CryptoSeminar Bielefeld

Digitale Selbstverteidigung gegen Massenüberwachung

digitalcourage Hochschulgruppe

(Bild: CC-BY, Daniela Vladimirova)

Kurze Vorstellung

- Georg Gottleuber
- Sebastian Lisken
- Leif Rottmann
- Jan Schötteldreier

Digitalcourage e.V.

- Gemeinnütziger Verein für Datenschutz und Bürgerrechte
  - "Für eine lebenswerte Welt im digitalen Zeitalter"
  - Big Brother Awards
  - Aktionen zu aktuellen Themen

- Digitalcourage-Hochschulgruppe
  - CryptoPartys
  - Backup-Partys
  - Linux-Install-Partys
  - Regelmäßige Treffen an der Uni

CryptoParty

- Digitale Selbstverteidigung
- Schutz vor Massenüberwachung

- Öffentlich, nicht-kommerziell, weltweit

- https://cryptoparty.in

**Ich will nicht in einer Welt leben,
in der alles, was ich sage, alles was ich mache,
der Name jedes Gesprächspartners,
jeder Ausdruck von Kreativität,
Liebe oder Freundschaft aufgezeichnet wird.**

Edward Snowden

Agenda Freitag

von	bis	Titel
10:00	12:00	Vortrag: Privatsphäre im Zeitalter der Massenüberwachung
12:00	12:10	- Kurze Pause -
12:10	13:10	Digitale Selbstverteidigung I (W10, Passwörter)
13:10	14:00	- Mittagspause -
14:00	15:30	Digitale Selbstverteidigung II (Datenträgerverschlüsselung, Browser)
15:30	15:40	- Kurze Pause -
15:40	17:00	Praxis
		Open End

https://digitalcourage.de/hsg

Agenda Samstag

von	bis	Titel
10:00	11:00	Digitale Selbstverteidigung III (E-Mails)
11:00	11:15	- Kurze Pause -
11:15	13:00	Praxis
13:00	14:00	- Mittagspause -
14:00	15:00	Digitale Selbstverteidigung IV (Mobilgeräte)
15:00	15:15	- Kurze Pause -
15:15	17:00	Praxis
		Feedback, Diskussion / Open End

E-Mail-Verschlüsselung

Alternativen zu „kostenlosen“ E-Mail-Anbietern

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

Vorteile

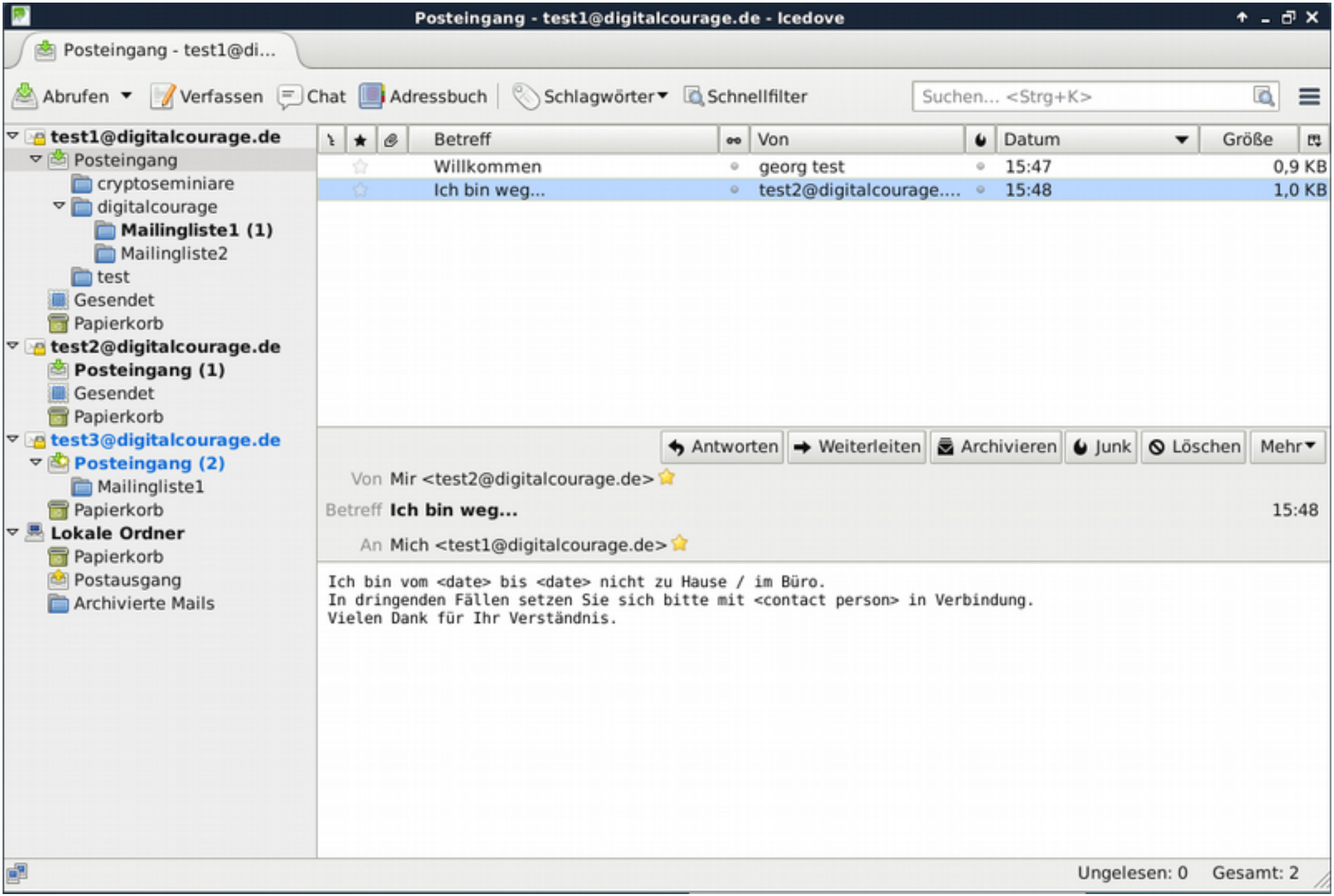
- Standort in Deutschland
- Datensparsamkeit
- Keine Inhaltsanalyse
- Keine Werbung
- Anonyme Nutzung möglich
- Datenschutz hat Priorität

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 / GnuPG)

Vorteile

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

Nachteile

- Metadaten (von, an, Betreff[2] etc). bleiben unverschlüsselt
  ([2] Enigmail ab 2.0 kann Betreff verschlüsseln)
- Absender & Empfängerin müssen PGP nutzen

Benötigte Software:

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

Verschlüsselung – was ist das eigentlich?

