



Cybercrime, Hacking, Datenschutz: Was ist zu tun?!

Marit Hansen
Landesbeauftragte für Datenschutz
Schleswig-Holstein

28.02.2019, Kaltenkirchen



www.datenschutzzentrum.de

Überblick



- Warum Datenschutz?
- Cybercrime, Hacking & more*)
- Datenschutz & Datensicherheit
 - Meine Rechte
 - Was kann ich selbst machen?
 - Was muss sich ändern?
- Fazit

*) hier auch: unfaire Praktiken
auf Basis von Daten

Beim Datenschutz geht es um ~~Daten~~



 Source: Ashtyn Renee

Menschen mit ihren Rechten

Wichtig bei der
Gestaltung:

- Auswirkungen auf Menschen?
- Auswirkungen auf die Gesellschaft?

Datenschutz
nötig:

Machtgefälle
zwischen
Individuen
und
Organisationen



 Bild: beludise via Pixabay

Vereinheitlichung und Modernisierung

- Idee: Eine für alle
und
alle für eine
- Ziel:
echte Harmonisierung
- Rechtssicherung durch mehr
Gleichklang der Aufsicht
- Spürbare Sanktionen möglich



 Bild: skyllarvision via Pixabay

Überblick



- Warum Datenschutz?
- Cybercrime, Hacking & more
- Datenschutz & Datensicherheit
 - Meine Rechte
 - Was kann ich selbst machen?
 - Was muss sich ändern?
- Fazit

Old-School-Sicherheit



 Bild: Das Wortgewand via Pixabay

Doxing: Januar 2019

Doxing (von engl.: dox, Abkürzung für documents, dt.: Dokumente), auch doxxing, ist das internetbasierte Zusammentragen und anschließende Veröffentlichen personenbezogener Daten, zumeist mit böswilligen Absichten gegenüber den Betroffenen. Zum Teil geht damit auch die Identifikation von anonymen Personen einher.

Doxing – Wikipedia

<https://de.wikipedia.org/wiki/Doxing>

Unter den veröffentlichten Daten sind auch private Adressen, hunderte Handynummern Briefe und Bankinformationen.

shz.de von **afp, dpa, Lorena Dreusicke und Tobias Schmidt**
04. Januar 2019, 14:07 Uhr

Exklusiv für
shz+ Nutzer

shzo

HAMBURG/BERLIN | Ministerpräsident Stephan Weil ist wütend: „Woher haben Sie diese Nummer?“ Ungebetene Anrufe auf seinem persönlichen Handy will der niedersächsische SPD-Chef nicht haben. Daniel Günther, ...

<https://www.shz.de/deutschland-welt/politik/Hackerangriff-auf-hunderte-Politiker-und-Prominente-id22143397.html>

„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 können 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 **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 werfen für unseren Dienst nur öffentlich im Internet verfügbare Quellen aus und können keine Vollständigkeit garantieren. Wir berücksichtigen 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

pwned websites

6,474,028,664

pwned accounts

87,869

pwned

96,570,719

pwned accounts

Von

Betreff Ignore my former mails today

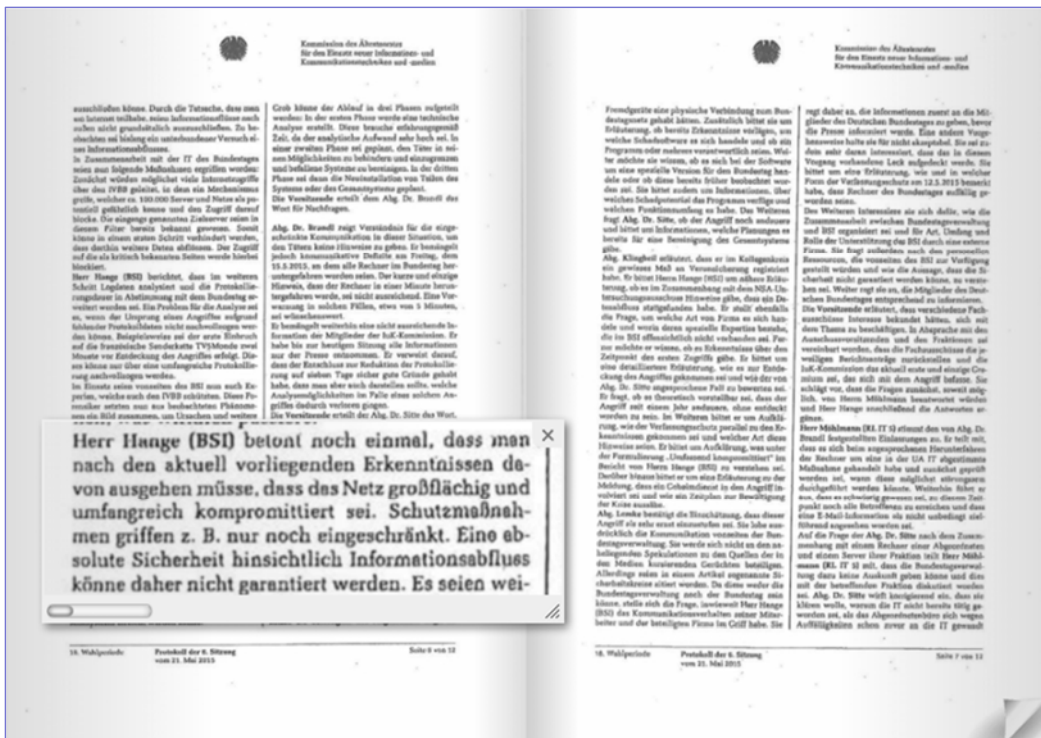
24.01.2019, 19:46

I was hacked.

