Digitale Selbstverteidigung für Engagierte in der Geflüchtetenhilfe

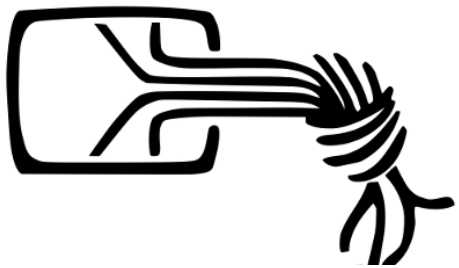
Marius Melzer (CCC Dresden), Jonas Wielicki (FSFW Dresden)

17.03.2016

Freie Software Freies Wissen

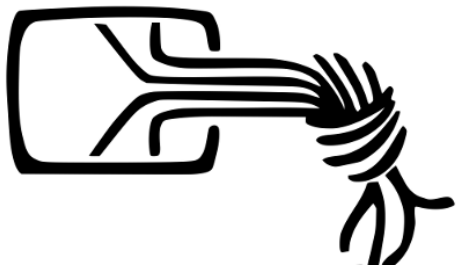
- Hochschulgruppe, gegründet Ende 2014
- Für Freie Software, Schutz persönlicher Daten und Zugänglichkeit von Wissen

Chaos Computer Club



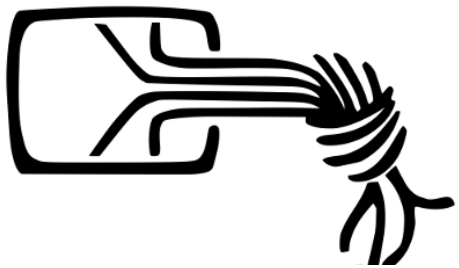
- Verein wurde 1981 gegründet (`https://ccc.de`)

Chaos Computer Club



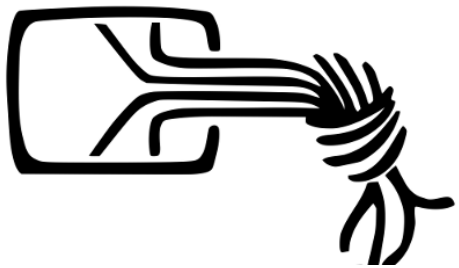
- Verein wurde 1981 gegründet (`https://ccc.de`)
- Aktuell > 6000 Mitglieder

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`)
- 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`)

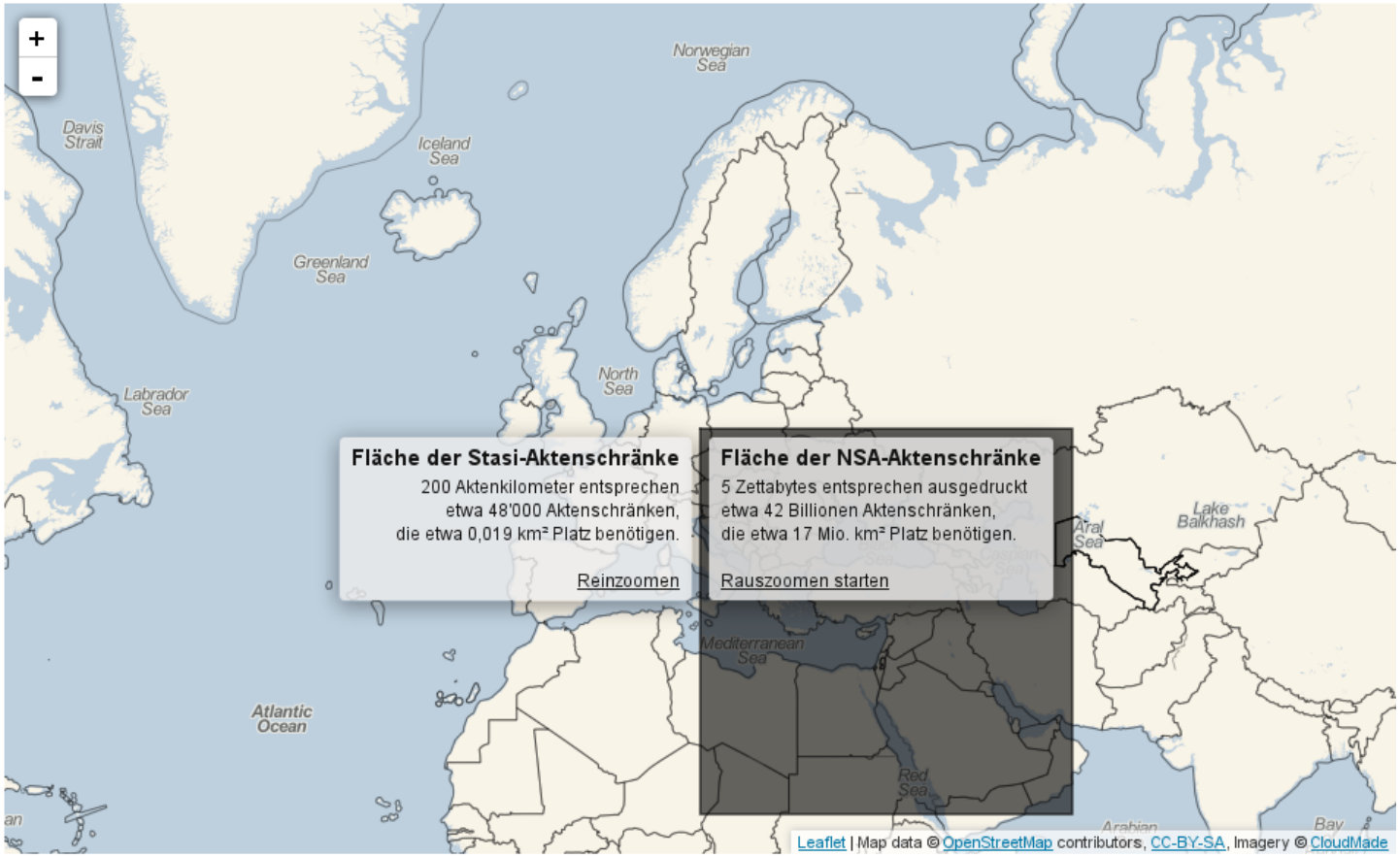
Bundespräsident Gauck zur NSA-Überwachung

"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.

“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)

