Schutz von sensiblen Daten und Kritischen Infrastrukturen

– Herausforderungen und Lösungen aus Sicht des Datenschutzes –

Marit Hansen

Landesbeauftragte für Datenschutz
Schleswig-Holstein

Kiel, 22.09.2017

forum <privatheit>
selbstbestimmtes_leben_in_der_digitalen_welt

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Das ULD

- **ULD** = Unabhängiges Landeszentrum für Datenschutz
- **Leiterin:**
  Landesbeauftragte für Datenschutz Schleswig-Holstein

- **Zuständig** für Datenschutz und Informationszugang
- Jeder hat das Recht, sich an die Landesbeauftragte für Datenschutz zu wenden
- Auch Beratung von Unternehmen angeboten

- **Mehr Informationen:** `www.datenschutzzentrum.de`

Aktuelles System der deutschen Datenschutzbehörden

- **1 Bundesbeauftragter**
  - für den öffentlichen Bereich auf Bundesebene; Rechtsgrundlage: **Bundes**-DSG*)
  - für Telekommunikation; Rechtsgrundlage: TKG
- **16+ Landesbeauftragte für 16 Länder**
  - für den öffentlichen Bereich; Rechtsgrundlage: 16x LDSG++
  - für den nicht-öffentlichen Bereich, d.h. Firmen in den Ländern; Rechtsgrundlage: **Bundes**-DSG
- **Eigene Datenschutzbeauftragte** für Kirchen und Rundfunkanstalten

*) 25.05.2018: Geltung Datenschutz-Grundverordnung

Überblick

- Eingebaute Sicherheit
  - Gültiger Startpunkt?
- Datenschutz
  - Perspektivwechsel
  - Anforderungen aus Europa
- Eingebauter Datenschutz
  - Datenschutz „by Design“
  - Datenschutz „by Default“
- Fazit

Aktuelle Hacking-Angriffe

Handelsblatt

ATTACKE ÜBER SOFTWARE CCLEANER

Tech-Konzerne waren Hauptziel der Hacker

Datum: 21.09.2017 19:58 Uhr

Hacker hatten über einen Virus im Update der CCleaner-Software versucht, über zwei Millionen Rechner zu kontrollieren. Eine IT-Sicherheitsfirma hat nun herausgefunden, dass die Attacke Technologie-Riesen galt.

https://www.handelsblatt.com/my/unternehmen/it-medien/attacke-ueber-software-ccleaner-tech-konzerne-waren-hauptziel-der-hacker/20362252.html

WELT N24 DIGITAL ZEITUNG TV

WIRTSCHAFT

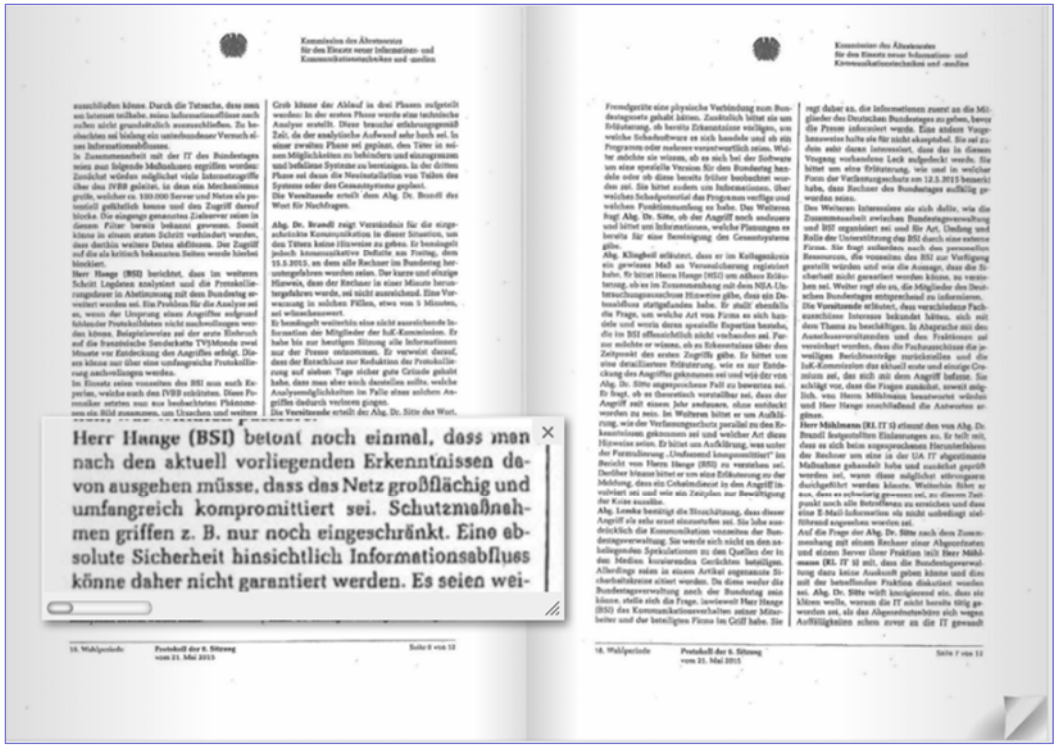
Hacker greifen Börsenaufsicht in den USA an

Stand: 06:23 Uhr

Ein Hackerangriff auf die US-Börsenaufsicht SEC hat Cyberkriminellen womöglich illegale Finanzgeschäfte ermöglicht. Der Angriff auf eine Datenbank der Börsenaufsicht sei bereits im vergangenen Jahr erfolgt, teilte die SEC mit. Im August diese Jahres habe die Behörde dann in Erfahrung gebracht, dass die erbeuteten Daten die Angreifer möglicherweise in die Lage versetzten, „illegale Gewinne“ aus Börsengeschäften zu erzielen. Die Angreifer nutzen demnach eine Softwarelücke aus, die kurz nach der Cyberattacke geschlossen werden konnte. Dennoch sei es den Hackern gelungen, Zugriff auf „nicht öffentliche Informationen“ zu erhalten. In der betroffenen Datenbank sind etwa Angaben über Geschäfte von börsennotierten Firmen enthalten.

https://www.welt.de/print/welt_kompakt/print_wirtschaft/article168912192/Hacker-greifen-Boersenaufsicht-in-den-USA-an.html

Brüchiges Fundament?



