

Digitale Selbstverteidigung

AUGE-Workshop

30.11.2015



CryptoParty Graz



Wer ist die CryptoParty Graz ?

Vorstellung CryptoParty Graz

CryptoParties gibt es seit 2012 auf der ganzen Welt, in Graz seit 2013

Die **CryptoParty Graz** besteht aus einer Kerngruppe von etwa 10
Personen, die sich regelmäßig treffen

<https://cryptoparty.at/graz>

CRYPTO
PARTY



Unsere „Themen“

- Bewusstseinsbildung
- Email-Verschlüsselung
- Web-Tracking und Gegenmaßnahmen
- Passwörter und Tresore
- Festplatten-Schutz durch Verschlüsselung
- Sicherheit am Handy



Cryptoparty-Montag

(1. Montag im Monat)

Nächste Termine:

- 7.12.2015
- 4.1.2016
- 1.2.2016
- 7.3.2016

Ab 19 Uhr im **Spektral**,

Lendkai 45



Hilfe, Tipps, Party und mehr !



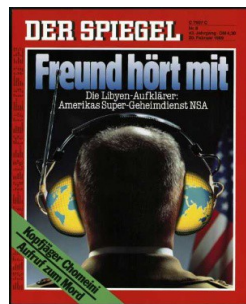
Überwachung

Seit den Aufdeckungen von Edward Snowden wissen wir, dass unsere digitale Kommunikation weltweit von Geheimdiensten überwacht wird.

Manche wussten / vermuteten das auch schon vorher...

vor 25 Jahren:

- z.B. Der Spiegel vom 20.2.1989
 - “NSA: Amerikas großes Ohr“
 - <http://www.spiegel.de/spiegel/print/d-13494509.html>



Echelon-System = globales elektronisches Aufklärungssystem

- Siehe z.B. Erich Moechel, www.fuzo-archiv.at/artikel/1652079v2



Totalüberwachung

- Warum wird überwacht ?
- Wer überwacht uns?
- Wo wird überwacht ?
- Was kann man/frau dagegen tun ?



Warum Überwachung ?

- **Staatliche Überwachung:**
 - Schutz vor Verbrechen und Terrorismus („Krieg gegen Terror“)



Warum Überwachung ?

Firmen als Überwacher:

- „Wir wollen den KundInnen maßgeschneiderte, optimierte Produkte anbieten.“
- „Deshalb sollten wir die Wünsche der KundInnen genau kennen.“
- Und deshalb sammeln wir
 - Interessensprofile
 - Tätigkeitsprofile
 - Persönlichkeitsprofile

Prognosen über zukünftiges Verhalten können gemacht werden



Wer sammelt Daten ?

- Der Staat als Datensammler
- Geheimdienste als Datensammler
- Firmen als Datensammler
- Internet der Dinge
- Kriminelle
- Ich selbst



Der Staat als Datensammler

- **Vorratsdatenspeicherung** in Ö und EU gekippt, nun aber wieder in Diskussion (wurde in Deutschland wieder eingeführt)
 - keine präventive Wirkung gegen Terroranschläge
- Melderegister der Gemeinden
- Finanzämter
- Versicherungen
- Grundbuch
- ...

Verknüpfung von online und offline Daten



Geheimdienste als Datensammler

Geheimdienst NSA:

- NSA speichert **täglich 6 Milliarden Metadaten** (Emails, Telefonate, SMS)
- das entspricht etwa der Menge von 500 Millionen Büchern pro Tag
(Quelle: Heise-Newsticker 31.3.2014)
- aktuell anfallende Datenmenge im Internet:
 $2,5 \cdot 10^{18}$ Bytes pro Tag = 2.500.000 Terabytes pro Tag

(Quelle: www1.logistik.fh-dortmund.de/IT-Sicherheit/IW_und_Ueberwachungsstaat.pdf)



Geheimdienste als Datensammler

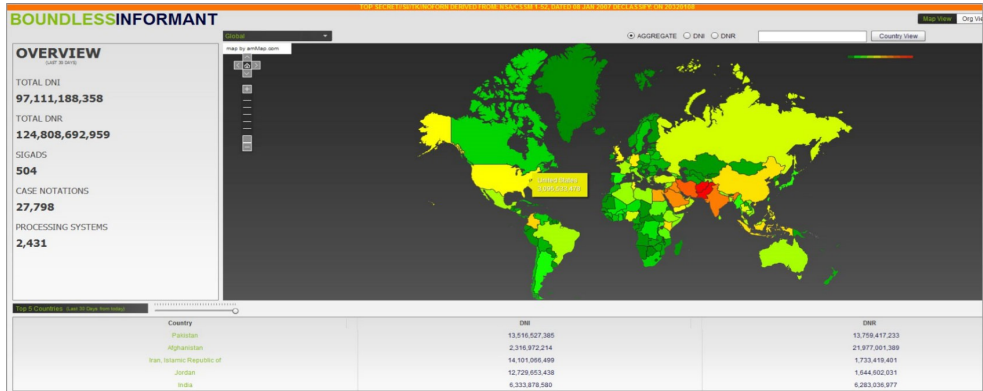
Britischer Geheimdienst GCHQ:

- Speicherte 2012 **täglich 50 Milliarden Metadaten** (Emails, Telefonate, SMS, Suchabfragen, Telefonstandorte, ...)
- Bis Jahresende 2012 war eine Verdopplung der Datenmenge geplant
- Die Datensammlung erfolgt bei grossen Webseiten
- Auswertung geschieht beinahe in Echtzeit
- Metadaten werden 1 – 6 Monate gespeichert, Kommunikationsinhalte 3 - 30 Tage lang
- Diese Daten stehen auch anderen Geheimdiensten zur Verfügung

Quelle: The Intercept, Der Standard 25.9.2015



Boundless Informant (eines der Überwachungsprogramme der NSA)



During a 30-day period, 97 billion internet data records (DNI) and 124 billion telephony data records (DNR) were collected.

Quelle: http://en.wikipedia.org/wiki/Boundless_Informant



PRISM (eines der Überwachungsprogramme der NSA)



Current Providers

- Microsoft (Hotmail, etc.)
- Google
- Yahoo!
- Facebook
- PalTalk
- YouTube
- Skype
- AOL
- Apple



What Will You Receive in Collection
(Surveillance and Stored Comms)?

It varies by provider. In general:

- E-mail
- Chat – video, voice
- Videos
- Photos
- Stored data
- VoIP
- File transfers
- Video Conferencing
- Notifications of target activity – logins, etc.
- Online Social Networking details
- **Special Requests**

Complete list and details on PRISM web page:
Go PRISMFAA

TOP SECRET//SI//ORCON//NOFORN

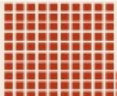


Firmen als Datensammler

- Bei **Anmeldung im Internet**:
 - Sind die Angabe von Name, Vorname, Straße, Ort, Postleitzahl und E-Mail- Adresse nötig ?!?
- Firmen benötigen **Kundendaten** für „Rechtsgeschäfte“ (z.B. Online-Einkauf)
 - Wohin sonst sollen sie die Ware schicken?
 - Woher sonst sollen sie ihr Geld bekommen?
- **Daten-Sammelwut** :
 - Bei vielen Anmeldungen würde nur ein Bruchteil der abgefragten Informationen genügen !



Die Macht der Internetkonzerne

	Umsatz ¹ 2013	Gewinn ¹ 2013	Beschäftigte 2013
 Apple	 191,9	 41,6	 80.300
 amazon	 83,7	 0,3	 117.300
 Google	 67,2	 14,5	 47.756
 Facebook	 8,8	 1,7	 6.337
Alle 20 ATX-Konzerne	 113,1	 5,1	 334.450

Quelle: „Vorstandsvergütung in ATX-Unternehmen“ AK (2014);
 U.S. Securities and Exchange Commission; Statista; AK/ÖGB-Darstellung.

¹ Mrd. Euro

Firmen als Datensammler

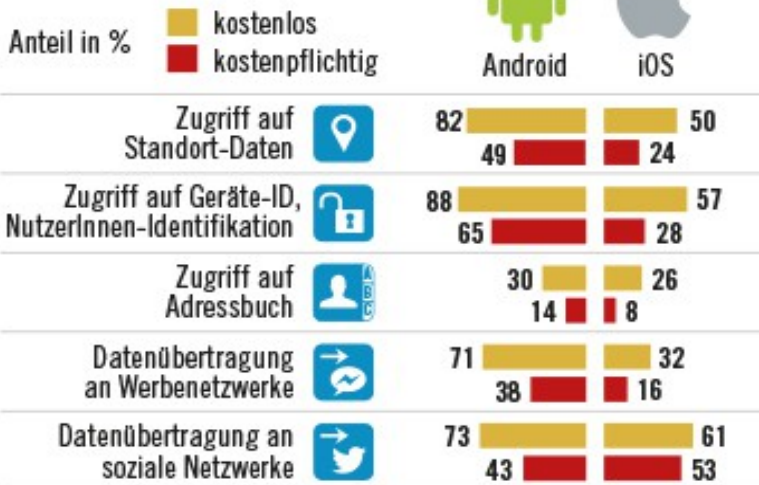
Daten sammeln als Geschäftsmodell

Wenn der Dienst gratis ist, sind wir die Waren
(aber auch, wenn er nicht gratis ist...)



Apps: Spione in der Hosentasche

Top-100-Apps



5



Internet der Dinge

Gemessen und gespeichert wird, alles, was möglich ist:

- Smartmeter – Stromverbrauch
- Wasserverbrauch
- Kühlschränke: kennen unser Ernährungsverhalten
- Autoversicherung: Sensoren im Auto erfassen Fahrverhalten
- Smart Cities



Kriminelle

- Kriminelle, die an unsere Kennwörter und Bank-Konten heranwollen

z.b.