- Alice schreibt an Bob, Eve will mithören (eavesdrop) / Mallory (malicious) will manipulieren → man in the middle

- Beispiele und Grundprinzipien
  - meist gibt es ein **Verfahren** mit **Schlüssel**
  - Caesar-Verschlüsselung: einheitliche Verschiebung, 3 Positionen – wurde tatsächlich von Caesar und lange danach eingesetzt
  - ab 16. Jahrhundert komplexere Verfahren, noch im 1. Weltkrieg handschriftlich, 2. Weltkrieg Enigma – entscheidende Misserfolge
  - Vertrauen in moderne Kryprographie beruht darauf, dass das **Verfahren offen**, der **Schlüsselraum sehr groß** und als Angriff eigentlich **nur brute force** (alle Schlüssel probieren) bekannt ist

Unterschied symmetrische / asymmetrische Verschlüsselung

Symmetrische Verschlüsselung

- **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

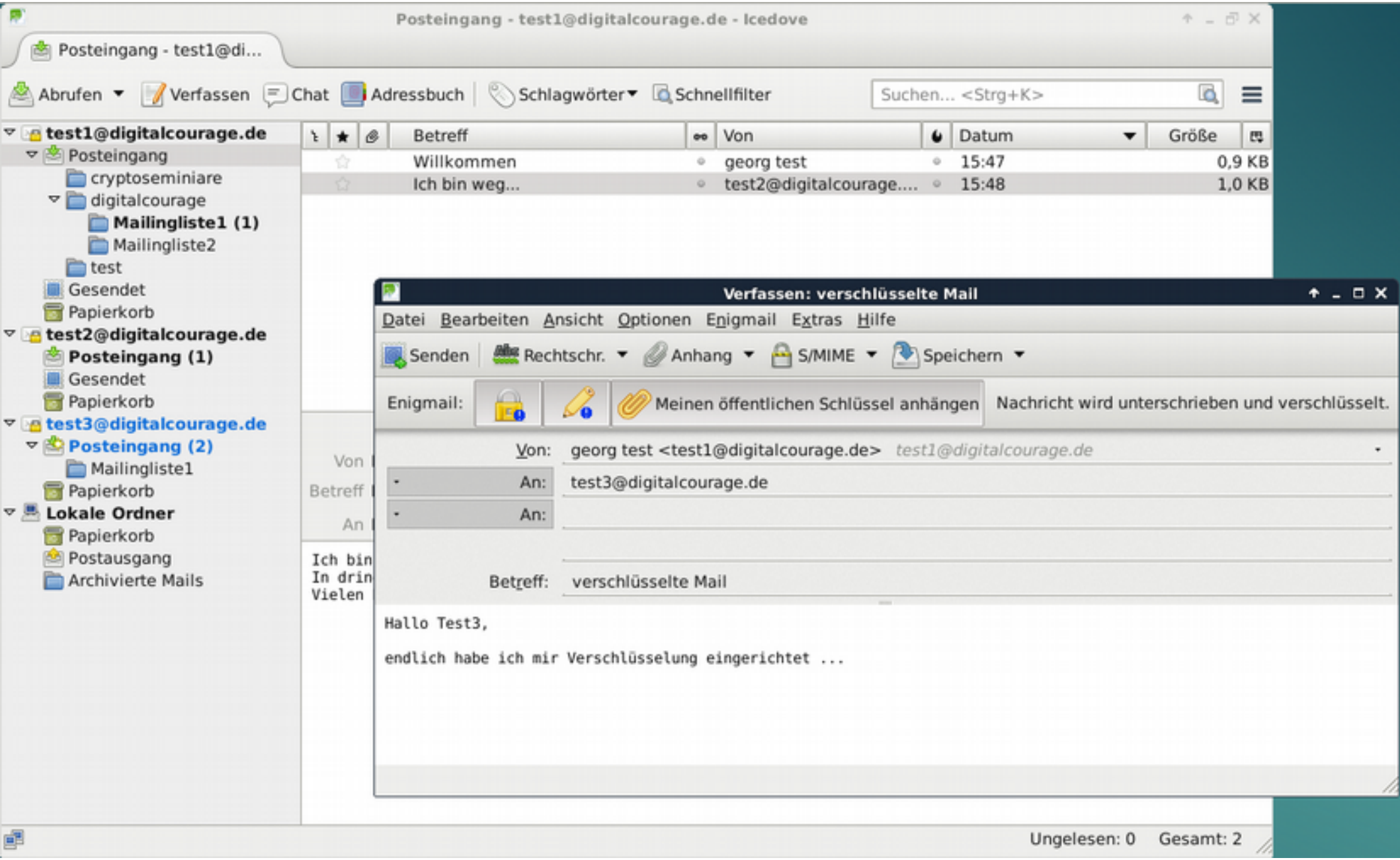
- Öffentlicher Schlüssel
  - kann und muss verteilt werden (an alle, über unsichere Kanäle)
- Privater Schlüssel
  - bleibt privat – gut schützen und sichern, niemals herausgeben!
- Zentrale Voraussetzungen
  - private Schlüssel können von niemand sonst benutzt werden
  - öffentliche Schlüssel sind unverfälscht und korrekt zugeordnet

E-Mails verschlüsseln und signieren

- Verschlüsseln
  - sichert Vertraulichkeit der Nachricht
  - verwendet den **öffentlichen Schlüssel des Empfängers**
    (nur der Empfänger kann mit privatem Schlüssel entschlüsseln)
- Signieren
  - sichert Unverfälschtheit der Nachricht und wer sie verfasste
  - nicht verwechseln mit Unterschrift und Fußzeile („Signatur“)
  - ein Fingerabdruck der Nachricht wird verschlüsselt und angehängt
  - verwendet den **privaten Schlüssel der Absenderin**
    (niemand anders konnte diesen Schlüssel einsetzen)
- Verschlüsseln und Signieren sind unabhängig voneinander

