

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>)
- 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)

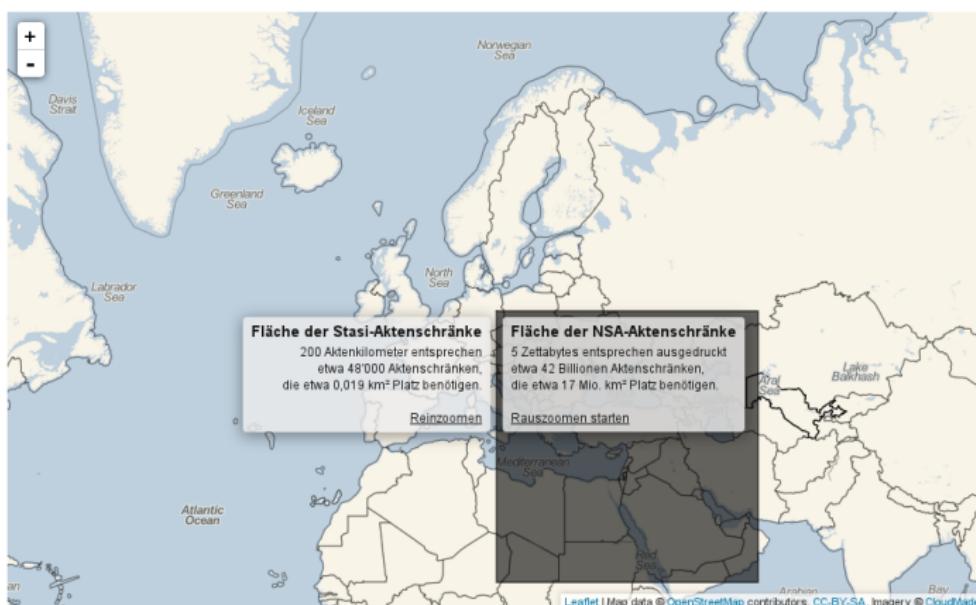
Stasi vs. NSA



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 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)

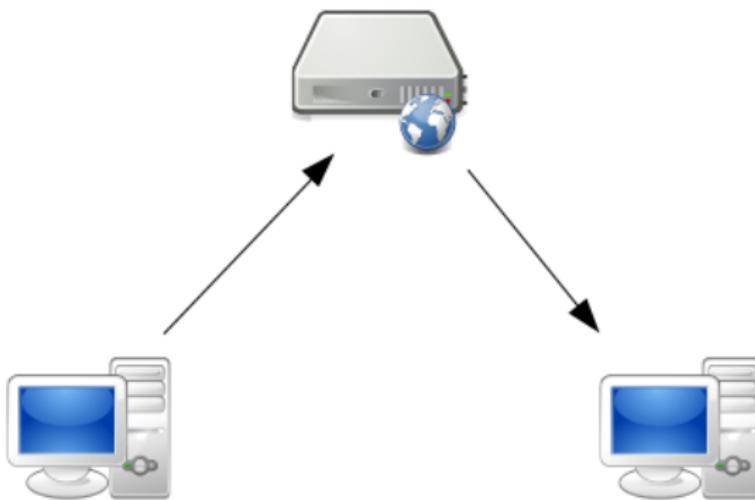
Samsung vs. 1984

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.

