
CRYPTO
PARTY

„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

Was ist eine CryptoParty?

- Workshop zur digitalen Selbstverteidigung
- Tupperware-Party gegen Massenüberwachung
- Einsteigerfreundlich
- Öffentlich & unkommerziell
- Fokus auf Freier Software
- Von Anwendern für Anwender → Gelerntes weitertragen

Agenda

- Inputvortrag zu:
  - Sichere Passwörter
  - Verschlüsselung von E-Mails (PGP)
  - Tracking beim Browsen vermeiden / Tor
  - 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 einer Liste ausprobieren
- Social Engineering
  - Phishing: Person austricksen, um PW zu erfahren

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!

- DBiR&dSd90M!
  - Merksatz: »**D**er **B**all **i**st **R**und **&** **d**as **S**piel **d**auert **90** **M**inuten**!**«
- HausLocherTasteMeloneBagger
  - Wortreihung – Wortlisten zum „Auswürfeln“ → *Diceware*
- 2UrN47oCfK6jAZ8xuKHiop4upPsI73
  - Passwortgenerator

Passwortverwaltung

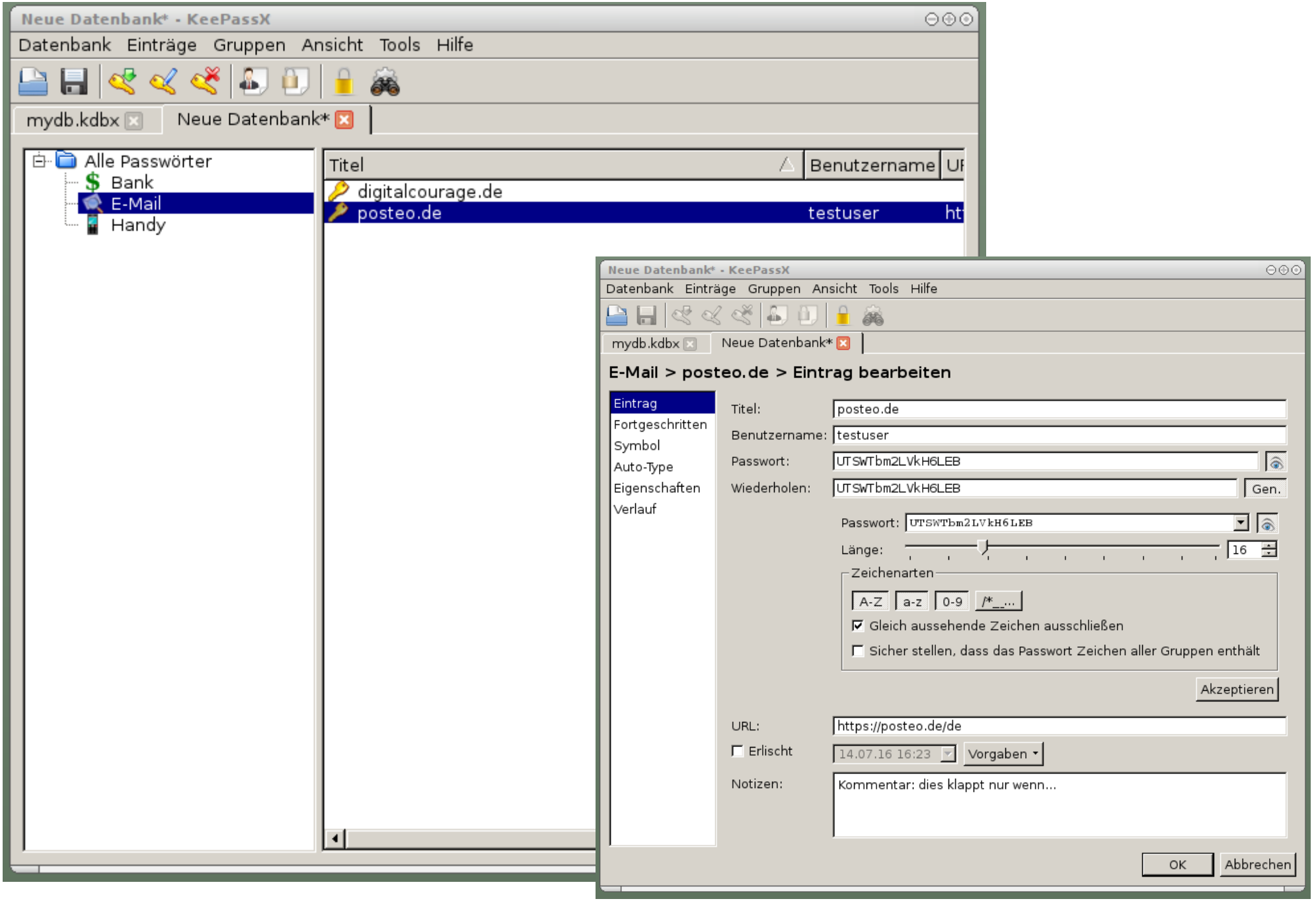
Software: **KeePassX**

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
Neue Datenbank* - KeePassX
Datenbank Einträge Gruppen Ansicht Tools Hilfe
mydb.kdbx
Neue Datenbank*
E-Mail > posteo.de > Eintrag bearbeiten
Eintrag
Fortgeschritten
Symbol
Auto-Type
Eigenschaften
Verlauf
Titel: posteo.de
Benutzername: testuser
Passwort: UTSWTbm2LVkH6LEB
Wiederholen: UTSWTbm2LVkH6LEB
Gen.
Passwort: UTSWTbm2LVkH6LEB
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

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

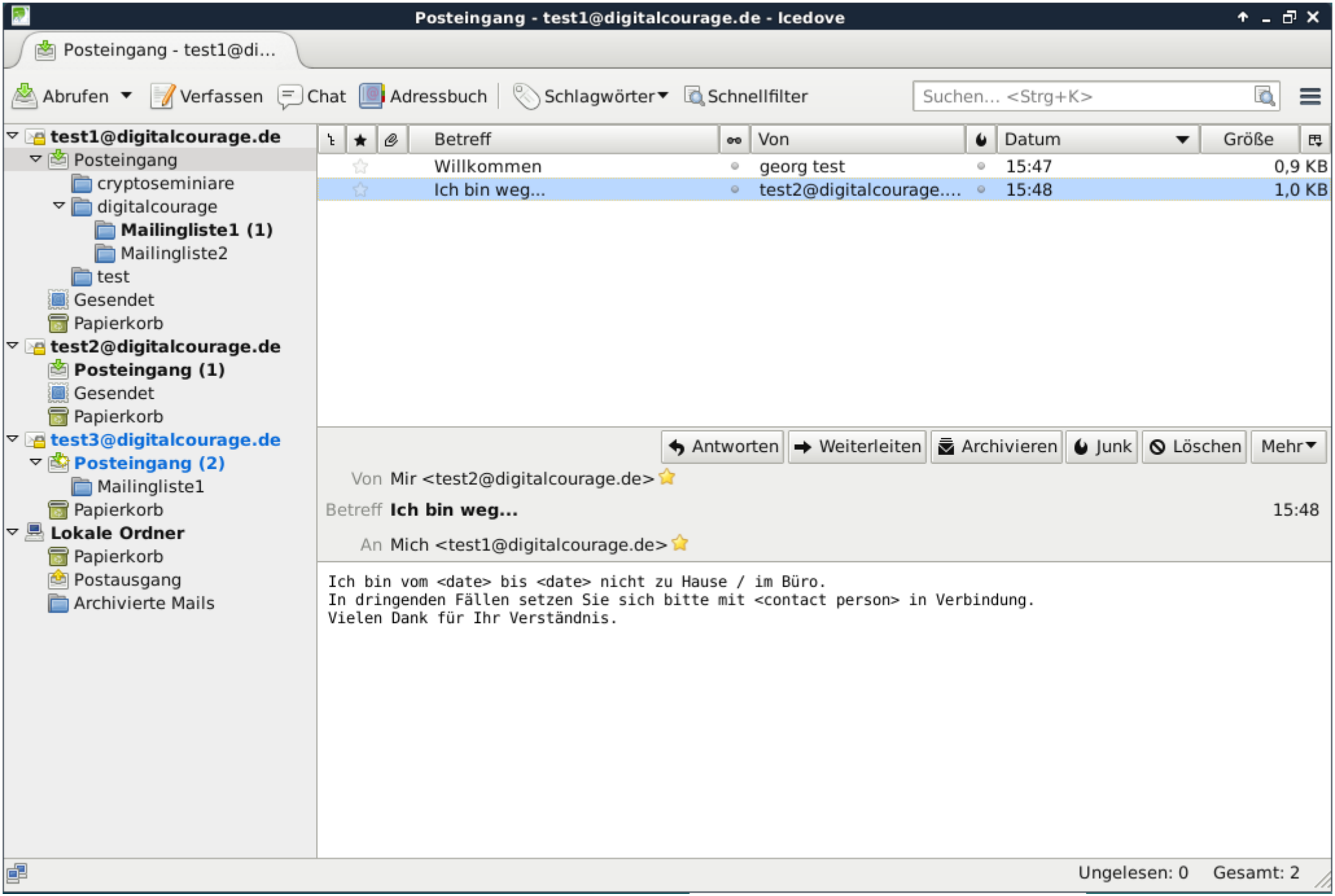
- Standort in Deutschland
- Datensparsamkeit
- Keine Inhaltsanalyse
- Keine Werbung
- Anonyme Nutzung möglich
- Datenschutz hat Priorität

