Kontrollverluste durch Informationstechnik

Marit Hansen

Sommerakademie 2010

Codex digitalis

Optimierter Persönlichkeitsschutz – digital und vernetzt

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Überblick

- Datenschutz und Kontrolle
- Ist Informationstechnik kontrollierbar?
- Lösungsansätze
- Auswirkungen von Kontrollverlust
- Fazit

Datenschutz basiert auf Kontrolle

Rechtlich gefordert:

- Kontrollmöglichkeiten für **Betroffene:**
  zur Umsetzung des Rechts auf informationelle Selbstbestimmung
- Kontrollmöglichkeiten für **Daten verarbeitende Stellen:**
  über ihre Verarbeitung personenbezogener Daten
- Kontrollmöglichkeiten für **Aufsichtsbehörden**

⇒ Insbesondere: **Kontrolle über Informationstechnik (IT)**

Informationstechnik ist kontrollierbar

- Basis von Informationstechnik
  - Mathematik (und Physik)
  - Wissenschaftliche Grundlagen gut verstanden

nicht was Du willst

- Ein Computerprogramm tut, was Du schreibst.
- Beispiel für eine einfache Berechnung:

```
z:=0;
n:=10;
for i=1 to n do
  z:=z+i
endfor;
```

Lesbarer Programm-Code

- Code kann **durchaus lesbar und nachvollziehbar** sein
- Beispiel aus dem Datenschutz-Projekt PrimeLife mit pseudonymen Autorisierungen (Identity Mixer):

PrimeLife

```
ProvenStatements{
  Credentials{
    randName1:http://www.ch.ch/passport/v2010/chPassport10.xml =
      [FirstName:id1, LastName:id2, CivilStatus:id4];
    randName2:http://www.ibm.com/employee/employeeCert.xml =
      [LastName:id2, Position:id5, Band:5, YearsOfEmployment:id3];
    randName3:http://www.ch.ch/health/v2010/healthCert10.xml =
      [FirstName:id1, LastName:id2, Diet:id6] }
  Enums{
    randName1:CivilStatus = or[Marriage, Widowed]
    randName3:Diet = or[Diabetes, Lactose-Intolerance] }
  Pseudonyms{ randNymName; http://www.ibm.com/employee/ }
  VerifiableEncryptions{ PublicKey1 = [Label,u1] }
  Message { randMsgName = "Term 1:We will not use this data for ..." }
}
```