Herr Hange (BSI) betont noch einmal, dass man nach den aktuell vorliegenden Erkenntnissen davon ausgehen müsse, dass das Netz großflächig und umfangreich kompromittiert sei. Schutzmaßnahmen griffen z. B. nur noch eingeschränkt. Eine absolute Sicherheit hinsichtlich Informationsabfluss könne daher nicht garantiert werden. Es seien wei-

Beispiel: „Bundestags-Hack“

Kommission des Ältestenrates für den Einsatz neuer Informations- und Kommunikationstechniken und –medien, Protokoll vom 21.05.2015

Sicherheit durch Ausbauen

THE VERGE

TRENDING NOW
This is VAIO's Windows phone

39 NEW ARTICLES
63 COMMENTS

US & WORLD

Dick Cheney had the wireless disabled on his pacemaker to avoid risk of terrorist tampering

By Carl Franzen on October 21, 2013 06:54 pm Email @carlfranzen

http://www.theverge.com/2013/10/21/4863872/dick-cheney-pacemaker-wireless-disabled-2007

http://resources.infosecinstitute.com/hcking-implantable-medical-devices/

WWW mit oder ohne

The Register®
Biting the hand that feeds IT

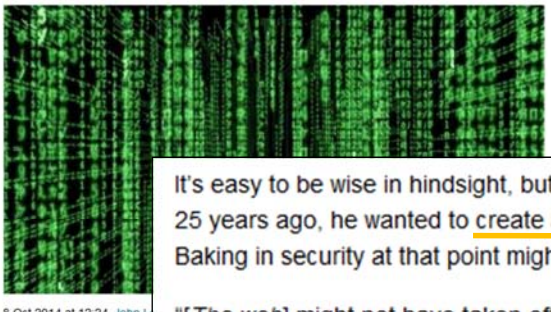
DATA CENTRE SOFTWARE NETWORKS SECURITY INFRASTRUCTURE DEVOPS BUSINESS HARDWARE SCIENCE BOOTNOTES FORUMS

Security

Sir Tim Berners-Lee defends decision not to bake security into www

'The idea that privacy is dead is hopelessly sad'

More like this
Tim Berners-Lee



8 Oct 2014 at 12:24, John L

IP Expo Sir Tim Berners-Lee wide web.

It's easy to be wise in hindsig 25 years ago, he wanted to Baking in security at that po

"[*The web*] might not have ta this morning.

Sir Tim's views are in contras regretted not building in sec current push towards always more to do with timing and priorities than principles.

During a keynote presentation at the infrastructure conference, Sir Tim discussed a vision for the web where users are more in control of managing their privacy.

"The idea that privacy is dead is hopelessly sad," Sir Tim Berners-Lee said. "We have to build systems that allow for privacy."

It's easy to be wise in hindsight, but Sir Tim explained that at the point he invented the world wide web 25 years ago, he wanted to create a platform that developers would find familiar and easy to use. Baking in security at that point might have worked against that goal, he said.

"[*The web*] might not have taken off if it had been too difficult," he told an audience at IPExpo Europe this morning.

Sir Tim's views are in contrast with those of another internet pioneer, Vint Cerf, who recently said he regretted not building in security to basic internet protocols. Berners-Lee strongly supported the current push towards always-on crypto (https) for websites now underway, so his differing views are more to do with timing and priorities than principles.

„timing and priorities“ – Sicherheit kann nachrangig sein

http://www.theregister.co.uk/2014/10/08/sir_tim_bernerslee_defends_decision_not_to_bake_security_into_www/

Alle wollen Sicherheit – oder?

- Massives Interesse an Unsicherheit

- Lukrativer Markt
  für Zero-Day-Exploits
  (Angriffsmöglichkeit, bevor es eine Gegenmaßnahme gibt; Entwickler haben 0 Tage Zeit zum Reagieren)

http://tegenlicht.vpro.nl/backlight/zerodays.html
https://www.youtube.com/watch?v=4BTTiWkdT8Q

Rolle von Hintertüren – Manipulation der Infrastruktur (siehe Snowden Files)

Foto: anyjazz65

Foto: Nic McPhee

Geschwächter Sicherheitsstandard

09/2013: NIST (National Institute of Standards and Technology) warnt vor Dual_EC_DRBG (Pseudozufallszahlengenerator)

NIST works to publish the strongest cryptographic standards possible, and uses a transparent, public process to rigorously vet its standards and guidelines. If vulnerabilities are found, NIST works with the cryptographic community to address them as quickly as possible.

In light of the concerns expressed regarding Dual_EC_DRBG, ITL is taking the following actions:

Recommending against the use of SP 800-90A Dual Elliptic Curve Deterministic Random Bit Generation: NIST strongly recommends that, pending the resolution of the security concerns and the re-issuance of SP 800-90A, the Dual_EC_DRBG, as specified no longer be used.

Re-issuing SP 800-90A as a draft for public comment: Effec 800-90A is being re-issued as a draft for public comment for concerns or recommendations for improvement regarding t *Generation Using Deterministic Random Bit* Generators are (http://csrc.nist.gov/publications/PubsDrafts.html). NIST wi comments received during this 60 day period.

On the Possibility of a Back Door in the NIST SP800-90 Dual Ec Prng

Dan Shumow
Niels Ferguson
Microsoft

Hintertüren / Master-Schlüssel?

Offline-Beispiel „TSA-Kofferschlösser“:

- Transportation Security Administration
- TSA-Beamte verwenden Master-Schlüssel


Photo: Willh26 (Wikipedia)

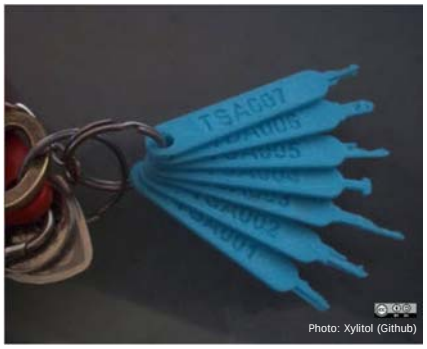
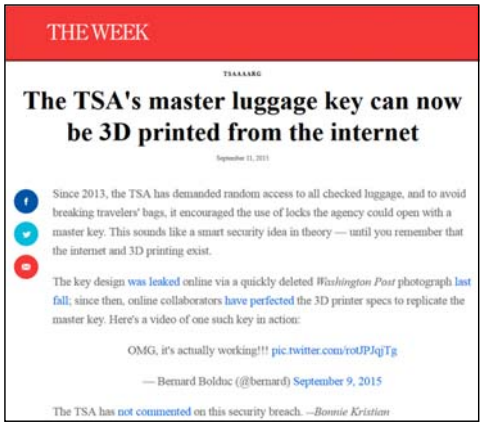


Photo: Xylitol (Github)



THE WEEK

The TSA's master luggage key can now be 3D printed from the internet

Since 2013, the TSA has demanded random access to all checked luggage, and to avoid breaking travelers' bags, it encouraged the use of locks the agency could open with a master key. This sounds like a smart security idea in theory — until you remember that the internet and 3D printing exist.