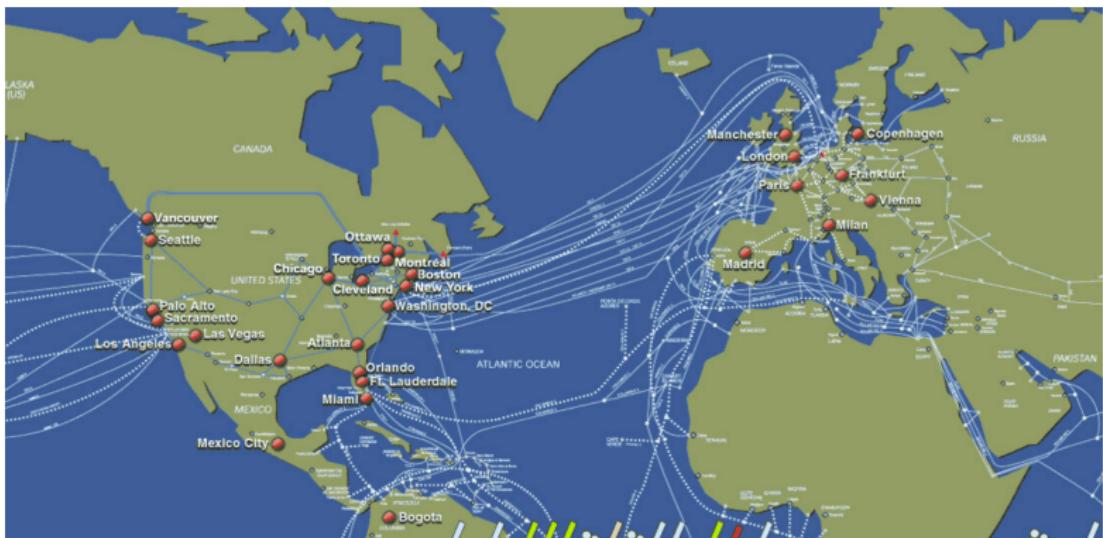
Wie kommunizieren wir im Internet?



Server im Rechenzentrum



Internetknoten (Router)

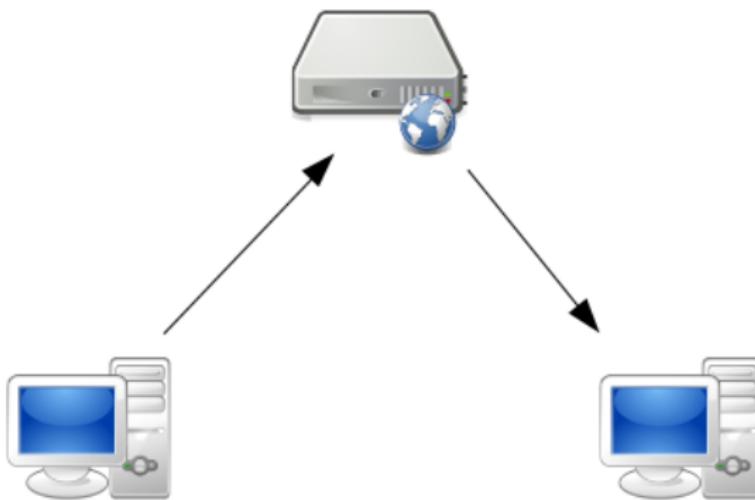


Internetknoten (DE-CIX in Frankfurt)



Grafik: Stefan Funke

Was ist zu schützen?



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.

Unerwünschte Funktionalität

The screenshot shows the Windows Settings interface under 'DATENSCHUTZ' (Data Protection). The left sidebar lists categories: Allgemein, Position, Kamera, Mikrofon, Spracherkennung, Freihand und Eingabe, Kontoinformationen, Kontakte, Kalender, Messaging, Funkempfang, Weitere Geräte, Feedback und Diagnose, and Hintergrund-Apps. The 'Allgemein' tab is selected. On the right, the 'Spracherkennung, Freihand und Eingabe' section is expanded, showing a toggle switch for 'Aus' (Off) which is currently selected. Below it, there is descriptive text about Microsoft sending information to improve input and writing functions. At the bottom of this section, there are links to 'Microsoft-Werbung und andere Personalisierungsinfos verwalten' and 'Datenschutzbestimmungen'.

Einstellungen

DATENSCHUTZ

Allgemein

Position

Kamera

Mikrofon

Spracherkennung, Freihand und Eingabe

Kontoinformationen

Kontakte

Kalender

Messaging

Funkempfang

Weitere Geräte

Feedback und Diagnose

Hintergrund-Apps

Einstellung suchen

Datenschutzoptionen ändern

Apps die Verwendung der Werbungs-ID für App-übergreifende Erfahrungen erlauben (bei Deaktivierung wird Ihre ID zurückgesetzt)

Aus

SmartScreen-Filter einschalten, um von Windows Store-Apps verwendete Webinhalte (URLs) zu überprüfen

Ein

Informationen zu meinem Schreibverhalten an Microsoft senden, um die Eingabe- und Schreibfunktionen in Zukunft zu verbessern.

