



IT-Sicherheit und Datenschutz – das eine tun und das andere nicht lassen

Marit Hansen

Landesbeauftragte für Datenschutz
Schleswig-Holstein

Kiel, 25.01.2019



www.datenschutzzentrum.de

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

IT-Sicherheit und Datenschutz - beides!

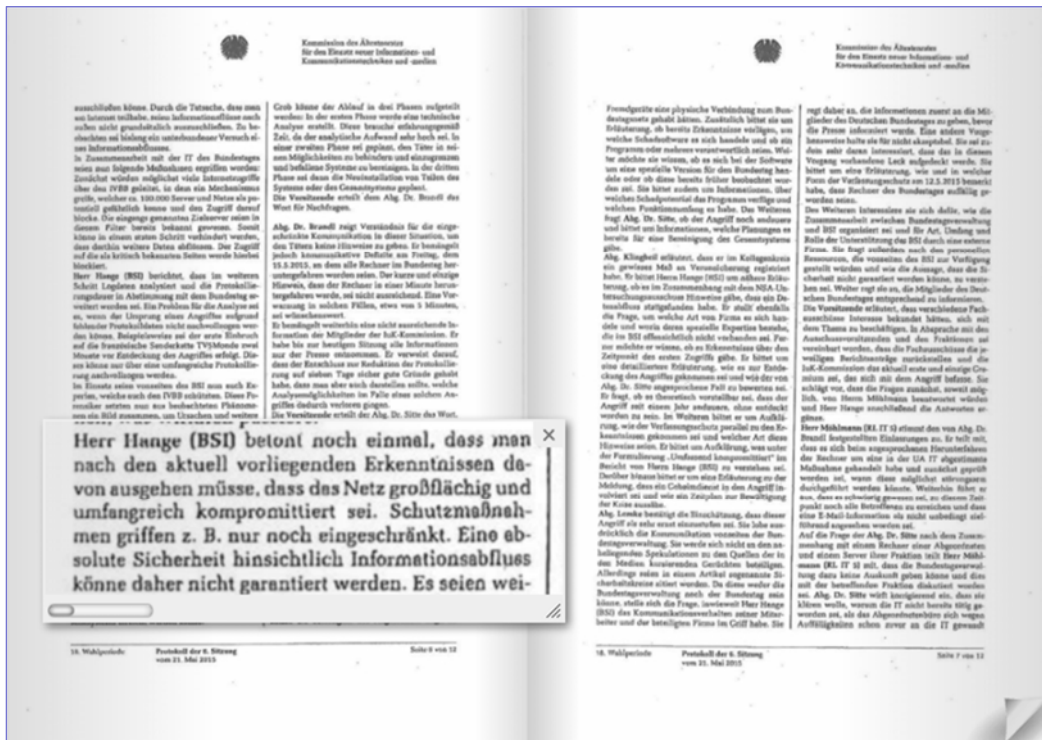
3

„Building Security In“ – Gary McGraw, 2004



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?



Beispiel:
„Bundestags-
Hack“

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

IT-Sicherheit und Datenschutz - beides!

5

„Collections“ – Daten-Leaks über Jahre

Ergebnis Ihrer Anfrage bei HPI Identity Leak Checker

Achtung: Ihre E-Mail-Adresse **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	Sozialversicherungs-nr.	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 Passwortern 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 **gmx.net**, bei denen das Passwort alter 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 werden 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 Betrugern ausgetauscht werden oder Daten die von Dokumenten (Reisepass, Ausweise, 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
pwned websites

6,474,028,664
pwned accounts

87,869
pwned

96,570,719
pwned accounts

Von **gmx.net** > **Ignore my former mails today**

24.01.2019, 19:46

I was hacked.

IT-Sicherheit und Datenschutz - beides!

6

Sicherheit durch Ausbauen

THE VERGE TRENDING NOW This is VAIO's Windows phone

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 @carlfranz

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



<http://resources.infosecinstitute.com/hacking-implantable-medical-devices/>

IT-Sicherheit und Datenschutz - beides!

7

The Register Biting the hand that feeds IT

DATA CENTRE SOFTWARE NETWORKS SECURITY INFRASTRUCTURE DEVOPS BUSINESS HARDWARE SCIENCE BOOTHNOTES 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 hindsight. 25 years ago, he wanted to Baking in security at that point might not have taken off 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.

