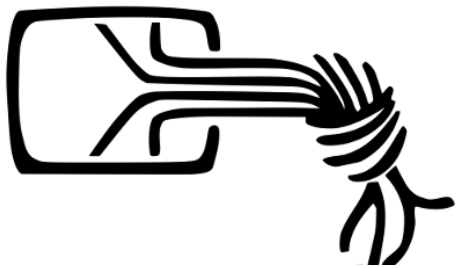
Digitale Selbstverteidigung

Marius Melzer (CCC Dresden)

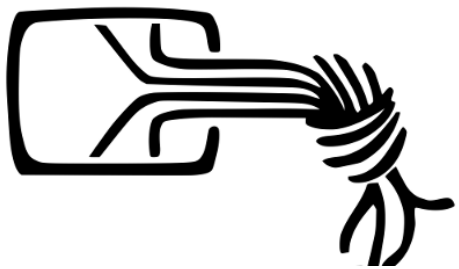
08.06.2016

Chaos Computer Club



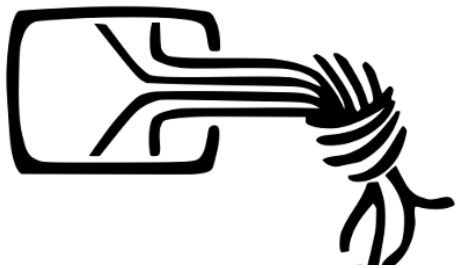
- Verein wurde 1981 gegründet (`https://ccc.de`)

Chaos Computer Club



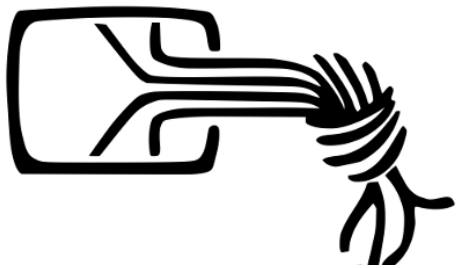
- Verein wurde 1981 gegründet (`https://ccc.de`)
- Aktuell > 6000 Mitglieder

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 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`)
- IT4Refugees

Chaos Computer Club

- Chaos Computer Club Dresden (`https://c3d2.de`)
- Datenspuren: Herbst 2016 (`https://datenspuren.de`)
- Podcasts (`https://c3d2.de/radio.html`)
- IT4Refugees
- Chaos macht Schule (`https://c3d2.de/schule.html`)

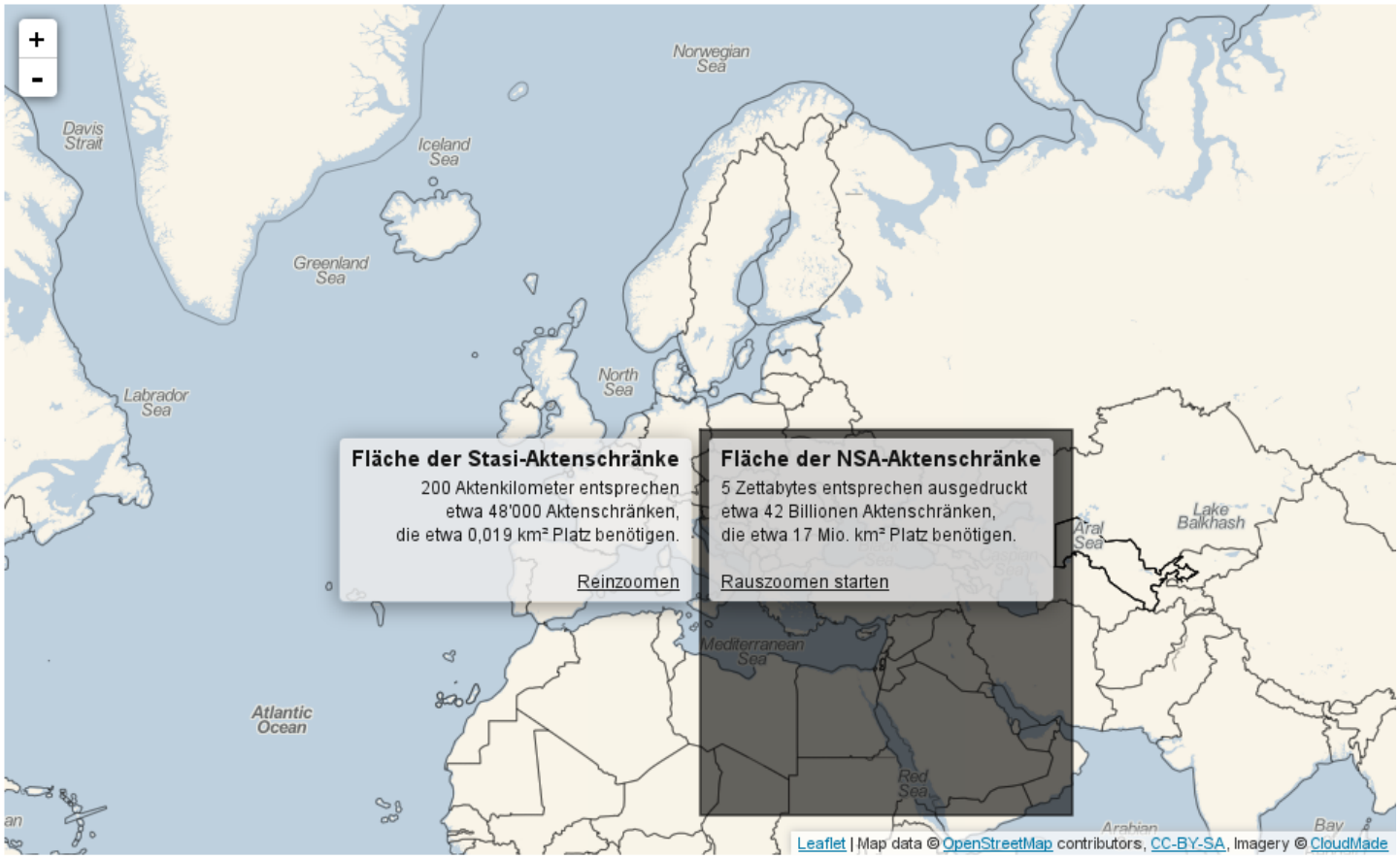
Bundespräsident Gauck zur NSA-Überwachung

"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



Realisiert von OpenDataCity. Anwendung steht unter CC-BY 3.0.

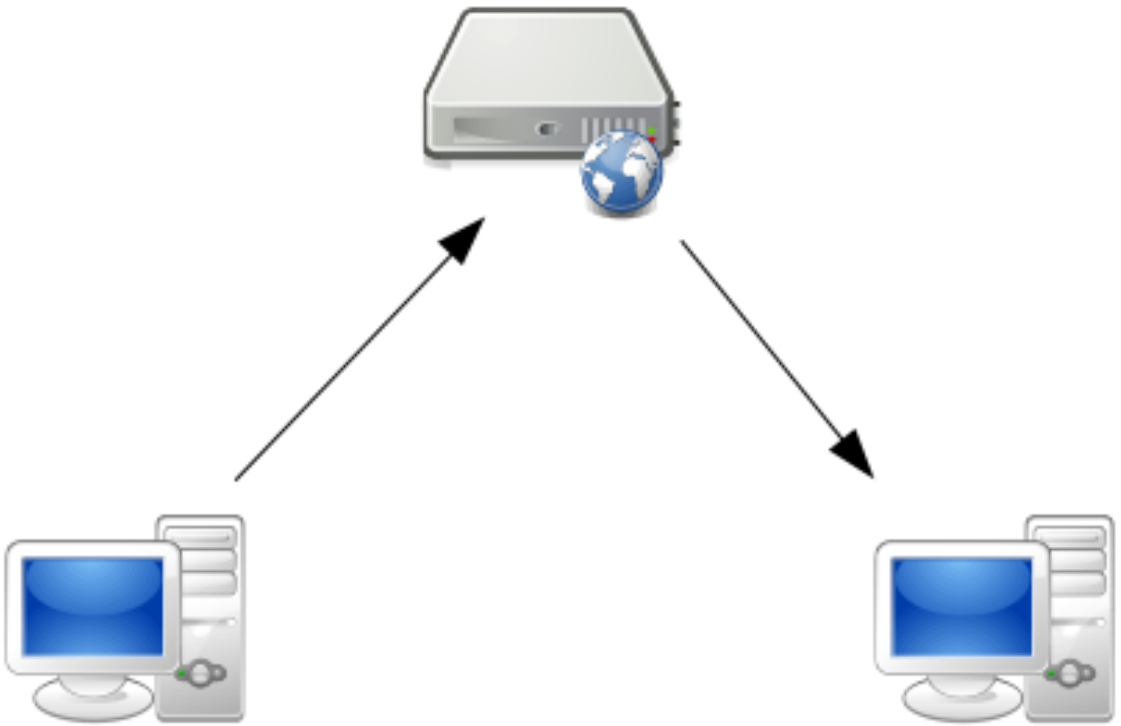
Samsung vs. 1984

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.

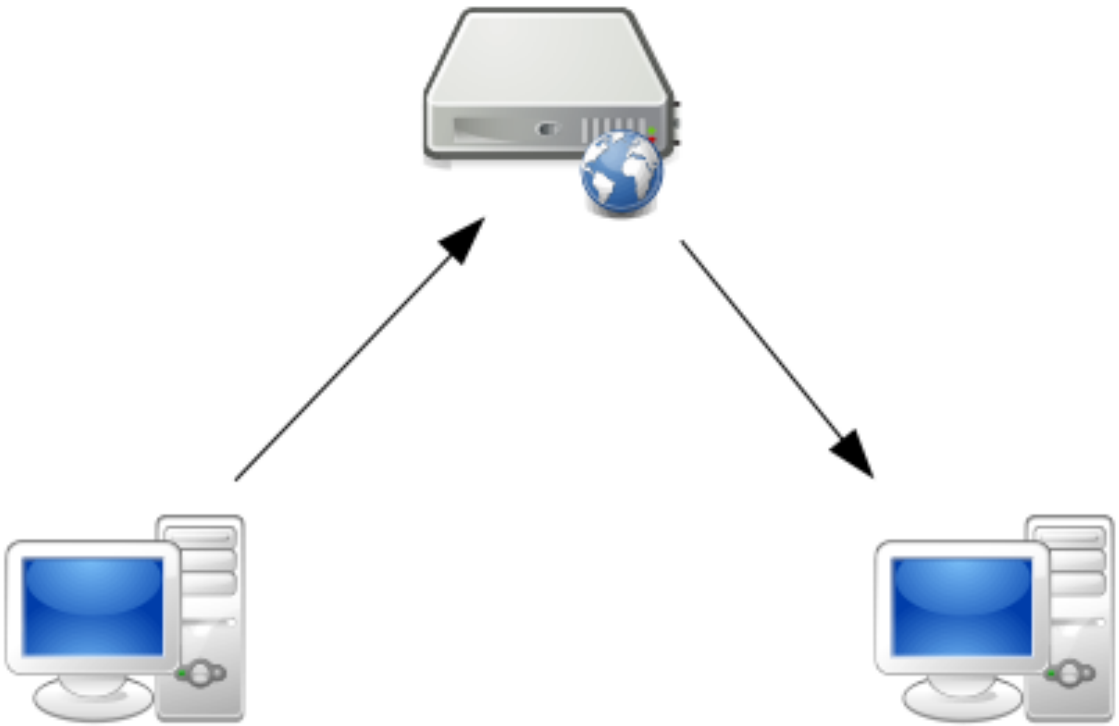
If you do not enable Voice Recognition, you will not be able to use interactive voice recognition features, although you may be able to control your TV using certain predefined voice commands. While Samsung will not collect your spoken word, Samsung may still collect associated texts and other usage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

