IT-Sicherheit und Datenschutz by Design und by Default

Marit Hansen

Landesbeauftragte für Datenschutz
Schleswig-Holstein

Informatica Feminale, September 2021

forum <privatheit>
selbstbestimmtes_leben_in_der_digitalen_welt

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Überblick

- Implementierte IT-Sicherheit
  - Ausgangsbasis oder Wunsch?
- Datenschutz
  - Perspektivwechsel
  - Anforderungen aus Europa
- Implementierter Datenschutz
  - … by Design
  - … by Default
- Fazit

Old-School-Sicherheit

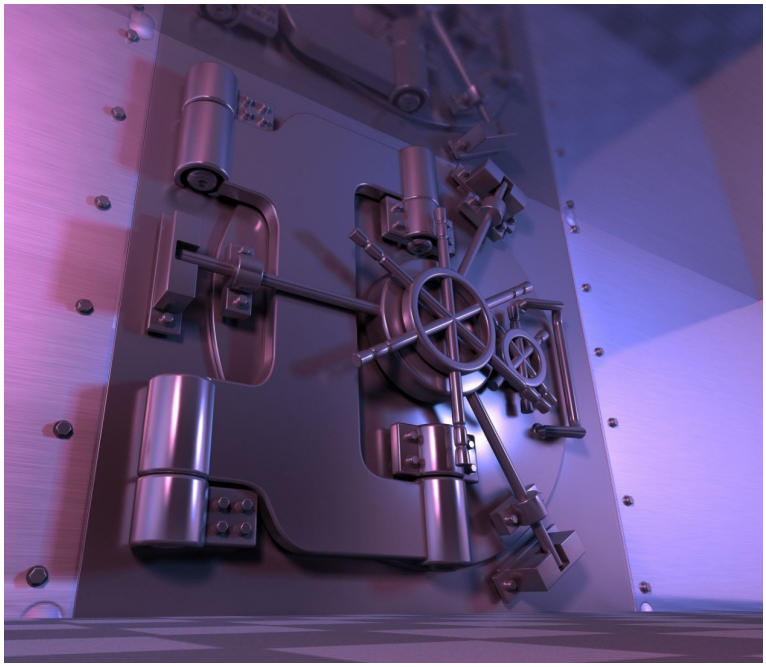
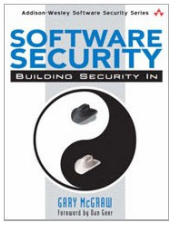


Bild: Das Wortgewand via Pixabay

„Building Security In" – Gary McGraw, 2004



Building Security In
Editor: Gary McGraw, gem@cigital.com

Software Security

Software security is the idea of engineering software so that it continues to function correctly under malicious attack. Most technologists acknowledge this undertaking's importance, but they need some help in understanding how to tackle it. This new department aims to provide that help by exploring software security best practices.

GARY McGRAW
Cigital

The software security field is a relatively new one. The first books and academic classes on the topic appeared in 2001, demonstrating how recently developers, architects, and computer scientists have started systematically studying how to build secure software. The field's recent appearance is one reason why best practices are neither widely adopted nor obvious.

A central and critical aspect of the computer security problem is a software problem. Software defects with security ramifications—including implementation bugs such as buffer overflows and design flaws such as inconsistent error handling—promise to be with us for years. All too often, malicious intruders can hack into systems by exploiting software defects.[1] Internet-enabled software applications present the most common security risk encountered today, with software's ever-expanding complexity and extensibility adding further fuel to the fire. By any measure, security holes in software are common, and the problem is growing: CERT Coordination Center identified 4,129 reported vulnerabilities in 2003 (a 70 percent increase over 2002, and an almost fourfold increase since 2001).[2,3]

Software security best practices leverage good software engineering practice and involve thinking about security early in the software life cycle, knowing and understanding common threats (including language-based flaws and pitfalls), designing for security, and subjecting all software artifacts to thorough objective risk analyses and testing. Let's look at how software security fits into the overall concept of operational security and examine some best practices for building security in.

...versus application security

Application security means many different things to many different people. In *IEEE Security & Privacy* magazine, it has come to mean the protection of software *after it's already built*. Although the notion of protecting software is an important one, it's just plain easier to protect something that is defect-free than something riddled with vulnerabilities.

Pondering the question, "What is the most effective way to protect software?" can help untangle software security and application security. On one hand, software security is about building secure software: designing software to be secure, making sure that software is secure, and educating software developers, architects, and users about how to build secure things. On the other hand, application security is about protecting software and the systems that software runs in a post facto way, after development is complete. Issues critical to this subfield include sandboxing code (as the Java virtual machine does), protecting against malicious code, obfuscating code, locking down executables, monitoring programs as they run (especially their input), enforcing the software use policy with technology, and dealing with extensible systems.

Application security follows naturally from a network-centric approach to security, by embracing standard approaches such as penetrate and patch[4] and input filtering (trying to block malicious input) and by providing value in a reactive way. Put succinctly, application security is based primarily on finding and fixing known security problems after they've been exploited in fielded systems. Software security—the process of designing, building, and testing software for security—identifies and expunges problems in the software itself. In this way, software security practitioners attempt to build software that can withstand attack proactively. Let me give you a specific example: although there is some real value in stopping buffer overflow attacks by observing HTTP traffic as it arrives over port 80, a superior approach is to fix the broken code and avoid the buffer overflow completely.

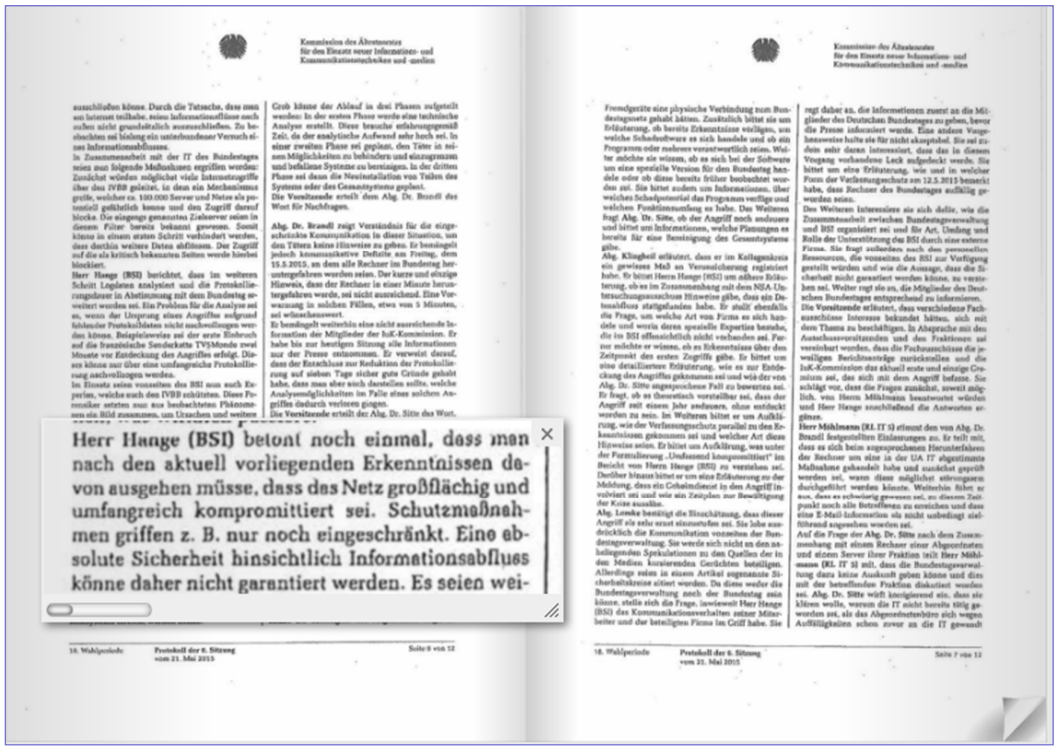
...as practiced by operations people

One reason that application security technologies such as firewalls have evolved the way they have is because

80 PUBLISHED BY THE IEEE COMPUTER SOCIETY ■ 1540-7993/04/$20.00 © 2004 IEEE ■ IEEE SECURITY & PRIVACY

> The software security field is a relatively new one. The first books and academic classes on the topic appeared in 2001, demonstrating how recently developers, architects, and computer scientists have started systematically studying how to build secure software. The field's recent appearance is one reason why best practices are neither widely adopted nor obvious.

