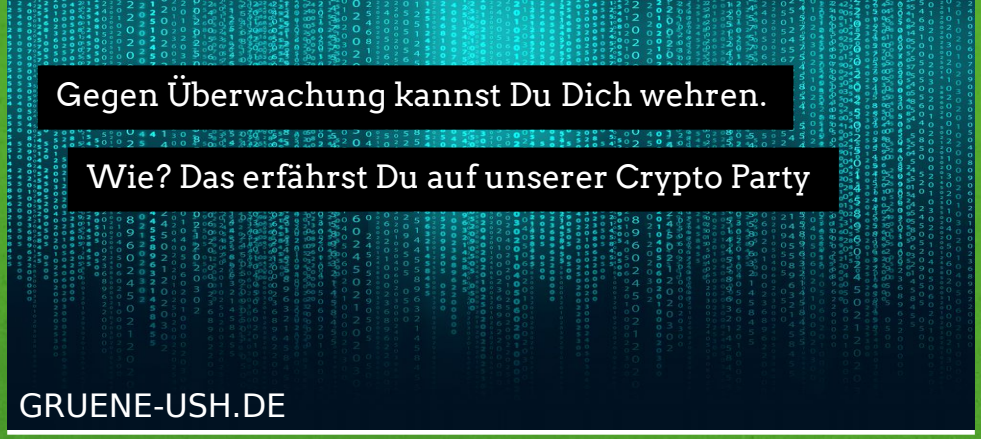


CRYPTO PARTY

mit Markus Wutzke

BÜNDNIS 90
DIE GRÜNEN

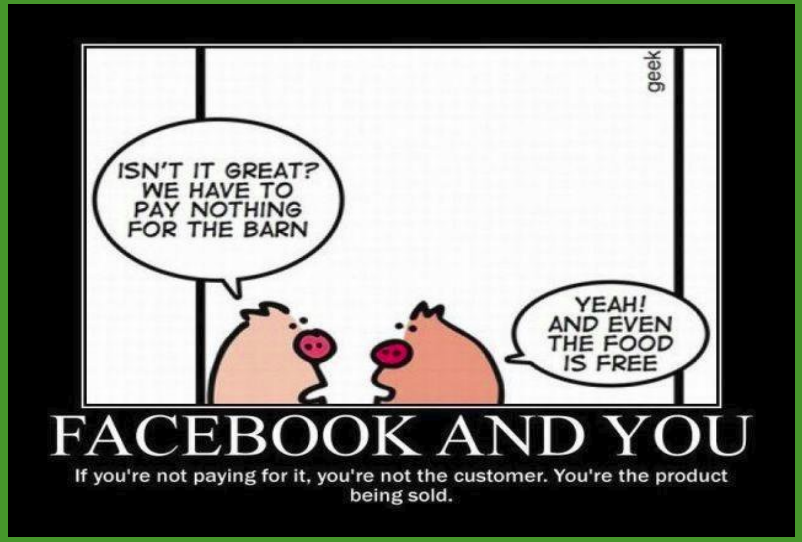
Ablauf

- Grundversorgung sichern
  - Bier, Mate oder Wasser
  - WLAN Zugang: Free WLAN USH
- Aufteilen nach Betriebssystem
- Impulsvortrag / Praktische Übung

Wer überwacht uns?

Staatliche Überwachung

Firmen



Nichts mehr wird so sein, wie es war.

11. September 2001

“Es geht nicht um umfassende Überwachung, sondern um Befugnisse, um Sie als Bürger vor terroristischen Anschlägen zu schützen.”

Dr. Hans-Peter Friedrich
(Bundesinnenminister)

Terrorismusgesetze

- 2005 Biometrischer Reisepass (EU/Schily)
- 2008 Vorratsdatenspeicherung (EU/Zypries)
- 2008 BKA-Novelle (Schäuble) - „Bundestrojaner“

Heribert Prantl in der SZ, am 15. Dezember 2001:
Ausweispapiere werden künftig Fingerabdrücke und „biometrische“ (zum Beispiel Gesichtsvermessungs-) Daten erhalten. Vielleicht haben die Grünen die „Biometrie“ ja deshalb für verträglich gehalten, weil darin das Wort „Bio“ vorkommt.

Der Geist des Präventionsstaates sieht so aus:

Jeder Bürger ist potenziell gefährlich; es muss also erst einmal festgestellt werden, dass er konkret nicht gefährlich ist – er muss sich also entsprechende Überprüfungen gefallen lassen.

Bisher war dies umgekehrt.
Man nannte das: Rechtsstaat

Heribert Prantl, SZ, 15.12.2001

Es war einmal, in einer Zeit noch vor Snowden...

