Crypto-Seminar

Digitale Selbstverteidigung gegen Massenüberwachung

(Bild: CC-BY, Daniela Vladimirova)

„Ich möchte nicht in einer Welt leben, in der alles, was ich sage, alles, was ich tue, jedes Gespräch, jeder Ausdruck von Kreativität, Liebe oder Freundschaft aufgezeichnet wird.

Das ist nichts, was ich bereit bin zu unterstützen.
Das ist nichts, das ich bereit bin mit aufzubauen.
Das ist nichts, unter dem ich zu leben bereit bin.
Ich denke, jeder, der eine solche Welt ablehnt, hat die Verpflichtung, im Rahmen seiner Möglichkeiten zu handeln.“

– Edward Snowden

Agenda

- Inputvortrag zu:
  - Sichere Passwörter
  - Verschlüsselung von E-Mails (PGP)
  - Tracking beim Browsen vermeiden / Tor
  - Dateiverschlüsselung
  - Mobilgeräte/Smartphones
- Praxis

Die vier Freiheiten der Freien Software

1) Uneingeschränktes Verwenden zu jedem Zweck.

2) Das Recht, die Funktionsweise zu untersuchen und zu verstehen.

3) Das Recht, Kopien der Software zu verbreiten.

4) Das Recht, die Software zu verbessern und die Verbesserungen zu verbreiten.

Sichere Passwörter

Wie werden Passwörter geknackt?

- Brute Force
  - Alle möglichen Kombinationen ausprobieren
- Listen / Wörterbuch-Angriffe
  - Alle Wörter aus einer Liste oder einem Wörterbuch ausprobieren
- Social Engineering
  - Phishing, Person austricksen um PW zu erfahren
  - Gerne auch durch Facebook, LinkedIn etc.

Wie erschwert man das Knacken des Passworts?

- Brute Force
  - ⇒ Länge (10+ Zeichen)
  - ⇒ Verschiedene Zeichentypen
    (Groß- und Kleinbuchstaben, Zahlen, Sonderzeichen)

Wie erschwert man das Knacken des Passworts?

- Brute Force
  - ⇒ Länge (10+ Zeichen)
  - ⇒ Verschiedene Zeichentypen
    (Groß- und Kleinbuchstaben, Zahlen, Sonderzeichen)
- Listen / Wörterbuch-Angriffe
  - ⇒ Kein einzelnes Wort als PW verwenden
  - ⇒ Keine Wörter aus dem Umfeld (Namen, Geburtsdaten)

Wie erschwert man das Knacken des Passworts?

- Brute Force
  - ⇒ Länge (10+ Zeichen)
  - ⇒ Verschiedene Zeichentypen
    (Groß- und Kleinbuchstaben, Zahlen, Sonderzeichen)
- Listen / Wörterbuch-Angriffe
  - ⇒ Kein einzelnes Wort als PW verwenden
  - ⇒ Keine Wörter aus dem Umfeld (Namen, Geburtsdaten)
- Social Engineering
  - ⇒ Niemandem das Passwort verraten!

Sichere Passwörter finden

- Wichtig:
  - Für jeden Dienst ein anderes Passwort verwenden!
  - Passwörter in regelmäßigen Abständen austauschen/ändern
- DBiR&dSd90M!
  - Merksatz: »**D**er **B**all **i**st **R**und **&** **d**as **S**piel **d**auert **90** **M**inuten**!**«
- HausLocherTasteMeloneBagger
  - Wortreihung
- 2UrN47oCfK6jAZ8xuKHiop4upPsI73
  - Passwortgenerator

Passwortverwaltung

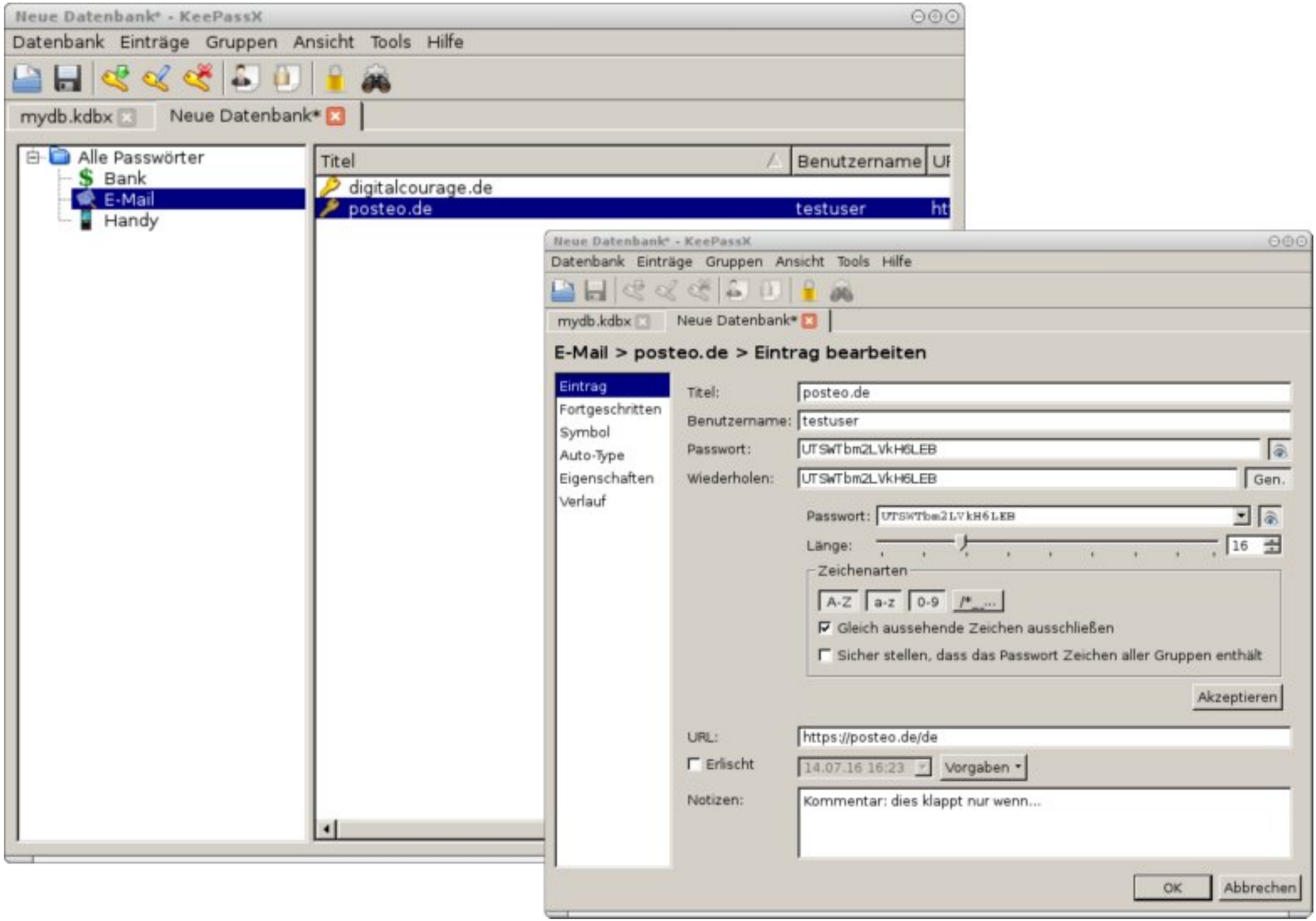
Software: **KeePassX**

Vorteile

- Freie Software
- Viele Plattformen
  - Win, Linux, Mac, Android
- Passwortgenerator
- Verschlüsselt gespeichert

Nachteile

- Masterpasswort
  - Darf nicht vergessen oder geknackt werden!
- Gefahr bei Verlust
  - „Setzt alles auf eine Karte“: PW-Datenbank gut sichern!
- Komfort
  - Kein Sync zwischen verschiedenen Geräten

