

Digitale Selbstverteidigung

Marius Melzer (marius@rasumi.net)
Chaos Computer Club Dresden

07.03.2016



Chaos Computer Club



- Verein wurde 1981 gegründet (<https://ccc.de>)

Chaos Computer Club



- Verein wurde 1981 gegründet (<https://ccc.de>)
 - Aktuell > 6000 Mitglieder

Chaos Computer Club



- Verein wurde 1981 gegründet (<https://ccc.de>)
 - Aktuell > 6000 Mitglieder
 - Technologie zum gesellschaftlichen Nutzen (und nicht ihrem Schaden)

Chaos Computer Club



- Verein wurde 1981 gegründet (<https://ccc.de>)
 - Aktuell > 6000 Mitglieder
 - Technologie zum gesellschaftlichen Nutzen (und nicht ihrem Schaden)
 - Betreibt u.a. Öffentlichkeitsarbeit und Politikberatung



Chaos Computer Club



Chaos Computer Club



Chaos Computer Club



- Chaos Computer Club Dresden (<https://c3d2.de>)

Chaos Computer Club



- Chaos Computer Club Dresden (<https://c3d2.de>)
 - Datenspuren: Herbst 2016 (<https://datenspuren.de>)



Chaos Computer Club



- Chaos Computer Club Dresden (<https://c3d2.de>)
 - Datenspuren: Herbst 2016 (<https://datenspuren.de>)
 - Podcasts (<https://c3d2.de/radio.html>)

Chaos Computer Club



- Chaos Computer Club Dresden (<https://c3d2.de>)
 - Datenspuren: Herbst 2016 (<https://datenspuren.de>)
 - Podcasts (<https://c3d2.de/radio.html>)
 - Chaos macht Schule (<https://c3d2.de/schule.html>)



Bundespräsident Gauck zur NSA-Überwachung

“Wir wissen z.B., dass es nicht so ist, wie bei der Stasi und dem KGB, dass es dicke Aktenbände gibt, wo unsere Gesprächsinhalte alle aufgeschrieben und schön abgeheftet sind. Das ist es nicht.” (Gauck, 30.06.2013 im ZDF-Sommerinterview)

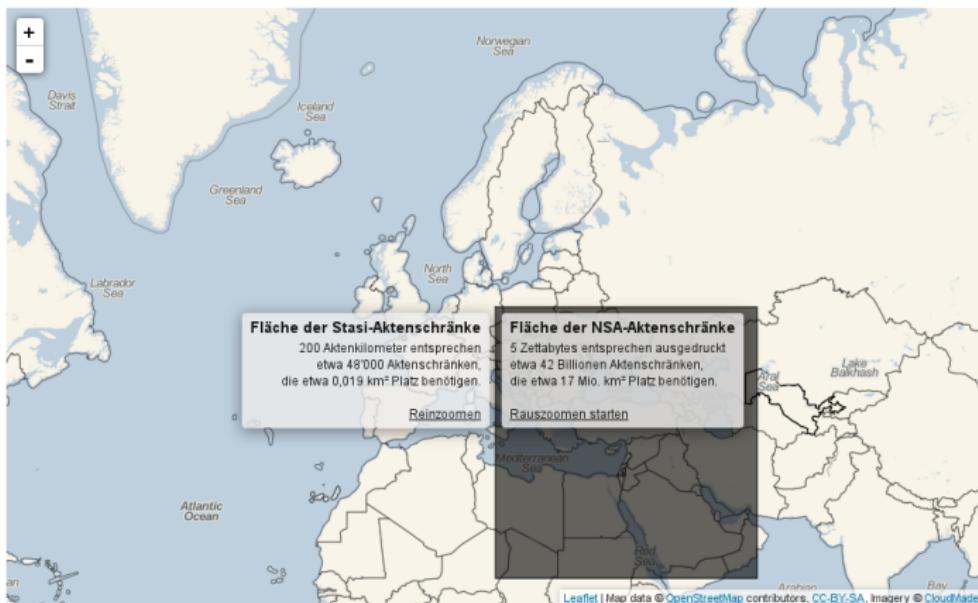
Stasi vs. NSA



Realisiert von [OpenDataCity](#). Anwendung steht unter CC-BY 3.0.



Stasi vs. NSA



“Ich hab ja nichts zu verbergen”

“Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say.” (Edward Snowden, 21.05.2015 auf Reddit)

Samsung vs. 1984

Recognition features to you. In addition, Samsung may collect and your device may capture voice commands and associated texts so that we can provide you with Voice Recognition features and evaluate and improve the features. Please be aware that if your spoken words include personal or other sensitive information, that information will be among the data captured and transmitted to a third party through your use of Voice Recognition.

If you do not enable Voice Recognition, you will not be able to use interactive voice recognition features, although you may be able to control your TV using certain predefined voice commands. While Samsung will not collect your spoken word, Samsung may still collect associated texts and other usage data so that

Behind Winston's back the voice from the telescreen was still babbling away about pig-iron and the overfulfilment of the Ninth Three-Year Plan. The telescreen received and transmitted simultaneously. Any sound that Winston made, above the level of a very low whisper, would be picked up by it, moreover, so long as he remained within the field of vision which the metal plaque commanded, he could be seen as well as heard. There was of course no way of knowing whether you were being watched at any given moment. How often, or on what system, the Thought Police plugged in on any individual wire was guesswork. It was even conceivable that they watched everybody all the time. But at any rate they could plug in your wire whenever they wanted to. You had to live--did live, from habit that became instinct--in the assumption that every sound you made was overheard, and, except in darkness, every movement scrutinized.

Wer sind potenzielle Angreifer?

Wer sind potenzielle Angreifer?

- andere Nutzer (eines Dienstes)

Wer sind potenzielle Angreifer?

- andere Nutzer (eines Dienstes)
- Fremde (“Hacker”)

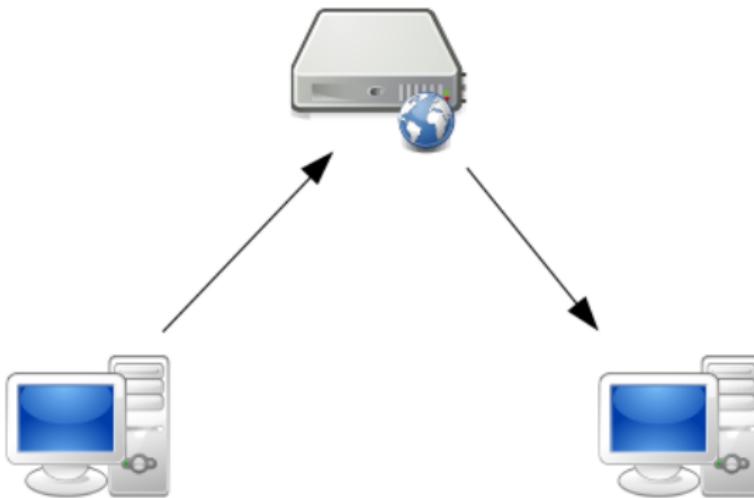
Wer sind potenzielle Angreifer?

- andere Nutzer (eines Dienstes)
- Fremde (“Hacker”)
- Dienstanbieter (z.B. für Werbung)

Wer sind potenzielle Angreifer?

- andere Nutzer (eines Dienstes)
- Fremde (“Hacker”)
- Dienstanbieter (z.B. für Werbung)
- staatliche Institutionen, Netzbetreiber

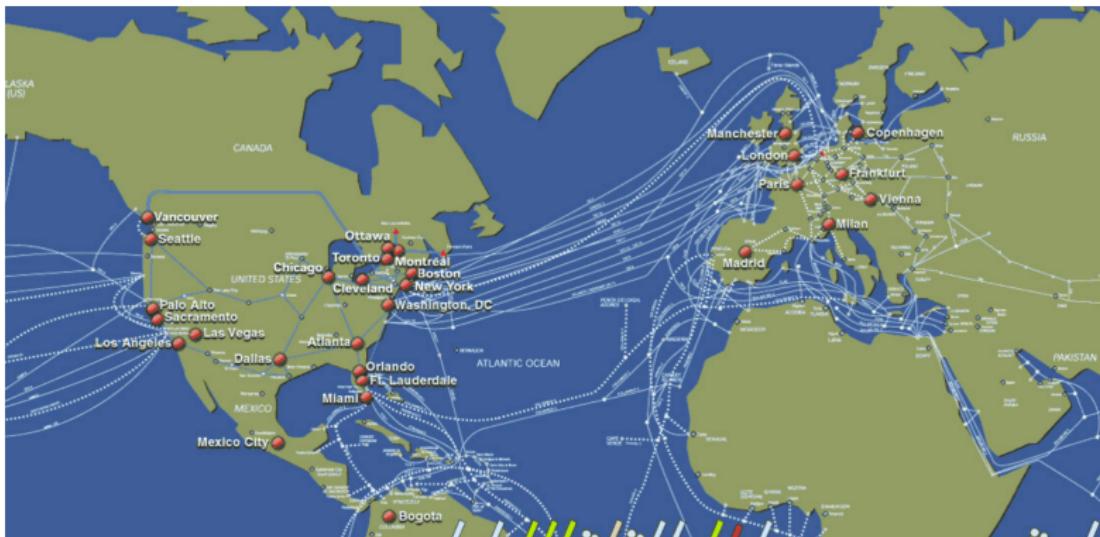
Wie kommunizieren wir im Internet?