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/

IT-Sicherheit und Datenschutz - beides!

8

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/zeroday.html>
<https://www.youtube.com/watch?v=4BTTiWkdT8Q>

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: Effective 10/1/2013, SP 800-90A is being re-issued as a draft for public comment for concerns or recommendations for improvement regarding the Generation Using Deterministic Random Bit Generators are (http://csrc.nist.gov/publications/PubsDrafts.html). NIST will accept comments received during this 60 day period.

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

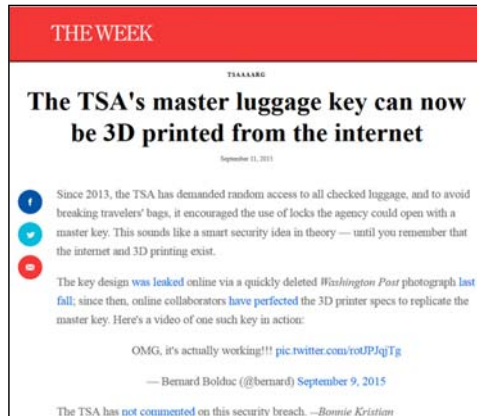
Dan Shumow
Niels Ferguson
Microsoft



Hintertüren / Master-Schlüssel?

Offline-Beispiel „TSA-Kofferschlösser“:

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



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

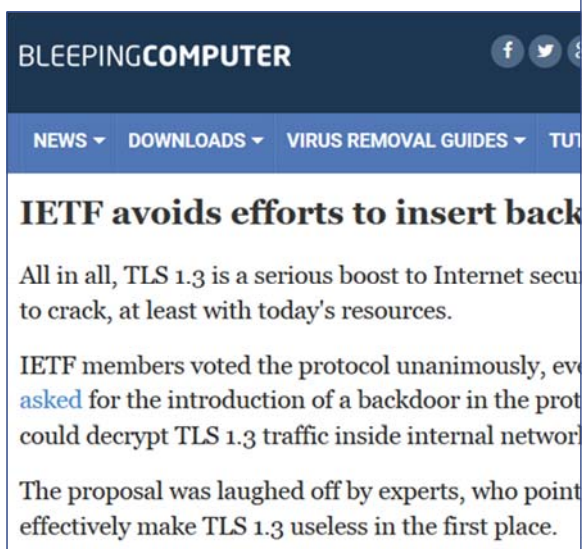


https://en.wikipedia.org/wiki/File:Wafer_Lock_Try-Out_Keys.jpg
https://en.wikipedia.org/wiki/File:Lol_key_escrow.jpg
 License: CC-BY-SA –
<https://creativecommons.org/licenses/by-sa/4.0/>

IT-Sicherheit und Datenschutz - beides!

11

Transportverschlüsselung im Fokus: Streit um TLS 1.3



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/>

IT-Sicherheit und Datenschutz - beides!

12

Lessons Learned – gut aufgestellt für die Zukunft?

Hacker nehmen Industrie 4.0 immer häufiger ins Visier - Digitales ...
<https://digitales-wirtschaftswunder.de/hacker-nehmen-industrie-4-0-immer-haeufiger-...>
 24.05.2018 - In der vernetzten Industrie 4.0 bieten Sensoren, Aktoren, Maschinen und Anlagen Cyber-Kriminellen viele Angriffsflächen. Das zeigt der VDE ...

Videos



Industrie 4.0: Hacker bedrohen die vernetzte Fabrik
 Digitaler Mittelstand
 YouTube - 31.03.2015



Live Hacking Tag 1: Sicherheitskonzepte für „Industrie 4.0“
 itandbusiness
 YouTube - 05.10.2016



Hack the Factory: Werde zum Hacker einer smarten Fabrik | ZVEI
 Die Elektroindustrie
 YouTube - 26.09.2018

Videos



Hacking a smart light bulb
 DEKRA Product Testing ...
 YouTube - 25.10.2018



35C3 - Smart Home - Smart Hack
 media.ccc.de
 YouTube - 29.12.2018



#140 IKEA Tradfri IOT Smart Lighting System Hack
 Andreas Spiess
 YouTube - 04.06.2017

smart light bulb | Hackaday
<https://hackaday.com/tag/smart-light-bulb/> Diese Seite übersetzen
 Equipped with a large donation of wireless bulbs controlled by a central ... Posted in home hacs is
 iphone hacks Tagged home automation, hue, philips, siri, smart ...