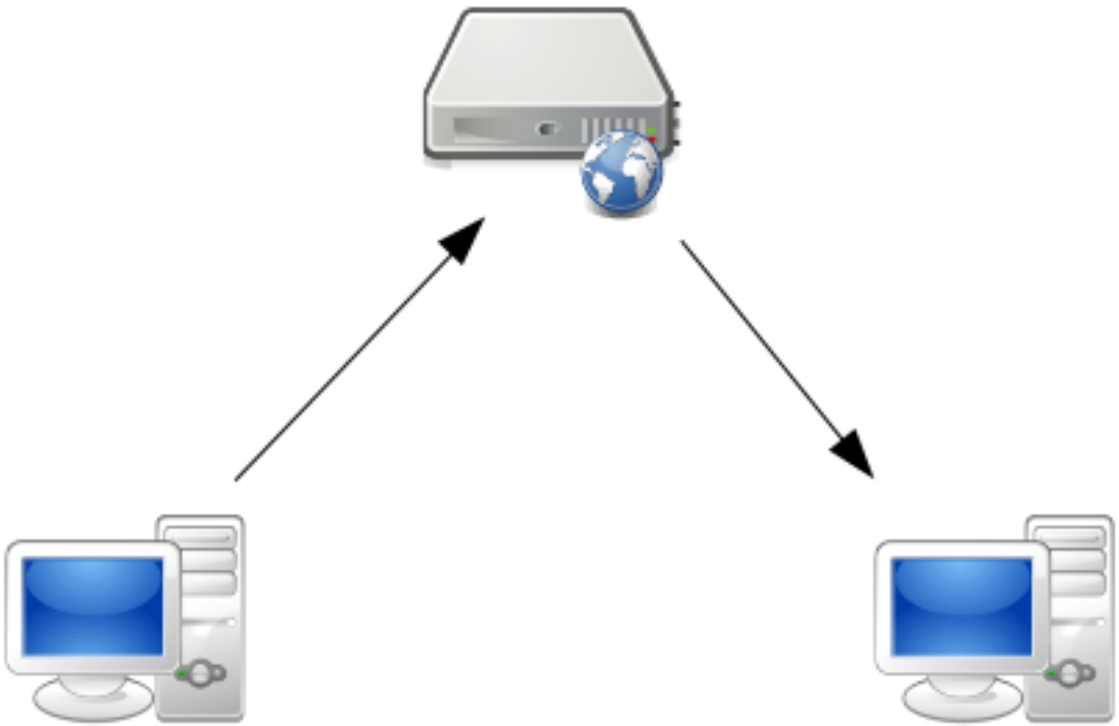
Samsung vs. 1984

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

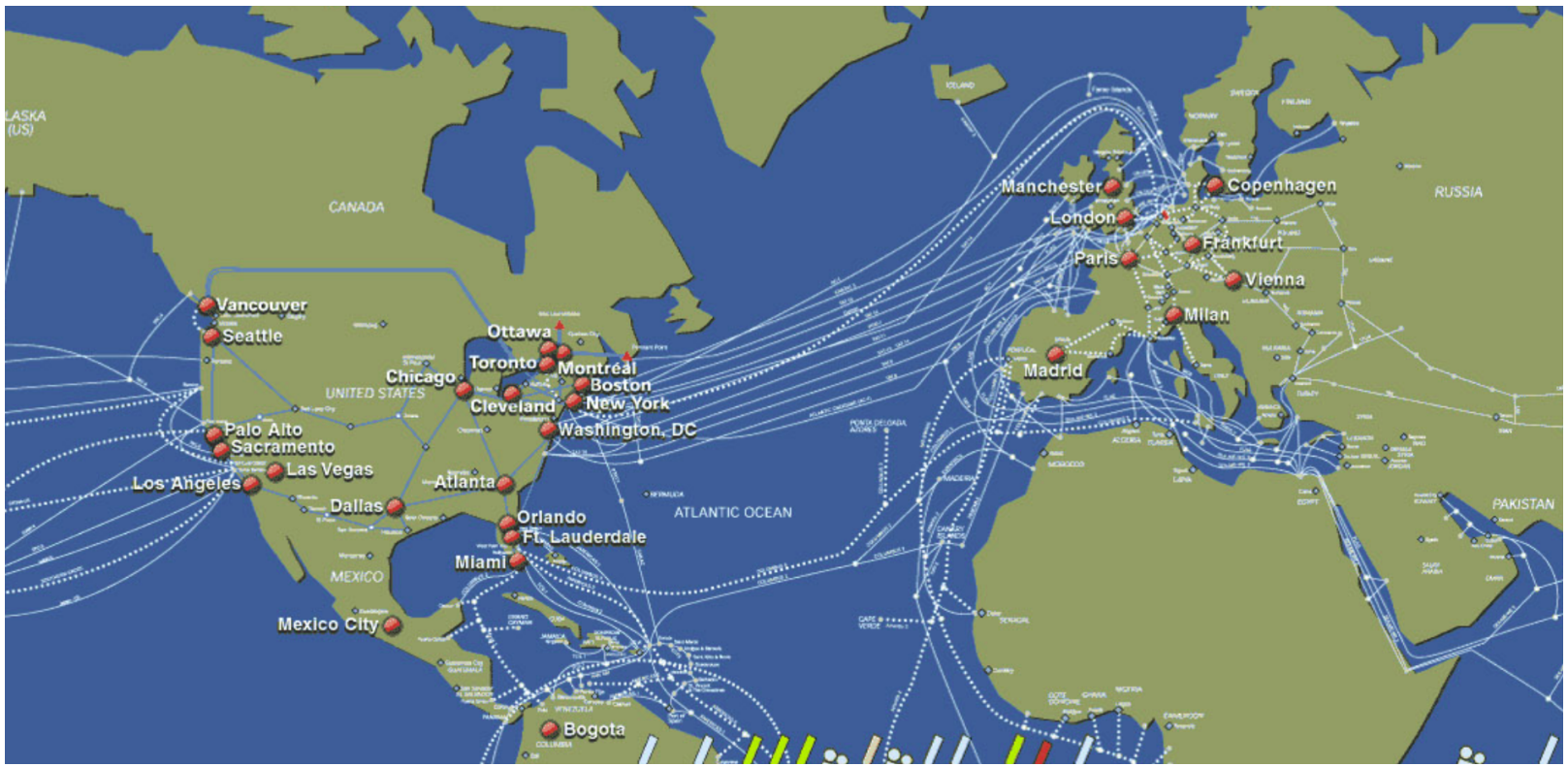
Behind Winston's back the voice from the telescreen was still babbling away about pig-iron and the overfulfilment of the Ninth Three-Year Plan. The telescreen received and transmitted simultaneously. Any sound that Winston made, above the level of a very low whisper, would be picked up by it, moreover, 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?



Server im Rechenzentrum

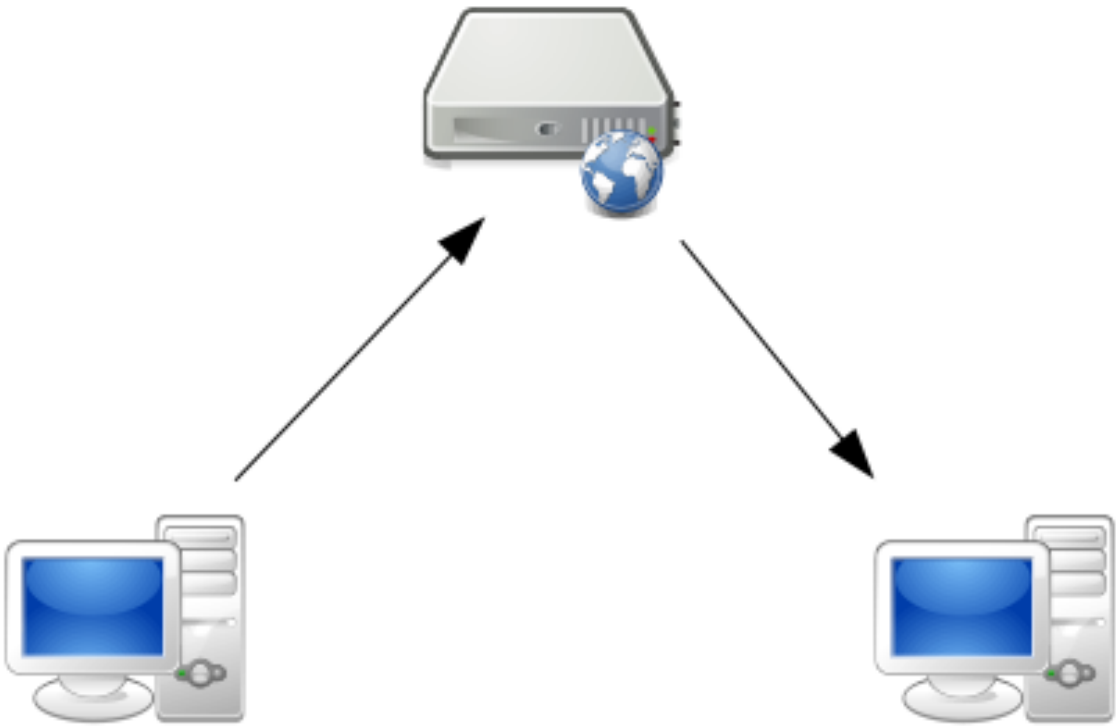
Internetknoten (Router)



Internetknoten (DE-CIX in Frankfurt)

Grafik: Stefan Funke

Was ist zu schützen?



Backdoors

Android-Virenscanner schnüffeln Surf-Verhalten aus

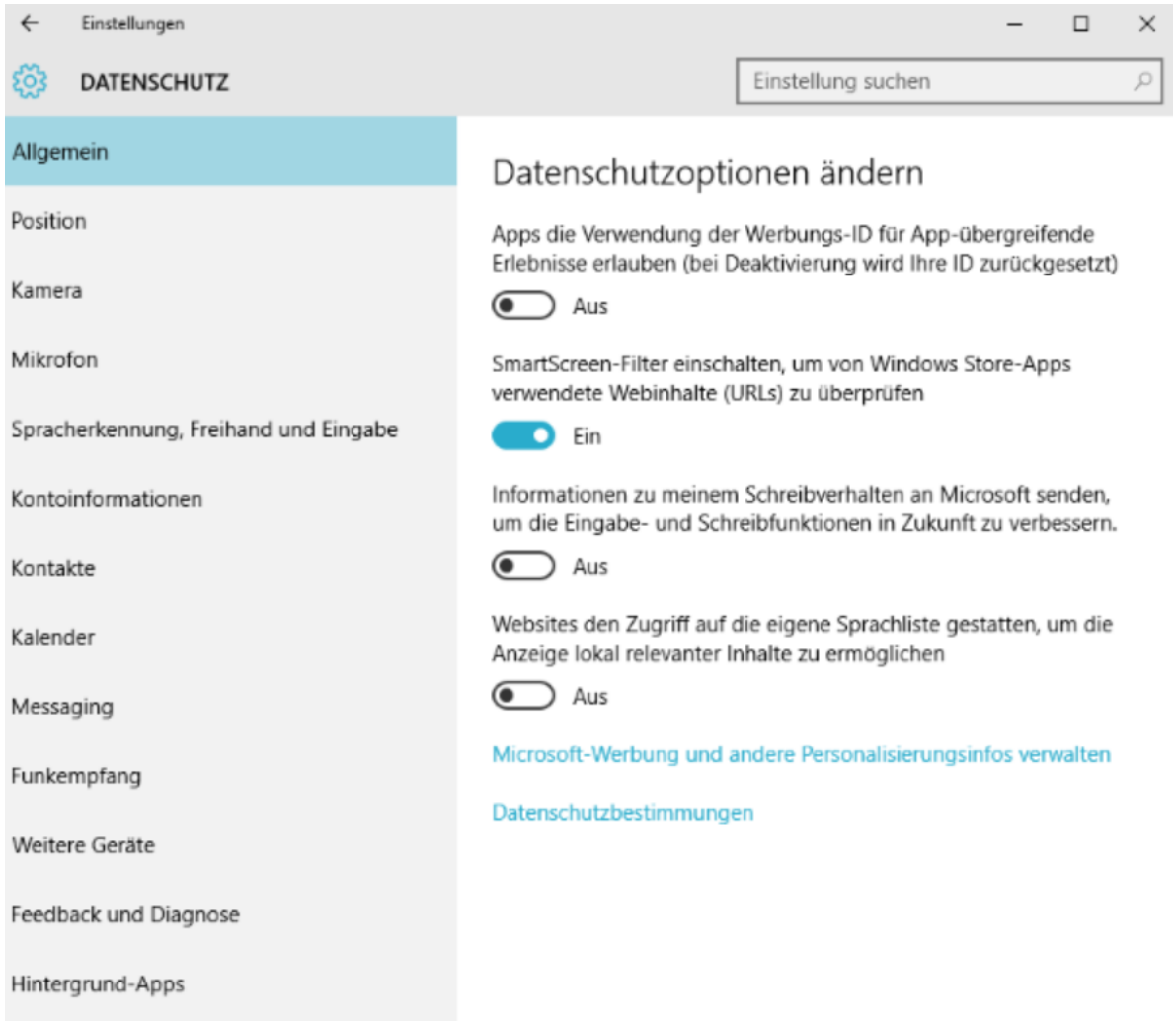
vorlesen / MP3-Download

Viele Virenscanner 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.