öffentliche PGP-Schlüssel austauschen

- E-Mail-Anhang
  - zur Verteilung im privaten Kreis
- Key-Server
  - bequem durchsuchbar
  - E-Mail-Adresse öffentlich einsehbar
- Habe ich den richtigen Schlüssel bekommen?
  - komplexes Thema → Schlüssel signieren, „Web of Trust“
  - pragmatische Lösung: Schlüssel auf mehreren Wegen finden (z.B. von persönlicher Website); Fingerprints austauschen und vergleichen (Visitenkarte, Telefon, Website, „Signatur“ unter Mails)

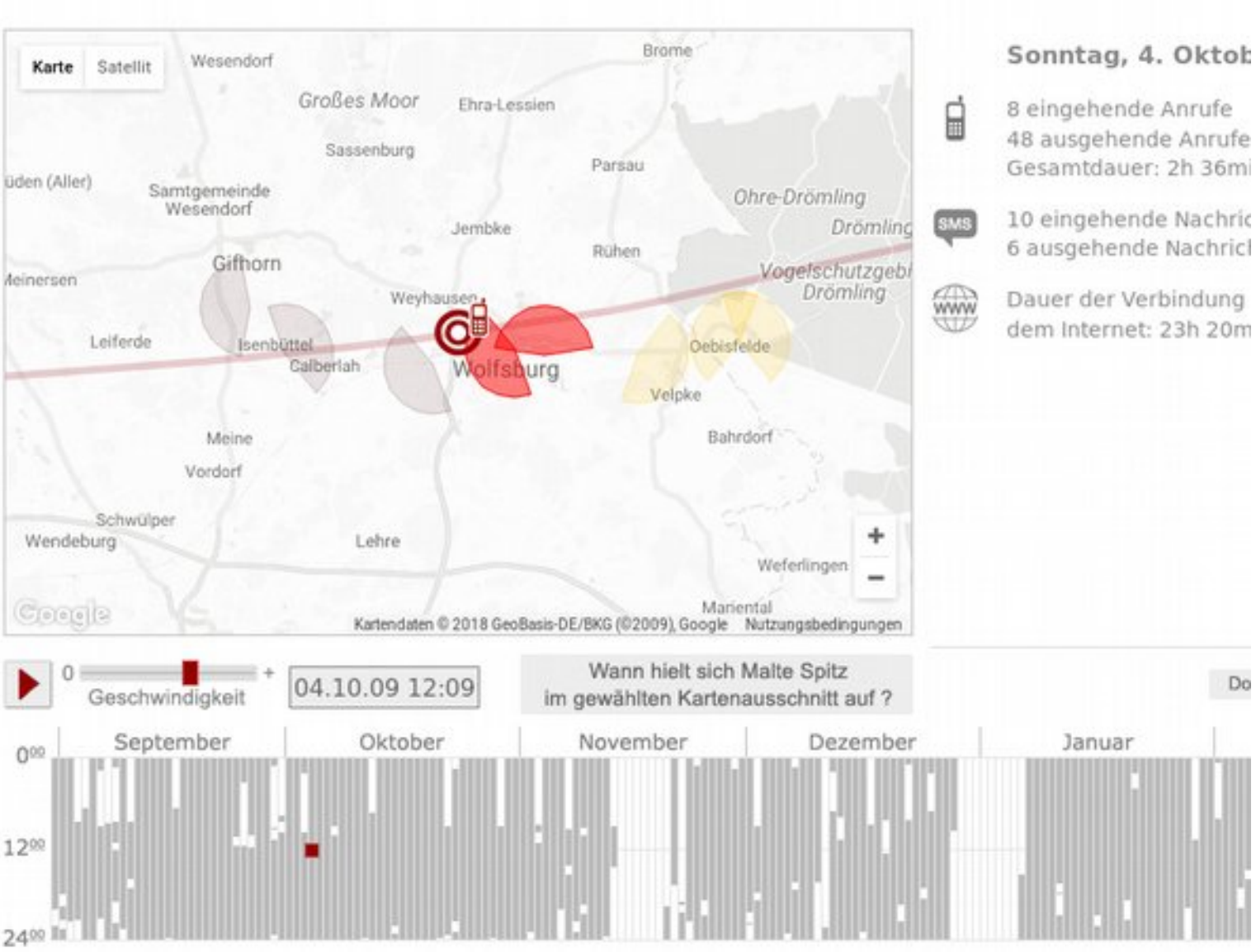

Posteingang - test1@digitalcourage.de - Icedove
Posteingang - test1@di...
Abrufen
Verfassen
Chat
Adressbuch
Schlagwörter
Schnellfilter
Suchen... <Strg+K>
test1@digitalcourage.de
Posteingang
cryptoseminiare
digitalcourage
Mailingliste1 (1)
Mailingliste2
test
Gesendet
Papierkorb
test2@digitalcourage.de
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

- Kurze Pause -

- Praxis -

Mobilgeräte

Verräterisches Telefon



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)

Smartphones & Tablets

- Hardware („Super-Wanze“)
  - Mikrofon, Kamera, GPS, Bewegungssensor
- Betriebssystem
  - iOS (Apple) oder Windows Phone/Mobile (Microsoft)
    = Pest oder Cholera
  - Apps nur aus einer Quelle (zentraler App-Store)
  - Geschlossene Systeme, keine Gerätehoheit
  - Mehr Freiheit durch Jailbreak (Gefängnisausbruch)