- Phishing-Mails
- Nigeria-Connection

Oder:

Festplatte wird durch Schadprogramm verschlüsselt

Und man wird erpresst, das Entschlüsselungs-Kennwort zu bezahlen



Ich

Wir selber „liefern“ viele Daten:

- durch Postings in Sozialen Netzen
- durch Verwendung von



- Kreditkarten
- Kundenkarten
- Fitness-Life-Tracker
- Flugbuchungen
- ...



Was passiert mit den Daten ?

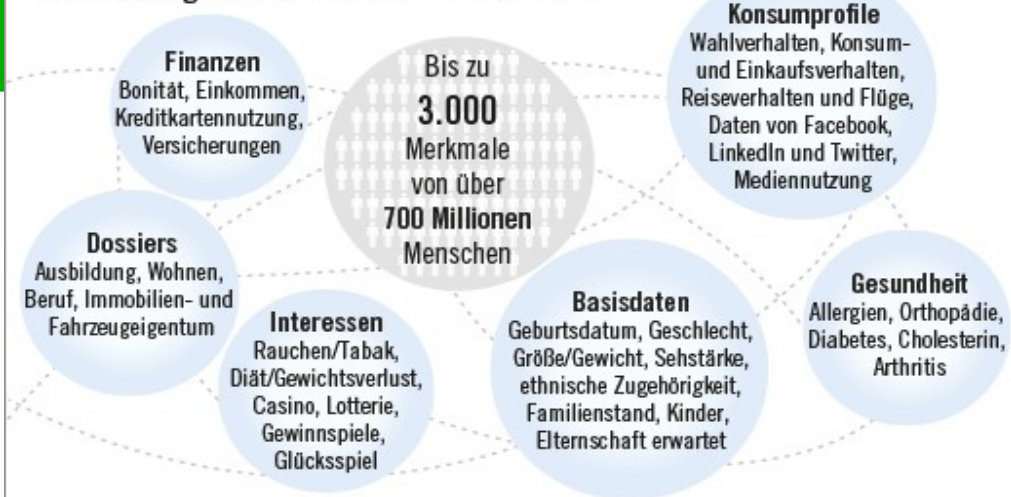
Aus den gesammelten Daten werden **Profile** der Internet-Benutzer erstellt

- „digitaler Schatten“
- „digitales Ich“

Diese **Datenprofile** mit tausenden Persönlichkeitsmerkmalen werden an Firmen verkauft (Versicherungen, Arbeitgeber, Banken, Internet-Werbefirmen ...)



Das Datenangebot des US-Datenhändlers Acxiom



Persönliche Daten sind bares Geld wert

		Adressen	Beschreibung	Preis pro T.
	Die Zeit	55.900	Shopkäufer und Buchserienkäufer	€ 210,00
	RTL Club	510.000	aktive Kunden	€ 180,00
	Elderly & Disabled	110.000	Spender	€ 175,00
	Tag des Herrn	52.400	Abonnenten katholische Wochenzeitung	€ 170,00
	Lehrer	246.100	mit Privatanschrift	€ 170,00
	Lehrer	367.700	mit Schulanschrift	€ 170,00
	Die Zeit	374.000	aktuelle Leser und ehem. Abonnenten	€ 160,00
	Passive Ältere	3.051.100	Adressen gesamt	€ 155,00
	Versa Distanzhandel	55.700	aktive Käufer 0-6 Monate (Beate Uhse)	€ 150,00
Gewinnspielteilnehmer		215.500	Gewinnspielteiln. Drogerieartikel	€ 150,00
Große Tageszeitung		2.155.000	Werbedatei einer großen Tageszeitung	€ 110,00



Was kann man aus den Daten lesen ?



Quelle: www.crackedlabs.org; AK/ÖGB-Darstellung.

Arbeit & Wirtschaft 7/2015

ÖGB-VERLAG/APA-AUFTRAGSGRAFIK



Einige aktuelle „Ereignisse“

Windows 10 wird automatisch auf den Computer geladen, ohne dass der Anwender gefragt wird.

Wegen der grossen Datenmenge (3 - 6 GB) fallen möglicherweise hohe Online-Kosten an.

Microsoft hat in der Windows10-Grundeinstellung Zugriff auf sehr viele persönliche Benutzerdaten.



Einige aktuelle „Ereignisse“

Google hat weitreichende Zugriffsmöglichkeiten auf Android-Handies. Betroffen sind Versionen bis Android 4.4 (40 % aller Geräte). Dazu gibt es noch keine offizielle Stellungnahme von Google

DELL-Computer haben eine gravierende Hintertüre zur Verschlüsselung von Windows-Systemen. Es besteht eine akute Gefahr für Angriffe !

