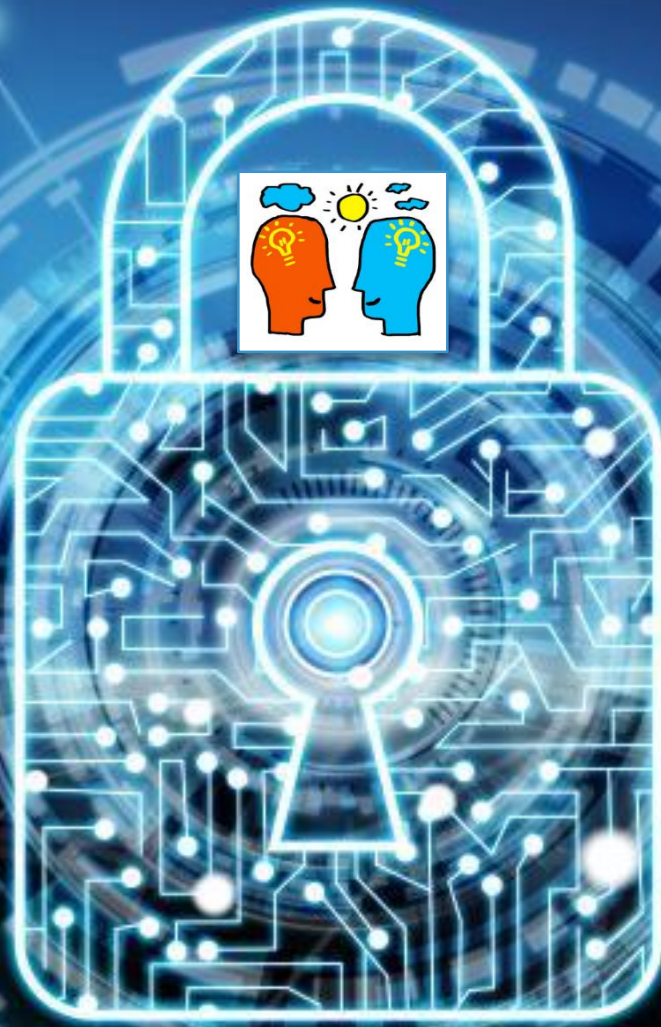


Datenschutz & Datensicherheit



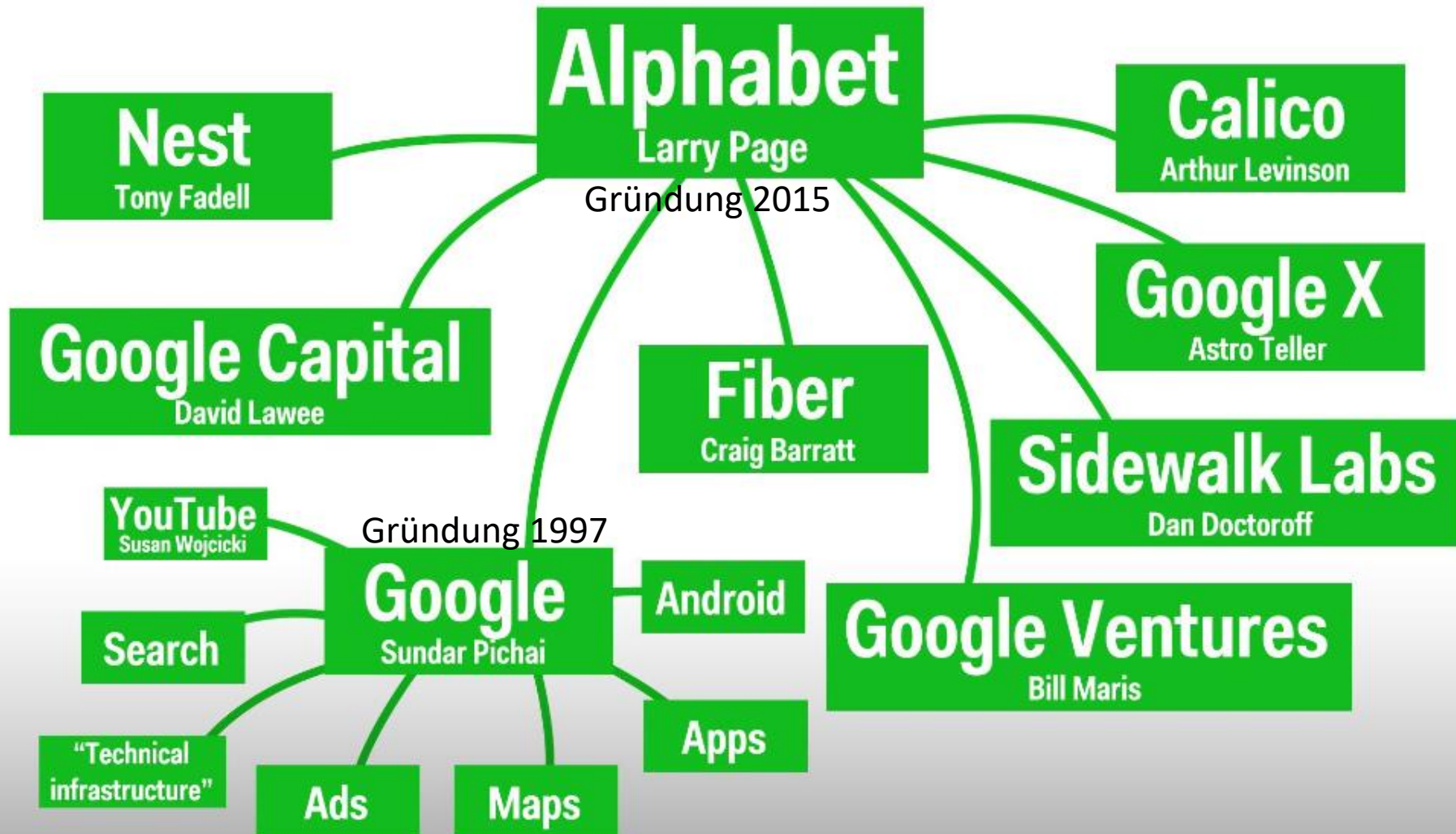
- **Daten: das neue Gold des digitalen Zeitalters**

Agenda

- Kann man mit den Daten der Anderen zum Milliardär werden?
- Das sind die Alphabet-Unternehmen
- Was ist das überhaupt: Datenschutz und Datensicherheit?
- 100%iger Datenschutz: nur noch für moderne Höhlenbewohner möglich?!
- Einführung: Datenschutzgrundverordnung (Video)
- Unterschiede von Datenschutz und Datensicherheit
- Warum wird ein Datenschutzgesetz benötigt?
- Persönliche Daten gehören der Person (Video)
- Datenschutzgesetze
- Datenschutzbeauftragter
- Datenschutzverordnung (DSGVO) als Chance
- Wann dürfen Daten erhoben, verarbeitet und genutzt werden?
- Datenschutz: Ich habe doch nichts zu verbergen?
- Big Data: Woher kommen die Daten?
- »Daten-Fetischisten« – Wer hat Interesse an den Daten?
- Mein digitales Ich
- Ist die Kontrolle der Daten noch möglich?
- Big-Data: automatisierte Persönlichkeitsanalyse
- Identitätsdiebstahl
- Big-Data: Profiling und Marketing
- Big Data: Jeder ist einzigartig
- Big Data: Was erzählt der Internet-Browser?
- Big Data: Was ist Tracking?
- Kekse und Cookies
- Big Data: Klassifikation, Scoring
- Big Data: Geolocation, Bewegungsprofile
- Big Data: Zusammenfassung
- Wer ist für die Datensicherheit verantwortlich?
- Backup und Datensicherheit
- Datenschutz und Windows 10
- Video: Identitätsdiebstahl



Kann man mit den Daten der Anderen zum Milliardär werden?



Die Struktur des Google-Imperiums (Alphabet Holding, vereinfachte Darstellung).

Am Beginn, konnten die Gründer Larry Page und Sergey Brin ihr »Gold« auf einer einzigen Diskette speichern.

2018 erzielte Google einen Betriebsgewinn von 36,5 Milliarden US-Dollar. Alphabet: Umsatz 136,8 Milliarden US-Dollar, Betriebsgewinn 26,3 Milliarden US-Dollar.

