sicherheitskultur.at

Der traurige Zustand der Informationssicherheit

Philipp Schaumann

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

Agenda

Der Zustand der Informations-Sicherheit

Was könnte getan werden?

Was sollte getan werden?

Der Zustand

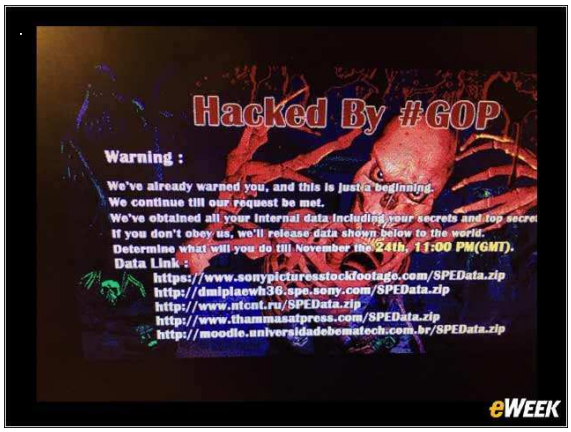
Das ganze scheint eine unendliche Geschichte zu sein ☹

Jede Menge Ärger und kein Licht am Ende des Tunnels

2014 – Das Jahr der Mega-Verwundbarkeiten und Leaks

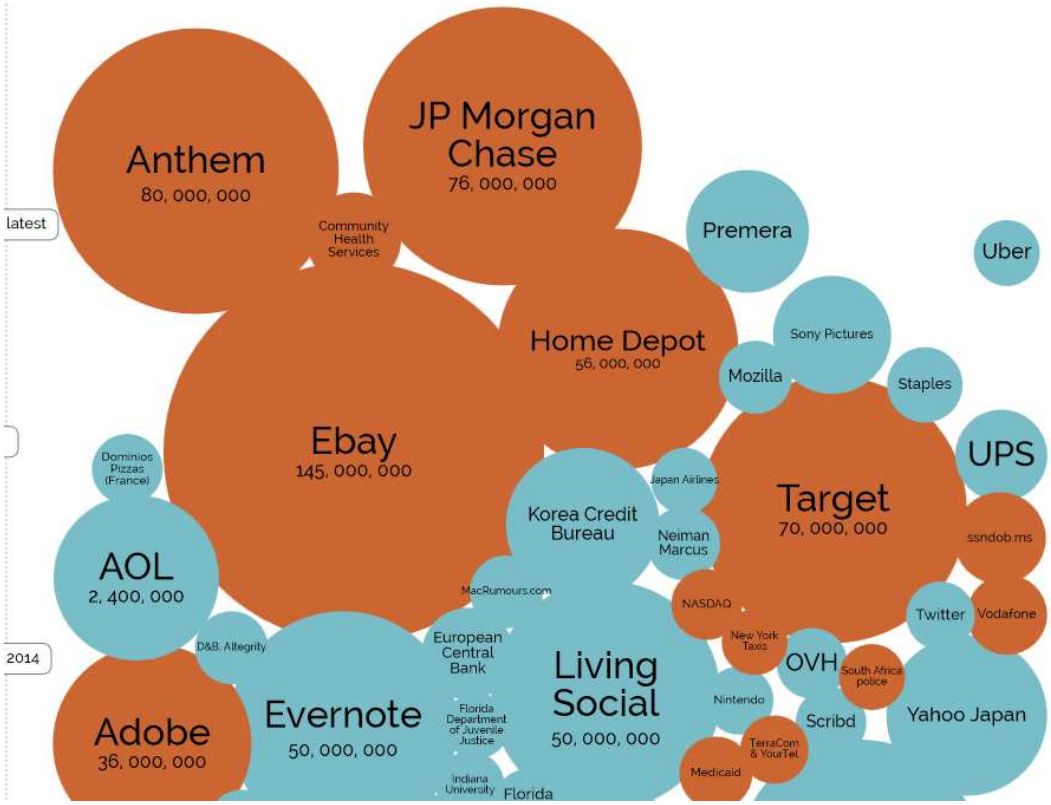
Poodle
(man-in-the-middle downgrade exploit)

Heartbleed
(SSL-Vulnerability)



Sony

2015, 2014 Data Leaks



http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Wir wissen heute, wie man sichere Systeme implementiert, aber . . .