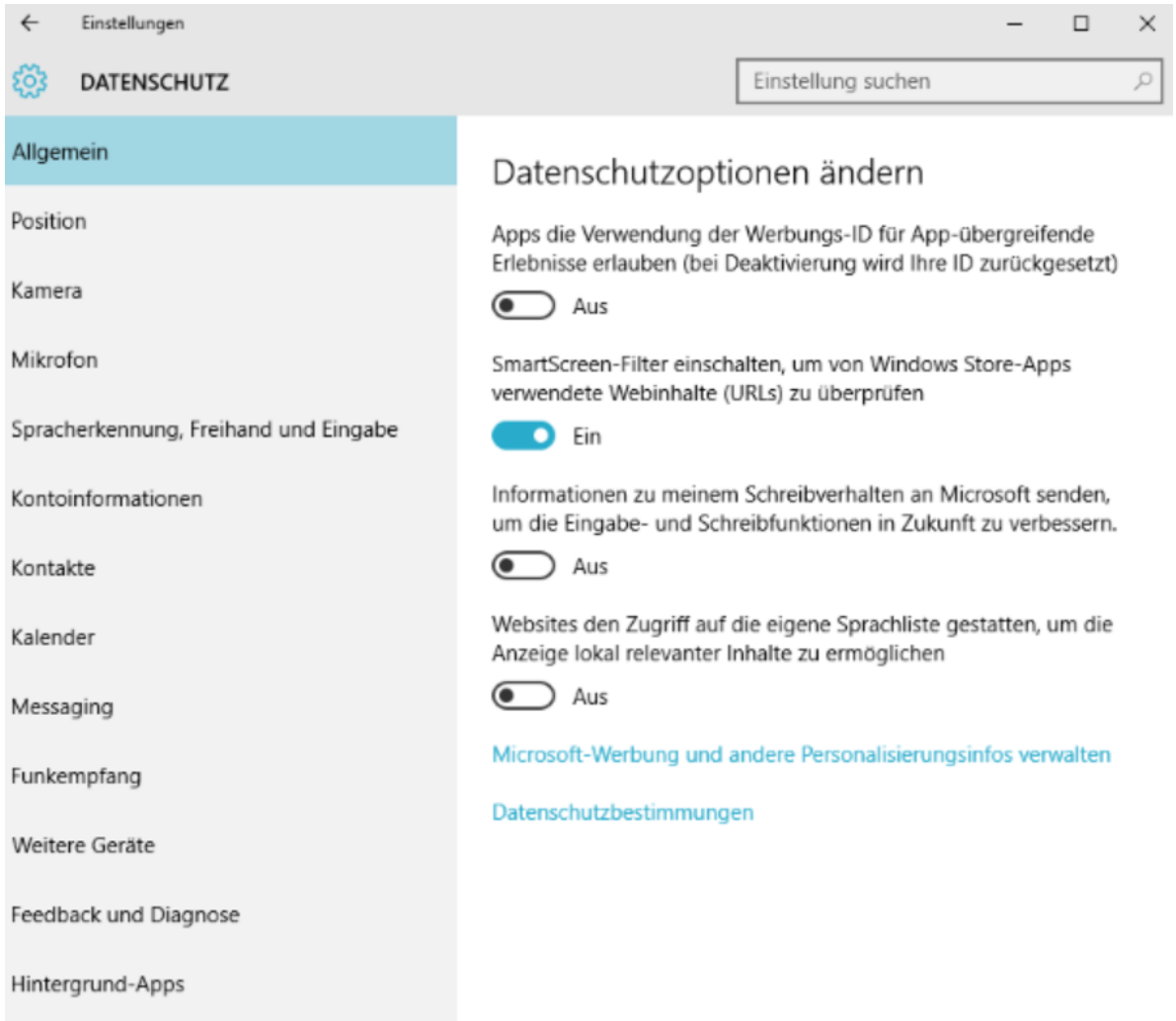
Wie kommunizieren wir im Internet?



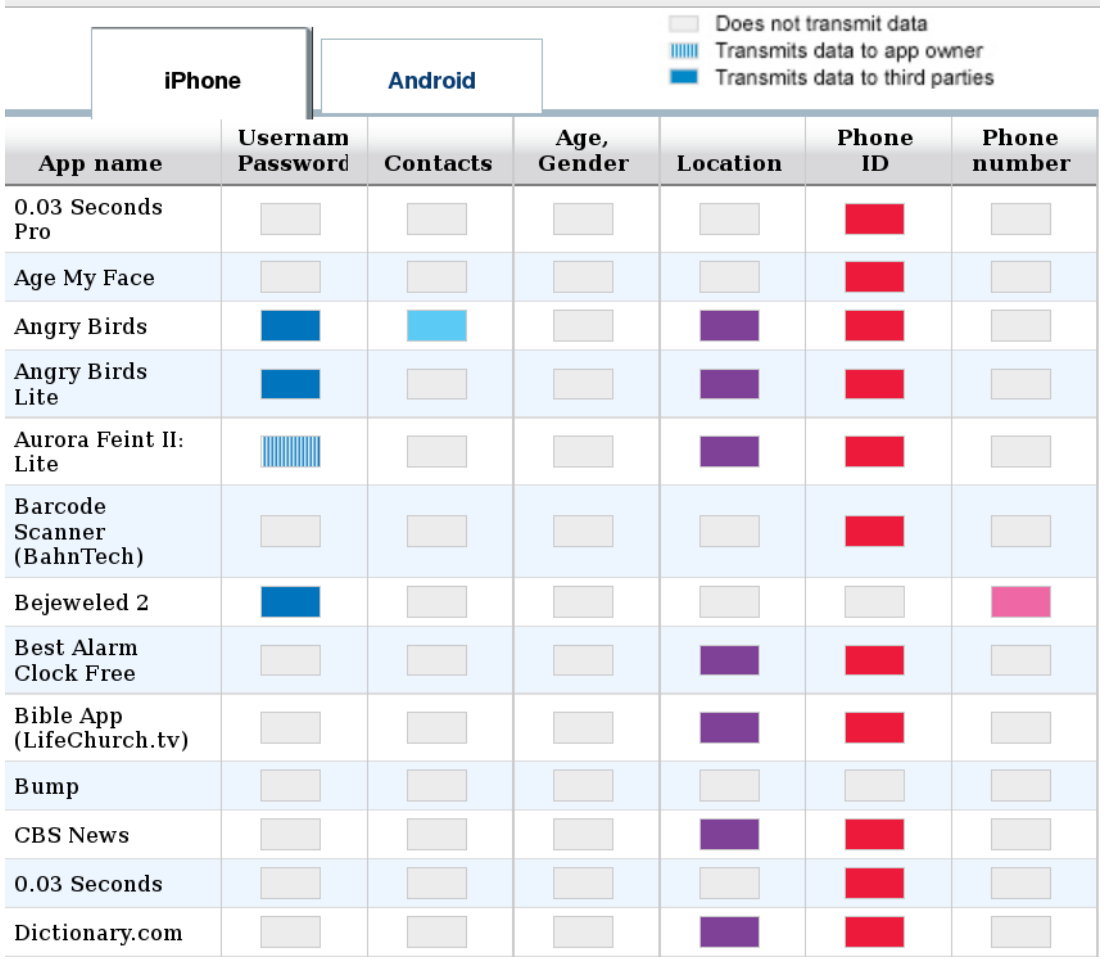
Was ist zu schützen?



Unerwünschte Funktionalität



Unerwünschte Funktionalität



iPhone | Android

Does not transmit data
Transmits data to app owner
Transmits data to third parties

App name	Usernam 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						

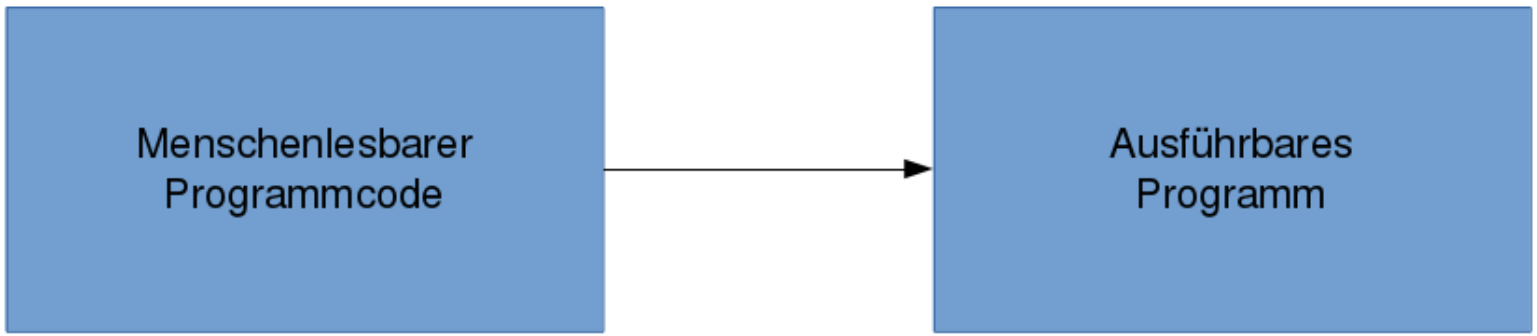
Wie schütze ich meine Geräte?

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

Vertrauenswürdige Software?

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

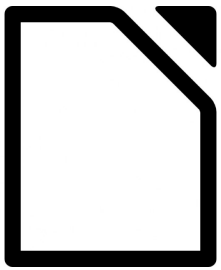
Kompilierung von Software



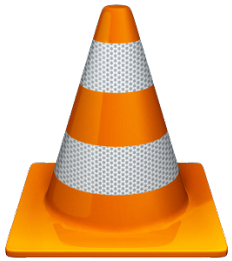
Freie Software auf Computern

Firefox

Thunderbird



LibreOffice



VLC Media Player

Freie Software auf dem Smartphone

F-Droid
Android-Appstore für freie Software

iOS Open Source Apps
`https://github.com/dkhamsing/open-source-ios-apps`

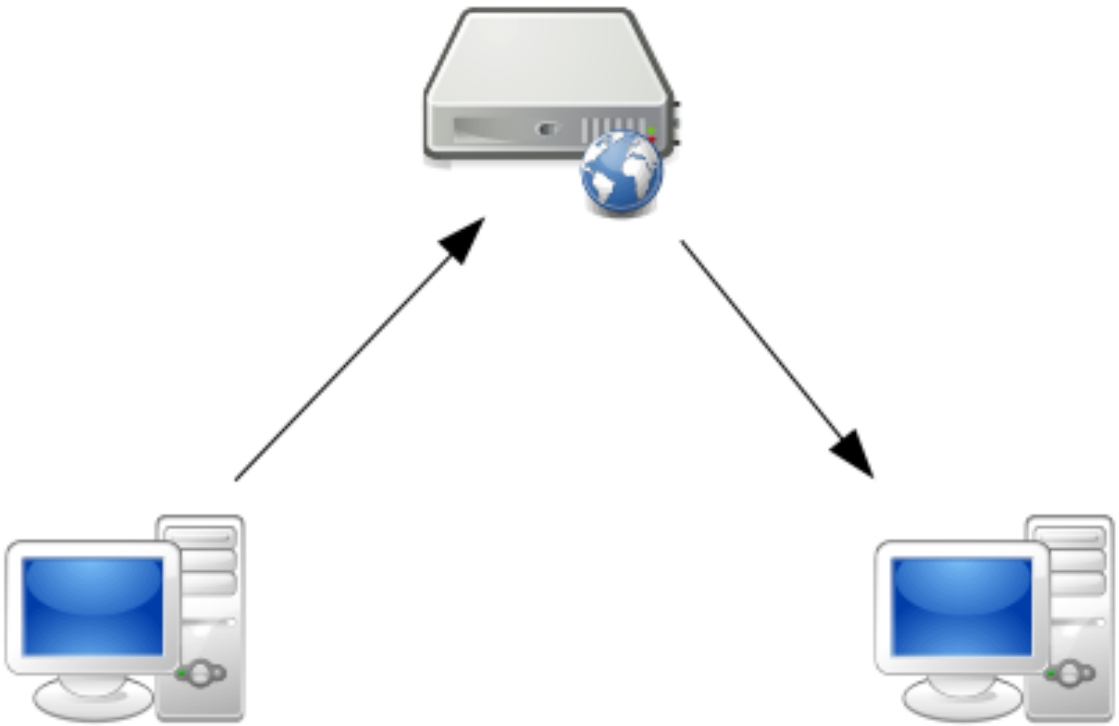
Cyanogenmod, Replicant

- basiert auf Open Source Teil von Android
- ersetzt teilweise die proprietären Apps durch freie
- **Problem:** Verlust der Garantie bei Installation