Android

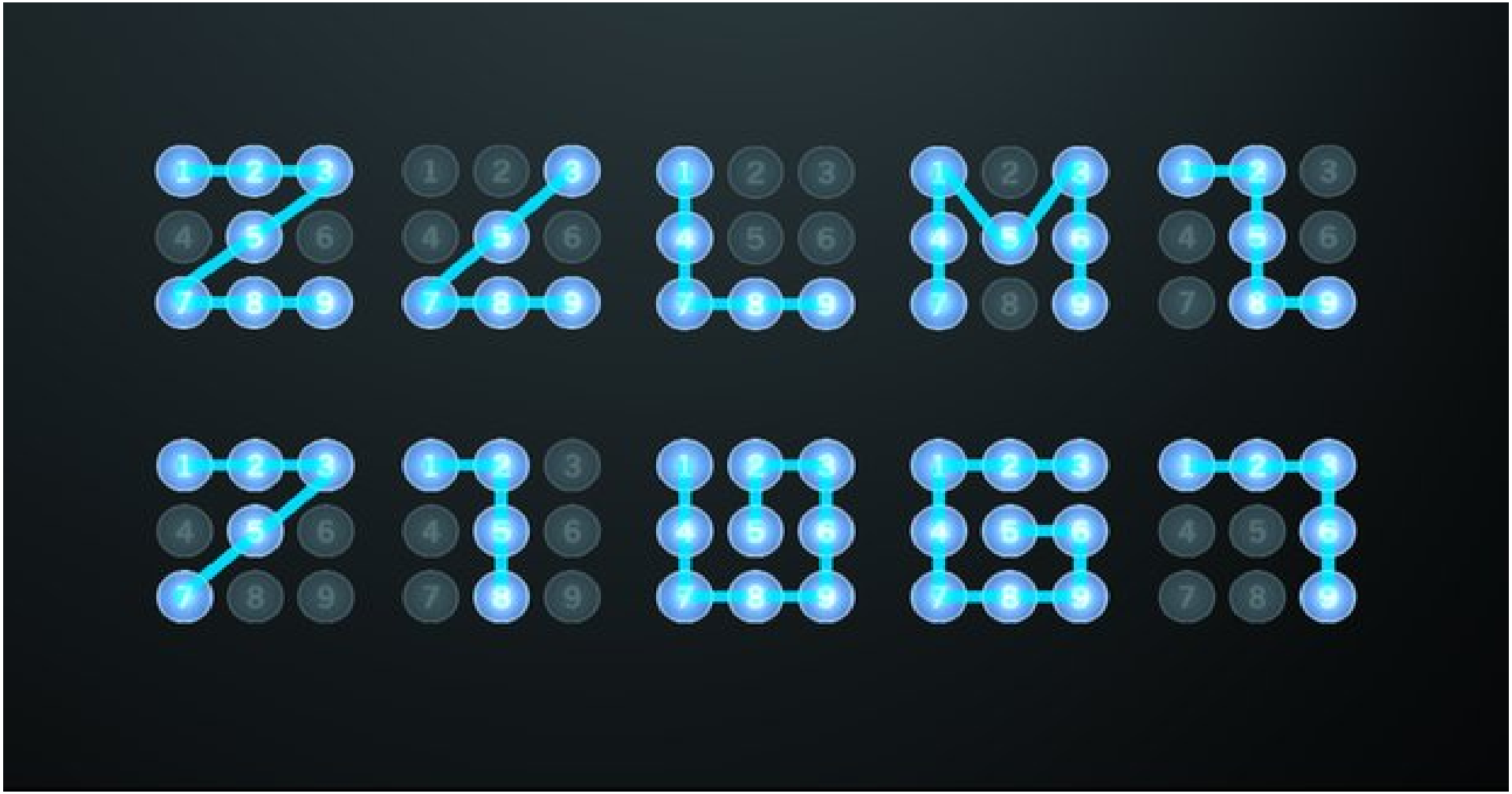
- Theoretisch gute Basis...
  - Linux-basiert, freie Software

- **Aber:** tiefe Integration proprietärer Google-Software
  - Suche, Browser, Gmail, Maps, Kalender- / Kontakte-Sync …
  - Play Store & Google-Dienste
  - Fernzugriff, Datenübermittlung
  - Standardmäßig keine Gerätehoheit
  - Je nach Hersteller 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?

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
  - Telefonstatus und Identität abrufen
- Anrufliste lesen
  - 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)

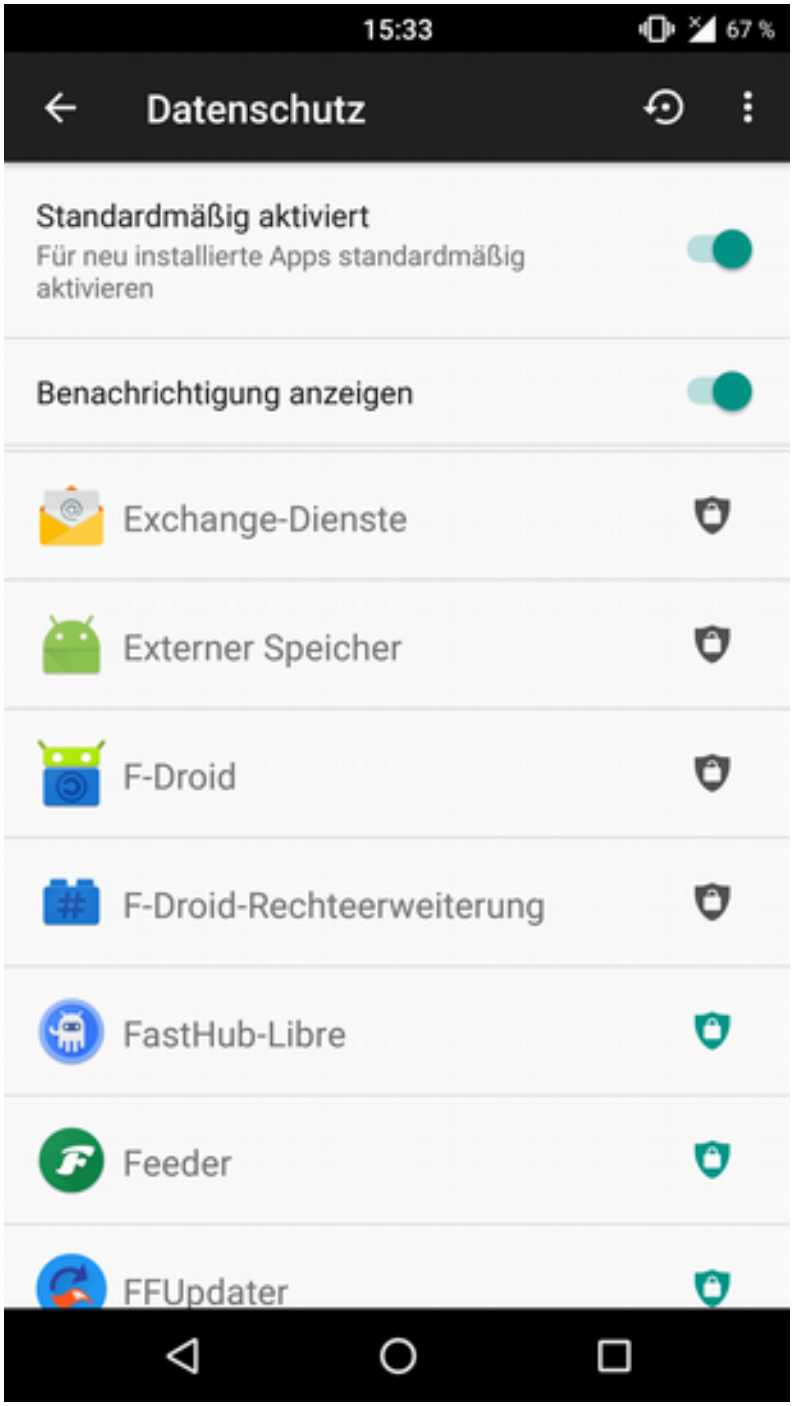
- Kamera
  - Bilder und Videos aufzeichnen
- Mikrofon
  - Ton aufzeichnen
- WLAN-Verbindungsinformationen
  - WLAN-Verbindungen abrufen
- Geräte-ID & Anrufinformationen
  - Telefonstatus und Identität