Informationstechnik ist mehr als reine Mathematik

- Hardware
- Betriebssysteme
- Anwendungs-Software

- ... und das alles vernetzt

Foto: foskarulla

CC BY SA

Foto: ZakVTA

cc BY NC SA

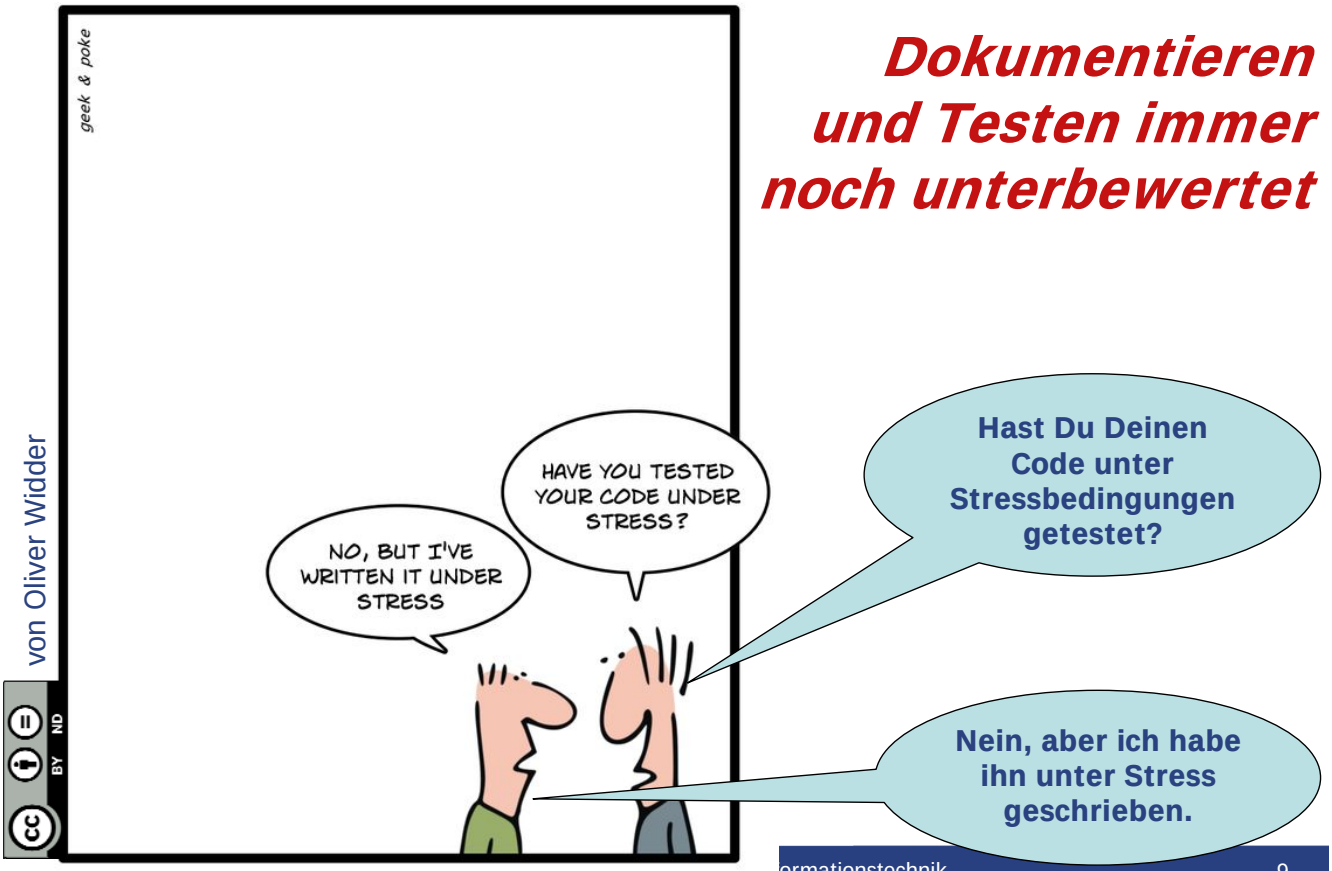
Einsatz von IT zum Design von IT

- Programmierung
- mit Programmier-Werkzeugen
- ... die programmiert wurden
- ... mit Programmier-Werkzeugen
- ... die programmiert wurden
- ... mit Programmier-Werkzeugen
- ... die programmiert wurden
- ...

- ... mit vielen unterschiedlichen Beteiligten über einen längeren Zeitraum

Die schlechte Nachricht: Fehler überall

Dokumentieren und Testen immer noch unterbewertet



Beweisbar korrekte Software

Diskutiert seit Anbeginn der Informatik
(also schon vor dem Zeitalter der PCs)

Trend: IT-Design als Handwerkskunst?

Beispiel von 1976

SOME CLASSES OF NATURALLY PROVABLE PROGRAMS

S. K. Basu and J. Misra
Department of Computer Sciences
University of Texas at Austin
Austin, Texas 78712

Example 9. Consider the following program,

```
z ← 0;
for i ← 1 to n do
X ← X + 1;
z ← z + X
endfor;
```

We would like to prove at output $z = n X_o + \frac{n(n+1)}{2}$.

Applying theorem 4, we would obtain

$$(z=n X_o + \frac{n(n+1)}{2}) \{X \leftarrow X+1; z \leftarrow z+X\} (z=(n+1)X_o + \frac{(n+1)(n+2)}{2})$$

But this cannot be proved since no relation between X_o and X is known. [...]

ULD www.datenschutzzentrum.de

Wir haben uns daran gewöhnt

„Bananen-Software“

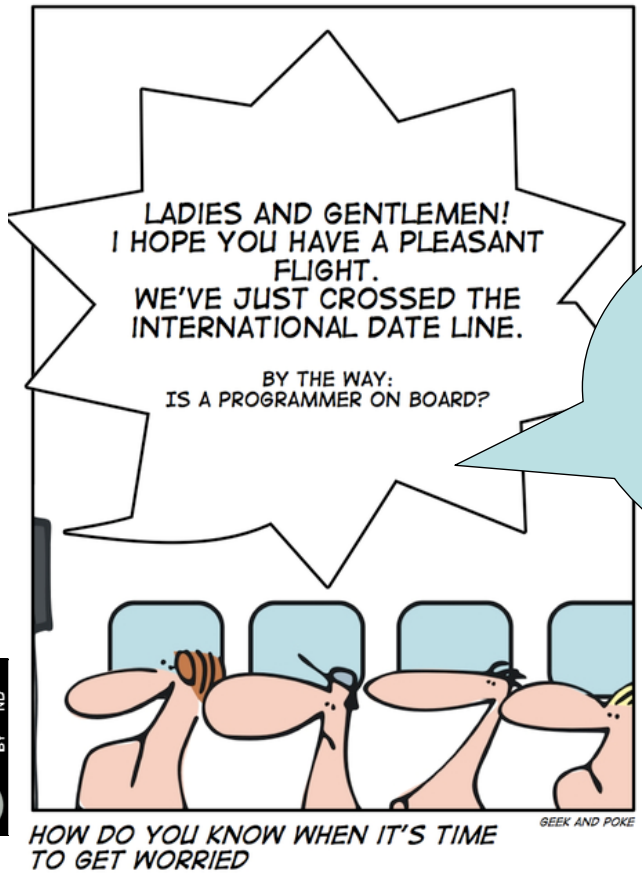
Die unreife Software reift beim Kunden.