Hintertüren in Kabelmodems, eine ist schon seit 2009 bekannt.



Einige aktuelle „Ereignisse“

AntiVirenhersteller AVG verkauft seine gesammelten Nutzerdaten, um weiterhin Gratis-Software anzubieten

- Werbe-Kennung des Geräts
- Surfverlauf
- Suchverlauf
- Anonymisiert ???

Weitere aktuelle Vorfälle:

- Siehe: <http://datenleck.net>



Nichts zu verbergen?

- Nichts zu verbergen haben, bedeutet nicht, allen alles zu zeigen
- Überwachung verletzt **Menschenwürde** und **Menschenrechte**
- Wir ändern unser Verhalten, wenn wir davon ausgehen, überwacht zu werden
- Wir schränken unser demokratisches, politisches Handeln ein
- Auch wenn wir nichts Illegales tun, können wir plötzlich in Verdacht geraten durch die Kombination verschiedener Daten



Es geht nicht um Datenschutz,
sondern um Menschenrecht.

(Jacob Appelbaum)



Probleme

- **Personalisierte Werbung** – aber das kann ja auch ganz praktisch sein
- Daten über **Krankheiten** können von **Versicherungen** benutzt werden, um **Prämien** zu erhöhen
- Wer nach einer **Schuldnerberatung** sucht, bekommt möglicherweise keinen Bank-Kredit
- Was **illegal** ist kann sich ändern, frühere Daten können **gegen** einen selbst verwendet werden



Probleme

- beim Erstellen der Profile können **falsche Schlüsse** gezogen werden
- aus Maßnahmen zur Terrorbekämpfung wird eine **Generalüberwachung**
- das Grundvertrauen des Staats gegenüber dem Bürger wird zu einem **Grundmisstrauen**
- wer kontrolliert die Behörden gegen **Missbrauch** ?



Probleme – einige Beispiele

- Auch Behörden können sich irren
 - Cobra-Kommando stürmt falsche Wohnung
 - 29.8.2014, <http://kaernten.orf.at/news/stories/2665663>
- Sicherheitspannen:
gespeicherte Daten können „abhanden“ kommen
 - Datenprofile von Aktivitätsmessern bei Google suchbar
 - <http://gizmodo.com/5817784/dear-fitbit-users-kudos-on-the-30-minutes-of-vigorous-sexual-activity-last-night>
 - <http://techcrunch.com/2011/07/03/sexual-activity-tracked-by-fitbit-shows-up-in-google-search-results/>
 - <http://blog.fitbit.com/updates-to-your-profile-page/#i.1noso2bzzedga1>



Was tun?

Mögliche Reaktionen auf die täglich neuen
Horormeldungen über Überwachung und Datenklau:

- **Ist mir egal**, ich habe nichts zu verbergen
- **Resignation** – ich kann eh nix machen
- **Paranoia** und Wunsch nach absoluter Anonymität /
Komplettverweigerung



Was können wir tun ?

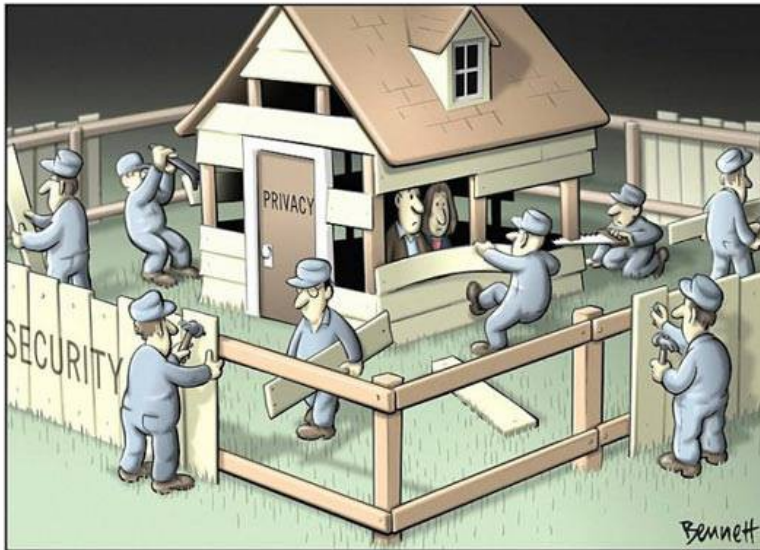
- Es gibt **keine „isolierte“ Maßnahme** – außer als Einsiedler in den Busch zu kehren –die etwas gegen diese Möglichkeit der Überwachung ausrichten könnte.
- Es braucht eine **Fülle von Maßnahmen** – gesellschaftlich wie technologisch –um Europas Abhängigkeit zu verringern.
- Vor allem aber braucht es dafür:

Das **Bewusstsein** dieser Sachverhalte und die daraus resultierenden Konsequenzen für unsere Gesellschaft

(Josef Pichlmeier, Security Day, FH St. Pölten 2014)

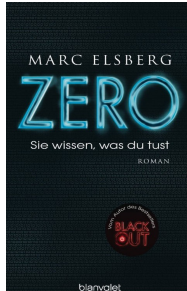


Security vs. Privacy



10 Schritte zur digitalen Selbstverteidigung

Marc Elsberg: Zero



<http://zero-das-buch.de/selbstverteidigungstipps.php>



Selbstverteidigungstipps Elsberg (1)

Surfen Sie wenn möglich nur auf gesicherten Seiten, deren Adresszeile mit „https“ anfangen.