Server im Rechenzentrum



Internetknoten (Router)



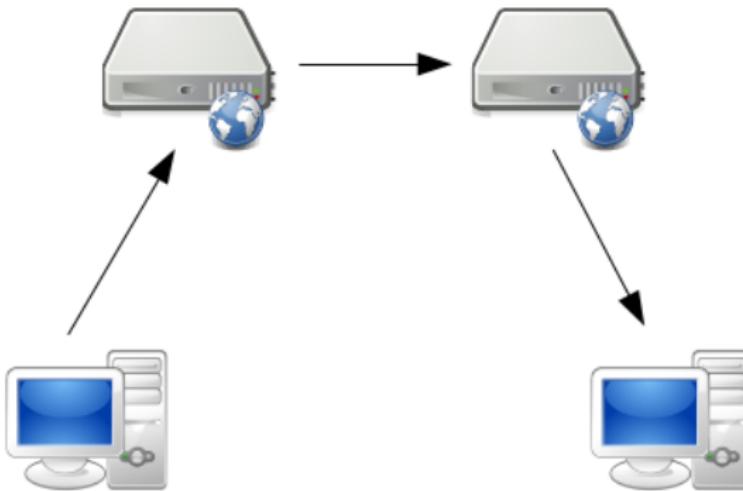
Internetknoten (DE-CIX in Frankfurt)



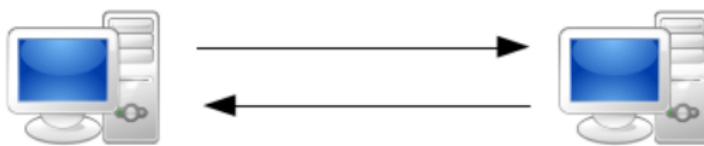
Grafik:  Stefan Funke



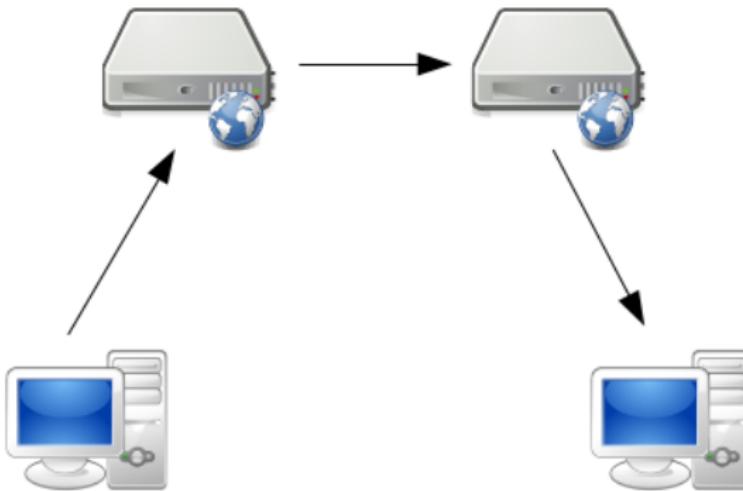
Föderation



P2P



Was ist zu schützen?



Problematisches Verhalten von Software

Problematisches Verhalten von Software

- Sicherheitslücken

Problematisches Verhalten von Software

- Sicherheitslücken
- Backdoors

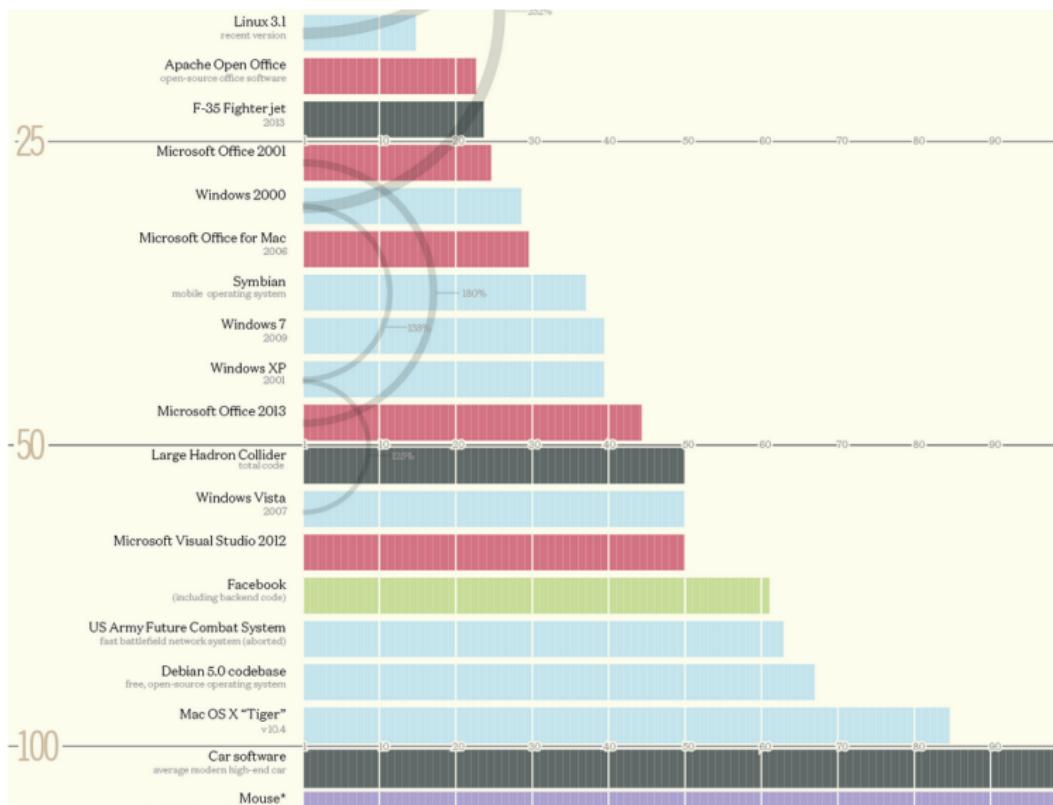
Problematisches Verhalten von Software

- Sicherheitslücken
- Backdoors
- Unerwünschte Funktionalität

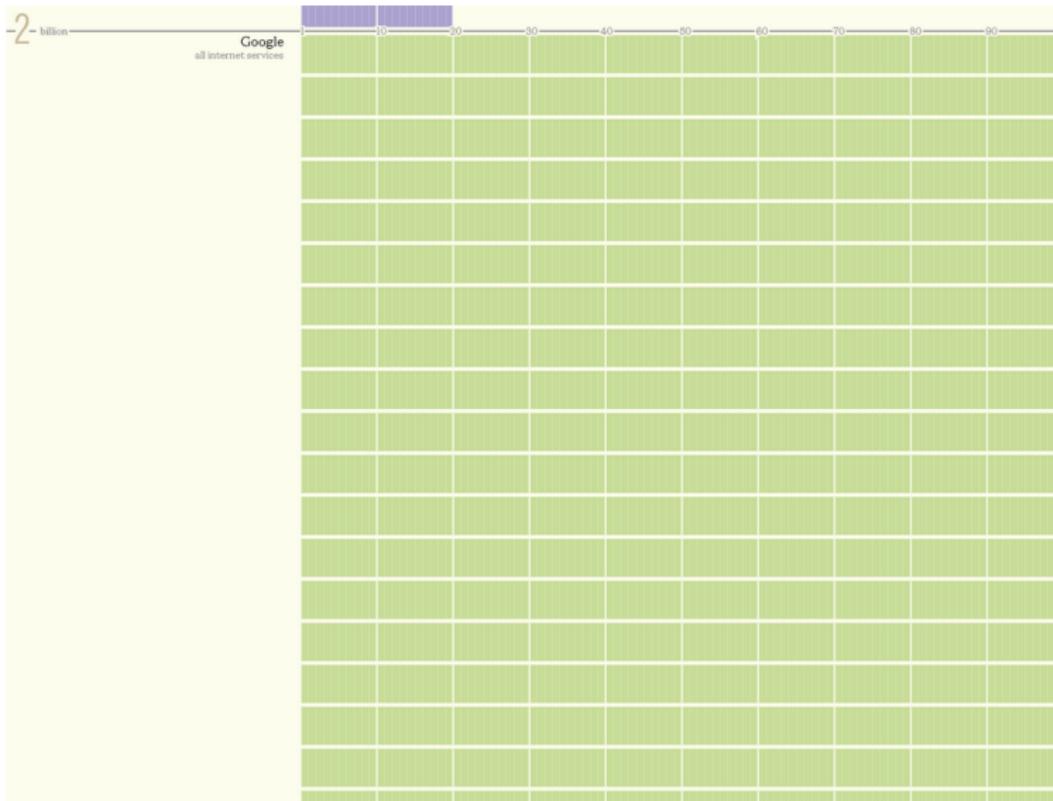
Schwachstellen

```
1 #include "stdio.h"
2
3 int main(int argc, char** argv) {
4     char* secret_number = "Dies ist mein Passwort!\n";
5     printf(argv[1]);
6     return 0;
7 }
```

Größe von Softwareprojekten



Größe von Softwareprojekten



Backdoors

The screenshot shows the homepage of c't magazin. The header features the logo 'c't magazin' with a blue background. Below the header is a navigation bar with links: Startseite, Artikel (which is highlighted in a red box), c't-Projekte, Hotline & FAQ. Underneath the main menu are secondary navigation links: Magazin, Internet, Software, Hardware, Know-how, Praxis, and Artikel-Foren. A breadcrumb trail 'c't > aktuell' is visible. The main content area displays an article by Micha Borrmann and Jürgen Schmidt titled 'Microsofts Hintertür'. The article headline is 'Zweifelhafte Updates gefährden SSL-Verschlüsselung'. Below the headline is a paragraph of text: 'Was macht Windows, wenn es auf ein Verschlüsselungszertifikat trifft, dessen Echtheit es nicht überprüfen kann? Es schlägt nicht etwa Alarm, sondern fragt bei Microsoft nach, ob man dort zufällig jemanden kennt, der das Zertifikat für echt erklären möchte.' At the bottom right of the page, there is a small box containing 'c't 17/13'.

Magazin Internet Software Hardware Know-how Praxis Artikel-Foren

c't > aktuell

Micha Borrmann, Jürgen Schmidt

c't 17/13

Microsofts Hintertür

Zweifelhafte Updates gefährden SSL-Verschlüsselung

Was macht Windows, wenn es auf ein Verschlüsselungszertifikat trifft, dessen Echtheit es nicht überprüfen kann? Es schlägt nicht etwa Alarm, sondern fragt bei Microsoft nach, ob man dort zufällig jemanden kennt, der das Zertifikat für echt erklären möchte.

Backdoors

Android-VirensScanner schnüffeln Surf-Verhalten aus



vorlesen / MP3-Download

Viele VirensScanner für Android senden mehr Daten an ihren Hersteller, als sie sollten. c't hat sie dabei ertappt, wie sie Privates übertragen und HTTPS unterwandern. Eine der größten Datenpetzen wurde über 100 Millionen Mal installiert.