Passworte auf Firmen-Websites sind oft

- In Klartext gespeichert oder
- als broken-Hash (MD-5) oder ohne Salz

Viele Websites ermöglichen SQL-Injection

Report from CENZIC (2013)

99% der Websites hat Sicherheitsprobleme
16% erlauben SQL-injection
80% haben Probleme beim Session-Handling
61% erlauben XSS
13% haben Authentication Probleme

Vertrauliche Daten werden über HTTP gesendet

Smartphone Apps mit HTTPS erlauben trotzdem Man-in-the-middle Angriffe (40%)

Wir predigen den IT-Departments, aber . . .

Webservers nutzen veraltete Software Versionen

- Word-press
- vBulletin
- Php
- . . . . (und alles andere)

Reports Frühling 2013
420 000 Geräte (home routers) können via telnet als {admin/admin, root/root, admin/ , or root/ } übernommen werden
21.7 Mio open DNS resolvers stehen für DNS amplification attacks zur Verfügung

Web Entwickler fehlen oft die Grundlagen sicherer Web-programme

Das Internet scheint nicht verteidigbar

Resilence

Ein System ist dann widerstandsfähig, wenn es Diversität und Redundanzen gibt.

Jede Art von Zentralisierung macht verwundbar.

Myriam Dunn Cavelty – ETH Zürich

Der Trend zu Monopolen (1)

- Statt wie in den 60igern und 70igern 8 – 10 große System-Anbieter haben wir heute
  - Microsoft
  - Apple
  - Google
  - Linux (Stichwort →Heartbleed)
- 2 Smartphone-Anbieter
- Gemalto für 50% aller SIM-Karten

Der Trend zu Monopolen (2)

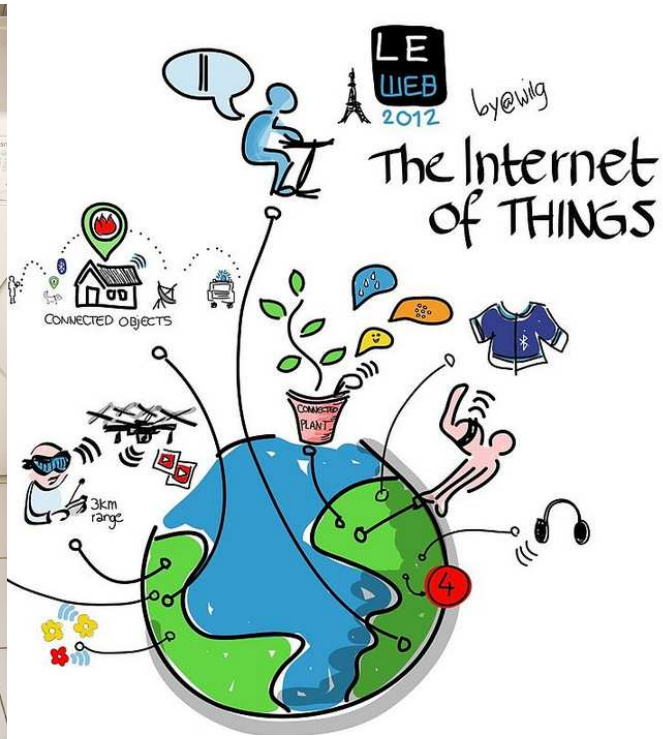
- 5 – 6 große (US-)Cloud Infrastrukturen
- Facebook + 5 andere Social Networks
- Amazon, Alibaba, eBay teilen sich den Handel
- Google dominiert die Suchmaschinen

The Internet: Unsafe by Design

- Ursprünglich entwickelt als „quick-and-dirty“ Hack, Hauptsache es funktioniert – Basis ist „jeder traut jedem“
- Versuche, Sicherheit (z.B. Verschlüsselung) einzufügen scheiterten entweder an dann teurer Hardware oder den Einsprüchen der Geheimdienste
- Protokolle wie BGP (Border Gateway Protocol) ist vollkommen auf Trust-Basis. Jeder ISP kann kurzfristig beliebigen Verkehr „zu sich umleiten“