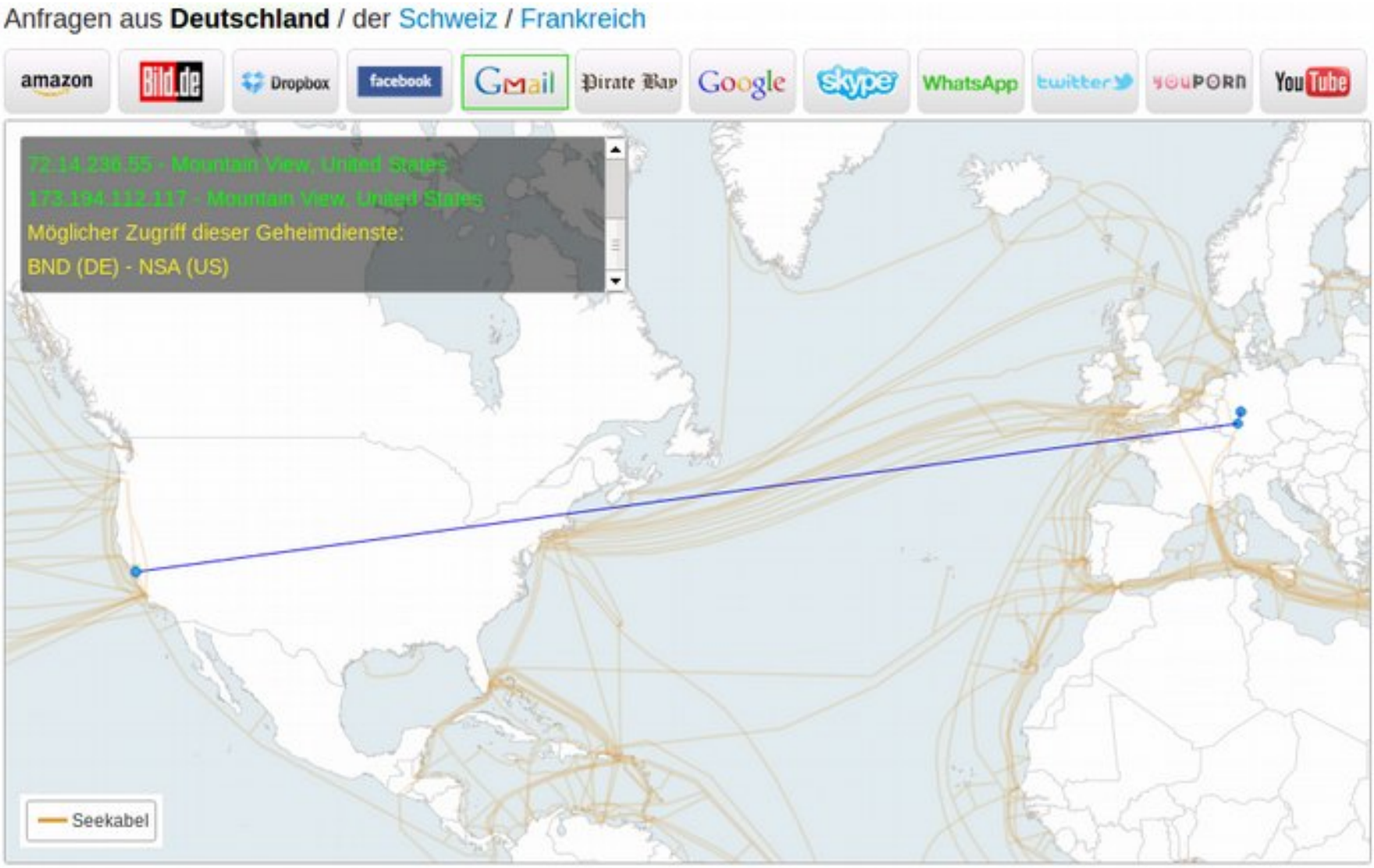

Neue Datenbank* - KeePassX
Datenbank Einträge Gruppen Ansicht Tools Hilfe
mydb.kdbx
Neue Datenbank*
Alle Passwörter
Bank
E-Mail
Handy
Titel
Benutzername
digitalcourage.de
posteo.de
testuser
E-Mail > posteo.de > Eintrag bearbeiten
Eintrag
Fortgeschritten
Symbol
Auto-Type
Eigenschaften
Verlauf
Titel: posteo.de
Benutzername: testuser
Passwort: UTSWTbm2LVkH6LEB
Wiederholen: UTSWTbm2LVkH6LEB
Gen.
Länge: 16
Zeichenarten
A-Z
a-z
0-9
Gleich aussehende Zeichen ausschließen
Sicher stellen, dass das Passwort Zeichen aller Gruppen enthält
Akzeptieren
URL: https://posteo.de/de
Erlischt
14.07.16 16:23
Vorgaben
Notizen: Kommentar: dies klappt nur wenn...
OK
Abbrechen

Videoempfehlung

- Video von Alexander Lehmann " Passwörter Einfach Erklärt" an; abrufbar unter: https://vimeo.com/138839266

E-Mail-Verschlüsselung

E-Mail Anbieter



Quelle: http://apps.opendatacity.de/prism/de

Alternativen zu „kostenlosen“ E-Mail-Anbietern

- **Posteo.de** oder **mailbox.org**
- 24h-Einmal-E-Mail-Adresse, gratis: anonbox.net (CA-Cert)

Vorteile

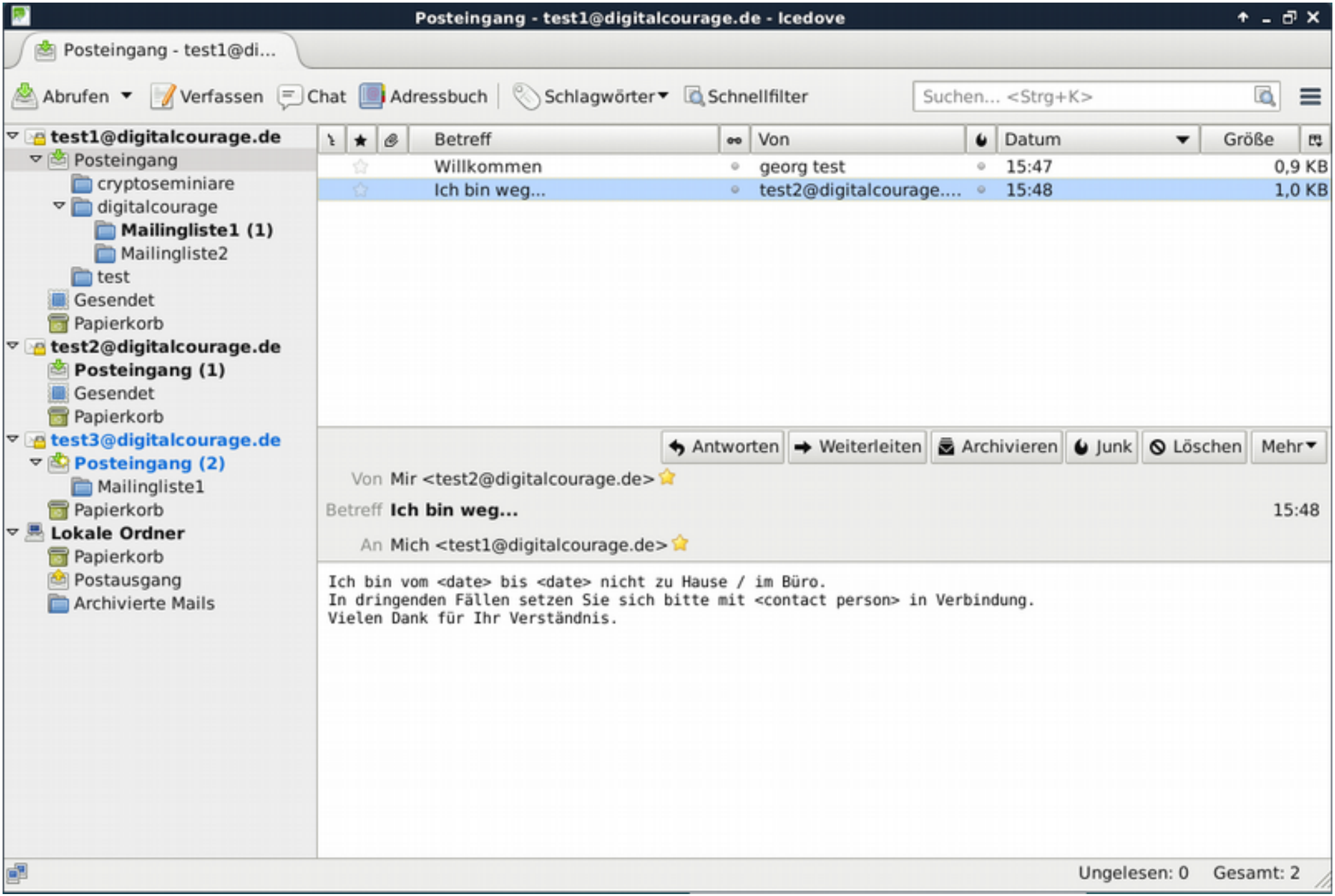
- Standort in Deutschland
- Datensparsamkeit
- Keine Inhaltsanalyse
- Keine Werbung
- Anonyme Nutzung möglich
- Datenschutz hat Priorität

Nachteile

- posteo.de und mailbox.org kosten 1 € pro Monat

E-Mail-Verwaltung

- Software: **Mozilla Thunderbird**
  - Freie Software
  - Mehrere Mail-Konten möglich
  - Verwaltung mit Filtern und Ordnern
  - HTML abschalten möglich
  - Mails offline lesen, speichern und durchsuchen
  - Add-ons: Kalender, Massenmails, **Verschlüsselung**


Posteingang - test1@digitalcourage.de - Icedove
Posteingang - test1@di...
Abrufen
Verfassen
Chat
Adressbuch
Schlagwörter
Schnellfilter
Suchen... <Strg+K>
test1@digitalcourage.de
Posteingang
cryptoseminiare
digitalcourage
Mailingliste1 (1)
Mailingliste2
test
Gesendet
Papierkorb
test2@digitalcourage.de
Posteingang (1)
Gesendet
Papierkorb
test3@digitalcourage.de
Posteingang (2)
Mailingliste1
Papierkorb
Lokale Ordner
Papierkorb
Postausgang
Archivierte Mails
Betreff
Von
Datum
Größe
Willkommen
georg test
15:47
0,9 KB
Ich bin weg...
test2@digitalcourage....
15:48
1,0 KB
Antworten
Weiterleiten
Archivieren
Junk
Löschen
Mehr
Von Mir <test2@digitalcourage.de>
Betreff Ich bin weg...
15:48
An Mich <test1@digitalcourage.de>
Ich bin vom <date> bis <date> nicht zu Hause / im Büro.
In dringenden Fällen setzen Sie sich bitte mit <contact person> in Verbindung.
Vielen Dank für Ihr Verständnis.
Ungelesen: 0
Gesamt: 2

E-Mail-Verschlüsselung (PGP)

Vorteile

- Inhalt Ende-zu-Ende-verschlüsselt
- Absender[1] & Empfängerin werden eindeutig
([1] mit PGP-Signatur)

Nachteile

- Metadaten (von, an, Betreff etc). bleiben unverschlüsselt
- Absender & Empfängerin müssen PGP nutzen

Benötigte Software:

- E-Mail Programm: Thunderbird
- Add-on: **Enigmail**

Unterschied symmetrische / asymmetrische Verschlüsselung

Symmetrische Verschlüsselung

- Wie analoge Schlüssel
- **Derselbe Schlüssel** zum Ver- und Entschlüsseln
- Alle Beteiligten brauchen diesen (geheimen) Schlüssel
- Problem: um Nachrichten (auf unsicheren Kanälen) zu senden, muss zuerst der Schlüssel (auf sicherem Kanal) verteilt werden

Unterschied symmetrische / asymmetrische Verschlüsselung

Asymmetrische Verschlüsselung → PGP

- **Schlüsselpaar:** was **ein** Schlüssel **ver**schlüsselt, muss mit dem **anderen** Schlüssel **ent**schlüsselt werden
- Alle Beteiligten erzeugen ein eigenes Schlüsselpaar

- Öffentlicher Schlüssel (zum Verschlüsseln)
  - kann und muss verteilt werden (an alle, über unsichere Kanäle)

- Privater Schlüssel (zum Entschlüsseln)
  - bleibt privat – gut schützen und sichern, niemals herausgeben!