Quelle: www.heise.de



Das sind die Alphabet-Unternehmen

- **Access & Energy:** Betreibt unter anderem das Netzwerk »Project«.
- **Calico:** Das Unternehmen forscht tatsächlich am ewigen Leben.
- **Chronicle Cyber Security,** soll für mehr Sicherheit im Internet sorgen.
- **Deepmind:** Die Tochter rund um die Erforschung der Künstlichen Intelligenz.
- **Google Capital Alphabets Bank:** Stellt Kapital für andere Unternehmen zur Verfügung.
- **Google Ventures:** Der Risikokapitalgeber, über den Alphabet an Hunderten weiteren Startups beteiligt ist.
- **Jigsaw Think Tank** beschäftigt sich rund um die Sicherheit & Datenschutz im Internet.
- **Nest:** Die Alphabet-Tochter rund um das Smart Home.
- **Sidewalk Labs Innovationen** beschäftigt sich rund um Städtebau & Stadtprojekte.
- **Verily:** Thema Gesundheit, hat unter anderem die smarte Kontaktlinse und die Baseline Study hervorgebracht.
- **Waymo:** Entwicklung & Betrieb der selbstfahrenden Autos, könnte in Zukunft zur zweiten Cashcow (Geldkuh, Goldesel) werden.
- **X Labor** für hochexperimentelle Technologien, aus dem schon Waymo, Chronicle oder auch Google Glass stammte.

Der Großteil der heutigen Alphabet-Unternehmen waren Projekte oder Töchter der Google Inc., die durch die Umstrukturierung von dem Unternehmen getrennt wurden, das sich nun wieder rein auf die Kernkompetenzen konzentrieren kann.



Was ist das überhaupt: Datenschutz und Datensicherheit?

Datenschutz: Beim Datenschutz geht es um den Schutz von personenbezogenen Daten, wobei der Kernpunkt nicht der Inhalt oder die Bedeutung der Daten ist, sondern die informationelle Selbstbestimmung. Weisen die erhobenen, verarbeiteten oder genutzten Daten einen Personenbezug auf, so ist die Rede von *personenbezogenen Daten*, dabei können sie direkt (bestimmt), zum Beispiel der Name, oder indirekt (bestimmbar) unter Zuhilfenahme einer weiteren Informationsquelle, einer Person zugeordnet werden.

Hinweis: Der Datenschutz wird gesetzlich in der Datenschutz-Grundverordnung (DSGVO, 2018) geregelt.



Datensicherheit: Die Datensicherheit behandelt die Frage, was überhaupt möglich ist, um Daten sicher aufzubewahren. Kernpunkt der Datensicherheit sind Maßnahmen, um den Schutz der Daten vor Missbrauch (*Kontrollierbarkeit*), Verfälschung (*Integrität*), Verlust (*Verfügbarkeit*) und unberechtigter Zugriffe (*Vertraulichkeit*), zu gewähren.

Hinweis: Für die Datensicherheit, die über den Regelungen der DSGVO hinausgehen, ist jeder selbst verantwortlich.



*100%tiger Datenschutz: nur noch für moderne
Höhlenbewohner möglich?!*



Einführung: Datenschutzgrundverordnung



Die Datenschutz-Grundverordnung ist am 25. Mai 2018 europaweit in Kraft getreten.

Die Neuerungen betreffen alle Unternehmen, Organisationen und die EU-Bürger.



Unterschiede von Datenschutz und Datensicherheit

Datenschutz



- Schutz vor Datenmissbrauch und Datenpannen (Grundsätze der Datensparsamkeit, Zweckbindung)
- Schutz personenbezogener Daten
- Schutz der informationellen Selbstbestimmung (Privatsphäre)
- Gesetzliche Vorschriften
- **Theorie:** Beim Datenschutz wird dem theoretische Ansatz gefolgt »**Was soll erfüllt werden?**«.

Hinweis: Der Datenschutz wird gesetzlich in der Datenschutz-Grundverordnung (DSGVO, 2018) geregelt.

Datensicherheit

- Schutz von Daten
- Schutz vor Verlust, Zerstörung, Missbrauch, Zugriff durch Unberechtigte
- Technische Maßnahmen / Lösungen
- **Praxis:** Bei der Datensicherheit geht es unter anderem um die Umsetzung der Anforderungen des Datenschutzes, wobei der praktische Ansatz, »**Was ist möglich?**«, verfolgt wird.

Hinweis: Für die Datensicherheit, die über den Regelungen der DSGVO hinausgehen, ist jeder selbst verantwortlich.



Warum wird ein Datenschutzgesetz benötigt?

Ein allgemein respektiertes Gesetz für Datenschutz ist Voraussetzung, damit die Bürger ihre Daten auch übergeben.

Die Regierungen, Behörden und Unternehmen sind auf die Daten der Bürger existenziell angewiesen.

Ohne die Daten der Bürger können keine vernünftigen, auf reale Daten basierende, Entscheidungen getroffen oder Beschlüsse umgesetzt werden.



Persönliche Daten gehören der Person



Viviane Reding -
EU-Kommissarin
für Justiz,
Bürgerschaft und
Grundrechte

[...]
In der digitalen
Welt funktioniert
nichts ohne Daten.
**Wir brauchen die
Daten ...**

Aus dem
Dokumentarfilm
»Democracy - Im
Rausch der Daten«



Datenschutzgesetze

Zwar steht der Schutz der Daten in Deutschland sehr hoch, jedoch gibt es neben der **Datenschutz-Grundverordnung** (DSGVO) weitere Gesetze, deren Gültigkeit weder das **Bundesdatenschutzgesetz** noch die **Datenschutz-Grundverordnung** (DSGVO) außer Kraft setzen.

Überall wo es spezielle Regelungen gibt, gilt das spezielle Gesetz. Als Beispiele unter vielen dienen an dieser Stelle das **Telemediengesetz** (TMG), **Kreditwesengesetz**, **Geldwäschegesetz** oder das **Handelsgesetzbuch** (HGB).



Bedeutung der DSGVO für Personen: Die DSGVO gilt für alle Bewohner der Europäischen Union. Aber auch Daten die innerhalb der EU erstellt werden unterliegen der Datenschutz-Grundverordnung. Also auch wenn außereuropäisch tätige Unternehmen diese Daten nutzen oder verarbeiten möchten.

Hinweis: Landesdatenschutzgesetze gelten weiterhin, aber lediglich für Verwaltungen und Behörden.

Achtung: EU-Recht hat Anwendungsvorrang gegenüber dem nationalen Recht.



Datenschutzbeauftragter



- 1. Begriff:** Person, die die Einhaltung datenschutzrechtlicher Vorschriften zu überwachen hat. Einen Datenschutzbeauftragten haben alle Unternehmen zu bestellen, die mind. **fünf Arbeitnehmer** ständig mit der automatisierten oder **20 Arbeitnehmer** mit der nicht automatisierten Verarbeitung personenbezogener Daten beschäftigen. **Hinweis:** Die Nichtbestellung wird als Ordnungswidrigkeit (bis 50.000 Euro) geahndet.
- 2. Aufgabe:** ständige Kontrolle der Einhaltung des Bundesdatenschutzgesetzes (BDSG) in einem Unternehmen (Datenschutz); im besonderen durch Überwachung der verwendeten Software, Schulung der Mitarbeiter und beratende Mitwirkung bei der Personalauswahl. Der Datenschutzbeauftragte kann sich bei Zweifelsfällen an eine staatliche Aufsichtsbehörde (etwa den Regierungspräsidenten) wenden, die zugleich seine Tätigkeit kontrolliert.
- 3. Rechtsstellung:** Der Datenschutzbeauftragte ist unmittelbar der Geschäftsführung eines Unternehmens zu unterstellen. Er arbeitet weisungsfrei; seine Berufung kann nur aus wichtigem Grund widerrufen werden.

Hinweis: Ein Datenschutzbeauftragter kann Mitarbeiter dieser Organisation, des Unternehmens sein oder als externer Datenschutzbeauftragter bestellt werden.



Datenschutzverordnung (DSGVO) als Chance

Die DSGVO ist die perfekte Gelegenheit, eine bessere Kontrolle über Daten, dem Kapital eines jeden Unternehmens, zu ermöglichen.

Langfristig werden diejenigen Unternehmen, die diese Kulturverschiebung am erfolgreichsten umsetzen, einen Wettbewerbsvorteil gegenüber denjenigen haben, die sich weniger bemühen, engagieren.

Auch jenseits der DSGVO sollte die verantwortungsvolle Datenverarbeitung ein Grundprinzip für jedes Unternehmen sein.



Nicht gegen die DSGVO arbeiten, sondern proaktiv tätig werden:

- neue Leitlinien überwachen,
- die Datenaufzeichnung des Unternehmens auf den neuesten Stand bringen und verwalten,
- den Datengebrauch kontinuierlich überprüfen,

um die wichtigsten Vorteile der DSGVO zu nutzen. Diese sind:

- die Datensicherheit erhöhen,
- die Kundenorientierung verbessern und
- das Vertrauen der Kunden in die Marke stärken.



Wann dürfen Daten erhoben, verarbeitet und genutzt werden?