Car hacking remains a very real threat - USA Today

<https://www.usatoday.com/story/money/2018/01/.../car-hacking.../1032951001/>
 14.01.2018 - Automakers and suppliers are making progress in protecting vehicles from cyber attacks, but the car-hacking threat is still real and could get ...

Videos



How to Hack a Car: Phreaked Out (Episode 2)
 Motherboard
 YouTube - 29.05.2014



Car Hacking Demonstration: How The Government Could Hack Your ...
 TODAY
 YouTube - 09.03.2017



Hacking Cars Over the Internet
 TWIT Notcast Network
 YouTube - 02.05.2018

heit und Datenschutz - beides!

13

Datenpanne: Regel oder Ausnahme?

Hallo Mark, viel Spaß mit Deinen Erinnerungen auf Facebook 2018

Hallo Mark, viel Spaß mit Deinen Erinnerungen auf Facebook 2018

keine online

Cambridge Analytics, 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 bemerklicher. Es ist an der Zeit, sich etwas langweiliger zu bewegen und Dinge zu überdenken. *How slow and fix things.* Zudem bietet das Ende des Jahres eine schöne Gelegenheit zurückzuschauen. Auf das, was Du, Mark, mit Deiner Facebook Zeit, so alles erreicht hast.

Schließlich hast Du Großes vor: Am 4. Januar hast Du und Facebook *erwartet*, dass Du 2018 wichtige Dinge überarbeiten willst. Du wusstest zu viele Fehler begreifen und eure Tools können mitbewertet werden. Du, Mark, hast es in Deiner persönlichen Herausforderung erklärt, dass Facebook am Ende des Jahres besser dastehen sollte als Menschen gefiel.

Martin Strathmann arbeitet als Redakteur für keine online. Zuerst 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-Berichter *gibt Facebook Mittelstand zu Verbrechen gegen Menschenrechte in Myanmar*: Facebook sei das wichtigste soziale Netzwerk in dem Land und Beiträge darauf würden immer wieder Konflikte schüren.
- Das Datenanalytische Unternehmen Cambridge Analytics *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.
- Wird Facebook und WhatsApp Datenschutzverletzungen verliert haben, *mussten sie in Spanien jeweils 200.000 Euro zahlen* – die Höchststrafe.
- Du, Mark, hast bei einer Anhörung im US-Kongress konkrete Fragen ausgeschrieben. *Fürchter fanden heraus*, dass beim „Login mit Facebook“ Skizzen von Drittfirmen die Facebook-Identität des Benutzers nachvollziehen können.
- Jährlich waren persönliche Daten von 2 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-Deinen-Erinnerungen-auf-Facebook-2018-4254681.html>

2 von 3

<https://www.heise.de/newsticker/meldung/Hallo-Mark-viel-Spaß-mit-Deinen-Erinnerungen-auf-Facebook-2018-4254681.html>