Unterschied symmetrische / asymmetrische Verschlüsselung

- Es gilt:
  - Absender braucht **öffentlichen Schlüssel der Empfängerin**
  - nur Empfängerin kann (mit ihrem privaten Schlüssel) entschlüsseln

PGP Public Keys austauschen

- E-Mail Anhang
  - .asc Datei
- Key-Server
  - Bequem durchsuchbar
  - E-Mail-Adresse öffentlich einsehbar

Digitale Signatur mit PGP

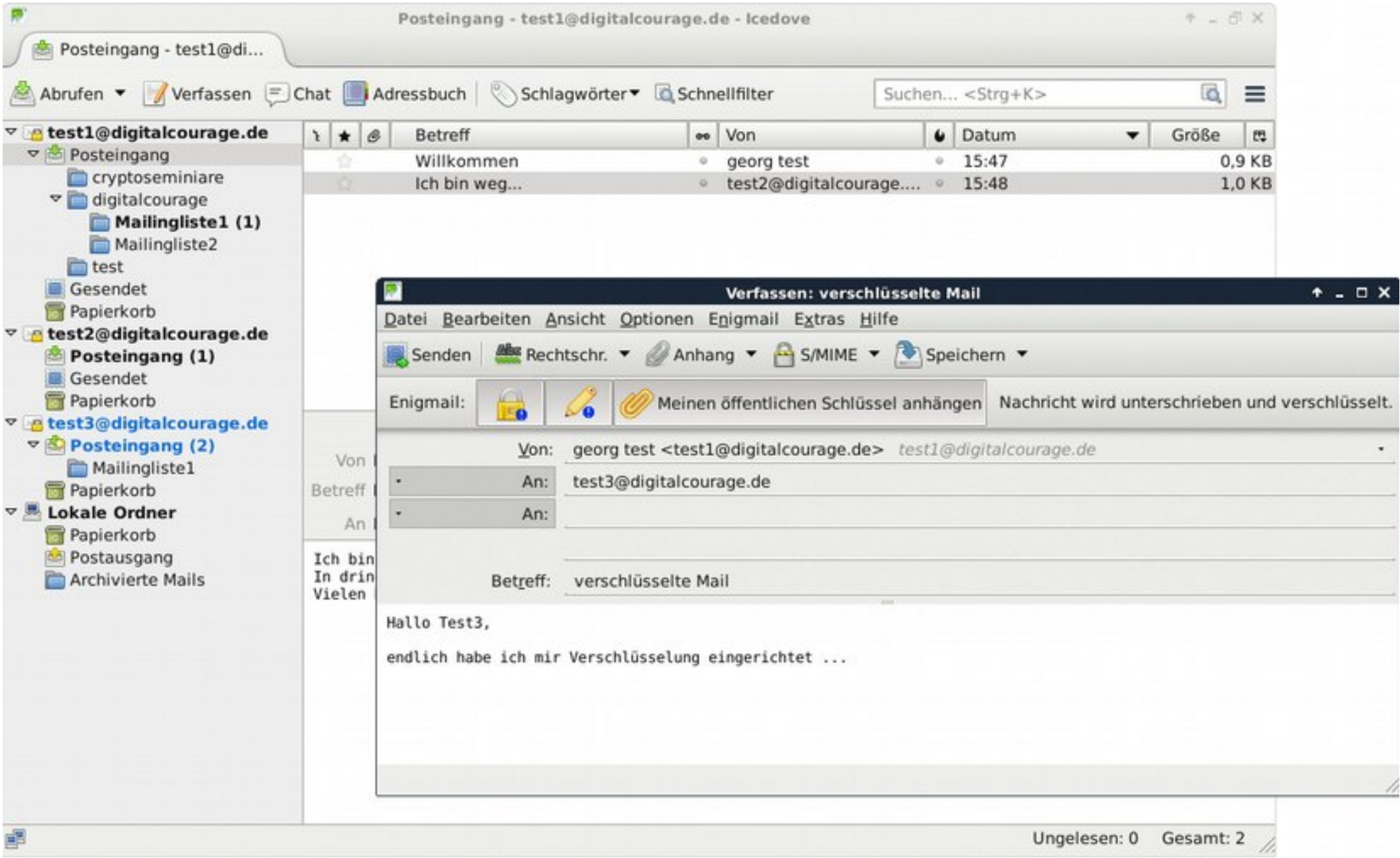
- Analoger Vergleich: Siegel
  - Sender eindeutig: Authentizität
  - Nachricht nicht manipuliert: Integrität

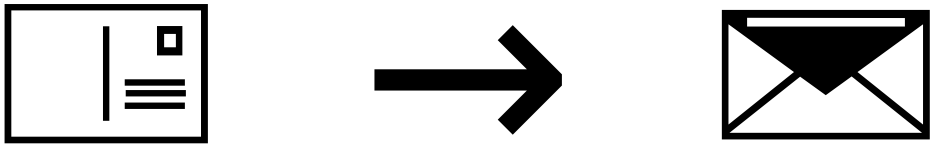
- Auch ohne Verschlüsseln möglich
- Beispiel:

```
-----BEGIN PGP SIGNATURE-----
iQA/AwUBONpOg40d+PaAQUTlEQIc5ACdGkKSzpOrsT0Gvj
3jH9NXD8ZP2IcAn0vj/BHT+qQCtPCtCwO1aQ3Xk/NL=1CZt
-----END PGP SIGNATURE----
```

Schlüssel-Fingerabdruck

- Echtheit von öffentlichen Schlüsseln überprüfen
- Eine Art "Quersumme"
- Weltweit nur auf einen Schlüssel passend
- Beispiel:
  - Fingerprint zum öffentlichen Schlüssel mit der ID 0x315DFB0A
  - DF31 49DD 7046 0F3A 7F17 3C4A 4818 84B5 315D FB0A


Posteingang - test1@digitalcourage.de - Icedove
Posteingang - test1@di...
Abrufen
Verfassen
Chat
Adressbuch
Schlagwörter
Schnellfilter
Suchen... <Strg+K>
test1@digitalcourage.de
Posteingang
cryptoseminiare
digitalcourage
Mailingliste1 (1)
Mailingliste2
test
Gesendet
Papierkorb
test2@digitalcourage.de
Posteingang (1)
Gesendet
Papierkorb
test3@digitalcourage.de
Posteingang (2)
Mailingliste1
Papierkorb
Lokale Ordner
Papierkorb
Postausgang
Archivierte Mails
Betreff
Von
Datum
Größe
Willkommen
georg test
15:47
0,9 KB
Ich bin weg...
test2@digitalcourage....
15:48
1,0 KB
Verfassen: verschlüsselte Mail
Datei Bearbeiten Ansicht Optionen Enigmail Extras Hilfe
Senden
Rechtschr.
Anhang
S/MIME
Speichern
Enigmail:
Meinen öffentlichen Schlüssel anhängen
Nachricht wird unterschrieben und verschlüsselt.
Von:
georg test <test1@digitalcourage.de>
test1@digitalcourage.de
An:
test3@digitalcourage.de
An:
Betreff:
verschlüsselte Mail
Hallo Test3,
endlich habe ich mir Verschlüsselung eingerichtet ...
Ungelesen: 0
Gesamt: 2



"Privacy is the right to a free mind."

– Edward Snowden

Tracking beim Browsen vermeiden

&

Tor

Datenschutzfreundliches Surfen mit Firefox

- „Das Web ist kaputt.“
- Auf fast allen Webseiten werden etliche Inhalte von Drittanbietern nachgeladen (nicht nur Werbung!)

