Vertrauensfrage:
Warum mobile IT in Behörden und Unternehmen so problematisch ist

Christian Krause
Dr. Malte Engeler
Unabhängiges Landeszentrum für Datenschutz
Schleswig-Holstein

Sommerakademie

Kiel, 31. August 2015

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Rechtsrahmen

- **Rechtliche Vorgaben für den Einsatz mobiler IT?**

- **Arbeitnehmerdatenschutz (§ 32 BDSG) und Kundendatenschutz (§ 28 Abs. 1 BDSG)**
  - Erforderlichkeit als Leitlinie kaum hilfreich
- **Technisch-organisatorische Maßnahmen (§ 9 BDSG)**
  - Was ist „best practice“ für Biometrie auf mobiler IT?
- **Telemedienrecht**
  - Datenschutzerklärung, Impressum
  - Inhalts- vs. Bestandsdaten
- **BetrVG (§ 87 BetrVG)**
  - Kontrolle der Arbeitnehmer oft mitbestimmungspflichtig
- **Fazit:** Gerade BDSG bietet derzeit kaum Antworten

Was ist mobile IT

- Mobile IT ist zunächst einmal „tragbar“
- Aber tragbare PCs unterscheiden sich nicht grundsätzlich von stationären Computern.
- Betriebssystem und Software sind in der Regel identisch mit der stationärer PCs
- Neue Problemfelder sind:
  - Mögliche Privatnutzung
  - Leichtes Abhandenkommen der Hardware
  - Andere Hardware- und Betriebssystemumgebungen

Oder anders ausgedrückt:

Wir möchten mit Ihnen nicht über Notebooks sprechen.

Stattdessen nun:

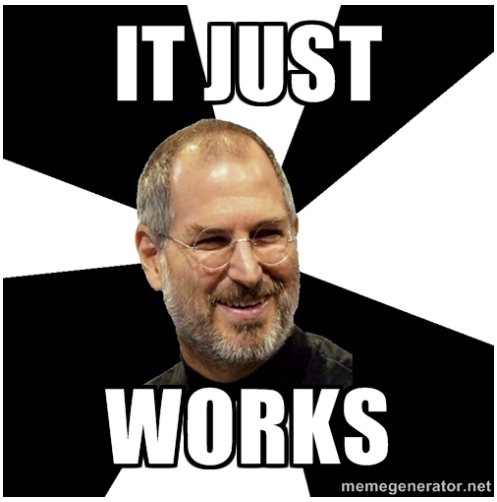
Der Verlust der Universalmaschine

Der klassische PC

- **Hardware**
- **Betriebssystem**
- **Treiber**
- **Applikationen**
- **Außerdem:**
  - **Unglaublich viel Zeit für**
    - Auswahl der Komponenten
    - Konfiguration
    - Wartung

Smarte Geräte

- **Entscheidung für eine Plattform oder einfach gleich BYOD**
- **Danach ein bisschen Entscheidung für Hardware und Applikationen**



Universalmaschine?