The key design was leaked online via a quickly deleted *Washington Post* photograph last fall; since then, online collaborators have perfected the 3D printer specs to replicate the master key. Here's a video of one such key in action:

OMG, it's actually working!!! pic.twitter.com/roUPJqjTg

— Bernard Bolduc (@bernard) September 9, 2015

The TSA has not commented on this security breach. —*Bonnie Kristian*

https://theweek.com/speedreads/576722/tsas-master-luggage-key-now-3d-printed-from-internet

NSA-Abt. TAO
(Tailored Access Operations)

SIGINT Enabling Project:

- „insert vulnerabilities into commercial encryption systems, IT systems, networks, and endpoint communications devices used by targets“
- „influence policies, standards and specification for commercial public key technologies“

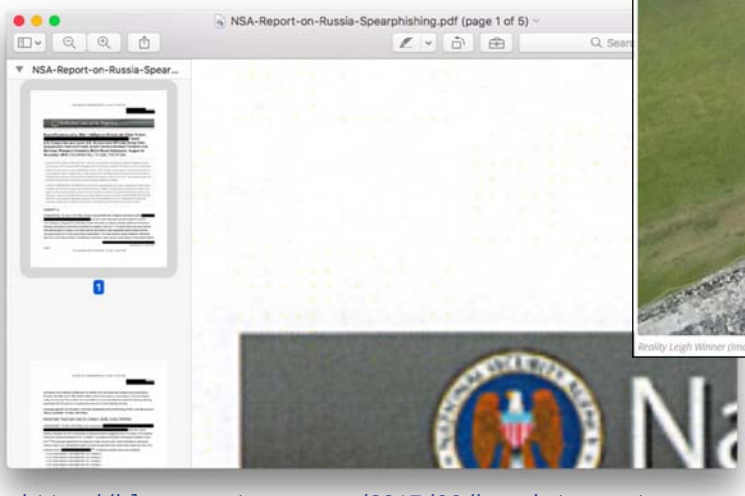
GCHQ-Abt. JTRIG
(Joint Threat Research Intelligence Group)

Manipulation:

- „using online techniques to make something happen in the real or cyber world“

Heutige Situation

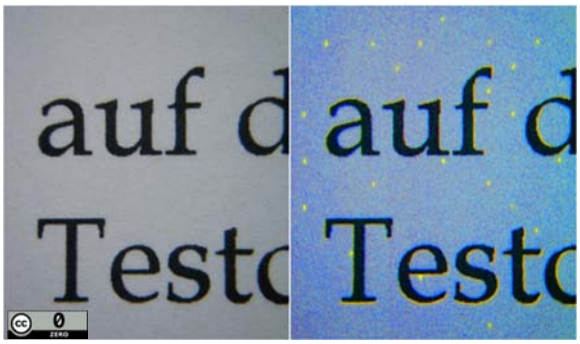
Eingebauter Datenschutz?
Im Gegenteil:
eingebaute Verkettbarkeit
und Identifizierbarkeit



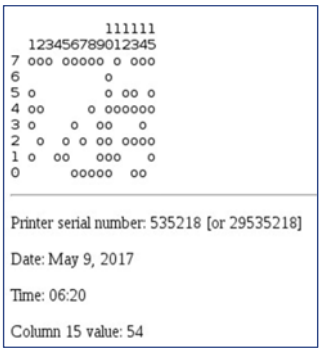
http://blog.erratasec.com/2017/06/how-intercept-outed-reality-winner.html

http://www.washingtontimes.com/news/2017/jun/6/reality-winner-suspected-nsa-leaker-printer-waterm/

Bsp.: „Machine Identification Code“ Gelbe Punkte im Druck



Vorratsdatenspeicherung im Farbdruck:
versteckte Wasserzeichen



https://cdn.arstechnica.net/wp-content/uploads/2017/06/eff-tool-stego.jpg

https://w2.eff.org/Privacy/printers/docucolor/

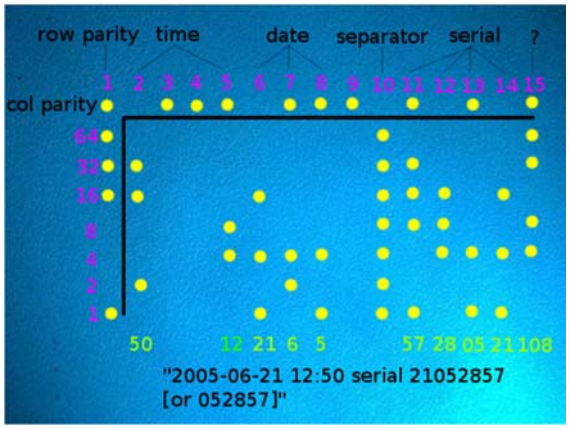


Bild: Electronic Frontier Foundation (EFF)

Speziell: Kritische Infrastrukturen

- Kritische Infrastrukturen (KRITIS):
  - Beispiele: Energie- und Wasserversorgung, TK, Finanz- und Versicherungswesen, Transport, Verkehr, Gesundheit, Ernährung
  - Ein Ausfall oder eine Beeinträchtigung der Versorgung hätte dramatische Folgen für Wirtschaft, Staat und Gesellschaft

- IT-Sicherheitsgesetz (2015)
  - Erhebliche IT-Sicherheitsvorfälle melden
  - „Stand der Technik“ umsetzen und dies ggü. BSI nachweisen
  - TK: Kunden warnen, wenn Missbrauch eines Anschlusses (z.B. Botnetz)
  - Absicherungspflicht auch für gewerbliche Webseiten-Betreiber / Online-Shops: aktuelle Softwareversionen, Updates, Patches

Nachfragen: BSI

Überblick

- Eingebaute Sicherheit
  - Gültiger Startpunkt?
- Datenschutz
  - Perspektivwechsel
  - Anforderungen aus Europa
- Eingebauter Datenschutz
  - Datenschutz „by Design“
  - Datenschutz „by Default“
- Fazit

Beim Datenschutz geht es um ~~Daten~~

Source: Ashtyn Renee

Menschen mit ihren Rechten

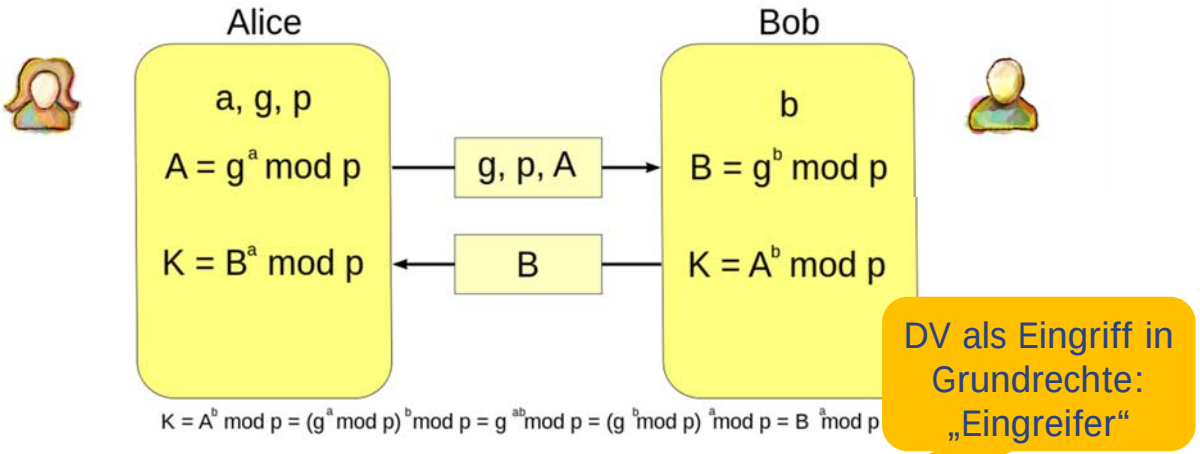
Prüffragen bei der Gestaltung:

- Auswirkungen auf Menschen?
- Auswirkungen auf die Gesellschaft?