Aus

Websites den Zugriff auf die eigene Sprachliste gestatten, um die Anzeige lokal relevanter Inhalte zu ermöglichen

Aus

[Microsoft-Werbung und andere Personalisierungsinfos verwalten](#)

[Datenschutzbestimmungen](#)

Unerwünschte Funktionalität

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



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?

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

Permissions

Android

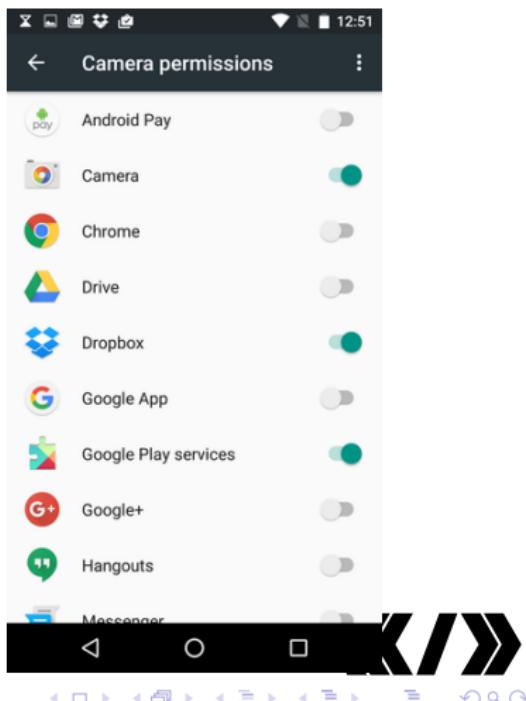
Einstellungen -> Apps -> Appname
-> Berechtigungen ändern

Einstellungen -> Apps -> Zahnrad
-> Appberechtigungen

iOS

Einstellungen -> Privatsphäre ->
Berechtigungsname

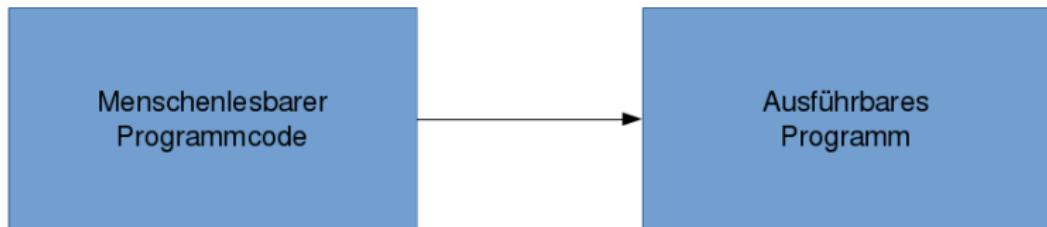
In den neuesten Versionen:
Entscheidung bei erster Benutzung



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](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



cyanogenmod

Ubuntu Phone, Sailfish OS



Geräteverschlüsselung auf Computern

Linux

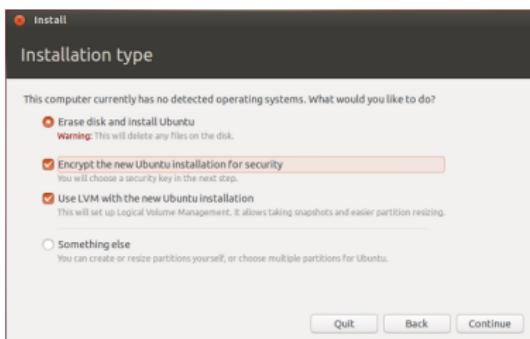
Standardmäßig vorhanden,
muss beim Installieren
ausgewählt werden