Millionenfach installierte VirensScanner für Android überwachen das Surf-Verhalten ihrer Nutzer und übermitteln ihre Erkenntnisse an die Hersteller. Dabei untergraben Sie sogar die Sicherheit von verschlüsselten HTTPS-Verbindungen. Dies berichtet c't in der aktuellen Ausgabe 6/14.

Wir analysierten bei sechs verbreiteten Android-Virenscannern die Kommunikation mit dem jeweiligen Hersteller und stießen in vier Fällen auf ernsthafte Datenschutzprobleme. Alle getesteten Apps bieten eine Safe-Browsing-Funktion, bei beim Besuch potenziell bösartiger Web-Seiten Alarm schlagen soll. Ob eine Seite bösartig ist oder nicht, erfragen die Apps bei der Hersteller-Cloud. Dabei gehen oft aber mehr Daten durch die Leitung als nötig.



Backdoors (politische Debatte)

Großbritannien: Cameron will gegen Verschlüsselung vorgehen

 heise online 13.01.2015 10:27 Uhr – Martin Holland

 vorlesen



David Cameron bei der Ankündigung seiner Gesetzespläne (Bild: Screenshot - BBC)

Als Reaktion auf die Anschläge in Paris hat Großbritanniens Premier David Cameron

Unerwünschte Funktionalität

The screenshot shows the Windows Settings app with the title "Einstellungen" at the top left. In the center, there's a search bar labeled "Einstellung suchen" with a magnifying glass icon. On the right side, there are window control buttons (minimize, maximize, close). The main area has a light blue header bar with the text "DATENSCHUTZ". Below it, a tab bar has the "Allgemein" tab selected, highlighted in light blue. The left sidebar lists various categories: Position, Kamera, Mikrofon, Spracherkennung, Freihand und Eingabe, Kontoinformationen, Kontakte, Kalender, Messaging, Funkempfang, Weitere Geräte, Feedback und Diagnose, and Hintergrund-Apps. To the right of the sidebar, several sections are displayed:

- Datenschutzoptionen ändern**: A section about advertising ID usage. It says "Apps die Verwendung der Werbungs-ID für App-übergreifende Erfahrungen erlauben (bei Deaktivierung wird Ihre ID zurückgesetzt)". There are two toggle switches: one for "Aus" (off) and one for "Ein" (on), with "Ein" currently selected.
- SmartScreen-Filter einschalten**: A section about checking URLs from Windows Store Apps. It says "SmartScreen-Filter einschalten, um von Windows Store-Apps verwendete Webinhalte (URLs) zu überprüfen". A toggle switch is shown, with "Ein" selected.
- Informationen zu meinem Schreibverhalten an Microsoft senden**: A section about sending writing behavior data to Microsoft. It says "Informationen zu meinem Schreibverhalten an Microsoft senden, um die Eingabe- und Schreibfunktionen in Zukunft zu verbessern". A toggle switch is shown, with "Aus" selected.
- Websites den Zugriff auf die eigene Sprachliste gestatten**: A section about allowing websites access to the speech dictionary. It says "Websites den Zugriff auf die eigene Sprachliste gestatten, um die Anzeige lokal relevanter Inhalte zu ermöglichen". A toggle switch is shown, with "Aus" selected.
- Microsoft-Werbung und andere Personalisierungsinfos verwalten**: A link to manage Microsoft advertising and personalization information.
- Datenschutzbestimmungen**: A link to view data protection terms.

Unerwünschte Funktionalität

App name	iPhone	Android				
	Username Password	Contacts	Age, Gender	Location	Phone ID	Phone number
0.03 Seconds Pro	■	■	■	■	■	■
Age My Face	■	■	■	■	■	■
Angry Birds	■	■	■	■	■	■
Angry Birds Lite	■	■	■	■	■	■
Aurora Feint II: Lite	■■■	■	■	■	■	■
Barcode Scanner (BahnTech)	■	■	■	■	■	■
Bejeweled 2	■	■	■	■	■	■
Best Alarm Clock Free	■	■	■	■	■	■
Bible App (LifeChurch.tv)	■	■	■	■	■	■
Bump	■	■	■	■	■	■
CBS News	■	■	■	■	■	■
0.03 Seconds	■	■	■	■	■	■
Dictionary.com	■	■	■	■	■	■

Unerwünschte Funktionalität

Google knows nearly every Wi-Fi password in the world

By [Michael Horowitz](#)

September 12, 2013 10:44 PM EDT [194 Comments](#)



If an Android device (phone or tablet) has ever logged on to a particular Wi-Fi network, then Google probably knows the Wi-Fi password. Considering how many Android devices there are, it is likely that Google can access most Wi-Fi passwords worldwide.

Recently [IDC reported](#) that 187 million Android phones were shipped in the second quarter of this year. That multiplies out to [748 million phones](#) in 2013, a figure that *does not* include Android tablets.

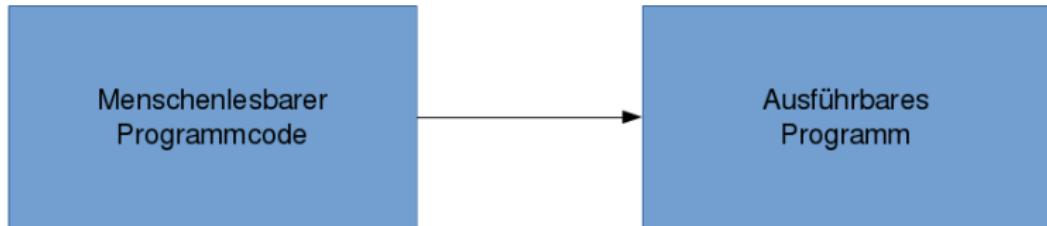
Wie schütze ich meine Geräte?

- (Virenscanner)
- Rechte von Applikationen einschränken (Permissions, Firewall)
- Aktuelle und vertrauenswürdige Software

Vertrauenswürdige Software?

Einer Software, die nicht quelloffen ist, kann man nicht vertrauen

Kompilierung von Software



Probleme von proprietärer Software

Probleme von proprietärer Software

- Kontrolle unterliegt einer Organisation

Probleme von proprietärer Software

- Kontrolle unterliegt einer Organisation
- Transparenz und Sicherheit

Probleme von proprietärer Software

- Kontrolle unterliegt einer Organisation
- Transparenz und Sicherheit
- “Rad neu erfinden”

Strategien moderner IT-Unternehmen

Strategien moderner IT-Unternehmen

- Hardware

Strategien moderner IT-Unternehmen

- Hardware
- Software

Strategien moderner IT-Unternehmen

- Hardware
- Software
- Internet(-dienste)

Strategien moderner IT-Unternehmen

- Hardware
- Software
- Internet(-dienste)
- ... aus einer Hand

Strategien moderner IT-Unternehmen

Strategien moderner IT-Unternehmen

- Fehlende Interoperabilität

Strategien moderner IT-Unternehmen

- Fehlende Interoperabilität
- vorgegebene Dienste und Programme

Strategien moderner IT-Unternehmen

- Fehlende Interoperabilität
- vorgegebene Dienste und Programme
- keine ausreichenden Nutzerrechte

Strategien moderner IT-Unternehmen

- Fehlende Interoperabilität
- vorgegebene Dienste und Programme
- keine ausreichenden Nutzerrechte
- Kopierschutz, Online-Zwang, ...

Strategien moderner IT-Unternehmen

“Tie all of our products together, so we further lock customers into our ecosystem” (Steve Jobs)

Strategien moderner IT-Unternehmen

WhatsApp to begin sharing your data with Facebook

By Killian Bell



The screenshot shows the WhatsApp Terms and Privacy Policy screen. At the top, there are three tabs: 'Terms and Privacy Policy' (selected), 'Account', and 'Security'. The 'Account' tab shows options like 'Privacy', 'Payment info', 'Change number', 'Delete my account', and 'Network usage'. The 'Security' tab shows a lock icon and text about end-to-end encryption. The main content area has sections for 'Simple. Personal. Real-Time Messaging' and a 'Download Now' button. At the bottom, there's a checkbox for sharing account info with Facebook and an 'AGREE' button.

Simple. Personal. Real-Time Messaging

Download Now

About

FAQ

Share my WhatsApp account information with Facebook to improve my Facebook experiences

AGREE

Terms and Privacy Policy

Account

Privacy

Payment info

Change number

Delete my account

Network usage

Share my account info

Share my WhatsApp account information with Facebook to improve my Facebook experiences

To make WhatsApp secure, your chats and calls are automatically end-to-end encrypted.

This means your content is private, so WhatsApp and third parties can't see it.

Learn more about WhatsApp security.

Show security indicators

If you'd like to verify your chats and calls are end-to-end encrypted, enable this setting and tap "verify security number" in contact info, group info, or when you're in a WhatsApp call. Your chats and calls are encrypted regardless of this setting.



