert werden. Da ist zum einen die Möglichkeit, dass jeder Teilnehmer aus einem Warteraum einzeln eingelassen werden muss (was bei großen Teilnehmerzahlen nicht möglich ist). Es können fast immer auch →Passworte gesetzt werden, was aber den Zugang für die breite Masse oft zu kompliziert macht. Des Weiteren kann beim Anlegen definiert werden, welche Rechte die Teilnehmer per-Default haben, z.B. Stummschaltung oder →Bildschirm teilen. Wenn dabei Fehler gemacht werden, so kann es zu Ereignissen wie →Zoom-Bombing kommen.

Es wird spekuliert, dass bei dem Durchbruch in 2020 auch →Metcalfe's Law relevant sein könnte. Vor 2020 fanden Meetings nur ausnahmsweise über →Webkonferenzsysteme statt, jedes Arbeiten von zu Hause zwang alle anderen ebenfalls zur Nutzung des Systems und die remote Nutzer waren nicht voll integriert. In 2020 wurde „remote" zum Standard und dies machte es einfacher für den

Einzelnen der zu Hause bleiben wollte

Webmail: Angebot vom →E-Mail-Zugriff über →Webbrowser (anstatt →POP3-Protokoll). Webmail hat den Vorteil, dass von jedem Internetzugang auf die Mails zugegriffen werden kann und dass dafür kein eigener Rechner benötigt wird. Oft als →Freemail angeboten

Web-of-Trust: Konzept, die Echtheit von digitalen →Schlüsseln durch ein Netz von gegenseitigen Bestätigungen (→Signaturen) zu sichern. Es stellt eine dezentrale Alternative zu → CAs dar. Siehe →PGP, →CACert

Web Page: →Webseite

Web Portal: →Website, die Benutzern den Zugang zu bestimmten Informationen, oder Angeboten erleichtern soll, manchmal die Informationen mehrerer Anbieter zusammenfassend, z.B. http://help.gv.at/, d.h. →Website, die über →Hyperlinks auf die anderen →Webserver verweist

Webradio: Übertragung kontinuierlicher Audioströme über das →Internet an vorgegebene →IP-Adressen, ohne dass der Nutzer einen bestimmten Titel angefordert hat. →Streaming Media, →Streamripper. Nutzung von Webradio durch die Mitarbeiter kann für Unternehmen einen Bandbreitenverlust darstellen und über Sicherheitslücken in der verwendeten Software zu zusätzlichen Risiken führen. Vergleiche dazu →Podcasting

Webradio-Recorder: Service, bei dem ein Nutzer einen bestimmten Musiktitel „bestellen" kann. Der Service „hört" bis zu 13000 Musikradio-Stationen und erzeugt, wenn dieser Titel irgendwo übertragen wird, eine →MP3-Datei. Dabei wird im Fall von Privatkopien in Ö das →Urheberrecht nicht verletzt

WebReady Document Viewing: Feature in Exchange 2007, durch die →E-Mail-→Anhänge vor deren Ansicht in →OWA zuerst in →HTML umgewandelt werden. Dies erhöht die Sicherheit

Webroot: Hauptverzeichnis in dem →Webseiten gespeichert sind. Auf alle →Dateien die im →Dateisystem des →Webservers innerhalb oder oberhalb des Webroots gespeichert sind, kann über Webzugriff zugegriffen werden und müssen daher sicher sein. →Angriffe versuchen oft, aus diesem Webroot auszubrechen und andere Verzeichnisse zu erreichen

WebRTC: (Web Real-Time Communication) ein Standard der Kommunikationsprotokolle und →APIs beschreibt, die eine direkte Verbindung von Rechner zu Rechner (ohne zentralen →Server) ermöglichen. Wird für →Webkonferenzsysteme, →Videokonferenzen, aber auch direkte →Dateitransfer genutzt. WebRTC ist in fast allen modernen →Webbrowsern implementiert. Die direkte Verbindung von Browser zu Browser ist aber bei Rechnern hinter einem →NAPT-→Router nur mit Hilfe von →STUN initial aufzubauen

Web Security Filter: (WSF) anderer Name für →WAF

Webseite: Objekt auf einer →Website, zumeist in →HTML-Format, das unter 1 →URL ansprechbar ist und Inhalte präsentiert, repräsentiert im →DOM. Typischerweise enthält 1 Website mehrere Webseiten. Eine Ausname bilden sog. →single-page applications die nur aus einer Seite bestehen, die mittels Javascript auf der Grundlage der Benutzereingaben dynamisch weitere Inhalte nachlädt, sehr oft genutzt für →e-Banking (siehe →REST, →SOAP). 2012 gab es bereits geschätzte 190 Mio Websites mit 8,42 Milliarden →Webseiten. Zusätzlich gibt es das →Deep Web

Webserver: Rechner mit dessen Hilfe eine →Website betrieben wird

Web Services: Protokolle und Standards, die die direkte Kommunikation zwischen Anwendungen im →Internet ermöglichen, meist beruhend auf →SOAP und →XML. Sicherheitsrelevant, die sich auch über diese Technologie Angriffe realisieren lassen werden, daher gibt es nun spezielle →Appliances zur Absicherung von Web Services und →XML

Webshop: Bereits 1984 von Tesco eingesetzte Lösung bei der ein Kunde Waren onlline bestellen kann. Heute, speziell nach →2020 sehr weit verbreitet, aber von einigen Firmen wie →Amazon sehr stark dominiert und in vielen Branchen, z.B. Elektronik, Reisebuchungen und Kameras eine Bedrohung für konventionelles Verkaufen. Siehe →Digital Market Act

Website: →Webauftritt im →Internet, das unter Nutzung des →HTTP-Protokolles Inhalte (zumeist im →HTML-Format) zur allgemeinen Betrachtung bereitstellt. Neben diesem Protokoll werden oft auch noch andere Protokolle und Inhalte verwendet, z.B. →Streaming Media oder →Active Content. Inhalte können statisch oder mittels →Web Applications interaktiv sein (siehe→single-page application, →REST, →SOAP). Websites bieten auch vielfältige Möglichkeiten zur Verbreitung bösartiger Software und ist auf Grund von oft fehlerbehafteter Implementierung oft selbst anfällig für Eindringversuche von außen. Jeder Website ist 1 URL zugeordnet (z.B. https://sicherheitskultur.at). Dieser URL ist dann ein →Webroot zugeordnet. Eine Website besteht typischerweise aus mehreren →Webseiten (z.B. https://sicherheitskultur.at/privacy). 2012 gab es geschätzte 190 Mio Websites mit 8,42 Milliarden Webseiten. Siehe auch →Deep Web

Web sockets: Funktionalität in →HTML5 mit deren Hilfe vom →Browser aus eine asynchrone Kommunikation mit einer Datenquelle aufgenommen kann. Diese Funktionalität könnte →AJAX ersetzen. Problematisch sind vor allem die →Schwachstellen in älteren Versionen die zum Teil noch

unterstützt werden und dass über →Cross-Origin Resource Sharing auch →Zugriffe auf anderen →Domains möglich sind

Websurfen: das Abrufen von Informationen von →Websites mittels eines →Web Browsers, dabei wird vor allem das →HTTP/ →HTTPS-Protokoll genutzt