Windows

TrueCrypt, Veracrypt

Mac

FileVault, muss beim
Installieren ausgewählt
werden



Geräteverschlüsselung auf Smartphones

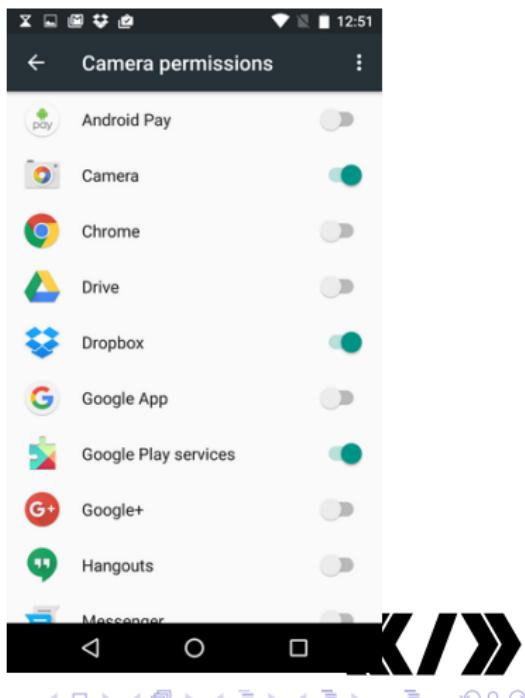
Android

Standard ab 6.0 Einstellungen ->
Sicherheit -> Telefon verschlüsseln

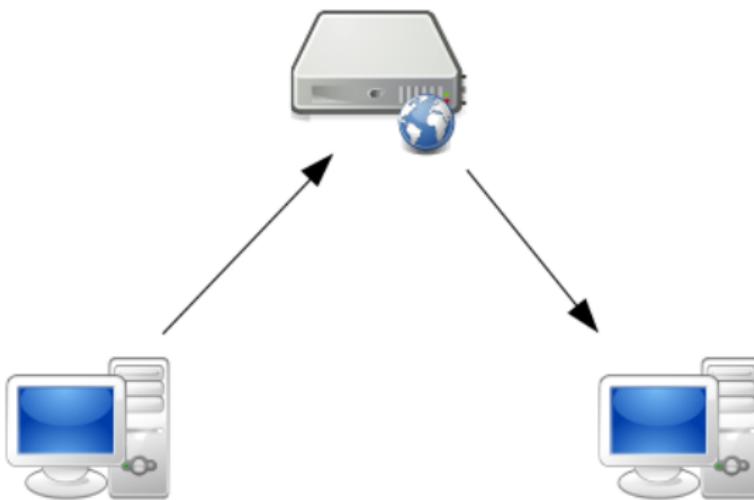
iOS

Standard

wichtig: gute PIN/Muster



Was ist zu schützen?