Nachgeladene Inhalte von Drittanbietern

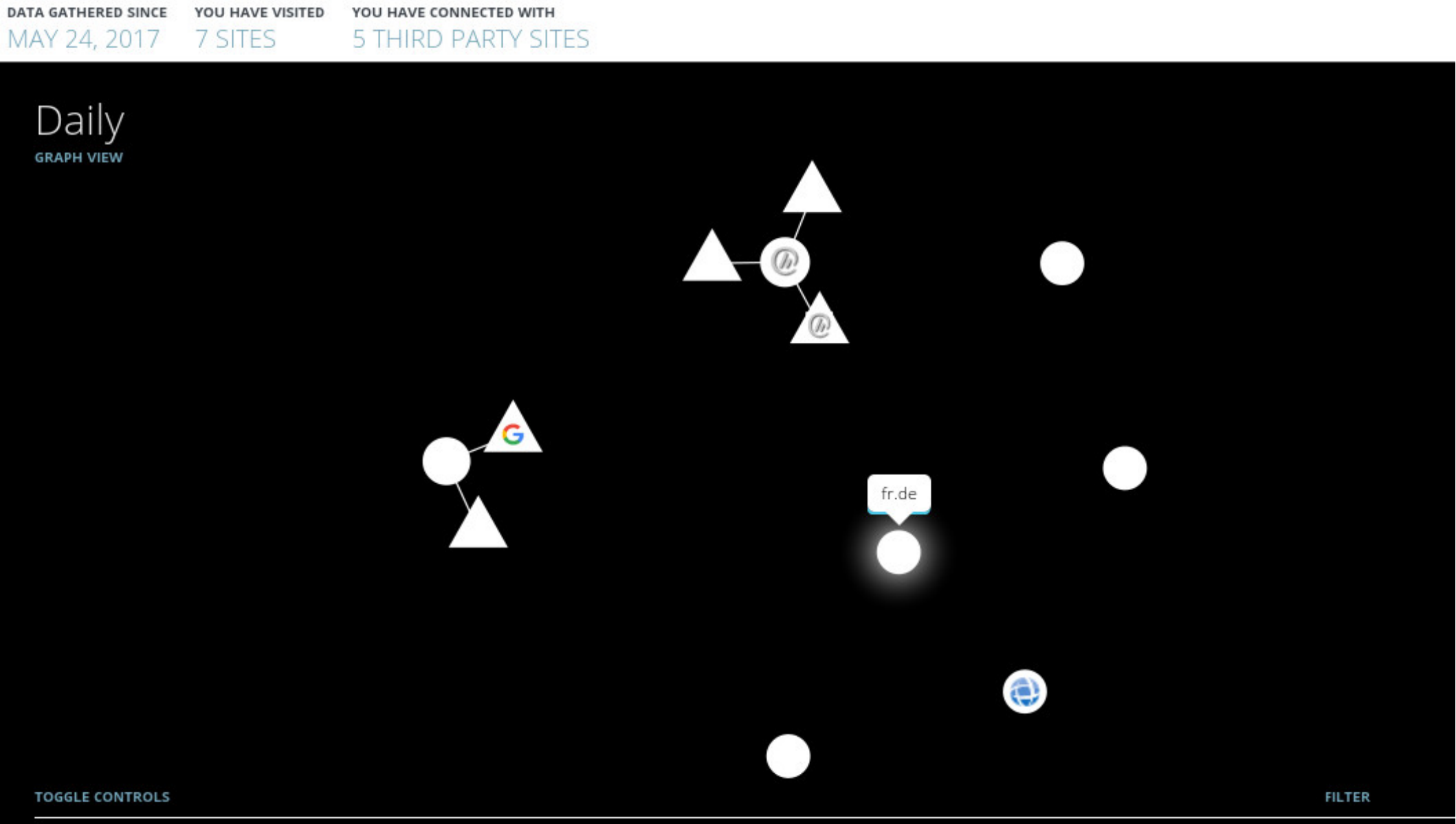
Beispiel: www.spiegel.de

Standard-Firefox, Debian 8 GNU/Linux

- 136 HTTP-GETs an folgende Domains...
- spiegel.de, meetrics.net, ioam.de, adition.com, yieldlab.net, criteo.com, *flashtalking.com*, exactag.com, parsely.com, meetrics.net, outbrain.com, *atdmt.com, ligatus.com*, doubleclick.net, adform.net, google-analytics.com, *t4ft.de*, *westlottol.com*, *ligadx.com,* googlesyndication.com, *lqm.io*, *soundcloud.com*,
- 1,6 MB; 59 Cookies von 19 Domains
- Ladezeit ca. 17 Sek. (Core i5 M560)

Analyse im Firefox mit Lightbeam

Analyse im Firefox mit Lightbeam



Wie kann eine Webseite mich verfolgen und identifizieren?

- Cookies:
  - kleine Textdateien, die die aufgerufene Webseite im Browser speichern und wieder abrufen kann.
- Nachladen von Drittanbieter-Inhalten
- Passive Merkmale:
  - IP-Adresse, Sprache, Browser, Betriebssystem
- Aktive Merkmale (Javascript, Flash, Java, h264, …)
  - Schriftarten, Browser-Add-ons, Bildschirmauflösung, uvm.

⇒ Eindeutiger Browser-Fingerabdruck

  - siehe https://panopticlick.eff.org/

Wie kann ich mich vor Tracking schützen?

- Browser-Wahl
  - Firefox
- Browser-Einstellungen
  - Do-not-Track Option
  - Benutzerdefinierte Chronik:
    Cookies (für Drittanbieter) deaktivieren
- Suchmaschinen
  - Ixquick.eu, Startpage.com, DuckDuckGo.com, MetaGer.de, etc.
    (im Gegensatz zu Google auch keine individuellen Ergebnisse)
- Browser-Add-ons! …

Schutz durch Firefox-Add-ons

- Tracker und Werbung blocken: **uBlock origin**
- Aktive Inhalte blocken: **NoScript**
  - Skripte allgemein erlauben (vom Hersteller nicht empfohlen)
- Webseiten immer verschlüsseln: **HTTPS Everywhere**
- Ein Klick statt about:config: **Privacy-Settings**
- **Adobe-Flash am besten entfernen oder deaktivieren!**

Etwas komplizierter und aufwendiger:

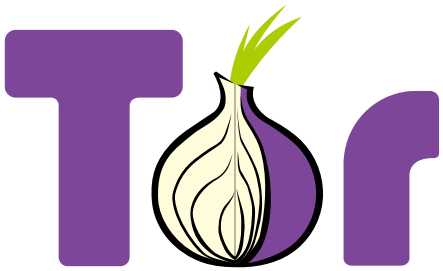
- Alle Skripte blocken mit **NoScript**
- Alle Drittanbieteranfragen blocken: **uMatrix**
- Referer blocken: **RefControl** (Vorsicht!)

Tor-Browser

Was ist der Tor-Browser?

- modifizierter Firefox
- enthält und nutzt Tor zum anonymen Surfen

Tor (von „The Onion Router“)



Was ist Tor?

- Netzwerk zur Anonymisierung von Verbindungsdaten
- IP-Adresse wird verschleiert

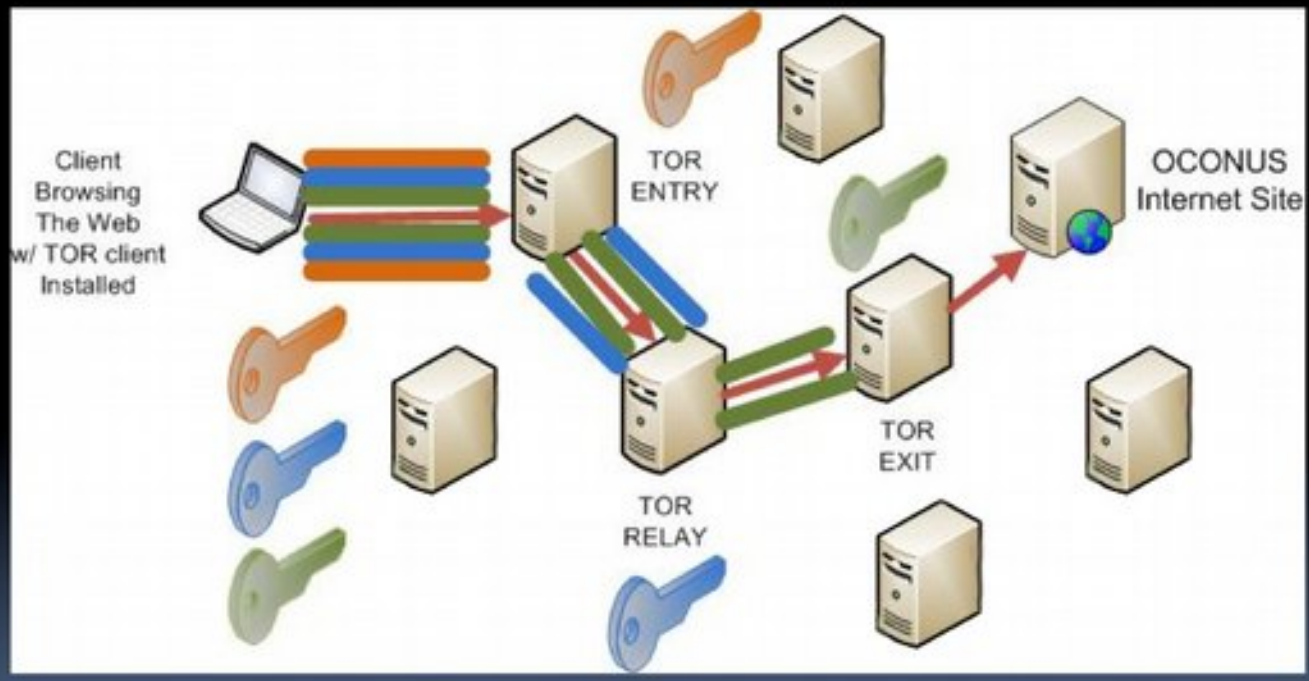
Vorteile

- Freie Software
- Anonymes Surfen

Nachteile

- Login bei personalisierten Seiten nicht sinnvoll

(U) What is TOR?