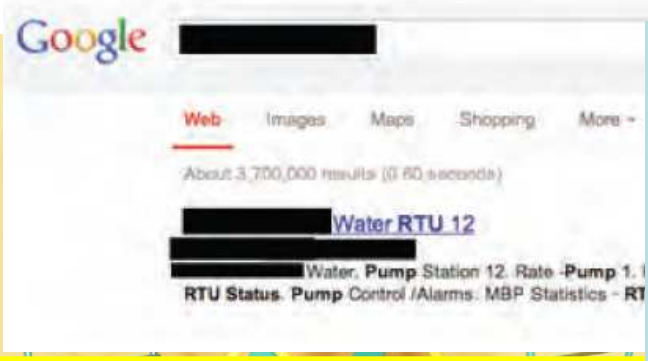
Ausführliche Geschichte der Unsicherheiten des Internets:
http://www.washingtonpost.com/sf/business/2015/05/30/net-of-insecurity-part-1/
http://www.washingtonpost.com/sf/business/2015/05/31/net-of-insecurity-part-2/
http://www.washingtonpost.com/sf/business/2015/06/22/net-of-insecurity-part-3/

Erst waren nur die Computer verwundbar, aber jetzt . . .



Erst waren nur die Computer verwundbar, aber jetzt . . .

Verwundbar-keiten in ICS und SCADA Systemen gefährden Strom- und Wasser-versorgung



Verwundbare SCADA Systeme werden über Google oder Nessus oder Scanner wie MODBUS gefunden

Heute sind verwundbar:

- Web-Cams
- Herz-Schritt-macher
- Insulin-pumpen
- Autos
- . . . .

End-Users Awareness ist die Lösung, aber . . .

Die Mehrheit nutzt einfache **Passworte**,

Dasselbe Passwort auf allen Websites

End-users machen keine **Backups**

End-users halten die **Software nicht aktuell**

Veraltete Software, es wird nicht besser . . .

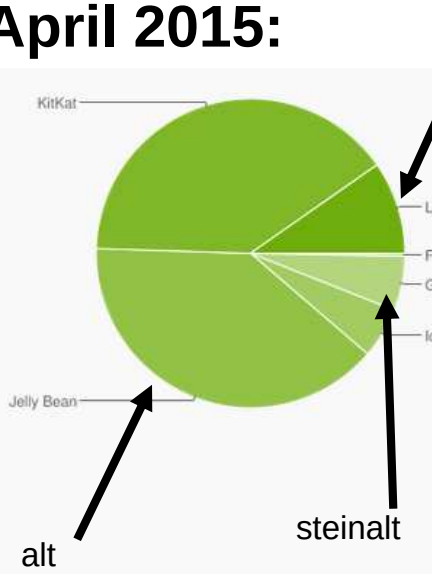
Nearly half of all Android devices are still vulnerable to two serious browser exploits

Lucian Constantin Oct 8, 2014 8:48 AM

Android Versionen April 2015:

Version	Codename	API	Distribution
2.2	Froyo	8	0.3%
2.3.3 - 2.3.7	Gingerbread	10	5.7%
4.0.3 - 4.0.4	Ice Cream Sandwich	15	5.3%
4.1.x	Jelly Bean	16	15.6%
4.2.x		17	18.1%
4.3		18	5.5%
4.4	KitKat	19	39.8%
5.0	Lollipop	21	9.0%
5.1		22	0.7%