Datenschutz nötig:
Machtgefälle

Wichtig:
mehrseitige Sicherheit

Perspektive: Alice & Bob



DV als Eingriff in Grundrechte: „Eingreifer“

IT-Sicherheit: Der Angreifer ist Eve (oder Mallory).

Datenschutz: Der Angreifer ist Bob!
(Jedenfalls auch.)

Datenschutz-Grundsätze

Für personenbezogene Daten:

- Rechtsgrundlage, z.B. Gesetz oder Einwilligung
- Zweckbindung
- Erforderlichkeit
- Transparenz
- Betroffenenrechte
- Datensicherheit

Worum geht es?

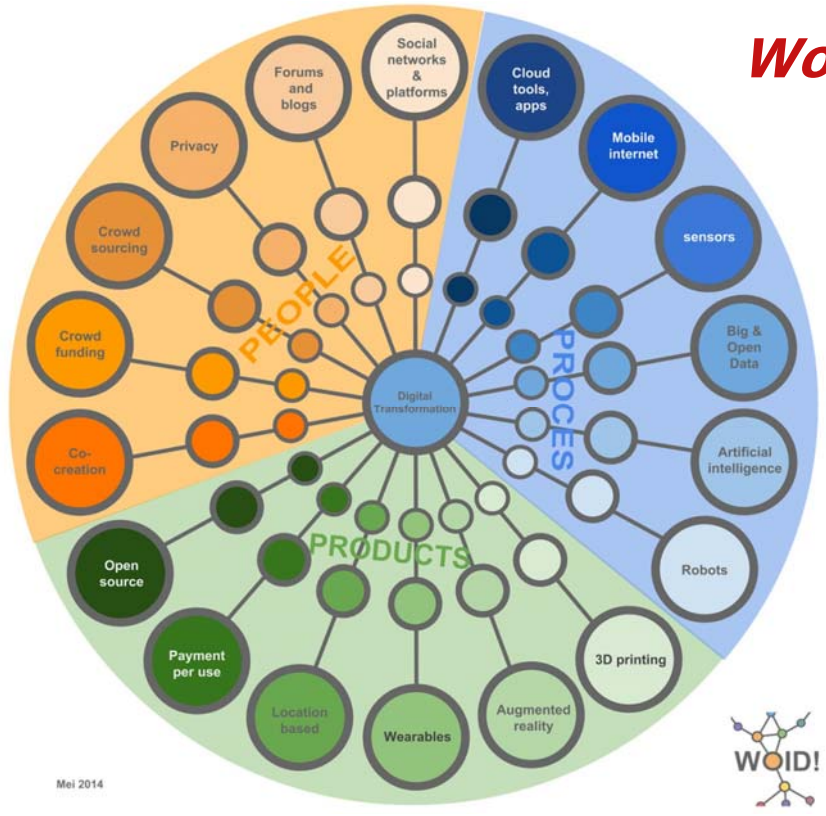


Bild: Detlef La Grand

Digitalisierung: einzelne Anwendungen

Bankautomaten:
Sicherheit einseitig oder mehrseitig?

Nachweis von Echtheit und Manipulations-freiheit

Digitalisierung: einzelne Anwendungen

Online-Banking:
Informationssicherheit

Phishing-Gefahr

Mehr-Faktor-Authenti-sierung als Standard

Digitalisierung: einzelne Anwendungen

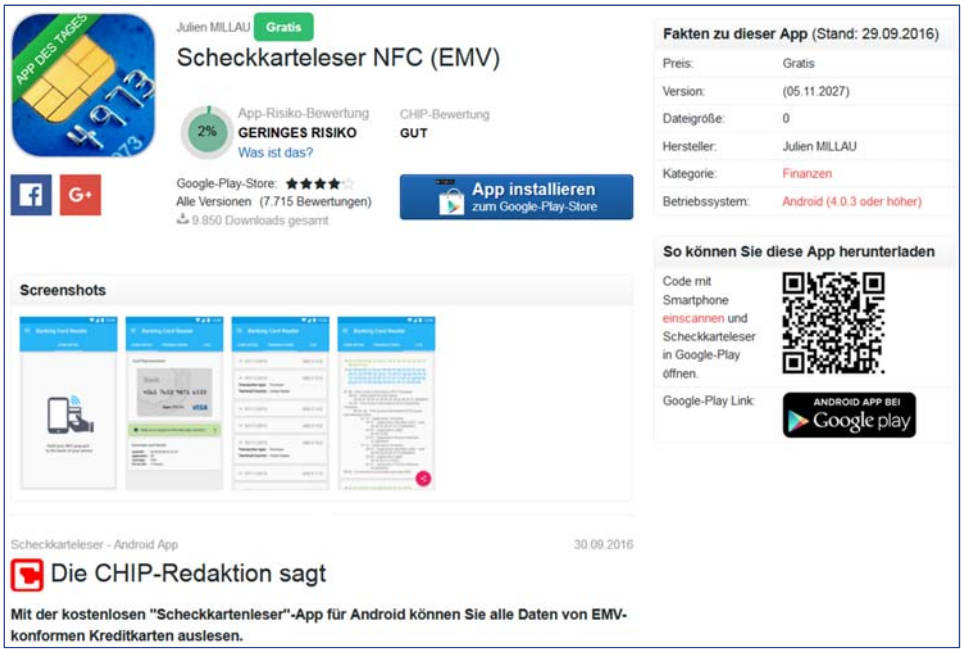
Bewusstsein der Nutzerinnen und Nutzer?