Was schreibt die Datenschutz-Grundverordnung vor:

- 1. Einwilligung:** Die Person hat vor der Erfassung der persönlichen Daten, in die Verarbeitung ihrer Daten eingewilligt. **Voraussetzung:** Die Person wurde umfassend über die Verarbeitung ihrer Daten informiert. Die Einwilligung kann schriftlich, mündlich oder elektronisch erfolgen. Der Widerruf der Einwilligung ist von Gesetzes wegen jederzeit möglich.
- 2. Vertragserfüllung:** Die Verarbeitung der Daten erfolgt zur Erfüllung eines Vertrages. Dazu zählen auch vorvertragliche Maßnahmen, z.B. das Zusenden einer Broschüre oder eine Angebotserstellung.
- 3. Rechtliche Verpflichtung:** Die Verarbeitung der Daten ist gesetzlich vorgeschrieben und muss deshalb erfolgen (Buchhaltung: Erfassung von Personendaten).
- 4. Schutz lebenswichtiger Interessen:** Die Verarbeitung der Daten erfolgt zum Schutz lebenswichtiger Interessen einer Person (z.B. Gesundheitswesen, Notfallmedizin).
- 5. Öffentliches Interesse:** Die Verarbeitung der Daten erfolgt im öffentlichen Interesse.

6. Berechtigtes Interesse: Ein Unternehmen hat ein berechtigtes Interesse an der Datenverarbeitung, welches gegenüber dem Interesse der betroffenen Person überwiegt (z.B. Betrugsprävention). Dieser letzte Punkt ist relativ unsicher geregelt, da hier die Interessen beider Parteien sorgfältig abgewogen werden müssen.



Datenschutz: Ich habe doch nichts zu verbergen? 1/3



»Harmlose« Informationen gibt es nicht!!

Das meiste, was man an Informationen hinterlässt, halten viele für völlig **harmlos**. Tatsächlich kann sich aber jede Information (**Stalking**: Telefon-Nr., Email-Adresse, Wohnort) gegen einen selbst richten.

Viele Websites sammeln zu gewerblichen Zwecken Informationen über ihre Nutzer.

Metadaten (IP-Adresse, Browser User Agent, Bildschirmauflösung, verwendete Spracheinstellung, ...) können hoch sensibel sein.

In nicht wenigen Fällen erlauben sie die Identifizierung einer Person (aus den Metadaten wird eine Identifikations-Nummer errechnet) und Analyse der Verhaltensweisen (Webseiten, Leseverhalten, Maus-Pointer-Bewegungen). Auch Unternehmen können so umfassend durchleuchtet werden.



Datenschutz: Ich habe doch nichts zu verbergen? 2/3



Der erste große Block von Rating-Interessenten sind die Marketing Leute. Sie sind diejenigen, die derzeit am heftigsten an diesen Techniken (Abfischen von Daten zur Bildung von Persönlichkeitsprofilen) arbeiten und sie auch bereits flächendeckend einsetzen.

Für Marketingzwecke ist es sehr interessant, die Interessen der Personen zu kennen, die gerade eine bestimmte Website besuchen.

Oft geschieht es heimlich. Aber warum? Wer hat Interesse an den Daten? Zu welchem Zweck werden die Daten genutzt? An wen werden sie weitergegeben?

Privatsphäre ist ein Menschenrecht ... und auch wer nichts zu verbergen hat, kann alles verlieren.

Rating-Gesellschaft: Der **gläserne Mensch** - überall bewertet, kategorisiert und bei Bedarf auch de-anonymisiert.



Datenschutz: Ich habe doch nichts zu verbergen? 3/3



Smartphones: Der Spion, den wir lieben.

Smartphones, Tablets, Notebooks werden für die Erstellung von Bewegungsprofile (Marketing, lokalisierte Werbung, Stauforschung, ...) benutzt.

Die Spione sind uns näher, als wir glauben: Hamburgs Flughafen wertet seit kurzem mithilfe der Handyprofile das Verhalten und die Interessen der Reisenden im Airport aus.

Eine spezielle Software analysiert anhand der Bewegungen von Mobiltelefonen mit aktiviertem Bluetooth-Funkchip auf den Meter genau, wo sich die Besucher gerade aufhalten, ob sie nach der Sicherheitskontrolle direkt zum Flugsteig gehen oder durch die Shops schlendern.

Der Nutzer merkt von all dem nichts.

Quelle: Handelsblatt – 01.07.2019



Big Data: Woher kommen die Daten?



Frage: Woher kommen die Daten?

Daten die wir freiwillig herausgeben (Befragungen, Telefonumfragen, Bewerbungen, ...), Benutzung von Kundenkarten, soziale Netzwerke und durch moderne technische Geräte.

Vier Kundenkarten besitzt jeder Deutsche im Schnitt. Allein damit legen wir detaillierte Spuren unserer Lebensgewohnheiten.

Key-Word für die Suchmaschine: Big-Brother-Awards



»Daten-Fetischisten« – Wer hat Interesse an den Daten?

1.

Staat | Geheimdienste

- ▶ Je nach Staat unterschiedliche Ziele
- ▶ Terror-Abwehr
- ▶ Unterdrückung politisch Andersdenkender
- ▶ [...]



2.

Unternehmen

- ▶ Aufbau von »Kunden-Profilen«
- ▶ Gewinnung vermarktbaren Erkenntnisse
- ▶ Manipulation durch passgenaue Werbung
- ▶ [...]



3.

Kriminelle

- ▶ Datenberge von Unternehmen / Staat äußerst interessant
- ▶ Zielgerichtete »Opfer-Selektion«
- ▶ Wer schützt die Datenberge eigentlich?
- ▶ [...]



Hinweis:
Abwesenheits-Nachrichten auf Twitter oder im Social Networking können für die Planung von Einbrüchen eingesetzt werden.



Mein digitales Ich 1/2

- ▶ **Unablässig** werden Daten von uns erhoben, gespeichert, verknüpft, bewertet und verkauft
- ▶ Das Vorgehen der Datensammler ist subtil und verdeckt
- ▶ Es entsteht ein nahezu **vollständiges** Profil

Verknüpfung von scheinbar harmlosen Daten mehrerer Anbieter, ergeben nicht mehr so harmlose Daten.

Ihr digitales Ich

- ▶ Wie viel verdienen Sie?
- ▶ Haben Sie Schulden?
- ▶ Leiden Sie an einer Blasenschwäche?
- ▶ Welches Auto fahren Sie?
- ▶ Was konsumieren Sie?
- ▶ Mit wem kommunizieren Sie?
- ▶ In welchem Viertel wohnen Sie?

[...]

Ein Drittanbieter hinter verschiedenen Webseiten, kann viele Daten sammeln. Nach einer Analyse, sind diese Daten nicht mehr so harmlos.



Mein digitales Ich 2/2


Fiktives Nutzerprofil

Name:..... Rainer **Hubertus**

Alter:..... 49 Jahre

Frau:..... Anna **Hubertus**



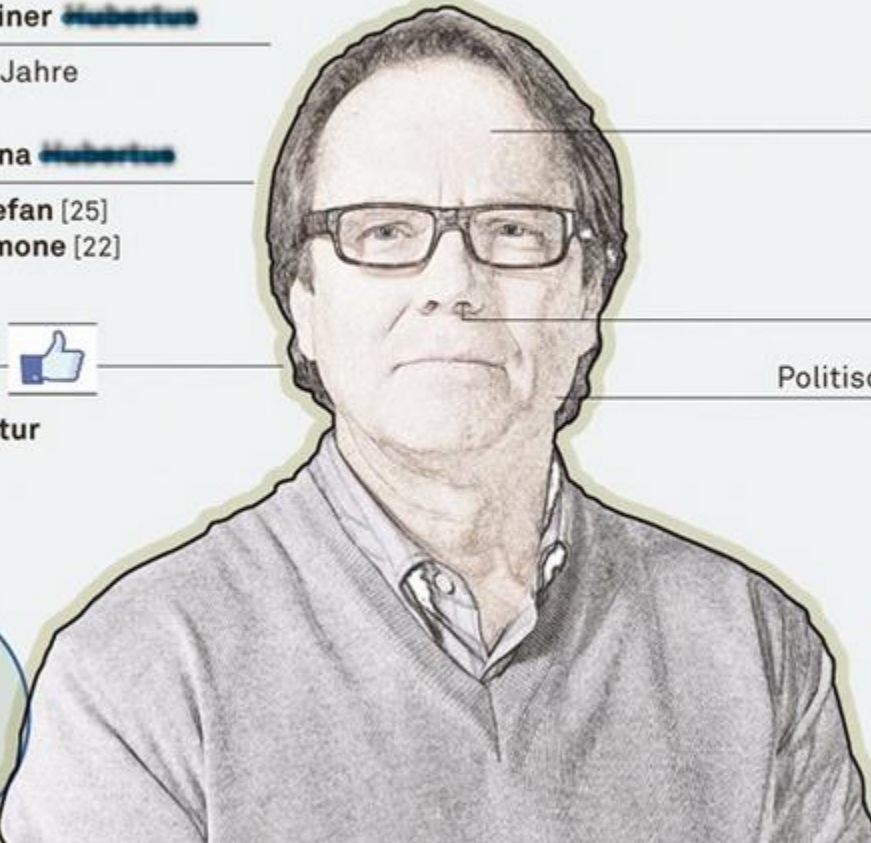
Kinder:..... Stefan [25]
Simone [22]