NETZPOLITIK.ORG

START DATENSCHUTZ DIGITALKULTUR NETZNEUTRALITÄT ÜBERWACHUNG URHEBERRECHT

Überwachung in Australien: Regierung fordert Vorratsdatenspeicherung und Zwang zum Entschlüsseln

von Andre Meister am 13. Juli 2012, 15:24 in Datenschutz / 23 Kommentare

Die Regierung in Australien will eine zweijährige Vorratsdatenspeicherung von Telekommunikationsdaten. Das fordert das Justizministerium in einem Diskussionspapier. Zudem soll es eine Straftat werden, die Entschlüsselung von Kommunikation zu verweigern.

Asher Wolf
@Asher_Wolf

Follow

I want a HUGE Melbourne crypto party! BYO devices, beer, & music. Let's set a time and place :) Who's in?

RETWEETS 10 LIKES 9

3:43 AM - 22 Aug 2012

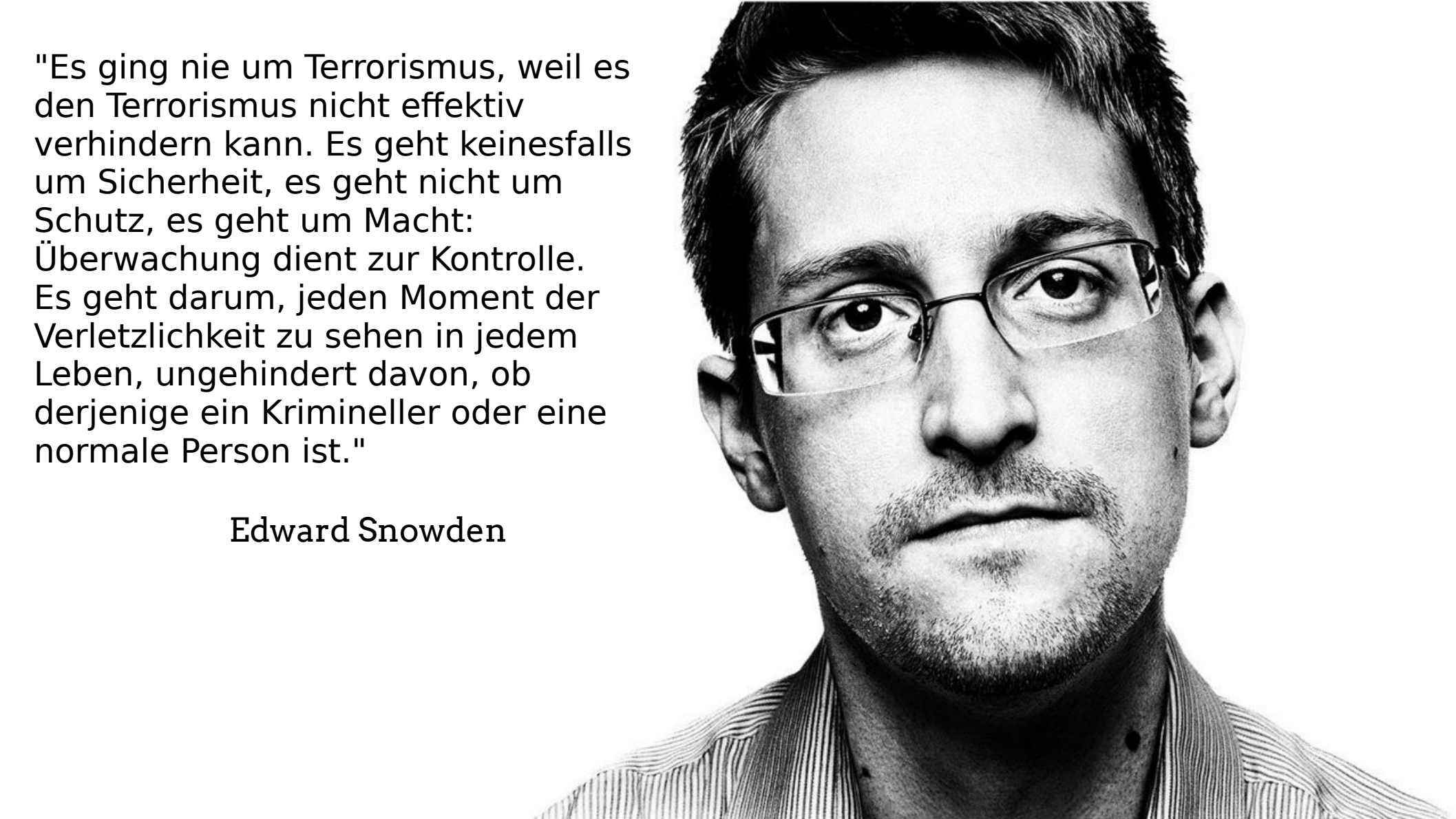
„Declaration of the Independence of Cyberspace“

1996, John Perry Barlow

- Cyberspace consists of transactions, relationships, and thought itself. Ours is a world that is both everywhere and nowhere, but it is not where bodies live.
- We are creating a world that all may enter without privilege or prejudice accorded by race, economic power, military force, or station of birth.
- We are creating a world where anyone, anywhere may express his or her beliefs, no matter how singular, without fear of being coerced into silence or conformity.