Cybercrime, Hacking, Datenschutz: Was ist zu tun?!

9

Brüchiges Fundament?



Beispiel:
„Bundestags-Hack“

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

Cybercrime, Hacking, Datenschutz: Was ist zu tun?!

10

Sicherheit durch Ausbauen

THE VERGE

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/>

Cybercrime, Hacking, Datenschutz: Was ist zu tun?!

11

Lessons Learned – gut aufgestellt für die Zukunft?

Hacker nehmen Industrie 4.0 immer häufiger ins Visier - Digitales ...
<https://digitales-wirtschafts-wunder.de/hacker-nehmen-industrie-4-0-immer-haeufiger-4-0/>
 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 15/11/19 24:10:13
 iphone hacks Tagged home automation, hue, philips, siri, smart ...

Car hacking remains a very real threat - USA Today
<https://www.usatoday.com/story/money/2018/01/11/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 Netcast Network
 YouTube - 02.05.2018

Cybercrime, Hacking, Datenschutz: Was ist zu tun?!

12

Datenpanne: Regel oder Ausnahme?

Hallo Mark, viel Spaß mit Deinen Erinnerungen auf Facebook 2018

keine 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 bemerklicher. Es ist an der Zeit, sich etwas länger zu besinnen und Dinge zu überdenken. *How slow and thoughtful*. Zudem bietet das Ende des Jahres eine schöne Gelegenheit zurückzuschauen. Auf das, was Du, Mark, mit Deiner Facebook Inc. so alles erreicht hast.

Schließlich hast Du Großen vor: Am 4. Januar **hast Du auf Facebook berichtet**, dass Du 2018 wichtiger Dinge überdenken willst. Du wusstest zu viele Fehler begangen und dass Du sie korrigieren möchtest. Du, Mark, hast es zu Deiner persönlichen Herausforderung erklärt, dass Facebook am Ende des Jahres besser dastehen soll als zu Beginn.

Maria Strathmann arbeitet als Redakteurin für keine online. Zuvor hat er für Chip Online, Focus Online, Zeit Online und die Süddeutsche Zeitung über Digitalis geschrieben.

Viel Spaß mit Deinen Erinnerungen auf Facebook 2018:

- US-Beobachter **erzählen Facebook Mitarbeiter in Verbindung setzen Nachrichten im Messenger**: Facebook sei das wichtigste soziale Netzwerk in dem Land und Beiträge darauf würden immer wieder Konflikte auslösen.
- Das Datenanalyse-Unternehmen Cambridge Analytica **ist als die Daten von bis zu 87 Millionen Facebook-Nutzern gewonnen**. Daraufhin kündigte Facebook an, den Zugriff von App-Entwicklern auf Nutzerdaten einzuschränken.
- Von Facebook und WhatsApp **Datenschutzbestimmungen** verfasst haben, **mussten sie in Spanien jeweils 100.000 Euro zahlen** – die Höchststrafe.
- Du, Mark, hast bei einer Anhörung im US-Kongress konkrete Fragen ausgeschrieben. **Forscher fanden heraus**, dass beim „Login mit Facebook“ Skripte von Drittfirmen die Facebook-Identität der Benutzer nachvollziehen können.
- Jährlich waren persönliche Daten von 3 Millionen Facebook-Nutzern **öffentlich zugänglich**.
- Du, Mark, hast bei einer Anhörung im EU-Parlament unangenehme Fragen ignoriert.