- Vor allem, wenn es um kritische und persönliche Daten (Bankverbindung, Adresse, etc.) geht.
- „Https“ steht für sicheres Hypertext-Übertragungsprotokoll und dient dazu, Daten abhörsicher zu übertragen.



Selbstverteidigungstipps Elsberg (2)

Deaktivieren Sie Cookies.

- Cookies sind kurze Datenbank- oder Verzeichniseinträge zum Informationsaustausch zwischen Computerprogrammen. Viele Webseiten tauschen sich untereinander über ihre Besucher aus. Das passiert u.a. über die Cookies, die von Werbebannern auf Ihren Rechner gelegt werden.
- Richten Sie Ihren Browser so ein, dass er Cookies (http-Cookie, Flash-Cookie, Web-Storage etc.) nach jeder Sitzung löscht.



Selbstverteidigungstipps Elsberg (3)

Verwenden Sie keine Clouds.

- Speichern Sie Ihre Daten lieber auf Datenträgern, Ihrer Festplatte oder Ihrem Heimserver.
- Wenn Sie Ihre Daten in einer Cloud oder in einem Online-Backup speichern, sollten diese verschlüsselt sein.



Selbstverteidigungstipps Elsberg (4)

Denken Sie sich immer neue Passwörter aus.

- Und zwar solche, die Sie sich zwar merken können, aber nicht einfach zu erraten sind.
- Verwenden Sie dabei Zahlen, Groß/Kleinschreibung sowie Sonderzeichen (z.B. %, &, *, /).



Selbstverteidigungstipps Elsberg (5)

Installieren Sie ein E-Mail-Programm auf Ihrem Computer.

- Indem Sie Ihre E-Mails auf Ihrem Rechner schreiben, verhindern Sie, dass jedes Wort, das Sie schreiben, zeitgleich online ist.
- Erst wenn Sie Ihre Nachricht versenden und/oder zwischenspeichern, geht diese ins Internet.



Selbstverteidigungstipps Elsberg (6)

Verschlüsseln Sie Ihre E-Mails und Ihre SMS.

- Dafür gibt es heute einfache Programme. Nichtsdestotrotz hilft es nicht viel weiter, wenn Sie Ihre E-Mail verschlüsseln und der E-Mail-Empfänger keine Verschlüsselung verwendet.
- Außerdem werden nur der Inhalt und die Anhänge codiert. d.h., dass ein potenzieller, unerwünschter Mitleser weiß, wem Sie wann eine E-Mail geschrieben haben.



Selbstverteidigungstipps Elsberg (7)

Chatten Sie nicht über zentrale Dienste,
sondern benutzen Sie freie Anbieter –
auf Ihrem PC und auch auf Ihrem Mobilgerät,
am besten mit OTR-Verschlüsselung.



Selbstverteidigungstipps Elsberg (8)

- **Schalten Sie auf Ihrem Smartphone die Ortungsfunktion aus** ebenso auf den verschiedenen Onlineplattformen, die sie besuchen.
- Dasselbe gilt für die Gesichtserkennungsfunktion.



Selbstverteidigungstipps Elsberg (9)

- **Nutzen Sie möglichst wenige kostenfreie Dienste.**
- Machen Sie sich stets bewusst, dass Sie hier in einer anderen Währung bezahlen: Mit Ihren Daten und Ihrer Freiheit.



Selbstverteidigungstipps Elsberg (10)

- **Vermeiden Sie, wenn möglich, regelmäßige Zahlungen** mittels Bankkarten, Bahncard oder sogenannter Rabattkarten, um zu verhindern, dass Ihre Konsum- und Reisegewohnheiten gespeichert werden.



Warum uns nicht egal sein sollte, welche Daten Google und Co. von uns sammeln

Artikel in der Wochenzeitung Futter

<http://fttr.at/2015/10/25/warum-uns-nicht-egal-sein-sollte-welche-daten-google-und-co-von-uns-sammeln/>



Nachdenken, bevor man auf Enter klickt

Wie so oft im Leben gilt auch hier die Devise: Hirn einschalten!

Klar, wir finden sie auch super lustig, diese nach dem fünften Bier von unseren lieben Freunden geschossenen Ich-lieg-k.o.-auf-der-Couch-und-hab-keinen-Plan-von-den-witzigen-Genital-Kritzeleien-in-meinem-Gesicht-Fotos. Aber ob das unser zukünftiger Arbeitgeber auch so lustig findet?