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)

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

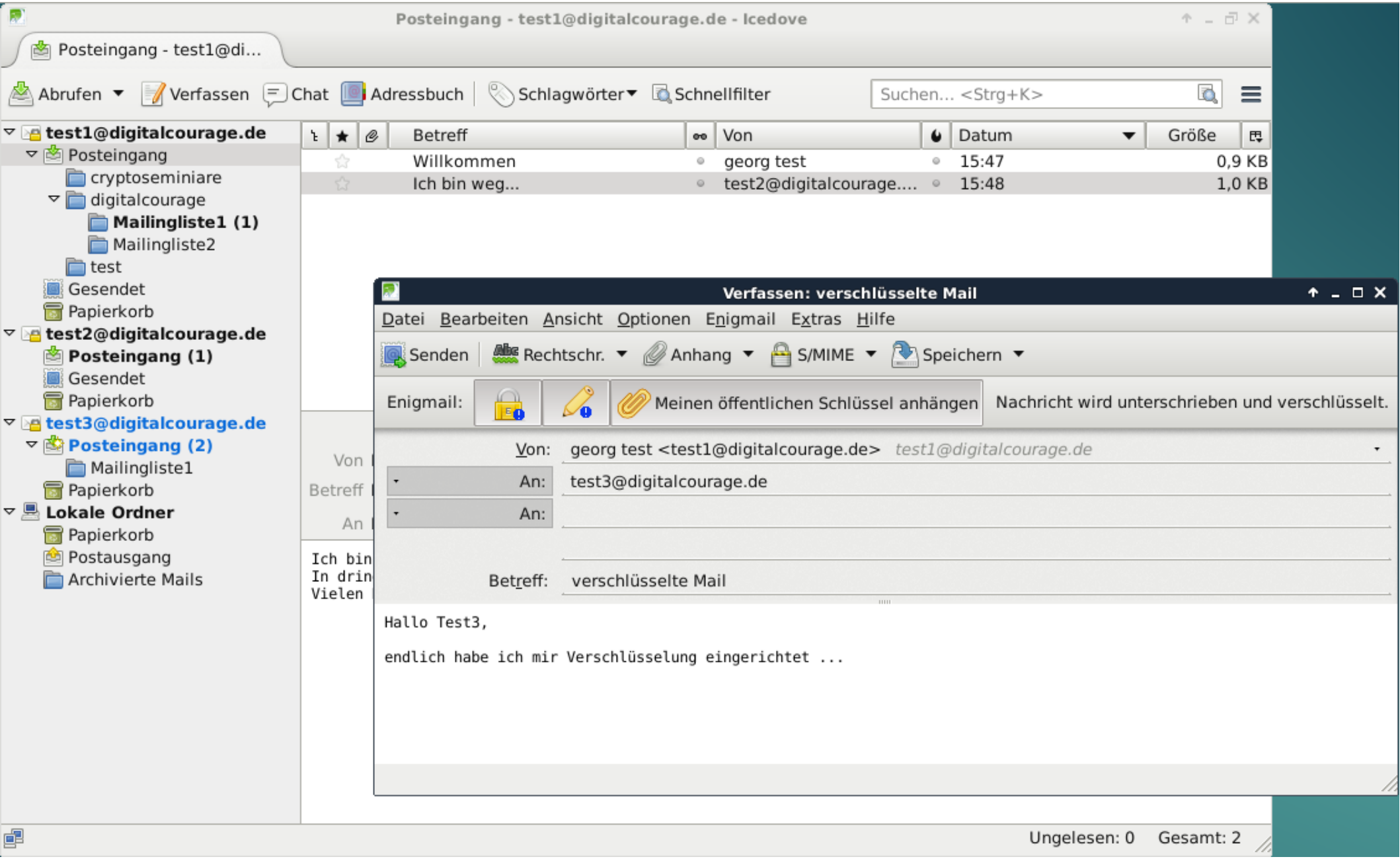
- Öffentlicher Schlüssel
  - kann und muss verteilt werden (an alle, über unsichere Kanäle)