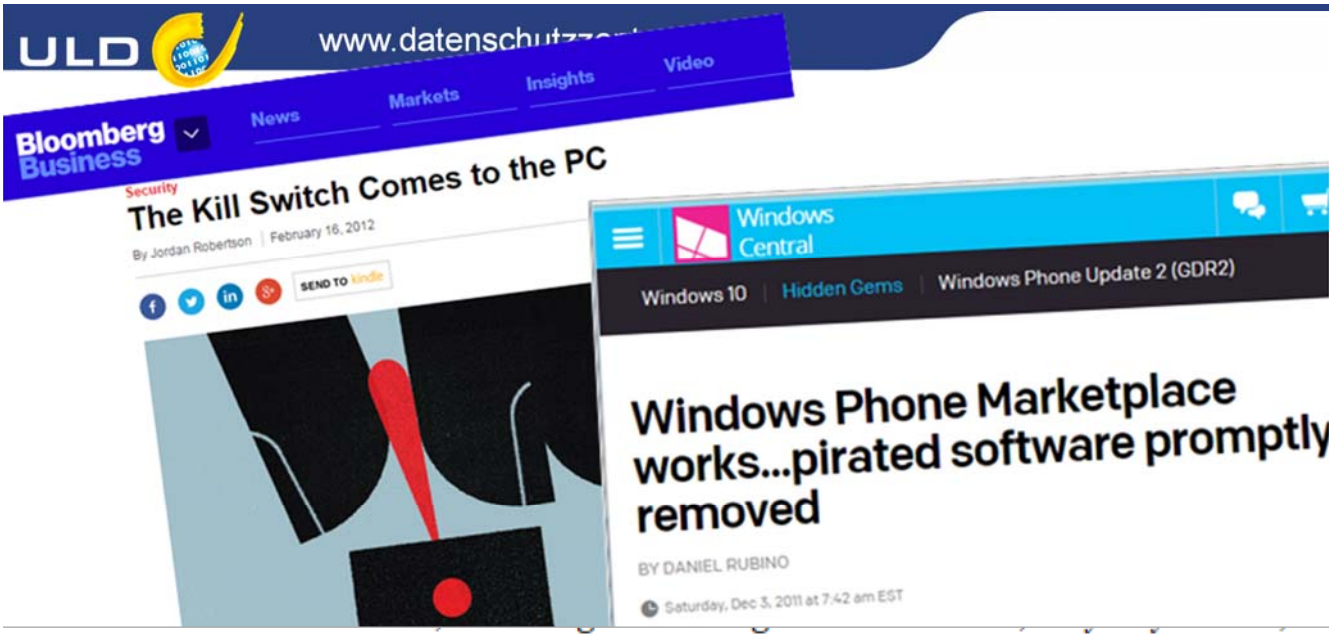
- **Der Nutzer kontrolliert Hard- und Software und entscheidet über ihre Verwendung**
- **Wenn der Nutzer es will, kann der Computer alle Programme ausführen, die er „versteht“:**
  - Gute und böse, funktionierende und bockige, hilfreiche und nutzlose

Apple verbietet feministische Masturbations-App

Mac&i 20.05.2014 13:53 Uhr – Ben Schwan vorlesen

Mit der App "HappyPlayTime" sollten Frauen ihren Körper entdecken können – und das durchaus geschmackvoll. Doch an Apples App-Store-Review-Team kam Entwicklerin Tina Gong nicht vorbei.

Wenn es um Inhalte sexueller Natur geht, kennt Cupertino in seinem App Store keinen Spaß – selbst Cover von Nachrichtenmagazinen, die an jedem deutschen Kiosk verfügbar sind, bekamen da schon mal Probleme. Der US-Entwicklerin Tina Gong war das durchaus bewusst. Trotzdem glaubte sie, dass ihre App "HappyPlayTime", mit der Frauen ihren Körper besser kennenlernen sollten, um das "Stigma der weiblichen Masturbation zu durchbrechen", zulassen würde.



who makes dice simulator apps. Kill switches are a standard part of most smartphones, tablets, and e-readers. Google, Apple (AAPL), and Amazon (AMZN) all have the ability to reach into devices to delete illicit content or edit code without users' permission. It's a powerful way to stop threats that spread quickly, but it's also a privacy and security land mine.

§202a StGB Ausspähen von Daten

Einschränkung durch Recht und Technik

SOPA
STOP ONLINE PIRACY ACT

CISPA
CYBER INTELLIGENCE SHARING & PROTECTION ACT

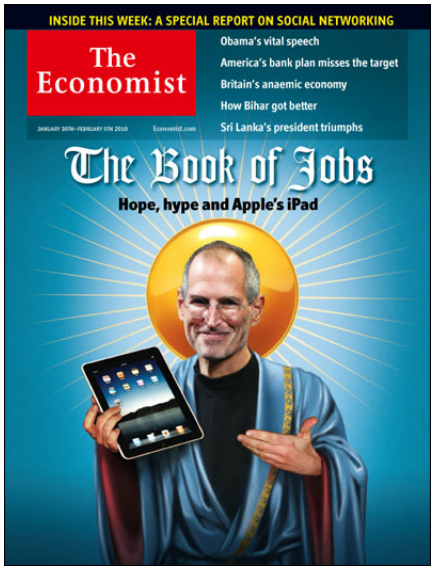
Smarte Geräte: Der Verlust der Universalmaschine

- **In diesem Sinn sind klassische Computer *eher* Universalmaschinen,**
- **Smartphones und Tablets definitiv nicht.**

- **Die Entscheidung, wer und was welche Dinge auf einer Maschine tun darf, wandert zunehmend vom Nutzer zum Hersteller der Maschine.**

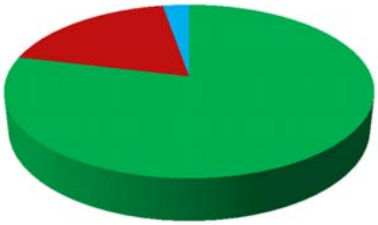
Nadelöhr Appstore

- Download auf mobile Endgeräte geschieht über zentrale Verteilerstelle in Herstellerhand.
- Betriebssystem- und Treiber-Updates liegen in Herstellerhand.
- Auch der Verbleib bereits installierter Software hängt vom Hersteller ab.