Aus Sicherheitssicht ist ein **ständiges „Nachreifen“** sogar Pflicht!

Foto: Shi Yali

Der „heilige Gral mathematisch beweisbarer Software“: immer noch unerreichbar

Informations-technik in Autos



von Oliver Widder

**Meine Damen und Herren!
Ich hoffe, Sie haben einen angenehmen Flug.
Wir haben gerade die Datumsgrenze passiert.**

**Übrigens:
Ist ein Programmierer an Bord?**

Informationstechnik in Flugzeugen

ULD www.datenschutzzentrum.de

Trojaner mitverantwortlich für Spanair-Absturz?

El ordenador de Spanair que anotaba los fallos en los aviones tenía virus - ELPAÍS.com - Mozilla Firefox

Trojanerattacke: Flugzeugabsturz möglicherweise von Computerschädling mitverursacht

EL PAÍS

21.08.2010 Drucken | Senden | Feedback | Merken

Trojanerattacke

Flugzeugabsturz möglicherweise von Computerschädling mitverursacht

DPA

Wrackteil der abgestürzten MD-82: Ist ein Computerschädling mitschuld am Absturz?

Eine Schadsoftware könnte mitverantwortlich an einem der schlimmsten Flugzeugabstürze in Spanien sein. Aufgrund eines Befalls mit Trojanersoftware soll ein Überwachungsrechner nicht rechtzeitig Alarm geschlagen haben. Ein Richter hat nun eine genaue Auswertung entsprechender Daten angeordnet.

Pérez, que pida a Spanair todas las anotaciones

Funksignal an Herzschrittmacher - Hack ins Herz - Digital - sueddeutsche.de - Mozilla Firefox

sueddeutsche.de

Home > Digital | Wikileaks | Software | Soziale Netzwerke | Cebit | iPad | IFA | Ressortarchiv

13.03.2008, 17:30

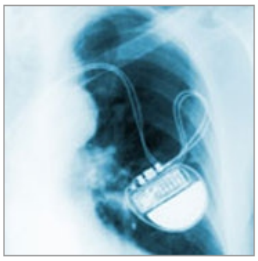
Funksignal an Herzschrittmacher

Hack ins Herz

Von Helmut Martin-Jung

Mit dem Computer hackten US-Forscher Herzschrittmacher. Es gelang ihnen sogar, die Geräte anzuweisen, Elektroschocks abzugeben. Droht hier Gefahr für Patienten?

Der Redner bricht mitten im Satz ab, zuckt wie von einem Schlag auf die Brust getroffen zusammen und fällt schließlich bewusstlos zu Boden, während hinten im Saal eine unauffällig gekleidete Person den Deckel ihres Laptops schließt und im allgemeinen Tumult unbemerkt durch eine Tür nach draußen schlüpft.



Ein Herzschrittmacher könnte per Funk angreifbar sein und Elektroschocks aussenden. (© Foto: iStock)

Selbst in besonders sensiblen Bereichen

Selbst in besonders abgesicherten Bereichen

Virus Infects Space Station Laptops (Again) | Threat Level from Wired.com - Mozilla Firefox

Virus Infects Space Station Laptops (Again)

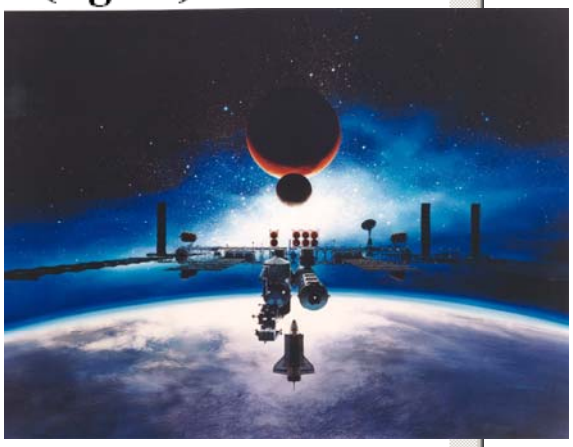
By Ryan Singel August 26, 2008 | 2:22:55 PM Categories: Hacks

...