Interessen 

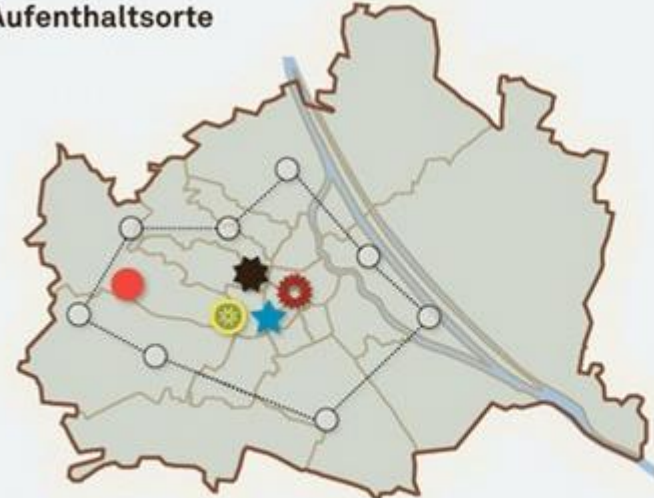
Wissenschaft
Kunst und Kultur
Sport

Krankheiten
Migräne
Allergien

Politische Ausrichtung
Mitte-links



Aufenthaltssorte



Algorithmen haben immer mehr Einfluss auf die Bewertung von Menschen.

- Arbeitsort [8-17 h]
- Lieblingsrestaurant
- Wohnung
- Besuchtes Nachtlokal
- Meistbenutztes Stadtgebiet
- Einkaufsrouten

Jahresgehalt
82.000 €

Freizeit
Joggen, Fitness, Kino
[läuft 21,3 Kilometer pro Woche]

 184 Freunde auf Facebook

 48 Follower auf Twitter

Facebook hat ein Patent angemeldet:

»Wenn ein Individuum einen Kredit beantragt, prüft der Gläubiger die Kreditwürdigkeit derjenigen Mitglieder in sozialen Netzwerken, die mit dem Individuum vernetzt sind.«

Hinweis: Bei jedem Internet-Besuch hinterlässt **jeder**, mehr oder weniger, harmlose Spuren. Die Verknüpfung dieser scheinbar belanglosen Daten mehrerer Anbieter, ergeben mit der Zeit nicht mehr ganz so harmlose Daten.



Ist die Kontrolle der Daten noch möglich?

1.

Bewusst

- ▶ Beitrag in einem sozialen Netzwerk
- ▶ Bild hochladen in die Cloud
- ▶ Versenden einer E-Mail
- ▶ Einkauf mit Payback-Karte
- ▶ [...]

Kontrolle vorhanden

2.

Unbewusst

- ▶ Cookies / IP-Adresse beim Surfen
- ▶ Smart-TV übermittelt Sehgewohnheit
- ▶ »Telemetrie-Daten« der Geräte
- ▶ SCHUFA-Scoring
- ▶ [...]

Eingeschränkte Kontrolle

3.

Heimlich

- ▶ Übermittlung eindeutiger IdNr.
 - ▶ Geräte-ID
 - ▶ IMSI-Nummer
- ▶ Smartphone-Apps
 - ▶ Adressbuch
 - ▶ SMS-Inhalte
- ▶ Adresshandel
- ▶ [...]

Kontrollverlust!

Hinweis: In der Internetgesellschaft sind bei den Kontakten zwischen eigentlich anonymen Menschen die tausende Jahre alte Verfahren zum Vertrauensaufbau entweder über direktes Kennenlernen oder über Reputation (Ansehen einer Person) in einem gemeinsamen Umfeld nicht mehr möglich.



Big-Data: automatisierte Persönlichkeitsanalyse

Datenübermittlung

- ▶ Zu welchem Zweck?
- ▶ Wer steckt dahinter?
- ▶ Wie geschieht es?
- ▶ [...]

Big-Data

- ▶ Speicherort?
- ▶ Für wie lange?
- ▶ Anonymisierung?
- ▶ [...]

Data-Dealing

- ▶ Weitergabe Daten?
- ▶ Zu welchem Zweck?
- ▶ Widerspruch?
- ▶ [...]



Die Realität



Datenhändler wissen nahezu **alles** über uns, wir hingegen fast **nichts** über sie



Bereits 2014 zeigt eine Studie über die Auswertung der Likes (engl.: gefallen), dass die Auswertung der Tweets (engl.: zwitschern, kurze Nachrichten) oder Facebook-Postings oder Facebook-Likes einer Person eine Persönlichkeitsanalyse gemacht werden kann, die bessere Aussagen macht als die von Familienangehörigen.

Quelle:

https://sicherheitskultur.at/Glaeserner_Mensch.htm



Identitätsdiebstahl



Wer soll schon etwas mit meinen Daten anfangen? Die interessieren doch keinen. Außerdem habe ich sowieso nichts zu verbergen.

Bei einem Identitätsdiebstahl ist unbedingt schnelles Handeln erforderlich. **Die eigene digitale Identität sollte einmalig bleiben.**

Gefährdete Daten, Informationen sind der vollständige Name, Geburtsdatum, Wohnort, Kreditkartennummer, Kontodaten und andere persönliche Informationen.

Wie erkennt man einen Identitätsdiebstahl?

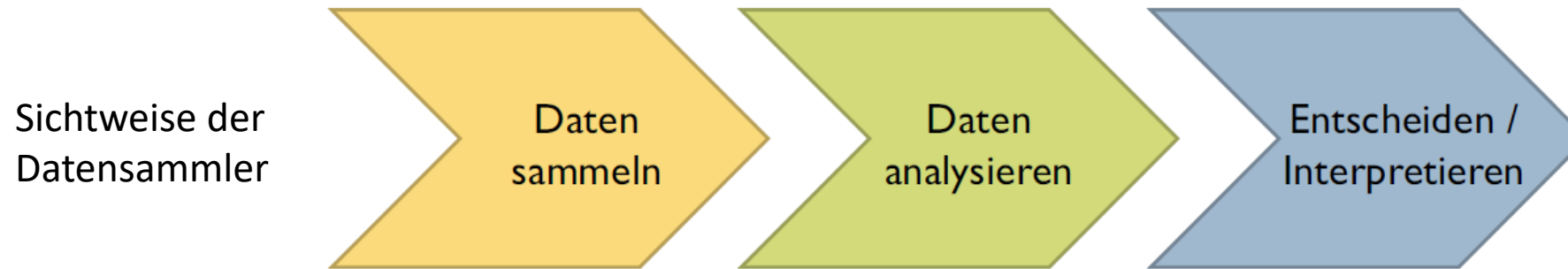
- verdächtige E-Mails
- Rechnungen über nicht bestellte Waren
- verdächtige Kontoauszüge
- nicht bestellte Lieferungen
- Post von Inkasso-Unternehmen

Um weiteren Betrug zu vermeiden, sind unverzüglich

- Kredit- und Bankkarte zu sperren
- der Online-Händler ist zu informieren
- die Passwörter sind zu ändern
- eine neue E-Mail Adresse anzulegen und die alte E-Mail Adresse zu löschen
- bei größeren Beträgen ist ein Rechtsanwalt oder ein spezialisierter Verein zu konsultieren
- Strafanzeige erstatten – dieser Schritt ist notwendig für den Versicherungsanspruch



Big-Data: Profiling und Marketing



Profiling bezeichnet die nutzbare Erstellung des **Gesamtbildes einer Persönlichkeit** für bestimmte Zwecke. Die Erstellung erfolgt durch das Zusammenführen von Daten, sowie deren anschließende Analyse und zweckbezogenen Auswertung. **Ziel des Profiling ist die Vorhersage von Verhalten und dessen zielgerichtete Beeinflussung und Veränderung.**

Im **Marketing** wird Profiling zur Erstellung von möglichst genauen und individuellen Kundenprofilen eingesetzt, um den Moment einer Kaufentscheidung möglichst genau vorherzusehen und beeinflussen zu können. **Hinweis:** Ohne Einwilligung des Betroffenen illegal (DSGVO Art. 6).

Professionelle Datensammler (Payback, Deutsche Post, Facebook, Microsoft, ...) setzen Profiling für die Erstellung von Persönlichkeits-, Verhaltens- oder Bewegungsprofilen, für die Bewertung der Kreditwürdigkeit, des Durchschnittseinkommen, Gesundheitszustand und vieles mehr ein.



