sicherheitskultur.at

Internet of Things

Quo Vadis?

Philipp Schaumann
IT-Security Erste Bank
philipp.schaumann@erstebank.at

Disclaimer:
- Alle hier präsentierten Positionen sind rein privater Natur
- Die technischen Details haben keinen Zusammenhang mit Angeboten oder Software meines Arbeitgebers

Computer überall
Pervasive Computing

Daran haben wir uns schon (fast) gewöhnt:

Smartphones, präsent in unserem Leben bis auf die Toilette und ins Bett.

Wearables und Self-Tracker, genutzt in jeder Lebenslage

Digitale Assistenten, Fernseher und Puppen die unsere Gespräche belauschen und analysieren

Na und?
Die tun ja niemandem was!

Die hören ja nur zu,
sammeln nur Daten über
mich und schicken diese
weiter

Und wenn die uns was tun könnten?

Geräte mit

- digitalen Prozessoren
- + Sensoren
- + Aktuatoren, d.h. Stellgliedern

sind keine Computer,
das sind Roboter.

Roboter, die aktiv in unser “richtiges Leben” eingreifen können

Einige (bedrohliche) Beispiele

Smart Homes steuern die Türschlösser, die Heizung, das Klimagerät, die Alarmanlage, das Licht, bald auch Herd, Kühlschrank, Waschmaschine, Verkehrsampeln, ……

Implantierte Medizingeräte steuern Herzschlag, Insulinpumpen und andere kritische Aspekte

Derzeitige (nicht-autonome) Autos kommunizieren bereits im Internet, verkünden ihren Standort, lassen sich abschalten, lassen sich ohne Schlüssel öffnen und starten, ……

Viele Geschäfts-Opportunities

- Überwachung der Nutzer und Verkauf der Daten
- “Steuerung” der Nutzer durch Handlungsvorschläge (Nudging)
- und vor allem Erpressung

Viele Erpressungs-Opportunities

- Spam- und Ransomware-Verteilung
- Das gute alte dDoS
- aber auch Blockierung von Schlössern und anderen Geräten
- Drohung der Störung der Produktion in Industrieunternehmen

  https://www.golem.de/news/ransomware-not-petya-angriff-kostet-maersk-200-millionen-us-dollar-1708-129525.html
  https://www.heise.de/newsticker/meldung/Krankenhaeuser-ruesten-sich-gegen-Cyber-Attacken-3758423.html

- . . . . .

Und das ist kein Science Fiction!

Avanti Diletanti !

Hersteller dieser Geräte sind zumeist gute Ingenieure, aber blutige Anfänger bei Fragen der IT-Sicherheit.

Die Techniker sind geschult in Elektrotechnik sie bringen die Geräte zum korrekten Funktionieren.

Sie übertragen die gesammelten Daten in einen Cloudspeicher, und verwenden den zum Empfang von Steuerkommandos vom Smartphone (des Besitzers und des Herstellers und ?)

Wenn Sie ihr Garagentor remote bedienen können, so können das andere auch

derStandard.at › Web › Netzpolitik

International Inland Wirtschaft Web Sport Panorama Etat Kultur Wissenschaft Gesundheit Bildung
Innovationen IT-Business Telekom Netzpolitik Games Webmix

Nach Kritik auf Amazon: Smartes Garagentor sperrt Besitzer aus

6. April 2017, 10:25 — 689 POSTINGS

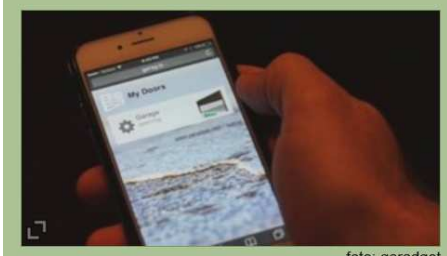


foto: garadget
Mit Garadget können Garagentore vernetzt werden.

Hersteller kappt Verbindung für Nutzer, der negative Rezension schrieb – Einlenken nach Shitstorm

"Verschwendet nicht euer Geld dafür": Mit diesen drastischen Worten warnte ein unzufriedener Nutzer auf Amazon vor dem smarten Garagentoröffner Garadget, dessen iPhone-App laut Nutzer "Müll" sei und dauernd abstürze. Dem Hersteller schmeckte diese Kritik gar nicht. Garadget-Chef Denis Grisak teilte dem User im Support-Forum mit, dass sich dessen Gerät "künftig nicht mehr mit dem Server verbinden kann". Er ließe sich die "beleidigende Wortwahl" nicht gefallen. Der Kunde konnte daraufhin sein Garagentor nicht mehr via App öffnen.

http://derstandard.at/permanent/2000055482466/Nach-Kritik-auf-Amazon-Smartes-Garagentor-sperrt-Besitzer-aus