Das GNU Projekt

- Begonnen von Richard Stallman im Jahr 1984
- Gründung der Free Software Foundation im Jahr 1985



 **FREE SOFTWARE
FOUNDATION**





Firefox und Thunderbird

Firefox

- Browser



Thunderbird

- Email-Programm



LibreOffice

- Textverarbeitung
- Tabellenkalkulation
- Präsentationen
- Formeleditor
- nutzt Open Document Format zur Speicherung



Freie Software für Android

F-Droid

- Installationsdienst für freie Android-Software



Signal

- Verschlüsselter Nachrichtenaustausch
- Verschlüsselte Speicherung



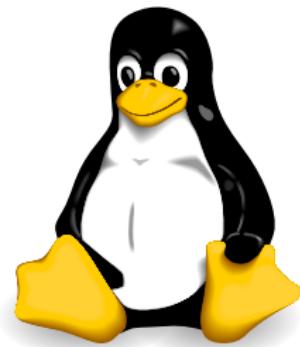
Replicant (Alternativ: Cyanogenmod)

- basiert auf Android
- Ziel, alle proprietären Komponenten durch freie zu ersetzen
- Einbindung von F-Droid
- **Problem:** Verlust der Garantie bei Installation

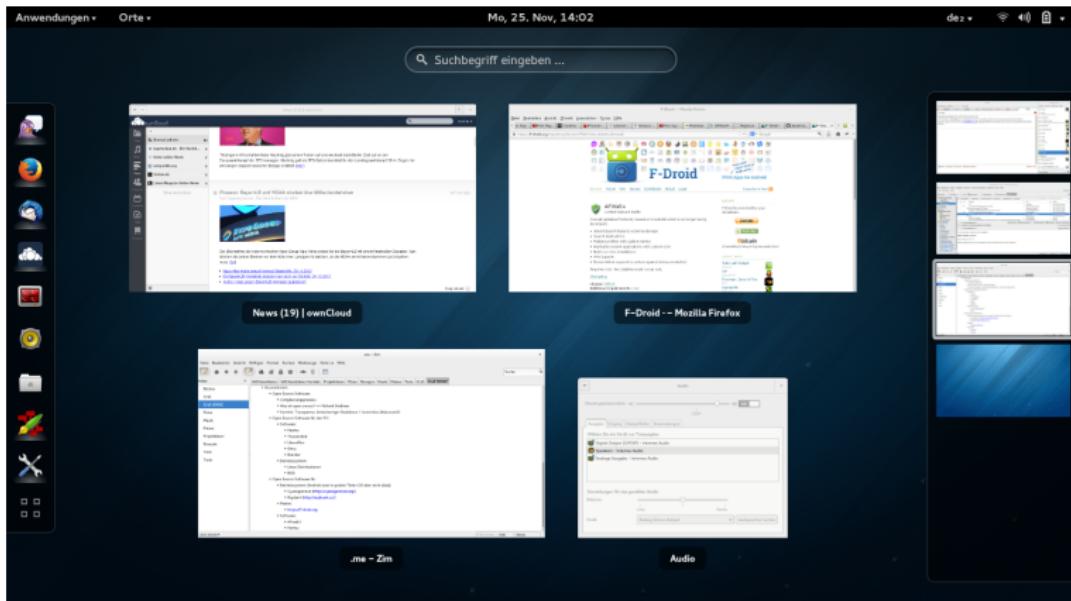


Linux

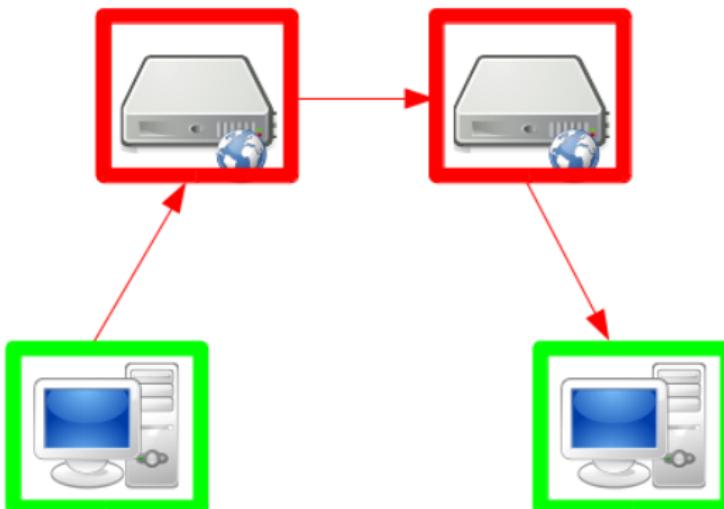
- Weit verbreitet als Server-Betriebssystem
- Bekannte Desktop-Varianten:
 - Ubuntu/Debian Linux
 - Linux Mint
- Können als Live-System ausprobiert werden
- Integrierte Software für Verschlüsselung, Webbrowsing, E-Mail, Textverarbeitung etc.



Linux



Was ist zu schützen?



Tempora

Home | Video | Themen | Forum | English | DER SPIEGEL | SPIEGEL-TV | Abo | Shop | Schlagzeilen | Wetter | TV-Programme | mehr ▾

SPIEGEL ONLINE NETZWELT

Login | Registrierung

Politik | Wirtschaft | Panorama | Sport | Kultur | Netzwerk | Wissenschaft | Gesundheit | einestages | Karriere | Uni | Schule | Reise | Auto

Nachrichten > Netzwerk > Netzpolitik > Überwachung > Internetüberwachung: Tempora ist schlimmer als Prism

Netz-Spähsystem Tempora: Der ganz große britische Bruder



Hehr als 200 Glasfaserkabel sollen die Briten angezapft haben

DPA/dpa/UKU/ingenitaucher.com

Das umstrittene US-Spähprogramm Prism? Ist harmlos im Vergleich dazu, in welchem Umfang ein britischer Geheimdienst unter dem Codenamen Tempora weltweit das Internet ausspielt - und damit auch deutsche Nutzer. Doch selbst Datenschutzaktivisten halten das Vergleichen für legal.

Samstag, 22.06.2013 - 20:24 Uhr

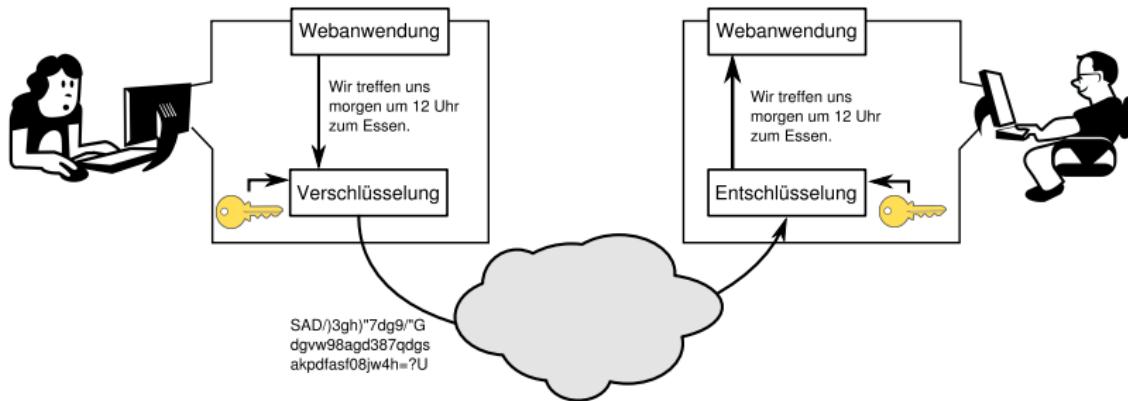
Drucken | Versenden | Merken

Nutzungsrechte | Feedback

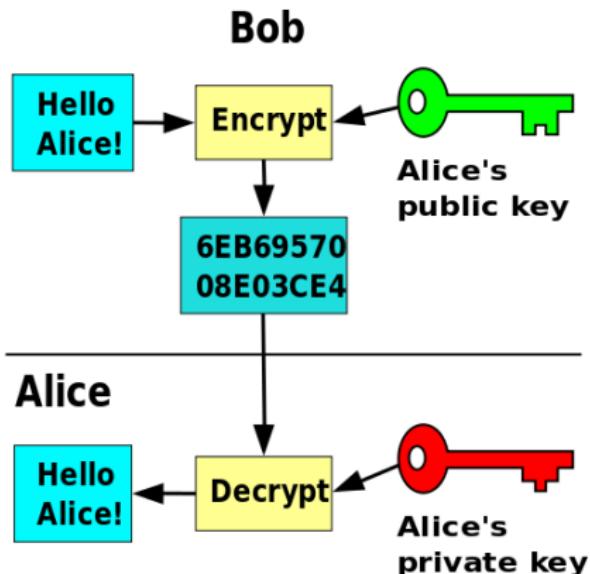
Kommentieren | 389 Kommentare

Hamburg/London - Die Aufregung war riesig, als bekannt wurde, dass die National Security Agency (NSA) im Rahmen ihres unter US-Präsident Barack Obama initiierten Spähprogramms Prism die Kunden von Telefon- und Internetfirmen ausleuchtet - Big Barack is watching you. Doch Brit Brother tut genau dies auch. Und in mancher Hinsicht scheint die Überwachung durch die britischen Netzsperne viel umfassender zu sein als die der Amerikaner.