Big Data: Jeder ist einzigartig

Tracking über Finger Printing

- ▶ Wiedererkennung eines Nutzers auch ohne Cookies (z.B. im privaten Surfmodus)
- ▶ Fingerabdruck: eindeutige Kombination von Browser-Eigenschaften (z.B. Betriebssystem, Sprache, Bildschirmgröße, installierte Plugins, ...)

Gegenmaßnahmen:

- Javascript abschalten
- Firefox Add-on: NoScript, Adblock Plus



<https://panoptick.eff.org>

Hinweis: Internet-Browser verraten vieles über ihren Benutzer. Solange der Nutzer vor diesem Browser sitzt, kann man ihn wiederfinden, auch wenn er versucht, seine Identität zu verschleiern. Deshalb versuchen die Netzwerke, alle nur erdenklichen Informationen aus dem Browser auszulesen.

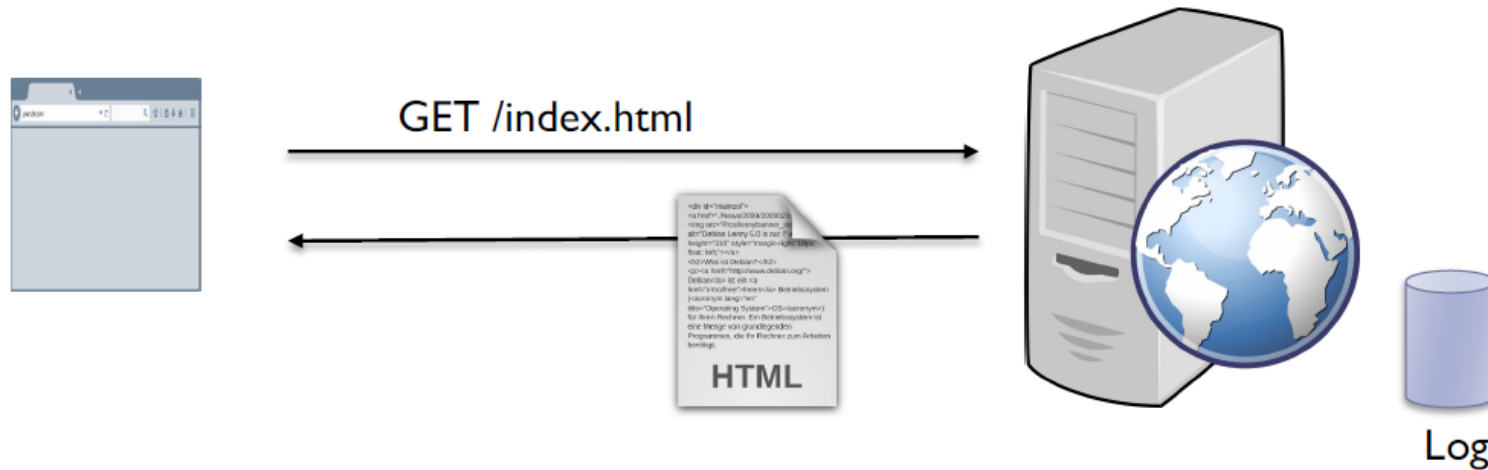


Big Data: Was erzählt der Internet-Browser?

Browser Tracking

► Erkennung

- von Zugriffen auf Websites („Wer liest Spiegel Online?“)
- sowie Wiedererkennung bzw. Zuordnung von Identitäten über verschiedene Zeiten, IP-Adressen und ggf. Geräte hinweg



► Techniken: Cookies, Finger Printing, Pixel Tracking

Browser-Tracker wie z.B. Google Analytics verfolgen Surfer über sämtliche Websites und Geräte hinweg und erstellen so detaillierte Persönlichkeitsprofile.

Pixel Tracking: Ein-Pixel-Bild, 1×1 gif-Bild, Clear.gif oder Web Beacon, sind kleine Grafiken in HTML-E-Mails oder auf Webseiten, die eine Logdatei-Aufzeichnung und eine Logdateianalyse ermöglichen.

Fingerprinting: Canvas-Fingerprinting macht sich die subtilen Unterschiede beim Rendering des Textes zu nutze. Diese Unterschiede lassen sich messen und in Sekundenbruchteilen in ein Fingerabdruck umrechnen, ohne dass der Anwender etwas davon bemerkt.



Big Data: Was ist Tracking?

Tracking mit Cookies

- ▶ Cookie = Textinformation, die vom Server zum Browser gesendet und später vom Browser zurückgeschickt wird
- ▶ Erkennung von Sitzungen über mehrere Aufrufe hinweg, z.B. für Warenkorb



Für Unternehmen und Agenturen sind die Informationen, welche über Tracking-Cookies gesammelt werden, überaus wertvoll.

Firefox Add-on z.B. Cookie Editor, Cookie Quick Manager

Mit dem Firefox Add-on NoScript kann man, die Webseite zur Datensparsamkeit anregen.

Super-Cookies oder Evercookies: Sie verwenden eine so große Sammlung von Methoden, dass es dem Benutzer nicht mehr möglich ist, alle Spuren zu löschen. Aus einem übersehenen Objekt, können die gelöschten Objekte wieder rekonstruiert werden. Super-Cookies oder Evercookies gehören zu den nicht löschbaren Cookies.



Kekse und Cookies

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	Session
▼ https://web.de (9)								
<input type="checkbox"/> um_cvt	74fefa51-64a9-47d6-...	.web.de	/		31	✓		✓
<input type="checkbox"/> SSLB	.0	.web.de	/		6			✓
<input type="checkbox"/> consentLevel	3	.web.de	/	1593238891	13			
<input type="checkbox"/> POPUPCHECK	1561789315037	web.de	/	1561789315	23		✓	
<input type="checkbox"/> clktype	AAOMAAEDjA	web.de	/	1593239040	17	✓	✓	✓
<input checked="" type="checkbox"/> ui_cid	rYgeeDopgmookiklBV9K	web.de	/	1593239040	26	✓		✓
<input type="checkbox"/> NGUserID	0a4a3211-84-156170...	.web.de	/	1592461441	32			
<input type="checkbox"/> inbox	false	.web.de	/	1561706642	10			
<input type="checkbox"/> wa	60d4e1cdd26d02cbff...	.web.de	/	1593239045	34	✓		✓
► https://adima.uimserv.net (2)								

Name: ui_cid
Domain: web.de
Path: /
Expiration (ISO): 27.06.2020
06:24:00.000
☒ HostOnly
☒ Secure
☐ Session
☐ HttpOnly

Firefox: Standard-Lebenszeit 0 - 90 Tage

Export - Reset Remove Expand

Firefox Add-on:
Cookie Editor,
Cookie Quick
Manager

Inhalt der Cookies:

- Session-ID
- Benutzer-ID
- verschlüsselte
Passwörter
- Lebenszeit des
Cookies
- verschiedene
Benutzer-
Informationen,
Benutzerprofil



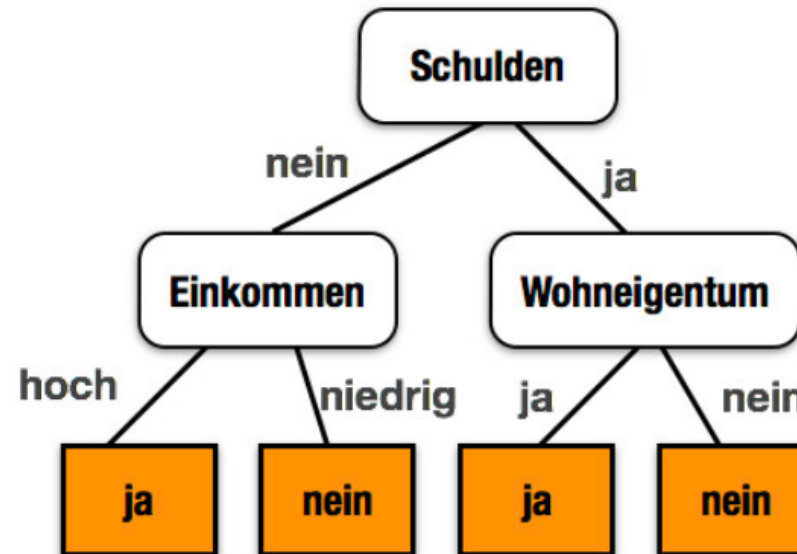
Big Data: Klassifikation, Scoring

Klassifikation

- ▶ Zuordnung von Objekten zu vorgegebenen Klassen, d.h. Vorhersage von Merkmalen (Klassenzuordnung) anhand bekannter Merkmale
- ▶ „Lernen“ des Klassifikationsmodells aus einer Trainingsmenge

Kunde	Schulden	Einkommen	Wohn-eigentum	Kredit-würdig
1	nein	hoch	ja	ja
2	nein	niedrig	nein	nein
3	ja	hoch	nein	nein
...