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

„Collections" – Daten-Leaks über Jahre

Ergebnis Ihrer Anfrage bei HPI Identity Leak Checker

Achtung: Ihre E-Mail-Adresse [redacted]@gmx.net taucht in mindestens einer gestohlenen und unrechtmäßig veröffentlichten Identitätsdatenbank (so genannter Identity Leak) auf. Folgende sensible Informationen wurden im Zusammenhang mit Ihrer E-Mail-Adresse frei im Internet gefunden:

Betroffener Dienst	Datum	Verifiziert	Betroffene Nutzer	Passwort	Vor- und Zuname	Geburtsdatum	Anschrift	Telefonnummer	Kreditkarte	Bankkontodaten	Sozial-versicherungsnr.	IP-Adresse
adobe.com	Okt. 2013	✓	152.375.851	Betroffen	–	–	–	–	–	–	–	–

Betroffen: Diese Daten wurden in der zum angegebenen Zeitpunkt veröffentlichten Identitätsdatenbank der jeweiligen Quelle gefunden.
–: Es wurden keine solche Daten gefunden.

Bei einem *verifizierten* Leak (dargestellt mit ✓) handelt es sich um ein vom Dienstbetreiber bestätigtes Datenleck bzw. das Vorliegen eines Datenlecks beim Dienst ist hochwahrscheinlich. Bei einem *nicht verifizierten* Leak (fehlendes ✓) ist die Herkunft der Daten und deren Legitimität ungewiss. Solche unverifizierten Daten könnten z.B. aus Sammlungen von Passwörtern oder Kombinationen mehrerer älterer Leaks stammen oder auch generiert sein. Das Vorkommen in einem solchen Leak ist demnach kein sicherer Indikator für ein Datenleck.

Bitte beachten Sie, dass wir aus Sicherheitsgründen keine Auskunft über die konkret betroffenen Daten in den aufgeführten Kategorien geben können.

Wir empfehlen die folgende Reaktion:

- **Passwort:** Ändern Sie Ihr Passwort für sämtliche Accounts mit der E-Mail-Adresse [redacted]@gmx.net, bei denen das Passwort älter oder gleich dem angegebenen Datum ist.
Generell gilt, dass je mehr Identitätsdaten über Sie veröffentlicht werden, desto leichter kann Ihre Identität missbraucht werden.
Es ist auf jeden Fall ratsam eine Anzeige beim Diebstahl von Informationen wie Bankdaten, Kreditkartendaten und Sozialversicherungsnummern zu erstatten.

Haftungsausschluss: *Wir übernehmen keine Haftung für die Vollständigkeit und Korrektheit der bereitgestellten Informationen unseres Dienstes. Die Daten werden automatisch gesammelt und entsprechend für Abfragen aufbereitet. Wir werten für unseren Dienst nur öffentlich im Internet verfügbare Quellen aus und können keine Vollständigkeit garantieren. Wir bereiten nur den Teil der im Internet veröffentlichten Identitätsdatenbanken auf und haben keinen Zugriff auf "analoge Daten", also z.B. Daten, die physikalisch von Betrügern ausgetauscht werden oder Daten die von Dokumenten (Reisepass, Ausweis, Rechnungen, persönliche Briefe) abgeschrieben wurden.*

Ihr HPI Identity Leak Checker Team
Webseite

Breaches you were pwned in

A "breach" is an incident where data has been unintentionally exposed to the public. Using the 1Password password manager helps you ensure all your passwords are strong and unique such that a breach of one service doesn't put your other services at risk.

Adobe: In October 2013, 153 million Adobe accounts were breached with each containing an internal ID, username, email, *encrypted* password and a password hint in plain text. The password cryptography was poorly done and many were quickly resolved back to plain text. The unencrypted hints also disclosed much about the passwords adding further to the risk that hundreds of millions of Adobe customers already faced.

Compromised data: Email addresses, Password hints, Passwords, Usernames

340	6,474,028,664	87,869	96,570,719
pwned websites	pwned accounts	pastes	paste accounts

Von [redacted].eu> ☆
Betreff **Ignore my former mails today** 24.01.2019, 19:46

I was hacked.
[redacted]

Sicherheit durch Ausbauen

THE VERGE

US & WORLD

TRENDING NOW
This is VAIO's Windows phone

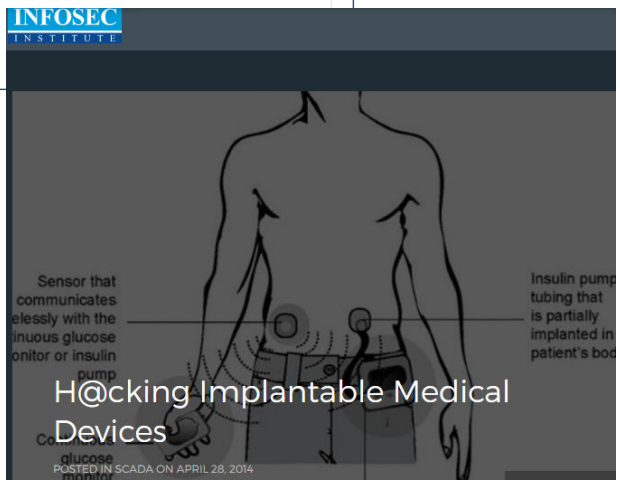
39 NEW ARTICLES

63 COMMENTS

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/

The Register®
Biting the hand that feeds IT

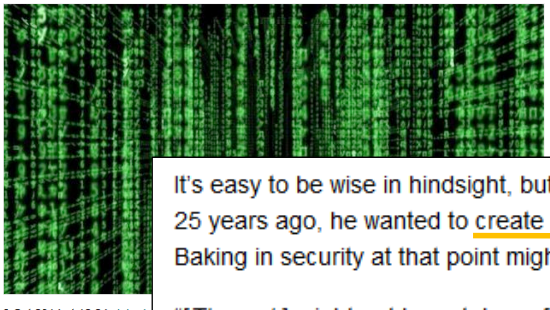
DATA CENTRE SOFTWARE NETWORKS SECURITY INFRASTRUCTURE DEVOPS BUSINESS HARDWARE SCIENCE BOOTNOTES FORUMS

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 contra 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."

WWW mit oder ohne?

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" – darf Sicherheit 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)
- Pegasus-Spyware: auch in der EU!

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

Pegasus (Spyware)

Pegasus ist eine Spyware des israelischen Unternehmens NSO Group zum Ausspähen von iOS- und Android-Geräten.[1] Die Software kann unbemerkt auf sämtliche Daten zugreifen und sie über das Internet versenden.[2][3] Pegasus wurde im August 2016 durch die Sicherheitsfirma Lookout und durch Citizen Lab (Universität Toronto) entdeckt und analysiert. Sie gilt als professionell und wird in erster Linie an Staaten vermarktet.

Journalisten, Menschenrechtler und Politiker wurden mit Hilfe von Pegasus ausgespäht.

https://de.wikipedia.org/wiki/Pegasus_(Spyware)

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


Foto: Willh26 (Wikipedia)

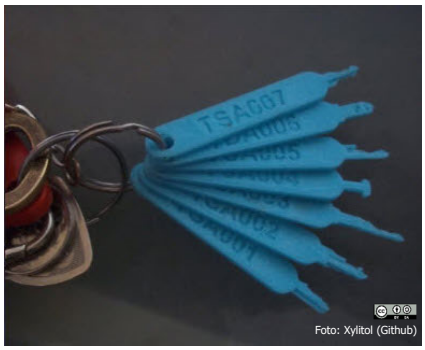


Foto: Xylitol (Github)

https://en.wikipedia.org/wiki/File:Wafer_Lock_Try-Out_Keys.jpg
https://en.wikipedia.org/wiki/File:Lol_key_escrow.jpg
License: CC-BY-SA - https://creativecommons.org/licenses/by-sa/4.0/

THE WEEK

TSAAAARG

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

September 11, 2015

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/rotJPJqjTg

— 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

Transportverschlüsselung im Fokus:
Streit um TLS 1.3 / „Enterprise Transport Security" (ETS/eTLS)

BLEEPINGCOMPUTER

NEWS ▾ DOWNLOADS ▾ VIRUS REMOVAL GUIDES ▾ TU

IETF avoids efforts to insert back

All in all, TLS 1.3 is a serious boost to Internet secu to crack, at least with today's resources.