WeChat: seit 2011 vielfältiger →Social Network Dienst von →Tencent. Er umfasst zusätzlich auch →Messaging und Zahlungsdienste. Seit 2018 die verbreitetste Mobile →App die speziell durch die Zahlungsdienste große Teile der Anforderungen für die meisten Benutzer abdeckt. „Official" accounts, die auch verifziert sein können, werden von Firmen, Behörden und Krankenhäusern für offizielle Dienste, wie z.B. Registrierungen oder Anträge genutzt. Die Zahlungsdienste erlauben ein Bezahlen bei sehr vielen Händlern und sind gegenüber dem traditionellen Bankensystem sehr bequem. Eine Konkurrenz dazu ist →Alibaba mit →Alipay

Weibo: →Micro-Blogging auf chinesisch. Am bekanntesten bei uns ist die Implemenierung von →Tencent Weibo und Sina Weibo, ähnlich zu →Twitter. Wobei in der chinesischen Schritt mit 140 Zeichen deutlich mehr kommuniziert werden kann als bei westlichen Schriften

WEP: (Wired Equivalent Privacy) Verschlüsselung für →Wireless Networks. Sie ist definiert im Standard 802.11. WEP erlaubt einem Administrator, mehrere Schlüssel für die Teilnehmer zu vergeben. Die Client PCs verwenden dann einen dieser ihnen zugewiesenen Schlüssel. Auch die neuste Version mit großer Schlüssellänge ist heute leicht zu knacken und daher unsicher. Nachfolger ist →WPA

Werbung: leider dominierendes Geschäftsmodell im heutigen Internet, hat das ursprünglich erwartete Modell von Abonnements weitgehend abgelöst (mit Ausnahmen ab ca. 2019, siehe z.B. →Netflix, →Spotify). Werbung wird seit ca. 2010 vor allem personenbezogen präsentiert. D.h. durch eine Analyse der auf dieser und vielen anderen →Websites über jeden einzelnen Benutzer gesammelten →Daten (→tracking) wird ein mehr oder weniger exaktes Persönlichkeitsbild gewonnen und dieses wird die Werbung zugeschnitten. Dies passiert während eine Seite geladen wird im Hintergrund durch Auktionen bei denen verschiedene Werbungskonzerne auf Grund der Daten über diesen Nutzer entscheiden, wem dieser Werbeplatz auf der Website am meisten Wert ist. Problematisch wenn dabei Werbung geschaltet wird die gezielt Probleme und Schwächen der Nutzer ausnützt, z.B. Suizidgefährdung, Esstörungen und ähnliches. Details siehe https://sicherheitskultur.at/spuren_im_internet.htm#eff

Western Union: weltweit aktiver Finanzdienstleister der anonyme Barauszahlungen ermöglicht und daher gern für kriminelle Aktivitäten wie z.B. →Ransomware, →DoS-Erpressungen o.ä. verwendet wird. →Money Mule. Ab ca. 2018 weitgehend von →Cryptowährungen für diese Zahlungen abgelöst, was zu einem Boom bei Ransomware geführt hat

Wetware: Bezeichnung der Bioholoniker für das menschliche Gehirn

WGA: (Windows Genuine Advantage) →Windows Software die prüfen soll, ob eine →Raubkopie eingesetzt wird. Positiv ist, dass Sicherheits→Patches auch in nicht-lizensierten Systemen eingespielt werden können

Whacking: Kurzform von 'wireless hacking'. Gemeint sind Hackerangriffe auf mobile Geräte, also Handys, →PDAs oder Notebooks. Mit der zunehmenden Vernetzung und Internetverbindung dieser Geräte werden solche Angriffe, oder auch Virenattacken, immer wahrscheinlicher

WhatsApp: →Messaging →Smartphone → App die für →Chat und →Messaging genutzt wird und bei Jugendlichen die Nutzung von (kostenpflichtigen) →SMS weitgehend abgelöst hat. Wie bei →Social Networks werden Gruppen von →friends gebildet, die sich gegenseitig über diese App erreichen können. Zumindest in der Anfangszeit gab es zahlreiche Schwachstellen, z.B. Übernahme fremder →Accounts. Mittlerweile wird →End-to-end →Verschlüsselung implementiert. Jedoch fallen beim Betreiber trotzdem →Meta-Daten an, nämlich wer mit wem wie intensiv kommuniziert. Problematisch ist ebenso, dass die Nutzung nur dann möglich ist, wenn der Nutzer den →Zugriff auf sein Adressbuch erlaubt. Das Konzept erlaubt den Zugriff auf die Profile von allen Personen, deren Handynummer man kennt. WhatsApp war zu Beginn nicht kostenlos, sondern kostete 1 US$ im Jahr, was bei 450 Mio Nutzern durchaus lukrativ war. Bereits 2014 wurden darüber weltweit so viele WhatsApp-Nachrichten wie →SMS gesendet. Whatsapp wurde von →Facebook (jetzt →Meta) gekauft und die Nutzerdaten mit →Instagram und Facebook integriert. Aus diesem Anlass wird über Alternativen berichtet, die sich ebenfalls durch End-to-end Verschlüsselung auszeichnen: →Signal, →Threema, MyEnignma, Heml.is, Whistle, →Telegram, →Matrix mit Element-Client

Whistleblower: Informant, der Missstände, illegales Handeln im Unternehmen, Korruption, Insiderhandel) oder allgemeine Gefahren an die Öffentlichkeit oder Behörden weitergibt, nachdem eine Behebung im Unternehmen ohne Erfolg verlief. Entsprechende Hotlines innerhalb des Unternehmens werden in →SOX gefordert, die Implementierung muss auf den →Datenschutz Rücksicht nehmen. Bekannte

Whistleblower sind →Edward Snowden, Bradley Manning, Daniel Ellsberg. Bis Ende 2021 müssen alle EU-Länder einen verbesserten Whistleblower-Schutz gesetzlich verankert haben, die meisten Länder sind in Verzug. →TOR ist ein gutes Tool um solche Dokumente so zu übermitteln, dass die eigene Identität nicht aufzudecken ist. Dafür gibt es zB. im →Darket →Websites von großen Zeitungen wie Süddeutsche, Spiegel, New York Times, →derStandard, Guardian, die auf diese Weise erreichbar sind. Aber auch für andere Whistleblower-Websites wie sie nun von Behörden und Firmen eingerichtet werden kann die Nutzung von →TOR die Identität schützen. →Messaging Systeme wie →Whatsapp sind nicht optimal, da dort, auch wenn die Nachrichteninhalte verschlüsselt übermittelt werden, doch umfangreiche Daten über die jeweiligen Nutzer vorliegen auf die Behörden (mittels Richterbeschluss) zugreifen können. Auch bessere Messenger wie →Signal sind für anonyme Aktivitäten nicht wirklich geeignet, da Signal dem Kommunikationspartner die Telefonnummer des Anfrufers immer anzeigt. Siehe auch →WikiLeaks, →NARUS,

White hat: in der IT Begriff für einen →Hacker mit „guten Absichten“, der z.B. →Penetration Tests durchführt

Whitelist: Verfahren im Kampf gegen →Spam und andere Schadsoftware. Der Empfänger gibt eine Liste von Adressen (bzw. Anwendungen) vor, von denen er bereit ist, →E-Mail zu empfangen, bzw. diese Programme auszuführen. Alle anderen Versender oder Programme werden abgelehnt. Dieses Verfahren ist deutlich sicherer als das →Blacklist Verfahren, erfordert aber mehr Verwaltungsaufwand verglichen mit einer automatisierten Aktualisierung einer Blacklist durch einen externen Service, z.B. →Virenschutzanbieter. Siehe →Greylist