"This is not the first time we have had a worm or a virus," NASA spokesman Kelly Humphries said. "It's not a frequent occurrence, but this isn't the first time."

...

NASA declined to name the virus, but SpaceRef.com, which broke the story, reported that the worm was W32.Gammima.AG worm -- a worm first detected in August 2007 that installs software that steals credentials for online games.

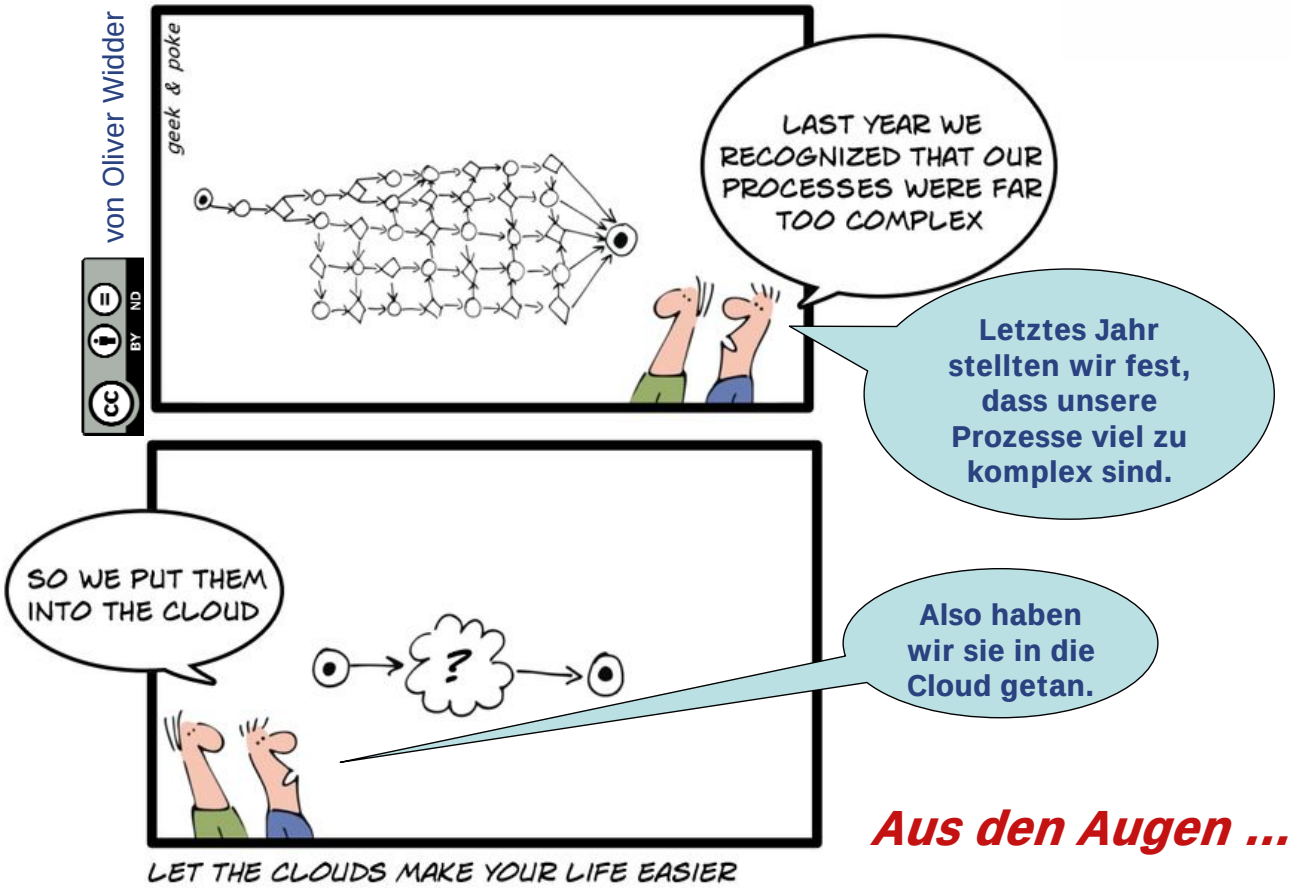


...