- Privater Schlüssel
  - bleibt privat – gut schützen und sichern, niemals herausgeben!

- womit verschlüsseln?
  - Absender braucht **öffentlichen Schlüssel der Empfängerin** → nur Empfängerin kann entschlüsseln

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

Tracking beim Browsen vermeiden

&

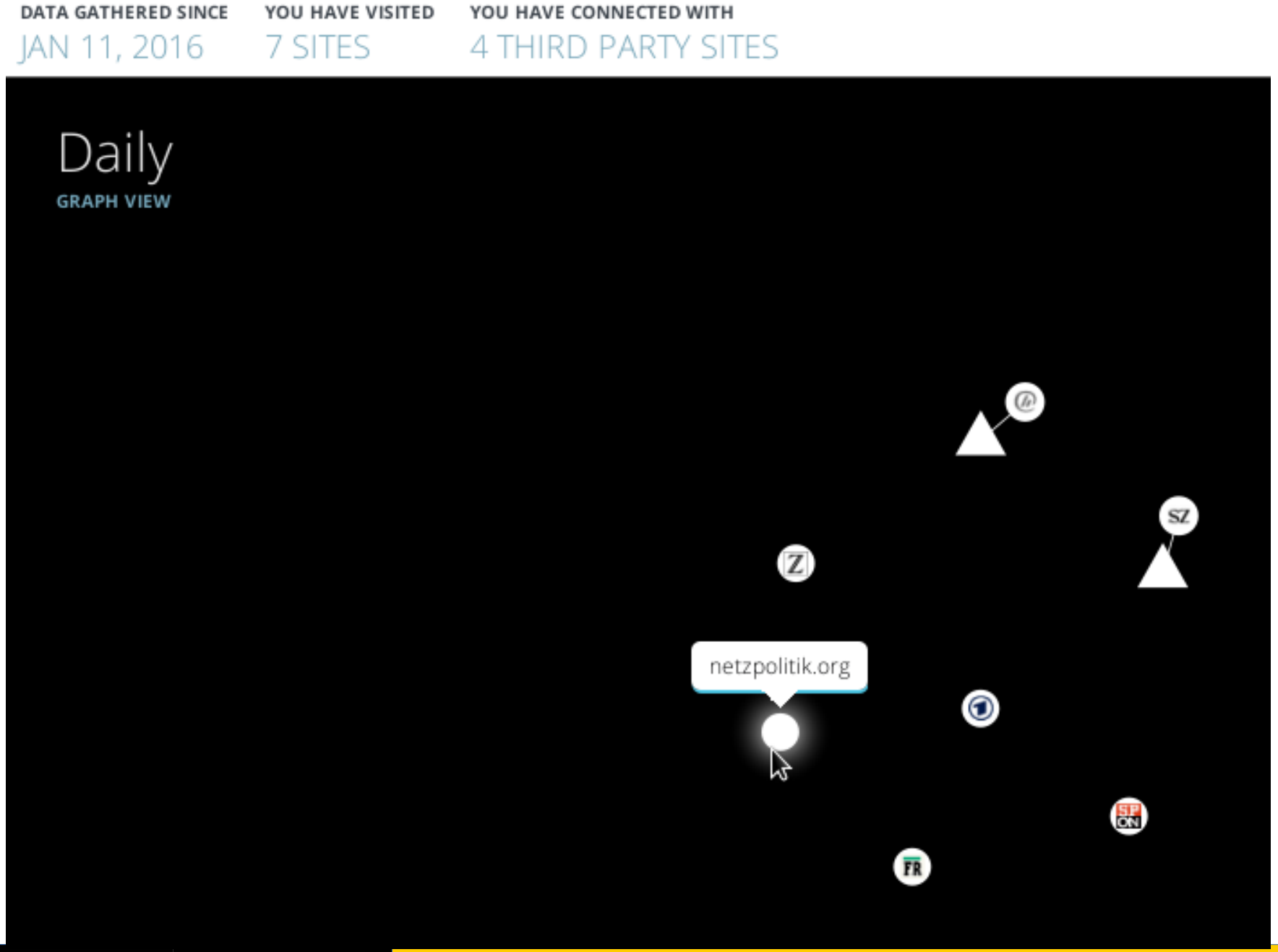
Tor

Datenschutzfreundliches Surfen mit Firefox

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

Analyse mit Firefox-Add-on Lightbeam

Analyse mit Firefox-Add-on Lightbeam



Wie kann ein Webserver mich identifizieren und verfolgen (Tracking)?

- Cookies:
  - kleine Textdateien, die die aufgerufene Webseite im Browser speichern und wieder abrufen kann.
- 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 Add-ons (Firefox)

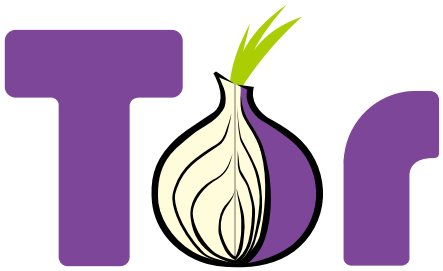
- Tracker und Werbung blocken: **uBlock origin**
- Verbesserung der Sicherheit **NoScript**
  - Skripte allgemein erlauben (laut Hersteller nicht empfohlen)
- Webseiten immer verschlüsseln: **HTTPS Everywhere**
- Flash-Cookies löschen: **BetterPrivacy**
  - **Besser**: Flash gar nicht benutzen