White Space: In der Telekommunikation Frequenzen, die einem Rundfunkservice zugeordnet sind (häufig im UHF-Bereich), aber wegen der Umstellung auf DVB-T nicht mehr genutzt werden. In den USA wurde bereits eine Regel verabschiedet, dass solche Frequenzen durch unlizensierte Geräte genutzt werden können,z.B. um →Internet-Anbindungen zu erzeugen. Einige Bibliotheken, speziell in ländlichen Gebieten wo kein Breitband angeboten wird, wollen auf diese Weise ihre Ortschaften mit Breitband versorgen. Ähnliche Aktivitäten gibt es auch in anderen Ländern. In der EU befindet sich die Nutzung dieser Frequenz in Untersuchung

Whois: Dienst, mit dem →DNS Daten abgefragt werden können. Z..B. http://www.ripe.net/perl/whois

Widget: kleines →Programm das auf einer →Webseite eingebettet ist und eine bestimmte Funktionalität bietet, oft implementiert in →DHTML, →JavaScript oder →Flash. Sehr oft genutzt auf →Social Networking →Websites und im Rahmen von →Web 2.0. Kann natürlich auch schädlich sein

Wiederherstellung: (engl. →Recovery) nach einem →Vorfall oder →Disaster →Daten oder →Systeme wieder in einen betriebsbereiten Zustand. Dies setzt in der Regel eine vorherige →Datensicherung voraus

WiFi: Trademark der Wi-Fi Alliance. Firmenkonsortium, das Geräte mit Funk-Schnittstellen zertifiziert, Begriff wird synonym für →WLAN genutzt (WLAN ist nur im deutschsprachigen Raum gebräuchlich). Mehr Details unter →wireless networks

WiMAX: (Worldwide Interoperability for Microwave Access) drahtlose Technologie (IEEE 802.16) für den Austausch von →Daten und Sprache, die im Gegensatz zu →WLAN auch über große Entfernungen funktioniert, Breitbanddatenübertragung bis 6 km und bis 15 mbit/s. Dabei werden für verschiedene Frequenzbereiche unterschiedliche Verfahren eingesetzt. 2006 gibt es noch keine direkten Einschübe für →PCs, daher muss über ein spezielles →Modem die Verbindung zum →ISP hergestellt werden**.** Mögliche Konkurrenz zu →UMTS (2 mbit/s), altenative Option ist →White Space

Windows: Kurzbezeichnung für die verschiedenen Generation des MS Windows →Betriebssystem von Microsoft. Die Versionen bis einschließlich Windows ME enhielten fast keine Sicherheitsfeatures. Neuere Versionen sind erheblich sicherer, wegen ihrer breiten Verbreitung und den immer noch zahlreichen →Verwundbarkeiten sind sie jedoch vielfältigen Angriffen ausgesetzt. Siehe →Vista, Windows XP

Windows Phone 7: 2011 →Betriebssystem von Microsoft für mobile Geräte wie →Smartphone. →Sicherheitskonzepte inkludieren → Sandboxes für →Apps und kontrollierter →Market für Apps. Die weitere Entwicklung muss erst abgewartet werden. Windows Phone 7 ist 2012 durch Windows 8 ersetzt worden, das für →PCs und Smartphones eingesetzt wird

Windows XP: Sehr erfolgreicher Vorgänger von →Vista, auf dem Markt seit 2001, für den Anfang 2014 keine Security →Patches mehr zur Verfügung standen, aber noch auf >300 Mio Rechnern eingesetzt wird. Problematisch, da Angreifer aus den Patches für spätere Systeme wie →Vista sehr oft →Verwundbarkeiten von XP „→re-engineeren“ können, gegen die diese XP-Rechner dann keinen Schutz haben. Der Umstieg auf Win7 erfordert sehr oft neue Hardware, auch bei Geräten wie Druckern, weil für etwas ältere Geräte oft keine Treiber mehr verfügbar sind (→Obsoleszenz von an sich funktionsfähigen

Geräten) 2019 wird Windows XP zum Teil immer noch auf Spezialgeräten eingesetzt, z.B. Ansteuerungen für medizinische Großgeräte, bei denen bei jeglicher Änderung, z.B. →Patchen von →Verwundbarkeiten oder Aktualisierung auf ein sichereres Betriebssystem eine neue Zulassungsprüfung notwendig wäre. Solche Geräte sollten auf keinen Fall mit dem →Internet verbunden werden damit sie nicht angegriffen werden können (→airgap). Leider kann das aber nicht immer durchgängig implementiert werden

Wiki: →Programm zur Erstellung und Organisation von Informationen im Internet, die von den Benutzern nicht nur gelesen, sondern auch online geändert werden kann und zwar von allen. Bekannt ist →Wikipedia

WikiLeaks: Projekt zur Schaffung einer →Website, auf die anonym Dokumente geladen werden können, (z.B. über →TOR), die typischerweise über →Datendiebstahl gewonnen wurden. Diese Anonymität soll dem Schutz von Dissidenten und →Whistleblowern dienen. Eine wichtige Veröffentlichung war 2007 das Video „Collateral Murder" das die Erschießung von Journalisten im Irak durch eine Hubschrauberbesatzung zeigt. Die US-Soldatin Chelsea Manning musste dafür ins Gefängnis, wurde 2017 entlassen, kam 2019 - 2020 noch mal in Beugehaft: Bei der Publikation des Afghan War Diarys und der Iraq War Logs war intensiv mit verschiedenen Medienunternehmen zusammengearbeitet worden.

WikiLeaks bekam 2010/11 große internationale Aufmerksamkeit durch die Veröffentlichung einer großen Zahl von diplomatischen Berichten der USA und Dokumenten über das Gefangenenlager in Guantanamo Bay Naval Base. Auch die Veröffentlichungen des Abu-Ghuraib-Gefängnisses im Irak und viele weitere wichtige Veröffentlichungen sind dort passiert. Mittels →Domain-Sperrungen durch Behörden, aber auch →dDoS-→Angriffe durch →US-Behörden (mit Gegenangriffen durch →Anonymous) und die De-Aktivierung von Spendenmöglichkeiten wurde versucht, Wikileaks zu stoppen. Da bei Whistleblowing auch Unschuldige zu Schaden kommen können sind Aktionen auch kritisiert worden. Julian Assange, einer der Gründer wurde 2010 wegen einer schwedischen Anzeige zu sexueller Nötigung in Großbritannien verhaftet, verbrachte dann 2012 – 2019 in der Botschaft von Ecuador. 2019 wurde er in London verhaftet, es liegt ein Auslieferungsantrag der USA vor die eine Maximalstrafe von 175 Jahren bedeuten könnte. Seitdem wird seine Auslieferung juristisch bekämpft

Wikipedia: im →Internet in vielen Sprachen verfügbare Enzyklopädie, die von Nutzern selbst inhaltlich erstellt und gepflegt wird. Enthält viele wertvolle Hinweise auch zu allen Fragen der Informationssicherheit. Alle Informationen unterliegen dem →Copyleft-Prinzip und →Creative Commons und werden in Anlehnung an ein →Open Source Modell erstellt. Wikipedia ist es innerhalb relativ kurzer Zeit gelungen, die jahrhunderte alte Tradition von kommerziell erstellten Lexika oder Enzyklopädien (oft in einer großen Zahl von Bänden) zu zerstören. 2020 ist sie der wichtigste nichtkommerzielle Dienst im →Internet. Sie enthält heute mehr als 55 Millionen Beiträge in knapp 300 Sprachen.