Verschlüsselung: symmetrisch

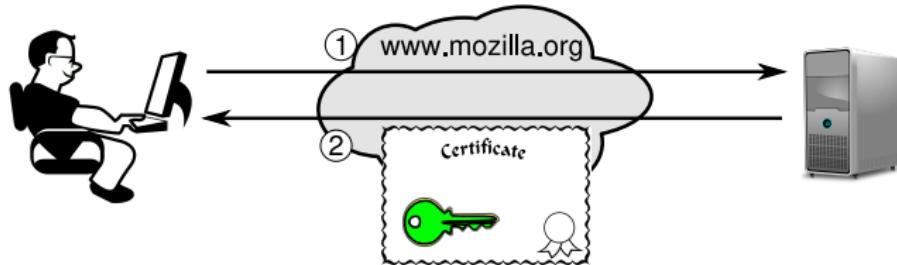


Verschlüsselung: asymmetrisch

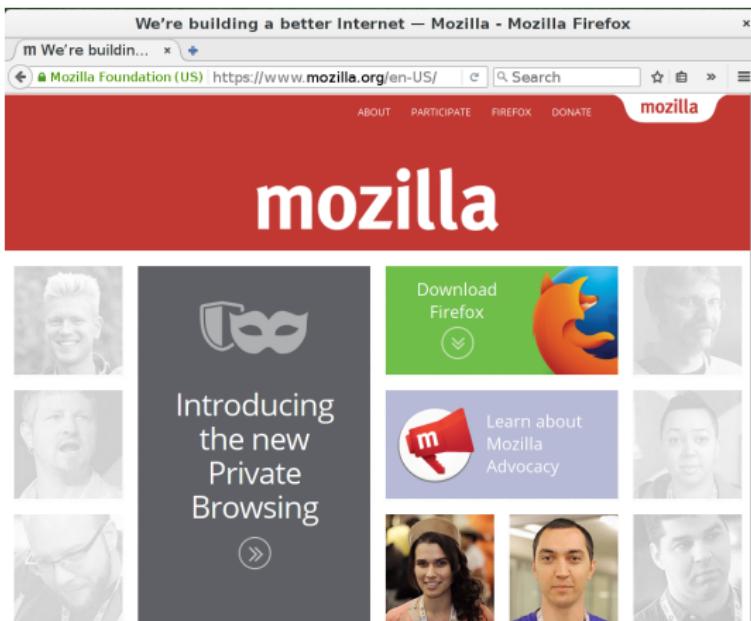


Transportwegverschlüsselung

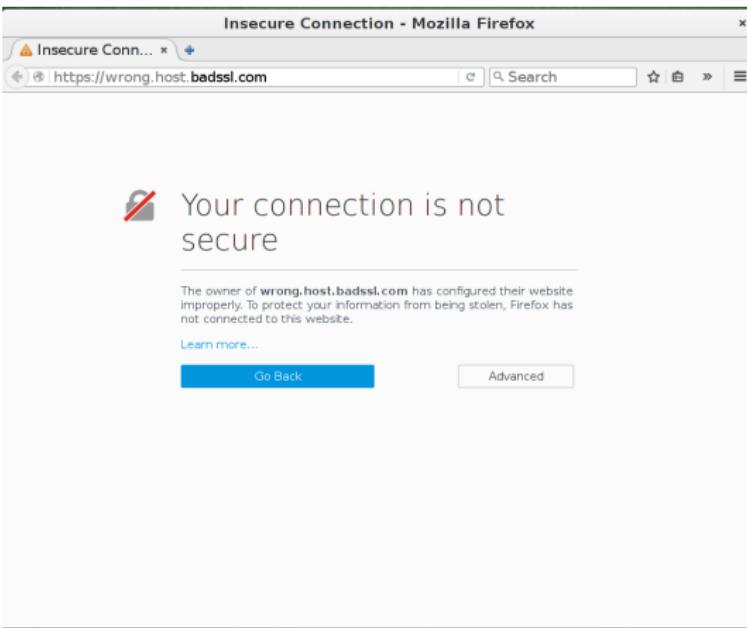
SSL = Secure Socket Layer / TLS = Transport Layer Security



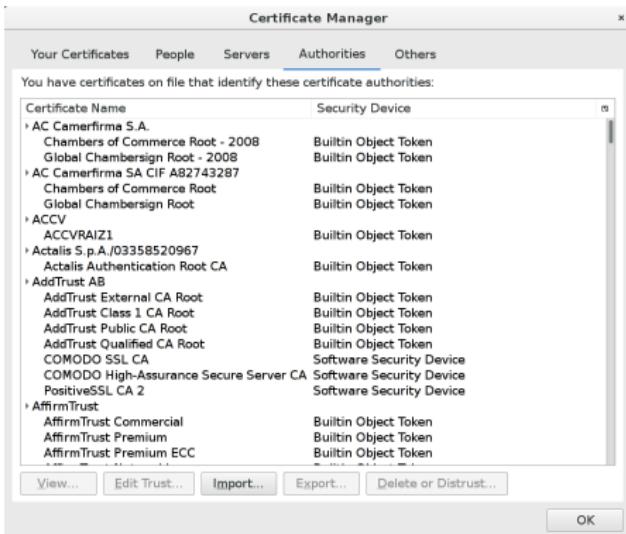
SSL im Browser



Ungültiges Zertifikat



Zertifizierungsstellen



HTTPS Everywhere



ELECTRONIC FRONTIER FOUNDATION
DEFENDING YOUR RIGHTS IN THE DIGITAL WORLD

 SEARCH

HOME ABOUT OUR WORK DEEPLINKS BLOG PRESS ROOM TAKE ACTION SHOP



[HTTPS Everywhere](#)

[FAQ](#)

[Report Bugs / Hack On The Code](#)

[Creating HTTPS Everywhere Rulesets](#)

[How to Deploy HTTPS Correctly](#)

HTTPS Everywhere is a Firefox, Chrome, and Opera extension that encrypts your communications with many major websites, making your browsing more secure. [Encrypt the web: Install HTTPS Everywhere today.](#)



[Install in Firefox
Version 3 Stable](#)



[Install in Chrome
Beta Version](#)



[Install in Opera
Beta Version](#)

Donate to EFF

Stay in Touch

Email Address

Postal Code (optional)

SIGN UP NOW

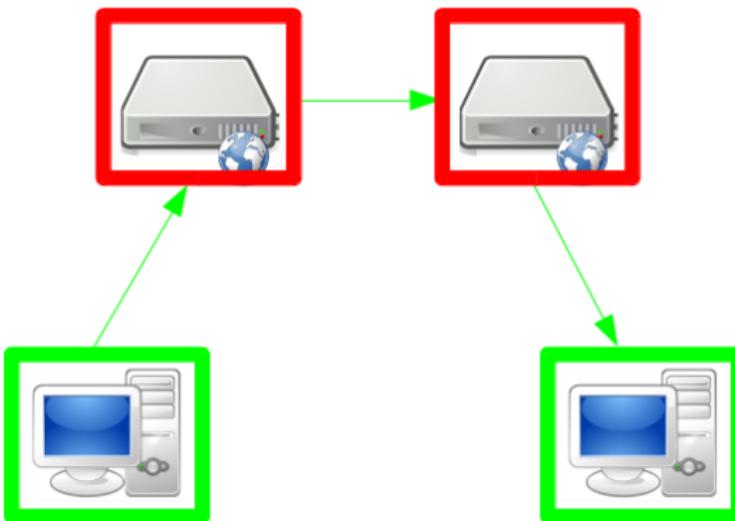
NSA Spying

eff.org/nsa-spying

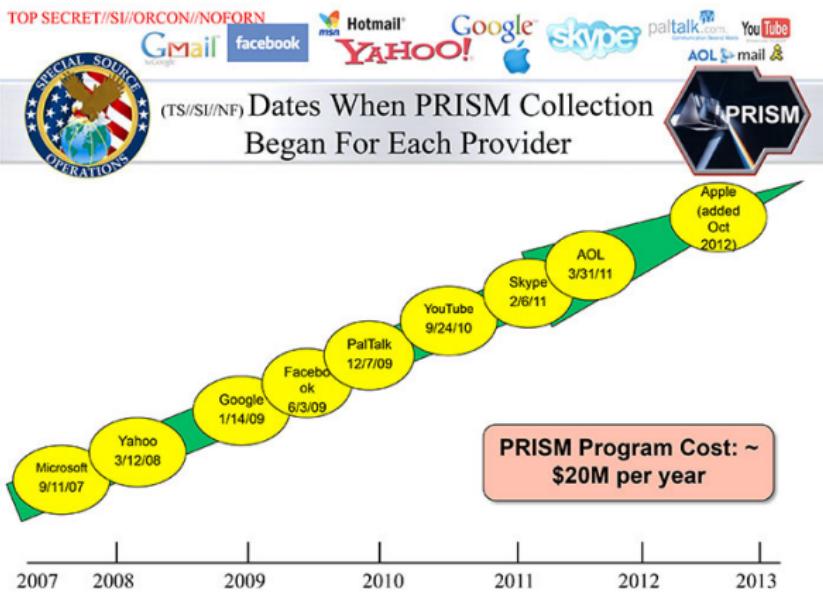
EFF is leading the fight against the NSA's illegal mass surveillance programs. Learn more about what the program is, how it works, and what you can do.



Was ist zu schützen?



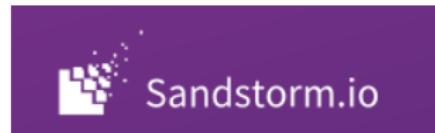
Prism



Dezentrale Dienste



E-Mail



Ende-zu-Ende-Verschlüsselung

- GPG für E-Mails

Ende-zu-Ende-Verschlüsselung

- GPG für E-Mails
- OTR für Jabber:
 - Pidgin mit OTR-Plugin für Linux und Windows
 - ChatSecure oder Xabber für Android
 - Adium für Mac, ChatSecure für iOS

Ende-zu-Ende-Verschlüsselung

- GPG für E-Mails
- OTR für Jabber:
 - Pidgin mit OTR-Plugin für Linux und Windows
 - ChatSecure oder Xabber für Android
 - Adium für Mac, ChatSecure für iOS
- palava.tv, talky.io, Tox, Linphone für Videotelefonie

Ende-zu-Ende-Verschlüsselung

- GPG für E-Mails
- OTR für Jabber:
 - Pidgin mit OTR-Plugin für Linux und Windows
 - ChatSecure oder Xabber für Android
 - Adium für Mac, ChatSecure für iOS
- palava.tv, talky.io, Tox, Linphone für Videotelefonie
- Signal

E-Mail-Selbstverteidigung

E-MAIL-SELBSTVERTEIDIGUNG

LANGUAGE [GNU/LINUX](#) [MACOS](#) [WINDOWS](#) SHARE

SIEH DIR UNSERE INFOGRAFIK AN UND VERBREITE SIE WEITER 

Hassenüberwachung verstößt gegen unsere Grundrechte und bedroht die freie Meinungsäußerung. Diese Anleitung bringt dir eine einfache Selbstverteidigungsmethode bei E-Mail-Verschlüsselung. Wenn du fertig bist, kannst du E-Mails senden und empfangen, die von Überwachern oder Kriminellen, die deine E-Mails abhören, nicht gelesen werden können. Alles, was du brauchst, ist ein Computer mit einer Internetverbindung, ein E-Mail-Konto und eine halbe Stunde Zeit.

Auch wenn du nichts zu verborgen hast, die Verwendung von Verschlüsselung schützt die Privatsphäre der Menschen, mit denen du kommunizierst, und macht den Systemen der Hassenüberwachung das Leben schwer. Wenn du doch etwas wichtiges verborgen möchten, bist du in einer Gesellschaft. Dies sind die gleichen Werkzeuge, die Edward Snowden benutzt hat, um seine bekannten Geheimnisse über die NSA zu verbreiten.