Hallo Mark, viel Spaß mit Deinen Erinnerungen auf Facebook 2018

- Handy-Hersteller **konnten Nutzerdaten von Facebook-Freunden nutzen**. Google **erzählt**, auch wenn sie die Weitergabe ihrer Daten ausdrücklich deklariert haben.
- Die **regulierten privaten Beiträge von bis zu 14 Millionen Facebook-Nutzern wurden möglicherweise massenhaft mit der ganzen Welt geteilt**.
- **Ausgewählte Firmen konnten auch noch 2018 auf die Daten von Facebook-Freunden einen Zugriff erhalten** – eigentlich sollte die Funktion für alle Entwickler abgeschaltet werden. Manche Unternehmen haben um mehr Zeit gebittet, um ihre Projekte umzustellen, sagte Facebook.
- Geopirte 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 **verurteilten sich Gerichte über mögliche kriminelle Handlungen auf WhatsApp und stellten Einschränkungen an**. Mehr als 20 Menschen sind von Mai bis Juli im Tode getötet worden. Davorhin schaltete der Messenger die Weiterleitung von Nachrichten ein. WhatsApp gehört zur Facebook Inc.
- In Europa gab es erstmals **einen rechtlichen Eintrag der Facebook-Strategie**.
- Facebooks VR-App Oculus **erlaubt den gesamten Internetzugang**, der über ihre Server lief – sie verbiete auch Display-Aktivität und Datenverbrauch aus. Auf Druck von Apple **entfernte Facebook die Anwendung aus dem App Store**.
- Facebook **verwendet die Telefonnummern**, die Nutzer für die Zwei-Faktor-Authentifizierung eingetragen hatten, um Werbung zielgenauer auszuspielen.
- Etwas 30 Millionen Facebook-Nutzer **sahen von einem Hacker direkt Werbung**.
- Die Abrechnung der Videos auf Facebook waren fehlerhaft: Die durchschnittliche Zeit, die Nutzer Videos auf Facebook schauten, **ist nicht um die halbe Stunde überschätzt worden**. Medien investierten anhand dieser Statistiken viel Geld in Facebook-Videos, um Nutzer zu erreichen.
- Facebook **zahlte im vierten Quartal 10.000 Euro**, weil das Geschäft eines Finanziers aus Hannover ungewollt mit einer Seite auf dem sozialen Netzwerk vertreten war.
- Über Facebook **ließen sich Werbeanzeigen an Interessenten von „hate speech“ (hassvolle Rede) schalten**. Nach Beschwerden wurde die Werbekategorie gelöscht.
- Hacker boten private Facebook-Nachrichten von mehr als 10.000 Kontakten **zum Verkauf an**.
- Facebook **besuchte eine PR-Firma dafür**, **Kritiker zu beschwichtigen**. Sie verbotene unter anderem, dass der Investor George Soros Kampagnen gegen Facebook finanzieren habe.
- Instagram **verlor das Passwort von manchen Nutzern im Klartext**; Instagram gehört zu Facebook, Inc.
- Du, Mark, hast lieber nicht zu einer **Anhörung im britischen Parlament erschienen**.
- Die italienische Wettverbandsbehörde **verurteilte Facebook zu einer Geldstrafe**.
- **Straten** in Höhe von insgesamt 10 Millionen Euro.
- **Benutzungen wie „Nicht mehr Nacht noch Spiel 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 **gaben sensible Daten der Nutzer an Facebook weiter**.
- Über einen Fehler in der Foto-API konnten Apps von Drittanbietern **kurze Zeit auf unzählige statische Bilder von Nutzern zugreifen**. Die russische Datenschutzbehörde **erzählte**.
- Zwei Studien haben gezeigt, dass russische Staatstrojaner auf Instagram **zahlreiche erfolgreiche** **ihre Inhalte verbreiten konnten**.
- Und das Jahr ist doch eigentlich schon im Ende, da **beendet sich Facebook noch einen dicken Klopfer**. Oder besser: Der Klopfer kommt herau, dass **Facebook private Daten in anderen Tech-Kontexten weitergegeben hat**. Ein Waden, den WhatsApp, IC, mittlerweile kritisiert gegen Facebook **haben** **Erklärung beim 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.

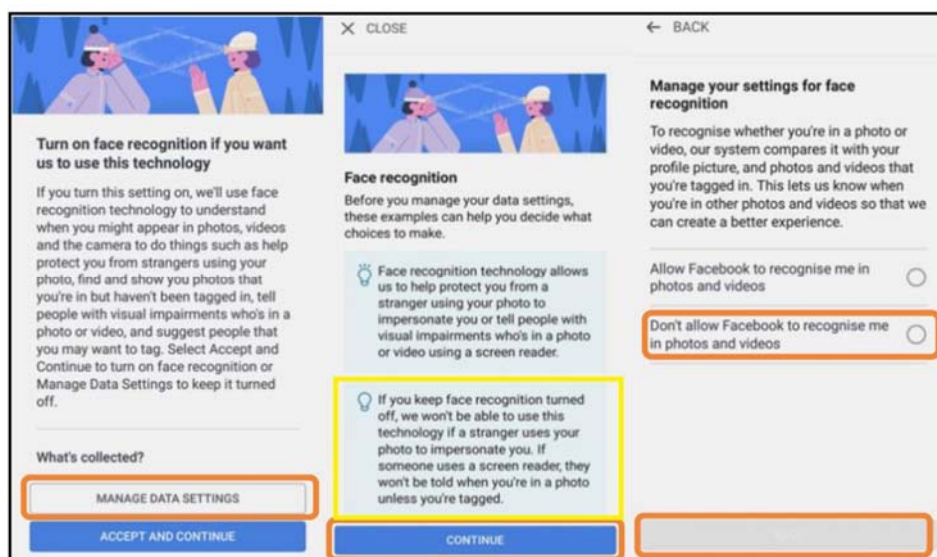
Strathmann, Heise, 25.12.2018, <https://www.heise.de/newsticker/meldung/Hallo-Mark-viel-Spass-mit-Deinen-Erinnerungen-auf-Facebook-2018-4254681.html>

Cybercrime, Hacking, Datenschutz: Was ist zu tun?!

13

„Dunkle Muster“ (Dark Patterns) – Report des norwegischen Verbraucherrats

Beispiel: Facebook bei biometrischem Gesichtsabgleich



Forbrukerrådet: „Deceived by Design“, 2018 (Seite 23)
<https://www.forbrukerradet.no/undersokelse/no-undersokelsekategori/deceived-by-design/>

Cybercrime, Hacking, Datenschutz: Was ist zu tun?!