Ubuntu Phone, Sailfish OS

Geräteverschlüsselung

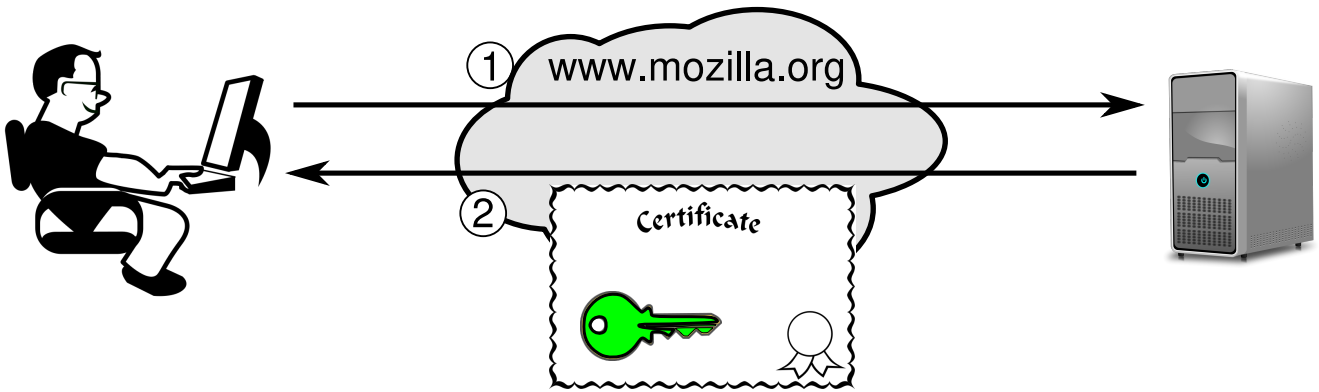
Was ist zu schützen?



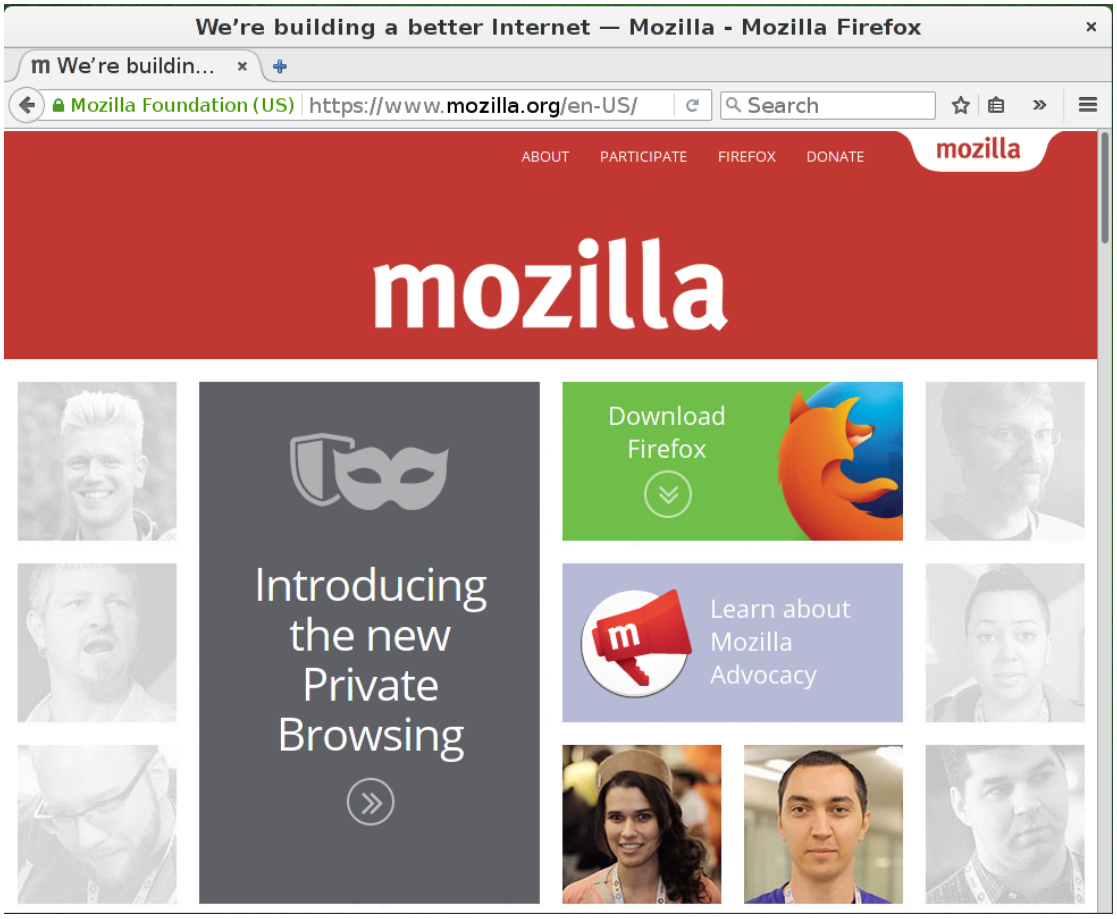
Angreifer im eigenen Netz

Transportwegverschlüsselung

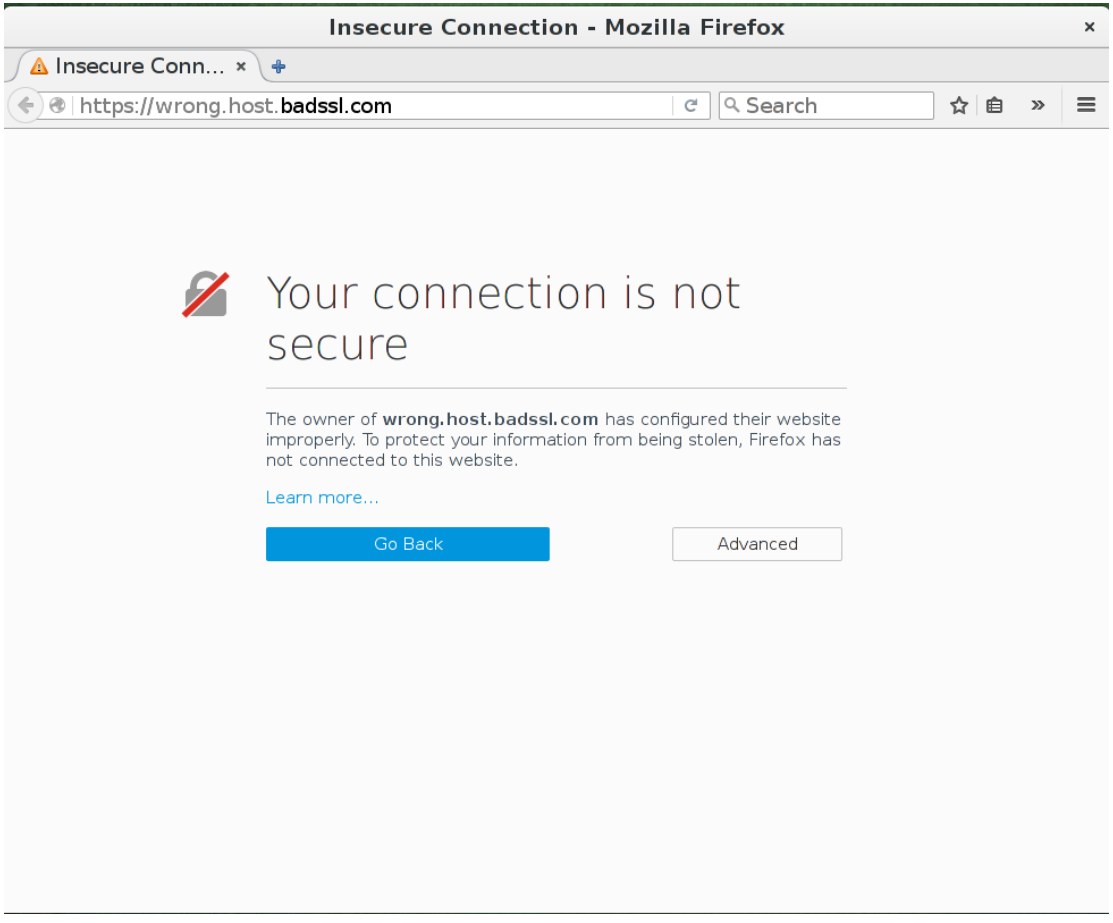
SSL = Secure Socket Layer / TLS = Transport Layer Security