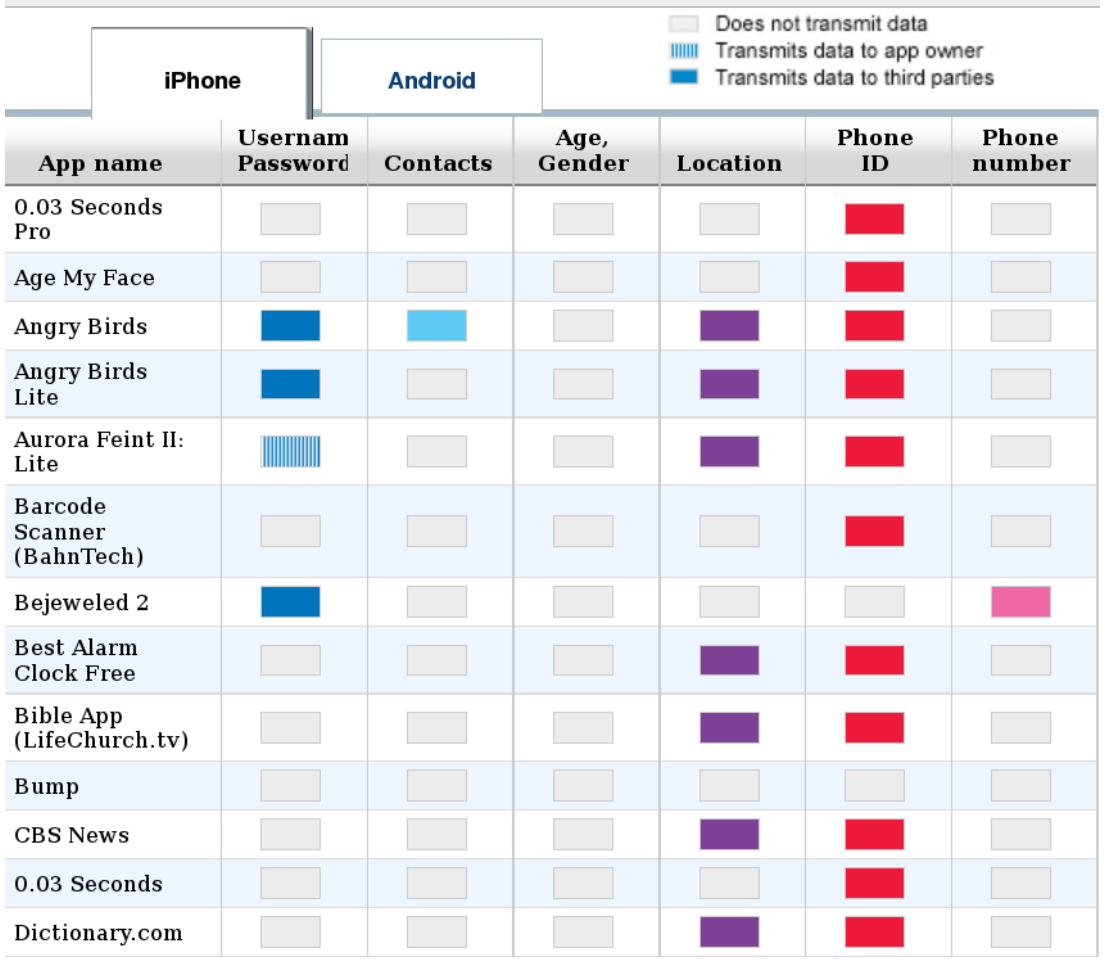
Millionenfach installierte Virenscanner für Android überwachen das Surf-Verhalten ihrer Nutzer und übermitteln ihre Erkenntnisse an die Hersteller. Dabei untergraben Sie sogar die Sicherheit von verschlüsselten HTTPS-Verbindungen. Dies berichtet c't in der aktuellen Ausgabe 6/14.

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.

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						

Unerwünschte Funktionalität

Google knows nearly every Wi-Fi password in the world

By Michael Horowitz

September 12, 2013 10:44 PM EDT 194 Comments

More

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?

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

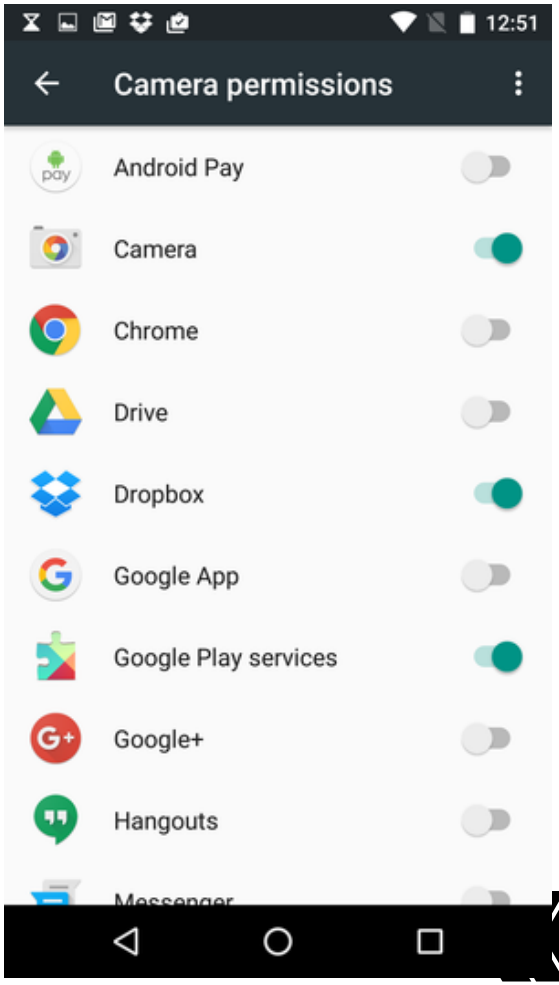
Permissions

Android
Einstellungen -> Apps -> Appname -> Berechtigungen ändern

Einstellungen -> Apps -> Zahnrad -> Appberechtigungen

iOS
Einstellungen -> Privatsphäre -> Berechtigungsname

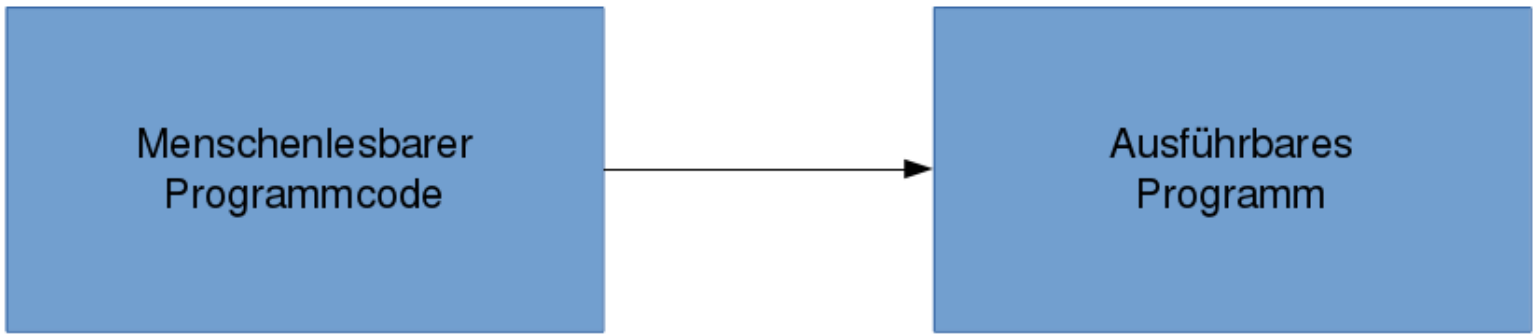
In den neuesten Versionen:
Entscheidung bei erster Benutzung



Vertrauenswürdige Software?