IT-Sicherheitsprobleme sollten längst Vergangenheit sein

Vor 5 Jahrzenten

Programmiersprachen hatten bereits

- Strong typing
- Automatische Diagnose von vielen Programmierfehlern
- Buffer overflow prevention

IT-Sicherheitsprobleme sollten längst Vergangenheit sein

Vor 3 Jahrzenten

Public Key Encryption als Lösung aller Sicherheitsprobleme

Trennung von Code und Daten auf Hardware-Ebene

IT-Sicherheitsprobleme sollten längst Vergangenheit sein

Vor 2 Jahrzenten

Threat assessment Methodologien können die Sicherheit von IT-Systemen nachweislich deutlich erhöhen

Avanti Diletanti !

Aber die Hersteller wissen nicht,

- Wie man eine verschlüsselte Verbindung absichert
- Wie man Man-in-the-Middle verhindert
- Wie man Passworte sicher ablegt
- wie man sichere Software-Updates implementieren könnte
- Wie man mittels Signaturen überprüfen könnte, ob die Software auch nicht verändert wurde
- Wie man eine Certificate Chain verifizieren könnte

Viele Geschäfts-Opportunities

- Überwachung der Nutzer und Verkauf der Daten
- “Steuerung” der Nutzer durch Handlungsvorschläge (Nudging)
- und vor allem Erpressung

Viele Erpressungs-Opportunities

- Spam- und Ransomware-Verteilung
- Das gute alte dDoS
- aber auch Blockierung von Schlössern und anderen Geräten
- Drohung der Störung der Produktion in Industrieunternehmen

  https://www.golem.de/news/ransomware-not-petya-angriff-kostet-maersk-200-millionen-us-dollar-1708-129525.html
  https://www.heise.de/newsticker/meldung/Krankenhaeuser-ruesten-sich-gegen-Cyber-Attacken-3758423.html

- . . . . .

Was sind die Anreize für den Hersteller?

Hauptanreiz für den Hersteller ist ein Gerät, das schnellstmöglich auf dem Markt ist, das keine Konfiguration durch den Benutzer benötigt und das billig herzustellen ist.

Jeder Security-Test verteuert das Gerät und verzögert die Markteinführung

Und die Unsicherheit tut ihm typischerweise nicht mal weh, die Schäden tragen andere

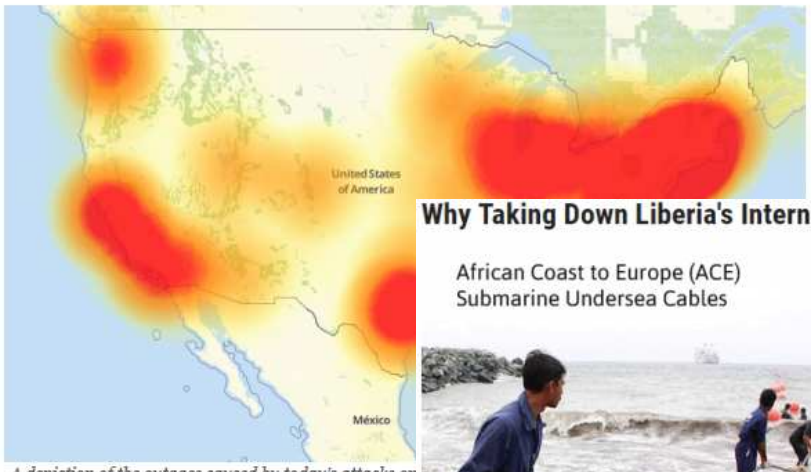
Was sind die Anreize für den Kunden?

Die Kunden kaufen ein Gerät und erwarten, dass sie es einstecken und geht schon
Sie wollen (mit Recht) kein Installation Manual lesen müssen

Sie wollen nicht selbst dran denken müssen, Default Passworte zu ändern

Manchmal treffen potentielle Schäden ihn selbst, oft treffen sie aber ganz andere –
Stichwort Mirai Botnet

Videokameras, Homerouter, etc. bilden das Mirai Botnetz



A depiction of the outages caused by today's attacks on
Downdetec

Und immer wenn man denkt: Schlimmer kann es nicht kommen

Mit den autonomen, vernetzten Fahrzeugen haben wir jetzt “Geräte”, die mit hoher Geschwindigkeit auf unseren Straßen unterwegs sind

Und die haben mindestens so viele Schwach-stellen und Angriffsflächen wie andere “Geräte”.

Wie wäre den ein Botnet, das die Kontrolle über alle Fahrzeuge eines Typs hat?