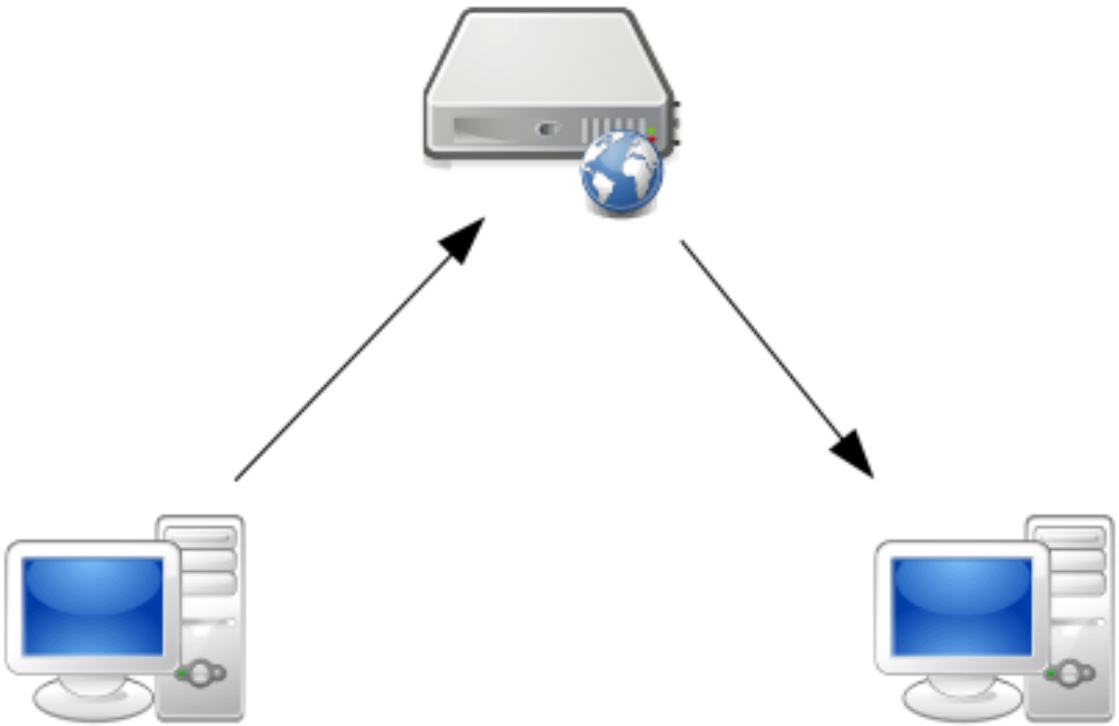
SSL im Browser



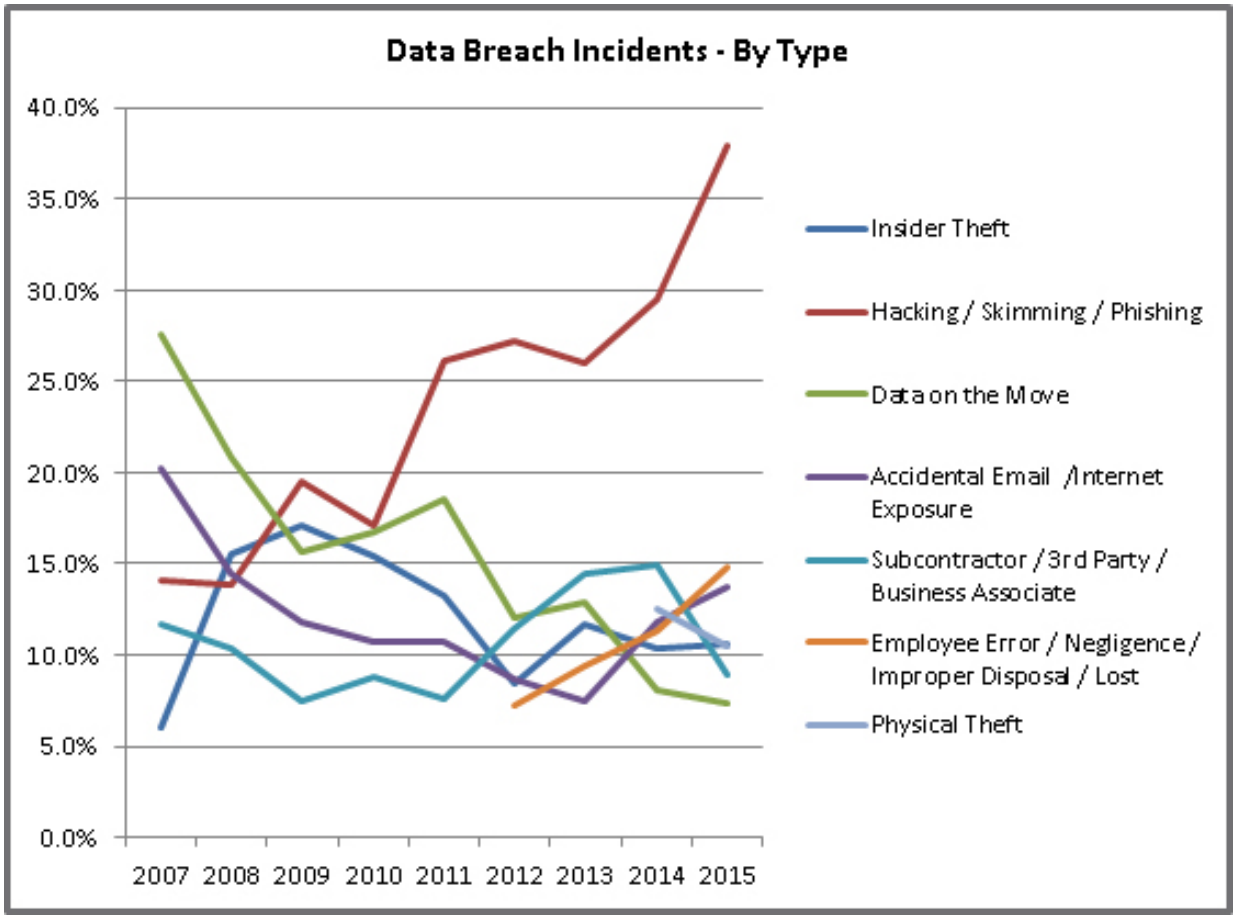
Ungültiges Zertifikat



Was ist zu schützen?



Informationsleaks



http://www.idtheftcenter.org/ITRC-Surveys-Studies/2015databreaches.html

Ende-zu-Ende-Verschlüsselung

- PGP für E-Mails

Ende-zu-Ende-Verschlüsselung

- PGP für E-Mails
- OTR/OMEMO für Jabber:
  - Pidgin für Linux und Windows
  - Conversations oder ChatSecure für Android
  - Adium für Mac, ChatSecure für iOS

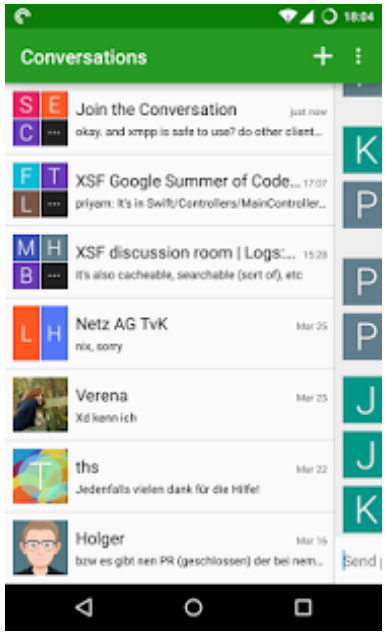
Ende-zu-Ende-Verschlüsselung

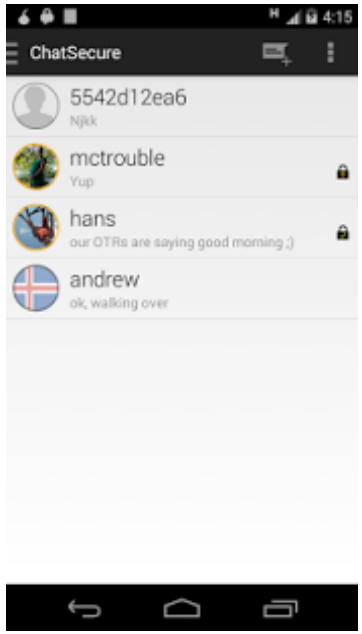
- PGP für E-Mails
- OTR/OMEMO für Jabber:
  - Pidgin für Linux und Windows
  - Conversations oder ChatSecure für Android
  - Adium für Mac, ChatSecure für iOS
- palava.tv, Tox, Linphone für Videotelefonie

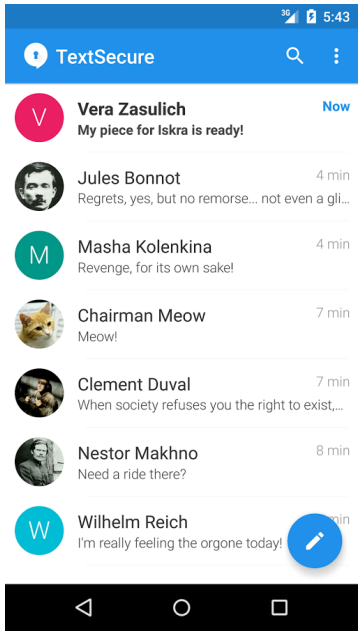
Ende-zu-Ende-Verschlüsselung

- PGP für E-Mails
- OTR/OMEMO für Jabber:
  - Pidgin für Linux und Windows
  - Conversations oder ChatSecure für Android
  - Adium für Mac, ChatSecure für iOS
- palava.tv, Tox, Linphone für Videotelefonie
- Signal

Alternative Messenger







`https://xmpp.net/directory.php`

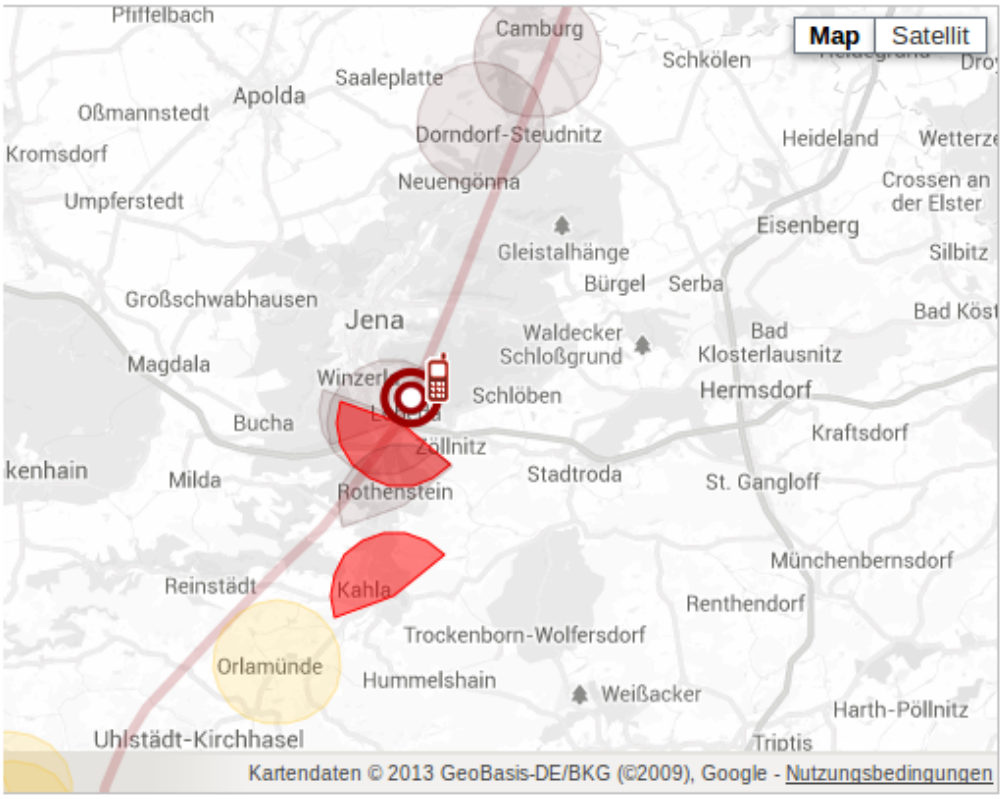
Aktuelle Cryptowelle

Facebook, Google and WhatsApp plan to increase encryption of user data

Spurred on by Apple's battles against the FBI, some of tech's biggest names are to expand encryption of user data in their services, the Guardian can reveal

Work on new encryption projects began before Apple entered a court battle with US authorities over the San Bernardino killer's iPhone. Photograph: Philippe Huguen/AFP/Getty Images

Metadaten - VDS



peed

31 Aug 09 15:30

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

Monday, 31 August 2009

Malte Spitz gives a speech to the Greens in Erfurt against internet censorship.
(source: Parteiwebsite)