IETF members voted the protocol unanimously, ev asked for the introduction of a backdoor in the prot could decrypt TLS 1.3 traffic inside internal networ

The proposal was laughed off by experts, who point effectively make TLS 1.3 useless in the first place.

heise Security http://www.heise.de/-4245220

IETF an ETSI: Finger weg von TLS

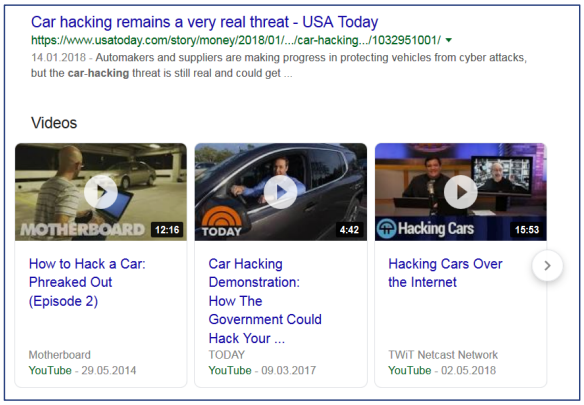
07.12.2018 12:53 Uhr
Monika Ermert

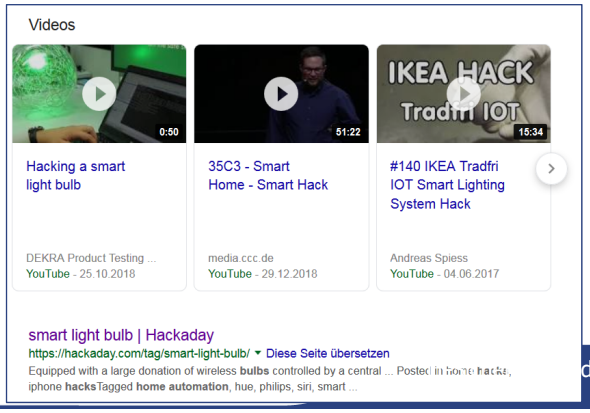

(Bild: JanBaby)

Die IETF moniert, dass TLS 1.3 mit dem neuen ETSI-Überwachungsstandard in einen Topf geworfen wird. Es gibt bereits ein Abwehrprotokoll gegen eTLS.

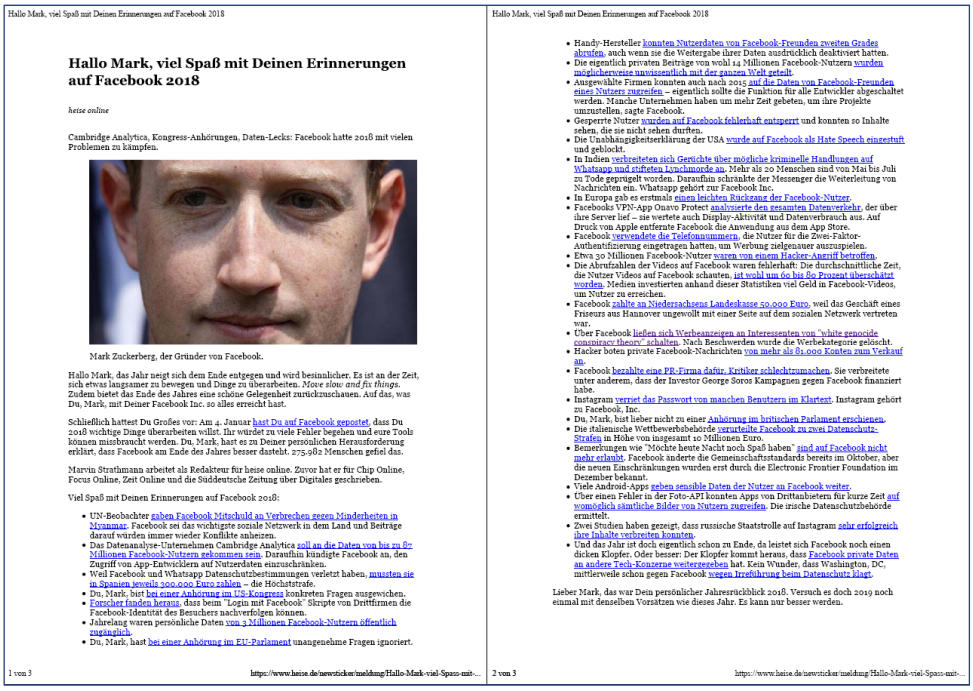
Cimpanu: IETF Approves TLS 1.3 as Internet Standard, Bleeping Computer, 25.03.2018
https://www.bleepingcomputer.com/news/security/ietf-approves-tls-13-as-internet-standard/

Lessons Learned – gut aufgestellt für die Zukunft?





Datenpanne: Regel oder Ausnahme?



Hallo Mark, viel Spaß mit Deinen Erinnerungen auf Facebook 2018

Hallo Mark, viel Spaß mit Deinen Erinnerungen auf Facebook 2018

heise online

Cambridge Analytica, Kongress-Anhörungen, Daten-Lecks: Facebook hatte 2018 mit vielen Problemen zu kämpfen.

Mark Zuckerberg, der Gründer von Facebook.

Hallo Mark, das Jahr neigt sich dem Ende entgegen und wird besinnlicher. Es ist an der Zeit, sich etwas langsamer zu bewegen und Dinge zu überarbeiten. *Move slow and fix things.* Zudem bietet das Ende des Jahres eine schöne Gelegenheit zurückzuschauen. Auf das, was Du, Mark, mit Deiner Facebook Inc. so alles erreicht hast.

Schließlich hattest Du Großes vor: Am 4. Januar hast Du auf Facebook gepostet, dass Du 2018 wichtige Dinge überarbeiten willst. Ihr würdet zu viele Fehler begehen und eure Tools könnten missbraucht werden. Du, Mark, hast es zu Deiner persönlichen Herausforderung erklärt, dass Facebook am Ende des Jahres besser dasteht. 275.982 Menschen gefiel das.

Marvin Strathmann arbeitet als Redakteur für heise online. Zuvor hat er für Chip Online, Focus Online, Zeit Online und die Süddeutsche Zeitung über Digitales geschrieben.

Viel Spaß mit Deinen Erinnerungen auf Facebook 2018:

- UN-Beobachter geben Facebook Mitschuld an Verbrechen gegen Minderheiten in Myanmar. Facebook sei das wichtigste soziale Netzwerk in dem Land und Beiträge darauf würden immer wieder Konflikte anheizen.
- Das Datenanalyse-Unternehmen Cambridge Analytica soll an die Daten von bis zu 87 Millionen Facebook-Nutzern gekommen sein. Daraufhin kündigte Facebook an, den Zugriff von App-Entwicklern auf Nutzerdaten einzuschränken.
- Weil Facebook und Whatsapp Datenschutzbestimmungen verletzt haben, mussten sie in Spanien jeweils 300.000 Euro zahlen – die Höchststrafe.
- Du, Mark, bist bei einer Anhörung im US-Kongress konkreten Fragen ausgewichen.
- Forscher fanden heraus, dass beim "Login mit Facebook" Skripte von Drittfirmen die Facebook-Identität des Besuchers nachverfolgen können.
- Jahrelang waren persönliche Daten von 3 Millionen Facebook-Nutzern öffentlich zugänglich.
- Du, Mark, hast bei einer Anhörung im EU-Parlament unangenehme Fragen ignoriert.

1 von 3 https://www.heise.de/newsticker/meldung/Hallo-Mark-viel-Spass-mit-...