Die Marktlage

- **Derzeit primär:**
  - Android (Google, **USA**)
  - iOS (Apple, **USA**)
  - Windows Phone 8 (Microsoft, **USA**)



Weltweite Verteilung Q1 2015
Zahlen von IDC.com

- **Hintergrund:**
  - Apple und Microsoft waren zuerst Hard-/Softwarehersteller
  - Google verkaufte zuerst Werbung

Vertrauensstufen

- **Einsatzszenarien für mobile Geräte in Behörden und Unternehmen**
  - Szenario 1: **Wie Privatnutzer**
    Private Geräte ohne Administration in Betrieb und Behörde
  - Szenario 2: **Managed Device / BYOD**
    Private Geräte unter Administration/dienstl. Nutzung
  - Szenario 3: **Container-Lösungen**
    Abgetrennte dienstl. Bereiche bzw. gekapselte Apps auf Privat-/Dienstgeräten
  - Szenario 4: **Kein Einsatz**
    Vollständiger Verzicht auf mobile IT

Vertrauensstufen

- **Szenario 1: Einsatz mobiler IT ohne Administration (wie Privatanwender)**

  - **Grundsatzprobleme aktueller mobiler Systeme**

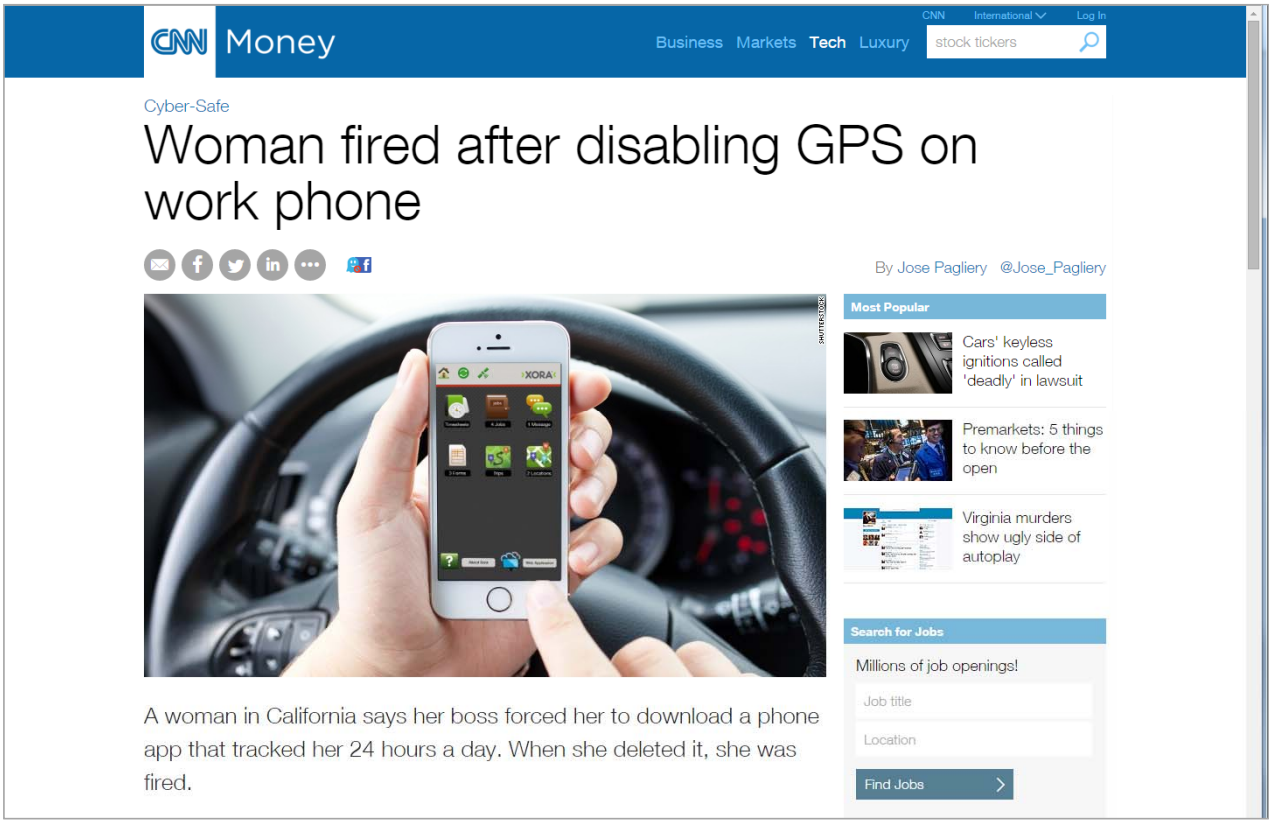
Android	iOS	Windows Phone
• Fragmentierung (Stagefright) • Biometrie unsicher • Rechteverwaltung • Werbenetzwerke und Nutzerprofile	• Kein Datenzugriff auf Systemebene • Schad-Apps über Entwickleraccount • iCloud als Rückgrat	• Appstore ohne QM • Verschlüsselung/ Rechteverwaltung kein Standard • Kein CardDAV, CalDAV