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

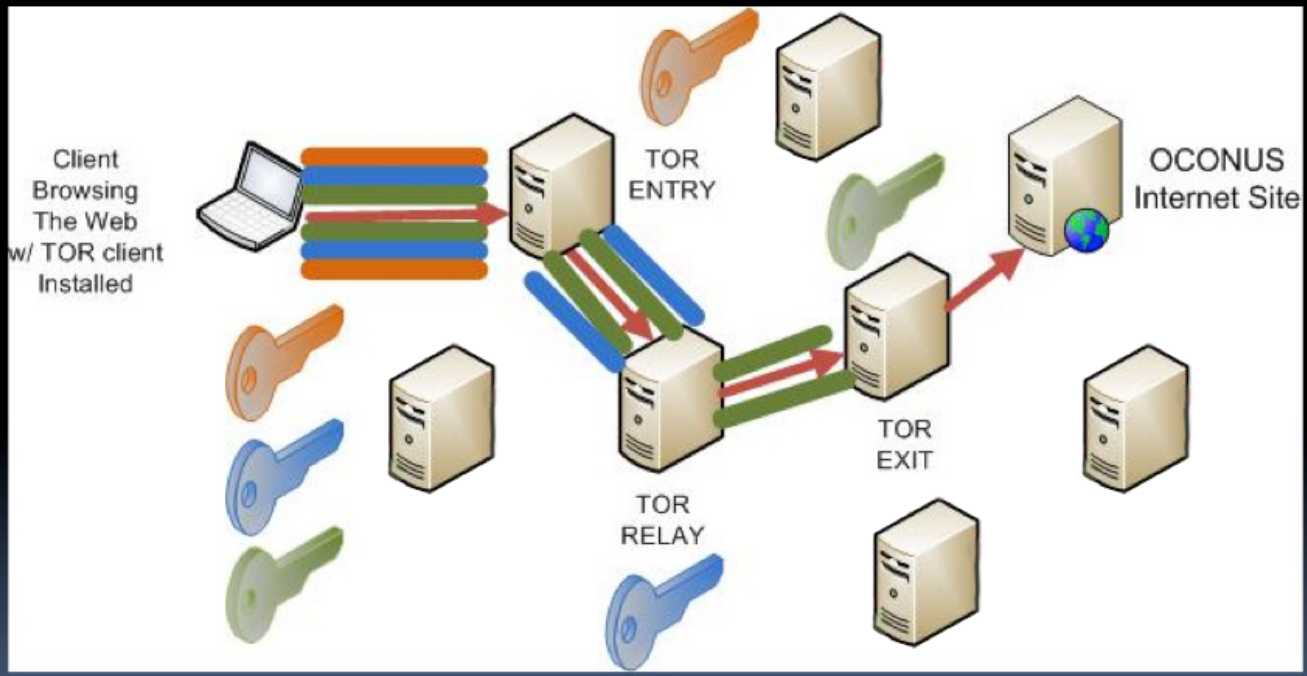
Vorteile

- 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

Software: **VeraCrypt**

- Software zur Datenverschlüsselung
- Quelloffen und auf allen gängigen Plattformen verfügbar