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

Kompilierung von Software



Das GNU Projekt

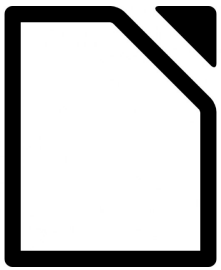
- Begonnen von Richard Stallman im Jahr 1984
- Gründung der Free Software Foundation im Jahr 1985

FREE SOFTWARE FOUNDATION

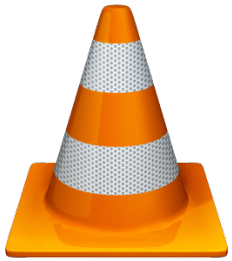
Freie Software auf Computern

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

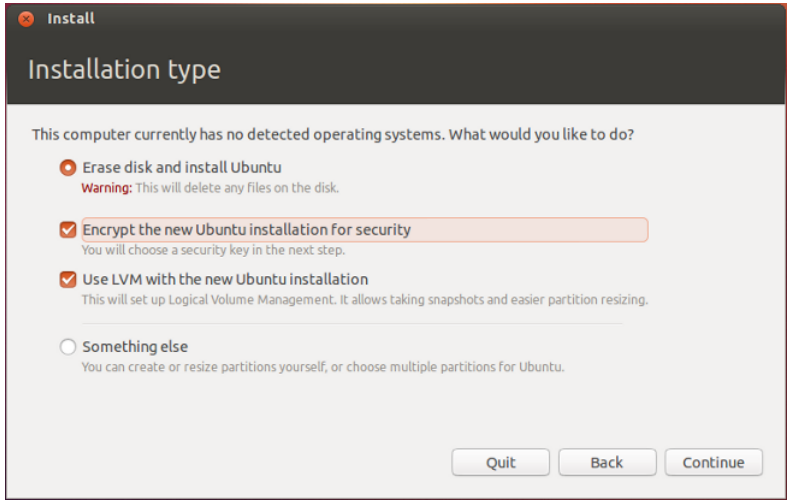
Ubuntu Phone, Sailfish OS

Geräteverschlüsselung auf Computern

Linux
Standardmäßig vorhanden, muss beim Installieren ausgewählt werden

Windows
TrueCrypt, Veracrypt

Mac
FileVault, muss beim Installieren ausgewählt werden

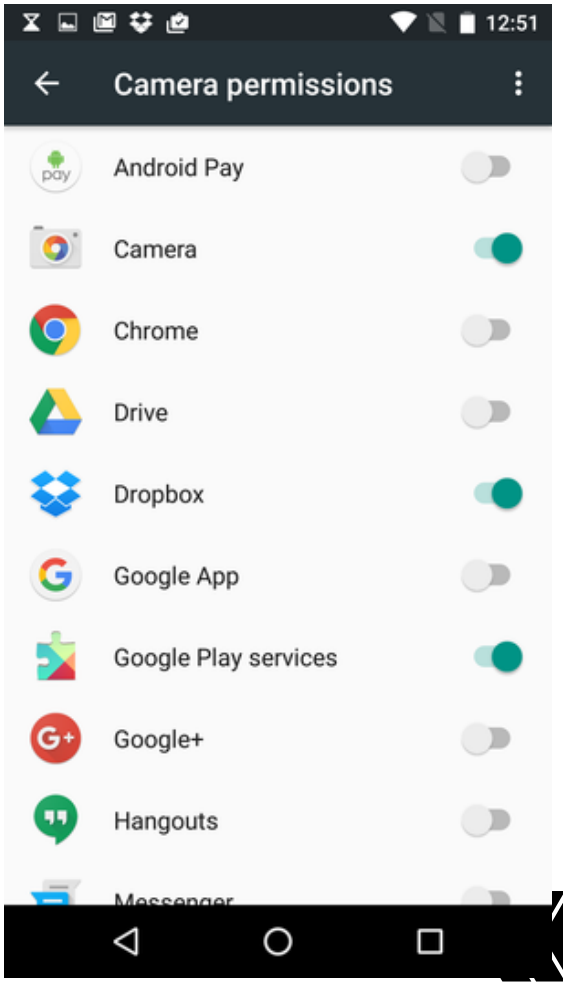


Geräteverschlüsselung auf Smartphones

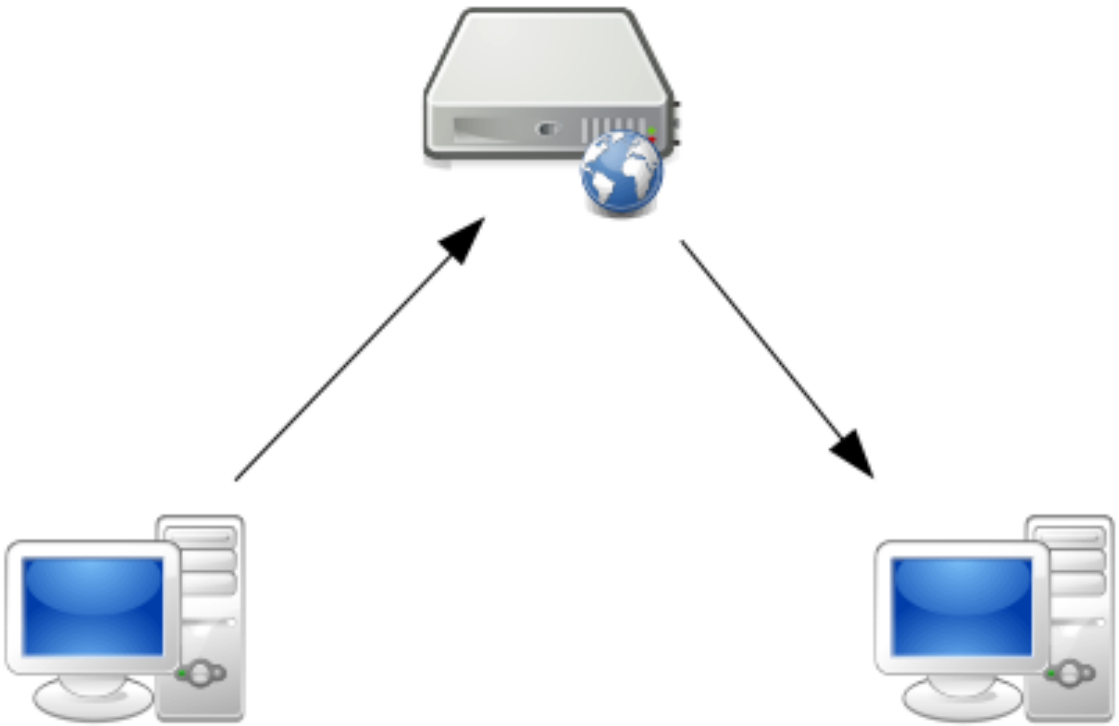
Android
Standard ab 6.0 Einstellungen -> Sicherheit -> Telefon verschlüsseln

iOS
Standard

wichtig: gute PIN/Muster



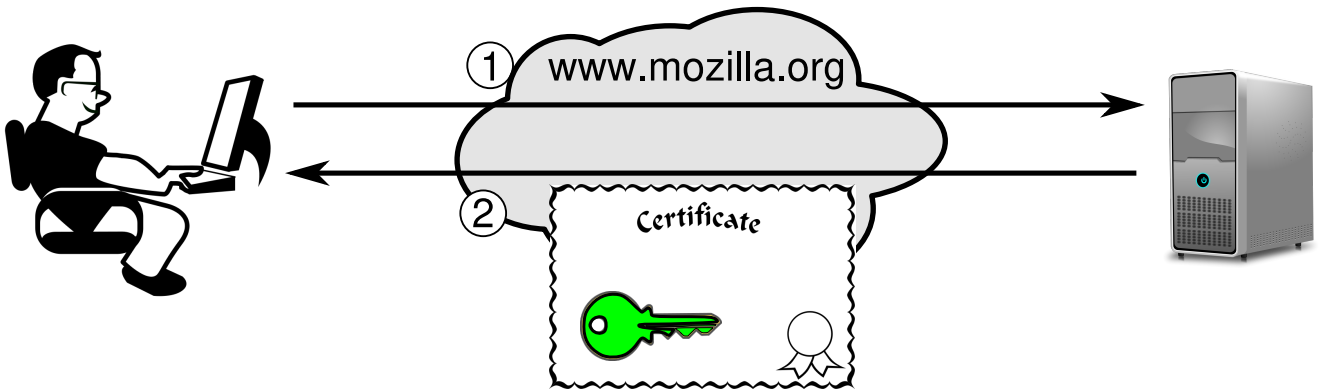
Was ist zu schützen?