Hallo Mark, viel Spaß mit Deinen Erinnerungen auf Facebook 2018

- Handy-Hersteller *konnten Nutzerdaten von Facebook-Freunden nutzen* Google *Alphabet*, auch wenn sie die Weitergabe ihrer Daten ausdrücklich dementiert hatten.
- Die eigentlich privaten Beiträge von wohl 14 Millionen Facebook-Nutzern *wurden missbrauchten* mit dem Namen *Wahl* geteilt.
- Ausgewählte Firmen konnten sich auch 2018 auf die Daten von Facebook-Freunden *einsetzen* – eigentlich sollte die Funktion für alle Entwickler abgeschaltet werden. *Hacker* Cyberkriminelle haben um mehr Zeit gebittet, um ihre Projekte umzusetzen, sagte Facebook.
- Geprüfte Nutzer *wurden auf Facebook fehlerhaft entzerrt* und konnten so Inhalte sehen, die sie nicht sehen durften.
- Die Unabhängigkeitsberichterstattung der USA *wurde auf Facebook als Hate Speech* eingestuft und gelöscht.
- In Indien *verbotene sich Gerichte über mögliche kriminelle Handlungen auf WhatsApp und stifteten Lockdowns an*. Mehr als 20 Menschen sind von Mai bis Juli in Tode getötet worden. Daraus schätzte der Minister der Verteidigung von Nordindien ein. WhatsApp gehört zur Facebook Inc.
- In Europa gab es erstmals *einen rechtlichen Einbruch der Facebook-Nutzer*.
- Facebooks VPN-App *Quinn* *wurde als Spion* des amerikanischen Geheimdienstes, 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 eingegeben hatten, um Werbung zielgerichteter auszuspielen.
- Etwa 30 Millionen Facebook-Nutzer *nutzen von einem Hacker* *abgeschaltet*.
- Die Abrufen des Videos auf Facebook waren fehlerhaft: Die durchschnittliche Zeit, die Nutzer Videos auf Facebook schauten, *ist nicht um 10 bis 15 Prozent überschätzt worden*. Medien investierten anhand dieser Statistiken viel Geld in Facebook-Videos, um Nutzer zu erreichen.
- Facebook *zahlte im Jahresabschluss 10.000 Euro*, weil das Geschäft eines Freizeits aus Hannover ungewollt mit einer Seite auf dem sozialen Netzwerk vertreten war.
- Über Facebook *haben sich Werbeanzeigen an Interessenten von „letzte große“* *unangenehm* *schuldig*. Nach Berichten wurde die Werbekampagne gelöscht.
- Hacker haben private Facebook-Nutzerdaten *von mehr als 10.000 Konten* *ausgeklaut*.
- Facebook *bestrafte eine PR-Firma dafür*, *Verträge* *schlichtemachen*, die verbreitete unter anderem, dass der Investor George Soros Kampagnen gegen Facebook finanziert habe.
- Instagram *verlor das Passwort von manchen Nutzern im Twitter*, Instagram gehört zu Facebook, Inc.
- Du, Mark, hast lieber nicht zu einer *Anhörung im britischen Parlament erschienen*.
- Die italienische Wettbewerbsbehörde *verurteilte Facebook zu zwei Datenlecks*.
- *Stritten* in Höhe von insgesamt 10 Millionen Euro.
- Benutzern war *„Nicht mehr“* *noch* *Spill haben* *und 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 *gaben sensible Daten der Nutzer an Facebook weiter*.
- Über einen Fehler in der Foto-API konnten Apps von Drittanbietern *für kurze Zeit auf* *unendlich viele Bilder von Nutzern zugreifen*. Die australische Datenschutzbehörde *ermittelte*.
- Zwei Studien haben gezeigt, dass russische Staatstrojanen auf Instagram *zu* *erfolgreich* *das* *schlechte* *verbreiten konnten*.
- Und das Jahr ist doch eigentlich schon im Ende, da lernt sich Facebook noch einen kleinen Klopfer. Oder besser: Der Klopfer kommt bereits, dass Facebook *musste Daten* *in seinen Tech-Konten* *veröffentlichen* hat. Konrad Wieders vom Washington, DC, mittlerweile schon gegen Facebook *angefordert* *habe* *Datenschutz* *klagt*.

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

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

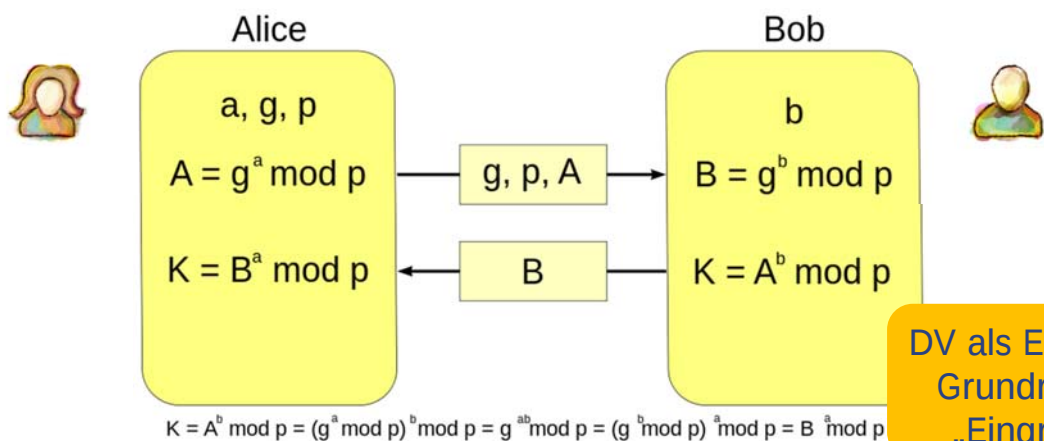


Bild: beludise via Pixabay

IT-Sicherheit und Datenschutz - beides!