Digitalisierung: einzelne Anwendungen

Kontaktlose Bankkarten (per Near-Field Communication)

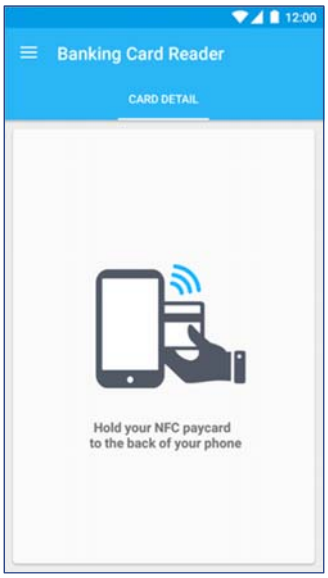
Unterschied
kontaktbehaftet
– kontaktlos

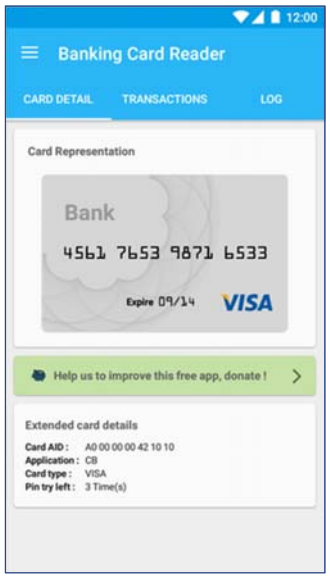
Digitalisierung: einzelne Anwendungen

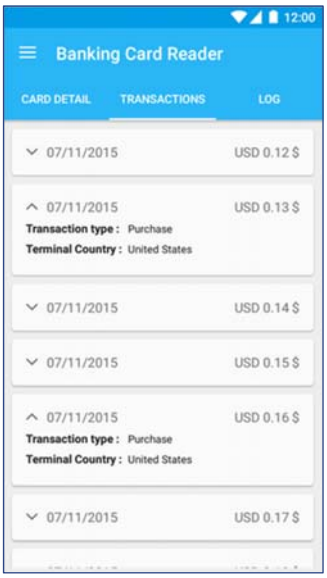


http://www.chip.de/news/NFC-Scanner-fuer-Android-Diese-kostenlose-App-liest-Kreditkartendaten-aus_100745465.html

Digitalisierung: einzelne Anwendungen







http://www.chip.de/news/NFC-Scanner-fuer-Android-Diese-kostenlose-App-liest-Kreditkartendaten-aus_100745465.html

Digitalisierung: einzelne Anwendungen

Drei Alternativen

Die häufigsten Online-Bezahlverfahren

Die umsatzstärksten Onlinehändler bieten am häufigsten die Online-Bezahlverfahren Paypal, Sofortüberweisung und Amazon Payments an. Sie funktionieren ohne extra Software und sind für Kunden kostenlos.

Paypal
Beim größten Anbieter der elektronischen Bezahlverfahren, Paypal, muss man die Kreditkarten- oder Kontodaten hinterlegen und ein Passwort generieren. Zum Bezahlen gibt man seine E-Mail-Adresse und das Passwort ein. Der Händler bekommt keine Bankdaten. Aber der Kunde übergibt diese einem amerikanischen Unternehmen und weiß nicht, was mit diesen Daten passiert.

Sofortüberweisung.de
Für das Bezahlverfahren muss man sich nicht registrieren. Mit einem Klick auf den Button Sofortüberweisung.de wird der Käufer auf die Seite der Sofort AG umgeleitet. Er gibt seine persönlichen Bankzugangsdaten sowie eine Transaktionsnummer (Tan) ein. Sofortüberweisung.de prüft, ob das Konto gedeckt ist. Der Kunde gibt seine persönlichen Bankdaten weiter, was „erhebliche Risiken für die Datensicherheit" birgt (Landgericht Frankfurt am Main, Az. 2-06 0 458/14).

Amazon Payments
Das Verfahren stammt vom Versandhandel-Riesen Amazon. Der Kunde zahlt damit über sein Amazon-Konto bei anderen Onlinehändlern, muss also kein weiteres Konto anlegen. Mit einem Klick auf „Bezahlen über Amazon", der Eingabe von E-Mail-Adresse und Passwort wird der Kauf über die bei Amazon hinterlegten Konto- oder Kreditkartendaten abgewickelt. Die Daten liegen bei einem amerikanischen Unternehmen.

Realität: verbreitete Bezahlverfahren sind nicht datenschutzkonform

3/2016 Finanztest

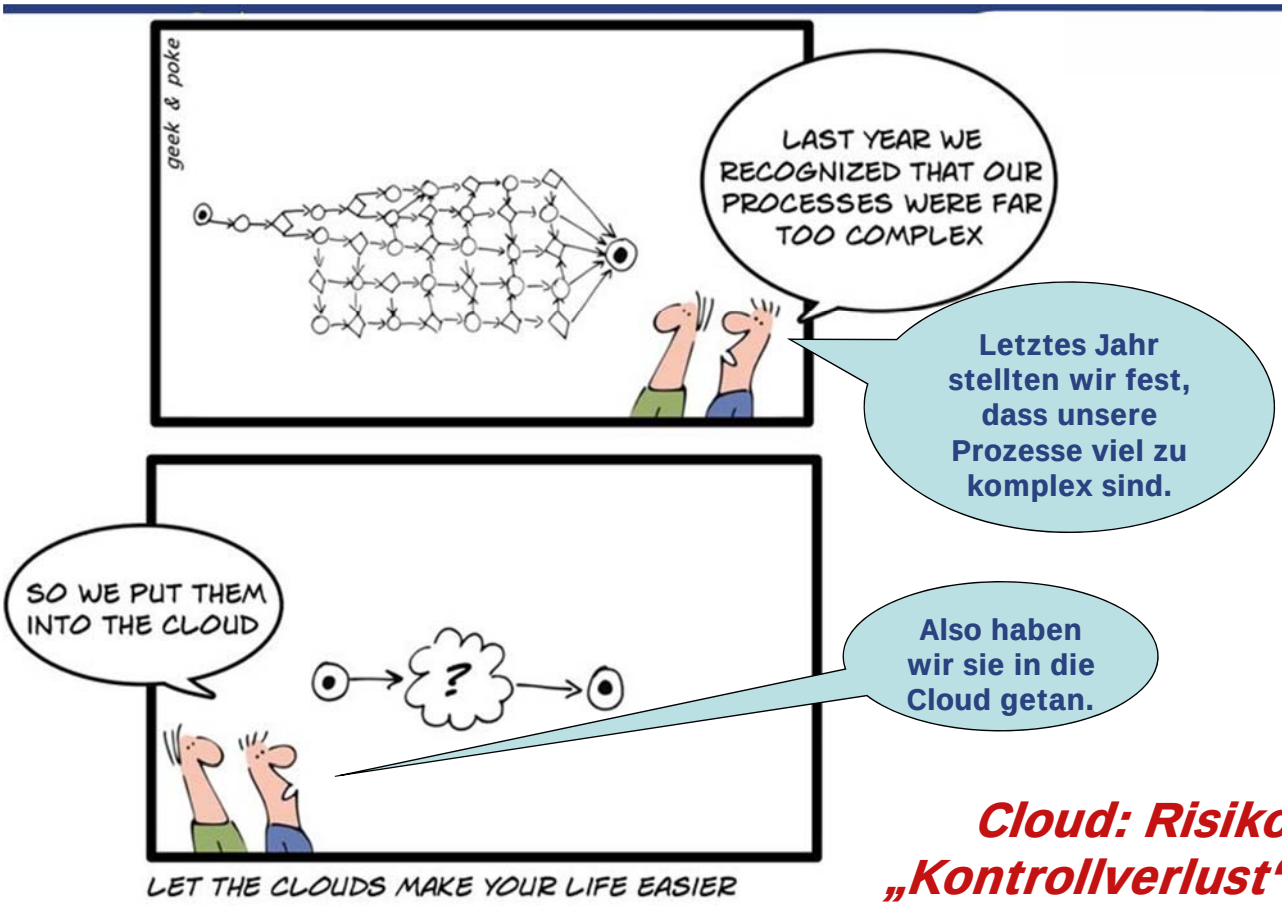
https://www.test.de/Online-Bezahlsystem-Paydirekt-Paypal-auf-Deutsch-4977641-4977647/