Client
Browsing
The Web
w/ TOR client
Installed
TOR
ENTRY
TOR
RELAY
TOR
EXIT
OCONUS
Internet Site

Dateiverschlüsselung

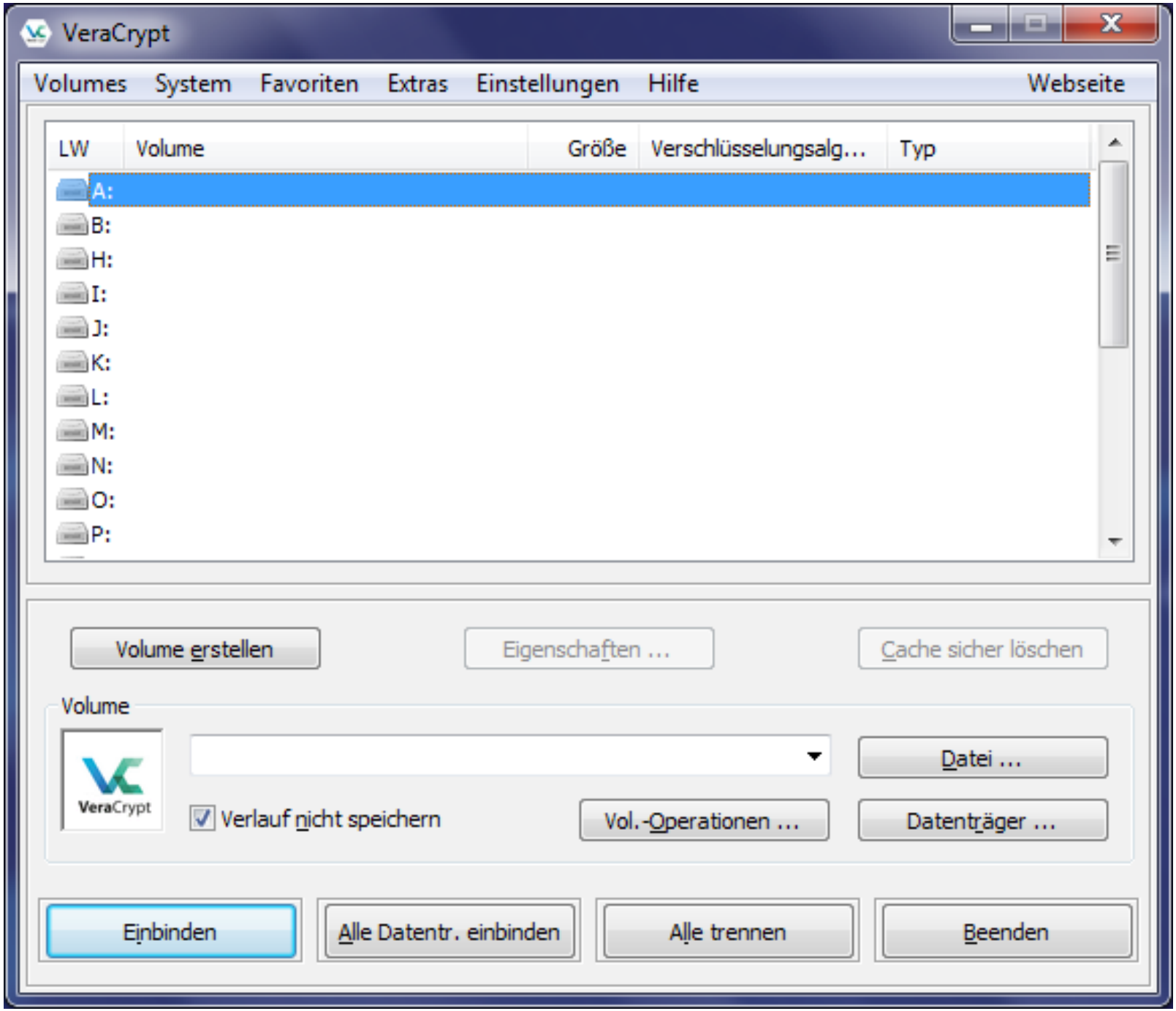
Dateiverschlüsselung

Software: **VeraCrypt**

- https://www.veracrypt.fr/
- Software zur Datenverschlüsselung
- Quelloffen und auf allen gängigen Plattformen verfügbar

Was kann ich mit VeraCrypt machen?

- Verschlüsselte Container (Ordner) erstellen, komplette Festplatten und Wechseldatenträger verschlüsseln


VeraCrypt
Volumes System Favoriten Extras Einstellungen Hilfe Webseite
LW Volume Größe Verschlüsselungsalg... Typ
A:
B:
H:
I:
J:
K:
L:
M:
N:
O:
P:
Volume erstellen
Eigenschaften ...
Cache sicher löschen
Volume
VeraCrypt
Datei ...
Verlauf nicht speichern
Vol.-Operationen ...
Datenträger ...
Einbinden
Alle Datentr. einbinden
Alle trennen
Beenden

Mobilgeräte

Überwachung

Geheimdienste sammeln...

- tägl. rund 5 Milliarden Standortdaten von Mobiltelefonen
- tägl. fast 200 Millionen SMS

Überwachung

…und werten sie unter bestimmten Blickwinkeln aus

(Kontaktbeziehungen, Reisedaten, Finanztransfers, …)

…bzw. setzen die gesammelten Daten gezielt ein

(z. B. in der Ukraine Anfang 2014. SMS an Teilnehmer einer Demonstration:

"Sehr geehrter Kunde, sie sind als Teilnehmer eines Aufruhrs registriert.")

Kommerzielle Datensammelungen

- Neuer Markt für optimierte personenbezogene Werbung
- Apps sammeln diverse Nutzerdaten (z. B. Standortdaten)

App-Berechtigungen: Facebook (1)

- Geräte- & App-Verlauf
  - Aktive Apps abrufen
- Identität
  - Konten auf dem Gerät suchen
  - Konten hinzufügen oder entfernen
  - Kontaktkarten lesen
- Kalender
  - Kalendertermine sowie vertrauliche Informationen lesen
  - Ohne Wissen der Eigentümer Kalendertermine hinzufügen oder ändern und E-Mails an Gäste senden
- Kontakte
  - Konten auf dem Gerät suchen
  - Kontakte lesen
  - Kontakte ändern

App-Berechtigungen: Facebook (2)

- Standort
  - Ungefährer Standort (netzwerkbasiert)
  - Genauer Standort (GPS- und netzwerkbasiert)
- SMS
  - SMS oder MMS lesen
- Telefon
  - Telefonnummern direkt anrufen
- Anrufliste lesen
  - Telefonstatus und Identität abrufen
  - Anrufliste bearbeiten
- Fotos/Medien/Dateien
  - USB-Speicherinhalte lesen
  - USB-Speicherinhalte ändern oder löschen
- Speicher
  - USB-Speicherinhalte lesen
  - USB-Speicherinhalte ändern oder löschen

App-Berechtigungen: Facebook (3)

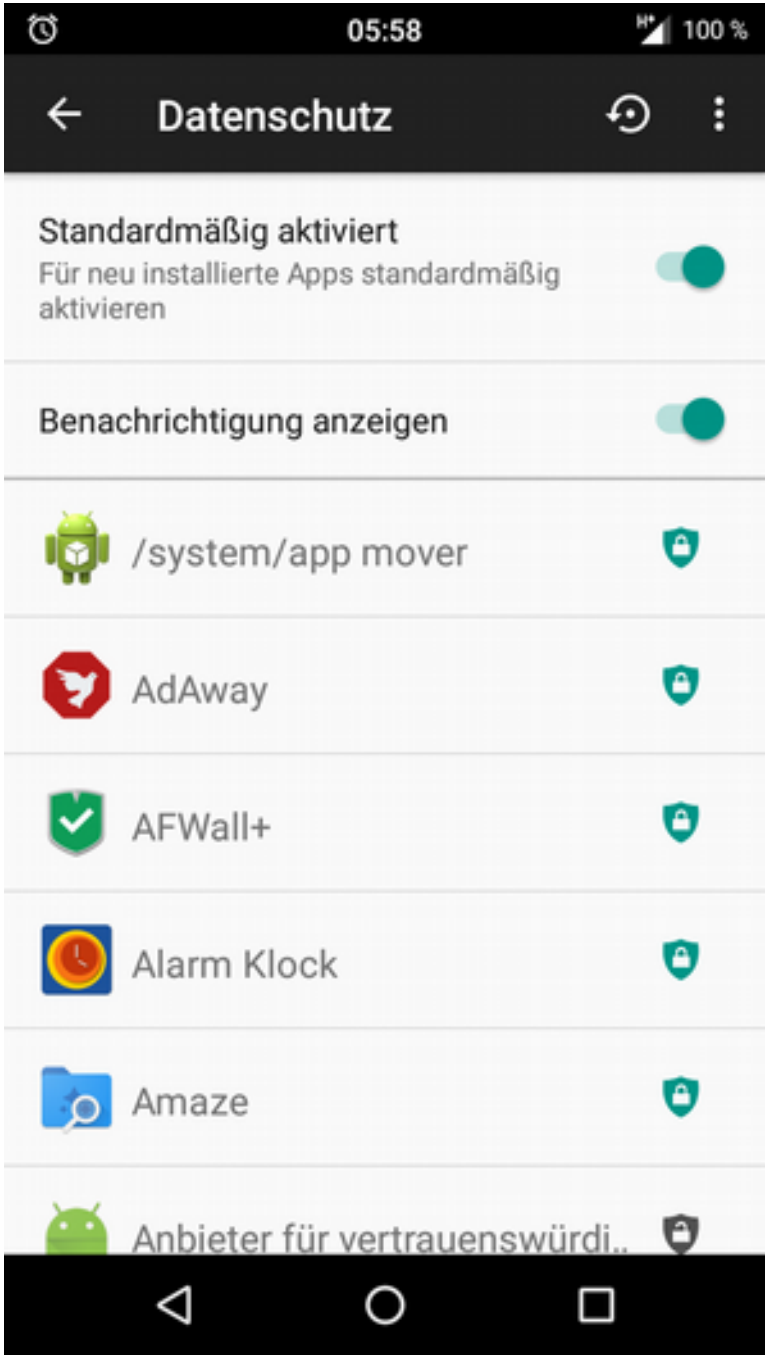
- Kamera
  - Bilder und Videos aufzeichnen
- Mikrofon
  - Ton aufzeichnen
- WLAN-Verbindungsinformationen
  - WLAN-Verbindungen abrufen
- Geräte-ID & Anrufinformationen
  - Telefonstatus und Identität