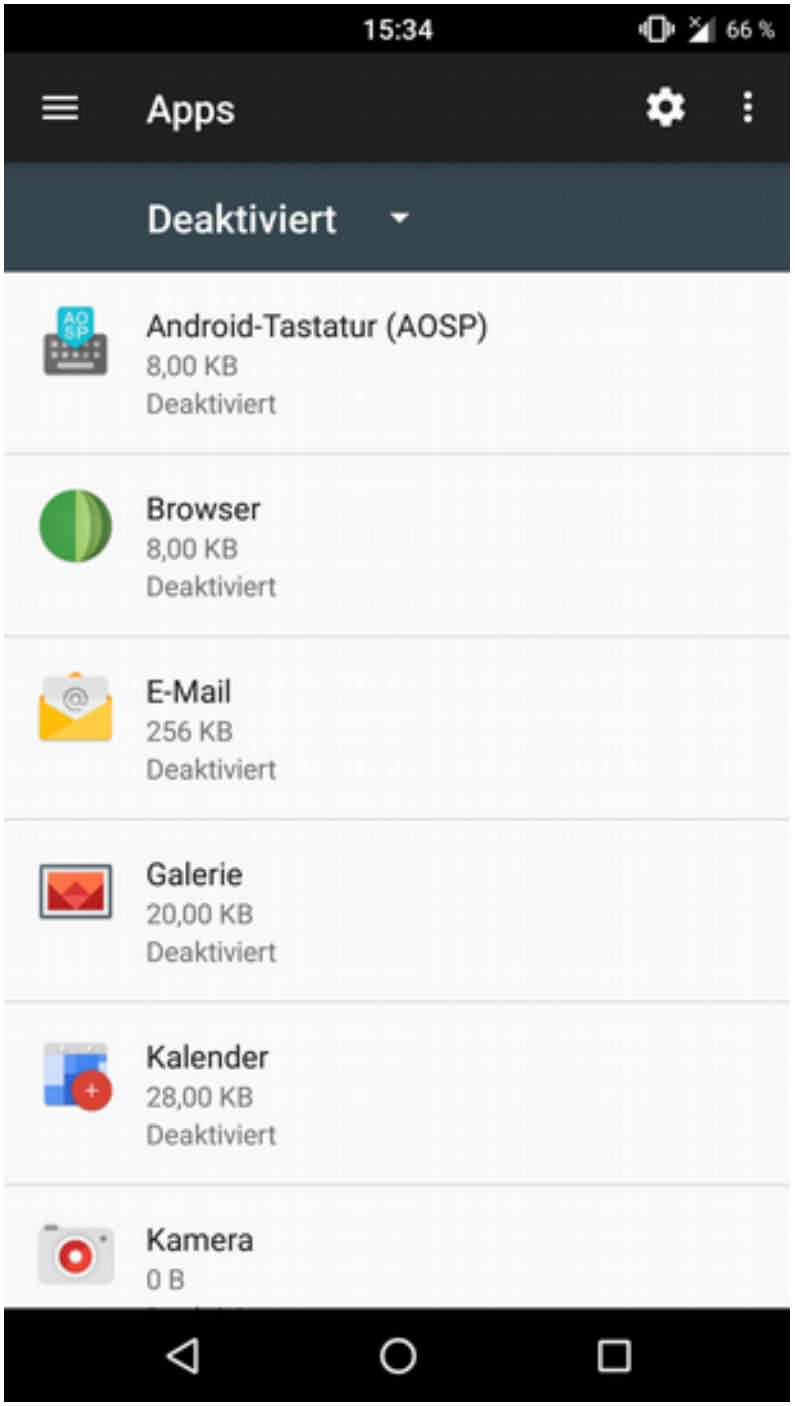
App-Berechtigungen: Facebook (4)

- 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 die immer 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!