14

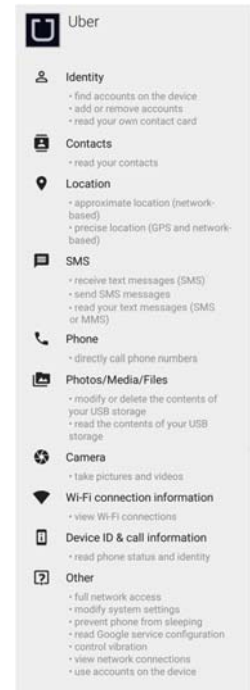
Heutige Situation

- 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...



Cybercrime, Hacking, Datenschutz: Was ist zu tun?!

15

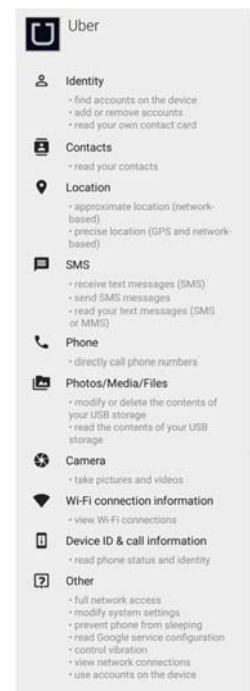
Heutige Situation

- 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>



16

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

Cybercrime, Hacking, Datenschutz: Was ist zu tun?!

17

Verbraucher werden kategorisiert (Beispiel Personix)

Kinderlos & aktiv	Paare 18 bis 40 Jahre, Ø 34 Jahre Mittlere bis hohe Einkommen	Meist kinderlose Paare bis 40, die als Angestellte mit mittleren Einkommen arbeiten. Sie leben überwiegend in Mehrfamilienhäusern in Großstädten und richten sich gepflegt ein. Interesse an Feinschmeckerküche, Wellness, Musik und Film sowie Computer und Internet.
Midlife-Single & kleines Budget	Singles 30 bis 50 Jahre, Ø 41 Jahre Niedrige Einkommen	Meist Arbeiter mit niedrigen Einkommen in Mietwohnungen mit dem niedrigsten Frauenanteil aller Gruppen. Trotz Interesse für Sport sind sie selten selber sportlich aktiv und verbringen ihre Freizeit sie überwiegend in ihrer Wohnung mit Fernsehen Musik, Video, Computer und Onlinespielen.
Familie & kleines Budget	Familien 30 bis 65 Jahre, Ø 45 Jahre Niedrige bis mittl. Einkommen	Meist Familien in ländlichen ostdeutschen Gebieten, wo sie trotz ihrer eher niedrigen Einkommen ein eigenes Haus finanzieren können. Ihr Leben ist oft geprägt von Familienaktivitäten. Wenig Interesse an Sport, hohe Haustierdichte.
Midlife plus & topsituiert	Familien und Paare 30 bis 65 Jahre, Ø 54 Jahre Sehr hohe Einkommen	Meist Paare und Familie mit hohem Bildungsabschluss. Sie verdienen gut als Manager, Selbstständige und Beamte, leben häufig im eigenen Haus und haben zahlreiche Geldanlagen. Interesse an Wirtschaft, Politik, Feinschmeckerküche, kulturellen Veranstaltungen, Golf, Tennis und Segeln.
Junge Familie & Mittelschicht	Familien 30 bis 40 Jahre, Ø 36 Jahre Mittlere bis hohe Einkommen	Meist Familien mit Hausfrauen-Ehen und guten Einkommen, die sich auf die Belange ihrer noch jungen Kinder einrichten. Sie mieten häufig Häuser in eher ländlichen Regionen und haben Bausparverträge. Interessen: Kleintiere, Vereine, Basteln und Heimwerken, preisgünstiger Breitensport.
Reife Familie & etabliert	Familien 30 bis 65 Jahre, Ø 49 Jahre Hohe Einkommen	Meist Eltern mit teilweise schon erwachsenen Kindern in ländlichen Regionen im eigenen oder gemieteten Haus. Trotz Hausfrauenehen sind die Einkommen oft gut. Interesse vor allem an Ausgestaltung des Heims, Garten- und Handarbeit.

Ausschnitt aus den 14 Hauptsegmenten von Personix Typologie von Acxiom Deutschland (S. 3):
https://gik.media/cms/wp-content/uploads/2018/04/Fact_sheet_Personix_Übersichtsbroschüre_2017.pdf

Cybercrime, Hacking, Datenschutz: Was ist zu tun?!