5 Schritte gegen Überwachung zu wählen: erfordert neben der Verwendung von Verschlüsselung den politischen Kampf dafür, dass weniger Daten über uns gesammelt werden. Aber der erste Schritt ist es, dich selber zu schützen und die Überwachung deiner Kommunikation so schwer wie möglich zu machen. Das geht so:

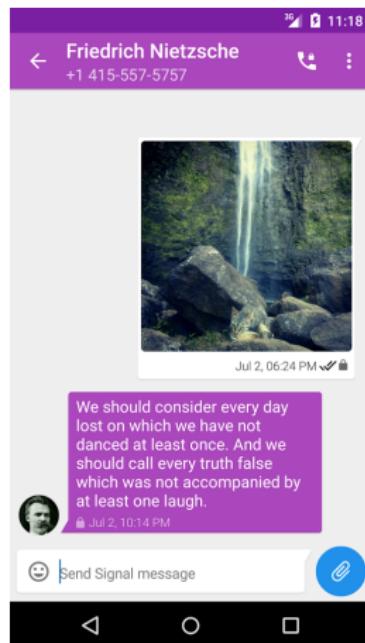
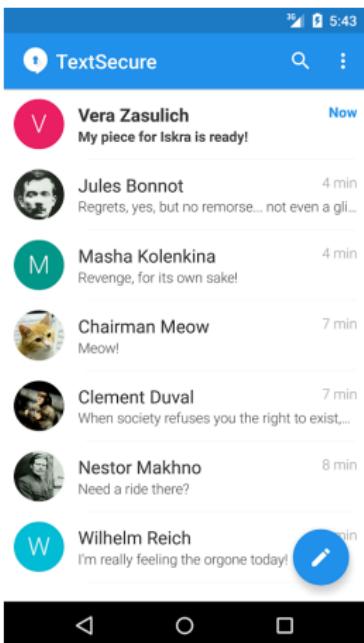
#1 INSTALLIERE DIE PROGRAMME

Diese Anleitung basiert auf freier Software. Freie Software ist transparent und kann von allen kopiert und angepasst werden. Dadurch ist sie sicherer vor Überwachung als nicht-freie Software (wie Windows). Lerne mehr über freie Software auf [fsf.org](#). Auf den meisten GNU/Linux-Systemen ist GnuPG bereits installiert, also musst du es nicht herunterladen. Wenn du GnuPG konfiguriert, brauchst du jedoch ein E-Mail-Programm. Bei den meisten GNU/Linux-Distributionen kann man eine freie Version des Programms Thunderbird installieren. E-Mail-Programme sind eine weitere Art auf E-Mail-Konten zuzugreifen, die ähnlich wie Webmail funktionieren, aber mehr Funktionen bieten.

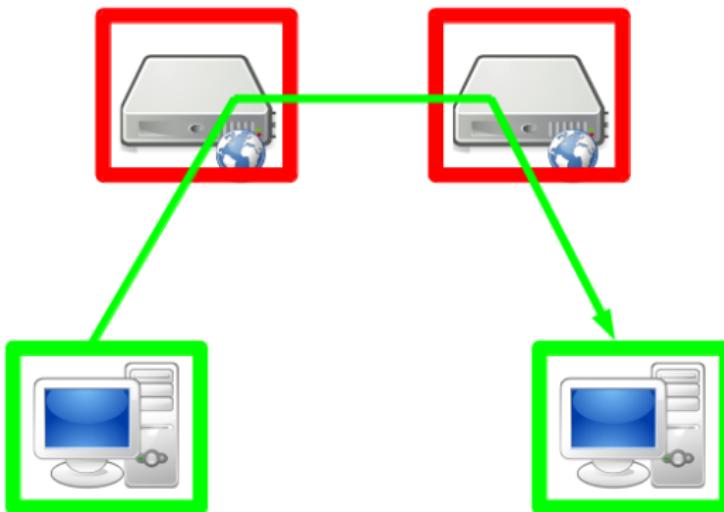
Wenn du bereits eines dieser Programme hast, kannst du zu [Schritt 1.b](#) springen.

<https://emailselfdefense.fsf.org/de/>

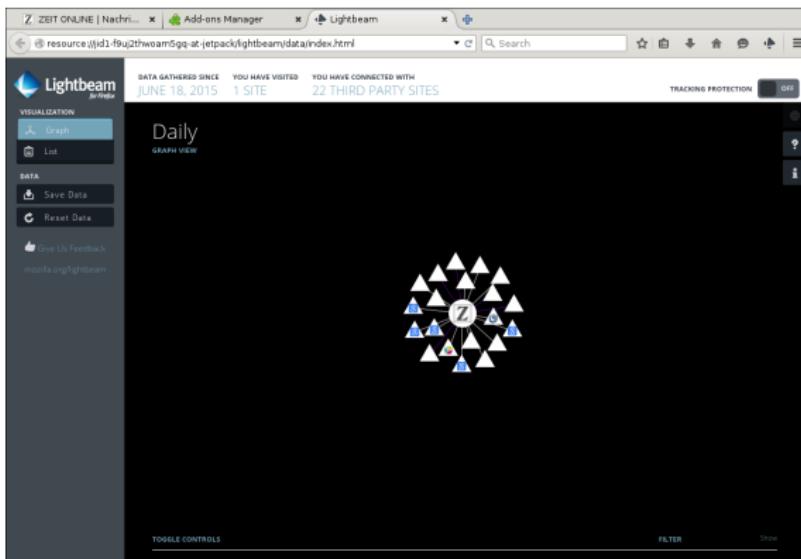
Signal



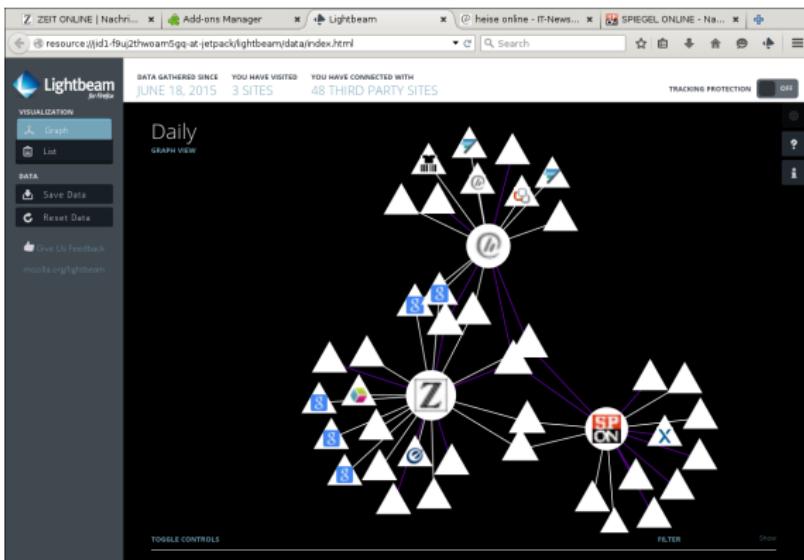
Ich will etwas von einem anderen Nutzer



Metadaten im WWW



Metadaten im WWW



Metadaten - Vorratsdatenspeicherung

- Handynetz
 - Telefonnummern
 - Zeitpunkt und Dauer (Telefonate, SMS)
 - Funkzelle (Ort)
- Internet
 - IP-Adresse (= ungefährer Ort)
 - Alle Verbindungen
 - Email: Adressen von Sender und Empfänger, Zugriff

Metadaten - Stille SMS

Überwachung: Die Stille SMS wird immer beliebter

(heise online 20.01.2016 07:37 Uhr – Christiane Schulzki-Haddouti)

[vorlesen]



(Bild: Heise)

Die Handy-Kommunikation wurde von den Ermittlungsbehörden im vergangenen Halbjahr deutlich intensiver überwacht. Das geht aus einer Antwort der Bundesregierung auf eine Anfrage der Bundestagsfraktion der Linken hervor.

Metadaten

The screenshot shows the golem.de homepage. At the top, there is a navigation bar with links for "HOME", "TICKER", and search fields. Below the header, a banner features the headline "EX-NSA-CHEF HAYDEN" and the sub-headline "Wir töten Menschen auf Basis von Metadaten". A video thumbnail of Michael Hayden speaking is shown on the right.

EX-NSA-CHEF HAYDEN

"Wir töten Menschen auf Basis von Metadaten"

Der frühere NSA-Chef Michael Hayden ist für provokante Äußerungen bekannt. Nun bestätigte er freimütig, zu welchen Zwecken Verbindungsdaten genutzt werden können.

Der frühere US-Geheimdienstchef Michael Hayden hat bestätigt, was durch die Enthüllungen von Edward Snowden schon seit längerem diskutiert wird: "Wir töten Menschen auf der Basis von Metadaten", sagte Hayden vor einigen Wochen auf einer Diskussionsveranstaltung der John-Hopkins-Universität (ab Min. 18:00) in Baltimore. In der Debatte hatte ihm der Juraprofessor David Cole, der das Zitat nun bekanntmachte, vorgehalten, dass es alleine mit Verbindungsdaten möglich sei, über das Leben eines Menschen fast alles zu erfahren. Dies sei "absolut korrekt", sagte Hayden. Allerdings würden die Daten, die von US-Amerikanern gesammelt würden, nicht zum Töten von Menschen eingesetzt.