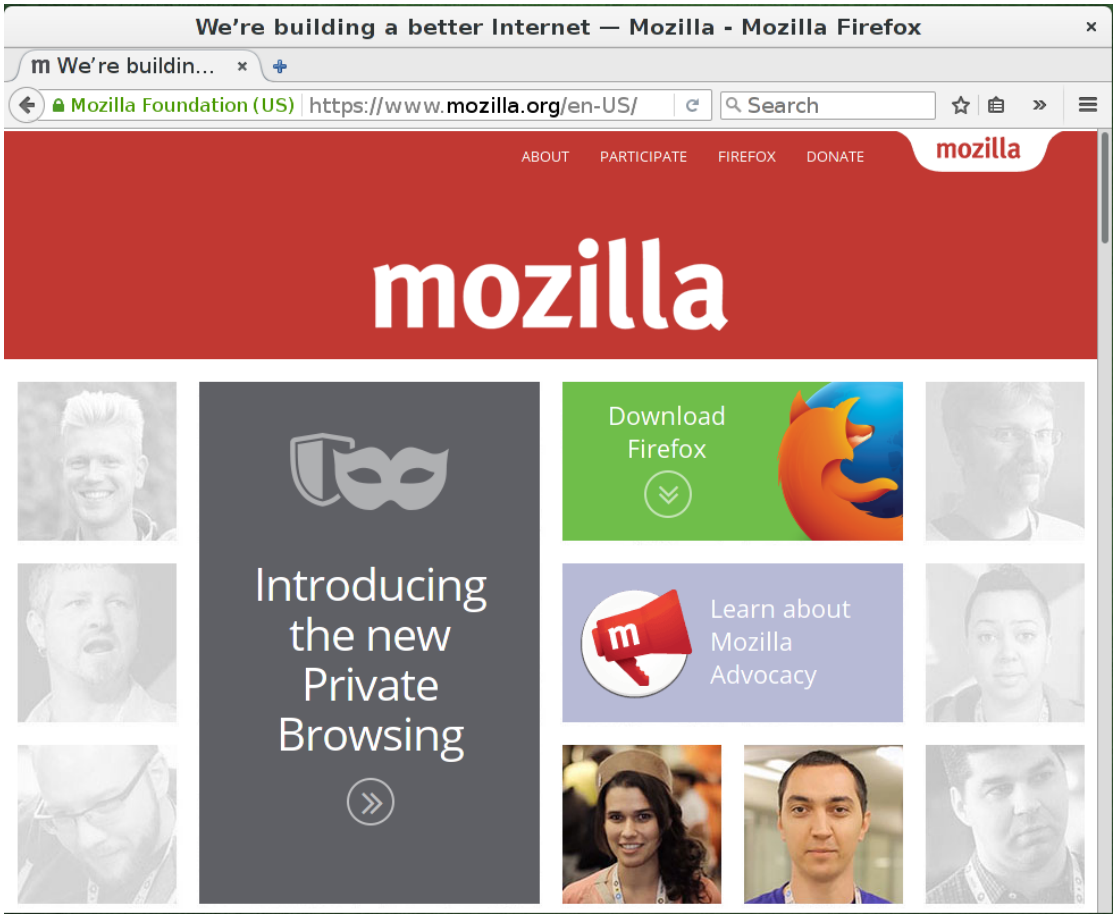
Angreifer im eigenen Netz

Transportwegverschlüsselung

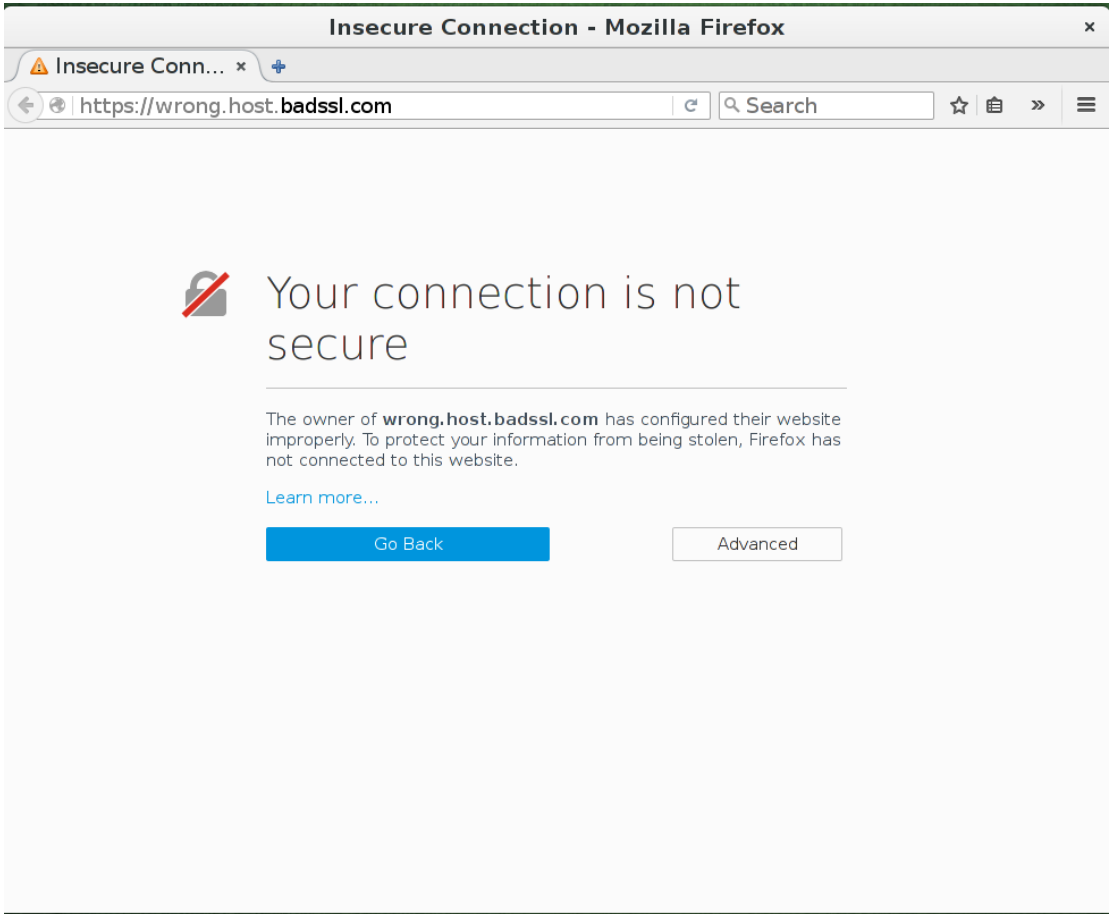
SSL = Secure Socket Layer / TLS = Transport Layer Security