"Es ging nie um Terrorismus, weil es den Terrorismus nicht effektiv verhindern kann. Es geht keinesfalls um Sicherheit, es geht nicht um Schutz, es geht um Macht: Überwachung dient zur Kontrolle. Es geht darum, jeden Moment der Verletzlichkeit zu sehen in jedem Leben, ungehindert davon, ob derjenige ein Krimineller oder eine normale Person ist."

Edward Snowden



Unsichere Passwörter

Minecraft Community Lifeboat gehackt: 7 Millionen Accounts geleakt

28.04.2016

Einem Sicherheitsforscher wurden Log-in-Daten von 7 Millionen Mitgliedern der Minecraft Community Lifeboat zugespielt. Eine Überprüf

https://w

Rekordhack bei Yahoo: Daten von halber Milliarde Konten kopiert

22.09.2016 UPDATE

Bei Yahoo wurden Ende 2014 Daten von 500 Millionen Usern abgegriffen. Diesen GAU gestand Yahoo am Donnerstag ein. Das Unternehme

dahinter.

https://www.h

l+f: Passwörter der Scham bei Ashley Madison

15.09.2015

Wer "whatthehellamidoing" oder "cheatersneverprosper" als Passwort bei einem Seitensprung-Portal verwendet, hatte wohl Zweifel an seinem Verhalten...

https://www.heise.de/security/meldung/l-f-Passwoer...

Top Ten der Passwörter auf .de-Domains

1. **hallo**
2. **passwort**
3. **hallo123**
4. **schalke04**
5. **passwort1**
6. **qwertz**
7. **arschloch**
8. **schatz**
9. **hallo1**
10. **ficken**

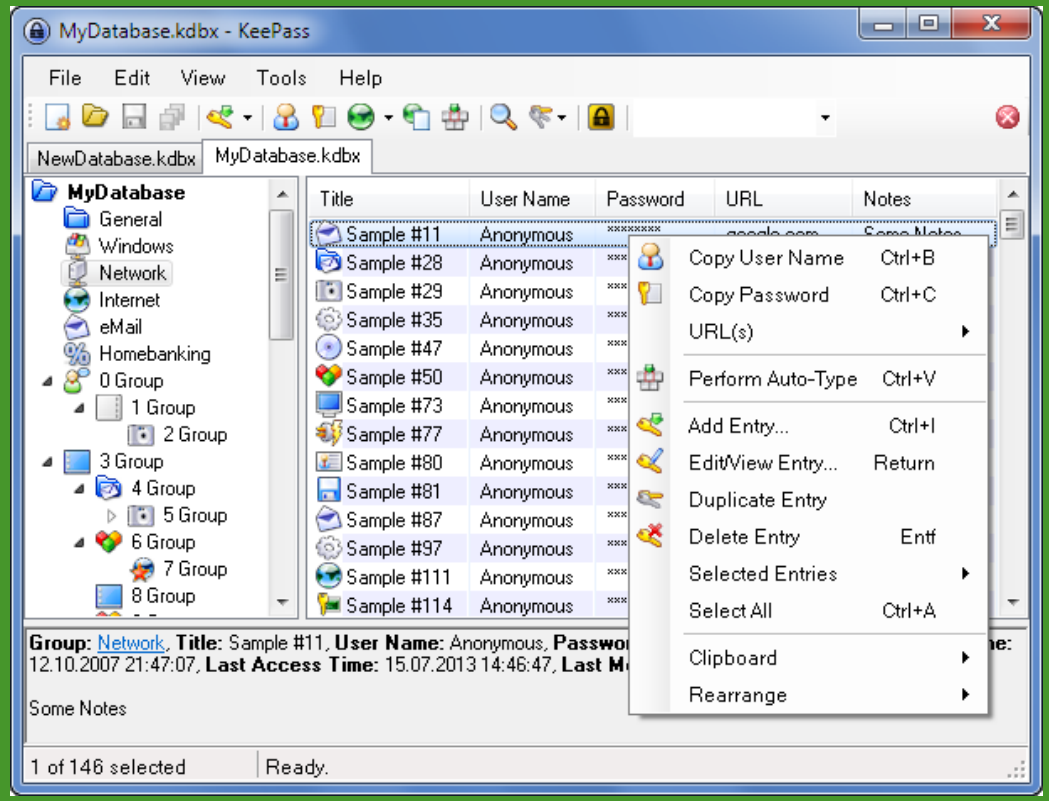
Quelle:
Hasso Plattner Institut, 2016

Sichere Passwörter

- Mindestlänge: 12 Zeichen
- Groß- und Kleinschreibung, Zahlen, Sonderzeichen, z.B. auf Basis eines Satzes:
  „WizWd5xaTfdG“ = ???
- Oder vier zufällige Wörter aneinander reihen:
  winterzeltstinkendeameisen1$
- Für jeden Account ein eigenes Passwort → Passwort-Safe