17

Perspektive: Alice & Bob



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

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

IT-Sicherheit und Datenschutz - beides!

18

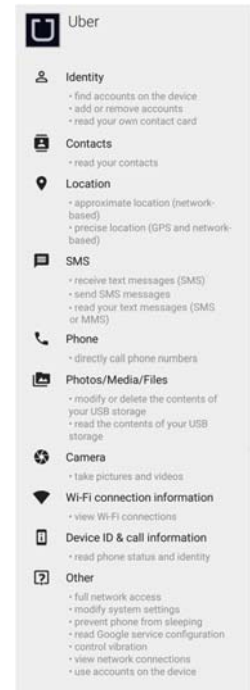
Heutige Situation

- 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, Ortsdaten, Mikrofon...



IT-Sicherheit und Datenschutz - beides!

19

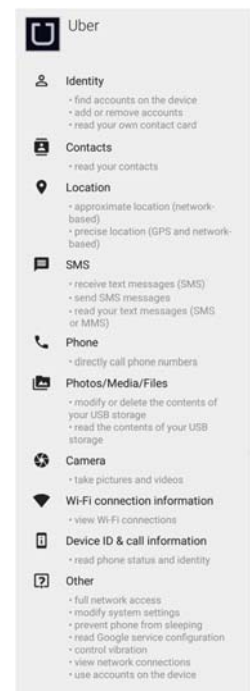
Heutige Situation

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

Kaum Wahlmöglichkeiten



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



20

Zugriff auf Batterie-Status relevant?

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

By Marion Dakers
22 MAY 2016 - 11:23AM

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

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>

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

IT-Sicherheit und Datenschutz - beides!

21

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 mehr sicher vor ihnen - neuerdings auch geräteübergreifend - mit Ultraschall.



© putlove_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: WEXA / PC-Magazin

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

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 Google's Play Store.

IT-Sicherheit und Datenschutz - beides!

22

Heutige Situation

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



republica T3M

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

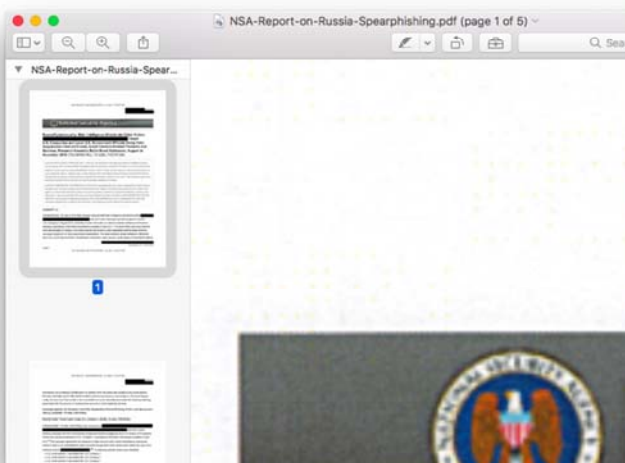
(*) basiert auf augenscheinlich zum Verlag gehörenden Domains/Subdomains

republica 2016 – Thorsten Schröder & Frank Rieger: Ad-Wars

Verantwortungs-
diffusion

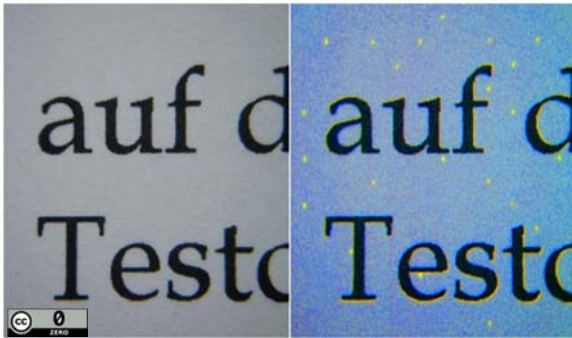
Heutige Situation

Eingebauter Datenschutz?
Im Gegenteil:
eingebaute Verkettbarkeit
und Identifizierbarkeit