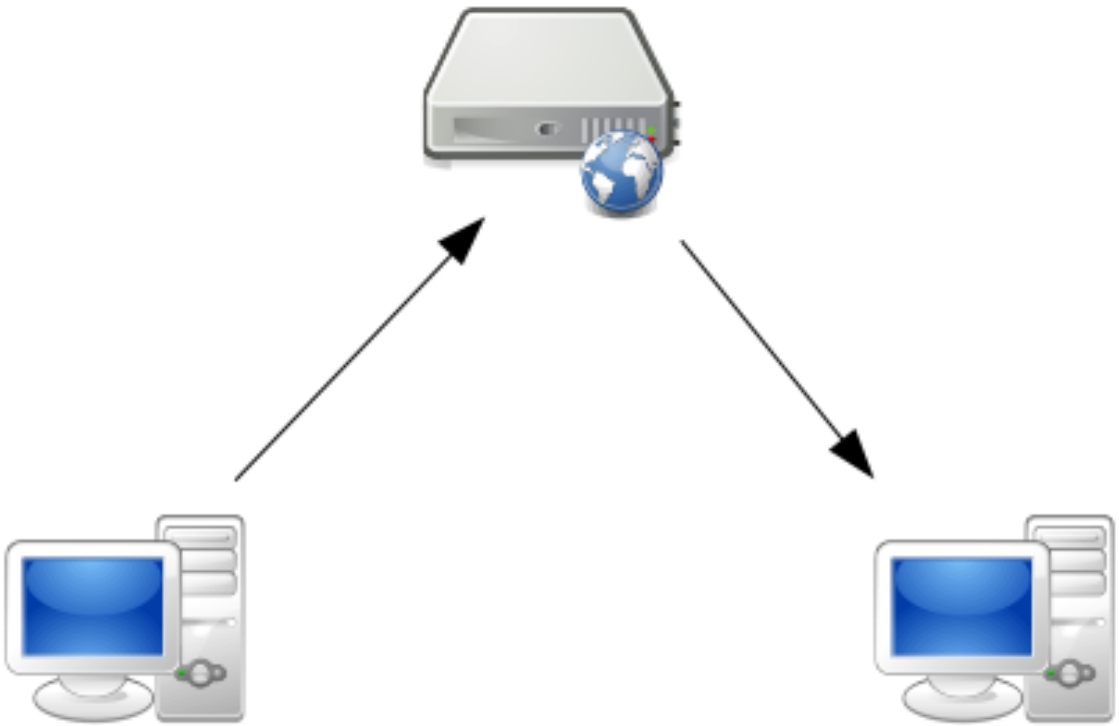
SSL im Browser



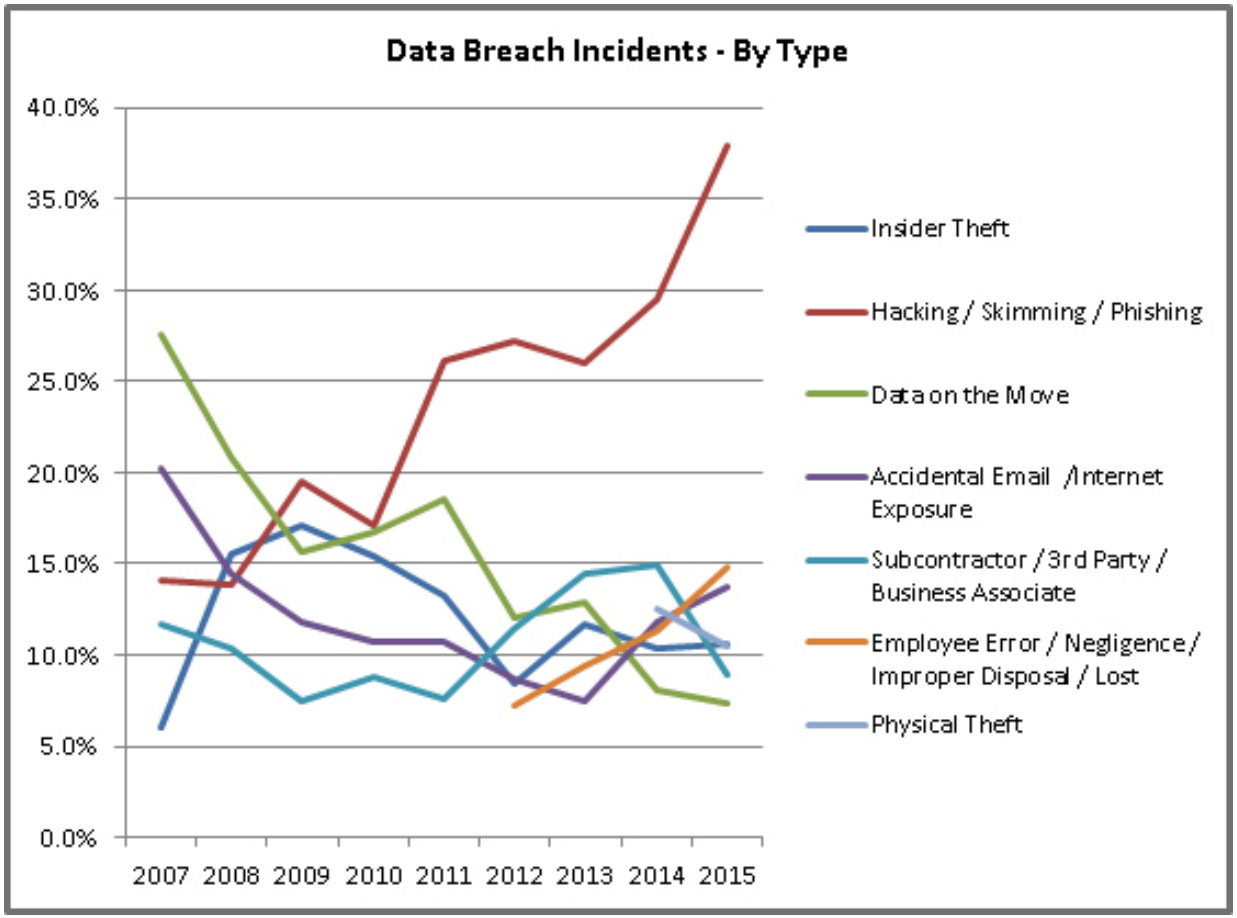
Ungültiges Zertifikat



Was ist zu schützen?



Informationsleaks



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

Ende-zu-Ende-Verschlüsselung

- GPG für E-Mails

Ende-zu-Ende-Verschlüsselung

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

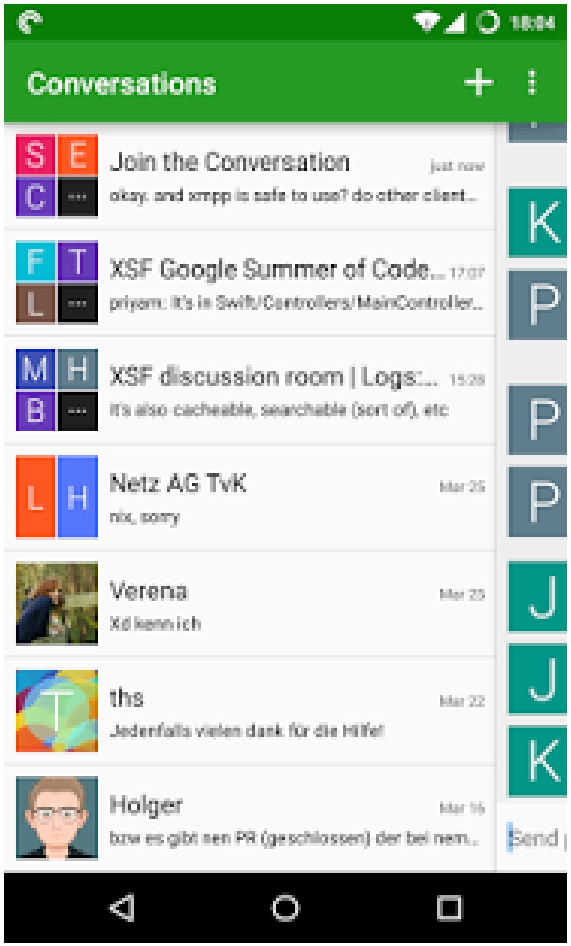
Ende-zu-Ende-Verschlüsselung

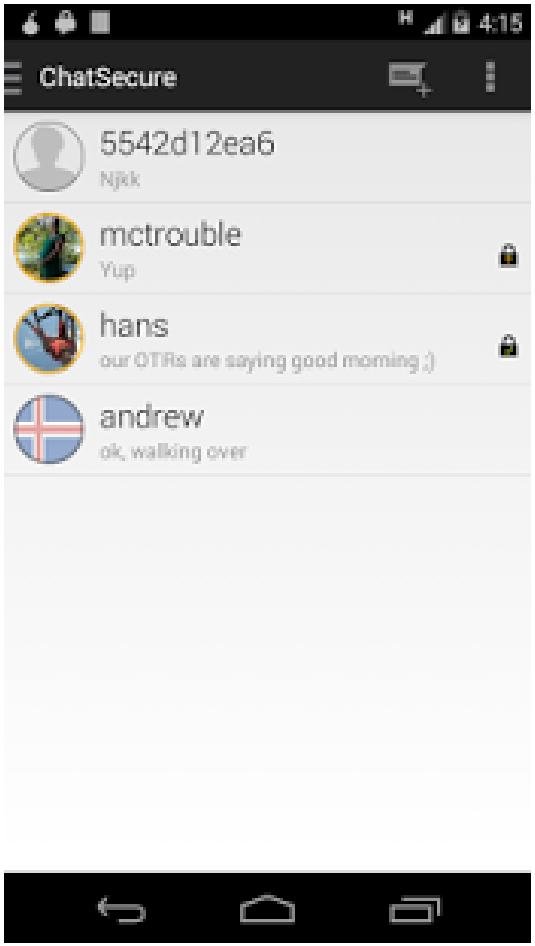
- GPG für E-Mails
- OTR/OMEMO für Jabber:
  - Pidgin für Linux und Windows
  - Conversations oder ChatSecure für Android
  - Adium für Mac, ChatSecure für iOS
- palava.tv, talky.io, Tox, Linphone für Videotelefonie

Ende-zu-Ende-Verschlüsselung

- GPG 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, talky.io, Tox, Linphone für Videotelefonie
- Signal

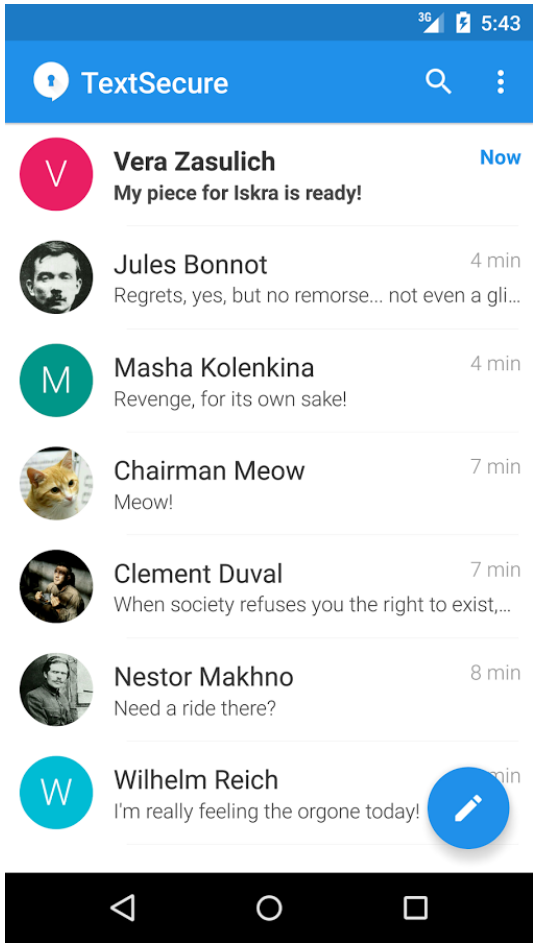
Jabber: Conversations, ChatSecure

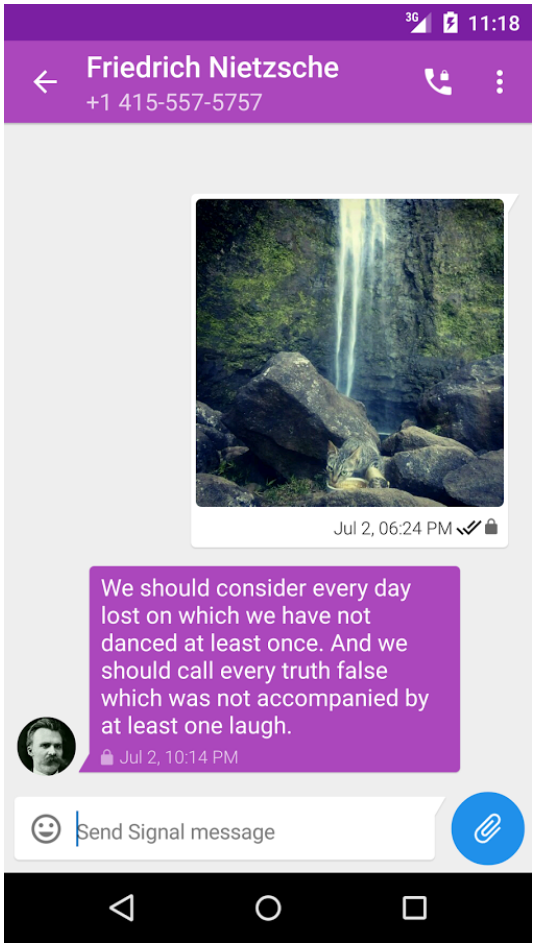




https://xmpp.net/directory.php

Signal

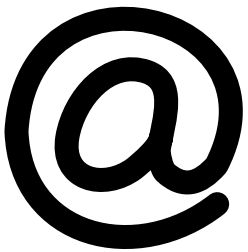

5:43
TextSecure
Vera Zasulich
Now
My piece for Iskra is ready!
Jules Bonnot
4 min
Regrets, yes, but no remorse... not even a gli...
Masha Kolenkina
4 min
Revenge, for its own sake!
Chairman Meow
7 min
Meow!
Clement Duval
7 min
When society refuses you the right to exist,...
Nestor Makhno
8 min
Need a ride there?
Wilhelm Reich
I'm really feeling the orgone today!


