sicherheitskultur.at

Internet of Things

Quo Vadis?

Philipp Schaumann

philippschaumann@mailbox.org

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

Pervasive Computing

Daran haben wir uns schon (fast) gewöhnt:

Smartphones, present in unserem Leben bis auf die Toilette und ins Bett
Wearables und Self-Tracker, genutzt in jeder Lebenslage
Digitale Assistenten, Fernsehen und Puppen die unsere Gespräche belauschen und analysieren

Na und?

Die tun ja niemandem was!

Die hören ja nur zu, sammeln Daten und schicken sie 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, ……
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, ……

Avanti Diletanti !

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
zum Übertragen der gesammelten Daten in einen Cloudspeicher,
zum Empfang von Steuerkommandos vom Smartphone (des Besitzers und des Herstellers ?)

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

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

Avanti Diletanti !

Aber sie 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

Was sind die Anreize für den Hersteller?

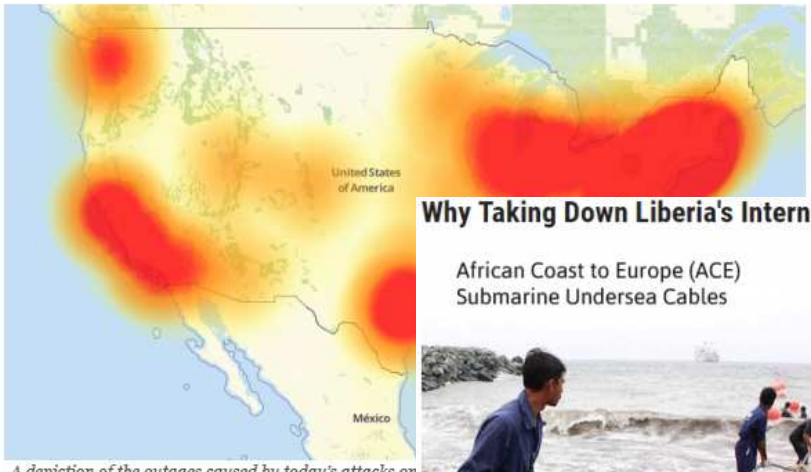
Hauptanreiz für den Hersteller ist ein Gerät, das schnellstmöglich auf dem Markt ist, das keine Konfiguration durch den Benutzer benötigt und das billig herzustellen ist
Jeder Security-Test verteuert das Gerät und verzögert die Markteinführung
Und die Unsicherheit tut ihm typischerweise nicht mal weh, 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 Dyndetect

Das waren wohl bisher nur Fingerübungen

Der Markt kann das nicht richten!

Der Markt hat 2 Hauptstellschrauben:

Haftung

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 eine Regierung regulieren, 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

Haben die Anforderung von VDE-Tests bzgl. elektrischer Sicherheit (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 die Hersteller nicht ignorieren

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

philippschaumann@mailbox.org