Hallo Mark, viel Spaß mit Deinen Erinnerungen auf Facebook 2018

- Handy-Hersteller konnten Nutzerdaten von Facebook-Freunden zweiten Grades abrufen, auch wenn sie die Weitergabe ihrer Daten ausdrücklich deaktiviert hatten.
- Die eigentlich privaten Beiträge von wohl 14 Millionen Facebook-Nutzern wurden möglicherweise unwissentlich mit der ganzen Welt geteilt.
- Ausgewählte Firmen konnten auch nach 2015 auf die Daten von Facebook-Freunden eines Nutzers zugreifen – eigentlich sollte die Funktion für alle Entwickler abgeschaltet werden. Manche Unternehmen haben um mehr Zeit gebeten, um ihre Projekte umzustellen, sagte Facebook.
- Gesperrte Nutzer wurden auf Facebook fehlerhaft entsperrt und konnten so Inhalte sehen, die sie nicht sehen durften.
- Die Unabhängigkeitserklärung der USA wurde auf Facebook als Hate Speech eingestuft und geblockt.
- In Indien verbreiteten sich Gerüchte über mögliche kriminelle Handlungen auf Whatsapp und stifteten Lynchmorde an. Mehr als 20 Menschen sind von Mai bis Juli zu Tode gejagt worden. Daraufhin schränkte der Messenger die Weiterleitung von Nachrichten ein. Whatsapp gehört zur Facebook Inc.
- In Europa gab es erstmals einen leichten Rückgang der Facebook-Nutzer.
- Facebooks VPN-App Onavo Protect analysierte den gesamten Datenverkehr, der über ihre Server lief – sie wertete auch Display-Aktivität und Datenverbrauch aus. Auf Druck von Apple entfernte Facebook die Anwendung aus dem App Store.
- Facebook verwendete die Telefonnummern, die Nutzer für die Zwei-Faktor-Authentifizierung eingetragen hatten, um Werbung zielgenauer auszuspielen.
- Etwa 30 Millionen Facebook-Nutzer waren von einem Hacker-Angriff betroffen.
- Die Abrufzahlen der Videos auf Facebook waren fehlerhaft: Die durchschnittliche Zeit, die Nutzer Videos auf Facebook schauten, ist wohl um 60 bis 80 Prozent überschätzt worden. Medien investierten anhand dieser Statistiken viel Geld in Facebook-Videos, um Nutzer zu erreichen.
- Facebook zahlte an Niedersachsens Landeskasse 50.000 Euro, weil das Geschäft eines Friseurs aus Hannover ungewollt mit einer Seite auf dem sozialen Netzwerk vertreten war.
- Über Facebook ließen sich Werbeanzeigen an Interessenten von "white genocide conspiracy theory" schalten. Nach Beschwerden wurde die Werbekategorie gelöscht.
- Hacker boten private Facebook-Nachrichten von mehr als 81.000 Konten zum Verkauf an.
- Facebook bezahlte eine PR-Firma dafür, Kritiker schlechtzumachen. Sie verbreitete unter anderem, dass der Investor George Soros Kampagnen gegen Facebook finanziert habe.
- Instagram verriet das Passwort von manchen Benutzern im Klartext. Instagram gehört zu Facebook, Inc.
- Du, Mark, bist lieber nicht zu einer Anhörung im britischen Parlament erschienen.
- Die italienische Wettbewerbsbehörde verurteilte Facebook zu zwei Datenschutz-Strafen in Höhe von insgesamt 10 Millionen Euro.
- Bemerkungen wie "Möchte heute Nacht noch Spaß haben" sind auf Facebook nicht mehr erlaubt. Facebook änderte die Gemeinschaftsstandards bereits im Oktober, aber die neuen Einschränkungen wurden erst durch die Electronic Frontier Foundation im Dezember bekannt.
- Viele Android-Apps geben sensible Daten der Nutzer an Facebook weiter.
- Über einen Fehler in der Foto-API konnten Apps von Drittanbietern für kurze Zeit auf womöglich sämtliche Bilder von Nutzern zugreifen. Die irische Datenschutzbehörde ermittelt.
- Zwei Studien haben gezeigt, dass russische Staatstrolle auf Instagram sehr erfolgreich ihre Inhalte verbreiten konnten.
- Und das Jahr ist doch eigentlich schon zu Ende, da leistet sich Facebook noch einen dicken Klopfer. Oder besser: Der Klopfer kommt heraus, dass Facebook private Daten an andere Tech-Konzerne weitergegeben hat. Kein Wunder, dass Washington, DC, mittlerweile schon gegen Facebook wegen Irreführung beim Datenschutz klagt.

Lieber Mark, das war Dein persönlicher Jahresrückblick 2018. Versuch es doch 2019 noch einmal mit denselben Vorsätzen wie dieses Jahr. Es kann nur besser werden.

2 von 3 https://www.heise.de/newsticker/meldung/Hallo-Mark-viel-Spass-mit-...

Strathmann, Heise, 25.12.2018, https://www.heise.de/newsticker/meldung/Hallo-Mark-viel-Spass-mit-Deinen-Erinnerungen-auf-Facebook-2018-4254681.html

Überblick

- Implementierte IT-Sicherheit
  - Ausgangsbasis oder Wunsch?
- Datenschutz
  - Perspektivwechsel
  - Anforderungen aus Europa
- Implementierter Datenschutz
  - … by Design
  - … by Default
- Fazit

Beim Datenschutz geht es um ~~Daten~~

Source: Ashtyn Renee

Menschen mit ihren Rechten

Prüffragen bei der Gestaltung:

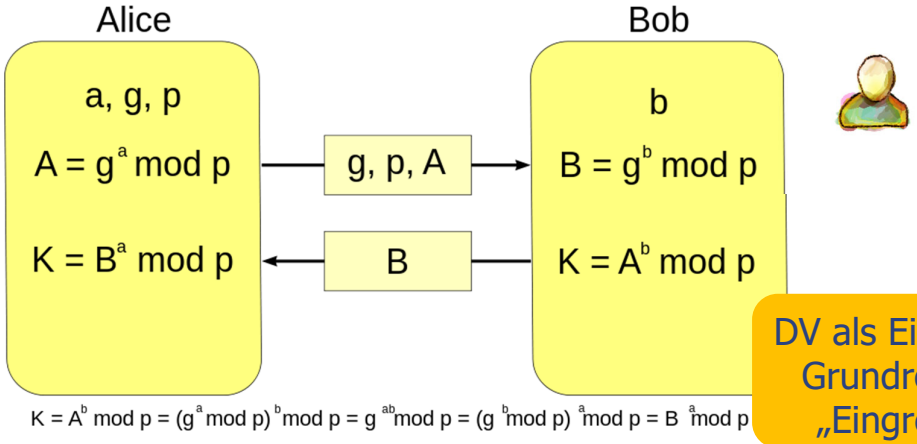
- Auswirkungen auf Menschen?
- Auswirkungen auf die Gesellschaft?

Datenschutz nötig:

Machtgefälle zwischen Individuen und Organisationen

Bild: beludise via Pixabay

Perspektive: Alice & Bob



$K = A^b \bmod p = (g^a \bmod p)^b \bmod p = g^{ab} \bmod p = (g^b \bmod p)^a \bmod p = B^a \bmod p$

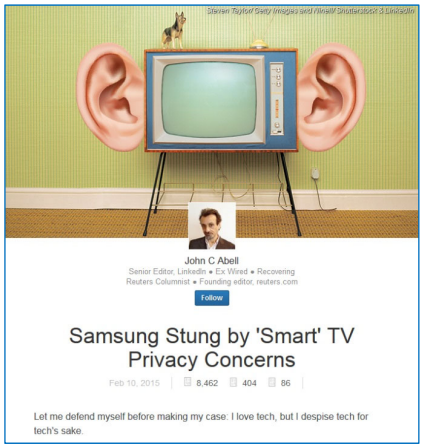
DV als Eingriff in Grundrechte: „Eingreifer"

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

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

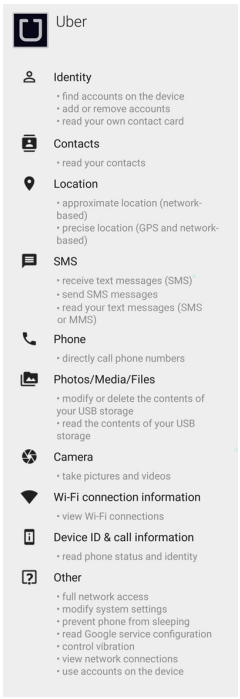
Heutige Situation

- Eingebauter Datenschutz?
- Nein, eingebaute Verkettbarkeit und Identifizierbarkeit



https://www.linkedin.com/pulse/when-good-tech-goes-bad-smart-tv-edition-john-c-abell

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



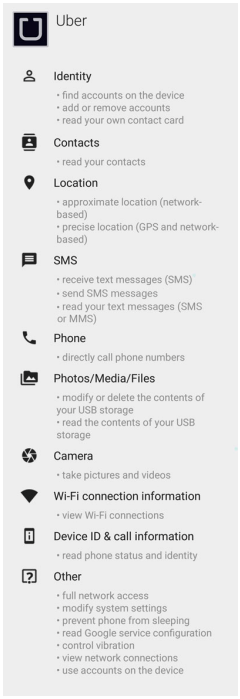
ULD www.datenschutzzentrum.de

Heutige Situation

- Eingebauter Datenschutz?
- „Take it or leave it", z. B. bei Apps

Kaum Wahl-möglichkeiten

https://ethicsalarms.files.wordpress.com/2015/12/take-it-or-leave-it1.jpg



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

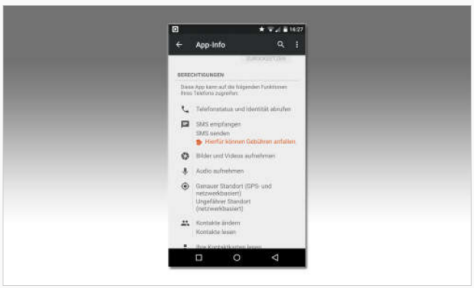
21.1.2016 von Claudia Frickel

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.