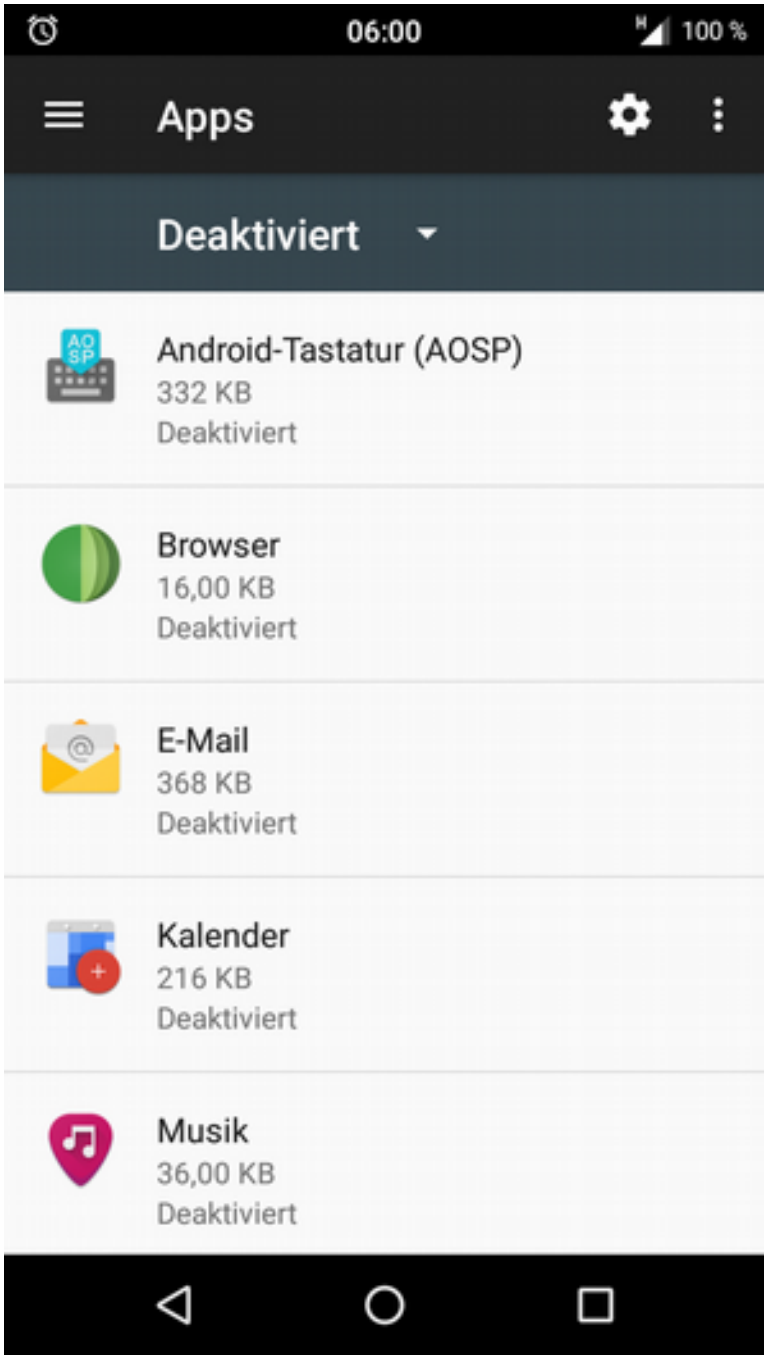
App-Berechtigungen: Facebook (4)

- Sonstige
  - Dateien ohne Benachrichtigung herunterladen
  - Größe des Hintergrundbildes anpassen
  - Daten aus dem Internet abrufen
  - Netzwerkverbindungen abrufen
  - Konten erstellen und Passwörter festlegen
  - Akkudaten lesen
  - dauerhaften Broadcast senden
  - Netzwerkkonnektivität ändern
  - WLAN-Verbindungen herstellen und trennen
  - Statusleiste ein-/ausblenden
  - Zugriff auf alle Netzwerke
  - Audio-Einstellungen ändern
  - Synchronisierungseinstellungen lesen
  - Beim Start ausführen
  - Aktive Apps neu ordnen
  - Hintergrund festlegen
  - Über anderen Apps einblenden
  - Vibrationsalarm steuern
  - Ruhezustand deaktivieren
  - Synchronisierung aktivieren oder deaktivieren
  - Verknüpfungen installieren
  - Google-Servicekonfiguration lesen

App-Berechtigungen

- Sich selbst immer die Frage stellen, ob Apps bestimmte Berechtigungen für ihre Funktion benötigen.
- Einzelne Berechtigungen von Apps entziehen.
- Alternative Apps nutzen, die weniger Berechtigungen benötigen.
- Falls verfügbar: Datenschutzmodus aktivieren!


05:58
100 %
Datenschutz
Standardmäßig aktiviert
Für neu installierte Apps standardmäßig aktivieren
Benachrichtigung anzeigen
/system/app mover
AdAway
AFWall+
Alarm Klock
Amaze
Anbieter für vertrauenswürdi..


06:00
100 %
Apps
Deaktiviert
Android-Tastatur (AOSP)
332 KB
Deaktiviert
Browser
16,00 KB
Deaktiviert
E-Mail
368 KB
Deaktiviert
Kalender
216 KB
Deaktiviert
Musik
36,00 KB
Deaktiviert

Smartphones & Tablets

- Hardware („Super-Wanze“)
  - Mikrofon, Kamera, GPS, Bewegungssensor
- Betriebssystem: iOS & Windows Phone/Mobile
  - „Pest oder Cholera"
  - Apps nur aus einer Quelle (zentraler App-Store), häufig mit massiven Hürden für freie Software
  - Geschlossene Systeme, keine Gerätehoheit
  - Mehr Freiheit durch Jailbreak (Gefängnisausbruch)

Android

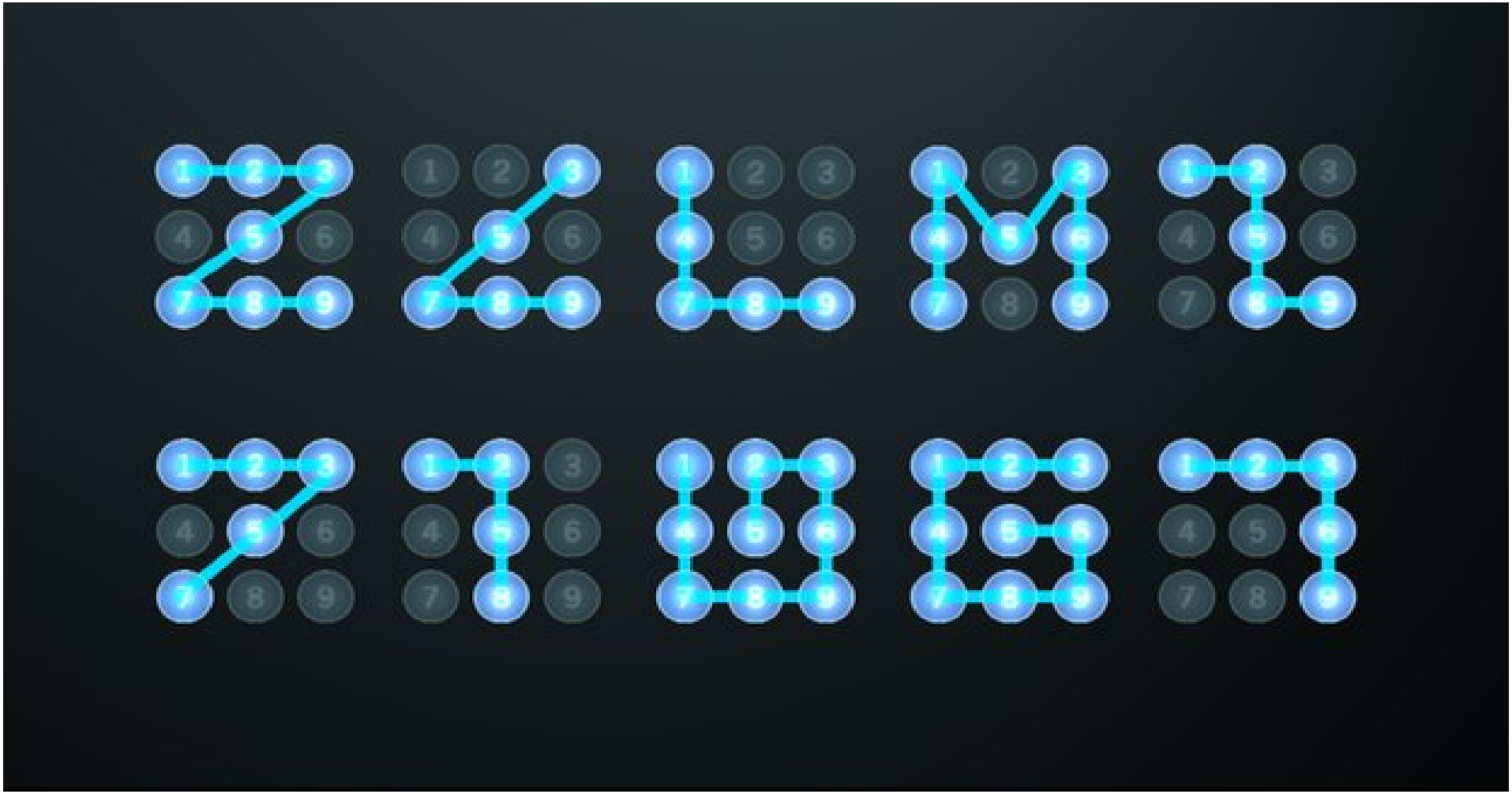
- Theoretisch gute Basis
  - Linux-basiert, Freie Software