Was kann ich mit VeraCrypt machen?

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

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

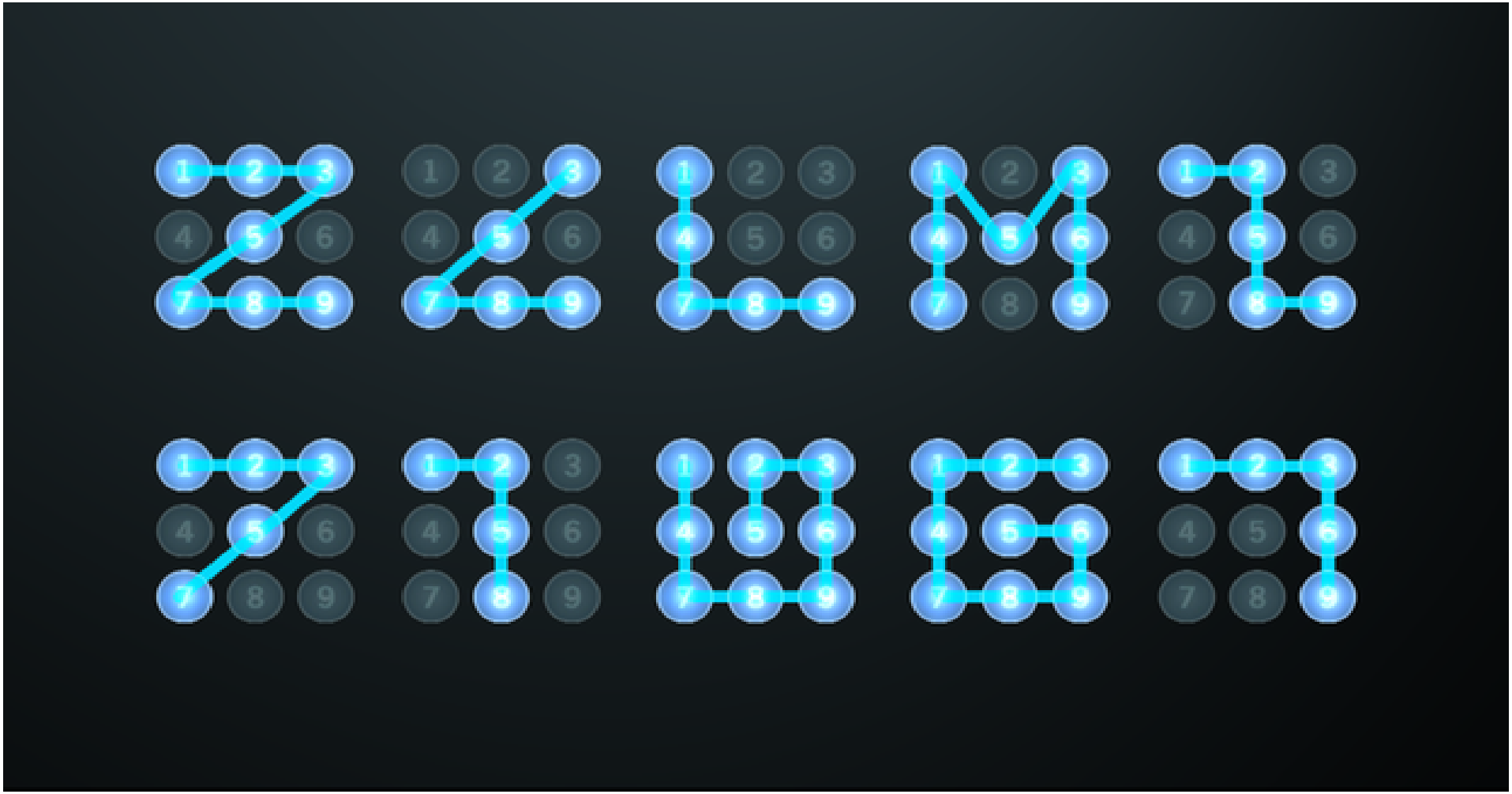
- Theoretisch gute Basis
  - Linux-basiert, Freie Software