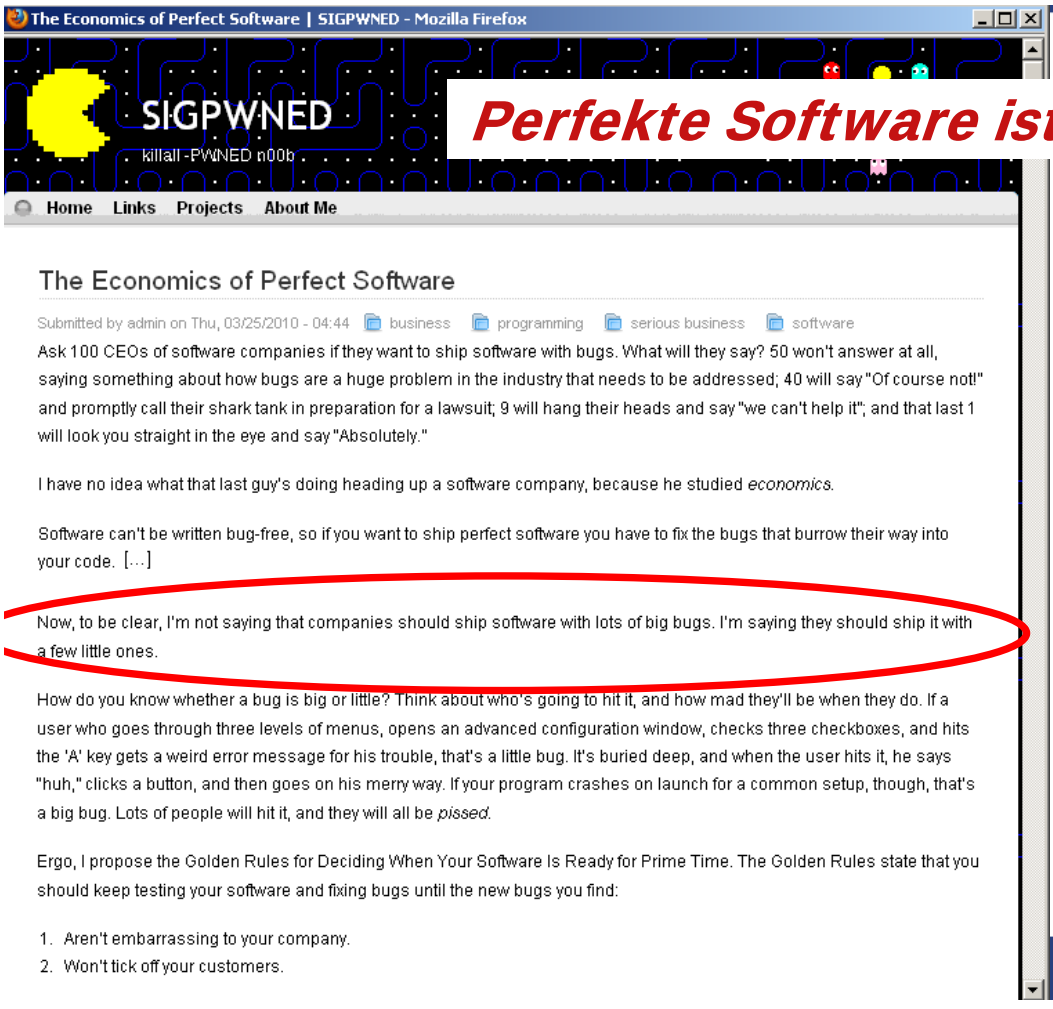
"Everything is scanned before it goes up, so it's an indirect connection," Humphries said.

As for whether mission critical systems are connected to the same network as these kinds of laptops?

"I don't know and even if I did, I wouldn't be able to tell you for IT security reasons," Humphries said.



Aus den Augen ...



Perfekte Software ist zu teuer

Das darf **keine Ausrede** sein bei kritischen Infrastruk-turen oder „System-relevantem“.