Passwort-Safe

- http://keepass.info/
- Ein sicheres Passwort schützt alle anderen Passwörter



Recht auf informationelle Selbstbestimmung

- 15.12.1983: „Volkszählungsurteil“ des BVerfG
- Das Bundesverfassungsgericht leitete dieses Recht aus Art. 2 Abs. 1 Grundgesetz (GG), dem Recht auf freie Entfaltung der Persönlichkeit, und aus Art. 1 Abs. 1 GG, der Unantastbarkeit der Menschenwürde, ab.
- Das Recht des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen.
- Wer nicht wisse oder beeinflussen könne, welche Informationen bezüglich seines Verhaltens gespeichert und vorrätig gehalten werden, passe aus Vorsicht sein Verhalten an (Panoptismus). Dies beeinträchtige nicht nur die individuelle Handlungsfreiheit, sondern auch das Gemeinwohl, da ein freiheitlich demokratisches Gemeinwesen der selbstbestimmten Mitwirkung seiner Bürger bedürfe.

EU Datenschutz-Grundverordnung 25. Mai 2018

- Harmonisierung des Datenschutzniveaus
- Verbotsgesetz mit Erlaubnisvorbehalt
  - Einwilligung des Betroffenen
- Informierte eindeutige Einwilligung
- Recht auf Vergessenwerden
- Höhere Bußgelder

Jan Philipp Albrecht,
MdEP für Die Grünen

Noch bis 21. Februar in der Arte Mediathek

Panorama 3 – 01.11.2016: Nackt im Netz – Millionen Nutzer ausgespäht

Was war der Grund?