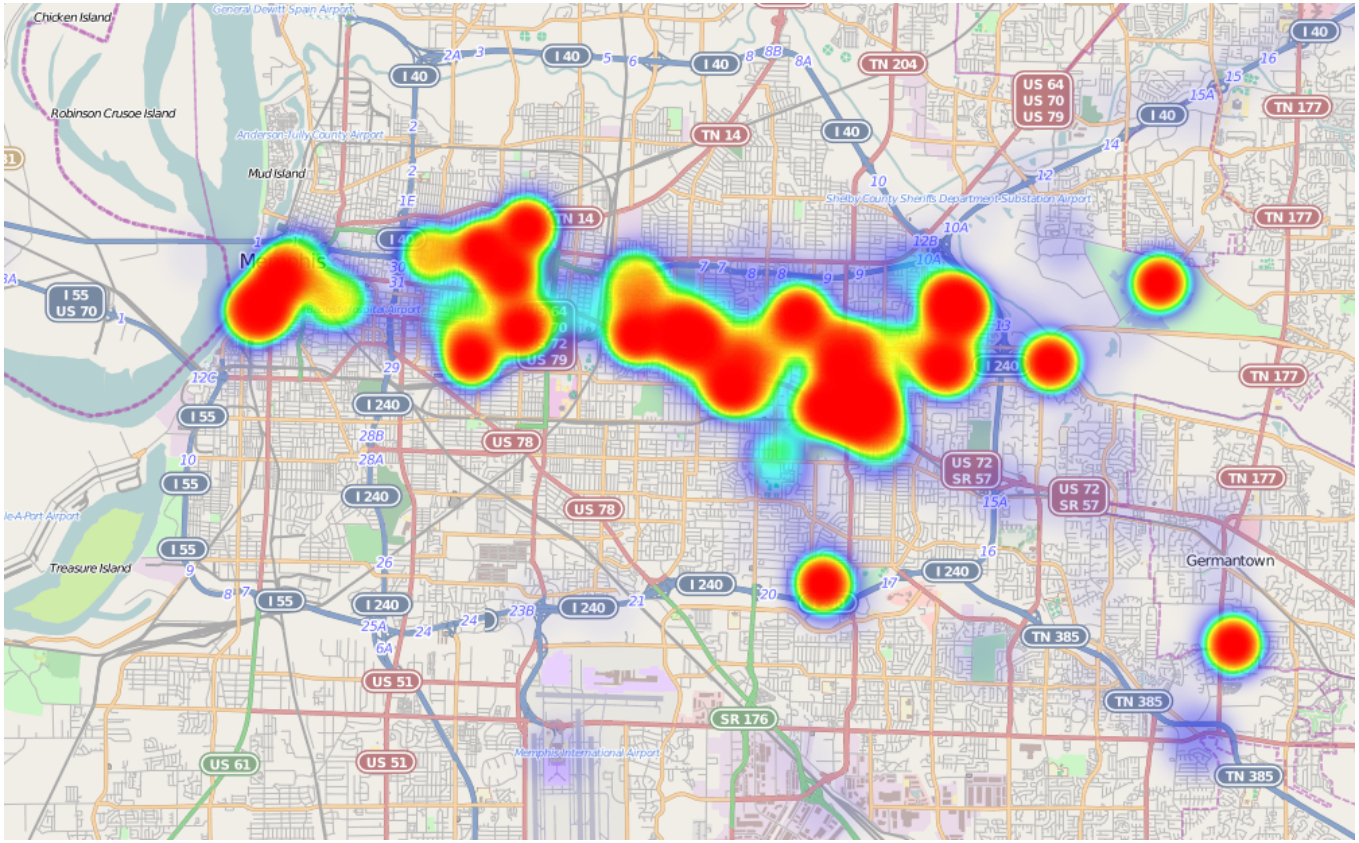
6 incoming calls
21 outgoing calls
total time: 1h 16min 8s

34 incoming messages
29 outgoing messages

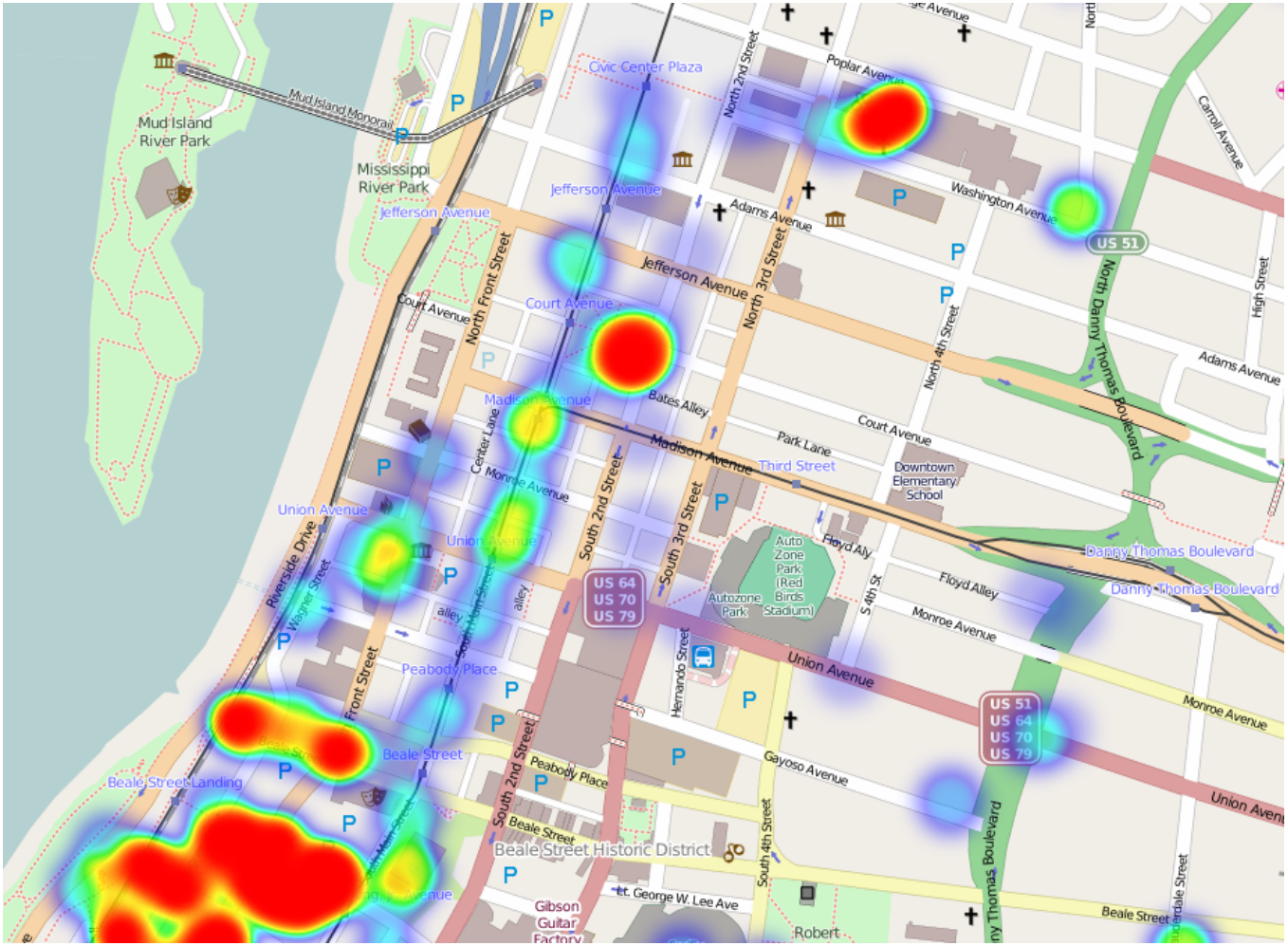
duration of internet connection:
21h 17min 25s