15:33
67 %
Datenschutz
Standardmäßig aktiviert
Für neu installierte Apps standardmäßig aktivieren
Benachrichtigung anzeigen
Exchange-Dienste
Externer Speicher
F-Droid
F-Droid-Rechteerweiterung
FastHub-Libre
Feeder
FFUpdater

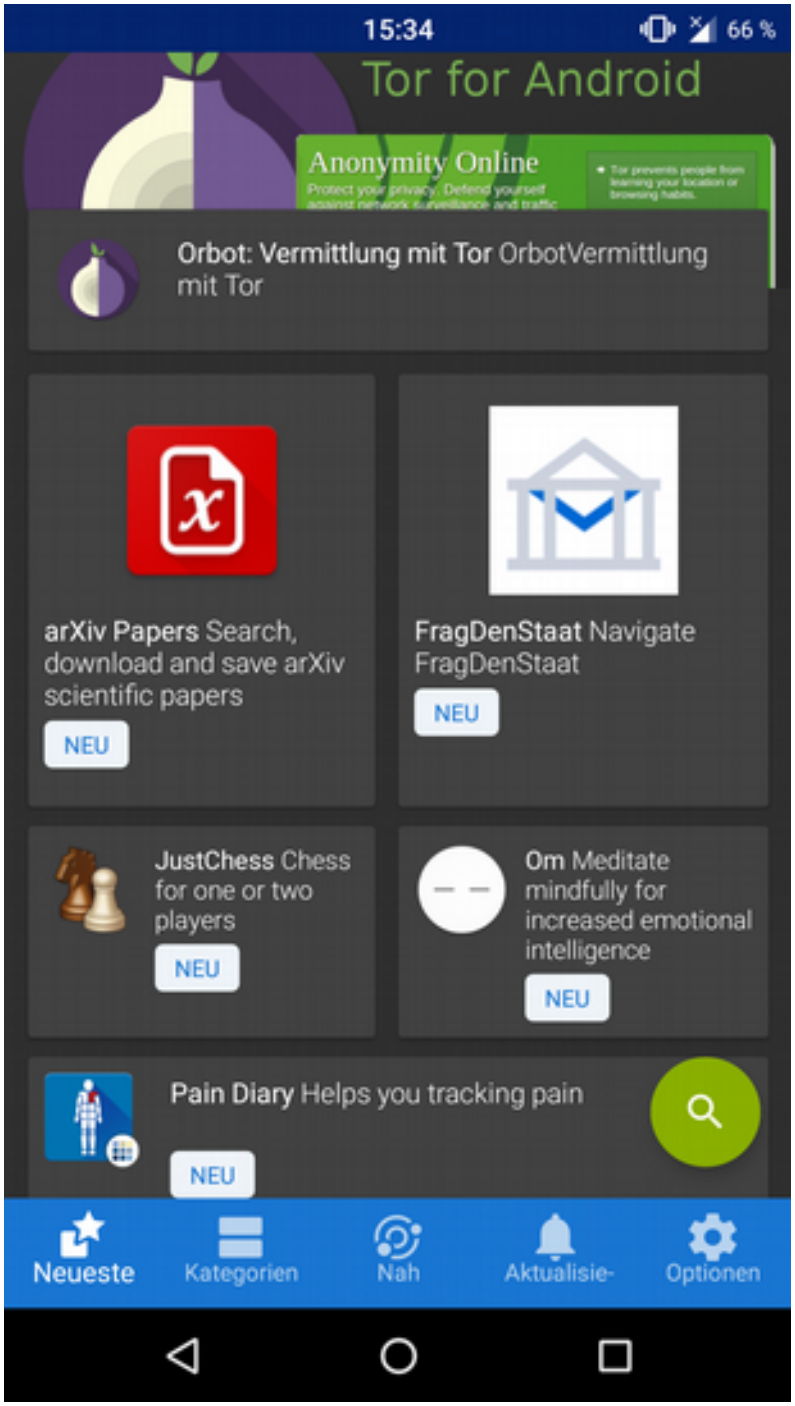

15:34
66 %
Apps
Deaktiviert
Android-Tastatur (AOSP)
8,00 KB
Deaktiviert
Browser
8,00 KB
Deaktiviert
E-Mail
256 KB
Deaktiviert
Galerie
20,00 KB
Deaktiviert
Kalender
28,00 KB
Deaktiviert
Kamera
0 B