Beispiel: Ausgangspunkt, Konzeption für eine automatisierte Bewertung der Kunden



Die Aufgabe der Kundenklassifizierung ist die Aufteilung der Kunden in wichtige und unwichtige Kunden. Dazu sind die Kunden auf ihre aktuelle und vor allem auch auf die zukünftige Bedeutung für das Geschäft zu klassifizieren.

»Der Kunde ist König« ist ebenso ein überholtes Sprichwort wie »Kleinvieh macht auch Mist«.

Stichwort: ABC-Analyse



Big Data: Geolocation, Bewegungsprofile

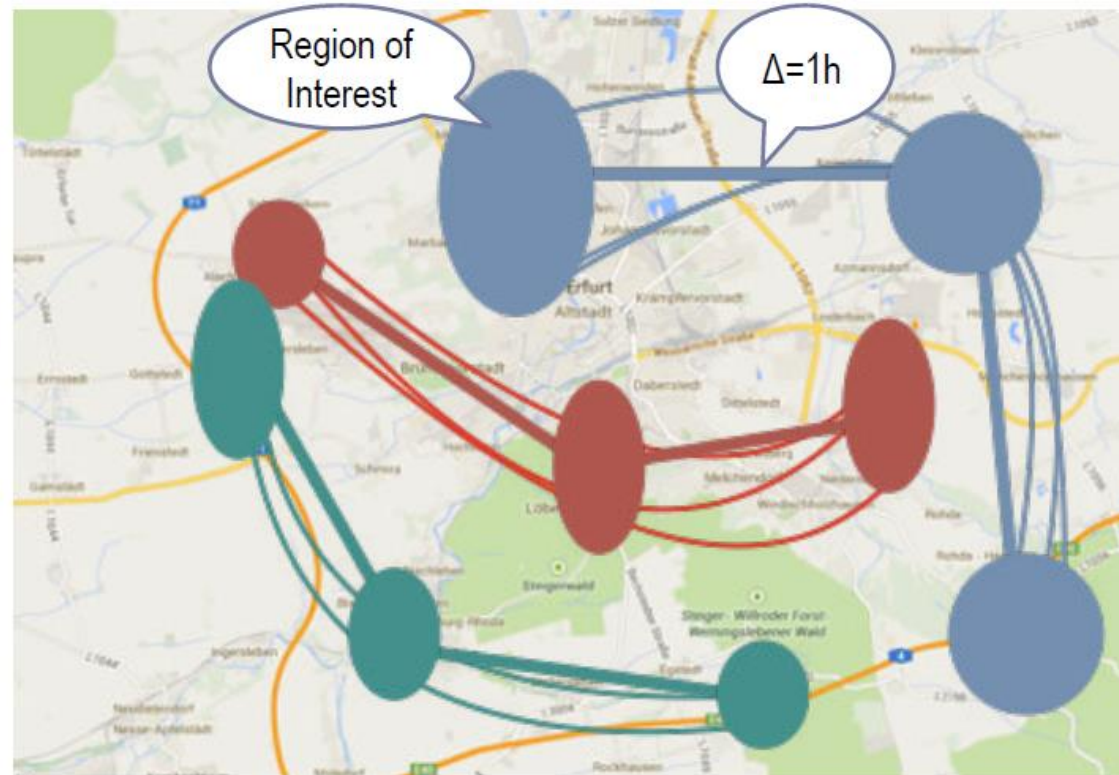
Bewegungsprofile

- ▶ Generierung georeferenzierter Daten durch
 - ▶ Navigationssysteme, GPS-Tracker, Smartphones (Mobilfunk, GPS), Fitness-Tracker, ...

#ID; Zeit; Ort
42; 15:00; 51.9, 10.4
42; 15:05; 51.9, 10.7
45; 15:06; 52.2, 9.8 ...

Ermittlung von persönlichen Daten:

- Wohn- und Arbeitsort (Branche, Beruf)
- Orte die häufiger aufgesucht werden (finanzielle Situation, Interessen, Gesundheit)
- Netzwerke



- Bei einer umfassenden Speicherung können auch bei anonymisierten Standortdaten Bewegungsprofile erstellt werden, mit denen sich bestimmte Personen identifizieren lassen.
- Speicherung der Bewegungsprofile über längere Zeiträume.
- Der Standortverlauf lässt sich deaktivieren. Standortdienste sollten nur bei Bedarf zugeschaltet werden.



Big Data: Zusammenfassung

Fazit: Risiken

- ▶ Persönliche Daten in **falschen Händen**
 - ▶ Surfgewohnheiten, politische Einstellung, Lebensweise, ...
 - ▶ Datensammlung ohne Wissen der Nutzer
- ▶ **Filterblase**: Personalisierung von Suchergebnissen, Nachrichten, etc.
 - ▶ Ranking/Filterung von Suchergebnissen bei Suchmaschinen durch Signale wie Suchhistorie, Nutzung, Ads, ...
 - ▶ Risiko der „intellektuellen Isolierung“ durch Einschränkung / Ranking der Suchergebnisse
- ▶ **Falsche Vorhersagen** durch fehlerbehaftete personenbezogene Daten
 - ▶ Kreditwürdigkeit bei Banken
 - ▶ Risikobeurteilung zu Gesundheit, Fahrweise etc. bei Versicherungen
 - ▶ „missbräuchliche“ Nutzung von Kreditkarten, Straffälligkeit, ...
- Kontrollverlust durch die zunehmende Anhäufung von personenbezogene Daten in fremde Hände.
- **Das Internet vergisst nichts!**
- **Achtung**: Wir leben in einer Informations-Gesellschaft. Digitalisierte Daten sind das neue Gold.



Wer ist für die Datensicherheit verantwortlich?



Datenschutz ist lästig!?

Datensicherheit umfasst jegliche **technische** und **organisatorische Maßnahmen**, die zur Datensicherheit gehören und die Datensicherheit vergrößern. Basisschutz liefern z.B. die klassischen Sicherheitswerkzeuge wie der Schutz vor Viren, Malware und Phishing.

Datensicherheit muss einen ins »Fleisch und Blut« übergehen, um nicht mehr lästig zu sein.

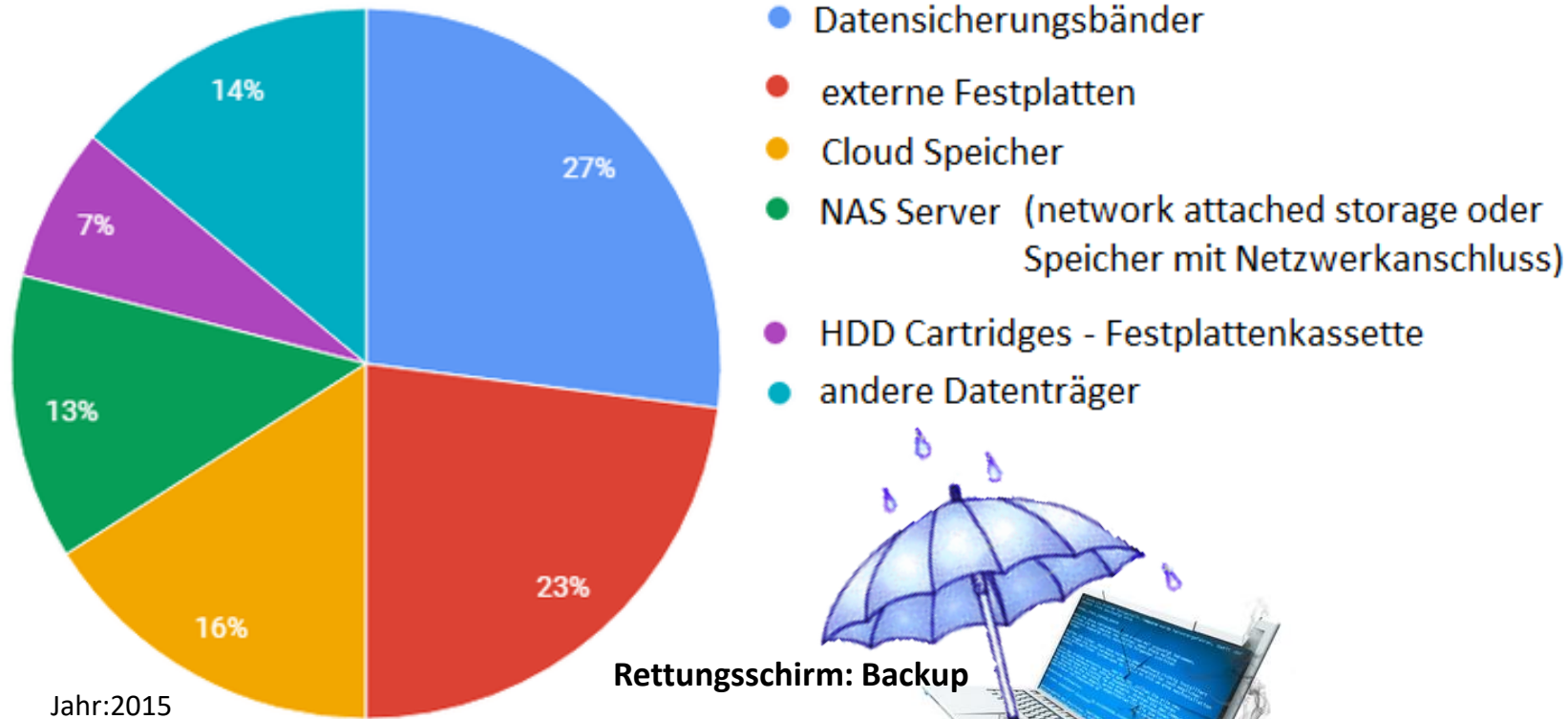
Hinweis: Wer seine eigenen Daten nicht schützen kann oder will, kann die Daten der Firma ebenfalls nicht schützen.