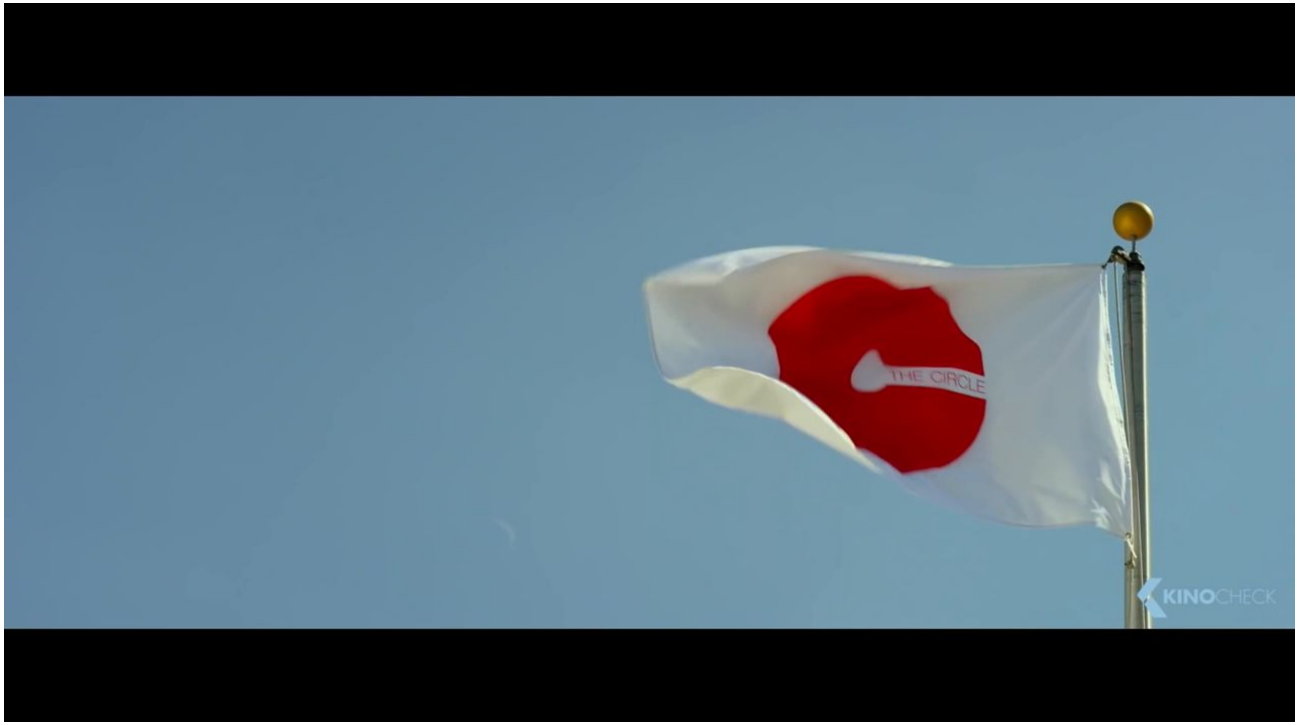
- Brower Plugin „Web of Trust“

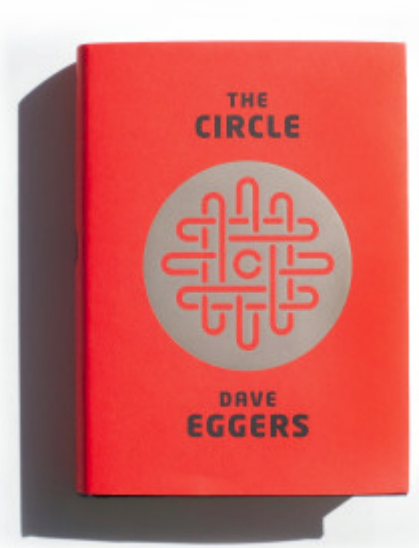
Zweckbindung und Datensparsamkeit

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

„Wir müssen auch im Bereich der Rechtsetzung und der Rechtsprechung das entsprechende Fachwissen haben, damit die Urteile entsprechend der neuen Zeit gefällt werden können.
Denn das Prinzip der Datensparsamkeit, wie es vor vielen Jahren galt, kann heute nicht die generelle Richtschnur für die Entwicklung neuer Produkte sein.“

Angela Merkel, IT Gipfel, 2016





The Circle von Dave Eggers
Ab 25. Mai 2017 im Kino oder jetzt schon im Buchhandel.

Konzept für spurenarmes Surfen
Erste Maßnahmen

- Datensammelnde Dienste kann man meiden.
- Tracking durch Browser Add-ons verhindern

Alternativen zu Google

Suchmaschine mit eigenem Index

- DuckDuckGo.com speichert keine IP-Adressen und Nutzer-Profile.

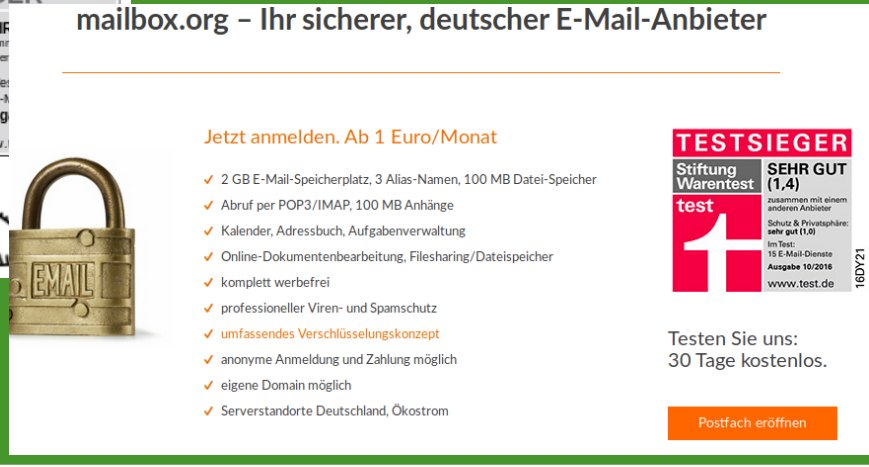
Metasuchmaschinen

- Startpage.com ist mit dem Datenschutzsiegel EuroPriSe zertifiziert. Die Suchmaschine speichert keine IP-Adressen und keine Profile der Nutzer. Im Hintergrund wird die Google-Suche verwendet.
- Metager.de ist ein deutscher Klassiker vom Suma e.V. Neben klassischen Such-diensten wird auch die Peer-2-Peer Suche Yacy einbezogen. Dadurch verzögert sich die Anzeige der Ergebnisse etwas.

Alternative E-Mail Anbieter

posteo.de

mailbox.org



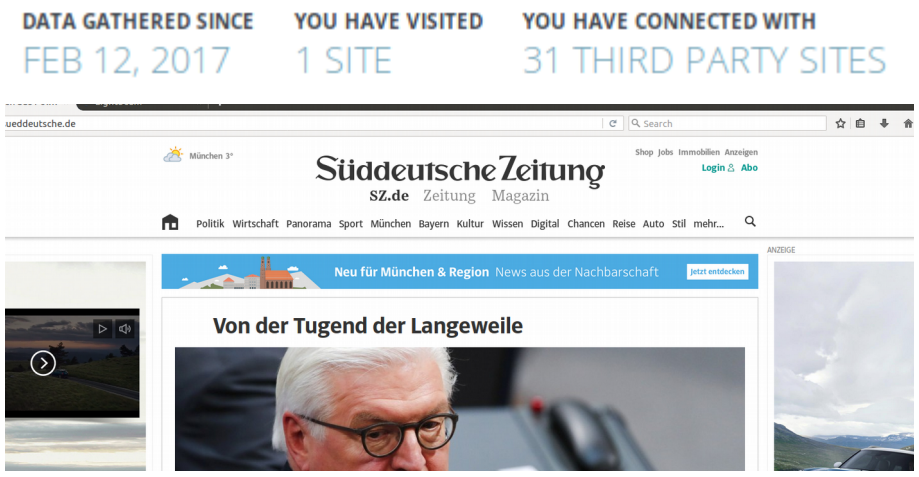
Wie kann ich sehen, an wen meine Daten geschickt werden?