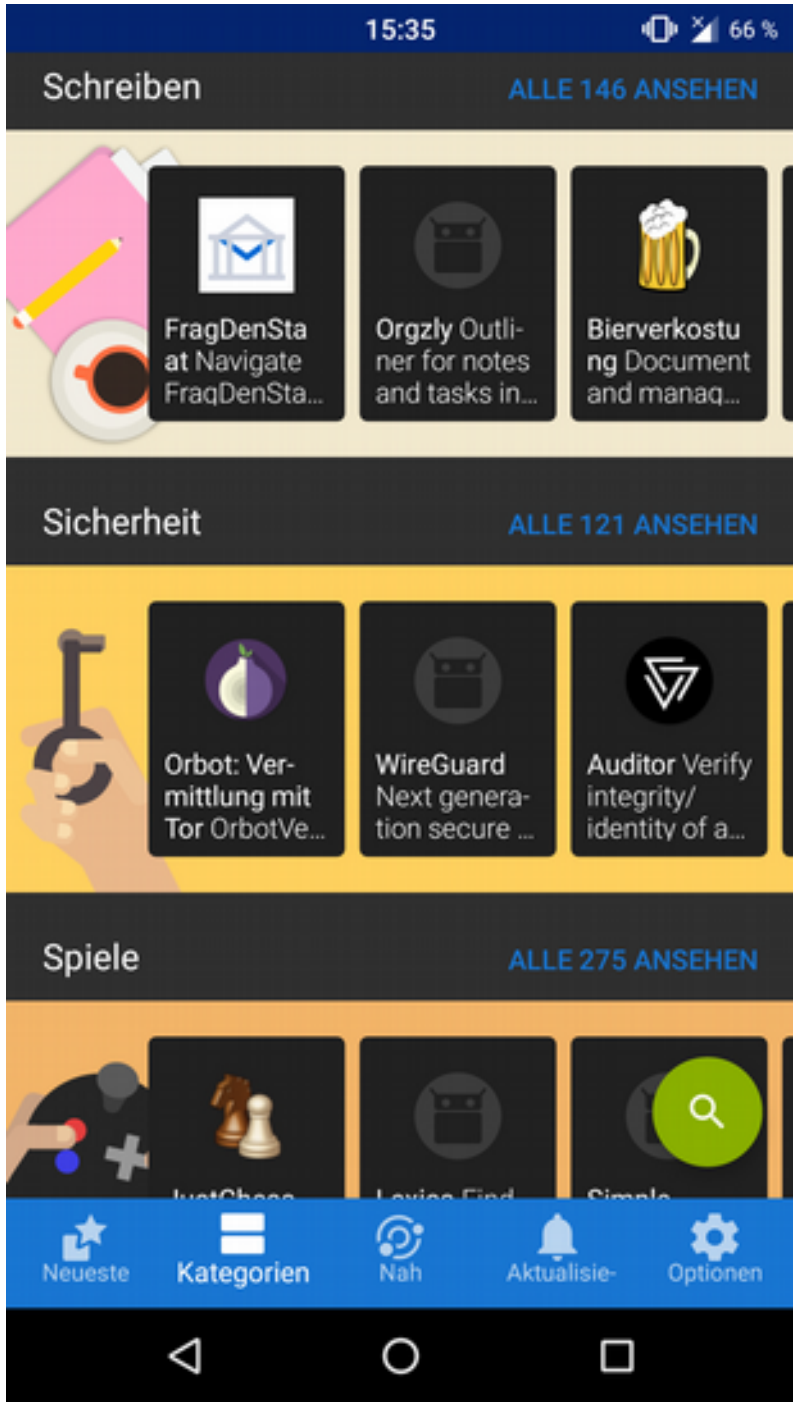
Android ‚entgoogeln‘

1. Apps und Dienste von Google deaktivieren/deinstallieren
   - 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)


15:34
66 %
Tor for Android
Anonymity Online
Orbot: Vermittlung mit Tor OrbotVermittlung mit Tor
arXiv Papers Search, download and save arXiv scientific papers
NEU
FragDenStaat Navigate FragDenStaat
NEU
JustChess Chess for one or two players
NEU
Om Meditate mindfully for increased emotional intelligence
NEU
Pain Diary Helps you tracking pain
NEU
Neueste
Kategorien
Nah
Aktualisie-
Optionen


15:35
66 %
Schreiben
ALLE 146 ANSEHEN
FragDenSta at Navigate FragDenSta...
Orgzly Outli- ner for notes and tasks in...
Bierverkostu ng Document and manag...
Sicherheit
ALLE 121 ANSEHEN
Orbot: Ver- mittlung mit Tor OrbotVe...
WireGuard Next genera- tion secure ...
Auditor Verify integrity/ identity of a...
Spiele
ALLE 275 ANSEHEN
Neueste
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 (Android

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

Empfehlenswerte Messenger

- **Conversations (Legacy)** (Android)

  bzw. ChatSecure (iOS)

  - Nutzen das offene Protokoll **XMPP** (Jabber), 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)
  - Als Conversations Legacy auch kostenlos im Play Store

Alternative zu WhatsApp & Co

- **Signal** (Android, iOS)

  - Freie Software
  - Sicherer Verschlüsselungsalgorythmus
  - Unterstützt verschlüsselte Text- und Sprachnachrichten, Telefonie und SMS.
  - Telefonnummer zwingend erforderlich, zentrale Struktur
  - Kostenlos im Play bzw. App Store, für Android auch als APK:
    - https://signal.org/android/apk/

Empfehlenswerter Browser

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

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**

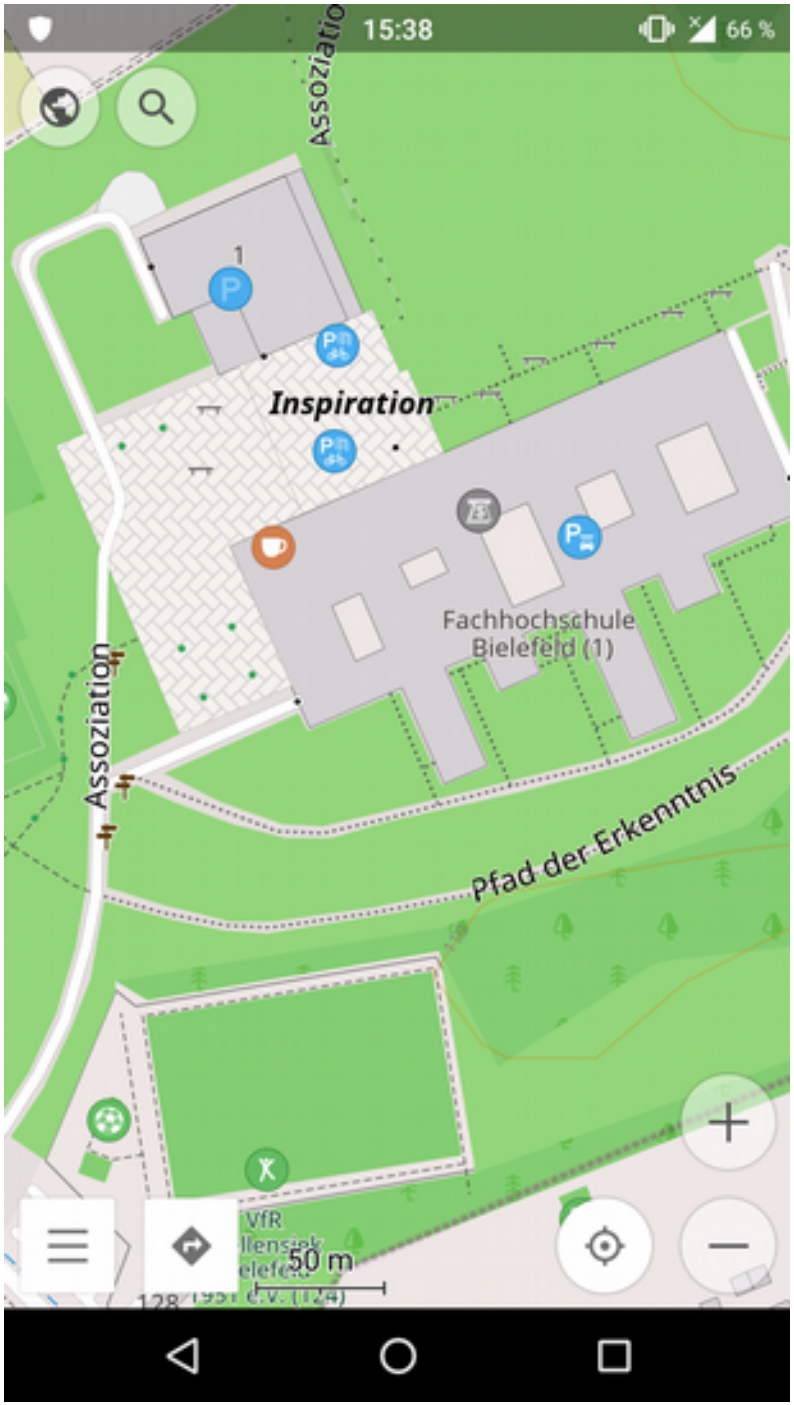
  - Implementierung von OpenPGP unter Android
  - agiert außerdem als Schlüsselverwaltung
  - Problem: private Schlüssel auf Mobilgerät zu gefährdet?