Alle Autos MÜSSEN “im Internet” sein (z.B. eCall) - Dazu kommt V2V und V2I

Auch Ampeln werden intelligent und sollen auf Kommandos von außen reagieren können
https://www.heise.de/tr/artikel/Ampel-App-hilft-Fussgaengern-3786287.html

Der Markt kann das nicht richten!

Der Markt hat 2 Hauptstellschrauben:

Haftung durch die Hersteller

Kundenentscheidung

Falsche Belohnungen (1)

Hersteller werden durch den Markt “bestraft”

- time-to-market steht über “sicher”
- “features” steht über “sicher”
- “bequem” oder “cool” steht über “sicher”

Falsche Belohnungen (2)

Hersteller haben kaum ein Risiko dabei weil

- Typischerweise keine Haftung für “Bugs” oder Unsicherheiten
- Benutzer können “Sicherheit” sowieso nicht beurteilen

Der Markt kann das nicht richten!

Der Hersteller haftet nur in Ausnahmefällen für etwaige Schäden durch unsichere Software

Der Kunde könnte von der Unsicherheit betroffen sein (gestohlenes Auto, abgeschaltete Alarmanlage, ferngesteuertes Auto, tödliche Insulinpumpe), aber wer denkt als Käufer schon an so was –

und außerdem kann er die Sicherheit eh nicht beurteilen

Was der Markt nicht richten kann, das muss reguliert werden, aber . . .

Wir haben es mit einem globalen Markt zu tun.

Chinesische Hersteller verkaufen unsichere Geräte an Kunden in Österreich, die Geräte kommen in ein Botnet und greifen Systeme in der ganzen Welt an.

Wie kann so ein Problem gelöst werden?

Warum kann Software nicht wie Schlagbohrer sein?

Schlagbohrer

Wir haben die Anforderung des VDE-Tests bzgl. elektrischer Sicherheit (Pflicht in so vielen Ländern, dass sich der Test rechnet) - 100,000 Produkt Tests pro Jahr für 5,000 Hersteller weltweit

Getestet gegen einen einheitlichen safety standard
Der VDE-Sticker informiert die Kunden (transparent market)

Anspruch auf Ersatz wenn das Gerät nicht funktioniert wie beschrieben

Haftung für Schäden durch Fehler der Maschine

Was könnte so ein Zertifikat für IoT-Geräte bringen?

Verbraucher hätten eine Orientierung, wüssten ob der Hersteller einen externen Sicherheitstest hat machen lassen.
Lokale Behörden (z.B.Verbraucherschutz) könnten diesen Test so verpflichtend machen wie die VDE-Prüfung.
Auch wenn nur die USA und die EU diesen Test verlangen, so könnten ihn die Hersteller nicht ignorieren

Siehe auch ENISA:
https://www.enisa.europa.eu/news/enisa-news/enisa-works-together-with-european-semiconductor-industry-on-key-cybersecurity-areas

Haben wir den schon Kriterien für den Test?

Ja, reichlich:

"Internet of Things (IoT) Broadband Internet Technical Advisory Group, Nov 2016.
"IoT Security Guidance," Open Web Application Security Project (OWASP), May 2016.
"Strategic Principles for Securing the Internet of Things (IoT)," US Department of Homeland Security, Nov 2016.
"Security," OneM2M Technical Specification, Aug 2016.
"Security Solutions," OneM2M Technical Specification, Aug 2016.
"IoT Security Guidelines Overview Document," GSM Alliance, Feb 2016.
"IoT Security Guidelines For Service Ecosystems," GSM Alliance, Feb 2016.
"IoT Security Guidelines for Endpoint Ecosystems," GSM Alliance, Feb 2016.
"IoT Security Guidelines for Network Operators," GSM Alliance, Feb 2016.
"Establishing Principles for Internet of Things Security," IoT Security Foundation, undated.
"IoT Design Manifesto," www.iotmanifesto.com, May 2015.
"NYC Guidelines for the Internet of Things," City of New York, undated.
"IoT Security Compliance Framework," IoT Security Foundation, 2016.
"Principles, Practices and a Prescription for Responsible IoT and Embedded Systems Development," IoTIAP, Nov 2016.
"IoT Trust Framework," Online Trust Alliance, Jan 2017.
"Five Star Automotive Cyber Safety Framework," I am the Cavalry, Feb 2015.
"Hippocratic Oath for Connected Medical Devices," I am the Cavalry, Jan 2016.
"Industrial Internet of Things Volume G4: Security Framework," Industrial Internet Consortium, 2016.
"Future-proofing the Connected World: 13 Steps to Developing Secure IoT Products," Cloud Security Alliance, 2016.
https://www.schneier.com/blog/archives/2017/02/security_and_pr.html

Danke

Philipp Schaumann

philipp.schaumann@erstebank.at