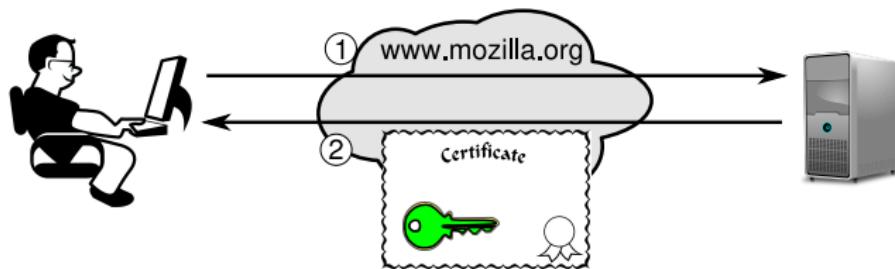


Angreifer im eigenen Netz

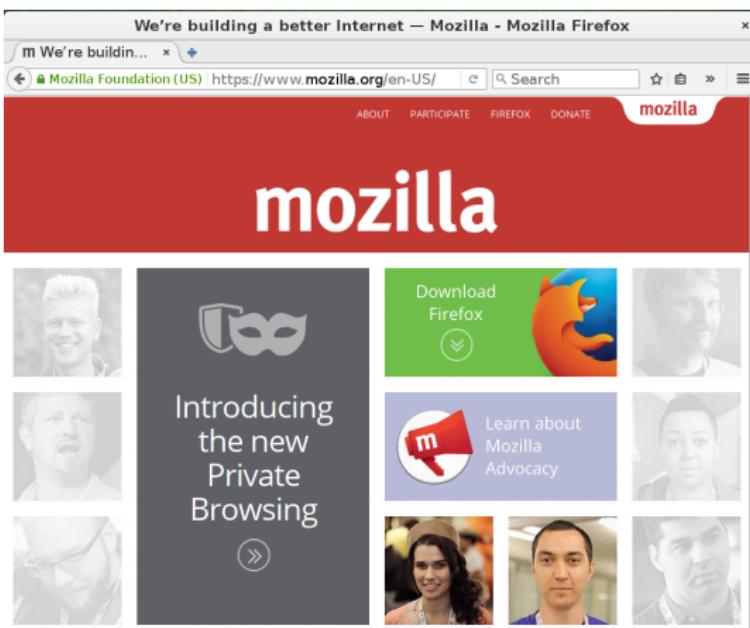


Transportwegverschlüsselung

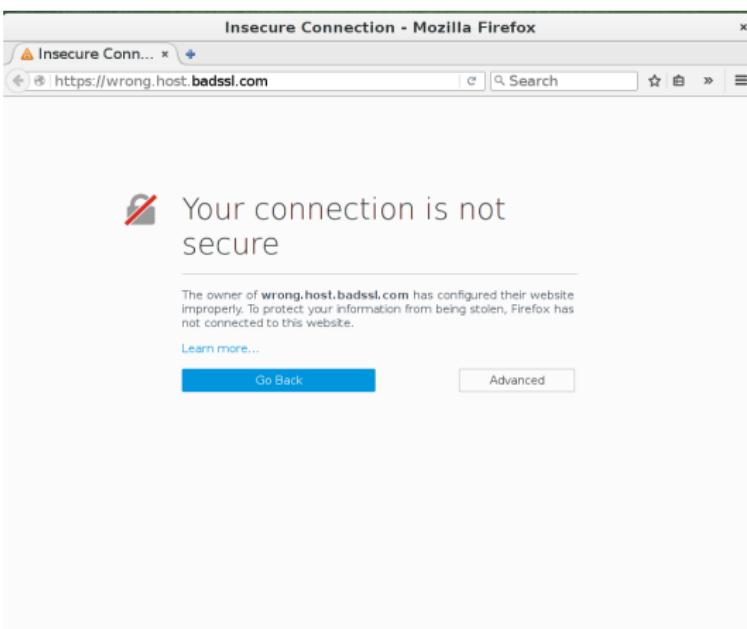
SSL = Secure Socket Layer / TLS = Transport Layer Security