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

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



Vorratsdatenspeicherung im
Farbdruck:
verstecktes Wasserzeichen

```

111111
123456789012345
7 000 00000 0 000
6
5 0 0 00 0
4 00 0 000000
3 0 0 00 0
2 0 0 00 0000
1 0 00 000 0
0 00000 00
    
```

Printer serial number: 535218 [or 29535218]
Date: May 9, 2017
Time: 06:20
Column 15 value: 54

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

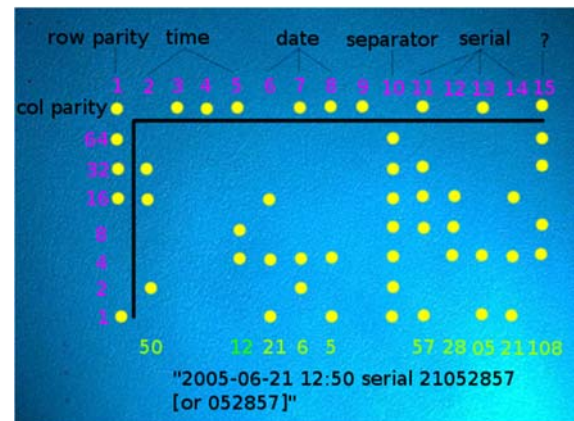


Bild: Electronic Frontier Foundation (EFF)

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

IT-Sicherheit und Datenschutz - beides!

25

Big Data: Target-Analyse

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.



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?"

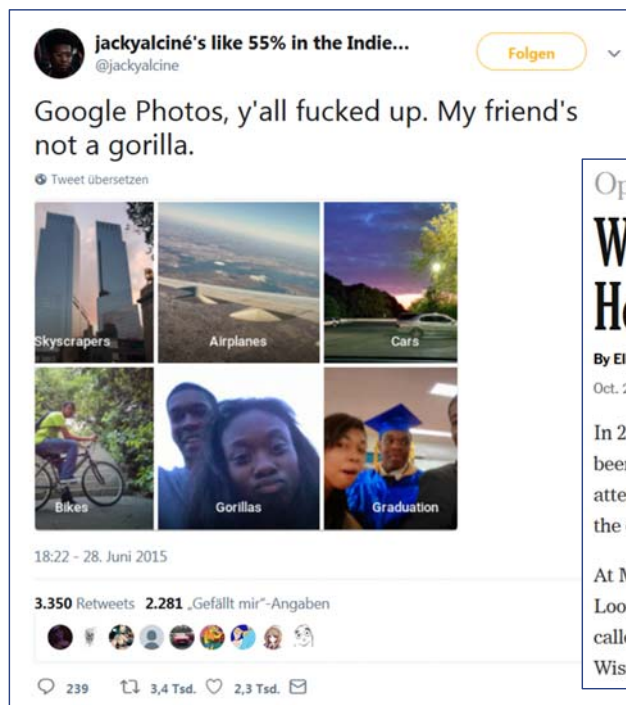
<http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html>

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

IT-Sicherheit und Datenschutz - beides!

26

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 Thadaneys Israni

Oct. 26, 2017

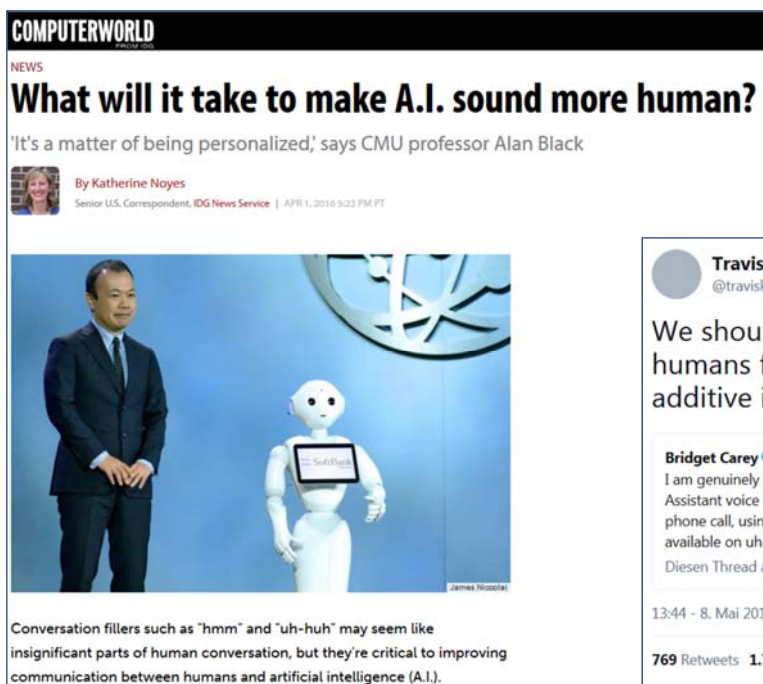
In 2013, police officers in Wisconsin arrested a man driving a car that had been used in a recent shooting. The man, Eric Loomis, pleaded guilty to attempting to flee an officer, and no contest to operating a vehicle without the owner's consent. Neither of his crimes mandates prison time.