- Lightbeam Plugin

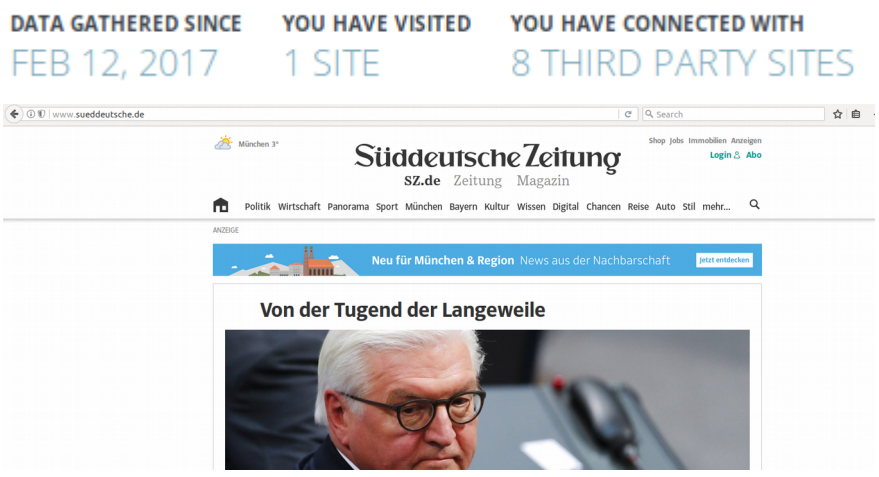
- Developer Tools (Aufrufen über F12), Network