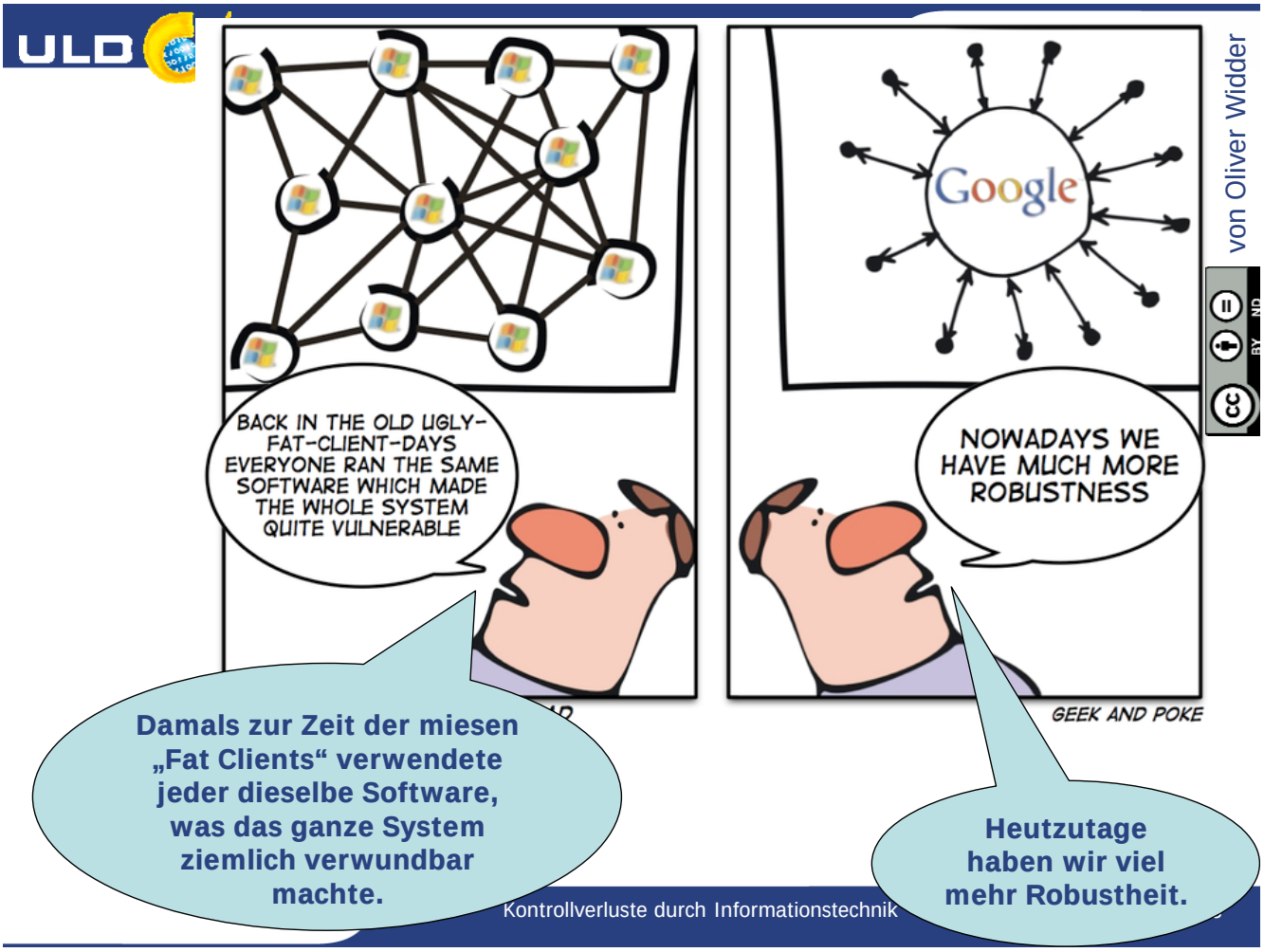
Generell:

„große“ Fehler vermeiden!