- **Aber:** tiefe Integration proprietärer Google-Software
  - Suche, Browser, Gmail, Maps, Kalender- / Kontakte-Sync …
  - Play Store & Google-Dienste
  - Fernzugriff, Datenübermittlung
  - Standardmäßig keine Gerätehoheit (Root-Zugriff)
  - Je nach Hersteller - wenn überhaupt - oft nur zwei Jahre lang Sicherheitsupdates

Erste Schritte: Konfiguration

- Sichere Bildschirmsperre
  - von unsicher zu sicherer:
    Wischgeste, Muster, Biometrisch, PIN, Passwort
- Speicher verschlüsseln
- WLAN, GPS, Bluetooth, etc. ausschalten, wenn nicht genutzt
- Browser (Firefox) gegen Tracking schützen

Typische Wischgesten



Super sichere Iris-Scanner?

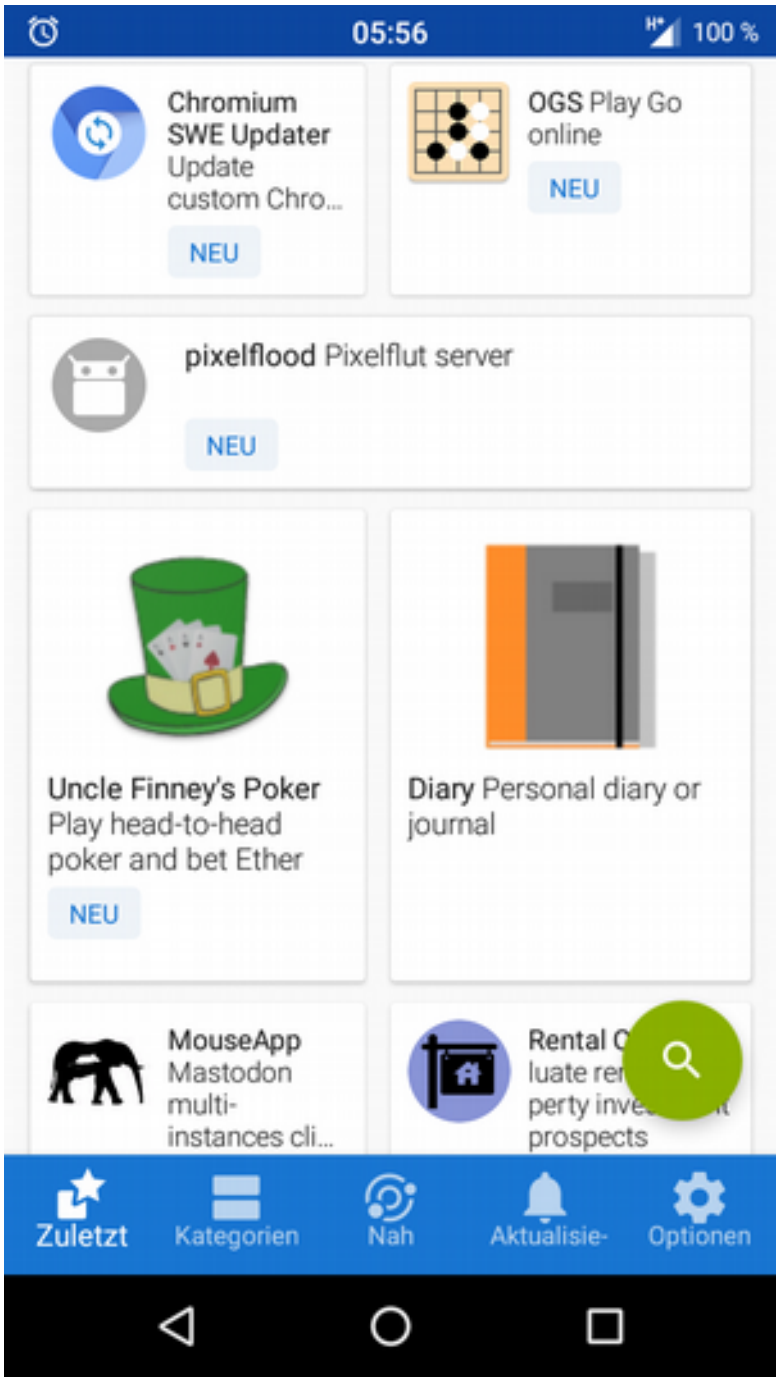
- https://media.ccc.de/v/biometrie-s8-iris-fun

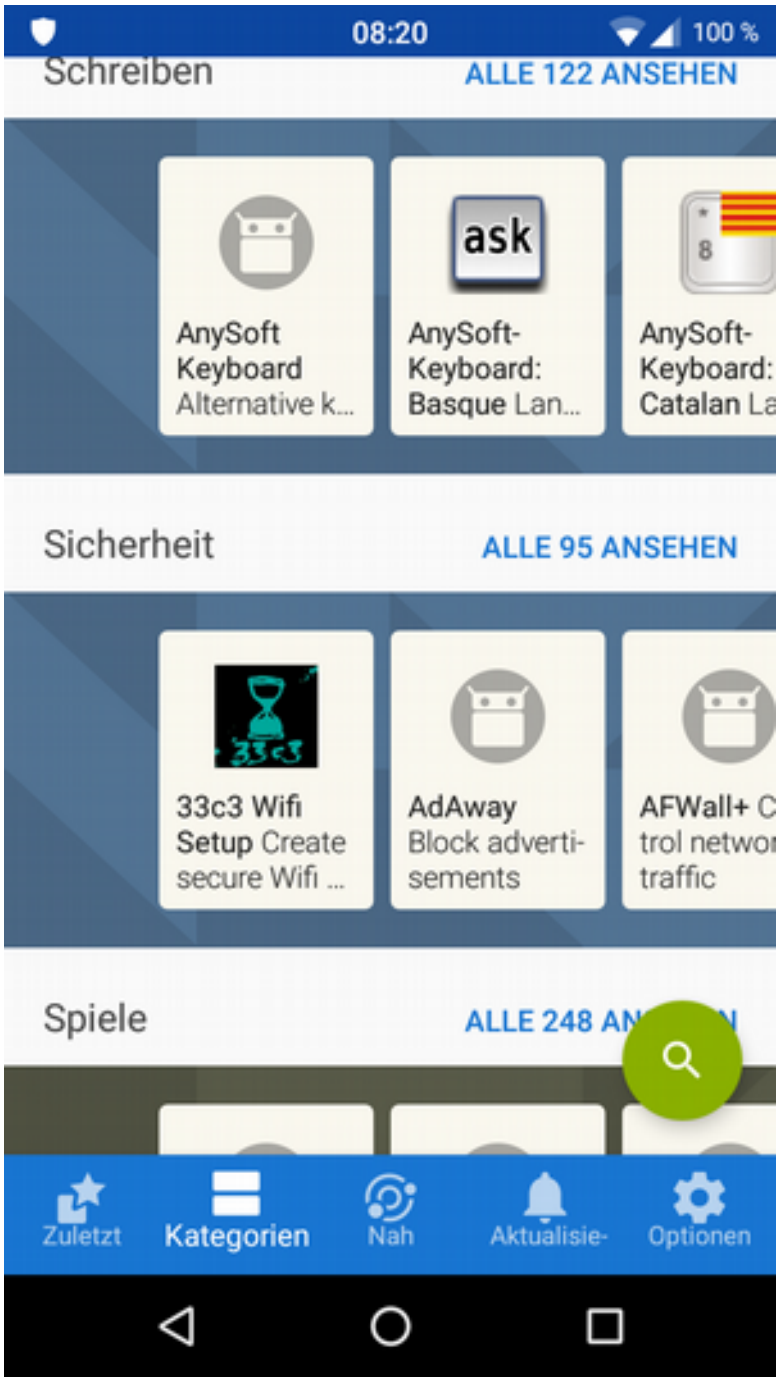
Android ‚entgoogeln‘

1. Unnötiges entfernen
   - Google-Einstellungen (G+, Standort, Suche, Werbe-ID, usw.)
2. Alternativ-Dienste nutzen
   - Browser, Suche, Mail, Sync für Kalender / Kontakte...
3. Play Store löschen / F-Droid nutzen
   - App-Alternativen nutzen
4. Freie Android-Variante installieren
   - z.B. LineageOS, Replicant

Empfehlenswerte Apps: F-Droid

- Alternative/Ergänzung zum Play Store: **F-Droid**
  - **https://f-droid.org/**
- Ausschließlich Software/Apps unter freier Lizenz
- Kein Nutzerkonto erforderlich
- Ergänzungen zum offiziellen F-Droid-Repository können von allen vorgeschlagen werden
- Es ist möglich, private Repositories zur Verfügung zu stellen und einzubinden
- Auch direkter Download von Apps über die Website möglich (dann keine automatischen Updates)