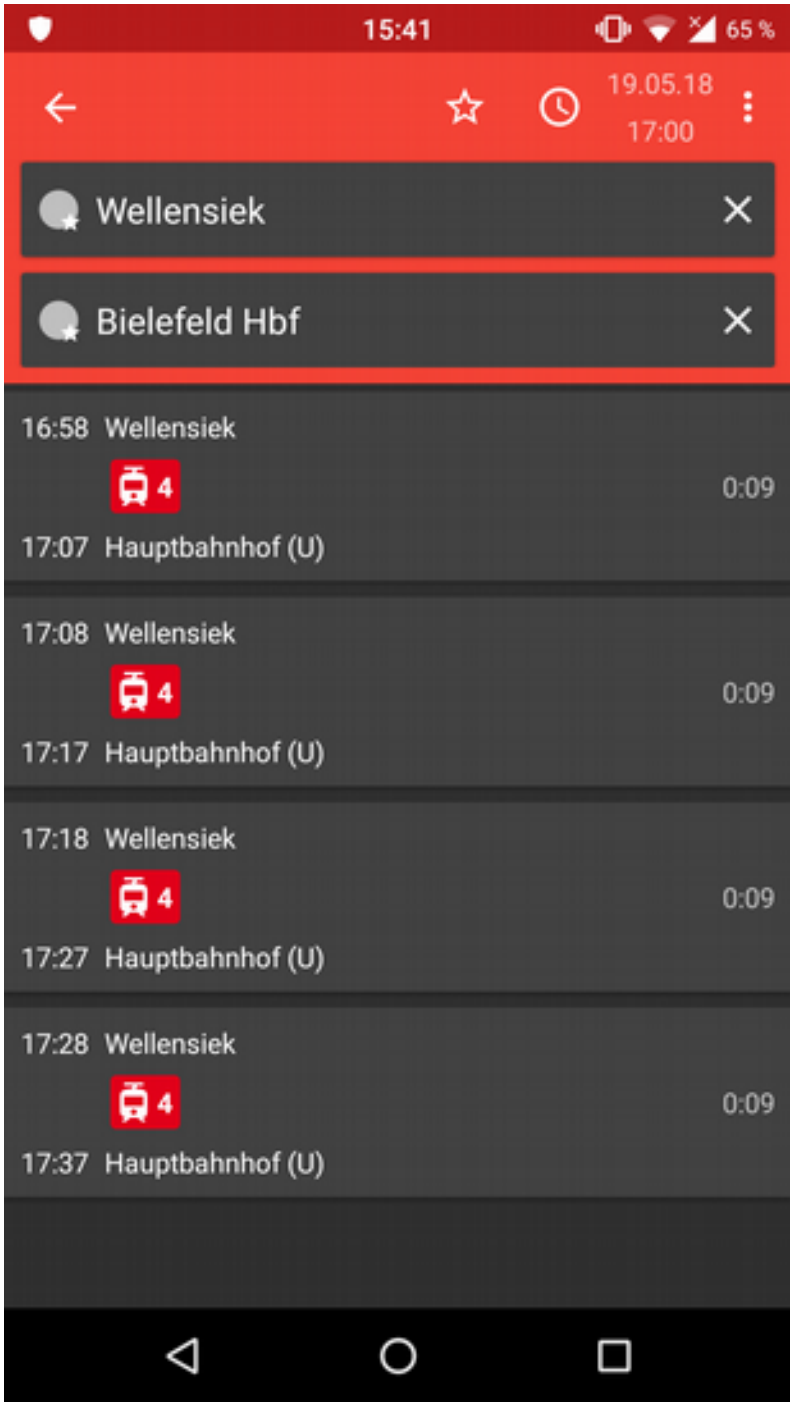
Weitere empfehlenswerte Apps

- **Transportr**
  - Fahrpläne des öffentlichen Nahverkehrs & Verbindungssuche

- **VLC**
  - Video- und Audioplayer

- **OsmAnd~**
  - Karten- und Navigationssoftware auf Basis von OpenStreetMap
  - unterstützt auch Offline-Karten


15:38
66 %
Assoziation
Inspiration
Fachhochschule
Bielefeld (1)
Assoziation
Pfad der Erkenntnis
50 m


15:41
65 %
19.05.18
17:00
Wellensiek
Bielefeld Hbf
16:58 Wellensiek
4
0:09
17:07 Hauptbahnhof (U)
17:08 Wellensiek
4
0:09
17:17 Hauptbahnhof (U)
17:18 Wellensiek
4
0:09
17:27 Hauptbahnhof (U)
17:28 Wellensiek
4
0:09
17:37 Hauptbahnhof (U)

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 (light) – Android unter Kontrolle

- 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)
  - Übersichts-Flyer hier im Raum zum Mitnehmen!
- **CryptoPartys weltweit!**
  - https://www.cryptoparty.in/ (auf Englisch)
- **Freifunk Bielefeld**
  - https://www.freifunk-bielefeld.de/

Anlaufstellen in Bielefeld

- **Digitalcourage e.V.**
  - Wöchentliches Kennenlerntreffen jeden Dienstag um 20 Uhr im Grec Tavernio (Niederwall 23).
  - https://digitalcourage.de/treffen-vor-ort

- **Digitalcourage-Hochschulgruppe**
  - Trifft sich jeden ersten und dritten Montag im Monat um 18 Uhr im SozCafé (X-C2-116)
  - https://digitalcourage.de/hsg

Vielen Dank
für die Aufmerksamkeit

Fragen?!

- Kurze Pause -

- Praxis -