Ihr könnt noch so sorgfältig jedes peinliche Foto der letzten Party aus eurem Gedächtnis löschen, das Internet tut das nicht.

Zusatz-Fact: 120-150 Likes auf Facebook reichen aus, um ein relativ genaues Profil von dir zu erstellen. Die Summe der Klicks verrät Geschlecht, sexuelle Orientierung, Beruf, Einkommen usw.



Nutzungsbedingungen lesen

Hand auf's Herz: Wer liest schon jedes Mal die Nutzungsbedingungen, die oftmals epische Ausmaße haben und in so einem Juristen-Kauderwelsch verfasst sind, dass sich eh niemand auskennt?

Genau. Sollte man aber, wissen die Experten der CryptoParty.

Unwissenheit schützt nämlich nicht. Mit jedem angekreuzten Hakerl und leichtfertigen Drücken der Enter-Taste gebt ihr den Anbietern oftmals legal (!) Zugriff auf eure privaten Daten.

Das heißt, vorher immer informieren und recherchieren.

Im Zweifelsfall: nicht installieren.



Alternative Suchmaschinen verwenden

Auch wenn Google die einzige Suchmaschine ist, die es in den Duden geschafft hat, sollten auch andere Suchmaschinen in eurem Vokabular existieren.

Die CryptoParty Graz empfiehlt Suchmaschinen wie Startpage („die diskreteste Suchmaschine der Welt“) oder DuckDuckGo.

Warum sind die besser? Sie sammeln nicht eure Daten, speichern nicht eure IP-Adresse und liefern ungefilterte Suchergebnisse.

So nett wie Google nämlich ist, treffen die vorab schon mal eine kleine Auswahl für euch.



Bei Software-Installationen nicht faul sein



Bei Software-Installationen nicht faul sein

Bei Software-Installationen aller Art neigen wir ja dazu, den Zeigefinger nicht von der Maus zu bewegen und immer stur auf die gleiche Abfolge zu klicken: Weiter, Weiter, Fertig. Ist ja so einfach.

Für die, die es nicht wussten, es gibt noch eine andere Möglichkeit: die benutzerdefinierte Installation. Die braucht man dann, wenn man keine nervigen Zusatzfeatures haben möchte.

Außerdem ist Software oftmals gratis, weil sie zusätzliche Werbung installiert. Die kann man damit auch ausschalten.

Einziger Nachteil: Man muss beim Installieren ein bisserl mehr lesen.



Für jeden Dienst ein eigenes Passwort

Die Experten raten, dass man bei den mindestens 20 Passwörtern, die jeder hat... Ähm, Moment, 20?!? Ja, ihr habt richtig gelesen.

Die goldene Regel lautet: Für jeden Dienst ein eigenes Passwort. Sich mit zwei, drei variierenden Passwörtern durchzuschummeln, ist nicht sehr klug.

Aber wie soll man sich das merken? Die CryptoParty Graz empfiehlt, die Gedächtnisleistung sogenannten Passwort-Managern wie z.B. KeePass zu überlassen. Dort werden alle deine Passwörter in einer verschlüsselten Datenbank sicher aufbewahrt und du darfst nur ein Passwort nicht mehr vergessen.

Und wie sieht nun ein perfektes Passwort aus? Auf die Länge kommt's an. Zwölf Zeichen sind vorbildlich. Bitte keine Worte, die im Duden zu finden sind. Auch wenn ihr eure Schmusekätzchen noch so lieb habt, Sternchen85 taugt als Passwort nicht.

Kleiner Trick der Experten: Man denke sich einen einprägsamen Satz aus, nehme die ersten Anfangsbuchstaben, variiere Groß-/Kleinschreibung, garniere das Ganze mit Sonderzeichen und fertig ist euer unknackbares Passwort.



Für Unwichtiges Wegwerf-E-Mail-Adressen verwenden

Bei manchen kostenlosen Softwaredownloads ist eine Registrierung beim Anbieter notwendig. Dazu gehört auch das Angeben einer E-Mail-Adresse. Auf die dann eh nur Spam kommt.

Für solche Fälle gibt es kostenlose E-Mail-Adressen, die nur eine begrenzte Gültigkeit haben.

Die CryptoParty schwört z.B. auf 10MinuteMail.com. Wie der Name bereits verrät, nach zehn Minuten ist die Mail-Adresse Geschichte.



Überlegt, was ihr auf eurer Cloud speichert

Schon oft gehört und nie ganz verstanden? Eine Cloud ist ein Online-Speichermedium, das es euch ermöglicht, eure dort gespeicherten Daten bequem von verschiedenen Rechnern und Smartphones abzurufen, zu bearbeiten und mit Freunden zu teilen. Klingt super.

Aber auf gut Deutsch: Eine Cloud ist der Rechner von jemand anderem. Der andere heißt dann z. B. Dropbox oder Google Drive.