Download Data

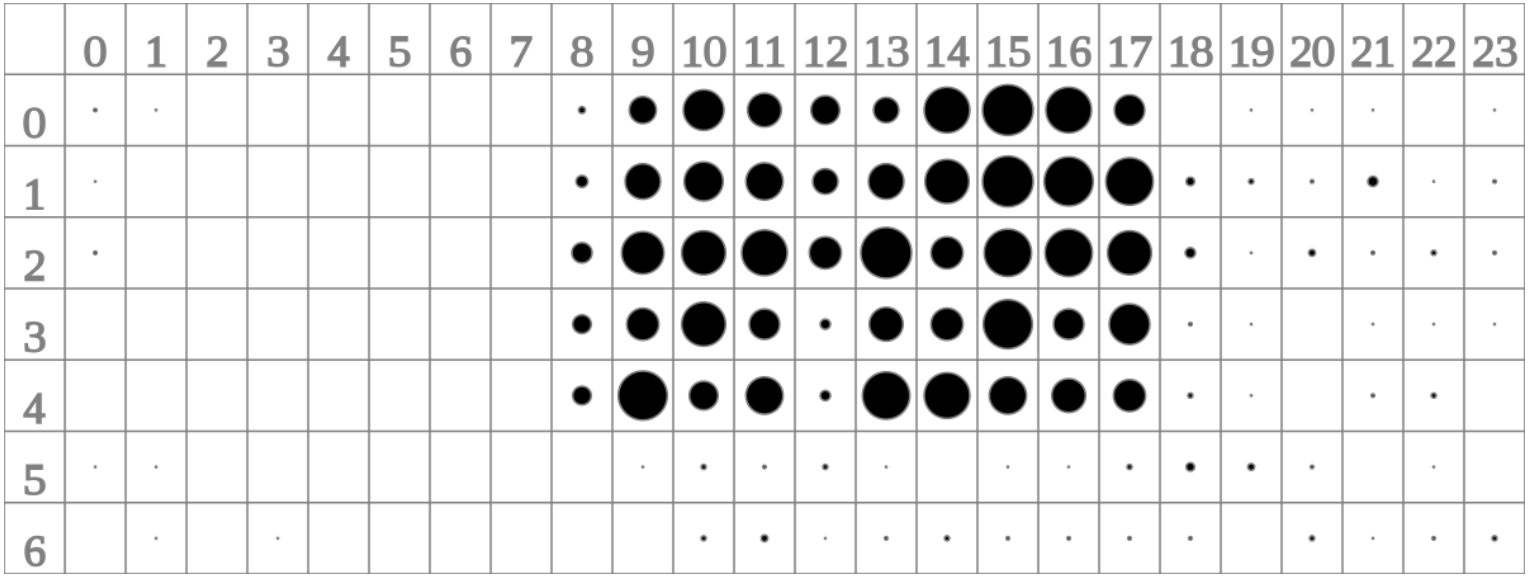
Google Takeout



Google Takeout

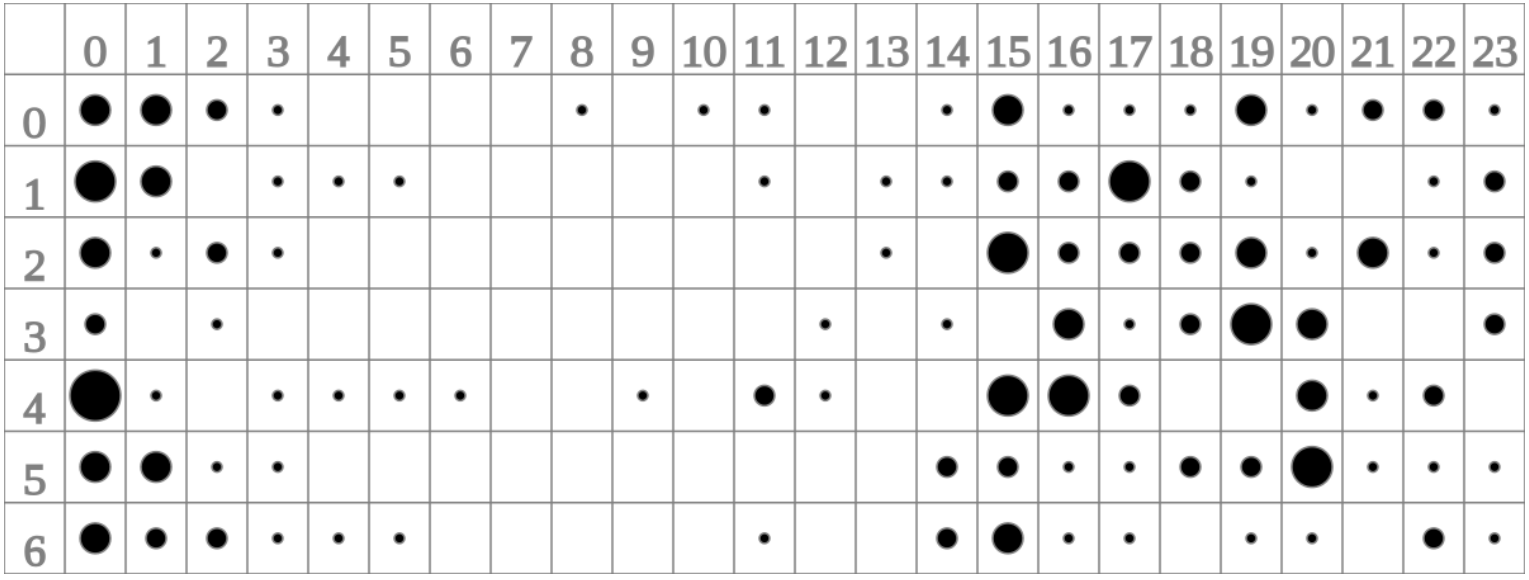


Zeitstempel



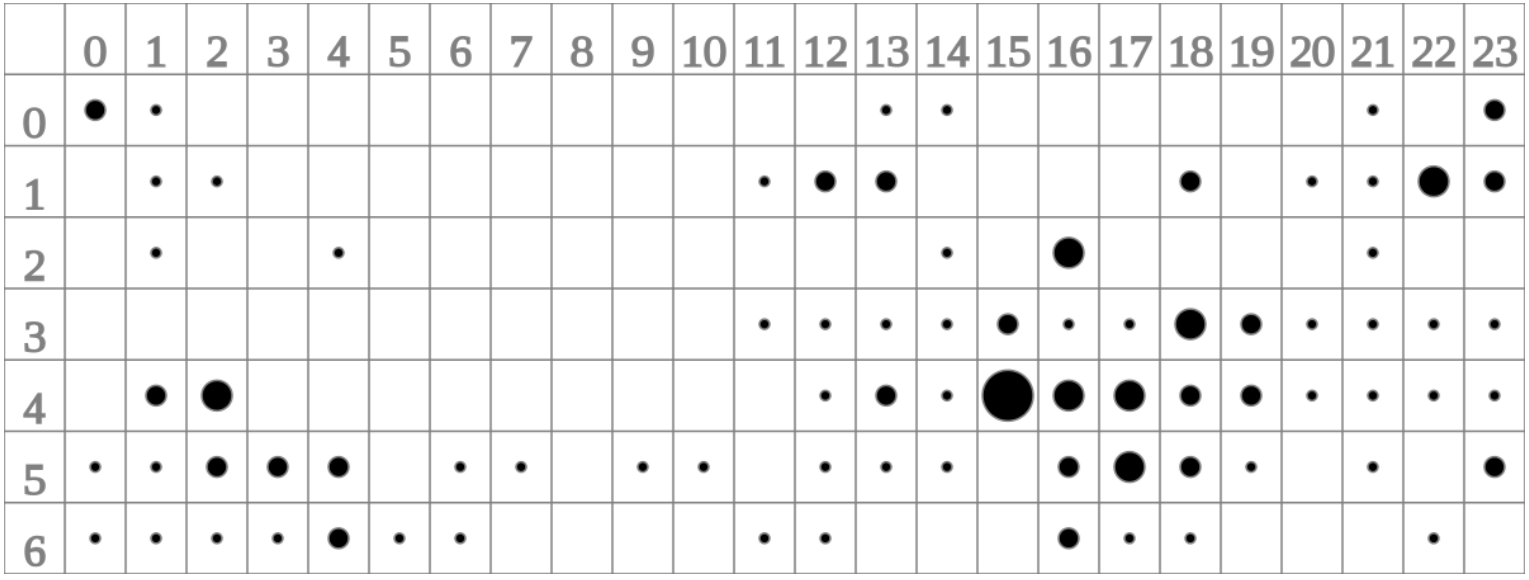
Alan, Microblogging

Zeitstempel



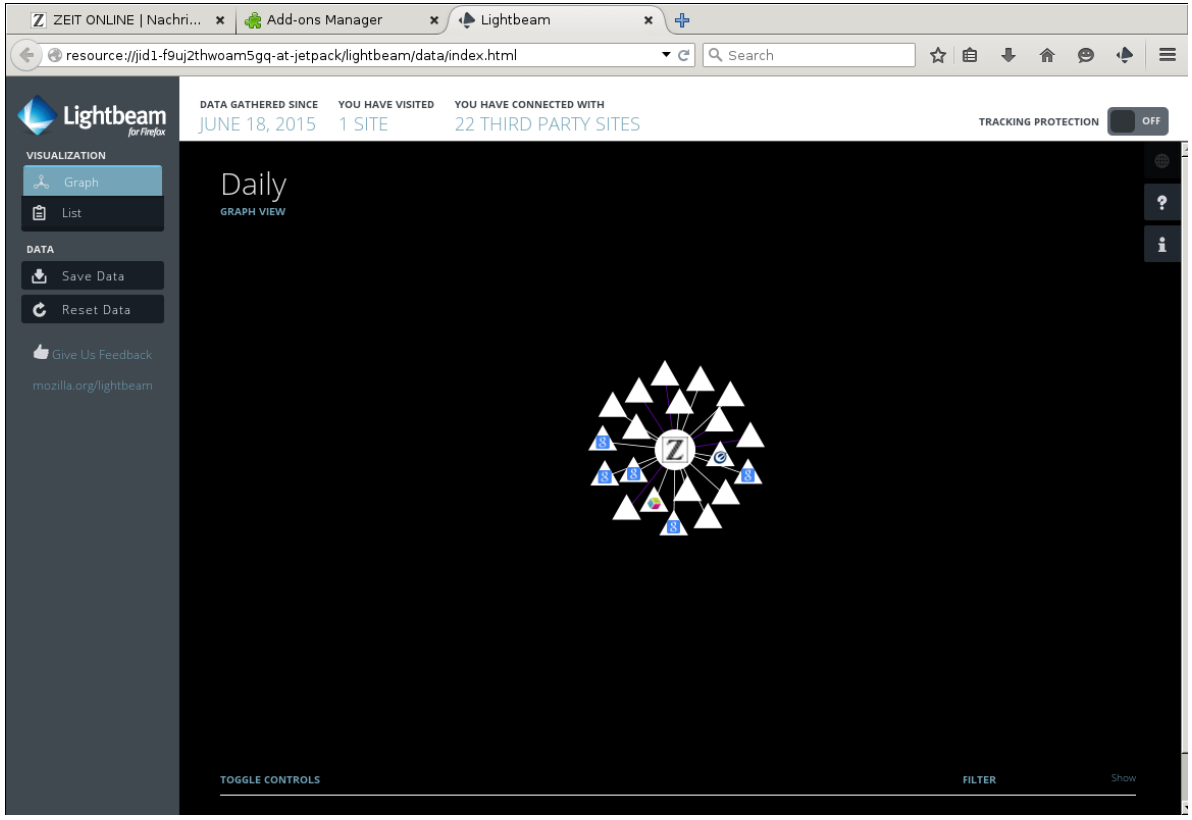
Bob, Microblogging

Zeitstempel

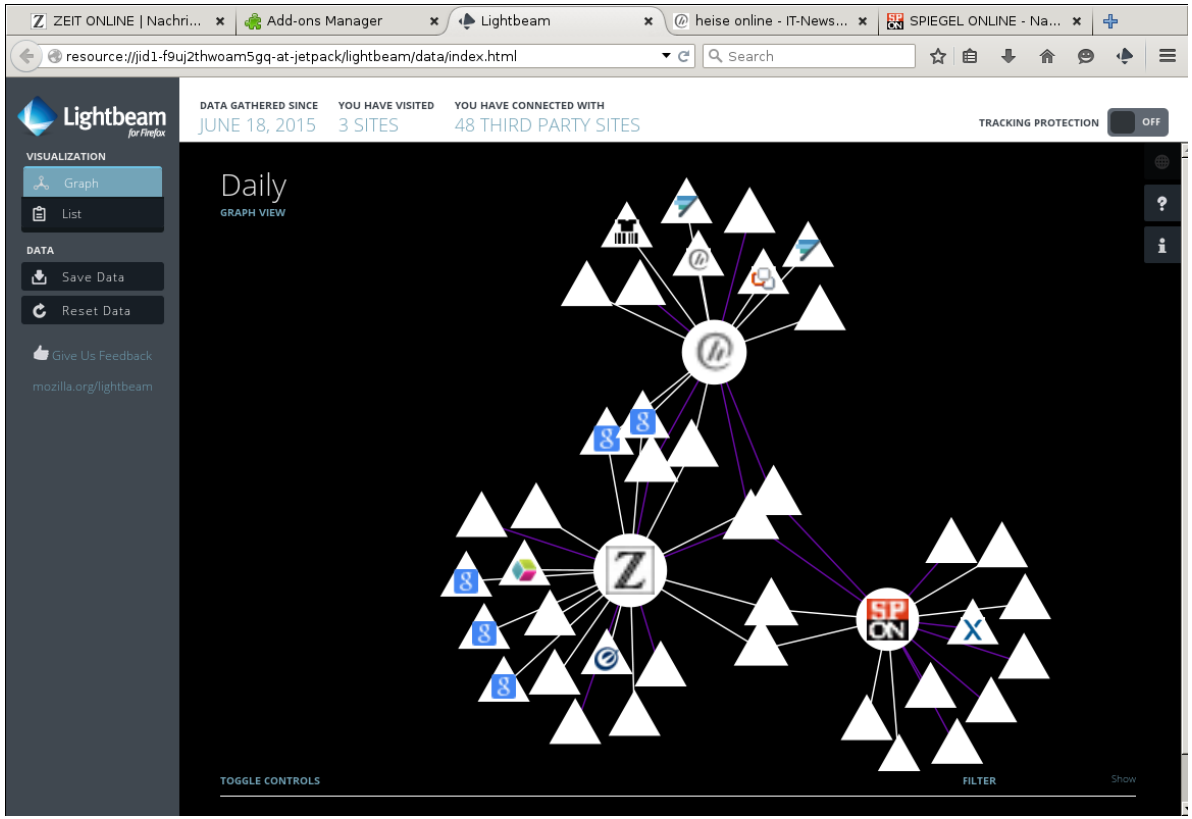


Charlie, Github

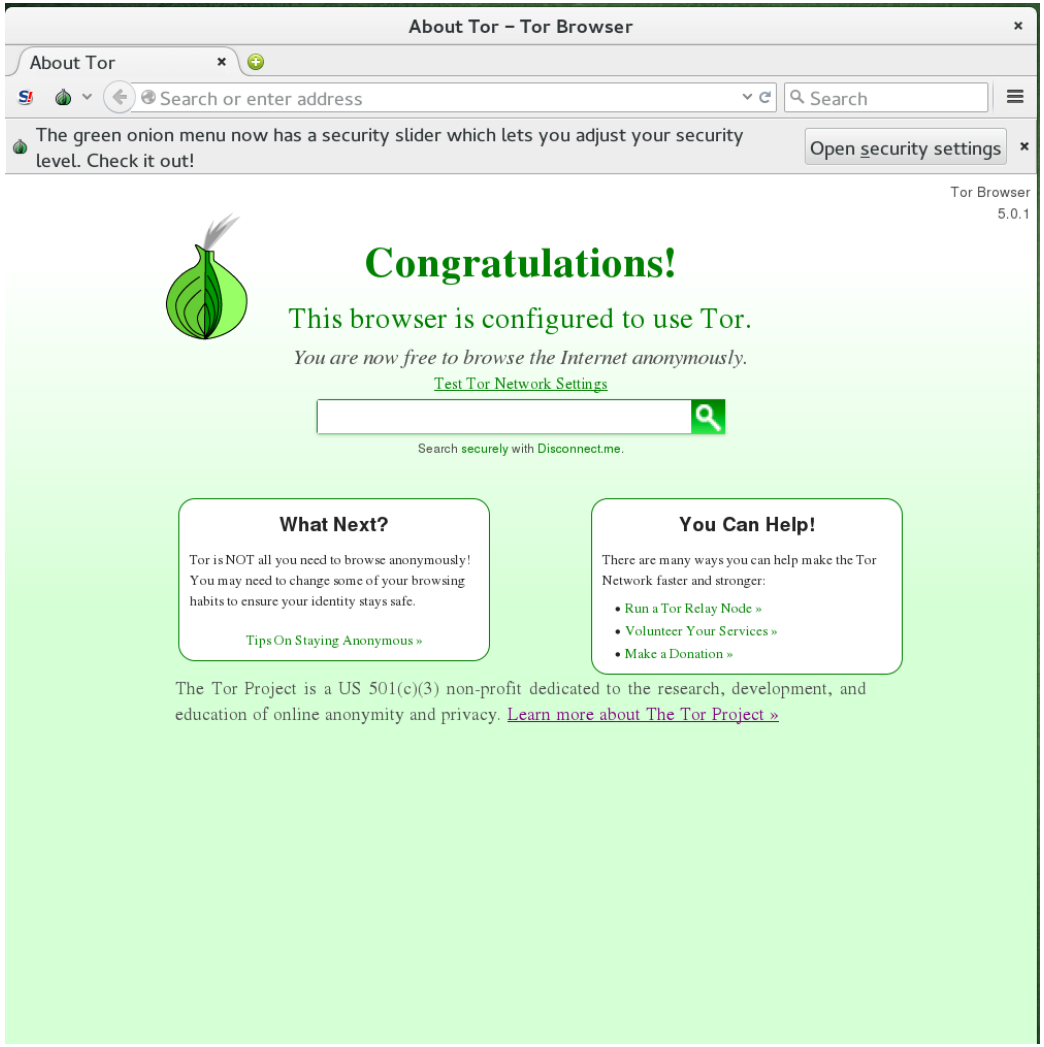
Metadaten im WWW



Metadaten im WWW



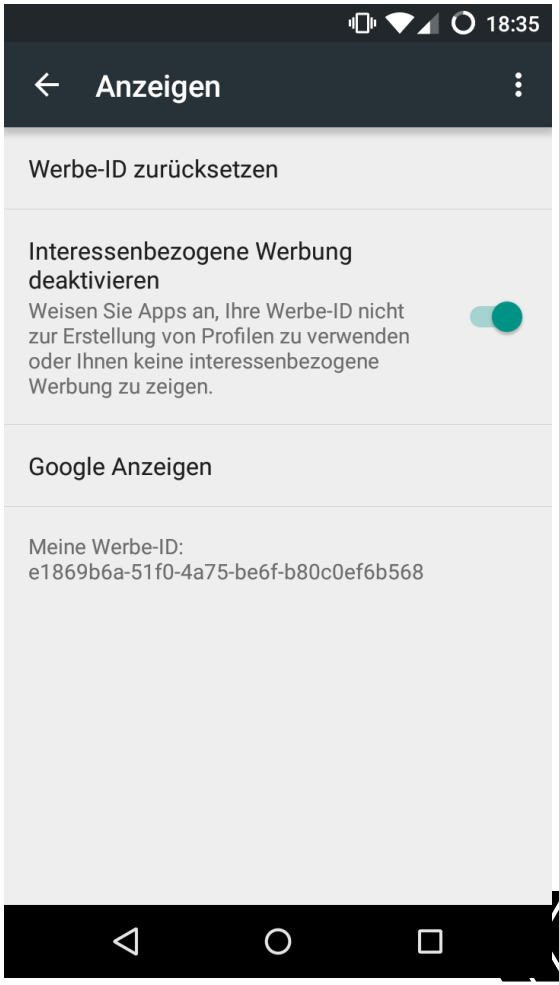
Tor


About Tor – Tor Browser
About Tor
Search or enter address
Search
The green onion menu now has a security slider which lets you adjust your security level. Check it out!
Open security settings
Tor Browser 5.0.1
Congratulations!
This browser is configured to use Tor.
You are now free to browse the Internet anonymously.
Test Tor Network Settings
Search securely with Disconnect.me.
What Next?
Tor is NOT all you need to browse anonymously! You may need to change some of your browsing habits to ensure your identity stays safe.
Tips On Staying Anonymous »
You Can Help!
There are many ways you can help make the Tor Network faster and stronger:
• Run a Tor Relay Node »
• Volunteer Your Services »
• Make a Donation »
The Tor Project is a US 501(c)(3) non-profit dedicated to the research, development, and education of online anonymity and privacy. Learn more about The Tor Project »