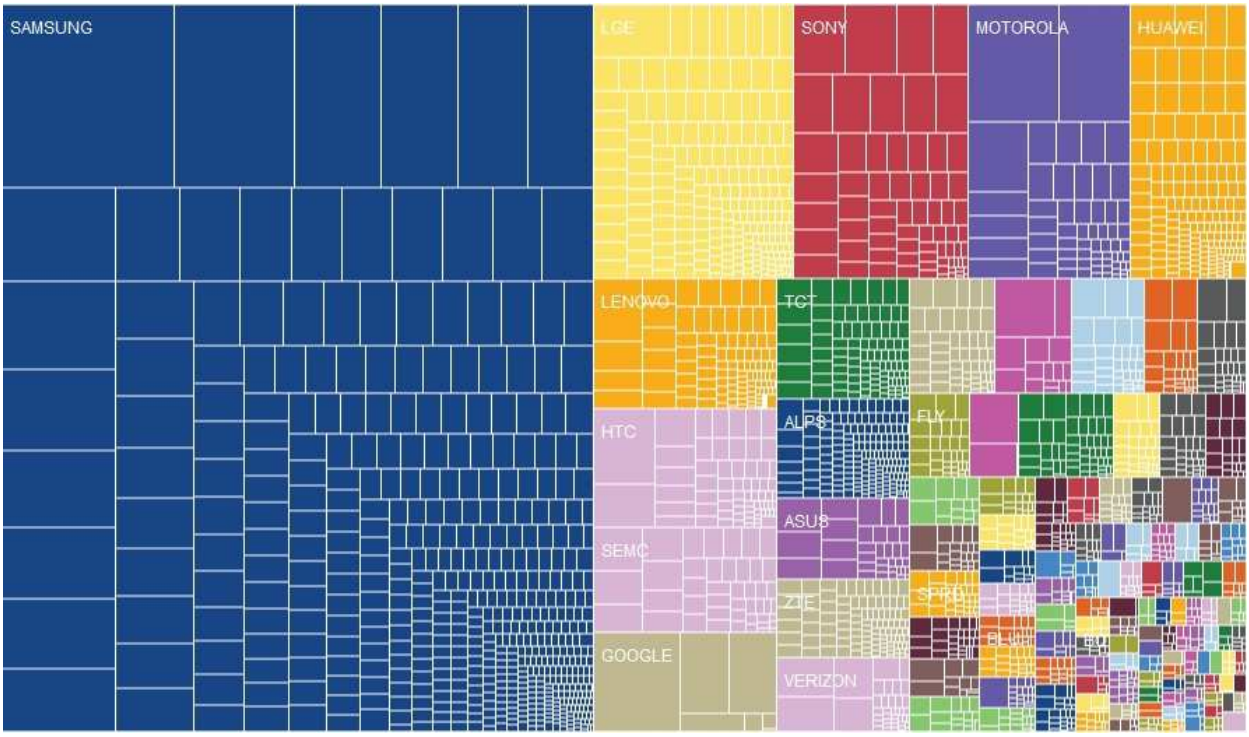
Data collected during a 7-day period ending on May 4, 2015.
Any versions with less than 0.1% distribution are not shown.



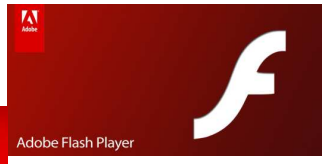
End-users halten die **Software nicht aktuell**

https://developer.android.com/about/dashboards/index.html

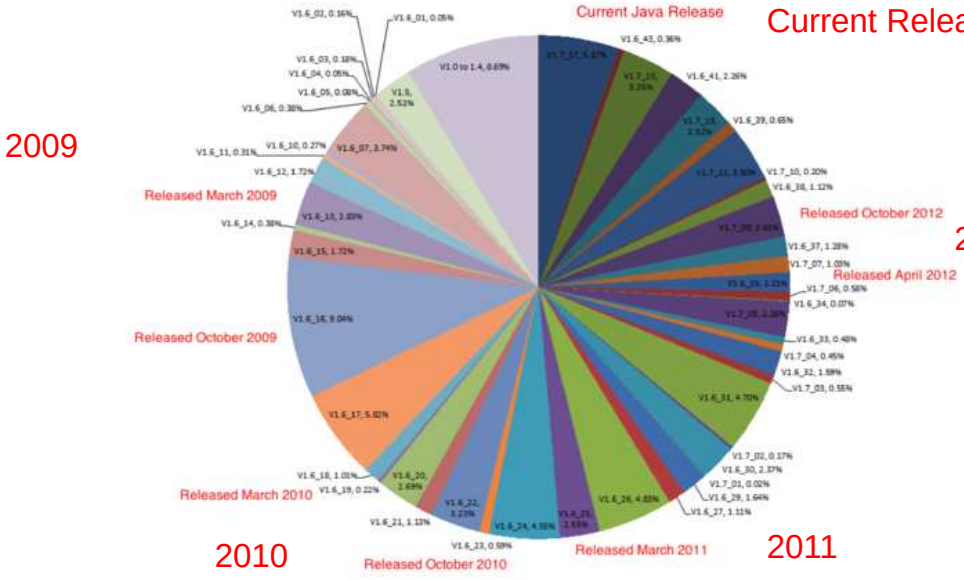
19 000 Android Varianten in 2014
Viel Spaß beim Patch Management



Veraltete Software, es wird nicht besser . . .