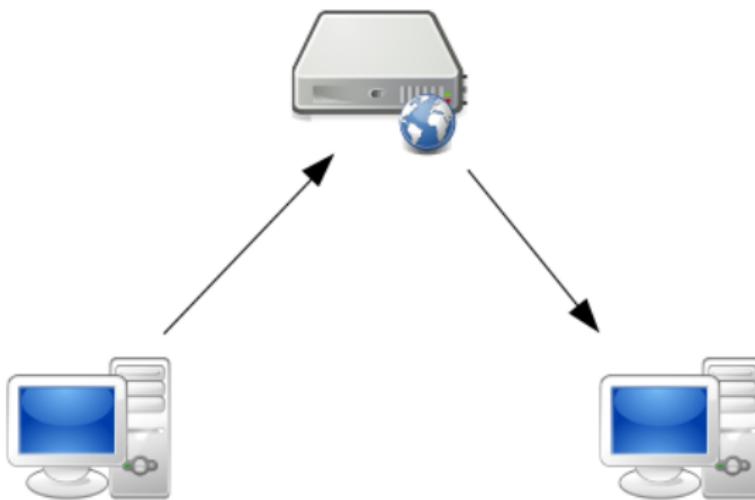
SSL im Browser



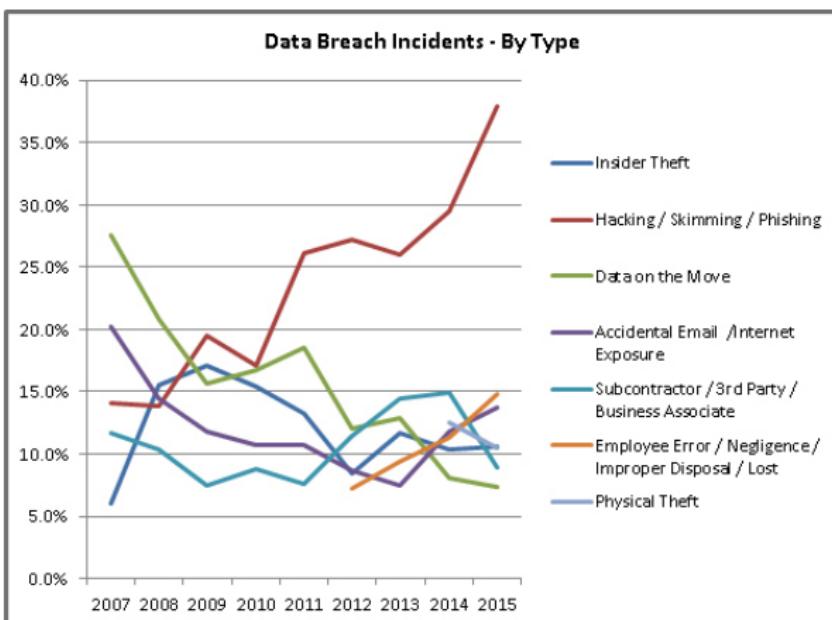
Ungültiges Zertifikat



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

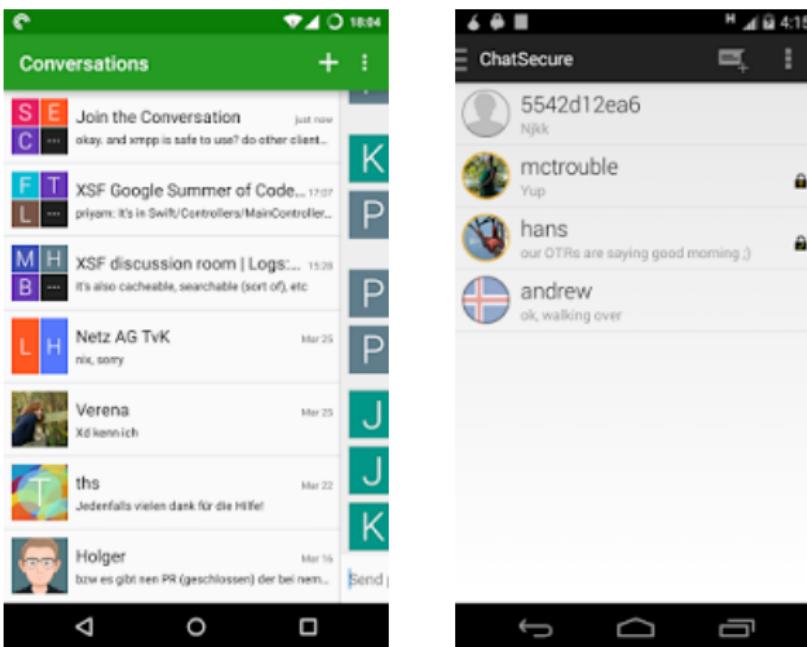
Ende-zu-Ende-Verschlüsselung

- 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

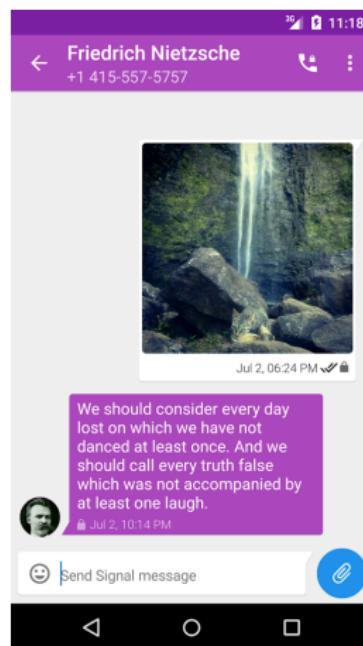
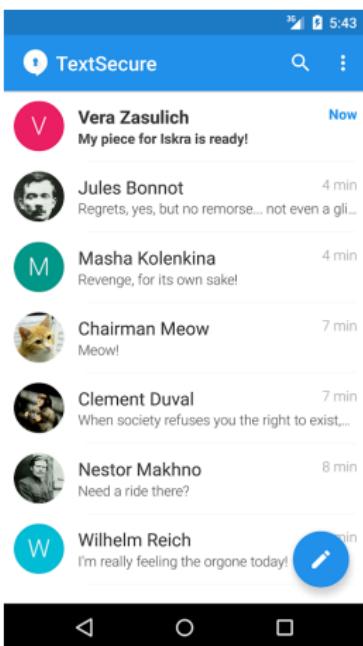
- GPG für E-Mails
- OTR/OMEMO für Jabber:
 - Pidgin für Linux und Windows
 - Conversations oder ChatSecure für Android
 - Adium für Mac, ChatSecure für iOS
- palava.tv, talky.io, Tox, Linphone für Videotelefonie
- Signal