Heutige Situation

- Eingebauter Datenschutz?
- Die dominierenden Player bestimmen die Regeln für alle

Wem gehört die Webseite?

	BILD.DE	SPON	SZ	ZEIT
Requests	2339	2514	1886	1130
Unique Hosts	195	184	172	122
3rd Party Hosts	182	172	160	113
Own Hosts (*)	13	12	12	9

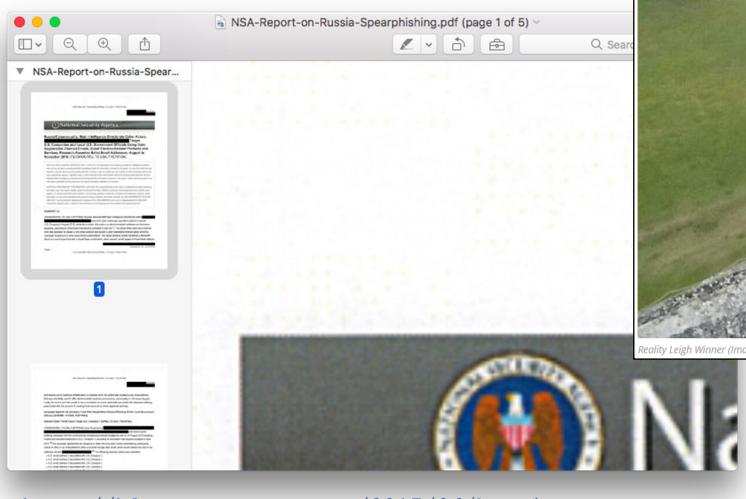
(*) basiert auf augenscheinlich zum Verlag gehörenden Domains/Subdomains

re:publica 2016 – Thorsten Schröder & Frank Rieger: Ad-Wars

Verantwortungs-diffusion

Heutige Situation

Eingebauter Datenschutz?
Im Gegenteil:
eingebaute Verkettbarkeit
und Identifizierbarkeit



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

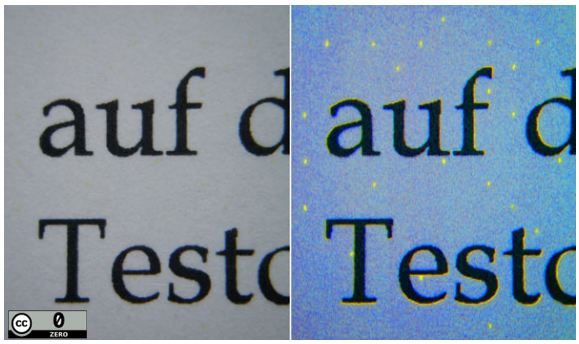
The Washington Times

Printer watermark likely helped identify Reality Winner as suspected NSA leaker: Report

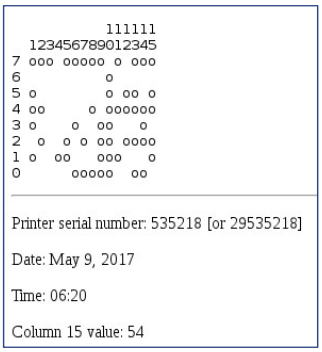
Reality Leigh Winner (Image: Facebook) more >

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:
versteckter Wasserzeichen



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

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

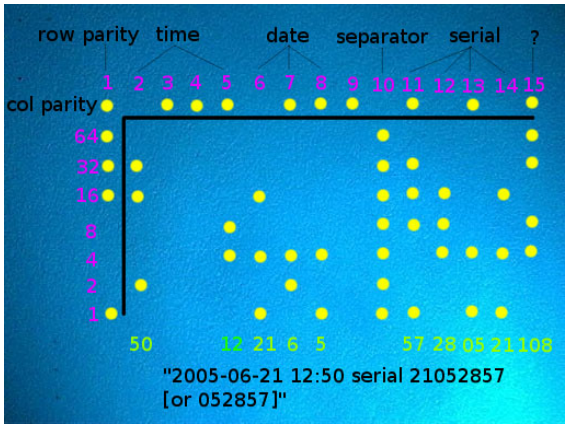


Bild: Electronic Frontier Foundation (EFF)

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

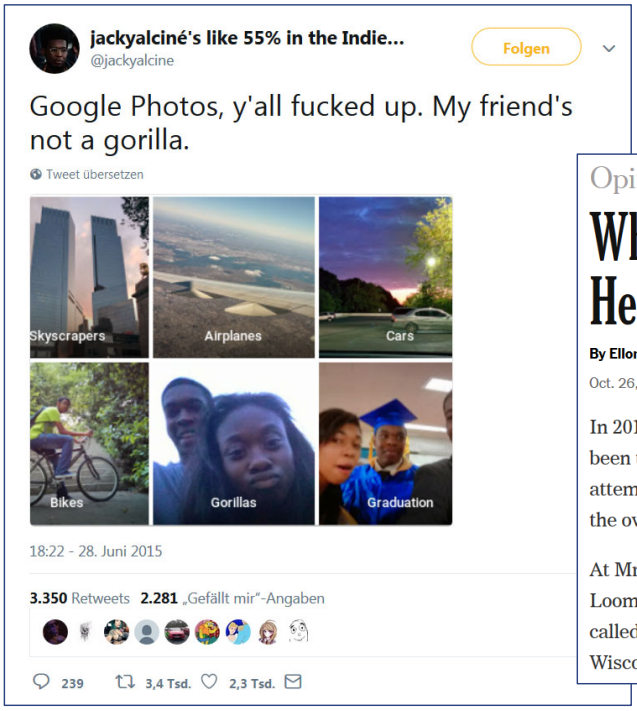
How Companies Learn Your Secrets

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

Training für selbstlernende Algorithmen?



https://twitter.com/jackyalcine/status/615329515909156865

https://www.nytimes.com/2017/10/26/opinion/algorithm-compas-sentencing-bias.html

Opinion

The New York Times

When an Algorithm Helps Send You to Prison

By Ellora Thadaney Israni

Oct. 26, 2017

In 2013, police officers in Wisconsin arrested a man driving a car that had been used in a recent shooting. The man, Eric Loomis, pleaded guilty to attempting to flee an officer, and no contest to operating a vehicle without the owner's consent. Neither of his crimes mandates prison time.

At Mr. Loomis's sentencing, the judge cited, among other factors, Mr. Loomis's high risk of recidivism as predicted by a computer program called COMPAS, a risk assessment algorithm used by the state of Wisconsin. The judge denied probation and prescribed an 11-year

Welche Regeln? z.B. bei AI-Bots

COMPUTERWORLD FROM IDG

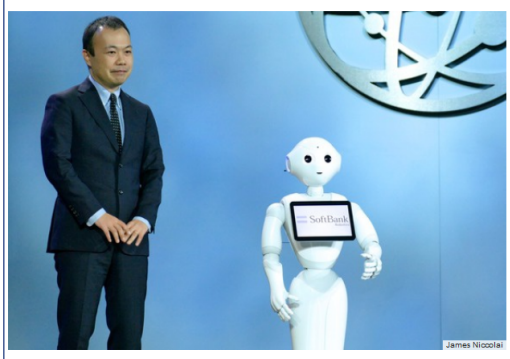
NEWS

What will it take to make A.I. sound more human?