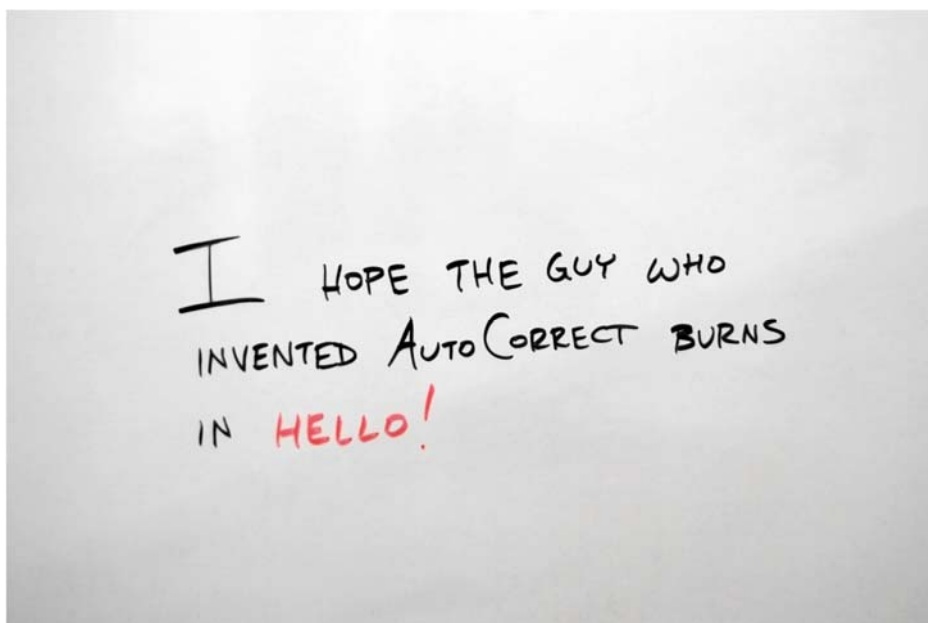
18

Überblick



- Warum Datenschutz?
- Cybercrime, Hacking & more
- **Datenschutz & Datensicherheit**
 - **Meine Rechte**
 - Was kann ich selbst machen?
 - Was muss sich ändern?
- Fazit

Korrekte Datenverarbeitung nötig



Rechte der Betroffenen

Stärkung der Rechte der betroffenen Personen:

- Artikel 7: **Einwilligung**: freiwillig, informiert, widerrufbar
- Artikel 12: Transparente **Information** [...]
- Artikel 13+14: Informationspflichten
- Artikel 15: **Auskunftsrecht** der betroffenen Person
- Artikel 16: Recht auf **Berichtigung**
- Artikel 17: Recht auf **Löschung** („Recht auf Vergessenwerden“)
- Artikel 18: Recht auf Einschränkung der Verarbeitung
- Artikel 19: Mitteilungspflicht im Zusammenhang mit Art. 17/18
- Artikel 20: Recht auf **Datenübertragbarkeit**
- Artikel 21: Widerspruchsrecht
- Artikel 22: **Automatisierte Entscheidungen** im Einzelfall / Profiling

Einwilligung



 Bild: Catkin via Pixabay

Widerruf der Einwilligung



 Bild: ivanacoi via Pixabay

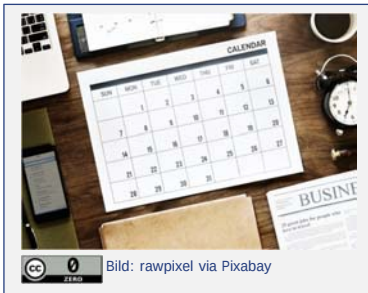
Vertrag



 Bild: geralt via Pixabay



 Bild: stux via Pixabay



Betroffenenrecht Information



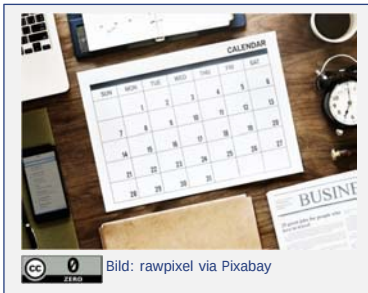
Bild: geralt via Pixabay



Betroffenenrecht Auskunft



Bild: geralt via Pixabay



Betroffenenrecht Berichtigung



Bild: stevepb via Pixabay



Betroffenenrecht Löschen



Bild: Hans via Pixabay



Bild: rawpixel via Pixabay

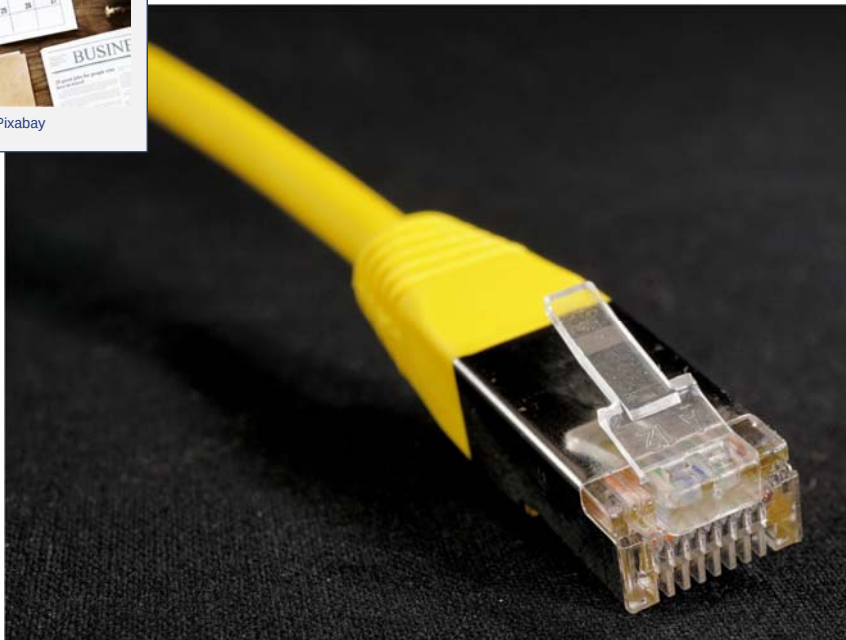


 Bild: webandi via Pixabay

Betroffenenrecht

Übertragbarkeit

Cybercrime, Hacking, Datenschutz: Was ist zu tun?!