Datensicherheit ist Chefsache: Internetkriminalität nimmt immer mehr zu. Ebenso **Daten-** und **Wirtschaftsspionage**. Dabei wissen die meisten Chefs, dass sich nur mit funktionierenden und sicheren IT-Systemen Gefahren wie **Informations-** und **Datenverluste** abwehren lassen. Doch immer noch wird der Datensicherheit eine zu geringe Bedeutung beigemessen. Und solange die Devise »Sicherheit kostet Geld und bringt keinen Nutzen« gilt, wird sich daran auch nichts ändern. Dabei ist IT-Datensicherheit längst Chefsache und der Datenschutz in Unternehmen mehr als nur eine teure Pflichtaufgabe.



Backup und Datensicherheit 1/3

Eingesetzte Backup-Medien



- Ob privat oder geschäftlich, Daten sind wertvoll und müssen gesichert werden.
- Für die Datensicherung gibt es verschiedene Backup-Methoden und Backup-Strategien.
- Die meisten Backup-Lösungen stellen dafür drei Methoden zur Verfügung: Die vollständige, die differenzielle und die inkrementelle Datensicherung.

- Für die Wahl der optimalen Hard- und Softwarelösung (Backup-System), sollte man sich ausreichend Zeit nehmen und sich nicht vom Preis leiten lassen. Mit dem Verlust wichtiger Daten, kann man sich schon auf den Besuch des Insolvenzverwalters »freuen« oder auch nicht.



Backup und Datensicherheit 2/3

Backup-Ratgeber: Welche Methode ist die richtige für mich?

Vollsicherung: Mit der Vollsicherung, wird eine tägliche System-Sicherung mit steigendem Speicherbedarf erstellt.

Die Vollsicherung ist nicht nur die einfachste Art der Datensicherung, sondern auch die wohl effektivste Backup-Methode. Bei der Vollsicherung werden alle Daten gesichert. Bei Bedarf wird das System aus einer einzigen Datei wiederhergestellt.

Vorteile: Eine einfache Sicherung und Wiederherstellung mit nur einer Backup-Datei.

Nachteile: Zeitaufwendiger Backup-Prozess mit einem sehr hohen Speicherbedarf.

Differenzielle Datensicherung: Bei der differenziellen Datensicherung wird zunächst eine Vollsicherung erstellt und danach - etwa einmal die Woche - eine Teilsicherung. Bei der Teilsicherung werden dann nur die Daten gesichert, die seit der letzten Vollsicherung verändert oder neu erstellt wurden.

Die differenziellen Backups werden Tag für Tag größer und umfangreicher, da mit jeder differenziellen Datensicherung die in einer vorherigen differenziellen Datensicherung bereits abgesicherten Daten, erneut gesichert werden.

Vorteile: Die differenzielle Sicherung benötigt weniger Speicherplatz – im Vergleich zu einer Vollsicherung, kann aber deutlich schneller als eine Vollsicherung durchgeführt werden.

Nachteile: Dateien, die nach der Vollsicherung nur einmal verändert wurden, werden mit jedem differenziellen Backup erneut gesichert.



Backup und Datensicherheit 3/3



Hinweis: Wichtige Backup-Datenträger oder dessen Kopien sollte man an einem sicheren, externen Ort lagern.

Inkrementelle Datensicherung: Die inkrementelle Datensicherung ähnelt der differenziellen Datensicherung - mit einem entscheidenden Unterschied. Zwar geht dem inkrementellen Backup auch eine Vollsicherung voraus, danach werden mit jeder Sicherung aber nur die Daten gesichert, die seit der letzten inkrementellen Sicherung erstellt oder verändert wurden.

Dadurch sind die einzelnen Datensätze alle miteinander verknüpft und zur Wiederherstellung der Daten benötigt man die erste Vollsicherung sowie alle nachfolgenden inkrementellen Sicherungen.

Vorteile: Inkrementelle Sicherungen haben einen geringen Speicherbedarf und können schnell angefertigt werden.

Nachteile: Zur Wiederherstellung wird die Vollsicherung inklusive **aller** inkrementellen Sicherungen benötigt.



Datenschutz und Windows 10

Was will Microsoft über die Windows-10-Benutzer wissen?

Die folgende Liste entstammt der Datenschutzerklärung von Microsoft mit Stand vom Juli 2018. Bei jeder Installation oder Upgrade müssen die Benutzer dieser Datenschutzerklärung zustimmen, ansonsten wird die Installation oder das Upgrade abgebrochen.

- Name und Kontaktdaten
- Anmeldeinformation
- demografische Daten (z.B. Alter, Geschlecht, Land und die bevorzugte Sprache)
- Zahlungsdaten
- Daten über Lizenzen und Abonnements
- Interaktionen
- Geräte- und Nutzungsdaten
- Zahlungsmethoden und Aktivitätsverlauf des Kontos
- Browserverlauf
- Geräte-Konnektivitäts- und Konfigurationsdaten
- Fehlerberichte
- Leistungsdaten

- Problembehandlung und Daten
- Interessen und Favoriten
- Nutzungsdaten von Inhalten
- Suchvorgänge und Befehle
- Sprachdaten
- Text, Eingabe- und Freihanddaten
- Bilder
- Kontakte und Beziehungen
- Soziale Daten (Vorlieben, Abneigungen, Ereignisse, Kontakte zu anderen Personen)
- Positionsdaten
- andere Angaben
- Inhalt (Mitteilungen z.B. per Mail, Audio, Video, Text oder Dateien)
- Videos und Aufzeichnungen (bezieht sich auf Aufnahmen in Microsoft-Gebäuden)
- Feedback und Bewertungen