Java:



End-users halten die **Software nicht aktuell**

93% sind verwundbar durch Java Exploits

Es wird nicht besser:
3 Billion Devices Run Java

Smartphones
Stärken und Schwächen

Stärken

- Sandboxes zur Isolierung von benutzer-installierten Prozessen – wichtigste Sicherheitsfeature
  Dadurch deutlich höhere Sicherheit verglichen mit MS Windows und MacOS

- Trend zu hardware-basierter Speicherverschlüsselung

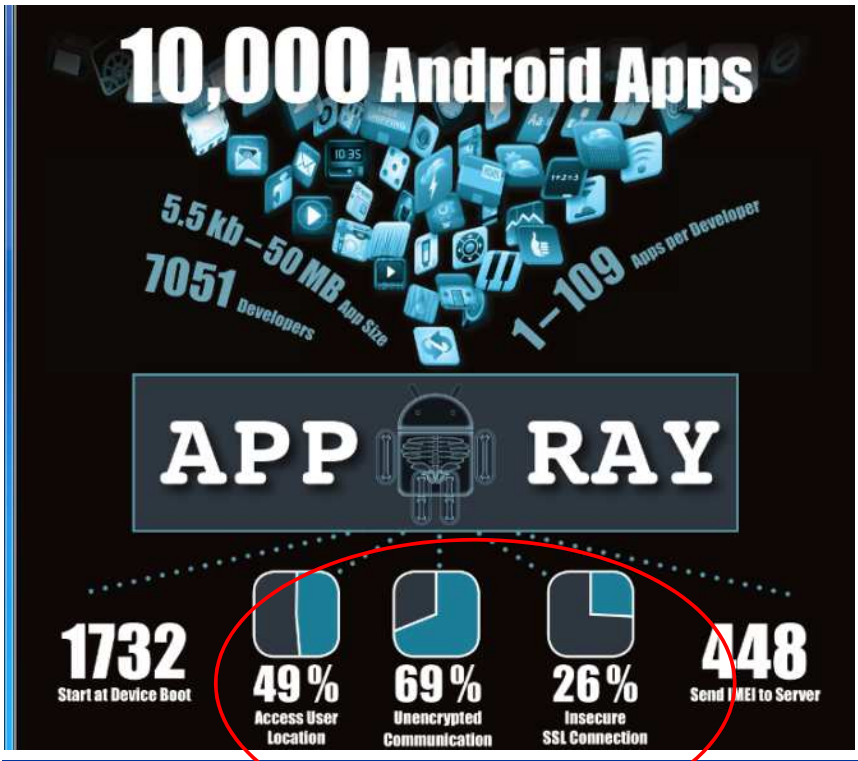
Behauptung:
Smartphones, von der Technologie her, sind sicherer als die meisten heutigen Computer

Fraunhofer März 2011:
http://www.dfn.de/fileadmin/3Beratung/Betriebstagungen/bt54/forum-mobileit-heider.pdf

Sicher - wären da nicht Cloud und der menschliche Spieltrieb

- Smartphones werden IMMER in Verbindung mit der Cloud genutzt
- Die Zahl der wirklich sicheren Cloud-Lösungen liegt sehr nahe bei Null
- „User Experience“ schlägt Sicherheitsbedürfniss jederzeit

App-Entwickler wissen nicht, wie man eine sichere Kommunikation programmiert



Apple iOS:

22% nicht verschlüsselt

14% mit SSL, aber falsch

http://www.heise.de/newsticker/meldung/SSL-Verschluesselung-auch-in-iOS-Apps-problematisch-2138829.html

Smartphones - Privat oder Business?

Seit wann sind die Privatgeräte der Mitarbeiter und Kunden ein Thema für uns in der Firmen-IT?

- **Kunde**
  den M
  der U-
- **Mitarb**
  Firmer
  Mitarb
  könner

Kontrollverlust bei der Firmen-IT

Kübler-Ross Modell - Five Stages of Grief

http://en.wikipedia.org/wiki/K%C3%BCbler-Ross_model

Acceptance:
„Bring Your Own Device“ B.Y.O.