Jabber: Conversations, ChatSecure



<https://xmpp.net/directory.php>

Signal



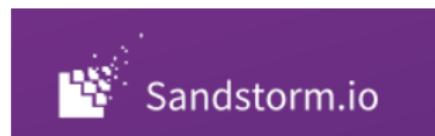
Vergleich Messenger

	Whatsapp	Threema	Telegram	Signal	Jabber
Verschlüsselung	orange	yellow	orange	green	green
Vertrauensw.	red	yellow	orange	green	green
Dezentr.	red	red	red	orange	green
Open Source	red	red	yellow	green	green
Mobileignung	green	green	green	green	yellow

Dezentrale Dienste

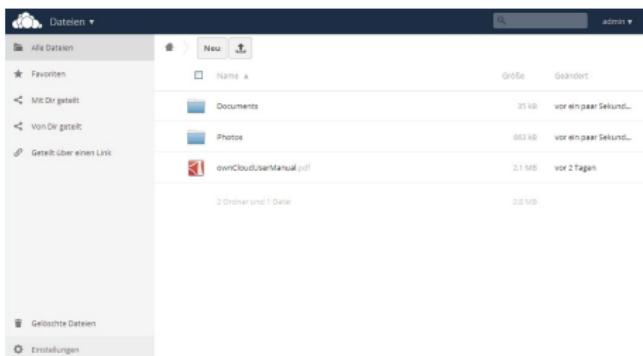


E-Mail



Owncloud

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



Owncloud als Ersatz für Dropbox

The screenshot shows the OwnCloud web interface. The top navigation bar includes a logo, the text "Dateien ▾", a search bar, and a user dropdown set to "admin ▾". On the left, a sidebar lists "Alle Dateien" (selected), "Favoriten", "Mit Dir geteilt", "Von Dir geteilt", and "Geteilt über einen Link". Below this are sections for "Gelöschte Dateien" and "Einstellungen". The main content area displays a list of files and folders:

Name	Größe	Geändert
Documents	35 kB	vor ein paar Sekund...
Photos	663 kB	vor ein paar Sekund...
ownCloudUserManual.pdf	2.1 MB	vor 2 Tagen

At the bottom, it shows "2 Ordner und 1 Datei" with a total size of "2.8 MB".



Owncloud als Ersatz für Google/Apple-Sync

Calendar - Week 11 of 2016

Day Week Month Today

+ New Calendar

ownCloud

Private

contact_birthdays

Meetings(user4)

Subscriptions

land_gig(user3)