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

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



Android ‚entgoogeln‘

1. Unnötiges entfernen
   - Google-Einstellungen (G+, Standort, Suche, Werbe-ID)
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. Replicant, LineageOS, CopperheadOS

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

Empfehlenswerte Apps

- 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)

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

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!

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
verzichtet auf Adressbuch-Zugriff	nein	nein	ja	(ja)	(ja)
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 als Protokoll, das im Gegensatz zu anderen Messengern dezentrale Kommunikationsstrukturen erlaubt
  - unterstützen verschlüsselte Chats via OpenPGP, OTR und OMEMO (nur Conversations)
  - verfügbar via F-Droid (Conversations) bzw. App Store (ChatSecure)

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**

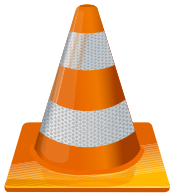
  - sehr funktionaler und freier Mail-Client
  - unterstützt IMAP/POP3
  - kann verschlüsselte Mails via PGP/MIME senden und empfangen

- **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

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

Weitere Projekte

- **PRISM Break:** (https://prism-break.org/de/all/)
  Liste datenschutzfreundlicher Software und Anbieter, z.B.:
  - *Startpage* und *DuckDuckGo* statt Google-Suche
  - *OpenStreetMap* statt Google Maps
  - *Dudle* statt doodle
  - *EtherCalc* und *EtherPad* statt Google Docs
  - *Diaspora** statt facebook oder Google+
  - …
- **Digitalcourage: Digitale Selbstverteidigung**
  (https://digitalcourage.de/digitale-selbstverteidigung)
  - Übersichts-Flyer hier im Raum zum Mitnehmen!

Kontakt & Termine

E-Mail: digitalcourage.hsg@uni-bielefeld.de
Key-ID: B1CB6584

Fingerprint: 2DD5 1926 5447 EB1C 78E1 8734 A279 303B B1CB 6584

Web: https://digitalcourage.de/hsg

Nächstes Treffen der HSG:

22. Mai, 18 Uhr im SozCafé (X-C2-116)

Linux-Install-Party am 1. Juni, 18 Uhr in U2-205