29



Bild: rawpixel via Pixabay

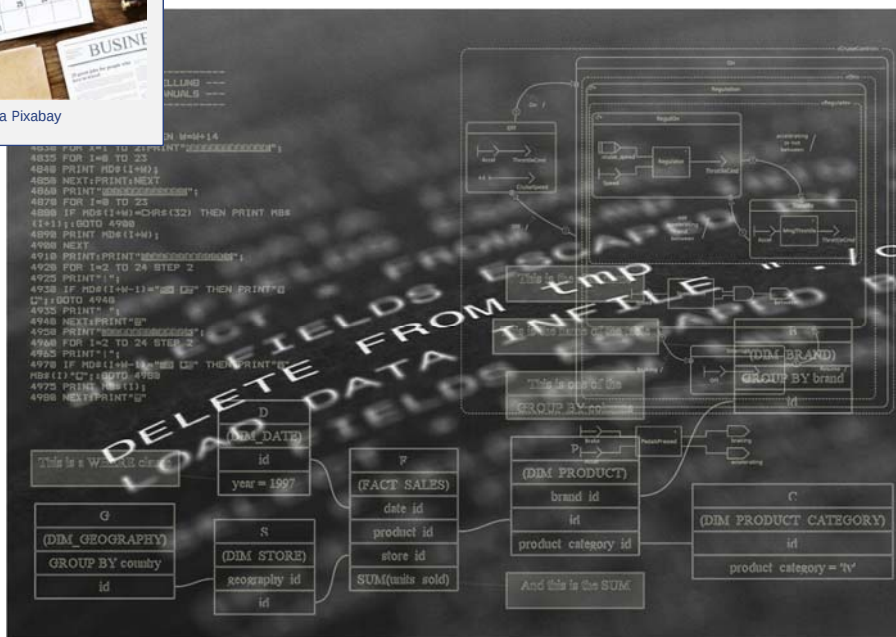


 Bild: geralt via Pixabay

Bei Einzelentscheidung: Information über Logik

Cybercrime, Hacking, Datenschutz: Was ist zu tun?!

30

Betroffenenrecht Beschwerde bei den Datenschutz-Aufsichtsbehörden



Bild: geralt via Pixabay

Neu: Datenschutz „by Design“ & „by Default“

- Anforderung der **EU-Datenschutz-Grundverordnung** (Art. 25 DSGVO)
- Pflicht für:
 - **Datenverarbeiter** (primär: Verantwortlicher)
 - Indirekt: Dienstleister und **Hersteller** von IT-Systemen
 - Nachfragen!
- Ziel: **eingebauter Datenschutz** von Anfang an
 - a) **datenminimierend**
 - b) mit möglichst **datenschutzfreundlichen Voreinstellungen**

Überblick



- Warum Datenschutz?
- Cybercrime, Hacking & more
- Datenschutz & Datensicherheit
 - Meine Rechte
 - Was kann ich selbst machen?
 - Was muss sich ändern?
- Fazit

Selbstschutz:

Welche Daten gebe ich heraus? Zu welchem Zweck?

Vorname

Nachname

Straße und Hausnummer

PLZ / Stadt

[Firma eintragen](#) [Adresse im Ausland](#)

E-Mail Adresse*

Telefon

Ihre Telefonnummer wird für eventuelle Rückfragen benötigt.

Geburtsdatum (optional) TT MM JJJJ

☐ Abweichende Lieferadresse angeben

ZAHlungsART

☐ Bankeinzug ¹ Bequem vom Konto abbuchen lassen. BANKEINZUG

☐ Bankeinzug mit Kontonummer und BLZ ¹ Bequem vom Konto abbuchen lassen. BANKEINZUG

☐ Kreditkarte ¹ Einfach mit Kreditkarte bezahlen. VISA MasterCard

☐ Rechnungsauf ¹ Erst bezahlen, wenn die Tickets da sind. RECHNUNG

☐ paydirekt ¹ Das neue Online-Bezahlverfahren Ihrer Banken und Sparkassen. paydirekt

☐ Onlineüberweisung mit giropay ¹ Direkt mit Onlineüberweisung bezahlen. giropay

☐ SOFORT Überweisung ¹ Direkt mit Onlineüberweisung bezahlen. SOFORT Überweisung

☒ Vorkasse (Ticketreservierung) ¹ Vorab mit Überweisung bezahlen. VORKASSE

Die notwendigen Zahlungsdaten erhalten Sie mit der Bestellbestätigung (auf der letzten Seite und zusätzlich per E-Mail).