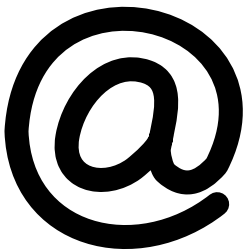
Antitracking auf dem Handy

Android: Google AdID
Google-Einstellungen -> Anzeigen -> Anzeigen

iOS: Apple IDFA
Settings -> General -> About -> Advertising



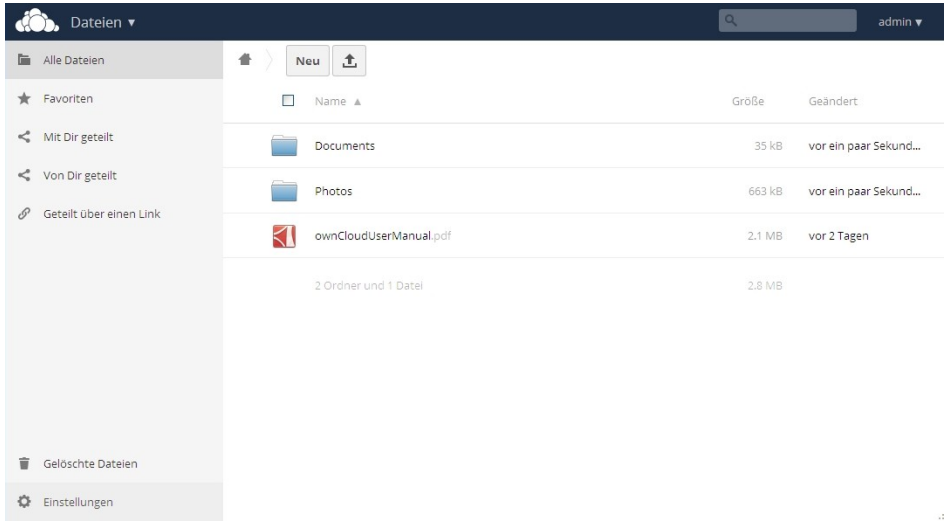
Dezentrale Dienste



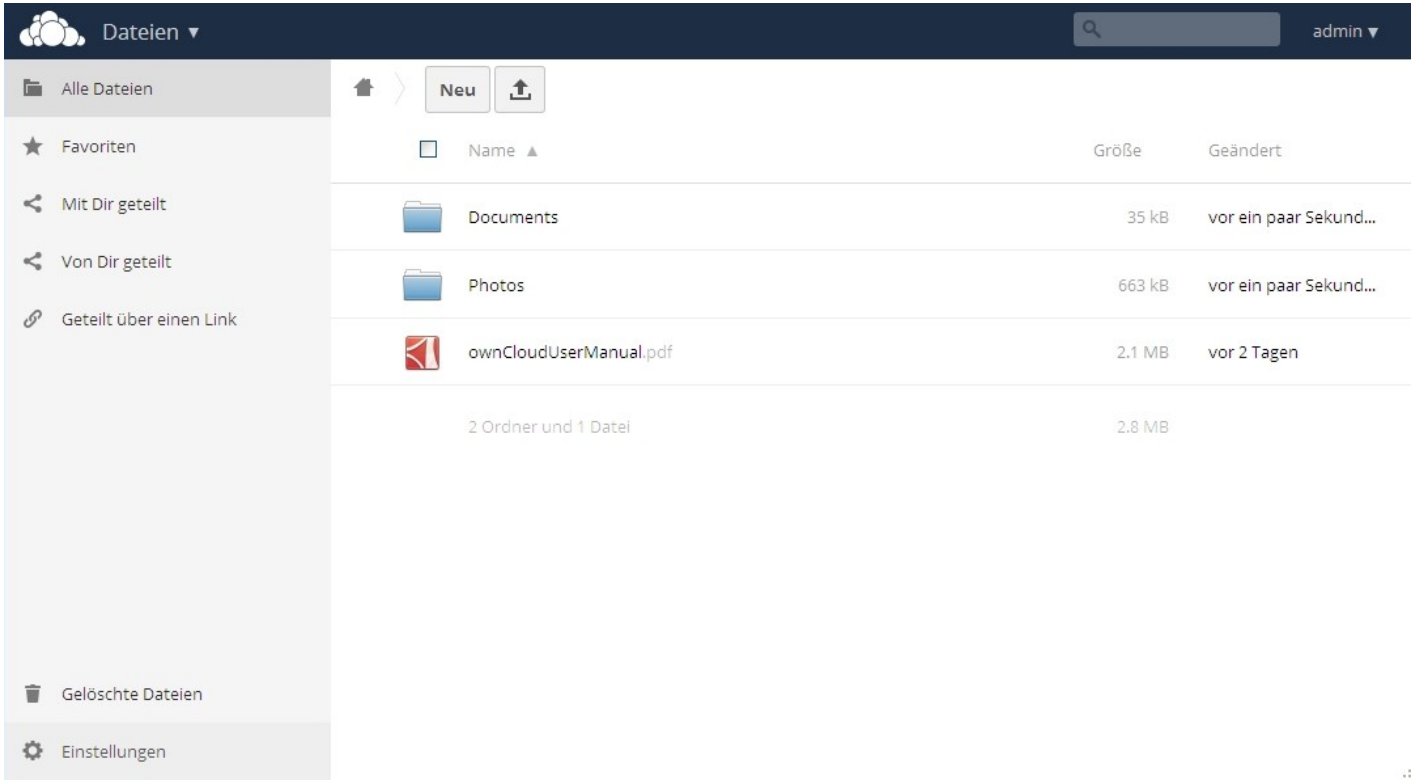
E-Mail

Owncloud

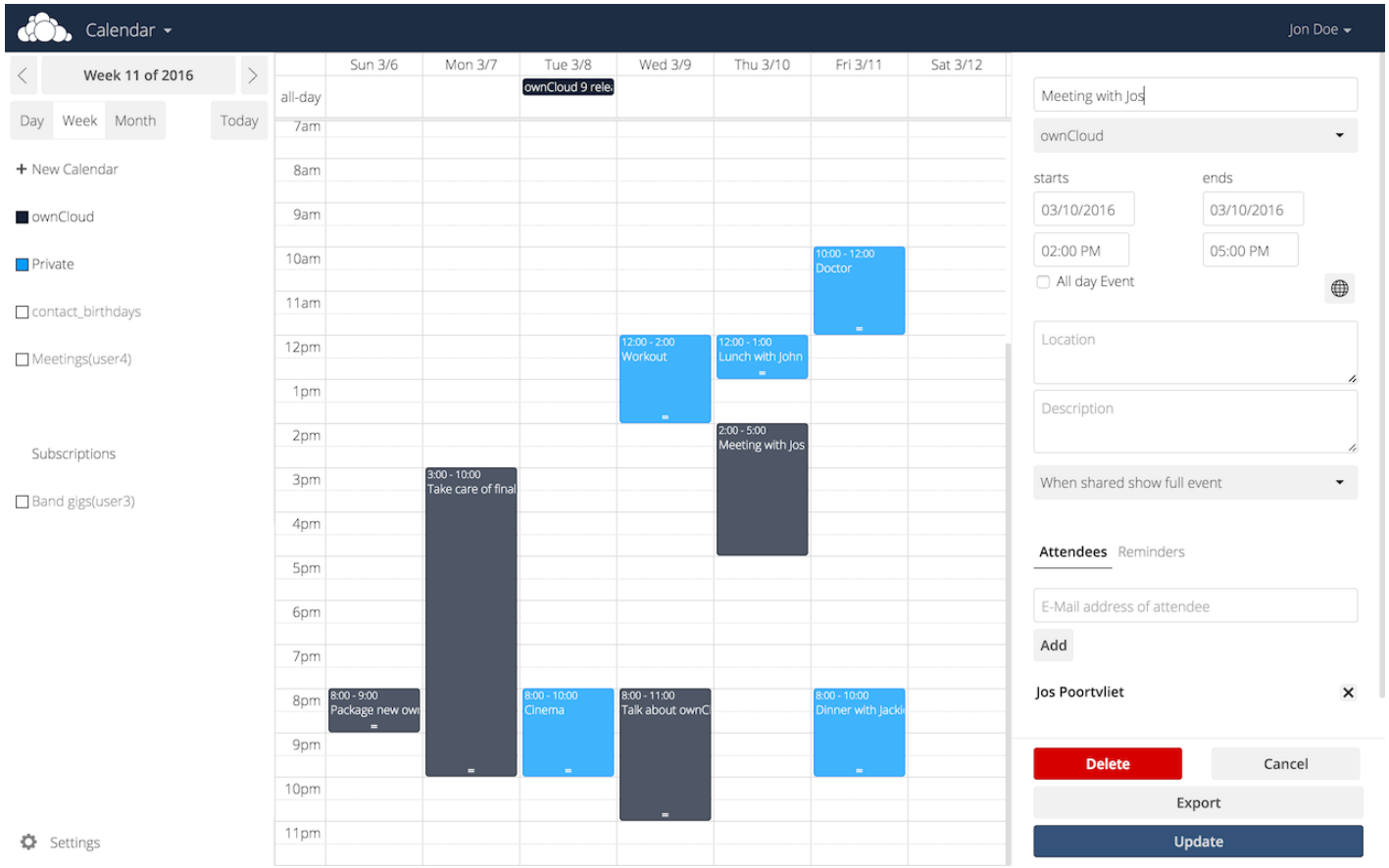
Plattformübergreifende Synchronisierung von Dateien, Dokumenten, Kalendern, Kontakten, Notizen und News.



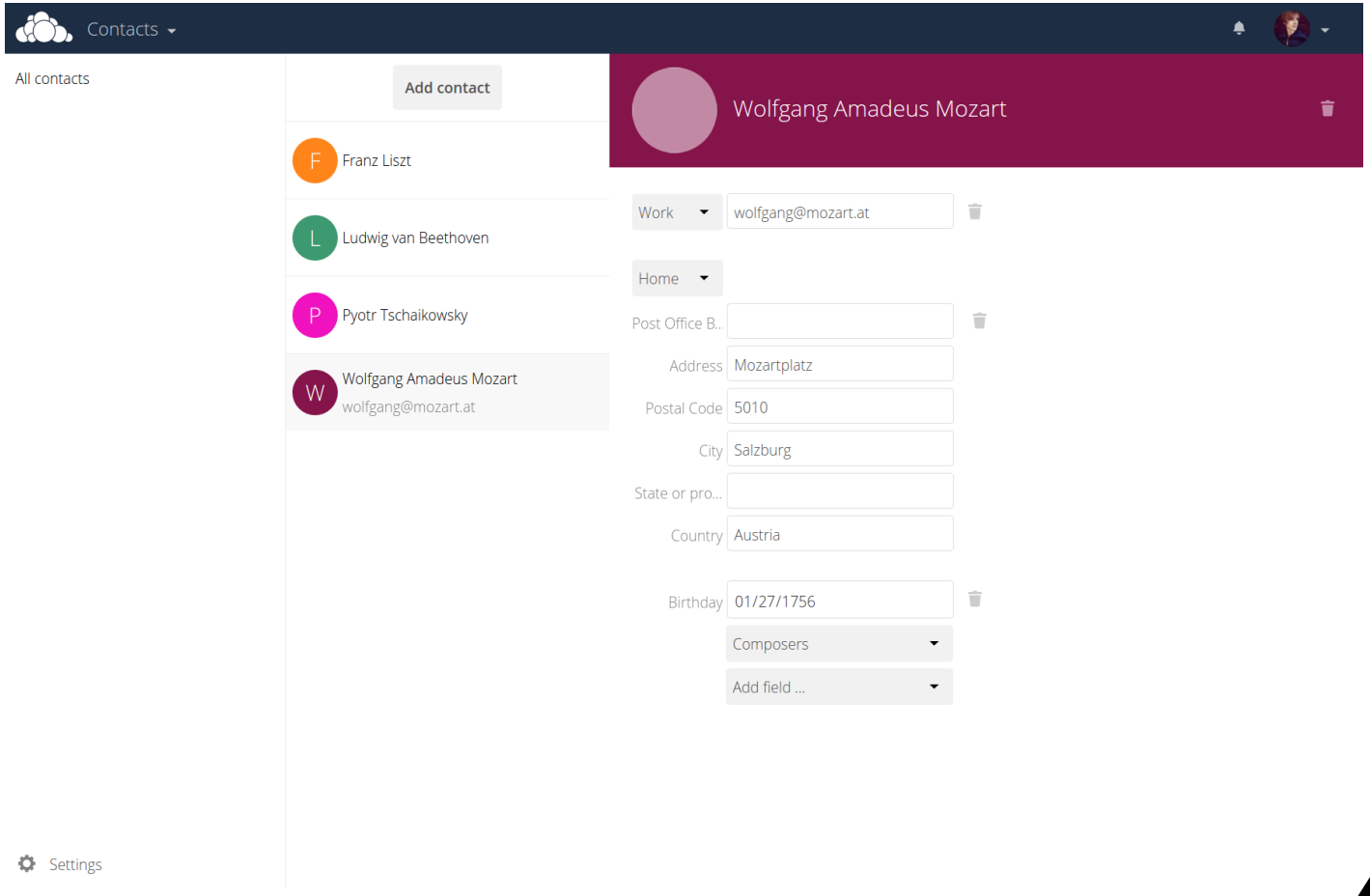
Owncloud als Ersatz für Dropbox



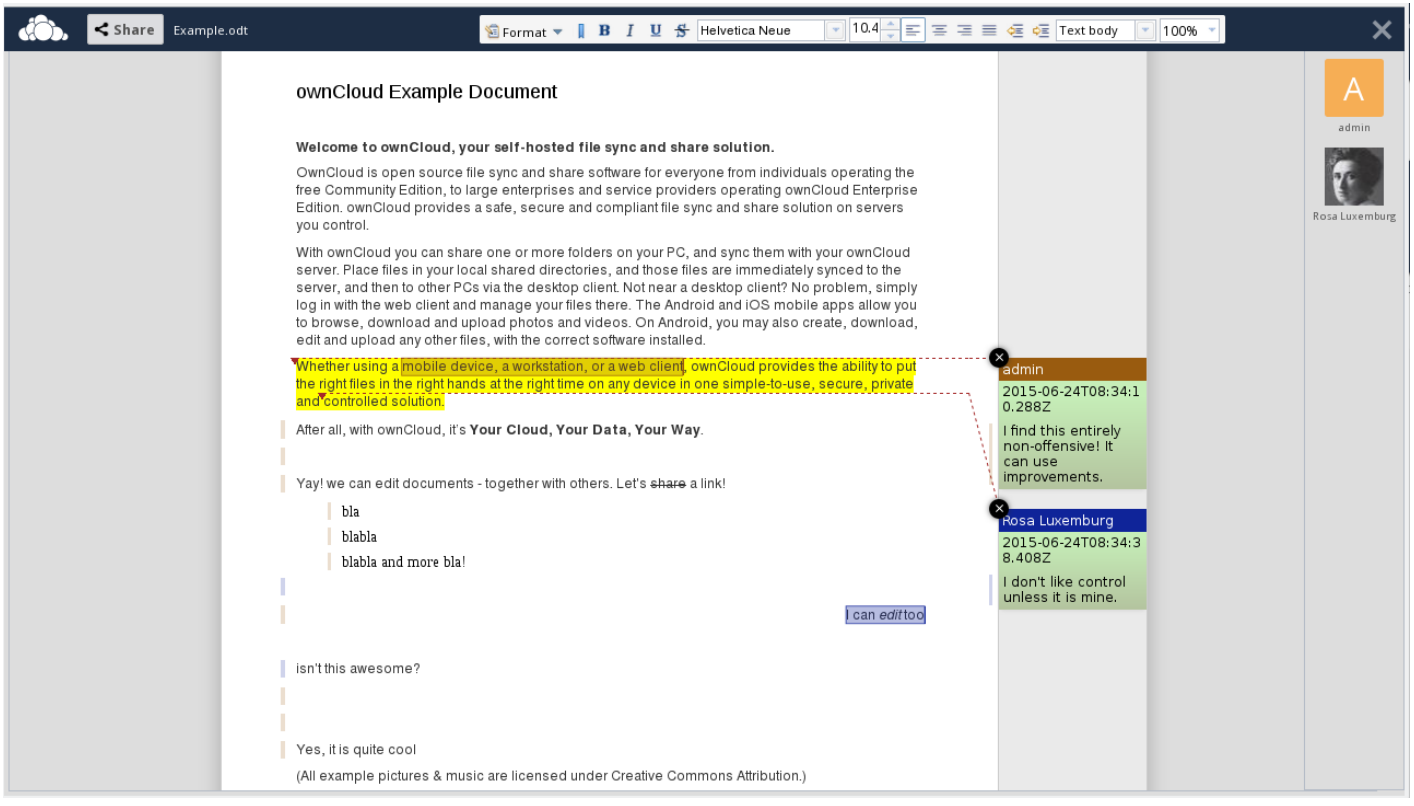
Owncloud als Ersatz für Google/Apple-Sync



Owncloud als Ersatz für Google/Apple-Sync



Owncloud als Ersatz für Google Docs



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
  - dadada

Passwörter

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

Passwörter

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

Passwörter

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

Passwörter

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

Passwörter

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

“Ich hab ja nichts zu vergergen”

“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)

Fazit

- Verschlüsselung nutzen (Signal, Conversations, ChatSecure)
- Dezentrale Dienste nutzen (Email, Jabber, Owncloud)
- Endgeräte schützen (Permissions, Freie Software, Geräteverschlüsselung)

CMS Dresden: schule@c3d2.de
Vortragender: Marius Melzer (marius@rasumi.net,
PGP-Fingerprint: 6730 E691 36B9 9BB8 FFB1 2662 A97B F176 52DE FC3E)