Berechtigte Frage: Wollt ihr eure Daten auf dem Rechner eines anderen haben? „Passwörter, Nacktfotos und andere private Dinge haben daher auf einer Cloud nichts zu suchen“, meint die CryptoParty Graz.



Kostenlose Dienste hinterfragen

(Fast) nichts gibt's geschenkt und schon gar nicht im Internet.

Deshalb merkt euch: Wenn der Dienst nichts kostet, seid ihr die Ware.

Gratis-Services leben vom Verkauf eurer Daten.

Natürlich gibt es Ausnahmen (Stichwort: Open-Source-Bewegung),
aber Ausnahmen bestätigen die Regel.

Keine Garantie, aber eine Spur sicherer: Statt kostenloser Apps sollte
man lieber die 99 Cent oder 1,90 Euro investieren.

Kostenpflichtige Apps saugen meistens weniger Daten und
schalten weniger Werbung.



Vorsicht bei öffentlichen Netzwerken (WLAN)

Kaum ein Lokal, das etwas auf sich hält, verweigert heutzutage seinen Kunden freien Internetzugang. Finden wir auch super.

Die Profis warnen allerdings: Öffentliche Netzwerke lassen jedes noch so minderbegabte Hacker-Herz höher schlagen. Um mitzuverfolgen, was ihr gerade auf eurem Laptop oder Smartphone treibt, braucht es nur ein Handy oder einen Laptop, das gleiche WLAN und vielleicht einen Zwei-Tage-Kurs bei Youtube. Und ihr kriegt davon nicht mal was mit.

Einfacher Tipp: Keine Mails schreiben, kein E-Banking durchführen, also nix machen, wo man sich einloggen muss.

Etwas kniffligerer Tipp: VPN nutzen. Garantiert eine Internetverbindung über einen sicheren Kanal. Kostet allerdings etwas und die Installation ist für Laien etwas komplizierter.



Für Unwichtiges Wegwerf-E-Mail-Adressen verwenden

z.b.

http://praxistipps.chip.de/wegwerf-email-adressen-diese-anbieter-gibts_1674

<http://www.dmoz.org/World/Deutsch/Computer/Internet/Misbrauch/Spam/Vorbeugung/>



Welche Software soll ich verwenden ?

PRISM BREAK

- Sehr ausführliche Liste an empfohlener Software gegen Massenüberwachung:
- <https://prism-break.org/de/>

Empfehlungen der Cryptoparty Graz

- Kurze Liste an empfohlener Software :
- <https://cryptoparty.at/graz:infomaterial>



EXTRA:

Was würde uns Edward Snowden
empfehlen ?

Quelle: Interview mit Micah Lee, 12.11.2015

<https://theintercept.com/2015/11/12/edward-snowden-explains-how-to-reclaim-your-privacy/>



Frage: Was sollte jeder tun, um sicher zu kommunizieren ?

1. Schritt: Verschlüsseln von Telefonanrufen und Textnachrichten

- z.B. mit Signal (Open Whisper Systems), erhältlich für Android und iOS

2. Schritt: Verschlüsseln der Festplatte

- Wenn der Computer gestohlen wird, sind die Daten nicht zu lesen

3. Schritt: Verwenden eines Passwort-Managers

- In der Praxis werden meist einfache, gleiche Passwörter benutzt
- Empfehlung: KeePassX

4. Schritt: Zwei-Faktor-Authentifizierung nutzen

Wenn das Passwort gestohlen wird, muss man noch weiteres Wissen oder ein Gerät besitzen (z.B. Handy oder eine TAN, ein Fingerabdruck, ...)



Edward Snowden empfiehlt

- **Signal**: am Smartphone
- **Tor-Netzwerk** zum Web-Surfen
- **OTR-Chats** (Off-the-Record Messaging): nach Beenden der Unterhaltung kann nicht bewiesen werden, dass einer der Kommunikationspartner eine bestimmte Aussage gemacht hat.
- Als sichere Betriebssysteme: **Tails** und **Qubes**
- Als Browser-Plugins: **HTTPS Everywhere**, **Adblock-Software**



Empfohlene Plugins für Webbrowser

Schutz gegen Web-Tracking:

- Privacy-Badger <https://www.eff.org/privacybadger>
- Ghostery <https://www.ghostery.com/our-solutions/ghostery-browser-extention/>

Visualisierung von Web-Tracking mit Lightbeam für Firefox:

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

Automatischer Aufruf von verschüsselter Datenübertragung:

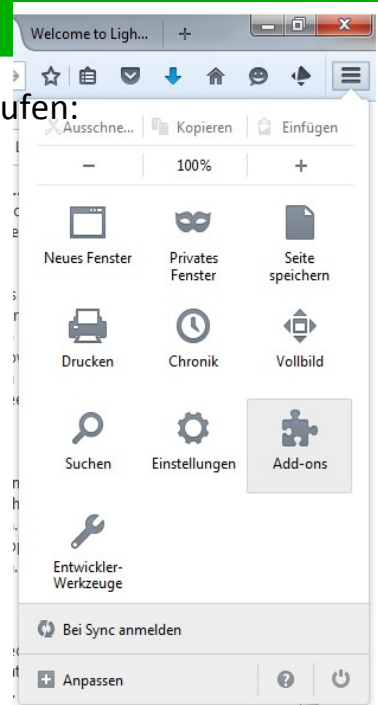
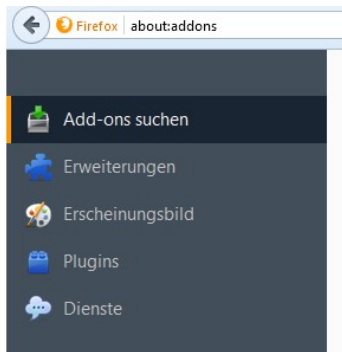
HTTPS Everywhere: <https://www.eff.org/https-everywhere>



Add-ons in Firefox installieren

Add-ons in Firefox werden im Menü rechts aufgerufen:

Und links oben kann man nach einzelnen Add-ons suchen :

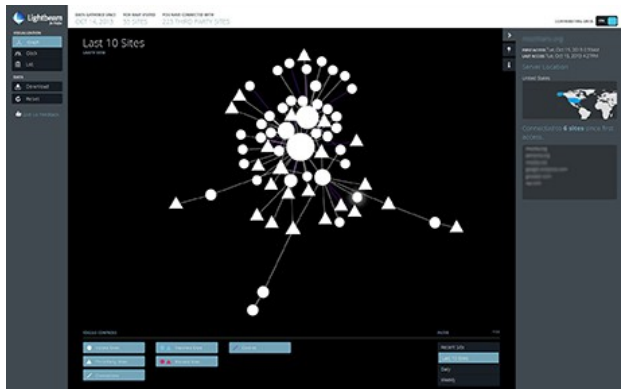


Visualisierung von Web-Tracking

mit Lightbeam für den Webbrowser Firefox:

<https://www.mozilla.org/en-US/lightbeam/>

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



Datenschutz-gerechtere Suchmaschinen

Versuchen Sie anstatt Google einmal diese Suchmaschinen zu verwenden:

- <https://startpage.com/>
- <https://duckduckgo.com/>
- <https://www.metager.de/>
-



Studie: Kommerzielle digitale Überwachung im Alltag

Erfassung, Verknüpfung und Verwertung persönlicher Daten im Zeitalter von Big Data: Internationale Trends, Risiken und Herausforderungen anhand ausgewählter Problemfelder und Beispiele.

Wien, November 2014. Projektleitung und Autor: Wolfie Christl. Eine Studie von Cracked Labs im Auftrag der österreichischen Bundesarbeitskammer.

Download der Studie:

- Vollständige Version: http://crackedlabs.org/dl/Studie_Digitale_Ueberwachung.pdf
- Kurzfassung: http://crackedlabs.org/dl/Studie_Digitale_Ueberwachung_Kurzfassung.pdf

» Online-Version : <http://crackedlabs.org/studie-kommerzielle-ueberwachung>



Digitalen Selbstverteidigung bei digitalcourage.de

Obwohl die Advent-Zeit schon vorbei ist, findet man hier 24 gut aufbereitete Themen der „digitalen Selbstverteidigung“:

<https://digitalcourage.de/support/digitale-selbstverteidigung/adventskalender2015>



Kurz-Videos von Alexander Lehmann

Wir lieben Überwachung

<https://www.youtube.com/watch?v=qGvZveB1osw>

Und ausserdem:

Sicher Surfen einfach erklärt <https://vimeo.com/147303156>

Passwörter einfach erklärt <https://vimeo.com/138839266>

<http://www.alexanderlehmann.net/>



Alles unter Kontrolle

Ein aktueller Dokumentarfilm zum Thema läuft derzeit im Kino:

Infomaterial zum Film:

- <http://www.allesunterkontrolle.at/AllesunterKontrolle.pdf>
- <http://www.allesunterkontrolle.at/DigitaleSelbstverteidigung.pdf>



Top Sites in Austria

<http://www.alexa.com/topsites/countries/AT>

29.11.2015

1. Google.at	11. Yahoo.com	21. Ebay.de
2. Facebook.com	12. Gmx.at	22. Geizhals.at
3. Youtube.com	13. Bing.com	23. Twitter.com
4. Amazon.de	14. Live.com	24. Chip.de
5. Google.com	15. Raiffeisen.at	25. Xhamster.com
6. Orf.at	16. Krone.at	
7. Wikipedia.org	17. Ebay.at	
8. Willhaben.at	18. Sparkasse.at	
9. Gmx.net	19. Amazon.com	
10. Derstandard.at	20. Google.de	