'It's a matter of being personalized,' says CMU professor Alan Black

By Katherine Noyes

Senior U.S. Correspondent, IDG News Service | APR 1, 2016 5:23 PM PT



Conversation fillers such as "hmm" and "uh-huh" may seem like insignificant parts of human conversation, but they're critical to improving communication between humans and artificial intelligence (A.I.).

https://www.computerworld.com/article/3051174/big-data/what-will-it-take-to-make-ai-sound-more-human.html

https://twitter.com/traviskorte/status/993954759932612608

Bild: athree23 via Pixabay

EU-Datenschutzreform: Vereinheitlichung und Modernisierung

- Idee: Eine für alle
  und
  alle für eine
- Ziel:
  echte Harmonisierung
- Rechtssicherung durch Gleichklang der Aufsicht
- Nicht ganz einheitlich:
  70 Spezifikationsklauseln für die Mitgliedstaaten

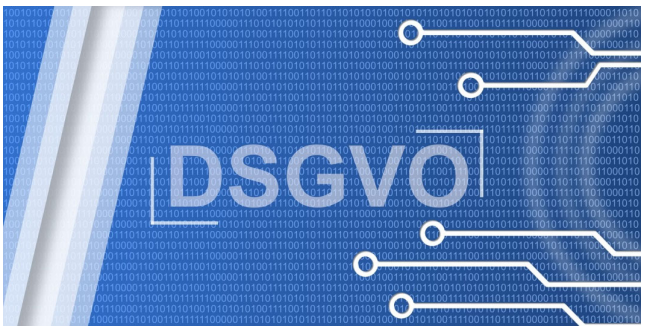


Bild: skylarvision via Pixabay

- Neu:
  - Risiko für Rechte und Freiheiten
  - Datenschutz „by Design" & „by Default"

Überblick

- Implementierte IT-Sicherheit
  - Ausgangsbasis oder Wunsch?
- Datenschutz
  - Perspektivwechsel
  - Anforderungen aus Europa
- Implementierter Datenschutz
  - … by Design
  - … by Default
- Fazit

Vorbemerkung: Wichtigkeit von „by Design"

Erwägungsgrund 4

„The processing of personal data should be designed to serve mankind. […]"

http://www.simulee.com/wp-content/uploads/2015/05/3.jpg

STRUKTUR 1

Grundsätze in der DSGVO

Art. 5 DSGVO
– immer zu erfüllen bei personenbezogenen Daten

Oberthema: Fairness

Abs. 1:

a) Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz
b) Zweckbindung
c) Datenminimierung
d) Richtigkeit
e) Speicherbegrenzung
f) Integrität und Vertraulichkeit (Datensicherheit)

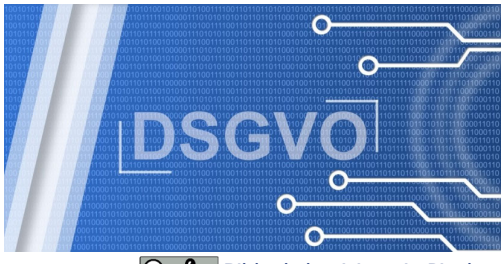


Bild: skylarvision via Pixabay

Abs. 2: Rechenschaftspflicht

Datenschutz „by Design" & „by Default"

- Anforderung in Art. 25 der EU-Datenschutz-Grundverordnung

- Richtet sich primär an: Datenverarbeiter („Verantwortliche")
- Indirekt (!): Hersteller von IT-Systemen

- Ziel: Gestaltung von Systemen + Diensten
  von Anfang an über den gesamten Lebenszyklus
  a) datensparsam
  b) mit möglichst datenschutzfreundlichen Voreinstellungen

Datenschutz durch Technikgestaltung

Artikel 25 Datenschutz durch Technikgestaltung […]

(1) Unter Berücksichtigung
des Stands der Technik,
der Implementierungskosten und
der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung
sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere
der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen

Viele möglicherweise begrenzende Bedingungen ↑↓

trifft der Verantwortliche sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen – wie z. B. Pseudonymisierung – trifft, die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen.

Datenschutz durch Technikgestaltung

Artikel 25 Datenschutz durch Technikgestaltung […]

(1) Unter Berücksichtigung
des Stands der Technik,
der Implementierungskosten und
der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung
sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen

Was ist zu tun? „Eingebauter Datenschutz", u.a. Art. 5 DSGVO betont, aber insgesamt DSGVO

trifft der Verantwortliche sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen – wie z. B. Pseudonymisierung – trifft, die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen.

Datenschutz durch datenschutzfreundliche Voreinstellungen

Artikel 25 […] durch datenschutzfreundliche Voreinstellungen

bedingungslos

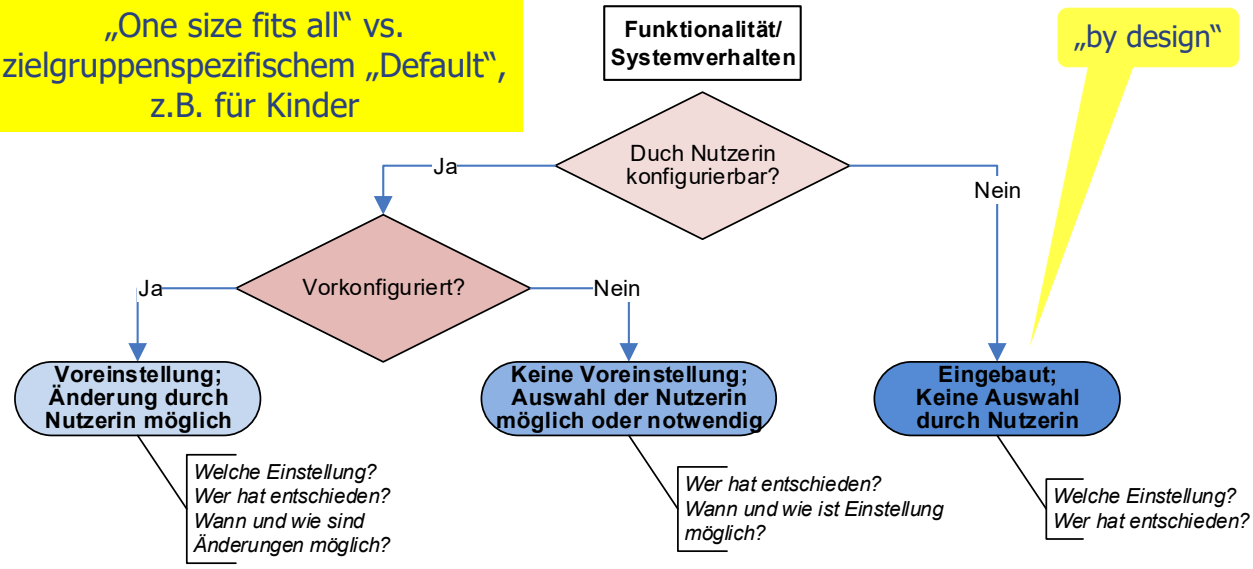
(2) Der Verantwortliche trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch Voreinstellung nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit.

Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.

Nicht nur minimaler Datenkatalog; auch generelle Risikominimierung

„... by Default": Drei Fälle der (Vor-)Konfiguration

„One size fits all" vs. zielgruppenspezifischem „Default", z.B. für Kinder



Bsp.: anonyme Nutzung, kein Tracking

Bsp.: Auswahl des Bezahl-Systems

Bsp.: verschlüsselte Kommunikation

s.a.: Marit Hansen: Data Protection by Default in Identity-Related Applications. Proc. IDMAN 2013, IFIP AICT 396, S. 4-17.

Datenschutz „by Design" & „by Default" gemäß Erwägungsgrund 78 DSGVO

- Nachweis durch interne Strategien & t+o Maßnahmen, u.a.
  - Datenminimierung
  - Schnellstmögliche Pseudonymisierung
  - Transparenz in Bezug auf Funktionen+Verarbeitung
  - Ermöglichung der Überwachung der Verarbeitung durch die betroffenen Personen
  - Ermöglichung für Sicherheitsfunktionen „on top" durch Verantwortlichen
- Ermutigung für Hersteller
- Berücksichtigung in öffentlichen Ausschreibungen

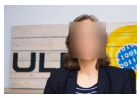
Aggregation
Anonymisierung
Attributbasierte Berechtigungszertifikate
Dashboard
Auskunftsportal
Elektronischer Datenbrief
Machine-readable Policies
Icons
Dezentralisierung
Zweck-Kennzeichnung
Kein Freitext
Automatisches Löschen
Sticky Policies
Schnittstellen zu Selbstdatenschutz-Tools

Mini-Checkliste

- ☐ Zwecke
- ☐ Mittel
- ☐ Risiko
- ☐ Garantien / Maßnahmen
- ☐ Rechtsgrundlage
  - ☐ Gesetz
  - ☐ Einwilligung
  - ☐ Vertrag
  - ☐ Berechtigte Interessen [nicht öD]
- ☐ Maßnahmen für
  - ☐ Datenminimierung
  - ☐ Datensicherheit
  - ☐ Transparenz
  - ☐ Betroffenenrechte …
- ☐ Kontrollen