Quelle: Zeitschrift »PCWELT « Sonderheft – Notfall-Handbuch 2019



Datenschutz und Windows 10

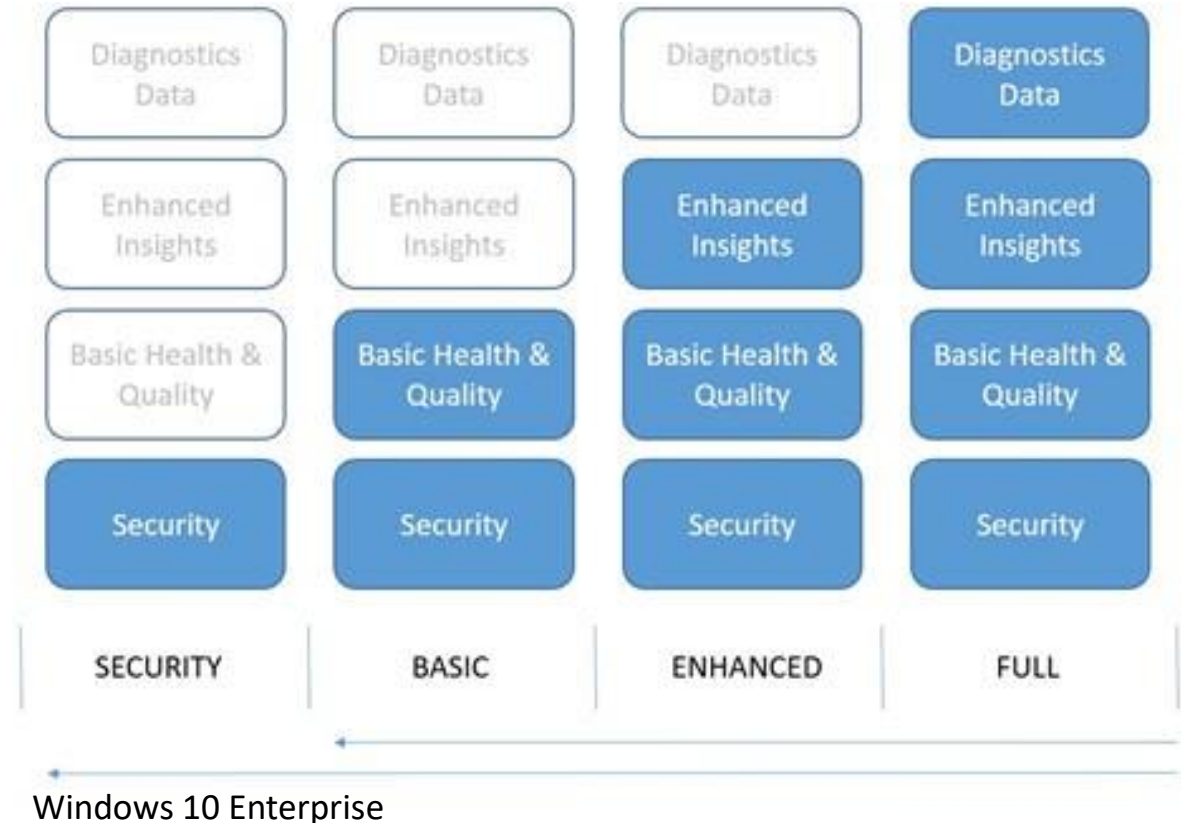
Telemetrie

Nach Einschätzung des BSI hat die in Windows 10 eingebaute Telemetrikomponente umfassende Möglichkeiten, auf System- und Nutzungsinformationen zuzugreifen und diese an Microsoft zu versenden. Nutzer können zwar unterschiedliche Telemetrie-Level einstellen, aber eine eindeutige Zuordnung der übertragenen Informationen zu diesen Stufen sei nicht möglich: Windows lädt mehrmals pro Stunde Konfigurationsdaten nach und ordnet damit die vorhandenen Telemetriequellen diesen Levels im laufenden Betrieb **dynamisch** zu.

Quelle:

<https://www.heise.de/newsticker/meldung/BSI-untersucht-Sicherheitseigenschaften-von-Windows-10-4227139.html>

Telemetrie ist die Übertragung von Messwerten eines am Messort befindlichen Sensors zu einer räumlich getrennten Stelle. An dieser Empfangsstelle können die Messwerte entweder nur gesammelt und aufgezeichnet oder auch sofort ausgewertet werden.



Datenschutzerklärung von Microsoft

Letzte Aktualisierung: Juni 2019 [Neuigkeiten](#)

✓ [Alles erweitern](#)

🖨️ [Drucken](#)

Datenschutzerklärung von Microsoft

<https://privacy.microsoft.com/de-de/privacystatement>
oder in den »Einstellungen« von Windows 10

Der Schutz Ihrer Daten ist uns sehr wichtig. In dieser Datenschutzerklärung wird erläutert, welche persönlichen Daten von Microsoft erfasst, wie und wofür das Unternehmen sie verwendet.

[...]

- Das BS Windows wird lizenziert, nicht verkauft. Unter diesem Vertrag gewährt Microsoft den Benutzern das Recht, die Software auf einem Gerät zur Verwendung zu installieren und auszuführen, solange alle Bestimmungen des Vertrages eingehalten werden.

- Dieser erste Satz aus der Datenschutzerklärung von Microsoft ist fast zu ehrlich.
- Diesen Satz kann man aus der Sichtweise der Benutzer und aus der Sichtweise von Microsoft lesen.
- In der heutigen Informationsgesellschaft (Big Data, Data Mining) sind die Daten der Menschen das neue Gold der Firmen und Organisationen.



Datenschutz und Windows 10

Mo, 3. Juni 2019, 08:14



Gesellschaft::Politik/Recht

Russisches Militär will Windows durch Astra Linux ersetzen

Das russische Militär könnte bald komplett von Windows auf das in Russland entwickelte Astra Linux umsteigen. Bereits im April erfolgte die Sicherheitsfreigabe für die höchste Geheimhaltungsstufe.

Von Ferdinand Thommes

Astra Linux soll schon bald beim russischen Militär das bisher verwendete Microsoft Windows als Betriebssystem ablösen. Astra Linux wurde in Russland auf der Basis von Debian entwickelt, um die Bedürfnisse an die Informationssicherheit des russischen Militärs und der Geheimdienste des Landes zu erfüllen. Die erweiterte Version Astra Linux »Smolensk Edition« in Version 1.6 hat die Zertifizierung des russischen Verteidigungsministeriums erhalten und erfüllt einen Grad an Datensicherheit, der auch die höchste Sicherheitsstufe einschließt.



- Im Internet wird auf keiner Webseite berichtet, dass Windows 10 eine Sicherheitsfreigabe erhalten hat.
- Um Windows 10 für Regierungen, Firmen und Organisationen in Bezug auf den Datenschutz sicher zu machen, wartet auf hochqualifizierte Administratoren viel Arbeit.



Datenschutz und Windows 10

https://netzpolitik.org/2018/politik-zur-datenschleuder-windows-10-aufsichtsbehoerden-muessen-handeln/#spendenleiste

133% ...

Suchen...



NETZPOLITIK.ORG

Datenschutz

Politik zur Datenschleuder Windows 10: Aufsichtsbehörden müssen handeln

Das Bundesamt für Sicherheit in der Informationstechnik bestätigte kürzlich offiziell, dass Windows 10 umfangreiche Nutzungsdaten an den Hersteller Microsoft sendet. NutzerInnen könnten sich davor nicht effektiv schützen. Wir haben Politik und Verwaltung gefragt, was sie mit den Ergebnissen anfangen.

29.11.2018 um 08:00 Uhr

[...] Das Betriebssystem Windows 10 wirkt wie ein einziger Datenschutz-Unfall. [...]



Datenschutz und Windows 10

SiSyPHuS Win10 - BSI nimmt Windows 10 unter die Lupe

Quelle: <https://curius.de/blog/32-betriebssysteme/windows/468-sisyphus-win10-bsi-nimmt-windows-10-unter-die-lupe>

Verfasst am 01. Juni 2019. Veröffentlicht in [Windows](#)

Windows 10 ist ein Datenschutz-Unfall. Diese Meinung vertreten seit Veröffentlichung der aktuellen Version des Microsoft-Betriebssystems nicht wenige. Kaum jemand hat sich aber so tief in das System eingearbeitet wie das BSI mit seinem Projekt **SiSyPHuS Win10**.

Das Thema ist nicht neu. Die [ersten Meldungen](#) diesbezüglich kamen schon aus dem vergangenen Oktober. Das gesamte Projekt lässt sich das [BSI einiges kosten](#), was aber auch an der Bedeutung von Windows für die Verwaltung liegt.

In der ersten Ankündigung gab das BSI schon einen Einblick in das Drama:

Den Analysen zufolge hat die in Windows 10 "ab Werk" eingebaute Telemetrikomponente umfassende Möglichkeiten, auf System- und Nutzungsinformationen zuzugreifen und diese an den Hersteller zu versenden. Obwohl die Nutzer unterschiedliche Telemetrielevel einstellen können, ordnet der Telemetriedienst die vorhandenen Telemetriequellen diesen Leveln im laufenden Betrieb dynamisch zu. Hierfür lädt der Dienst mehrmals pro Stunde Konfigurationsdaten nach. Eine Unterbindung der Erfassung und Übertragung von Telemetriedaten durch Windows ist technisch zwar möglich, für den einfachen Anwender allerdings nur schwer umzusetzen. Zudem haben auf dem Rechner installierte Anwendungen wie der Internet Explorer und Microsoft Office die Möglichkeit, auch ohne den zentralen Telemetriedienst des Betriebssystems Telemetriedaten zu erfassen und an den Hersteller zu versenden.

Quelle: [BSI Pressemitteilung vom 20.11.2018](#)

BSI ... Bundesamt für Sicherheit in der Informationstechnik

SiSyPHuS Win10 ... Studie zu Systemaufbau, Protokollierung, Härtung und Sicherheitsfunktionen in Windows 10

Telemetrie ... Telemetrie (nutzt die Funktionen von Windows Event Tracing - ETW) ist die Übertragung von Messwerten eines am Messort befindlichen Messfühlers zu einer räumlich getrennten Stelle. Telemetrie nutzt die Funktionen von Windows Event Tracing (ETW).



Video: Identitätsdiebstahl



Identitätsdiebstahl
kann jeden treffen.

Cyberkriminelle
rauben
Internetnutzern
gleich ganze
Identitäten und
missbrauchen sie für
ihre Zwecke.

In den sozialen
Medien finden sie
alles: vom Profilbild
über den Job bis hin
zum Wohnort und
den Hobbies ihres
Opfers.





Vielen Dank für ihre Aufmerksamkeit

Fragen?