11:18
Friedrich Nietzsche
+1 415-557-5757
Jul 2, 06:24 PM
We should consider every day lost on which we have not danced at least once. And we should call every truth false which was not accompanied by at least one laugh.
Jul 2, 10:14 PM
Send Signal message

Vergleich Messenger

	Whatsapp	Threema	Telegram	Signal	Jabber
Verschlüsselung					
Vertrauensw.					
Dezentr.					
Open Source					
Mobileignung					

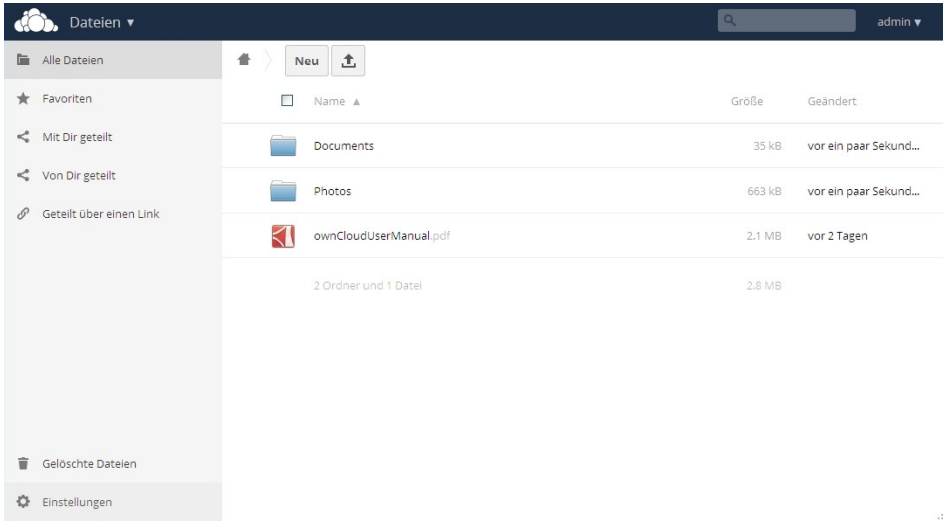
Dezentrale Dienste



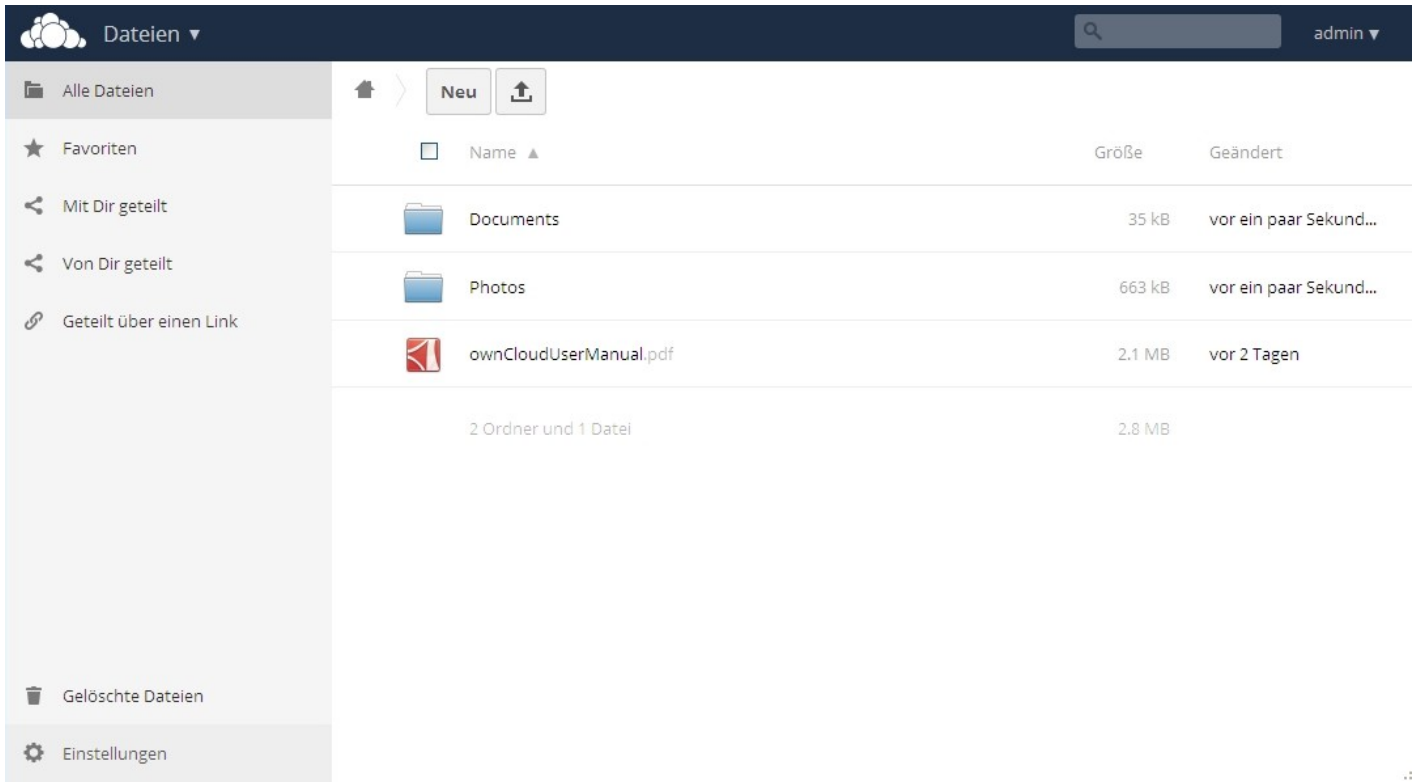
E-Mail

Owncloud

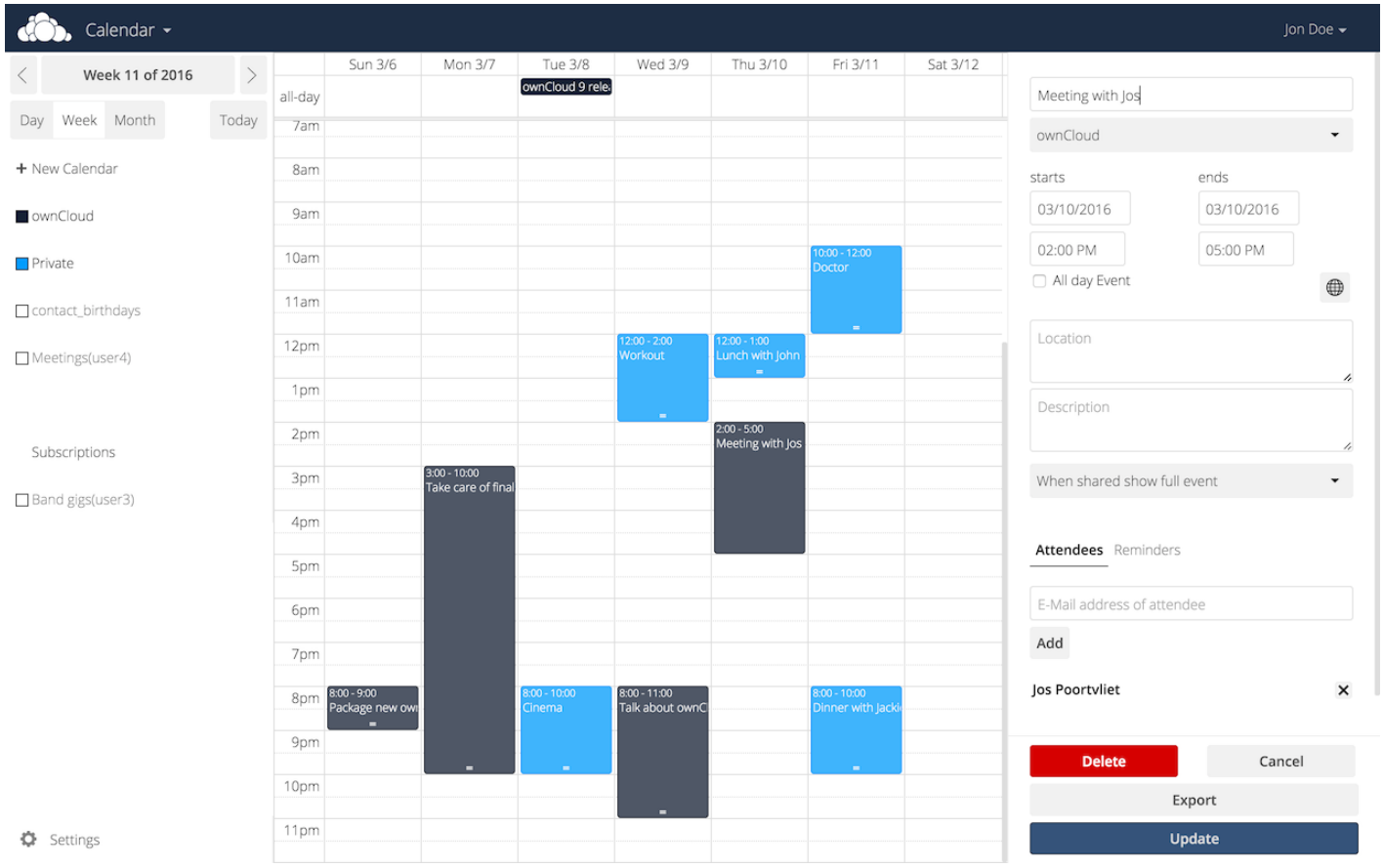
Plattformübergreifende Synchronisierung von Dateien, Dokumenten, Kalendern, Kontakten, Notizen und News.