Beispiel: Videoüberwachung nach der DSGVO

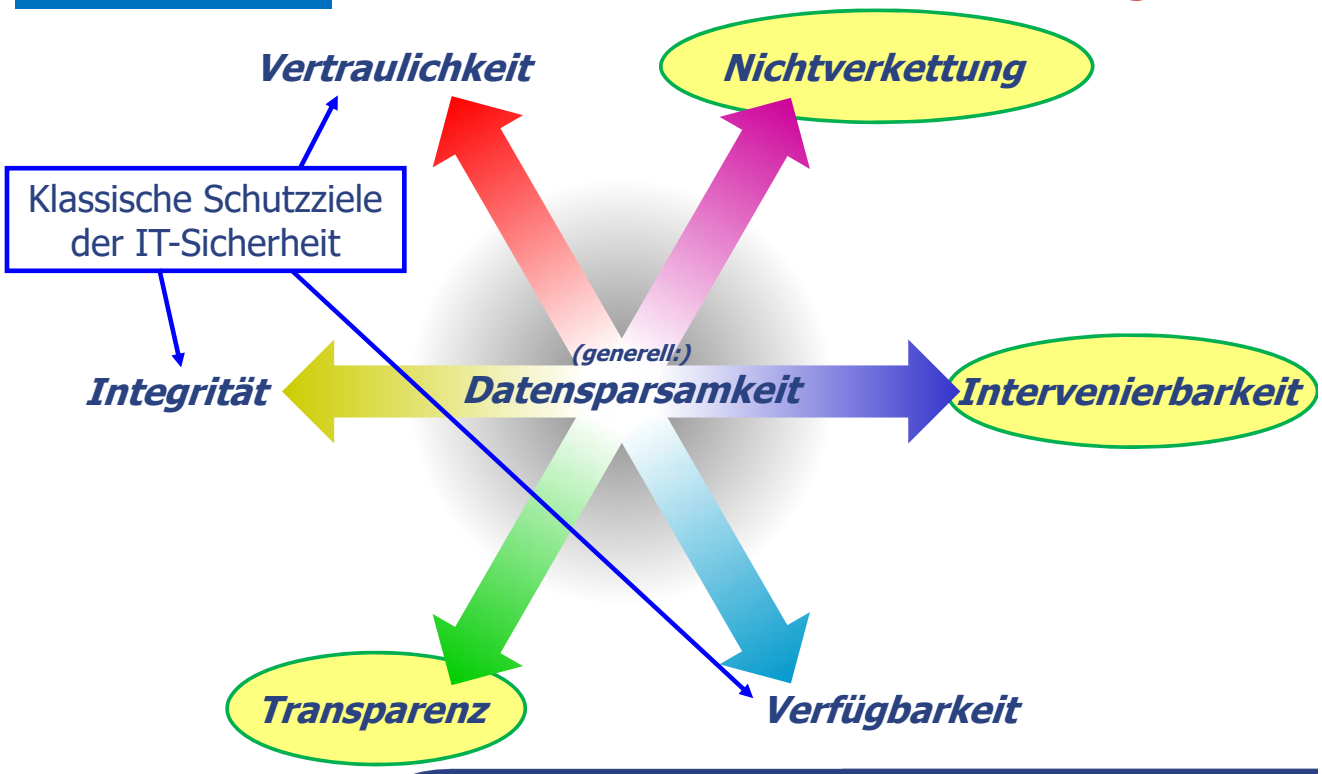
Sichere und datenschutzfreundliche Gestaltung



1. Rechtsgrundlage
2. Auswahl, Installation und Betrieb von Videoüberwachungs-systemen: sichere (Art. 32 DSGVO) und datenschutzfreundliche (Art. 25 DSGVO) Gestaltung
   - Inwieweit kann eine Videoüberwachung zeitlich eingeschränkt werden und welche Bereiche der Überwachung können ausgeblendet oder verpixelt werden?
   - „Verlängertes Auge" oder Aufzeichnung (wie? wie lange?)?
   - „Eingebauter Datenschutz" schon bei der Beschaffung: Nicht benötigte Funktionalität (z. B. freie Schwenkbarkeit, umfassende Überwachung per Dome-Kamera, Zoomfähigkeit, Funkübertragung, Internetveröffentlichung, Audioaufnahme) sollte von der beschafften Technik nicht unterstützt oder zumindest bei der Inbetriebnahme deaktiviert werden.

STRUKTUR 2

Gewährleistungsziele



Wie? Gewährleistungsziele implementieren

Nichtverkettung

Trennung von Domänen, Gewaltenteilung, Zweckbindung, Anonymisierung

Bild: ivanacoi via Pixabay

Transparenz

Ziel: Nachvollziehbarkeit & Überprüfbarkeit

Bild: geralt via Pixabay

z.B. (situationsgerecht): keine automatisierten Entscheidungen, Korrektur, Widerspruch, Rechtsschutz, Rückabwicklung, Haftung …

Bild: geralt via Pixabay

Ziel: Risikobeherrschung –
Risiko für die Rechte und Freiheiten natürlicher Personen
→ (Datenschutz-)Folgenabschätzung

Intervenierbarkeit

Risikobegriff der DSGVO

- Ein Risiko im Sinne der DSGVO ist das Bestehen der Möglichkeit des Eintritts eines Ereignisses, das selbst einen Schaden (einschließlich ungerechtfertigter Beeinträchtigung von Rechten und Freiheiten natürlicher Personen) darstellt oder zu einem weiteren Schaden für eine oder mehrere natürliche Personen führen kann.

- Zwei Dimensionen des Risikos:
  1. die Schwere des Schadens
  2. die Wahrscheinlichkeit, dass das Ereignis und etwaige Folgeschäden eintreten

- Kategorien:
  - (Nahezu) kein Risiko Art. 33 DSGVO
  - Risiko Art. 33 DSGVO
  - Hohes Risiko
    Artt. 34, 35, 36 DSGVO


DSK
Kurzpapier Nr. 18
Risiko für die Rechte und Freiheiten natürlicher Personen

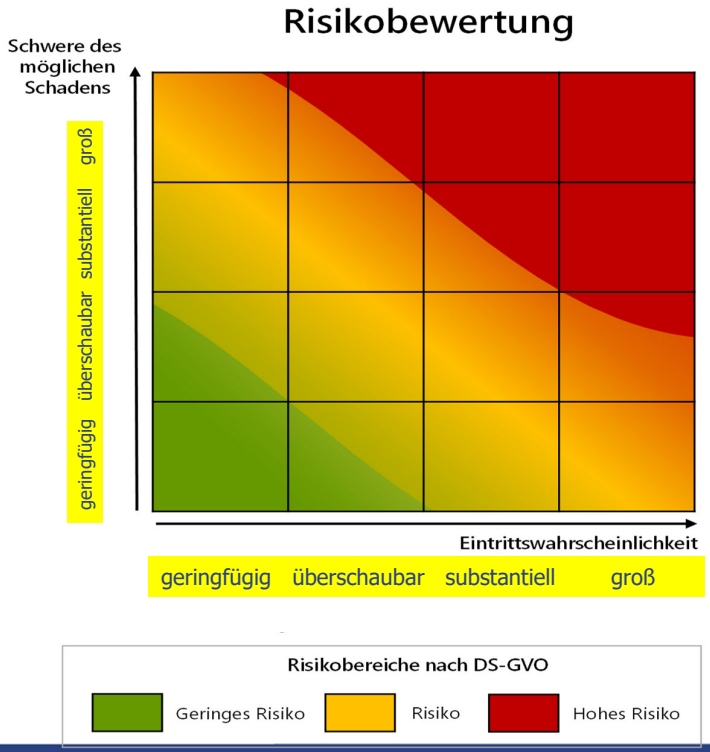
https://www.datenschutzzentrum.de/artikel/1225-.html

Risikobegriff der DSGVO

- Risiko = Schwere möglicher Schäden x Eintrittswahrscheinlichkeit
- Lässt sich nicht völlig quantifizieren
- Kann aber objektiv bestimmt werden

- Risiken für Rechte müssen mit technischen und organisatorischen Maßnahmen eingedämmt werden

→ Artt. 24, 25, 32, 35 DSGVO



Inkl. Beeinträchtigungen der Rechte und Freiheiten ErwGr. 94

Startpunkt Risiko

- Welche Schäden*) können für die natürlichen Personen auf der Grundlage der zu verarbeitenden Daten bewirkt werden?

physischer, materieller oder immaterieller Natur ErwGr. 75

- Wodurch, d.h. durch welche Ereignisse, kann es zu dem Schaden kommen?

Nichteinhaltung der Datenschutz-Grundsätze Art. 5 DSGVO inkl. der Betroffenenrechte Artt. 12 ff. DSGVO

- Wie, d.h. durch welche Handlungen und Umstände, kann es zum Eintritt dieser Ereignisse kommen?