Seit den 80iger Jahren wurden erste Lexika auf CD-ROM angeboten, ein Erfolg war vor allem die Microsoft Encarta. Nach 2001 übernahm die Wikipedia den gesamten Markt. Problematisch wird mittlerweile gesehen, dass durch die freiwillige und ungesteuerte Mitarbeit starke Verzerrung bei der Abdeckung von Inhalten entstehen. So sind europäische Themen sehr stark abgedeckt, afrikanische z.B. fast gar nicht. Deutschsprachige Inhalte haben einen überproportionalen Anteil (verglichen mit der Verbreitung der Sprache selbst). Ein weiteres Problem ist die manchmal schwierige Korrektur von inkorrekten Inhalten. Siehe →Wiki. http://de.wikipedia.org/

Wikiscanner: →Website zur Identifizierung von anonymen Änderungen auf →Wikipedia. http://wikiscanner.virgil.gr/

WinCE: mittlerweile obsoletes →Betriebssystem für →PDAs und →Smartphones von Microsoft, 2011 kaum noch in Benutzung, Nachfolger ist →Windows Phone 7, das mittlerweile ebenfalls obsolet ist

Window of Exposure: Zeitspanne von der Veröffentlichung einer →Schwachstelle (oder →Exploits) bis zur Behebung durch Implementierung des →Patches

WINE: öffentlich verfügbare Datensammlung von Symantec zu →Verwundbarkeiten. Schadsoftware und →Exploits seit 2008

Wipe: 1) mehrmaliges Überschreiben der →Daten einer →Festplatte mit Zufallszahlen bevor diese entsorgt wird. Ziel ist, sicher zustellen, dass ein zukünftiger Besitzer auch mittels →Data Recovery Techniken keine Daten mehr lesen kann. Kostenlose Programme stehen im Internet zur Verfügung. Bei neueren Platten ist bereits das einmalige Überschreiben ausreichend

2. Für das Löschen von →Flash-Speichern, z.B. →Smartphones, müssen spezielle Programme eingesetzt werden die mit dem Wear Leveling der Speicher umgehen können

2) →Remote Wipe →bei Smartphones

Wire: →Messaging →Software für verschlüsselte Kommunikation inkl. Sprache und Video, file sharing, etc. erzeugt von Wire Swiss

Wireless Networks: verschiedene Technologien um Geräte ohne Verkabelung miteinander zu einem Datennetz zu verbinden. Dabei

werden entweder Infrarot oder Radiowellen eingesetzt. Heute fast immer Synonym für die Vernetzung durch Radiowellen. Implementierungen sind z.B. →WLAN (Wi-Fi) und WiMAX oder die →Handy-Netze wie →GPRS, →UMTS, etc.

WLAN gilt auf Grund der relativ leichten Abhörbarkeit als eingeschränkt sicher (→Ethereal). Es werden zwar heute die Dateninhalte zumeist verschlüsselt, aber nicht die sog. Management frames. So wurde 2013 gezeigt, wie WiFi-gesteuerte Drohnen durch ein „deauthentication" Kommanda entführt werden können. WLAN sollte nur in Verbindung mit →WEP/→WPA oder sogar →VPN benutzt werden, aber auch dann besteht große Anfälligkeit gegen →DoS. Eine weitere Möglichkeit für Wireless Networks ist →Bluetooth

Wireshark: neuer Name für →Ethereal

Wiretap: legales →Abhören von Telefonaten nach Richterbeschluss. Diese Funktionalität ist in allen kommerziellen Telefonswitches integriert. Wurde in Griechenland 2006 illegal genutzt. Siehe →Lawful Intercept, →Überwachung http://www.spectrum.ieee.org/print/5280

Wirtschaftlichkeitsberechnung: Siehe →ROI, →NPV, →IRR

Wirtschaftskriminalität: interne oder externe Sicherheitsbedrohung für Unternehmen. Formen sind u.a. Betrug, Bilanzfälschung, Berichtsfälschung, →Wirtschaftsspionage / Industriespionage, →Social Engineering, Unterschlagung, Diebstahl, Bestechung, Korruption. Siehe →Sarbanes-Oxley Act, →KonTraG, →computer crime

Wirtschaftsspionage: private oder staatlich gelenkte oder gestützte, von fremden Nachrichtendiensten, oder anderen Organisationen, ausgehende Ausforschung im Zielbereich →Wirtschaft. Eine der Methoden ist →Social Engineering, aber auch →Erpressung und Bestechung werden eingesetzt, oft auch gezielt versendete speziell programmierte →Spyware. Siehe →ECHELON, →APT

Wissen: interpretierte, klassifizierte und in Beziehung gesetzte, vernetzte →Information

WLAN: (wireless LAN, auch Wi-Fi) drahtloses Netz auf der Grundlage von →IEEE 802.11. Mehr Details unter →Wireless Networks, →hotspot. Kenntnis der →Zugangs→passworte kann nach einer Trennung zu →digitaler Gewalt genutzt werden. Daher ist nach einer Trennung ein Zurücksetzen aller →Passworte wichtig

WLAN knocking: an → Port Knocking angelehnte Methode, um den Zugang zu einem →WLAN nur nach Durchführung mehrerer Schritte zu erlauben

WML: (Wireless Markup Language) →WAP

World-Check: privat betriebene kostenpflichtige Datenbank zur Verhinderung von Geldwäsche und Terrorismusfinanzierung mit 300.000 Einträgen, datenschutzrechtlich bedenklich. Wird weltweit genutzt (u.a. von der UN) und soll in Ö durch die Gewerbeordnung verpflichtend werden. Siehe →PEP

World of Warcraft: (WoW) Beispiel eines →MMORPGs mit 4,5 Mio. Benutzern. Wie alle anderen →virtuellen Welten auch Ort von →Angriffen und Betrügereien

World Wide Web: (www) Name für die Gesamtheit der über →Hyperlinks verknüpften Dokumente im →Internet. Internet und →Web werden oft synonmym genutzt, aber das Internet ist nur das Transportmedium für viele Dienste, eines davon ist Web, andere sind →E-Mail, →Messaging, →Telephonie wie →Skype, etc. →Suchmaschinen durchsuchen das Web, nicht das Internet. Das Web besteht nur aus den Diensten, die mittels →Browser genutzt werden und mit →URLs der Form →http:// oder →https:// beginnen.

Begründet wurden die grundlegenden Technologien wie Hyperlinks, →HTML, →Webbrowser und URLs 1989 durch Tim Berners-Lee, andere Aspekte wie →TCP/IP und →DNS lagen bereits vor. Der nächste Schritt war dann der Browser NCSA Mosaic in 1993, gefolgt vom sehr populären Browser →Netscape Navigator in 1994, das den Browsermarkt in den 90igern dominierte

WORM-Platten: (Write Once-Read Many) nur einmal beschreibbare, jedoch mehrfach lesbare Speichermedien, z.B. bespielbare CD-ROM oder →DVD. Die Unveränderbarkeit der →Daten nach der erstmaligen Bespielung ist vor allem in Hinblick auf die Beweiskraft der Aufzeichnungen wesentlich

WoW: (→World of Warcraft)

WPA: neuer Standard zum Verschlüsseln von →Wireless Networks, Nachfolger von →WEP, gilt als deutlich sicherer, wurde jedoch 2008 auch geknackt. Siehe →TKIP

WPAN: (Wireless Personal Area Network) drahtloses Netzwerk, verglichen mit →WLANs mit geringerer Sendeleistungen und Reichweite, z.B. auf →Bluetooth- oder →ZigBee-Basis

WPS: (Wi-Fi Protected Setup) standardisierter und vereinfachter Weg um bei einem →WLAN →Router die Einstellungen vorzunehmen, z.B. die Konfiguration →Verschlüsselung. 2011 wird eine Designschwäche entdeckt die über →Brute Force →Angriffe ausnutzbar ist. 2014 werden weitere noch effektivere Angriffe gefunden. Alternativ gibt es auch eine sichere Methode „push button connect"