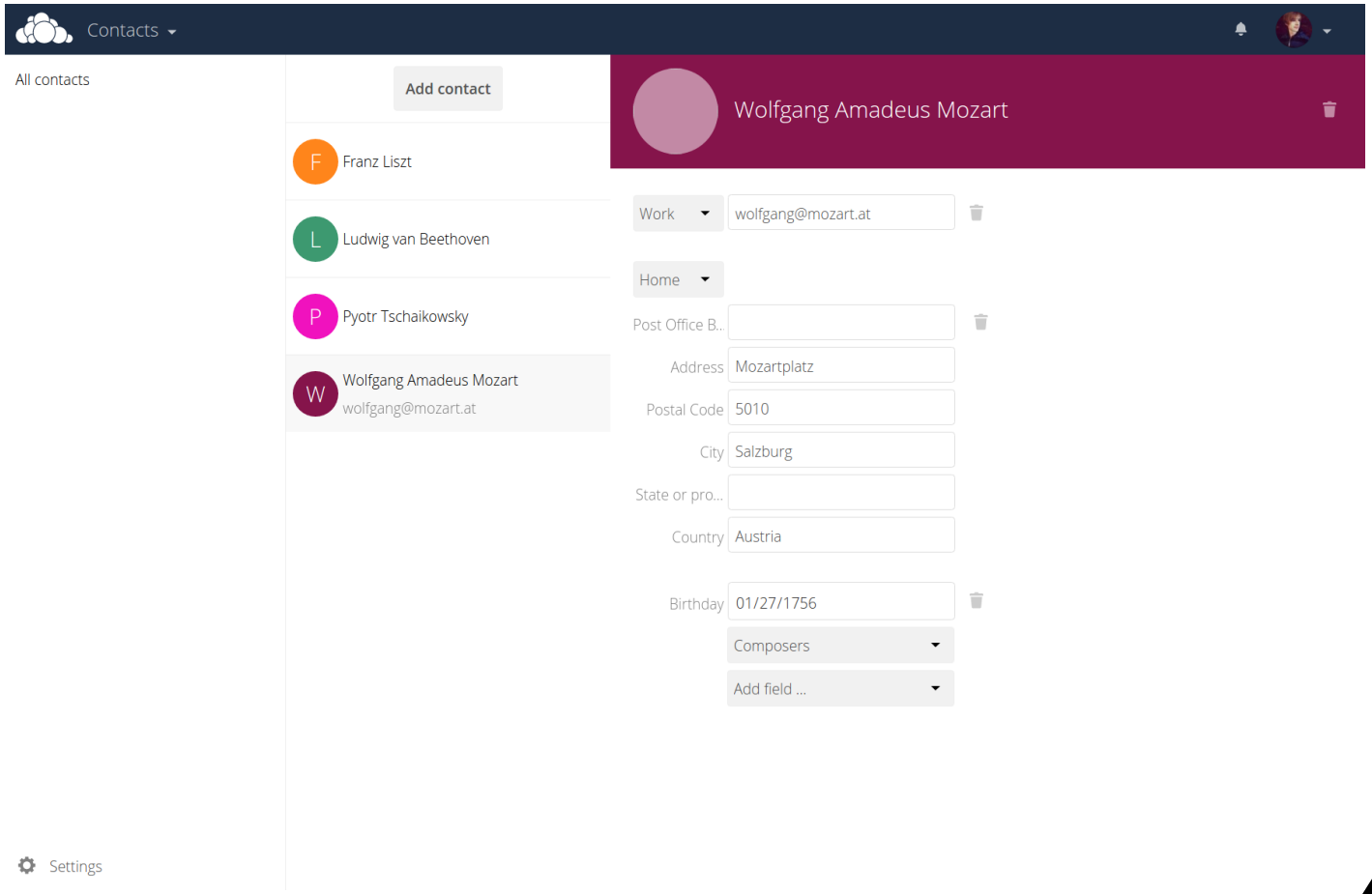
Owncloud als Ersatz für Dropbox



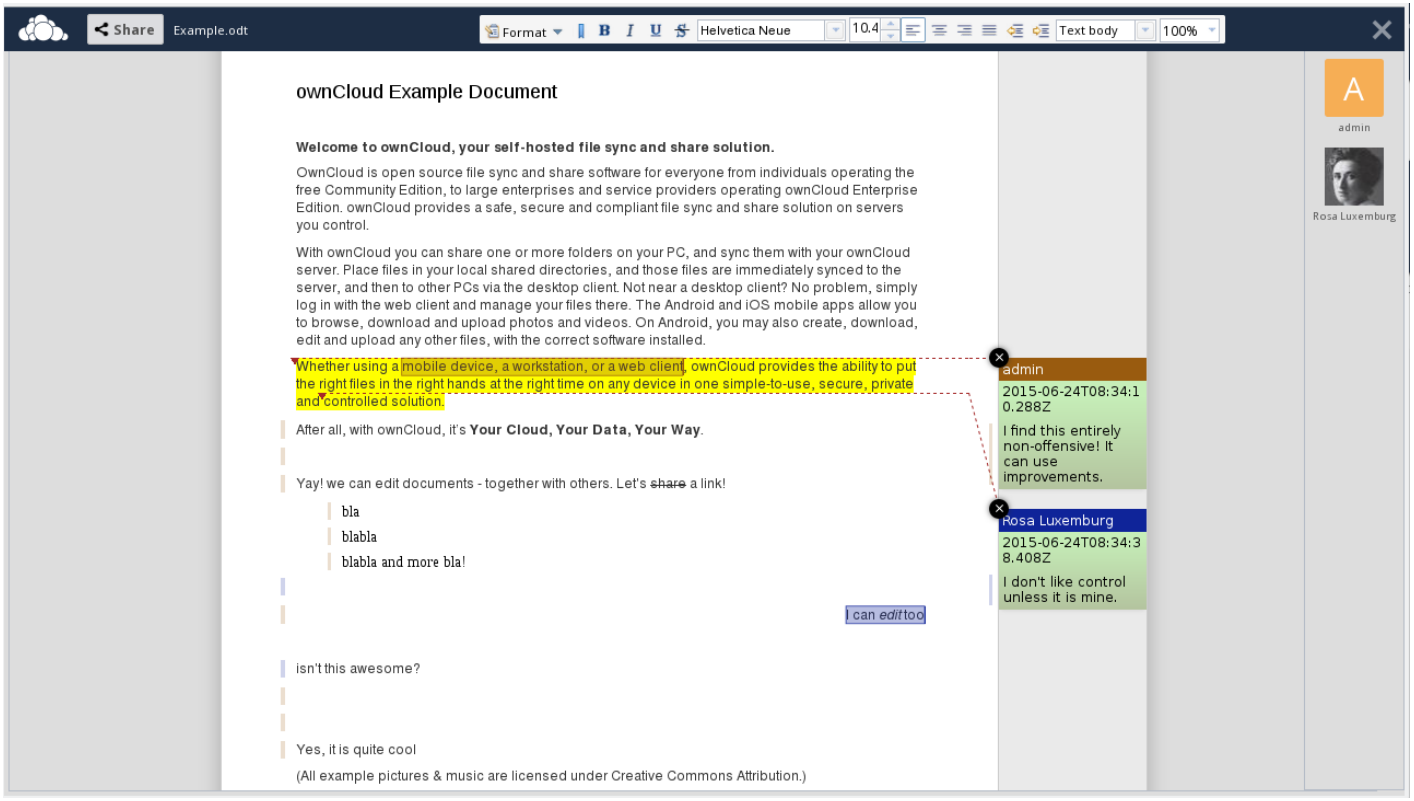
Owncloud als Ersatz für Google/Apple-Sync



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
  - .§)=/)=‘

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

CMS Dresden: schule@c3d2.de
FSFW: https://fsfw-dresden.de/