Ex-NSA-Chef Hayden räumt die Tötung von Menschen auf Basis von Metadaten ein. (Bild: Youtube.com/Screenshot: Golem.de)

Datum: 12.5.2014, 13:37

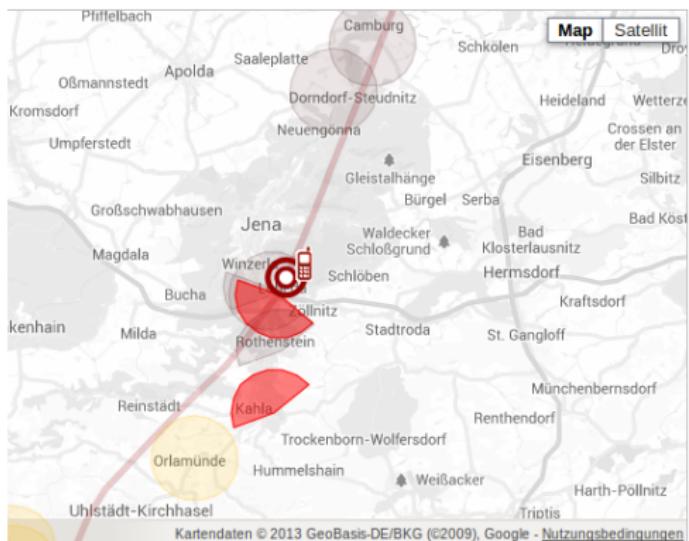
Autor: Friedhelm Greis

Themen: Datenschutz, Edward Snowden, NSA, Prism, Spionage, Verschlüsselung, Whistleblower, Überwachung, Internet, Politik/Recht

Teilen:



Metadaten - VDS



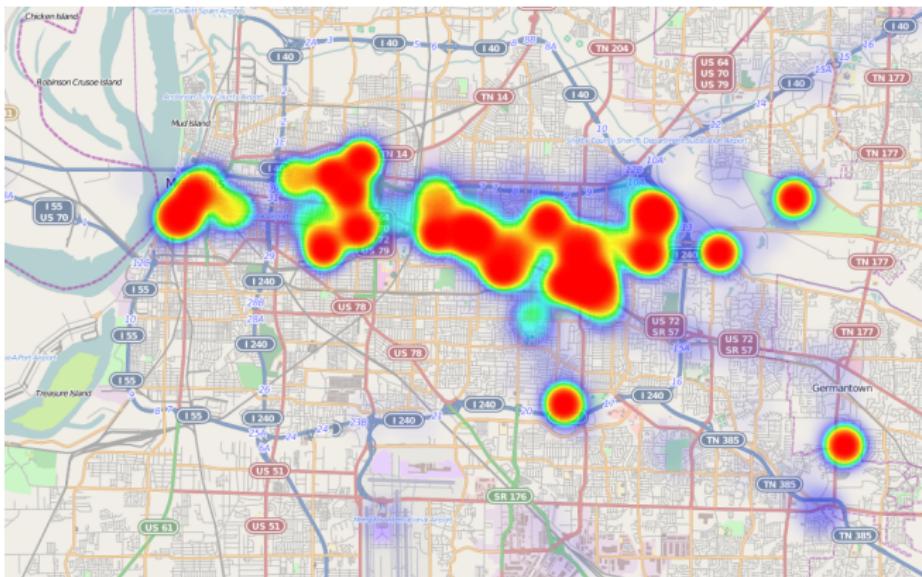
speed
31 Aug 09 15:30

Show the points in time, Malte Spitz was in the selected map segment, too

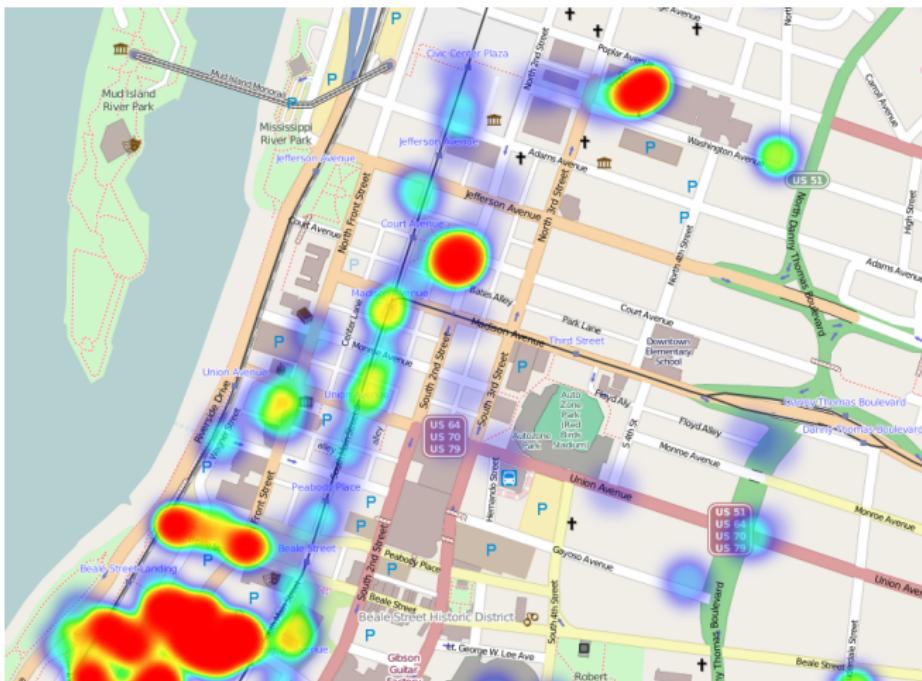
Download Data



Google Takeout



Google Takeout



Zeitstempel

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
0	●	●	●	●	●	●	●	●	●	●	
1	●	●	●	●	●	●	●	●	●	●	
2	●	●	●	●	●	●	●	●	●	●	
3	●	●	●	●	●	●	●	●	●	●	
4	●	●	●	●	●	●	●	●	●	●	
5	
6	

Alan, Microblogging





Zeitstempel

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
0	●	●	●	•							•	•	•			●	•	•	•	●	•	●	•	•
1	●	●		•	•	•					•		•	•	•	●	●	●	●	●	●		●	●
2	●		•	●	•	•							•		●	●	●	●	●	●	●	●	●	●
3	●			●									•		●	●	●	●	●	●	●	●		●
4	●	●		•	•	•	•	•	•	•	•	●	•	•		●	●	●	●	●	●	●	●	●
5	●	●	●	•	•	•									●	●	●	●	●	●	●	●	●	●
6	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●

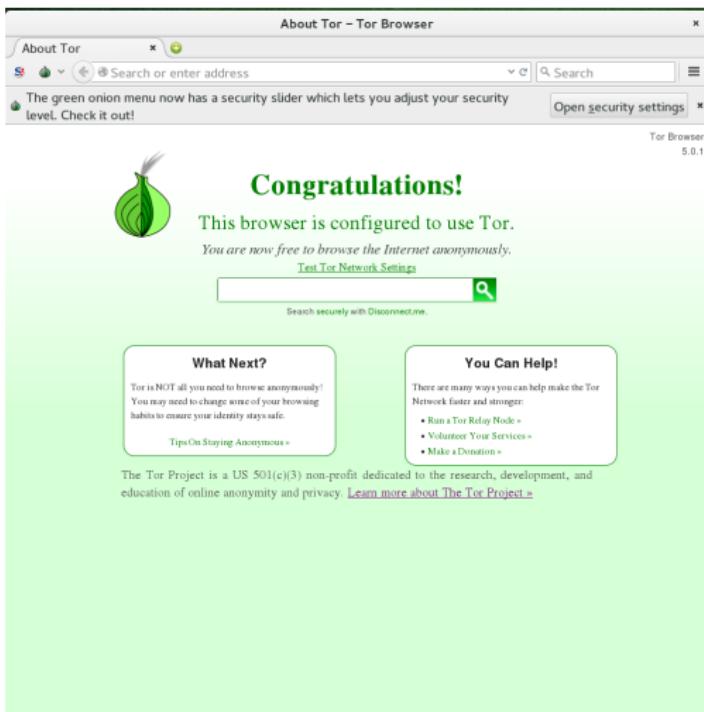
Bob, Microblogging

Zeitstempel

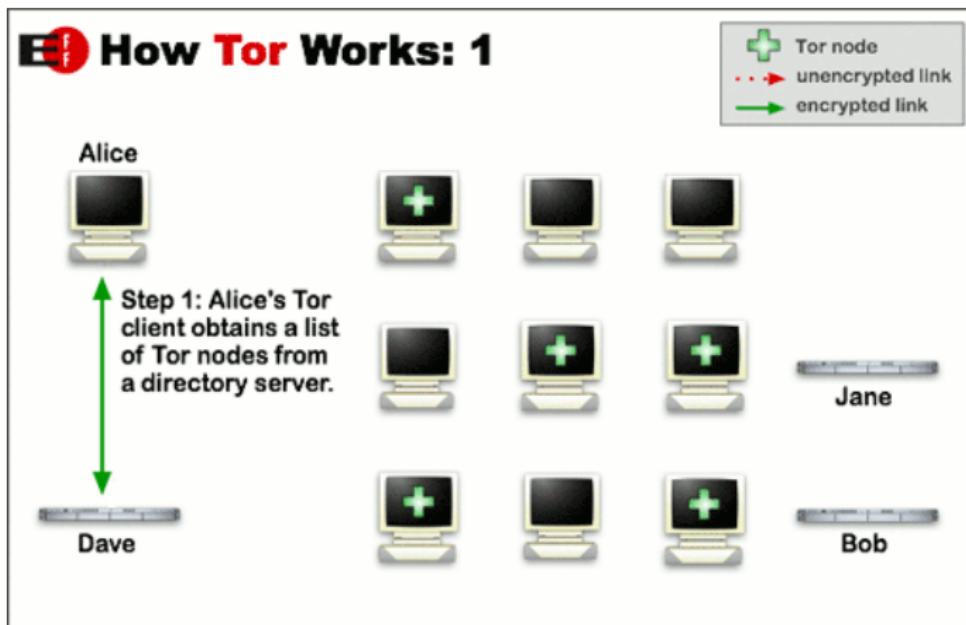
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
0	•	•																						•
1		•	•													•	•	•		•		•	•	•
2		•			•													•	•					•
3																•	•	•	•	•	•	•	•	•
4		•	•	•													•	•	•	•	•	•	•	•
5	•	•	•	•	•	•											•	•	•	•	•	•		•
6	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	