September 22, 2011 The New York Times

More Offices Let Workers Choose Their Own Devices

By VERNE G. KOPYTOFF

SAN FRANCISCO — Throughout the information age, the corporate I.T. department has stood at the chokepoint of office technology with a firm hand on what equipment and software employees use in the workplace.

They are now in retreat. Employees are bringing in the technology they use at home and demanding the I.T. department accommodate them. The I.T. department often complies.

Some companies have even surrendered to what is being called the consumerization of I.T. At Kraft Foods, the I.T. department's involvement in choosing technology for employees is limited to handing out a stipend. Employees use the money to buy whatever laptop they want from Best Buy, Amazon.com or the local Apple store.

I.T. Departments Lose Their Clout Over Phone Choices

By VERNE G. KOPYTOFF

http://bits.blogs.nytimes.com/2011/09/22/i-t-departments-lose-their-clout-over-phone-choices/
http://www.nytimes.com/2011/09/23/technology/workers-own-cellphones-and-ipads-find-a-role-at-the-office.html

Acceptance:
„Bring Your Own Device“ B.Y.O.

CISCO PRESS RELEASE

SAN JOSE, Calif. – Jan. 24, 2012

Global IT Survey Highlights Enthusiasm over Tablets in the Enterprise, Shows Customization, Collaboration and Virtualization as Key Features

Zitat:
Globally, 48% said their company would never authorize employees to bring their own devices (BYOD), yet 57% agreed that some employees use personal devices without consent.

http://newsroom.cisco.com/press-release-content?type=webcontent&articleId=658006

Die Probleme sollten längst gelöst sein

Vor 5 Jahrzenten

Programmiersprachen hatten bereits

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

Die Probleme sollten längst gelöst sein

Vor 3 Jahrzenten

Public Key Encryption als Lösung aller Sicherheitsprobleme

Trennung von Code und Daten auf Hardware-Ebene

Die Probleme sollten längst gelöst sein

Vor 2 Jahrzenten

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

Staaten schaffen einen „Hacker-Markt“

Die Geheimdienste vieler Staaten (nicht nur die NSA) haben einen riesigen und extrem lukrativen und (fast) legalen Markt für Verwundbarkeiten / Zero Days und Botnets geschaffen

Es gibt immer eine Lösung, die ist einfach, leuchtet allen ein und führt leider zu gar nichts . . .

Wir müssen einfach nur das Sicherheitsbewusstsein erhöhen!

Awareness Training für End-user, Entwickler, Manager, CEOs, …..

Die Schäden für Breaches sind (evt.) billiger als gute Sicherheit

- **Target:** 40 Mio Kreditkarten, 70 Mio Kundendaten
  $225 Mio Schaden - minus $162 Mio Versicherung – minus tax deductions = $105 Mio = 0.1% of sales

- **Sony Pictures:** $35 Mio for investigation and remediation – for a movie that cost $44 Mio to make and that made $46 Mio in sales over Xmas

- **Home Depot:** 56 Mio Kreditkarten + 53 Mio Email Adressen
  Netto Schaden nach Versicherung: $28 Mio = 0.01% of sales

http://www.techrepublic.com/article/data-breaches-may-cost-less-than-the-security-to-prevent-them/

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

- Keine Haftung für “Bugs”
- Benutzer können “Sicherheit” sowieso nicht beurteilen

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) - 1
  Hersteller w
- Getestet ge
- Der VDE-St
- Anspruch au
  beschrieben
- Haftung für

Zumindest brauchen wir so was wie die Pflicht zu Sicherheitsgurten in Autos!

Aber statt minimaler Sicherheit bekommen wir

- Mehr und mehr Überwachung und Daten-Sammelwut
- Viele Angebote über tolle Sicherheitsprodukte zur Minderung von Problemen, die fehlerhafte Software uns bringt

Und wie wäre so etwas für die IT?

In diesem Sinne

Diese App enthält:

- Ungesicherte Passwort-Übertragungen
- Unerlaubte Weitergabe Ihrer Kontakte und Ihrer Ortsposition

Und jetzt zur Diskussion