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

IT-Sicherheit und Datenschutz - beides!

27

Welche Regeln? z.B. bei AI-Bots



<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>

IT-Sicherheit und Datenschutz - beides!

28

Vereinheitlichung und Modernisierung

- Idee: Eine für alle
und
alle für eine
- Ziel:
echte Harmonisierung
- Rechtssicherung durch
Gleichklang der Aufsicht
- Aber: 70 Öffnungsklauseln
für die Mitgliedstaaten



 Bild: skylarvision via Pixabay

Überblick



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

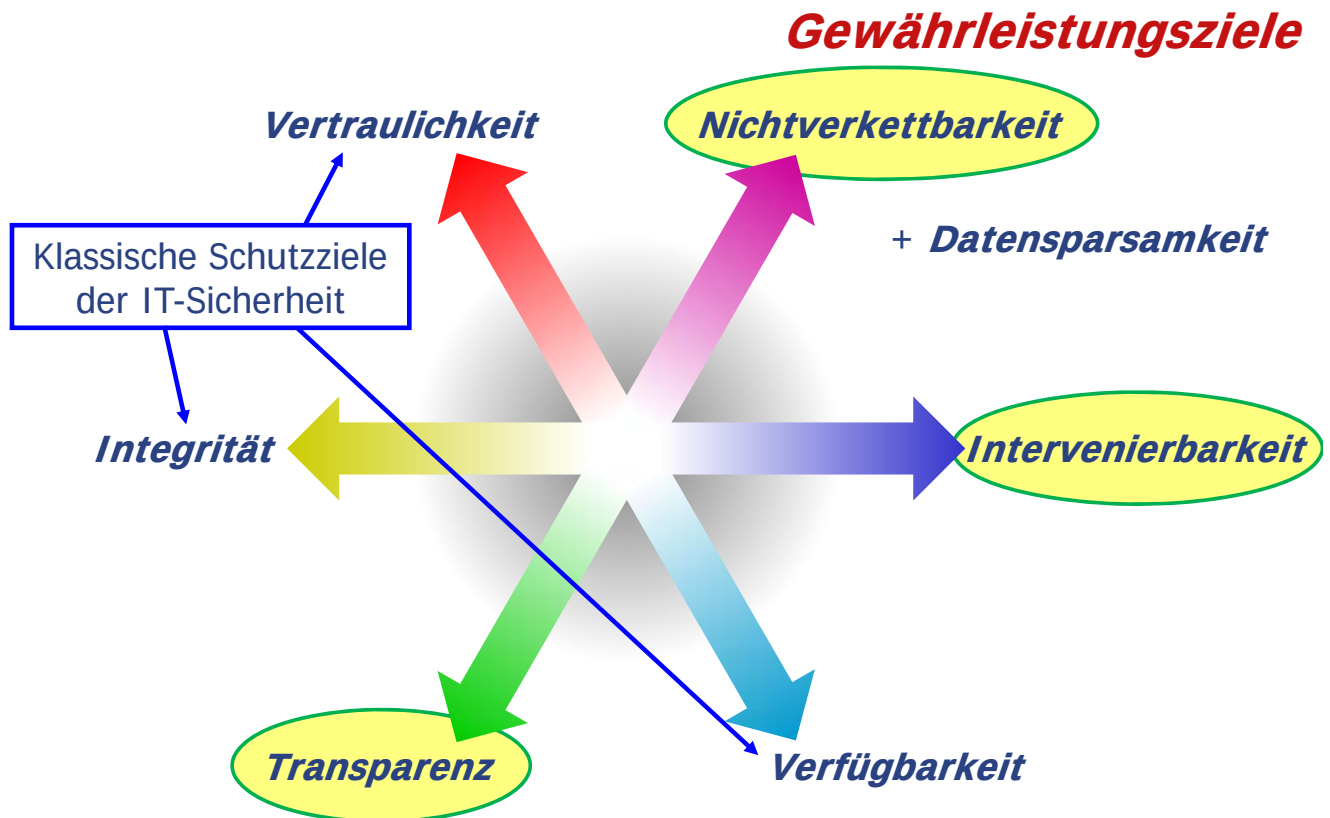
Vorbemerkung: Wichtigkeit von „by Design“