WSDL: (Web Services Description Language) Beschreibungssprache für →Web Services auf →XML Basis. Einsatz oft zusammen mit →SOAP für die Entwicklung von →single-page applications

WS FS: WS-Federation, Konzept von einer

Reihe von Firmen um auf der Basis von →Web Services →Authentisierungsdienste zu implementieren, die auch über Organisationsgrenzen hinweg funktionieren. Auf dieser Grundlage kann z.B. →SSO implementiert werden. Dabei werden Technologien wie →SAML, →OAuth und →OpenID genutzt

WSF: (web security filter) anderer Name für →WAF

WSS: (Web Services Security) →OASIS-Standard für Sicherheitsimplementierungen für →Web Services, enthält z.B. →Kerberos, →X.509 und →SAML. Siehe →SOAP

WSUS: (Windows Server Update Service) kostenloses →Programm von Microsoft zur zentralen Verwaltung von →Patches. Analyse des Patch-Zustandes und Verteilung der Patches. Arbeitet mit →„Automatic Update" im Client-PC zusammen, Nachfolger von →SUS. Siehe →SMS

Wuala: →Cloud service zum speichern von →Dateien, nutzt, so wie das korrekt ist, →Schlüssel die nur auf den Endgeräten des Benutzers gespeichert sind. Dadurch haben auch →Administratoren keinen Zugriff. Im Gegensatz dazu →Dropbox

Wurm: →Programm, das sich wie ein →Virus vervielfältigen kann, das aber im Gegensatz zum →Virus kein Wirtsprogramm benötigt, das infiziert wird. Versendet sich oft selbstständig an andere Rechner zwecks deren Infizierung. Eine Untermenge von →Malicious Code

WWN: (World Wide Name) 64-bit Kennung einer →Fibre Channel Komponente. Entspricht der →MAC-Adresse im Ethernet-Bereich. Sie wird für die →Ports von →Switches, →HBAs und →HAs vergeben

WWW: →World Wide Web

X.12: eigentlich ASC X.12. US-amerikanischer Standard für die Formatierung von Geschäftsdokumenten, →EDI-Standard. Unterstützt in der Standardimplementierung weder →Signatur noch →Verschlüsselung

X.25: veraltetes Verfahren zur Übertragung mehrerer Kommunikationsverbindungen über einen einzelnen Datenkanal. Heute durch →ATM und →Frame Relay verdrängt

X.400: alter →E-Mail Standard, heute durch →SMTP verdrängt. X.400 hatte eine Reihe von Sicherheitsfeatures, z.B. gegenseitige →Authentifizierung der →MailServer und optionale Rückmeldungen bei Zustellung und Lesen eines E-Mails, die sich nur rudimentär in SMTP finden. X.400 hat sich nicht durchgesetzt, u.a. weil es wegen der expliziten Authentisierung aller anderen MailServer aufwendiger zu implementieren und die Software [im Gegensatz zu sendmail (smtp)] kostenpflichtig ist

X.500: Standard für →Directories (→Verzeichnisdienst). Der Standard deckt nicht nur die Kommunikation einer Anwendung mit der Directory ab, sondern auch Verfahren für eine Synchronisation. Wird heute meist durch →LDAP ersetzt

X.509: Standardformat der →ITU-T für digitale →Zertifikate. Es beinhaltet den Namen des Ausstellers (Zertifizierungsinstanz), Informationen über die →Identität des Inhabers sowie den öffentlichen Schlüssel, signiert mit der digitalen Signatur des Ausstellers. http://www.ietf.org/rfc/rfc3280.txt

X.521: Standard für die Abbildung von Unternehmensstrukturen und Zugriffsberechtigungen in einer →X.500 Datenstruktur

X.800: Empfehlung der →ITU-T für „Security Standard for Open System Interconnection", definiert 8 Dimensionen von IT-Sicherheit: →Access Control, →Authentifizierung, →Non-Repudiation, →Vertraulichkeit, Kommunikationssicherheit (z.B. →VPN, →L2TP), →Integrität, →Verfügbarkeit, →Privatsphäre. Zu ergänzen ist m.E. noch →Accountability

X.805: Empfehlung der →ITU-T für „Security Architecture for Systems providing end-to-end Communication", sehr ähnlich zu →X.800. Definiert die Anforderungen für jede Schicht des OSI-Schichtenmodells →IEEE 802.2

x86: Beispiel einer →CPU-Architektur die bereits seit 1978 genutzt wird und heute noch stark eingesetzt wird. Die ursprünglichen Implementierungen kamen von →intel, solche Chips werden aber auch von AMD, Cyrix u.a. hergestellt. Seit 1981 kam diese Architektur in den →IBM-→PCs zum Einsatz und wurde so Teil des Durchbruchs der ‚personal computings'

XACML: (Extensible Access Control Markup Language) von der →OASIS Organisation vorgeschlagener Standard für die Kodierung von →Zugriffsberechtigungsinformationen in →XML Format

XAML: (Extensible Application Markup Language) von Microsoft entwickeltes Datenformat auf →XML-Basis, genutzt in →Silverlight und →XBAP

XBAP: (→XAML browser application) →Programm auf der Basis von →.NET, das in einem →Webbrowser gestartet werden kann. Es läuft in einer →Sandbox ab und hat eingeschränkte →Zugriffe zum System

Xbox: seit 2001 Spielkonsole von →Microsoft, seit 2013 als Xbox One mit Kamera im Kinect motion sensing die Bewegungen im Raum so analysieren kann, dass über Bewegungen die Spiele gesteuert werden können. Microsoft sieht die Xbox als Media Platform, über die auch Fernsehen, Filme, →Skype etc. genutzt werden sollen. Die Kamera kann dabei auch die Zahl und →Identität von Personen, Geschlecht und andere Details analysieren und weitermelden. Problematisch ist, dass die Kamera nicht ausgeschaltet werden kann und

das Gerät zuerst gar nicht ohne Verbindung zum →Internet nutzbar war

XCBF: (XML Common Biometric Format) von der →OASIS Organisation vorgeschlagener Standard für die Kodierung von →biometrischen Informationen zur →Authentisierung

xDSL: →DSL

XHMTL: (eXtensible HyperText Markup Language) Darstellungssprache im →Web, die die gleichen Darstellungsmöglichkeiten wie →HTML bietet, aber eine strengere Syntax hat. XHTML beruht nicht wie HTML auf →SGML, sondern auf →XML

XHR: (→XMLHttpRequest)

Xing: 2003 gegründetes hauptsächlich beruflich genutztes →Social Network mit Sitz in Hamburg. Eine Alternative zu →LinkedIn, das zu Microsoft gehört. Wie LinkedIn implementiert nach dem →walled garden Konzept, d.h. nur Xing Mitglieder können Xing-Nachrichten lesen. Wird sehr stark für die Suche nach Job-Angeboten und neuen Mitarbeitern genutzt. Aber auch →Social Engineering lässt sich über so eine Platform leicht betreiben

XKeyscore: Programm der →NAS für die intelligente Analyse (mittels sog. Selektoren) von →Daten die durch verschiedene Überwachungsmethoden gewonnen wurden, z.B. →Tempora oder →PRISM und vielen anderen. Bekannt wurde das Programm durch die Veröffentlichungen von →Edward Snowden