☐ Ratenkauf ¹ Wunschtickets in Raten zahlen. Wunschtickets

☐ Masterpass ¹ Das Wallet für Kreditkartenbesitzer. Masterpass

Selbstschutz: Aktualisierungen (Updates) zum Schließen von Sicherheitslücken



Bild: ElasticComputeFarm
via Pixabay

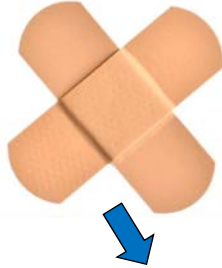


Bild: _Alicja_ via Pixabay



Bild: geralt via Pixabay

Selbstschutz: Passwörter – verschiedene!

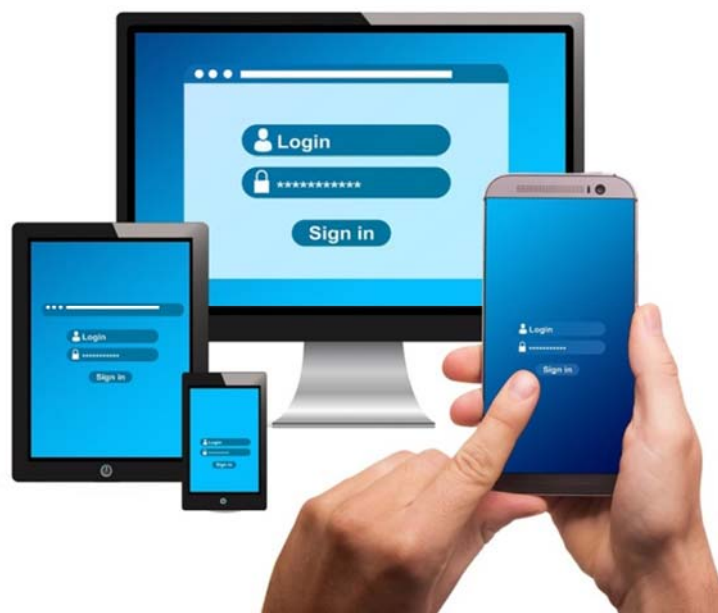


Bild: geralt via Pixabay

Selbstschutz: Passwörter – lang & komplex! Nicht im Duden, nicht Namen, nicht Geburtsdaten, nicht Tastaturmuster ... geschützt!



 Bild: monika1607
via Pixabay

1 2
3 4

 Bild: DavidZydd
via Pixabay



 Bild: Maklay62 via Pixabay

Die TOP 10 der Passwörter 2018 (nicht verwenden!)

USA

- 123456
- password
- 123456789
- 12345678
- 12345
- 111111
- 1234567
- sunshine
- qwerty
- iloveyou

<https://www.digitaltrends.com/computing/top-100-worst-passwords-2018/>

Deutschland

- 123456
- 12345
- 123456789
- ficken
- 12345678
- hallo123
- hallo
- 123
- passwort
- master

<https://t3n.de/news/beliebteste-passwoerter-2018-1133707/>

Selbstschutz: Passwörter – Hilfe per Passwort-Manager



 Bild: geralt via Pixabay

Selbstschutz: Zwei-Faktor-Authentifizierung



 Bild: geralt via Pixabay

 Bild: Clker-Free-Vector-Images
via Pixabay

Selbstschutz: Script-Blocker gegen unkontrollierte Verbindungen / Programme im Browser

ULD www.datenschutzzentrum.de

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	162	172	165	113
Open Hosts (*)	13	12	12	9

Verantwortungsdiffusion

Cybercrime, Hacking, Datenschutz: Was ist zu tun?!

Cybercrime, Hacking, Datenschutz: Was ist zu tun?!

41

Schutz der Daten: Verschlüsselung

sowohl bei der Übertragung
als auch für alle digitalen
Speichermedien
(z.B. USB-Sticks)

Bußgeld für Kontaktformulare ohne Verschlüsselung

30. NOVEMBER 2015 | 30 KOMMENTARE | VON DR. DATENSCHUTZ



Aus gegebenem Anlass soll an dieser Stelle noch einmal darauf hingewiesen sein, dass das Bayerische Landesamt für Datenschutzaufsicht derzeit Unternehmen in ihrem Zuständigkeitsbereich dahingehend überprüft, ob deren Webseiten, auf denen Kontaktformulare verwendet werden, anerkannte Verschlüsselungsverfahren implementiert haben. Die Anforderung betrifft aber nicht nur Webseiten mit Kontaktformularen.

Was passiert derzeit?

Das Bayerische Landesamt für Datenschutzaufsicht beanstandet zurzeit Webseiten, die trotz Verwendung von Kontaktformularen, mittels derer personenbezogene Daten elektronisch übertragen werden, keine angemessenen Schutzmaßnahmen wie beispielsweise eine verschlüsselte Datenübertragung implementiert haben.

<https://www.datenschutzbeauftragter-info.de/bussgeld-fuer-kontaktformulare-ohne-verschluesselung/>



Bild: Bru-nO via Pixabay

Cybercrime, Hacking, Datenschutz: Was ist zu tun?!