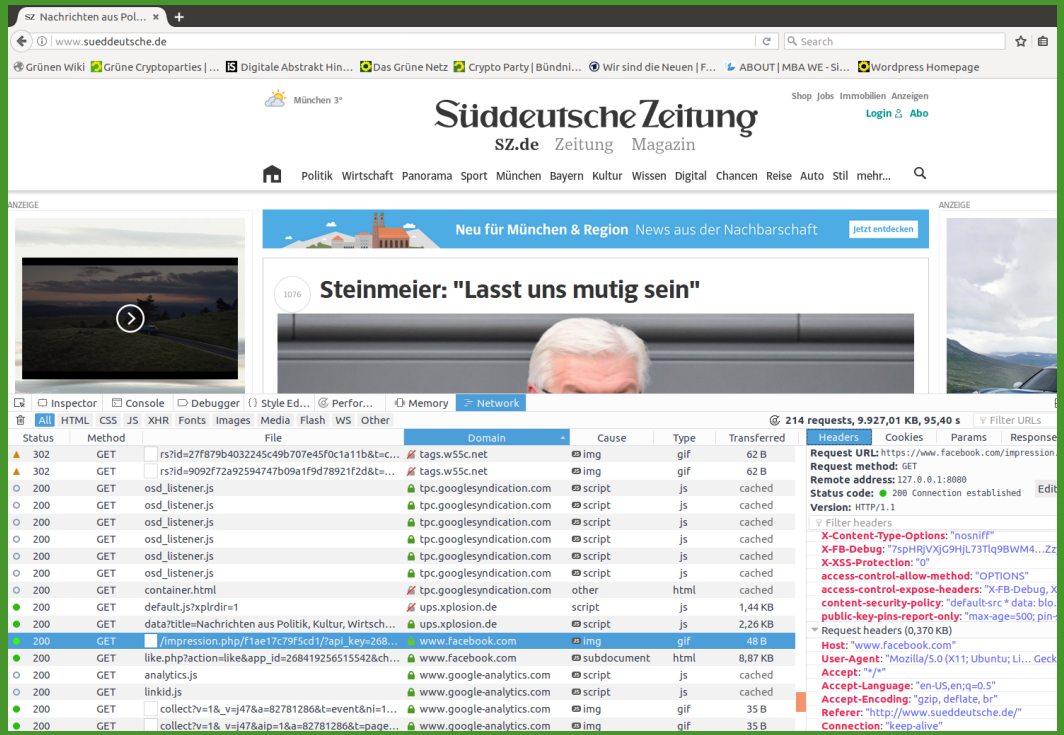
www.sueddeutsche.de

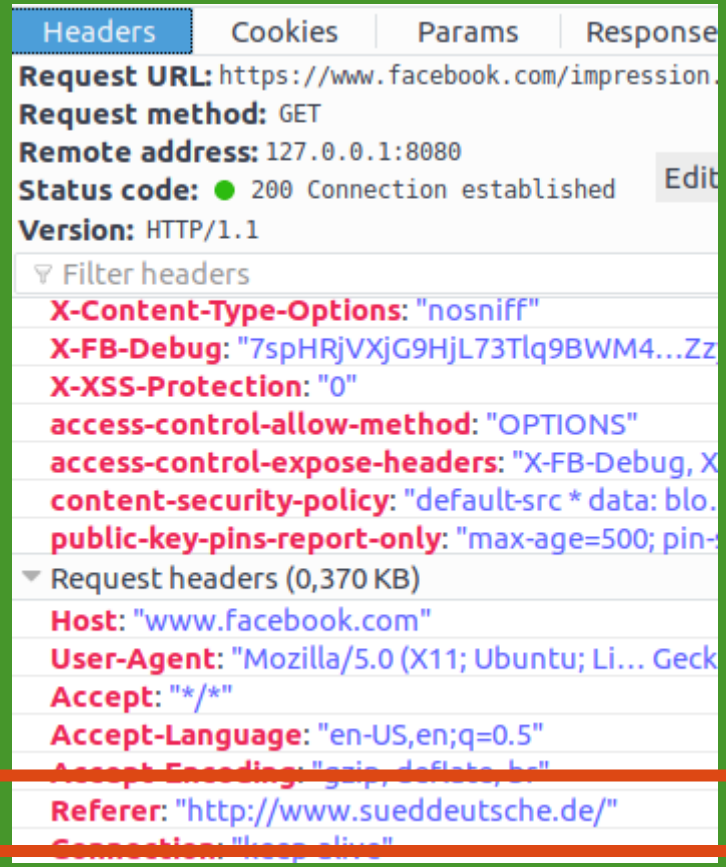
Standard Browser Einstellungen



Privater Modus



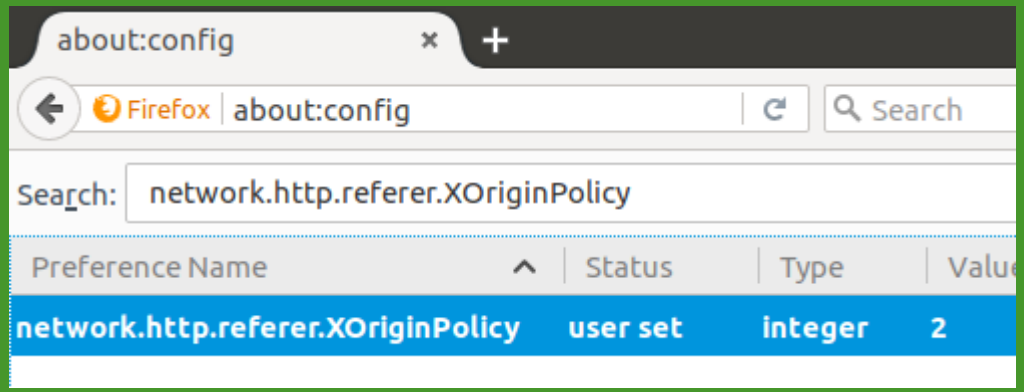




Der Referer verrät von welcher Seite wir eine Seite eines anderen Anbieters aufgerufen haben!

Referer Übertragung ausschalten

- about:config
- network.http.referer.XOriginPolicy suchen
- Wert auf 2 setzen



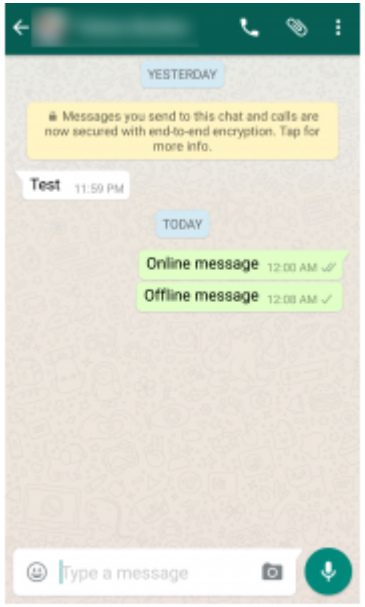
WhatsApp: Bug erlaubt Einblick in verschlüsselte Nachrichten

UPDATE

heise Security 13.01.2017 13:57 Uhr – Martin Holland vorlesen

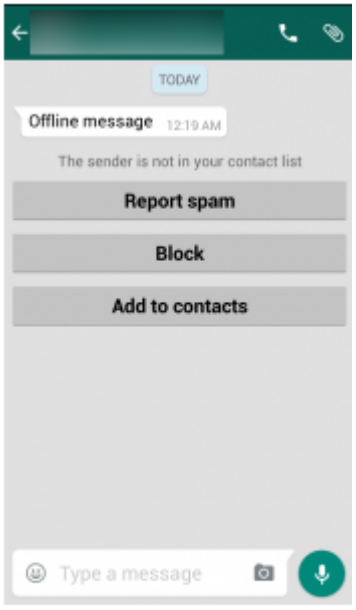
(Bild: Jan Persiel, CC BY-SA 2.0)

Seit einem Jahr werden Nachrichten auf WhatsApp Ende-zu-Ende verschlüsselt, wodurch nicht einmal der Betreiber sie lesen kann. Durch eine Besonderheit bei der Implementierung kann das aber wohl umgangen werden, was Sicherheitsbehörden ausnutzen könnten.