Umgang mit Fehlern

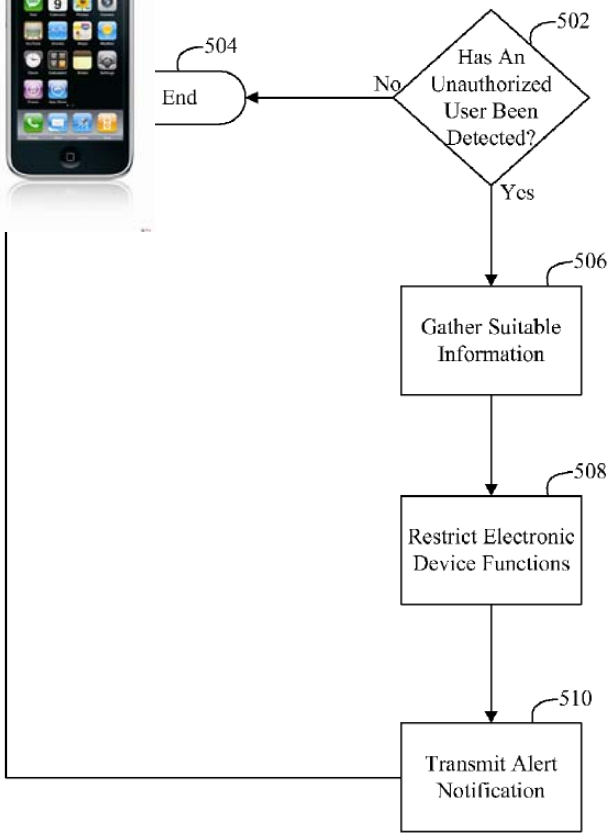
- **Bei Menschen**
  - „menschlich“
- **Bei Gesetzen**
  - Auslegung (z.B. teleologisch: nach Sinn und Zweck)
  - Rechtsweg
- **Bei Informationstechnik**
  - Syntax error: läuft nicht
  - Semantics error: läuft, aber tut etwas anderes als geplant – und dies nicht nur für wenige Einzelfälle
  - „Irren ist menschlich. Aber wenn man richtig Mist bauen will, braucht man einen Computer.“ (Dan Rather)

Kontrollverlust – nicht nur im Fehlerfall



von Oliver Widder

Apple-Patent zum Diebstahlschutz: via iPhone (Aug. 2010)



- „Systeme und Verfahren zum Identifizieren nicht-autorisierter Nutzer eines elektronischen Geräts“
- Identitätsprüfung per Foto, Stimme, Herzschlag, ...
- Läuft stets im Hintergrund mit

⇒ Viele Datenschutzfragen!

- **Kontrolle nur durch Apple?**

Lösungsansatz I: Professionelle Datenverarbeitung

Professionell Hardware, Betriebssystemen und Anwendungs-Software entwerfen und betreiben

- Ein **stabiles Fundament** entwickeln
- **Sicherheitsmechanismen** integrieren
- **Dokumentation, Test und Freigabe** realisieren
- **Evaluieren:** Audit und Gütesiegel
- **„Prüfpunkte“** für interne und externe Kontrollen vorsehen

Foto: Patrick Hoesly

Lösungsansatz II: Privacy by Design

- Zur Risikovermeidung: **Datenvermeidung**
- Für vorhandene Daten: **„Policies“**
  Vorgaben für Verarbeitung und Einschränkungen machen
  - maschinenlesbar
  - durchsetzbar
  - Sticky Policies:
    an die Daten geklebt
- **Transparenz** über Datenverarbeitung

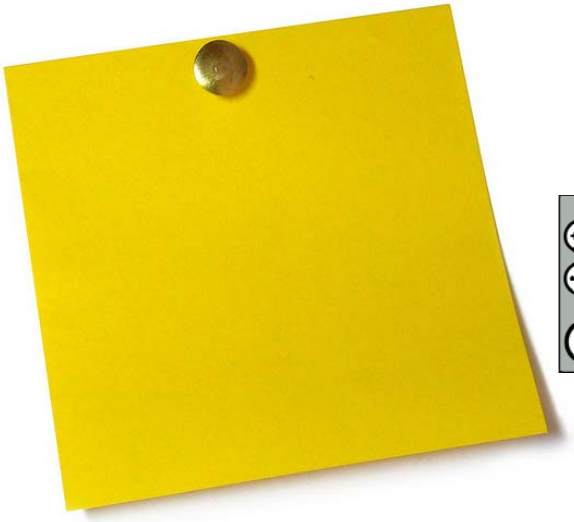


Foto: Peteris B

Kooperativ kann es funktionieren – aber wenn die Datenverarbeiter und Hersteller nicht mitziehen?

Kontrollverlust – psychologisch

- **Kontrollverlust:**
  abnehmende Auswirkung des eigenen Handelns auf Ergebnisse

- **Typische Reaktionen:**

1. **Aktives Handeln**, um Kontrolle zurückzugewinnen (nicht unbedingt zielgerichtet)