42

Überblick



- Warum Datenschutz?
- Cybercrime, Hacking & more
- Datenschutz & Datensicherheit
 - Meine Rechte
 - Was kann ich selbst machen?
 - Was muss sich ändern?
- Fazit

Neu: Nachweis- und Meldepflichten

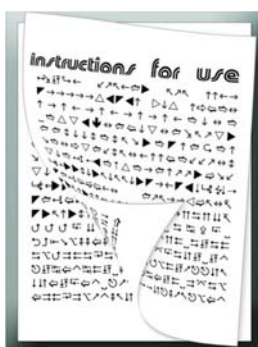


 Bild: geralt via Pixabay

- Der **Verantwortliche** ist verantwortlich
- Der **Auftragsverarbeiter** in seinem Bereich
- Ziel: **Risiko**beherrschung
- **Nachweis** des datenschutzkonformen Handelns



 Bild: Antrianis via Pixabay

- „Datenpanne“:
z.B. Daten gestohlen oder verloren
- **Meldung** an Aufsichtsbehörde
(innerhalb von 72 Stunden)
- Wenn Risiko für Betroffenen:
Benachrichtigung



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

Cybercrime, Hacking, Datenschutz: Was ist zu tun?!

45

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/>

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 Adressat 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 Silverpush 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.

Cybercrime, Hacking, Datenschutz: Was ist zu tun?!

46

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 collide

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 -1.49%}, 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.



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

THE LITTLE BLACK BOOK OF BILLIONAIRE SECRETS

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>

Cybercrime, Hacking, Datenschutz: Was ist zu tun?!

47

Training für selbstlernende Algorithmen?



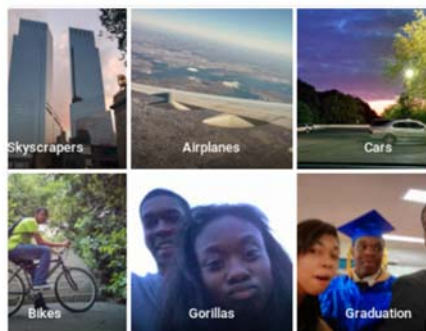
jackyalcine's like 55% in the Indie...

@jackyalcine

Folgen

Google Photos, y'all fucked up. My friend's not a gorilla.

Tweet übersetzen



18:22 - 28. Juni 2015

3.350 Retweets 2.281 „Gefällt mir“-Angaben



239 3,4 Tsd. 2,3 Tsd.

<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 Thadane 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

Cybercrime, Hacking, Datenschutz: Was ist zu tun?!

48

Welche Regeln? z.B. bei AI-Bots

COMPUTERWORLD
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>

Travis Korte
@traviskorte
Folgen

We should make AI sound different from humans for the same reason we put a smelly additive in normally odorless natural gas.

Bridget Carey @BridgetCarey
I am genuinely bothered and disturbed at how morally wrong it is for the Google Assistant voice to act like a human and deceive other humans on the other line of a phone call, using upspeak and other quirks of language. "Hi um, do you have anything available on uh May 3?" #io18
Diesen Thread anzeigen

13:44 - 8. Mai 2018

769 Retweets 1.725 „Gefällt mir“-Angaben

48 769 1,7 Tsd.

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

Cybercrime, Hacking, Datenschutz: Was ist zu tun?!

49

Aber: Bewusstsein muss mitwachsen

Bewusstsein der Nutzerinnen und Nutzer?

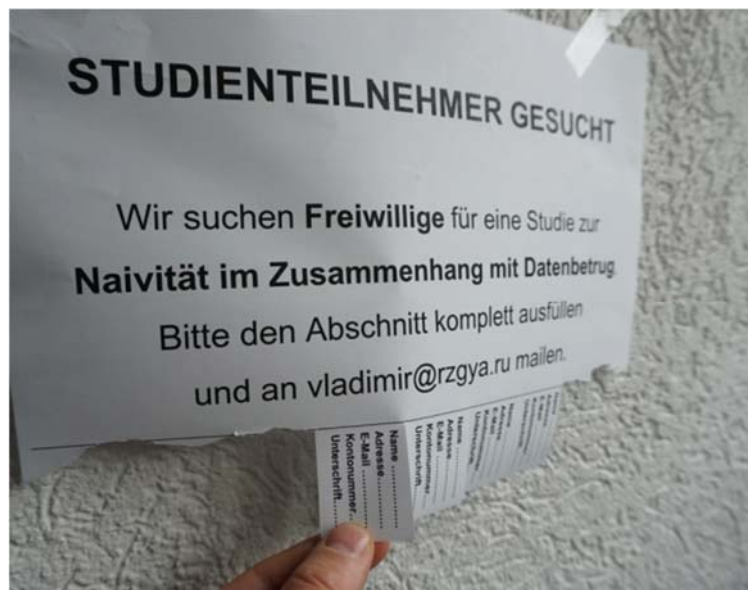


Bild: https://www.youngdata.de/fileadmin/youngdata/HM_datenschutz/00_seiteninhalt/bilder/Studeinteilnehmer2.jpg

Cybercrime, Hacking, Datenschutz: Was ist zu tun?!

50

Fazit



Bild: congerdesign via Pixabay

- Chancen durch „eingebauten Datenschutz“
- DSGVO als Startpunkt für Marktveränderungen
- Sie haben Rechte. Nehmen Sie sie wahr.
- Fragen Sie nach. Fordern Sie Datenschutz ein.



Vielen Dank für die Aufmerksamkeit!

Marit Hansen

<https://www.datenschutzzentrum.de/>