Charlie, Github

Tor

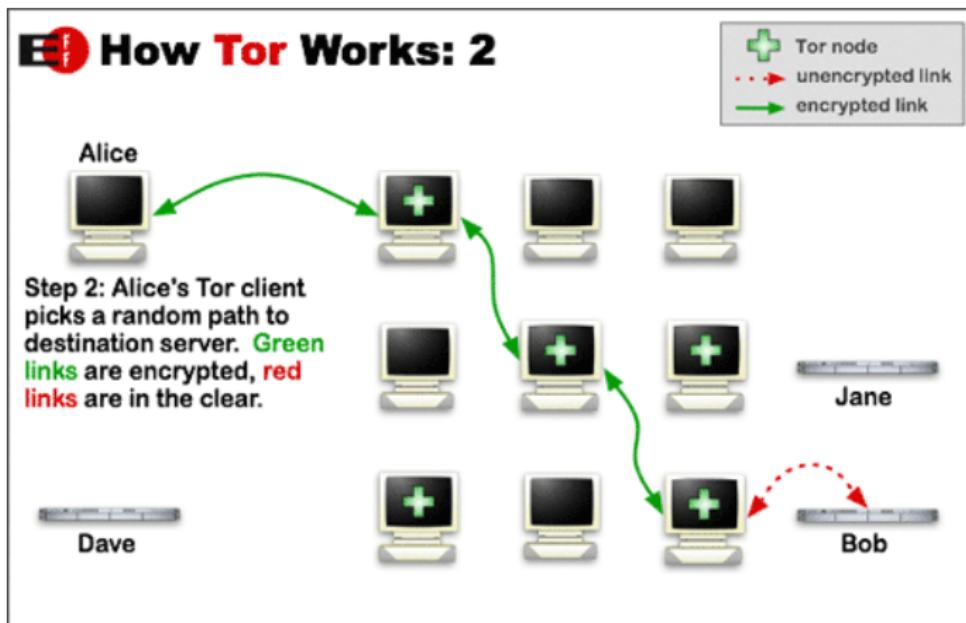


Tor



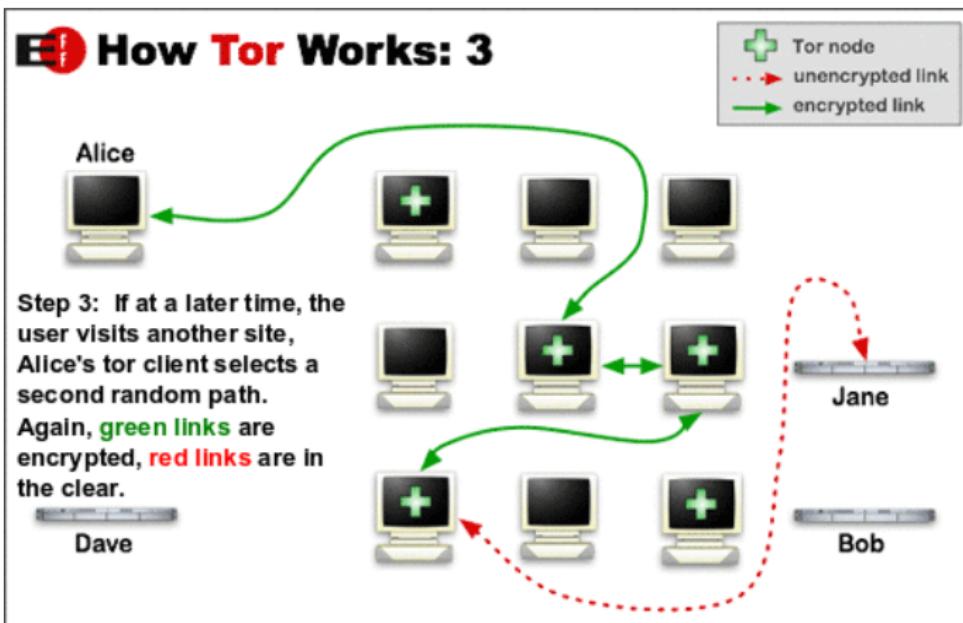
Grafik: The Tor Project

Tor



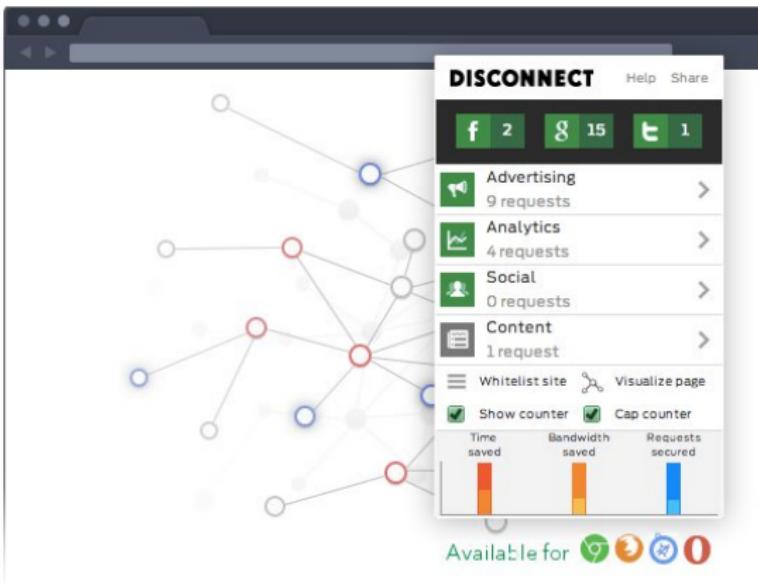
Grafik: The Tor Project

Tor

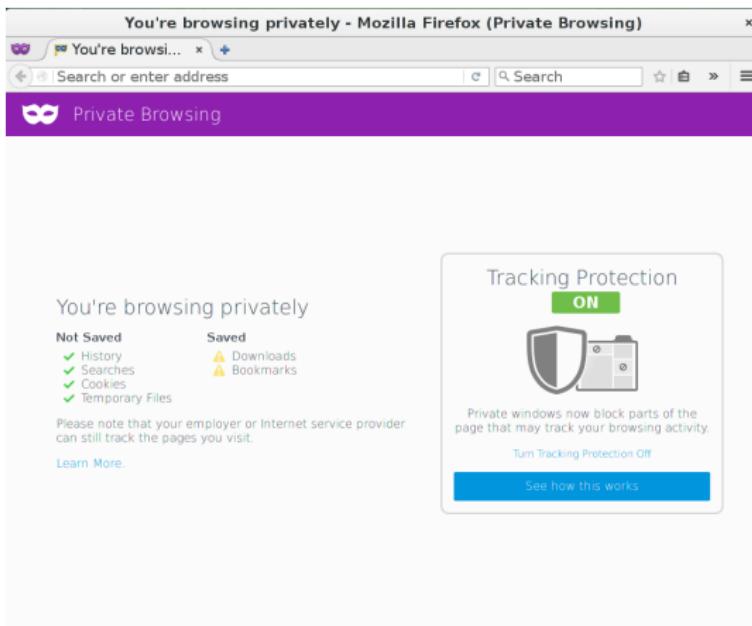


Grafik: The Tor Project

Disconnect, Privacy Badger (EFF), Ghostery



Antitracking im Firefox Privatmodus



Passwörter



Passwörter

- Keine einfachen Wörter

Passwörter

- Keine einfachen Wörter
- Groß-, Kleinbuchstaben, Ziffern, Sonderzeichen

Passwörter

- Keine einfachen Wörter
- Groß-, Kleinbuchstaben, Ziffern, Sonderzeichen
- Beispiele:

Passwörter

- Keine einfachen Wörter
- Groß-, Kleinbuchstaben, Ziffern, Sonderzeichen
- Beispiele:
 - dragon

Passwörter

- Keine einfachen Wörter
- Groß-, Kleinbuchstaben, Ziffern, Sonderzeichen
- Beispiele:
 - dragon
 - (nCuAj.§Tsm!f

Passwörter

- Keine einfachen Wörter
- Groß-, Kleinbuchstaben, Ziffern, Sonderzeichen
- Beispiele:
 - dragon
 - (nCuAj.§Tsm!f
 - IchLiebeDich

Passwörter

- Keine einfachen Wörter
- Groß-, Kleinbuchstaben, Ziffern, Sonderzeichen
- Beispiele:
 - dragon
 - (nCuAj.§Tsm!f
 - IchLiebeDich
 - .§)=/)='

Passwörter

- Keine einfachen Wörter
- Groß-, Kleinbuchstaben, Ziffern, Sonderzeichen
- Beispiele:
 - dragon
 - (nCuAj.§Tsm!f
 - IchLiebeDich
 - .§)=/)='
 - qwerty

Passwörter

- Keine einfachen Wörter
- Groß-, Kleinbuchstaben, Ziffern, Sonderzeichen
- Beispiele:
 - dragon
 - (nCuAj.§Tsm!f
 - IchLiebeDich
 - .§)=/)='
 - qwerty
 - Mks?o/.u,1Psw!

Passwörter

- Keine einfachen Wörter
- Groß-, Kleinbuchstaben, Ziffern, Sonderzeichen
- Beispiele:
 - dragon
 - (nCuAj.§Tsm!f
 - IchLiebeDich
 - .§)=/)='
 - qwerty
 - Mks?o/.u,1Psw!

Passwörter

- Keine einfachen Wörter
- Groß-, Kleinbuchstaben, Ziffern, Sonderzeichen
- Beispiele:
 - dragon
 - (nCuAj.§Tsm!f
 - IchLiebeDich
 - .§)=/)='
 - qwerty
 - Mks?o/.u,1Psw!
- Verschiedene Passwörter nutzen!

Passwörter

- Keine einfachen Wörter
- Groß-, Kleinbuchstaben, Ziffern, Sonderzeichen
- Beispiele:
 - dragon
 - (nCuAj.§Tsm!f
 - IchLiebeDich
 - .§)=/)='
 - qwerty
 - Mks?o/.u,1Psw!
- Verschiedene Passwörter nutzen!
- Passwort-Manager verwenden
(z.B. Keepass, Password Safe)

Fazit

- Verschlüsselung nutzen (HTTPS Everywhere, Signal, PGP)
- Anonymisieren (Antitracking-Plugins, Tor)
- Dezentrale Dienste nutzen (Email, Jabber, Owncloud)
- Endgeräte schützen (Rechte einschränken, Freie Software)



Folien: Chaos Computer Club Dresden

CMS Dresden: schule@c3d2.de

Vortragender: Marius Melzer (marius@rasumi.net,

PGP-Fingerprint: 6730 E691 36B9 9BB8 FFB1 2662 A97B

F176 52DE FC3E)