2. **„Erlernte Hilflosigkeit“** ⇒ Passivität, Apathie

Potenzielle Auswirkungen

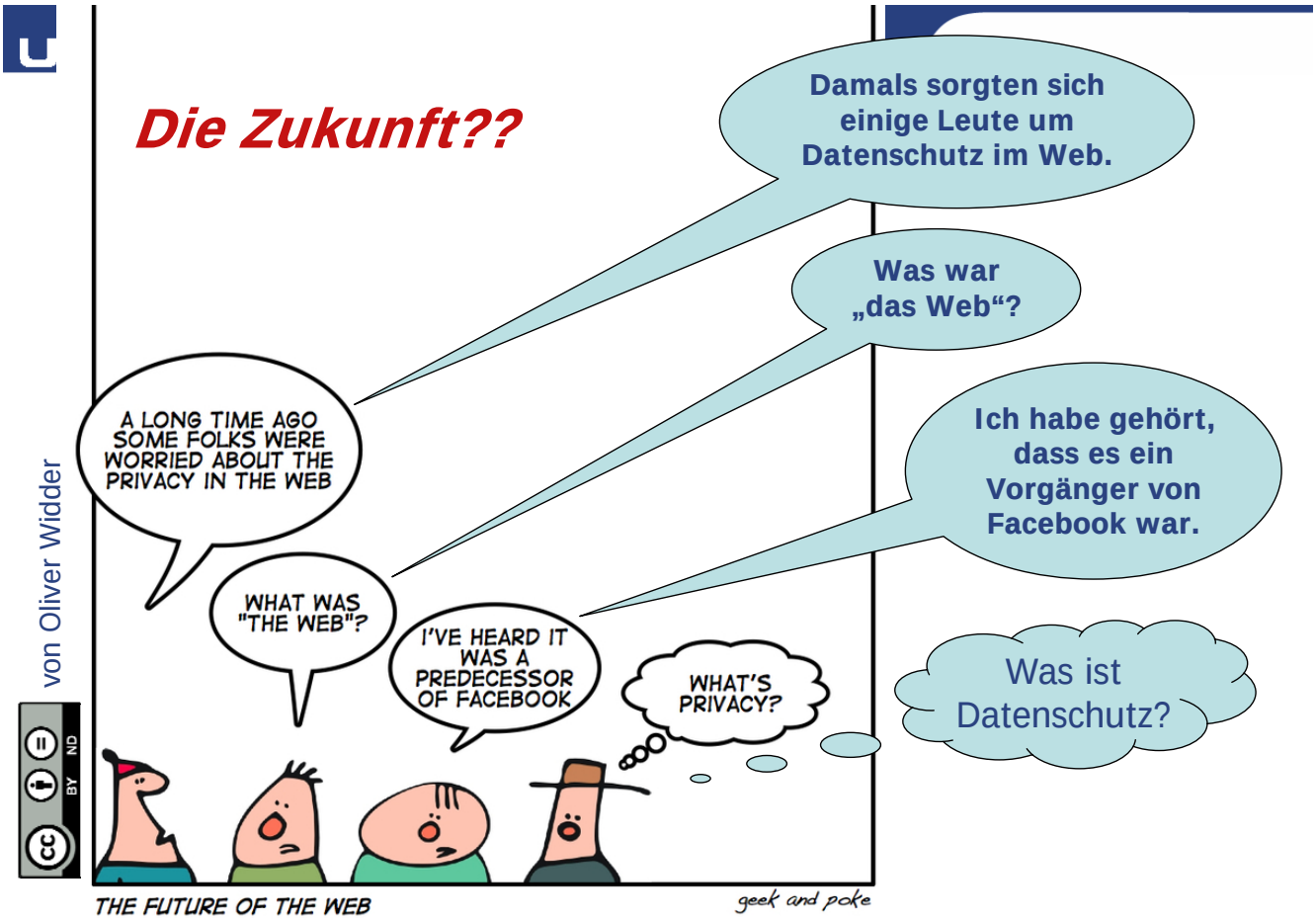
1. Für die weiterhin Kontrollbedürftigen

- Angebot von echten Kontrollmöglichkeiten
- Angebot von **Placebo-Kontrollmöglichkeiten**

2. Bei erlernter Hilflosigkeit

- **Auswirkungen auf Gesellschaft?**
- **Gewöhnungseffekt?**

Die Zukunft??



Fazit

- Die heutzutage verbreitete Informationstechnik bietet **keine ausreichende Kontrolle**
  - ... für Betroffene
  - ... für Daten verarbeitende Stellen
  - ... für Aufsichtsbehörden
- Völliges Neu-Design der IT-Welt wird nicht passieren, aber **stetiges Nachbessern** möglich (und nötig)
- **Privacy by Design** kann funktionieren; reiner Selbstdatenschutz reicht nicht!
- Offen: Werden **die internationalen Player die europäischen Datenschutz-Interessen umsetzen**?

Vielen Dank für Ihre Aufmerksamkeit!