05:56
100 %
Chromium SWE Updater Update custom Chro...
NEU
OGS Play Go online
NEU
pixelflood Pixelflut server
NEU
Uncle Finney's Poker Play head-to-head poker and bet Ether
NEU
Diary Personal diary or journal
MouseApp Mastodon multi-instances cli...
prospects
Zuletzt
Kategorien
Nah
Aktualisie-
Optionen


08:20
100 %
Schreiben
ALLE 122 ANSEHEN
AnySoft Keyboard Alternative k...
AnySoft-Keyboard: Basque Lan...
AnySoft-Keyboard: Catalan La
Sicherheit
ALLE 95 ANSEHEN
33c3 Wifi Setup Create secure Wifi ...
AdAway Block adverti-sements
AFWall+ C trol networ traffic
Spiele
Zuletzt
Kategorien
Nah
Aktualisie-
Optionen

Ansprüche an Messenger

- Für alle gängigen Betriebsysteme verfügbar
- Ende-zu-Ende-Verschlüsselung
- Sicherer Verschlüsselungsalgorithmus (AES)
- Dezentralität / Möglichkeit für eigene Server
- Quelloffen (Überprüfung durch unabhängige Experten)
- Upload von Daten (z.B. Adressbuch) nur mit ausdrücklicher Bestätigung des Nutzers
  - Adressbuch enthält Daten anderer Personen → Upload erlaubt?
- Unabhängige Installation und Betrieb
  - z.B. ohne Google Play Store & Google-Dienste

Messenger-Vergleich

	Signal	Telegram	Surespot	Threema	WhatsApp
Freie Software	ja	teils	ja	nein	nein
Ende-zu-Ende-Verschlüsselung	ja	(ja)	ja	(ja)	(ja)
unabhängiges Audit	ja	ja	nein	(ja)	nein
Adressbuch-Zugriff	ja	ja	nein	(nein)	(nein)
Nicknames (Pseudonyme)	nein	nein	ja	ja	nein
außerhalb Play-Store erhältlich	ja	ja	nein	ja	ja
funktioniert ohne Google-Dienste	ja	ja	nein	ja	nein
Verbreitung	mittel	weit	kaum	mittel	sehr weit

Empfehlenswerte Messenger

- **Conversations** (Android) bzw.

  ChatSecure (iOS)

  - Nutzen das offene **XMPP** (Jabber) als Protokoll, das im Gegensatz zu anderen Messengern dezentrale Kommunikationsstrukturen erlaubt
  - Unterstützen verschlüsselte Chats via OpenPGP, OTR und OMEMO
  - Verfügbar via F-Droid (Conversations) bzw. App Store (ChatSecure)
  - Conversations auch im Play Store, allerdings nicht kostenlos

Alternative zu WhatsApp & Co

- **Signal** (Android, iOS)
  - Freie Software
  - Sicherer Verschlüsselungsalgorythmus
  - Unterstützt verschlüsselte Text- und Sprachnachrichten, Telefonie und SMS.
  - Kostenlos im Play bzw. App Store, für Android auch als APK:
    - https://signal.org/android/apk/
  - **Vorsicht:** Benötigt Zugriff aufs Telefonbuch, Telefonnummer zwingend erforderlich, zentrale Struktur

Empfehlenswerter Browser

- **Mozilla Firefox**
  - Freie Software
  - Auch unter Android und iOS durch Add-ons erweiterbar (uBlock Origin, NoScript, HTTPS Everywhere etc.)
  - Konfiguration ähnlich zur Desktop-Version

Empfehlenswerter E-Mail-Client

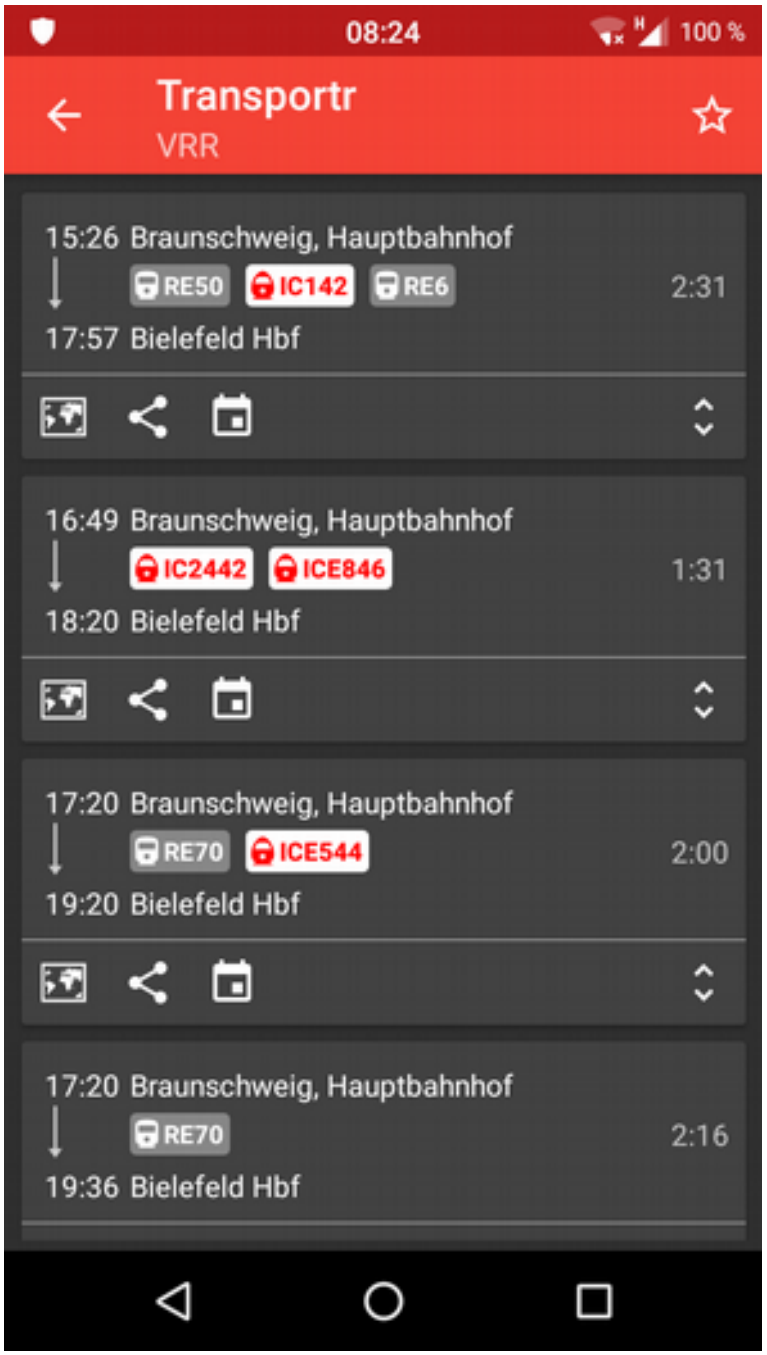
- **K-9 Mail**
  - sehr funktionaler und freier Mail-Client
  - unterstützt IMAP/POP3
  - kann verschlüsselte Mails via PGP/MIME senden und empfangen

- **OpenKeychain**
  - Implementierung von OpenPGP unter Android
  - agiert außerdem als Schlüsselverwaltung
  - Problem: private Schlüssel auf Mobilgerät zu gefährdet?

Weitere empfehlenswerte Apps

- **Transportr**
  - Fahrpläne des öffentlichen Nahverkehrs & Verbindungssuche
- **VLC**
  - Video- und Audioplayer
  - https://www.videolan.org/vlc/download-android.html
- **OsmAnd**
  - Karten- und Navigationssoftware auf Basis von OpenStreetMap
  - unterstützt auch Offline-Karten


08:20
100 %
Braunschweig
Platz am R
Schlossplat
Damm
Georg-Eckert-St
Bohlweg
Schloss
Fahrschein
Vorverkaufsstelle
50 m


08:24
100 %
Transportr
VRR
15:26 Braunschweig, Hauptbahnhof
RE50 IC142 RE6
2:31
17:57 Bielefeld Hbf
16:49 Braunschweig, Hauptbahnhof
IC2442 ICE846
1:31
18:20 Bielefeld Hbf
17:20 Braunschweig, Hauptbahnhof
RE70 ICE544
2:00
19:20 Bielefeld Hbf
17:20 Braunschweig, Hauptbahnhof
RE70
2:16
19:36 Bielefeld Hbf

Links & Literatur

- **PRISM Break zu Android & iOS**
  - https://prism-break.org/de/categories/android/
  - https://prism-break.org/de/categories/ios/
- **Mike Kuketz: Your phone Your data**
  - https://www.kuketz-blog.de/your-phone-your-data-teil1/
  - https://www.kuketz-blog.de/your-phone-your-data-light-android-unter-kontrolle/
- **Digitalcourage: Digitale Selbstverteidigung**
  - https://digitalcourage.de/digitale-selbstverteidigung/mobil

Weitere Projekte

PRISM Break: (https://prism-break.org/de/all/)
Liste datenschutzfreundlicher Software und Anbieter

- **Digitalcourage: Digitale Selbstverteidigung** (https://digitalcourage.de/digitale-selbstverteidigung)
  - Übersichtsflyer hier im Raum zum Mitnehmen!
- **Cryptopartys**
  - https://www.cryptoparty.in/

Lokale Anlaufstellen & Projekte

- **warpzone e.V. (Hackerspace)**
  - https://www.warpzone.ms/
- **Freifunk Münsterland**
  - https://freifunk-muensterland.de/
- **Cryptopartys in Münster**
  - https://www.cryptoparty.in/muenster
  - Vielleicht mal bei Interesse nachhaken, z.B. via Mail an cryptopartyms@systemli.org ;)

Vielen Dank
für die Aufmerksamkeit

Fragen?!