Risikoquellen: intern/extern; vorsätzlich/fahrlässig; Security/Safety oder Datenschutz

Vom IT-Grundschutz lernen

4.4 Szenarien bilden

Im Rahmen einer Risikoanalyse kann unter Umständen eine sehr große Anzahl an möglichen Risiken in Betracht gezogen werden. Für die weitere Behandlung der identifizierten Risiken ist es jedoch wenig praktikabel, jedes einzelne identifizierte Risiko gesondert zu behandeln. Daher sollten die relevanten Risiken gruppiert werden. Hierfür bieten sich zwei Strategien an:

- Sie fassen alle Risiken zusammen, die auf einen Prozess wirken,
- Sie gehen von den Ressourcen aus, beispielsweise dem Personal oder einem technischen System wie einer Produktionsanlage, und gruppieren die Risiken entsprechend.

In der Praxis hat es sich bewährt, einem Notfallplan eine überschaubare Anzahl von **Risikoszenarien** zugrunde zu legen. Beispiele für solche Szenarien sind:

- der Ausfall zentraler Computersysteme,
- der Zusammenbruch der Netzinfrastruktur,
- die Zerstörung wichtiger Gebäude,
- der Wegfall wichtiger Lieferanten oder
- ein erheblicher Ausfall von Mitarbeitern.

Szenario-Technik erleichtert realistische Notfallvorsorge

Mit Hilfe der Szenario-Technik können Sie analysieren, welche Auswirkungen solche Vorfälle auf die Geschäftsprozesse haben können. Dabei sollten Sie den Ablauf eines Notfalls plastisch durchdenken. Bedenken Sie nicht nur extrem negative Entwicklungen ("Worst-Case"-Szenarien). Auch möglicherweise weniger gravierende oder sogar positive Auswirkungen können wertvolle Hinweise für die zu entwickelnden Notfallkonzepte liefern. Da dieses Verfahren sehr aufwändig ist, sollten Sie maximal 15 Notfallszenarien beschreiben und den Schwerpunkt auf solche Szenarien legen, die hohe und realistische Risiken enthalten (= hohes Schadensausmaß, nicht zu geringe Eintrittswahrscheinlichkeit).

IT-Grundschutz-Schulung

- Online-Kurs IT-Grundschutz
- *Online-Kurs: Notfallmanagement*
  - Startseite Webkurs
  - Einführung
  - Notfallmanagement initiieren
  - Business Impact analysieren
  - *Risiken analysieren*
    - Risiken identifizieren
    - Risikenbewerten
    - **› Szenarien bilden**
    - Strategien wählen
    - Risikoanalyse dokumentieren
    - Test
  - Strategien entwickeln
  - Konzepte einführen
  - Notfälle bewältigen
  - Notfälle üben
  - Notfallmanagement verbessern
  - Glossar

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzSchulung/Webkurs1004/4_RisikenAnalysieren/3_Szenarien%20bilden/SzenarienBilden_node.html

Hilfreich für Szenario-Technik

Auswirkungen auf betroffene Person prüfen:
physisch (Leib & Leben), materiell (Finanzen, Aufwand), immateriell (Ruf, gesellschaftlich)

Achtung:

- Wenn der Schaden nicht oder kaum reversibel ist

oder

- die betroffene Person nur wenige oder beschränkte Möglichkeiten hat,
  - die Verarbeitung selbst zu prüfen oder gerichtlich prüfen zu lassen

  oder
  - sich dieser Verarbeitung zu entziehen, etwa, weil sie von der Verarbeitung gar keine Kenntnis hat.

Eintrittswahrscheinlichkeit

- Im Bereich der IT-Sicherheit:
  - Teilweise Statistiken, z.B. Personalausfall- oder Störfallzahlen
  - Aber: *„Exakte quantitative Angaben zu Eintrittswahrscheinlichkeiten sind […] in der Regel nicht möglich."* [BSI]

- Hilfreiche Überlegungen
  - Bei Vorsatz:
    - Interesse an dem Eintritt des Ereignisses?
    - Aufwand für das Herbeiführen des Ereignisses?
    - Risiko, entdeckt zu werden?
    - Häufigkeit der Vorgänge, bei denen ein Ereignis möglich ist?
  - Bei Fahrlässigkeit: Bewusstsein der Beschäftigten? Ausstattung?
  - Bei Naturereignissen o.ä.: Indikatoren?

Welche technischen und organisatorischen Maßnahmen? SDM-Bausteine

MASSNAHMENKATALOG

Hier sind die Bausteine veröffentlicht, die als verbindliche Versionen auf der Basis des SDM V2.0 dienen.

Die einzelnen von der Datenschutzkonferenz bzw. vom Arbeitskreis „Technik" freigegeben Bausteine des Katalogs werden hier sukzessive veröffentlicht und sind damit zur Anwendung freigegeben.

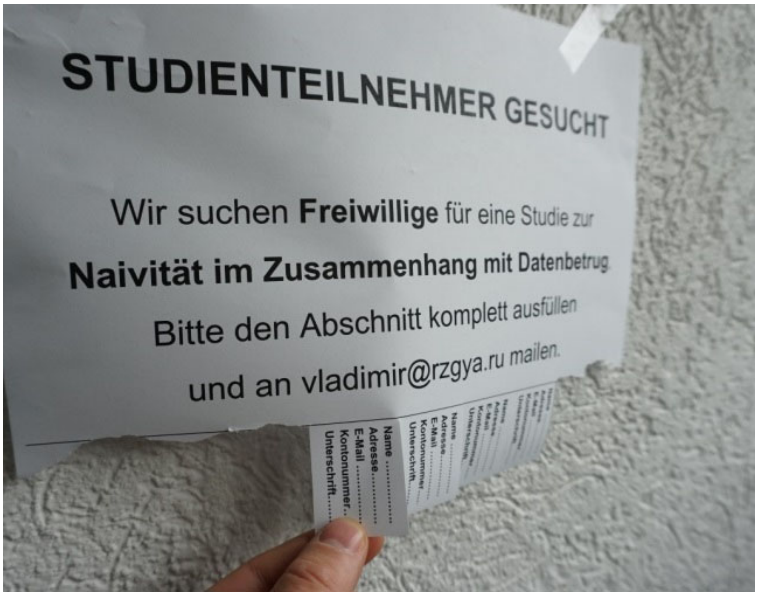
Wir empfehlen den Anwendern, ihre Erfahrungen bei der Erprobung der verbindlichen Bausteine den Datenschutzaufsichtsbehörden mitzuteilen (z.B. unter sdm@datenschutz-mv.de), und somit zur Weiterentwicklung von Methode und Maßnahmen beizutragen.

Bezeichnung	Format	Größe
Baustein 11 „Aufbewahren" (Version 1.0 vom 6. Oktober 2020)	PDF	0,75 MB
Baustein 41 „Planen und Spezifizieren" (Version 1.0 vom 25. März 2021)	PDF	1,08 MB
Baustein 42 „Dokumentieren" (Version 1.0a vom 2. September 2020)	PDF	0,12 MB
Baustein 43 „Protokollieren" (Version 1.0a vom 2. September 2020)	PDF	0,14 MB
Baustein 50 „Trennen" (Version 1.0 vom 6. Oktober 2020)	PDF	0,67 MB
Baustein 60 „Löschen und Vernichten" (Version 1.0a vom 2. September 2020)	PDF	0,14 MB
Baustein 61 „Berichtigen" (Version 1.0 vom 6. Oktober 2020)	PDF	0,52 MB
Baustein 62 „Einschränken der Verarbeitung" (Version 1.0 vom 6. Oktober 2020)	PDF	0,51 MB

https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/

Generelle Herausforderung

Bewusstsein der Nutzerinnen und Nutzer?



Überblick

- Implementierte IT-Sicherheit
  - Ausgangsbasis oder Wunsch?
- Datenschutz
  - Perspektivwechsel
  - Anforderungen aus Europa
- Implementierter Datenschutz
  - … by Design
  - … by Default
- Fazit

Von eingebauter Sicherheit zu eingebautem Datenschutz?

- Check: „eingebaute Sicherheit" kaum Realität
- Mögliche Gründe:
  - Keine klare Definition
  - Abhängigkeiten
  - Kosten vielerlei Art
  - Usability
  - Gegenläufige Interessen

 Foto: Horia Varlan

Von eingebauter Sicherheit zu eingebautem Datenschutz?

- Check: „eingebauter Datenschutz" kaum Realität

- Mögliche Gründe:
  - Keine klare Definition
  - Abhängigkeiten
  - Kosten vielerlei Art
  - Usability
  - Gegenläufige Interessen

Foto: Horia Varlan

Datenschutz + IT-Sicherheit mit der DSGVO gefordert

Fazit: verantwortungsvolle Gestaltung

- Startpunkt „Datenschutz"
- Folgenabschätzung
- Risiken im Griff

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