Realität heute: dominierende Anbieter für vielfältige Dienstleistungen

Problem, wenn Dienstleister Datenschutzrecht (D/EU) ignorieren

Aber: ab Mai 2018
DS-Grundverordnung
mit dem Marktort-Prinzip

PayPal
Microsoft
Google
Akamai
twitter
facebook
amazon



Cloud: Risiko „Kontrollverlust“

Bild: Oliver Widder

Web 2.0 – Präsenz in Social Media

Meist über zentrale Plattformen, die die Regeln bestimmen

WhatsApp WHATSAPP WEB FUNKTIONEN HERUNTERLADEN

Über unsere Dienste

Registrierung. Du musst dich für unsere Dienste registrieren und dafür korrekte Daten verwenden, deine aktuelle Mobiltelefonnummer angeben und diese im Falle einer Änderung unter Nutzung unserer In-App-Funktion „Nummer ändern“ aktualisieren. Du stimmst zu, SMS und Telefonanrufe mit Codes zur Registrierung für unsere Dienste (von uns oder unseren Drittanbietern) zu erhalten.

Adressbuch. Du stellst uns regelmäßig die Telefonnummern von WhatsApp-Nutzern und deinen sonstigen Kontakten in deinem Mobiltelefon-Adressbuch zur Verfügung. Du bestätigst, dass du autorisiert bist, uns solche Telefonnummern zur Verfügung zu stellen, damit wir unsere Dienste anbieten können.

https://www.whatsapp.com/legal/#terms-of-service

„kostenlos“ = Bezahlen mit Daten

Mit-Betroffene

Big Data: Target-Analyse

FEB 16, 2012 @ 11:02 AM 3,163,996 THE LITTLE BLACK BOOK OF BILLIONAIRE SECRETS

How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did

Kashmir Hill, FORBES STAFF

Welcome to The Not-So Private Parts where technology & privacy c

Every time you go shopping, you share intimate details about your consumption patterns with retailers. And many of those retailers are studying those details to figure out what you like, what you need, and which coupons are most likely to make you happy. Target TGT -1.48%, for example, has figured out how to data-mine its way into your womb, to figure out whether you have a baby on the way long before you need to start buying diapers.

Target has got you in its aim

https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/

The New York Times Magazine https://nyti.ms/AyNgCY

Magazine

How Companies Learn Your Secrets

By CHARLES DUHIGG FEB. 16, 2012

Andrew Pole had just started working as a statistician for Target in 2002, when two colleagues from the marketing department stopped by his desk to ask an odd question: "If we wanted to figure out if a customer is pregnant, even if she didn't want us to know, can you do that? "

http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html

Big Data: Auswirkungen auf Einzelne oder Gruppen

"Your recent Amazon purchases, Tweet score and location history makes you 23.5% welcome here."

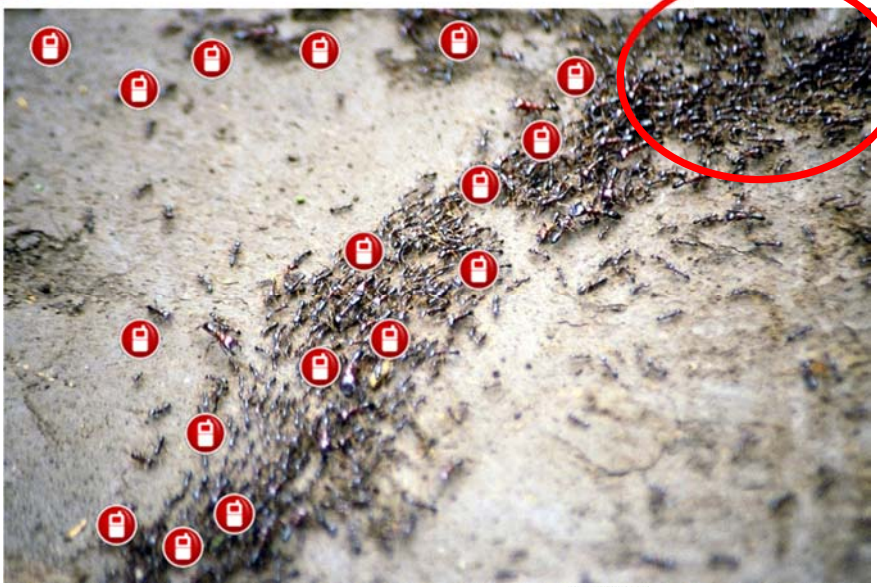
Quelle: Thierry Gregorius

Foto: Christian Heilmann

Big Data mit Bias?

Gründe, um **nicht** Daten zu liefern:

- Arm
- Alt
- Privacy-bewusst
- ...



- Auswirkung auf Entscheidungen?
- Manipulationsrisiko?

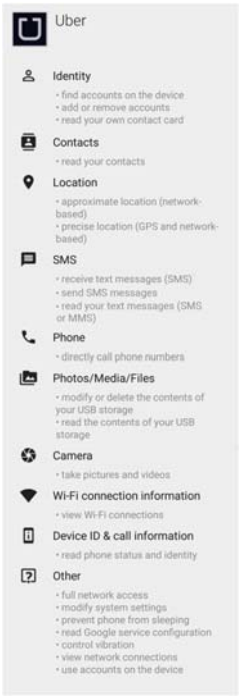
Heutige Situation

- Eingebauter Datenschutz? Im Gegenteil: eingebaute Verkettbarkeit und Identifizierbarkeit

Kaum Wahl-möglichkeiten

- Prinzip „Take it or leave it“, z. B. bei Apps

Oft Zugriff auf Adressbuch, Orts-daten, Mikrofon...