Settings

Sun 3/6 Mon 3/7 Tue 3/8 Wed 3/9 Thu 3/10 Fri 3/11 Sat 3/12

all-day 7am 8am 9am 10am 11am 12pm 1pm 2pm 3pm 4pm 5pm 6pm 7pm 8pm 9pm 10pm 11pm

7am 8am 9am 10am 11am 12pm 1pm 2pm 3pm 4pm 5pm 6pm 7pm 8pm 9pm 10pm 11pm

8am 9am 10am 11am 12pm 1pm 2pm 3pm 4pm 5pm 6pm 7pm 8pm 9pm 10pm 11pm

9am 10am 11am 12pm 1pm 2pm 3pm 4pm 5pm 6pm 7pm 8pm 9pm 10pm 11pm

10am 11am 12pm 1pm 2pm 3pm 4pm 5pm 6pm 7pm 8pm 9pm 10pm 11pm

11am 12pm 1pm 2pm 3pm 4pm 5pm 6pm 7pm 8pm 9pm 10pm 11pm

12pm 1pm 2pm 3pm 4pm 5pm 6pm 7pm 8pm 9pm 10pm 11pm

1pm 2pm 3pm 4pm 5pm 6pm 7pm 8pm 9pm 10pm 11pm

2pm 3pm 4pm 5pm 6pm 7pm 8pm 9pm 10pm 11pm

3pm 4pm 5pm 6pm 7pm 8pm 9pm 10pm 11pm

4pm 5pm 6pm 7pm 8pm 9pm 10pm 11pm

5pm 6pm 7pm 8pm 9pm 10pm 11pm

6pm 7pm 8pm 9pm 10pm 11pm

7pm 8pm 9pm 10pm 11pm

8pm 9pm 10pm 11pm

9pm 10pm 11pm

10pm 11pm

11pm

Meeting with Jos

ownCloud

starts 03/10/2016 ends 03/10/2016

02:00 PM 05:00 PM

All day Event

Location

Description

When shared show full event

Attendees Reminders

E-Mail address of attendee

Add

Jos Poortvliet

Delete Cancel Export Update

The screenshot shows a weekly calendar view from Sunday, March 6, to Saturday, March 12, 2016. The calendar lists several events, including 'Take care of final' at 3pm on Monday, 'Workout' at 12pm on Tuesday, 'Cinema' at 8pm on Wednesday, 'Talk about ownCloud' at 8pm on Thursday, and 'Dinner with Jos' at 8pm on Friday. A specific event, 'Meeting with Jos', is highlighted in blue and is being edited. The edit dialog shows the event title 'Meeting with Jos', the source 'ownCloud', and the date and time '03/10/2016' from '02:00 PM' to '05:00 PM'. There are checkboxes for 'All day Event' and 'Location', and a dropdown for 'Description' and 'When shared show full event'. Below the edit dialog, there are buttons for 'Delete', 'Cancel', 'Export', and 'Update', with 'Update' being the active button.



Owncloud als Ersatz für Google/Apple-Sync

The screenshot shows the OwnCloud Contacts application interface. At the top, there's a navigation bar with icons for file operations (New, Open, Save, etc.) and user settings. Below the bar, the title "Contacts" is displayed with a dropdown arrow. On the left, a sidebar lists "All contacts" with icons and names: Franz Liszt (orange), Ludwig van Beethoven (green), Pyotr Tchaikovsky (pink), and Wolfgang Amadeus Mozart (purple). The contact for Wolfgang Amadeus Mozart is currently selected and shown in detail on the right. The contact card includes fields for email (wolfgang@mozart.at), work phone number (Home), address (Mozartplatz, 5010 Salzburg, Austria), birthday (01/27/1756), and a dropdown for Composers. There are also buttons for "Add field ..." and a trash icon. At the bottom of the sidebar, there's a "Settings" icon.

Owncloud als Ersatz für Google Docs

The screenshot shows the ownCloud web interface with a document titled "Example.edt". The interface includes a toolbar with "Share", "Format" (bold, italic, underline, font), "Font" (Helvetica Neue), "Size" (10.4), "Text body", and "100%". The main content area displays the document's content and a sidebar for user "admin" (Rosa Luxemburg). A red dotted line highlights a comment from "admin" about file synchronization.

Welcome to ownCloud, your self-hosted file sync and share solution.

OwnCloud is open source file sync and share software for everyone from individuals operating the free Community Edition, to large enterprises and service providers operating ownCloud Enterprise Edition. ownCloud provides a safe, secure and compliant file sync and share solution on servers you control.

With ownCloud you can share one or more folders on your PC, and sync them with your ownCloud server. Place files in your local shared directories, and those files are immediately synced to the server, and then to other PCs via the desktop client. Not near a desktop client? No problem, simply log in with the web client and manage your files there. The Android and iOS mobile apps allow you to browse, download and upload photos and videos. On Android, you may also create, download, edit and upload any other files, with the correct software installed.

Whether using a mobile device, a workstation, or a web client, ownCloud provides the ability to put the right files at the right hands at the right time on any device in one simple-to-use, secure, private and controlled solution.

After all, with ownCloud, it's Your Cloud, Your Data, Your Way.

Yay! we can edit documents - together with others. Let's share a link!

bla
blab
blabla and more bla!

isn't this awesome?

Yes, It is quite cool

(All example pictures & music are licensed under Creative Commons Attribution.)

admin
2015-06-24T08:34:11
0.288Z

I find this entirely non-offensive! It can use improvements.

Rosa Luxemburg
2015-06-24T08:34:33
8.408Z

I don't like control unless it is mine.

I can edit too

Einleitung
oooooooooooo

Einführung
ooooo

Geräte
oooooooooooooooooooo

Inhalte
oooooooooooo

Dezentrale Dienste
ooooooo

Verhalten
●

Fazit
○

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, Gerätoverschlüsselung)



Folien: Chaos Computer Club Dresden

CMS Dresden: schule@c3d2.de

FSFW: <https://fsfw-dresden.de/>