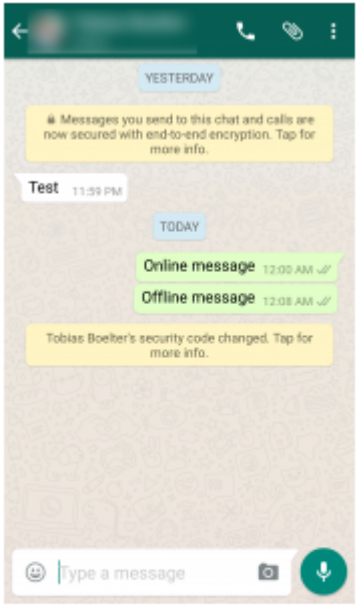
Die zweite Nachricht wird nicht zugestellt.

Bild: Tobias Boelter



Die entschlüsselte Nachricht beim Angreifer

Bild: Tobias Boelter



Der Sender bekommt erst danach den Hinweis auf den geänderten Schlüssel.

Bild: Tobias Boelter

Krypto-Experte: Keine Backdoor in WhatsApp

heise online 14.01.2017 19:10 Uhr – Gerald Himmelein vorlesen

(Bild: dpa, Martin Gerten/Illustration)

Eine Schwachstelle in der Verschlüsselung von WhatsApp wurde vorschnell als "Backdoor" kolportiert. Jetzt hat der Entwickler des Verfahrens eine Stellungnahme veröffentlicht.

Jemand, der die Fähigkeit besitzen, eine Rufnummer einem neuen Schlüssel zuzuordnen – am besten durch direkten Zugriff auf die WhatsApp-Server, kann empfange Nachrichten entschlüsseln.

Was kann ich tun?
In den Einstellungen unter „Account", „Sicherheit" die Option "Sicherheits-Benachrichtigungen anzeigen" aktivieren.

Die Option verhindert nicht, dass Nachrichten in unberechtigte Hände geraten. Die Benachrichtigung macht aber zumindest darauf aufmerksam, wenn die Gegenstelle womöglich nicht mehr die Person ist, mit der man glaubt zu kommunizieren.

Bewertung von Messengern

- Ende-zu-Ende Verschlüsselung
- Open Source
- Datenschutz: Angabe von E-mail oder Handy-Nr. notwendig?
- Schlüsselverifikation

FACEBOOK VERRÄT OFFENBAR PATIENTEN EINER PSYCHOLOGIN

01.09.2016 06:57 | 5.472

Netz - **Schlimme Datenpanne bei Facebook oder doch ganz normale Realität?**

Eine Psychologin hat herausgefunden, dass durch die Eingabe ihrer Telefonnummer bei Facebook, ihren Patienten angeboten wurde, sich zu vernetzen.

Wie DailyMail berichtet, fiel der Ärztin zunächst nur auf, dass das soziale Netzwerk ihr die eigenen Patienten als Freunde unter der Rubrik " Leute, die Du kennen könntest" anzeigte.

Doch kurze Zeit später erzählte ihr einer ihrer Klienten, dass er auf Facebook plötzlich Freundschaftsanfragen von Menschen bekommt, die er noch nie gesehen hat und mit denen er noch nie gesprochen hat.

Schnell stellte sich heraus, dass es sich dabei um Patienten der Psychologin handelt. Die Frau zeigte sich geschockt: "Ich habe Patienten, die HIV positiv sind, die versucht haben, sich umzubringen, oder Frauen, die häuslicher Gewalt ausgesetzt sind."

Wenn man den neuen Bedingungen von WhatsApp nicht widerspricht, gibt die App die eigene Handynummer und möglicherweise andere Daten an Facebook weiter.

Die Ärztin alarmierte Facebook, da sie in einer kleinen Stadt lebt und befürchtet, dass nun bald alle wissen, welche Person an welcher Krankheit leidet.

Später kam heraus, dass alle Patienten, denen angeboten wurde, sich zu befreunden, die Telefonnummer der Ärztin in ihrem Handy hatten. Sie hatte ihre Nummer bei Facebook angegeben.

Zwar streitet das Unternehmen die Theorie ab, doch angesichts der Tatsache, dass sogar WhatsApp mittlerweile die Handynummer an Facebook weitergibt, wenn man den neuen Bedingungen nicht widerspricht, ist dies durchaus sehr bedenklich.

WhatsApp Alternativen

	WhatsApp	Telegram	Threema	Signal
E2E	Ja	Ja - optional	Ja	Ja
E2E Gruppen-Chat	Ja	Nein	Ja	Ja
Open Source	Nein	Ja	Nein	Ja
Datenschutz	Handy-Nr.	Handy-Nr.	Keine Angabe notwendig	Handy-Nr.
Schlüssel-verifikation				

Lust auf mehr Parties?

Bitte eintragen in Newsletter...

Mögliche Themen:

- Email-Verschlüsselung mit GnuPG
- Anonymes Surfen mit dem TOR Browser
- Darknet / Bitcoin
- Windows 10: Datensammelwut beherrschen
- Linux ausprobieren

VIELEN
DANK.

BÜNDNIS 90
DIE GRÜNEN