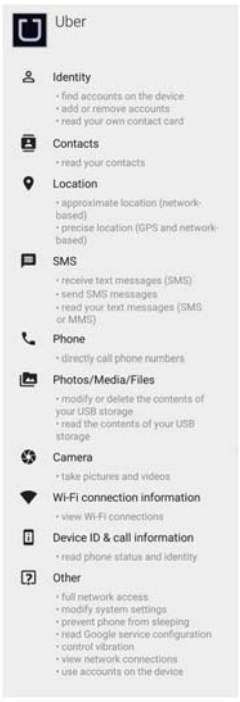


Heutige Situation

- Eingebauter Datenschutz?
  Im Gegenteil:
  eingebaute Verkettbarkeit
  und Identifizierbarkeit

Kaum Wahl-möglichkeiten

- Prinzip „Take it or leave it“,
  z. B. bei Apps



Zugriff auf Batterie-Status relevant?

Uber knows customers with dying batteries are more likely to accept surge pricing

Uber CREDIT: KAI PFAFFENBACH/REUTERS

By Marion Dakers
22 MAY 2016 • 11:22AM

The car-hailing service Uber can detect when a user's smartphone is low on battery, and therefore willing to pay more to book a ride.

Uber, which has faced the ire of London's tax drivers since launching in the capital in 2012, can tell when its app is preparing to go into power-saving mode, although the firm says it does not use this information to pump up the price.

Keith Chen, head of economic research at Uber, told NPR that users are willing to accept a "surge price" up to 9.9 times the normal rate, particularly if their phone is about to die.

The Telegraph

http://www.telegraph.co.uk/business/2016/05/22/uber-app-can-detect-when-a-users-phone-is-about-to-die/

theguardian

Your battery status is being used to track you online

Battery status indicators are being used to track devices, say researchers from Princeton University - meaning warnings of privacy exposure have come to pass

Running low on power? Now people can track you with that. Photograph: Martin Abegglen/Flickr

https://www.theguardian.com/technology/2016/aug/02/battery-status-indicators-tracking-online

Cross-Device-Tracking

PC Magazin

Cross-Device-Tracking: So schützen Sie sich

21.1.2016 von Claudia Frickel

Nicht nur online verfolgen unseriöse Werbetreibende ihre Opfer Schritt für Schritt, auch mobil ist der A
mehr sicher vor ihnen – neuerdings auch geräteübergreifend – mit Ultraschall.

© putilov_denis - Fotolia.com

Durch Cross-Device-Tracking können Nutzer ohne ihr Wissen ausspioniert werden.

http://www.pc-magazin.de/ratgeber/cross-device-tracking-daten-schutz-tipps-3195539.html

Avira hat Silverpushs Tracking-Software als Malware eingestuft - weil der Anbieter "invasiv und sorglos in der Übertragung von Nutzerdaten" sei, sagt Alexander Vukcevic, Director Virus Labs. Die Praxis, Nutzer über die Grenzen eines Geräts hinweg zu identifizieren "ist an sich schon fragwürdig", kritisiert Vukcevic. Darüber hinaus werden die Daten mit Sehgewohnheiten und zum Beispiel der Handy-Nummer kombiniert.

© Screenshot WEKA / PC-Magazin

Achten Sie auf App-Berechtigungen. Die Silverpush-Tracker verwenden Audio aufnehmen.

Aber wie schützt man sich davor? Avira erkennt Silverpush-Apps und warnt davor. Ansonsten hilft es, am Fernseher und Computer den Ton abzuschalten, wenn Werbung läuft. Der Avira-Experte rät zudem, bei der Installation von Apps generell "aufmerksam auf die angeforderten Berechtigungen zu schauen". Und vorsichtig bei App Stores von Drittanbietern zu sein. Silverpush-Anwendungen hat die Sicherheitsfirma vor allem bei solchen Shops gefunden, vereinzelt allerdings auch in Googles Play Store.

Überblick

- Eingebaute Sicherheit
  - Gültiger Startpunkt?
- Datenschutz
  - Perspektivwechsel
  - Anforderungen aus Europa
- Eingebauter Datenschutz
  - Datenschutz „by Design“
  - Datenschutz „by Default“
- Fazit

Ab Mai 2018: Datenschutz-Grundverordnung

Datenschutz-Grundverordnung (DSGVO):

- Marktortprinzip
- Ziel: ein Datenschutzniveau für ganz Europa
- Eindämmen der Datenschutzrisiken
- Mehr eingebauter Datenschutz, mehr Information
- Verantwortung der datenverarbeitenden Stelle

- Erhebliche Sanktionen möglich
  - 2% des Vorjahresumsatzes / -10 Mio. €
  - 4% des Vorjahresumsatzes / -20 Mio. €