XML: (Extensible Markup Language) Subset und Erweiterung von →SGML (Standard Generalized Markup Language), textorientierte Metasprache, von der →W3C entwickelt. Auf Basis dieser Konventionen erlaubt XML die Definition von spezifischen „Tags“, die auf bestimmte Aufgabenbereiche zugeschnitten sind. Ziel ist die semantische Beschreibung von Daten, so dass diese zwischen unterschiedlichen →Anwendungen ausgetauscht werden können. Der Einsatz von XML kann außer über das →Internet auch über jedes beliebige Kommunikationsmedium durchgeführt werden. Die in XML verwendeten „Tags“ werden in einer →DTD definiert. Das Dokument, zusammen mit seiner DTD, erlaubt eine automatische Überprüfung der Syntax und zusammen mit einem →XSL-Dokument die automatische Darstellung

XML DSig: von einer gemeinsamen Arbeitsgruppe von →W3C und →IETF vorgeschlagener Standard zur Repräsentation von →digitalen Signaturen mit Hilfe des →XML Formates

XMLHttpRequest: (→XHR) wichtiges Element von →AJAX. Erlaubt dynamisches Nachladen von Inhalten ohne Neuaufbau der Seite. Problematisch unter Sicherheitsaspekten, da der Benutzer bei „bösen“ XHR keine optische Rückmeldung des Datentransfers bekommt, wird von →Schadsoftware verwendet um →Schlüssel anzufordern, mit deren Hilfe →JavaScripts vor der Ausführung entschlüsselt werden

XMPP: (Extensible Messaging and Presence Protocol) wird genutzt für Anwendungen die →Chatrooms oder →Messaging Dienste implementieren wollen. →Verschlüsselungen, z.B mittels →TLS werden empfohlen, sowohl für die Verbindung vom →Client zu dem notwendigen zentralen →Server im →Internet, wie auch zwischen möglichen mehreren Servern. Trotzdem können solchen Dienste extrem unsicher sein, Hauptschwachstelle bei →WhatsApp ist z.B. die →Identifizierung und →Authentisierung der Benutzer. Dadurch ist es leicht andere Benutzer zu simulieren oder deren Botschaften zu empfangen. 2013 wird als Reaktion auf →Edward Snowden →end-to-end →Verschlüsselung geplant

XPS: (Extrusion Prevention System) neues Schlagwort als Folge des →California Security Breach Information Act. Lösungen, die einen →Vertraulichkeitsverlust von →sensiblen →Daten verhindern sollen, z.B. durch Kontrolle von →USB-Ports. Siehe →DLP

XSL: (Extensible Stylesheet Language) erlaubt die Spezifikation der Darstellung eines →XML Dokuments auf Schirm oder Papier

XSS: (cross-site scripting) →Angriff auf →Webbrowser, bei dem nicht-vertrauenswürdiger Inhalt in vertrauenswürdige →Websites eingefügt wird, z.B. im Rahmen eines Gästebuchs, einer Verkaufsanzeige, eines →Blog-Kommentars, nicht zu verwechseln mit →CSRF. Man unterscheidet persistent XSS und non-persistent.

Bei **non-persistent XSS** muss der Angreifer dem Opfer einen Link auf die verwundbare Website schicken, in dem der Angriffscode bereits enthalten ist.

Bei **persistent XSS** gelingt es dem Angreifer den Schadcode, z.B. als Kommentar in einem Blog oder Gästebuch in die →Datenbank des →CMS einfügen zu lassen. Dadurch werden alle Leser dieses Blogeintrags infiziert ohne dass der Angreifer noch mal aktiv werden muss. XSS eignet sich für eine Infektion des PCs mit →Malware oder →Authentication-Bypass z.B. durch →Zugriff auf →Cookies. Wird verhindert durch konsequentes Checken von Input und Output in →Web-Applications. →CSP ist ein Versuch in 2011 Funktionen anzubieten, mit denen dieser Angriff erschwert wird. Eine spezielle Variante ist →**self-XSS**. Dafür muss der Browser eine →Verwundbarkeit haben die es erlaubt, dass vom Angreifer eingefügter Code, zumeist →JavaScript, auf der Website ausgeführt wird. Um die Benutzer dazu zu bringen kann man z.B. erklären, dass dieser „magic code“ für ein Gewinnspiel notwendig sei (→Social Engineering).

Ziel von XSS ist oft der →Zugriff auf →Cookies, entweder → Session Cookies während das Opfer auf einer →Website (z.B. Bank) online ist, oder ein genereller Zugangs-Cookie der einen Zugriff ohne neuerliche →Authentisierung erlaubt. Siehe auch →HTML-Injection, →SOP

Y2020 bug: Siehe →Y2K bug

Y2K bug: →Software-Problem beim Wechsel in das 2. Jahrtausend. Programmierer hatten sich auf Grund der beschränkten Resourcen in frühen →Computern angewöhnt, Jahreszahlen nur 2-stellig zu speichern (z.B. ‚781231' für Sylvester 1978). Dies hätte am 1.1.2000 dazu geführt, dass dieses Datum als 1.1.1900 ausgewertet würde. Mit einem sehr sehr großen Programmieraufwand wurden alle →Programme auf diesen Fehler hin untersucht und (fast immer) die Speicherung des Jahres auf 4-stellig umgestellt. Bis auf einige Fälle, in denen folgende Logik im Programm eingebaut wurde: falls Jahreszahl <20, interpretiere dies als 20xx. Dies führte am 1.1.202 zum Ausfall von einigen Finanzsystemen, dies ist der Y2020 bug. Ob weitere ähnliche Fallen in alten Programmen versteckt sind werden weitere Jahreswechsel zeigen

Youtube: zugekaufter Videodienst von →Google. Auf Basis der Kommentierungs-funktion auch ein →Social Network. Wird auch für die Verbreitung von Videos genutzt die unter →Copyright stehen. In diesem Fall entfernt Google die Videos nach einer Beschwerde des Rechteinhabers. Wird auch für →Cyber Bullying genutzt. Benutzer die dies sehen können zu jedem Video eine entsprechende Meldung machen. Dann werden die Inhalte (zumeist) entfernt. Firmen müssen sich bei unerwünschten Videos gut überlegen, wie sie damit umgehen. Details unter →reputation repair. Seit ca. 2018 wird das Radikalisierungsp otential des Vorschlags-algorithmus von Youtube kritisch bewertet. Untersuchungen zeigen, dass die Vorschläge für weitere Videos dazu neigen, immer sensationellere Videos zu liefern. Dies soll dazu führen, dass die Nutzer möglichst lange auf Youtube bleiben. Alternativen sind z.B. Dailymotion, →Vimeo und →PeerTube (letzteres auf Basis der verteilten Konzepte von →ActivityPub)

YubiKey: hardware-basiertes →Authentisierungsgerät in Form eines Schlüsselanhängers. Implementiert ein one-time Passwort (→OTP) und unterstützt die →Protokolle →U2F und FIDO2. Wird in den →USB-Slot eines Gerätes eingesteckt und emuliert dort eine →Tastatur, d.h. kann die →Passworte direkt eingeben. Auch in einigen →Passwort Managern unterstützt. Implementiert →HOTP und →TOTP. Siehe auch →Nitrokey

Zahlendarstellung: Teil jeder →CPU-Architektur ist eine bestimmte Art, wie Zahlen im →Computer dargestellt werden. Dies geschieht immer im Binärformat. Bei positiven Ganzzahlen (→‚integer') ist dies typischerweise einfach die Übertragung aus dem „Zehnerland" in das „Zweierland". Bei negativen Zahlen wird das Vorzeichen oft als ‚höchstes' →Bit gespeichert und der Rest komplementiert („Zweierkomplement". Dies vereinfacht die Rechenarithmetik. Die Anzahl der Bits die für ein ‚integer' verwendet wird bestimmt die maximale Größe einer Zahl und hängt von der CPU-Architektur ab. In den →Programmiersprachen werden oft unterschiedlich lange Integer angeboten, oft von 8 bit bis 128 bit. Für spezielle Anforderungen der Numerik, z.B. Berechnung großer Primzahlen sind beide Darstellungen nicht geeignet. Dafür müssen die Zahlen in einer reinen Binärdarstellung abgelegt und verarbeitet werden, was der →Befehlssatz eigentlich nie direkt unterstützt.

Bei rationalen und reelen Zahlen (‚→Gleitkomma', ‚real', ‚floating point', ‚float') ist nur eine annähernde Darstellung möglich. Dabei wird die Zahl in eine Mantisse und den Exponenten zerlegt die in getrennten Bits abgelegt werden. Moderne CPU-Architekturen haben →Befehle für Gleitkommaarithmetik, zumeist getrennt für Zahlen einfacher und doppelter Genauigkeit (die sich durch die Anzahl der Bits der Mantisse unterscheiden). Da Gleitkommadarstellungen für die meisten Zahlen nicht exakt möglich sind, kommt es dabei zu Rundungsfehlern, die bei Geldberechnungen nicht akzeptabel sein können. Dort müssen Festkommadarstellungen genutzt werden, in einigen →Programmiersprachen als →Datentyp ‚currency'. Ein weiterer Spezialfall ist →BCD

Zapper: Klasse von Software die eingesetzt wird, um die →Buchführung von Restaurants o.ä. zu „frisieren", oft installiert auf →Flash-Speichern. Die Löschung von Einnahmen wird so durchgeführt, dass auch in der doppelten Buchführung keine Spuren verbleiben

Zeitstempel: mit einer →digitalen Signatur versehene digitale Bescheinigung einer →Zertifizierungsinstanz, die bescheinigt, dass bestimmte digitale Daten zu einem bestimmten Zeitpunkt vorgelegen haben (Beweis der Existenz zu einem Zeitpunkt)

Zero-Click Exploit: Eine →Verwundbarkeit, die ohne Nutzerinteraktion funktioniert. Ein Beispiel ist der ‚Pegasus' genannte →Angriff der Firma →NSO auf →iOS-Geräte von →Apple bei dem das Empfangen einer →Message ausreicht, um das Gerät bis zum nächsten Neustart zu kontrollieren. Ein solcher Exploit ist typischerweise auch ein →Zero Day Exploit

Zero Day: →Verwundbarkeit die noch nicht öffentlich bekannt ist und für die es daher noch keine →Pattern in →Antivirus-Software oder

→IPS gibt und es auch noch keinen →Patch gibt. Siehe →Bug Bounty

Zero Day Exploit: Tools zum →Angriff auf →Zero Day Schwachstellen. Zero Day Exploits werden heute kommerziell gehandelt. Neue →Exploits werden oft am Tag nach dem →PatchTuesday veröffentlicht, dies sichert mindestens 4 Wochen ungeschützte Systeme. Sie werden zum Teil auf online-Börsen gehandelt (zero day bounty). Gekauft werden sie von kriminellen Organisationen, aber auch von staatlichen Stellen für die Nutzung in →Bundestrojanern oder anderer staatlicher Überwachungssoftware (→Federal Spyware), aber auch für →targeted attacks im Rahmen von →Cyber Spionage oder →Cyberwar. Der Handel mit solchen Schwachstellen wie auch die Veröffentlichung dieser Schwachstellen bevor →Patches zur Verfügung stehen ist umstritten, das Thema wird als →Disclosure bezeichnet. Siehe →FinFisher/Finspy

Zero-order entropy: Entropy in der Informationsswissenschaft bezeichnet den Informationsgehalt eines Datenelements. Siehe →Passwort

Zero-knowledge proof: Verfahren der →Kryptographie, bei der ein Teilnehmer (*prover*) gegenüber einem anderen Teilnehmer (*verifier*) beweisen kann, dass eine Behauptung *wahr* ist. Im konkreten Fall normalerweise die Behauptung, eine gewisse Information zu besitzen, ohne diese jedoch preis zu geben. Eingesetzt als → Zero-knowledge password proof

Zero-knowledge password proof: (ZKPP) →Authentisierungsmethode, bei der eine Partei der anderen beweist, dass sie ein →Passwort kennt ohne das Passwort zu verraten, sicher gegen →Dictionary Attack. Durch →Hash-Funktionen soll diese Sicherheit erreicht werden. Siehe →SRP

Zertifikat: Beglaubing, Bescheinigung

Zertifikat (digitales): von einer vertrauenswürdigen Instanz digital signierter öffentlicher Schlüssel, damit dieser als authentisch anerkannt wird. Die verbreiteste und bekannteste Festlegung des Aufbaues und Codierung von Zertifikaten ist die →X.509-Norm, Zertifikate sind elektronische Gegenstücke zu Ausweisen. Ein Zertifikat bindet einen Namen einer Person oder Institution an deren öffentlichen Schlüssel. Ein Zertifikat ist eine spezielle Datenstruktur, die Informationen zu einem öffentlichen Schlüssel und dessen Besitzer beinhaltet, sowie einige Verwaltungsinformationen, wie z.B. den Gültigkeitszeitraum, den verwendeten →Verschlüsselungsalgorithmus, etc. Ein Zertifikat ist immer digital signiert, um seine Echtheit zu bestätigen. Diese elektronische Unterschrift sichert das damit unterzeichnete Dokument vor Verfälschung auf seinem Weg durch das Internet (→Public-Key-Verschlüsselung).

Eine so genannte Wurzel-(Root)-Zertifizierungsstelle autorisiert andere Institutionen oder Unternehmen (z. B. Finanzinstitute) dazu, ihrerseits als sekundäre Zertifizierungsstelle gegenüber Geschäftskunden aufzutreten. Die durch die Wurzel-(Root-) →Zertifizierungsstelle zertifizierten Unternehmen dürfen dann digitale Zertifikate an ihre Kunden ausgeben. →Trust Center (sekundäre Zertifizierungsstellen) erstellen und verwalten die elektronischen Schlüssel. Ein Zertifikat entsteht durch die technische Verknüpfung des öffentlichen Schlüssels eines asymmetrischen Schlüsselpaares mit den Identifizierungsdaten eines Benutzers, der im vordefinierten Rahmen einer Zertifizierungsrichtlinie registriert wurde. Siehe →Certificate Revocation List, →EV Certificate

Zertifizierungsstelle: vertrauenswürdige Stelle, die die Zuordnung von öffentlicher →Schlüssel zu Subjekten (Personen oder Firmen) bescheinigt. Mehr Details unter →CA

Zeus: sehr flexibles und erfolgreiches Tool zur Erstellung von Varianten von →Schadsoftware, hauptsächlich genutzt gegen →e-Banking. Gehört in die Klasse der →Trojaner und wird für Preise zwischen einigen Hundert bis einige Tausend $ angeboten. Enthält u.a. →Key-logging Features, kann aber als →Man-in-the-Browser auch konfiguriert werden um dynamisch mit →2-Faktor-Authentisierungen wie →SMS-TAN umzugehen und Geld zu überweisen. Der Baukasten enthält auch Komponenten zum Aufbau eines →Botnets, z.B. die →C&C Server. Eine moderne Implementierung (2015) wird Sphinx genannt. Konkurrenzprodukt ist →SpyEye