  - **Fazit: Kein ausreichendes Schutzniveau**

Vertrauensstufen

- **Szenario 2: Managed Device / BYOD**

  - **Warum BYOD?**
  - **Möglichkeiten …**
    - Verschlüsselung / Kennwörter vordefinieren
    - Verfügbarkeitskontrolle (Wo, wann, wie, wie lange)
    - App-Quellen unter Kontrolle
  - **… und Grenzen von Managed Device**
    - Kontaktdaten und Drittapps (Whatsapp, Facebook)
    - Grundsätzlich Datenschutzprobleme bleiben unberührt
  - **Arbeitnehmer-Überwachung als Nebenfolge?**
    - Ortung der Mitarbeiter
    - Analyse von Nutzungs- und Leistungsverhalten



Vertrauensstufen

- **Szenario 3: Container-Lösungen**
  - **Exciter, KNOX, Cortado, Good Technology etc.**
  - **Wie isoliert ist der „Container“?**
    - Schnittstellen zur Anwendungsprogrammierung (APIs)
    - Entschlüsselte Daten zur Laufzeit? (Google Login in iOS)
    - Display- und Tastaturtreiber vom OS
    - Siri Proactive vs. Google Now On Tap?
  - **Komfort vs. Sicherheit im Container**
    - Die Zwischenablage
    - Telefonieren aus der Sandbox?
  - **Vertrauen in das OS?**
    - Zufallszahlengenerator für Verschlüsselung (VPN, PGP, SSL)
    - Nach wie vor Kontrolle des Herstellers über Gerät und Software
    - Unerwartete Backdoors (Wortvorschläge, Spracheingabe)

Vertrauensstufen

- **Szenario 4: Verzicht auf mobile Geräte**
  - **Grenzen mobiler IT?**
    - Problemfall: Souveränitätsverlust des Staates
      - Patentanträge auf dem iPad?
      - Patientenplanung unter Android
      - Gemeindeverwaltung per Windows Phone
      - Polizeidienst mit mobiler IT
  - **Wann ist Verzicht einzige Möglichkeit?**
    - Schutzniveauprüfung nach Standard-Datenschutzmodell
    - Abwägung zwischen Schutzbedarf und mögl. Maßnahmen
  - **Fazit: Es gibt Bereiche, in denen aktuelle mobile IT nicht einsatzfähig ist**

Empfehlungen

- **Empfehlungen für den Einsatz mobiler IT**
  - **Schutzniveauprüfung nach SDM**
    - Hersteller vs. nutzendes Unternehmen: Wer hat die Kontrolle?
    - Abhängig von Schutzbedarf
    - Device Management, Container, Verzicht im Einzelfall
  - **Beratung durch Aufsichtsbehörden**
    - Betriebsvereinbarungen
    - Binding Corporate Rules
  - **Gütesiegel**
  - **Orientierungshilfen im Netz**
    - Z.B. „Verwendung von Tablets durch Gemeindevertreter“

Vielen Dank für Ihre Aufmerksamkeit!

Christian Krause | ULD
uld38@datenschutzzentrum.de

Dr. Malte Engeler | ULD
uld43@datenschutzzentrum.de

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
Holstenstraße 98, 24103 Kiel
0431 988 1200
mail@datenschutzzentrum.de