Erwägungsgrund 4

„The processing of personal data **should be designed** to serve mankind. [...]“



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



Wie? Gewährleistungsziele implementieren

Nichtverkettbarkeit



Bild: ivanacoi via Pixabay

Trennung von Domänen,
Gewaltenteilung,
Zweckbindung

z.B. (situationsgerecht):
Widerspruch,
Rechtsschutz,
Rückabwicklung von
Entscheidungen ...

Please,
help me!

Bild: geralt via Pixabay

Intervenierbarkeit

Transparenz



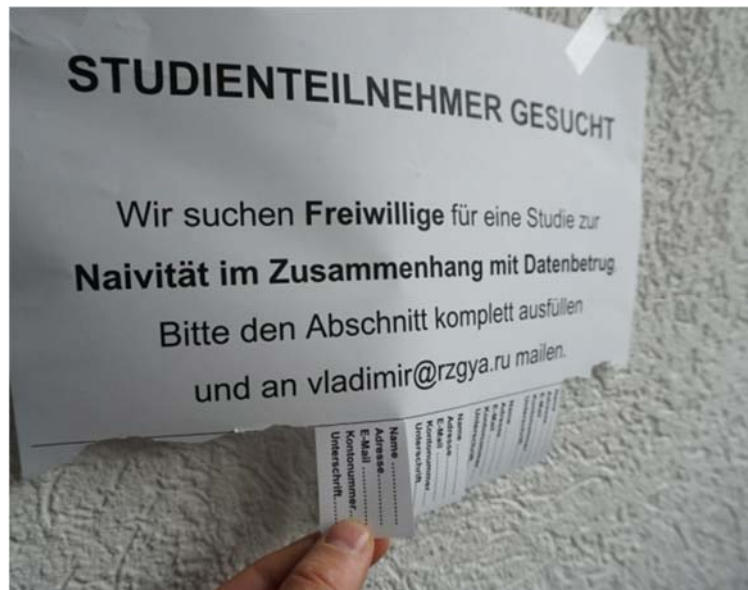
Ziel: Nachvollziehbarkeit
& Überprüfbarkeit

Bild: geralt via Pixabay

Ziel: **Risikobeherrschung** –
Risiko für die Rechte und Freiheiten
natürlicher Personen

Aber: Bewusstsein muss mitwachsen

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:**

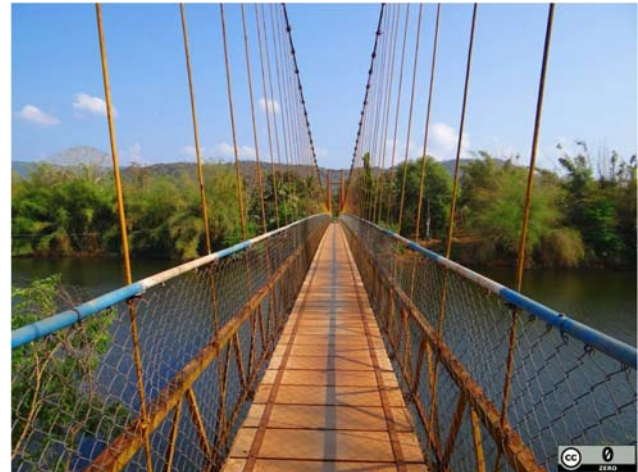
- Keine klare Definition
- Abhängigkeiten
- Kosten vielerlei Art
- Usability
- Gegenläufige Interessen



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/>