Zfone: (Achtung, nicht identisch mit zPhone) →Programm des →PGP-Entwicklers →Phil Zimmermann zum →Verschlüsseln von →VoIP-Verbindungen mittels →ZRTP und →SRTP Protokoll. Dabei findet der Schlüsselaustausch während des Aufbaus der Sprachverbindung statt. →Man-in-the-Middle Angriffe werden verhindert, wenn die Teilnehmer sich einen Security Code (→Fingerprint), der auf den Bildschirmen der Geräte gezeigt wird, vorlesen (→out-of-band). Das System ist kompatibel mit Programmen auf der Basis von SIP- and RTP-Technologie, z.B. X-Lite, Gizmo und Sjphone). Gilt auch 2014 als für die →NSA nicht entschlüsselbar. Siehe →PGPfone, →Skype

ZFS: →Dateisystem von Sun für die Verwendung im →Server und →Rechenzentrumsbetrieb. Dazu gehören z.B. die maximale Größe des System, →RAID-Integration, sowie integriertem →Integritätsschutz durch →Prüfsumme

ZigBee: Standard für drahtlose Kommunikation zum Aufbau von Netzen (→WPAN) mit dem Ziel einfacher und billiger als →Bluetooth zu sein. Dies könnte z.B. Grundlage von →HAN sein. Konkurrenz ist z.B. →Z-Wave

Zip: Dateiformat zur verlustfreien Kompri-

mierung von →Dateien, das auch eine symmetrische →Verschlüsselung erlaubt, die bei der Verwendung kurzer Schlüssel aber sehr leicht durch entsprechende „→Passwort-Recovery“ →Programme zu knacken ist

ZKPP: →Zero-knowledge password proof

ZMR: (zentrales Melderegister) in Ö eine →Datenbank aller Personen mit Wohnsitz in Ö

Zombie: in der EDV ein →PC (neuerdings auch →Smartphone oder →Tablet), der mittels →Schadsoftware, bzw. →RAT von einem Angreifer zu illegalen Zwecken genutzt wird. Eine große Zahl davon bilden ein →Botnet. Diese können für illegale Zwecke, z.B. →dDoS-Angriffe, aber auch die Verteilung von Pornographie, →Phishing, →Bitcoin-Mining oder →Spam genutzt werden. Es gibt viele Bot-Netze mit über 100 000 solcher Rechner. Seit ca. 2013 gelingt es Polizeibehörden, in Zusammenarbeit mit großen IT-Unternehmen wie z.B. →Microsoft und Firmen im Bereich IT-Sicherheit immer öfter, Botnets lahm zu legen. Diese Erfolge halten aber in der Regel nicht sehr lange an

Zone:

1) generell: Netzbereich mit einer bestimmten Sicherheitsanforderung, Beisp. →DMZ.
2) im Bereich Storage: mehrere →Fibre Channel →Ports, die miteinander kommunizieren dürfen

Zonealarm: Personal →Firewall, für Privatnutzung kostenlos

Zoning: im Bereich Storage: Unterteilung eines →Fabrics aus Sicherheitsgründen in Subnetzwerke, die sich auch überlappen können

Zoom: Anbieter eines →Webkonferenzsystems das 2020 durch intensive Nutzung von Online-Konferenzen zum Durchbruch kam. Im Gegensatz zu reinen →WebRTC-basierten Systemen wie →BigBlueButton oder →Jitsi vor allem mit dedizierter Client-Software genutzt, was manchmal die Benutzbarkeit für die Nutzer vereinfacht (eine Nutzung im →Webbrowser mit →WebRTC ist aber auch möglich). Hatte zu Begin von 2020 mit Sicherheitsproblemen zu kämpfen

Zoom-Bombing: Bei dem →Webkonferenzsystem →Zoom kam es Anfang →2020 zu einer Reihe von Sicherheitsproblemen (die bei unvorsichtiger Konfiguration bei jedem solchem System auftreten können. Durch eine ungeschickte Wahl der Sicherheitsvoreinstellungen für Zoom-Konferenzen war es per-Default für alle Teilnehmer möglich, ihren →Bildschirm frei zu geben. Dies wurde bei öffentlich publizierten Konferenz-→URLs zum Publizieren von unerwünschten Inhalten, z.B. Pornographie oder rechts-radikalen Inhalten genutzt. Da die grundsätzliche Möglichkeit des Teilens von Bildschirminhalten in allen diesen Systemen besteht ist diese Problematik in allen Konferenzsystemen inherent und muss durch bewusste Vergabe von Berechtigungen kontrolliert werden

ZRTP: von →Phil Zimmermann mitentwickeltes Protokoll für →VoIP, d.h. IP-basierte Telefonie. Schlüsseltausch mittels →Diffie-Hellman, verwendet im →Zfone (ebenfalls von Phil Zimmermann), →Signal und RedPhone (von Moxie Marlinspike). Gilt auch 2014 als für die →NSA nicht entschlüsselbar

Zuckerberg's Law: in 2008 von Mark Zuckerberg dargelegte Theorie, dass die Zahl der „Share“-Events auf →Facebook sich jedes Jahr verdoppelt. Der Medi Informationssicherheitan der →“friends“ liegt bei 100, für 2013 ergaben sich damit ca. 1500 Nachrichten pro Besuch eines Benutzers. Dieser Effekt wurde zu einem Problem für Facebook, das daher den →News Feed eingeführt hat, bei dem dieser Nachrichtenstrom nach von Facebook vorgegebenen →Algorithmen gefiltert wird (inkl. der „Werbenachrichten“ von den Firmen-Präsenzen auf FB, bei denen ein Benutzer „fan“ ist). Das bedeutet, dass nicht alle Nachrichten der „friends“ angezeigt werden, außer der Benutzer geht aktiv auf die Seite dieses Benutzers

Zufallszahlen: →random number

Zugang: →Access

Zugriff: →Access

Zugriffsberechtigung: Rechte, die ein Nutzer auf einem →System hat. Siehe →Autorisierung, →UAM

Zurechenbarkeit: der Empfänger kann eine Nachricht, inkl. Absender-→Authentisierung, als Beweis gegenüber Dritten verwenden. Ein Verfahren dafür ist die →digitale Signatur

Zutritt: räumliches Eindringen in einen (meist) privilegierten Bereich, siehe →Access

Zutrittssystem: elektronische Schutzeinrichtung zur Kontrolle des →Zutritts. Früher meist über Portier gelöst, heute oft mittels (meist kontaktloser) →Smartcard (→RFID). In Hochsicherheitsbereichen auch über →PIN-Eingabe oder →Biometrie

Z-Wave: drahtloses Übertragungsprotokoll für →HAN, d.h. home automation, Konkurrenz zu →ZigBee

Zweierkomplement: →Zahlendarstellung

Zwift: Größte Online-Plattform für virtuelles Training für Rad- und Laufsport. Radsportler brauchen entweder ein kompatibles Fahrradergometer oder einen →Smart Trainer in den das Rennrad (ohne Hinterrad) eingebaut wird. Dieses Gerät wird üblicherweise über → Bluetooth mit einem →Smartphone oder →PC verbunden, das oder der dann eine Verbindung zur →Plattform im →Internet herstellt. Virtuelle Landschaften können mittels →Bild-

schirmen dargestellt werden, z.B. die fiktive Insel →Watopia, mit Dinosauriern und Vulkanen, aber auch berühmten Rennstrecken. Bei (virtuellen) Steigungen kann der Tret-Widerstand automatisch von der Strecke auf das Gerät übertragen werden. Andere Teilnehmer werden als →Avatar dargestellt. Es werden auch Rennen ausgetragen, 2021 wird von Betrug mittels Manipulation der →Software berichtet. Zwift berichtet 2020 ca. 2 Mio. zahlende Nutzer (ca. 80 000 aus D.)