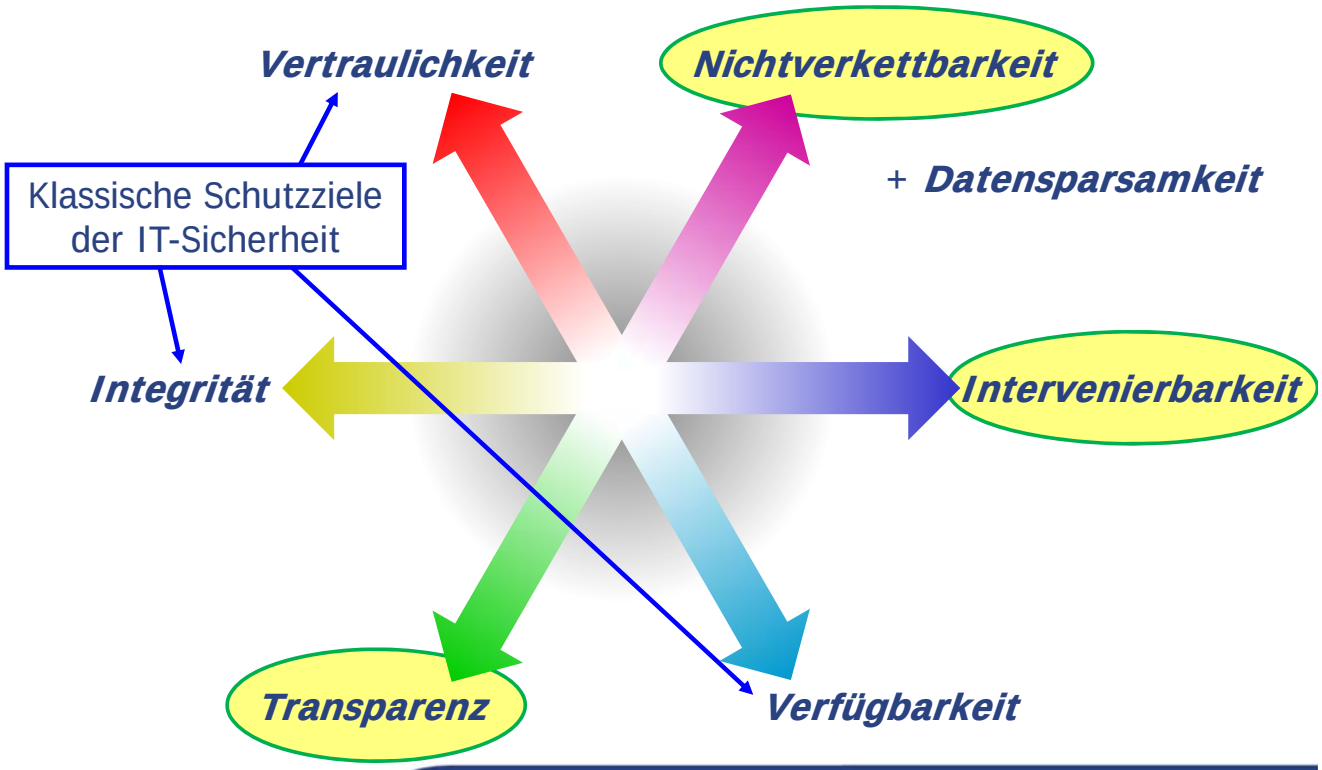
Datenschutz „by Design“ & „by Default“

- Kommt mit der EU-Datenschutz-Grundverordnung (Art. 25)
- Richtet sich primär an: Datenverarbeiter (auch im Auftrag) + (nur indirekt!) Hersteller von IT-Systemen
- Ziel: Gestaltung von Systemen + Diensten
  von Anfang an über den gesamten Lebenszyklus
  a) datensparsam
  b) mit möglichst datenschutzfreundlichen Voreinstellungen

Überblick

- Eingebaute Sicherheit
  - Gültiger Startpunkt?
- Datenschutz
  - Perspektivwechsel
  - Anforderungen aus Europa
- Eingebauter Datenschutz
  - Datenschutz „by Design“
  - Datenschutz „by Default“
- Fazit

Gewährleistungsziele



Nichtverkettbarkeit verbessern

Heutige eID-Lösungen

- Vollständige Daten

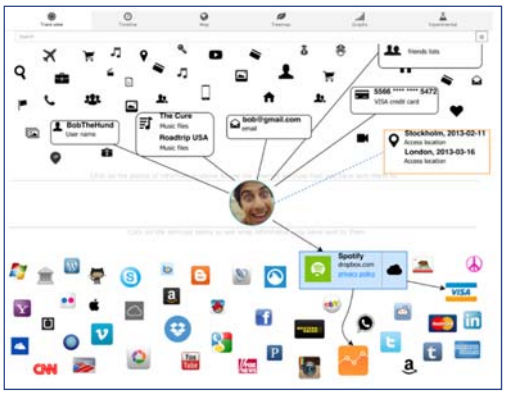
- Oft sind nicht alle Daten nötig

vs.

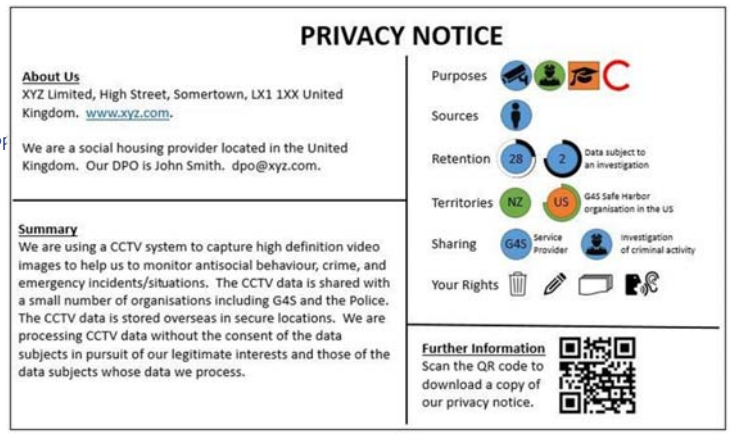
- Minimale Daten

Transparenz verbessern

- Klare und einfache Sprache
- „Layered Policies“
- Standardisierte Icons (Art. 12(7) GDPR)
- Maschinenlesbar



Source: Angulo et al. (2015): Usable Transparency with the Data Track: A Tool for Visualizing Data Disclosures, CHI EA '15 http://dx.doi.org/10.1145/2702613.2732701



Source: http://www.dataprotectionpeople.com/5918-2/ (January 2016)

Selbstdatenschutz reicht nicht aus

Intervenierbarkeit verbessern

- Eingreifen ist manchmal nötig:
  - Helpdesk / Beschwerdemanagement
  - Prozesse stoppen
  - Dienstleister wechseln

Source: Playing Futures: Applied Nomadology

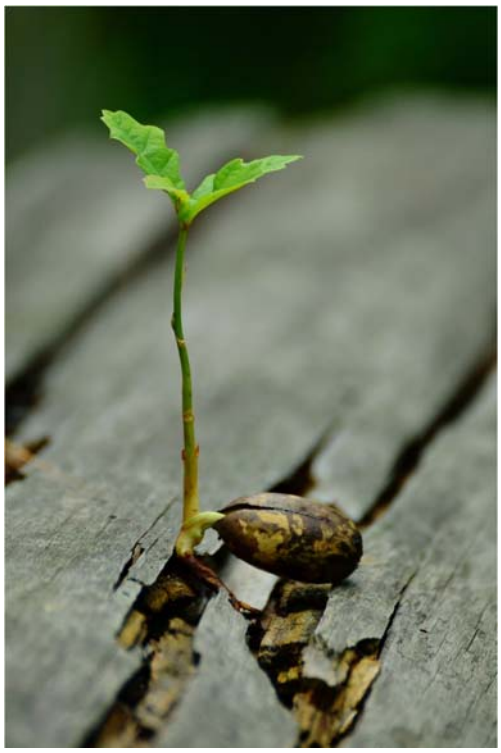
Source: Mark Hillary

- Verbraucher sollen eine echte Wahlmöglichkeiten erhalten ...
- ... auf der Basis von Datenschutz „by default“

Überblick

- Eingebaute Sicherheit
  - Gültiger Startpunkt?
- Datenschutz
  - Perspektivwechsel
  - Anforderungen aus Europa
- Eingebauter Datenschutz
  - Datenschutz „by Design“
  - Datenschutz „by Default“
- Fazit

Fazit



- „Eingebauter Datenschutz “ unbefriedigend:
  - Status Quo
  - europarechtlich
  - nationalgesetzlich
- Gestaltung ist mehr als Technik
- Wichtig: Lösungsraum kennen und erweitern
- Ins Datenschutz-Management integrieren

Vielen Dank für die Aufmerksamkeit!

Marit Hansen
https://www.datenschutzzentrum.de/

forum <privatheit> selbstbestimmtes leben in der digitalen welt

ULD Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein