Crypto-Seminar Braunschweig

Digitale Selbstverteidigung gegen Massenüberwachung

(Bild: CC-BY, Daniela Vladimirova)

Kurze Vorstellung

- Fabian Kurz
- Georg Gottleuber
- Jan Schötteldreier
- Leif Rottmann

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
  - 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: Einführung, Warum überhaupt Verschlüsselung?
12:00	12:45	- Mittagspause -
12:45	14:00	Digitale Selbstverteidigung I (W10, Passwörter, E-Mail, Dateiverschlüsselung)
14:00	14:15	- Pause -
14:15	16:00	Praxisteil
		Open End

Agenda Samstag

von	bis	Titel
10:00	12:00	Digitale Selbstverteidung II (Browser, Mobilgeräte)
12:00	12:45	- Mittagspause -
12:45	14:00	Praxisteil
14:00	14:15	- Pause -
14:15	16:00	Feedback Praxis, Diskussion
		Open End

Einführung

- Welche Daten von mir werden gesammelt?
- Wer hat Interesse daran?
- Warum sind meine Daten schützenswert?

- Später:
  - Wie kann ich mich schützen?

Einführung

- Allgemeines
- Datenwirtschaft
- Netzpolitik

Persönlicher Bereich

Privatsphäre

- Analog
  - Privatsphäre selbstverständlich akzeptiert
  - Einbrüche in Privates meist erkennbar
  - Gesetze zum Schutz der Privatsphäre
    - Unverletzlichkeit der Wohnung
    - Briefgeheimnis
    - Freie Entfaltung der Persönlichkeit
- Digital
  - Neuer Wirtschaftsraum
  - Neue technische Mechanismen / Möglichkeiten
  - Intransparente Datenerhebung und -nutzung
  - Technisches Verständnis häufig notwendig
  - Datenschutzgesetze nicht zeitgemäß, #neuland

Digitale Identität

Google-Dienste

- Was für Dienste bietet Google an?

Google Suchmaschine

- Marktanteil weltweit ca. 90%
- Als Standard vorinstalliert
  - Chrome, Firefox
  - Android (Widget, Gboard Tastatur)
- Google Sprachsuche

Erfasste Daten

- Suchbegriffe (Search History)
  - eingegeben, gesehen, angeklickt
- IP-Adresse
- Sprache
- Datum, Uhrzeit
- Gerät, Betriebssystem, Browser
- Standort (GPS oder Browser)

  - https://myactivity.google.com/

Ich weiß, was du letzten Sommer gesucht hast!

Google

Folgen

- Sehr viel Wissen über die Nutzer
  - Interessen, Krankheiten, sexuelle Vorlieben, Bewegungsprofil...
- Zusammenführung von Daten verschiedener Quellen
  - Suche, YouTube, Gmail, Analytics, AdWords, Android...
- Individualisierung der Suchergebnisse (Filter-Bubble)
- Big Data
  - Suchtrends (regional, weltweit)
- Datenhandel
  - Werbung, Kreditwürdigkeit, Versicherungen..

Zu niemandem ist man ehrlicher als zum Suchfeld von Google.

Constanze Kurz, Chaos Computer Club

Bundesdatenschutzgesetz

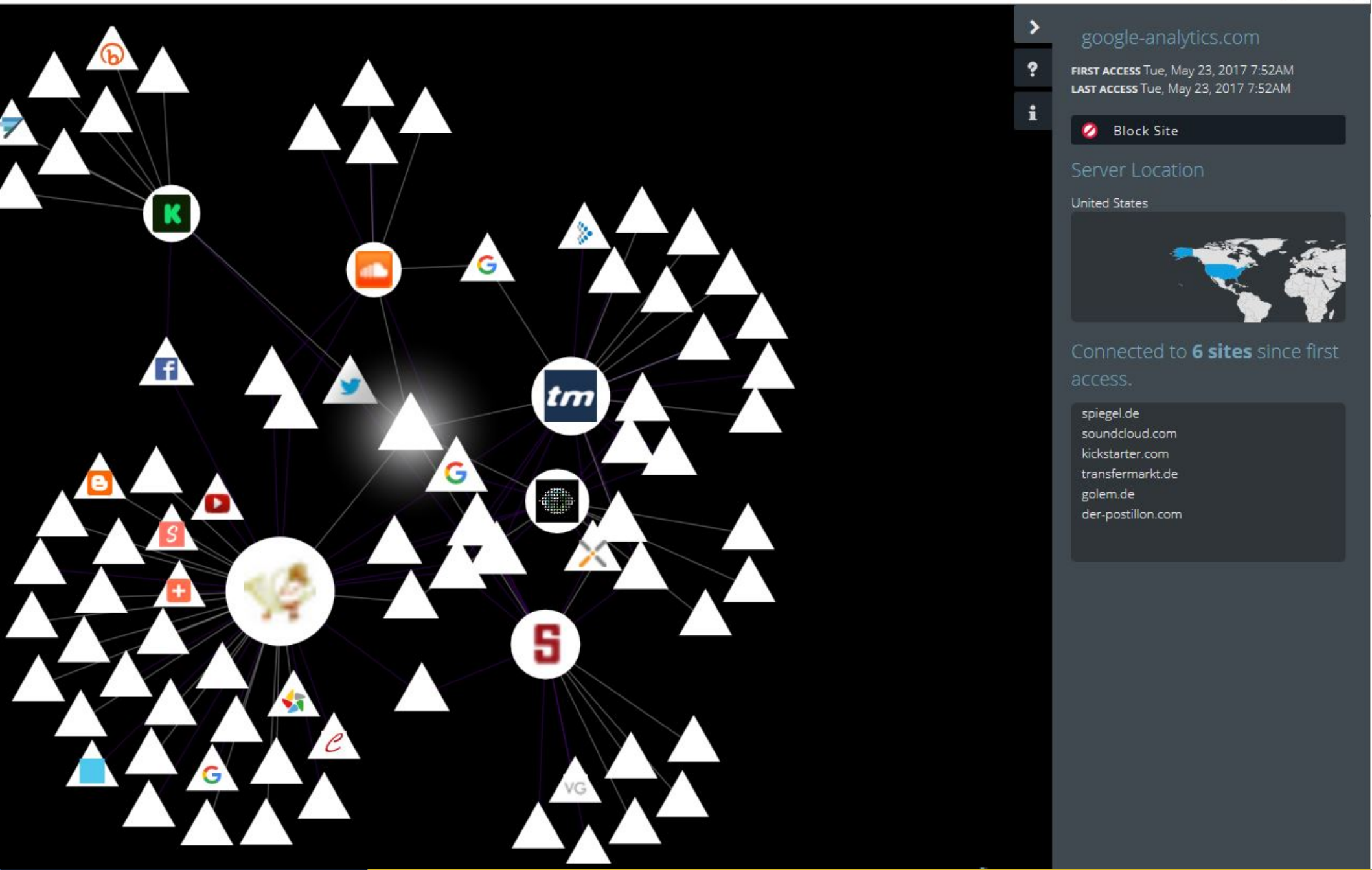
- Datensparsamkeit
  - So wenig personenbezogene Daten wie möglich erheben
- Zweckbindung
  - Personenbezogene Daten nur für vorher festgelegte und rechtmäßige Zwecke verwenden
- Informationelle Selbstbestimmung
  - Selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten bestimmen

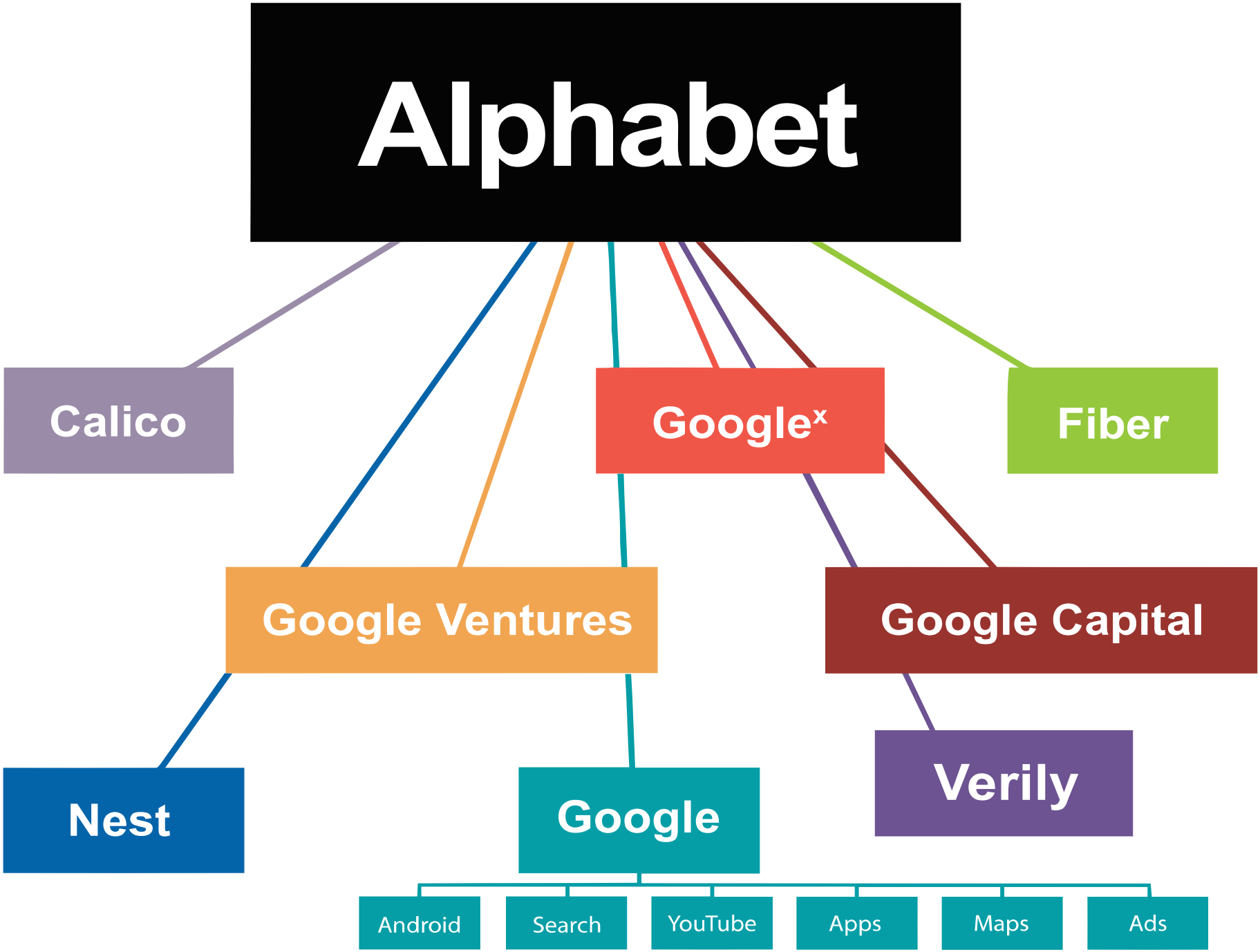
Google Analytics

- Einbindung auf der Webseite
- Statistiken für die Betreiber der Webseite
- Tracking der Besucher beim Seitenaufruf
  - IP-Adresse, Sprache, Land
  - Datum, Uhrzeit
  - Gerät, Betriebssystem, Browser
  - Bildschirmauflösung
  - Referer (von welcher Webseite gekommen)

Event Tracking

- Tracking der Interaktion mit der Webseite
  - Klick auf interne Links (Navigation, Teaser)
  - Klick auf externe Links
  - Interaktion mit Videos (zu wieviel % abgespielt)
  - Scrollverhalten
  - ...


TRACKING PROTECTION
OFF
google-analytics.com
FIRST ACCESS Tue, May 23, 2017 7:52AM
LAST ACCESS Tue, May 23, 2017 7:52AM
Block Site
Server Location
United States
Connected to 6 sites since first access.
spiegel.de
soundcloud.com
kickstarter.com
transfermarkt.de
golem.de
der-postillon.com


Alphabet
Calico
Google[x]
Fiber
Google Ventures
Google Capital
Nest
Google
Verily
Android
Search
YouTube
Apps
Maps
Ads

Facebook

- „Kostenlos“
- Datenschutzeinstellungen werden immer schwieriger
- Klarnamenpflicht
- Rechte an den Daten
- Intransparenz bei der Weitergabe
- Lock-In (kein Profil-Export)

Schön zusammengefasst von Alexander Lehmann (für X3)

- Video (https://vimeo.com/16203416)

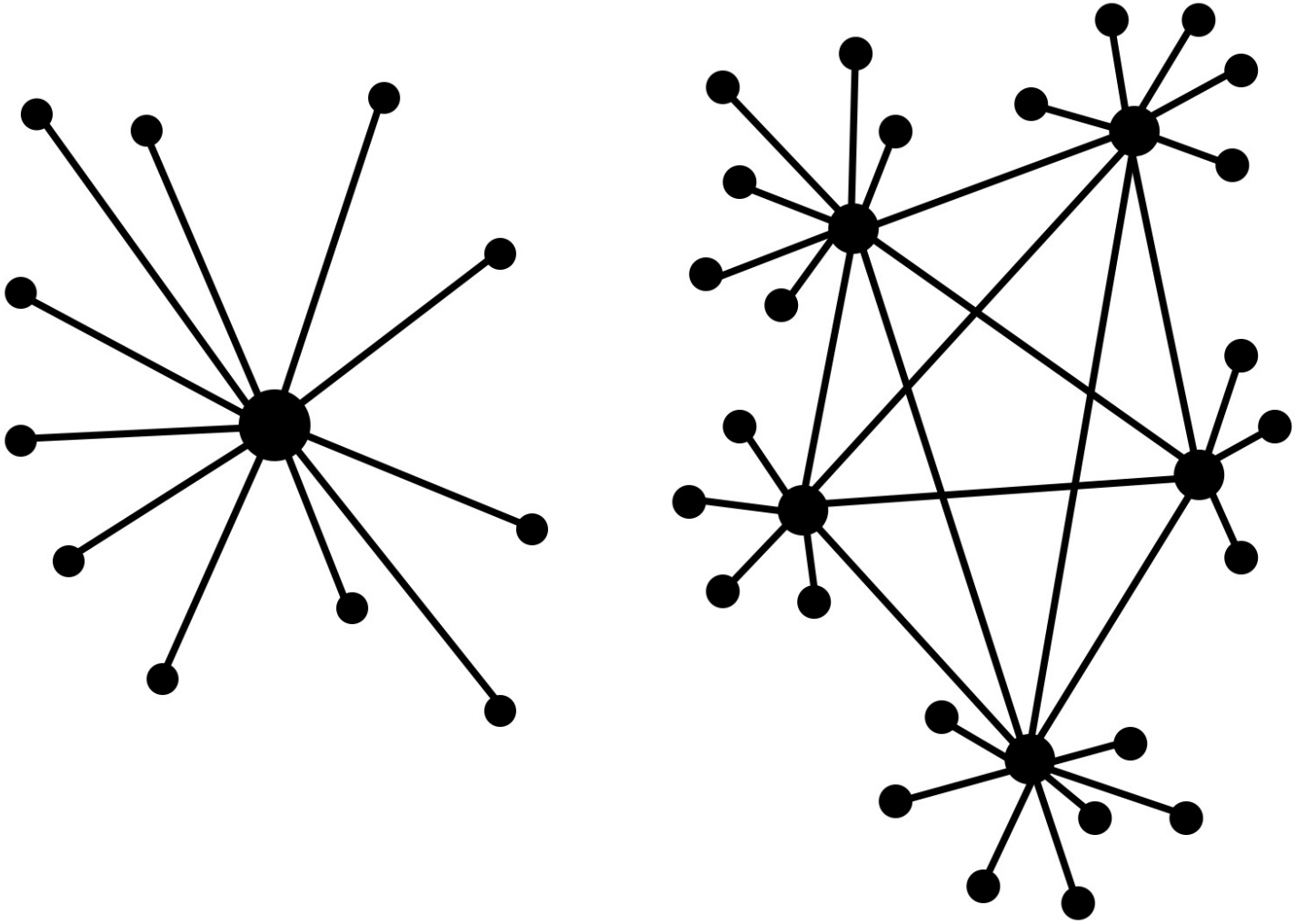
Datenwirtschaft

- "Kostenlose" Angebote
  - Daten sind eine neue Währung
  - Datenhändler kaufen Profile und verkaufen sie an die Werbeindustrie, Versicherungen, Schufa, etc.
- Geschlossene Systeme
  - Proprietäre Software
  - Keine offenen Schnittstellen
- Big Data
  - Zusammenführung, Analyse und Auswertung großer Datenmengen

Datenwirtschaft

- Sicherheit
  - Bedeutet Aufwand = Kosten
- Datenschutz
  - Weniger Daten für das Unternehmen
  - Weniger Rohmaterial zum Analysieren und Verkaufen
  - Privatsphäre "überholt"?

Zentral vs. Dezentral



Begriff: Metadaten

- Inhalt
- Metadaten (Nachricht)
  - Absender, Empfänger
  - Datum, Uhrzeit
  - IP-Adresse / Mobilfunknetz
- Metadaten (Foto)
  - Auflösung
  - Blende, Belichtungszeit
  - GPS Koordinaten

Lieber Max,

heute waren wir bei der Felsformation „Twelwe Apostles“ im Süden von Australien. War mega beeindruckend!

Viele Grüße
Leah

Begriff: Metadaten

In der Telekommunikation häufig *Verbindungsdaten* genannt.

- Kleine Datenmenge
- Leicht zu analysieren (im Gegensatz zu Inhalt)
- Schwierig zu verschlüsseln
  - da notwendig um die Kommunikation zu ermöglichen

Metadaten eignen sich perfekt zur Datenanalyse und Massenüberwachung!

We Kill People Based on Metadata

General Michael Hayden, Ex-Chef von NSA und CIA

VDS (Historie)

- 2006: EU-Richtlinie
  - Nach und nach von vielen Mitgliedsstaaten umgesetzt
- 2010: Vom Bundesverfassungsgericht als verfassungswiedrig erklärt
- 2014: Vom EuGh wegen Verstoß gegen die Charta der Grundrechte als ungültig erklärt

VDS-Zombie

- 2015 vom Bundestag beschlossen als:

  „*Einführung einer Speicherpflicht und Höchstspeicherfrist für Verkehrsdaten“.*

- Anfang 2017: Bundesverfassungsgericht lehnt Klärung im Eilrechtsschutzverfahren und Aufschub ab.
- Ab 1. Juli startet Speicherpflicht
- Verfassungsbeschwerden laufen

Neusprech Award 2015

- Vorratsdatenspeicherung
- Mindestspeicherfrist, Mindestspeicherdauer
- Mindestdatenspeicherung
- Speicherpflicht und Höchstspeicherfrist für Verkehrsdaten
- Private Vorsorgespeicherung
- Digitale Spurensicherung

VDS: Wer speichert?

- Telekommunikationsanbieter
  - ISP (Internet-Service-Provider) & Mobilfunkanbieter
  - Outsourcing: VDS as a Service

- Polizeibehörden fordern Daten zur Aufklärung "schwerer Straftaten" an.

VDS: Was wird gespeichert?

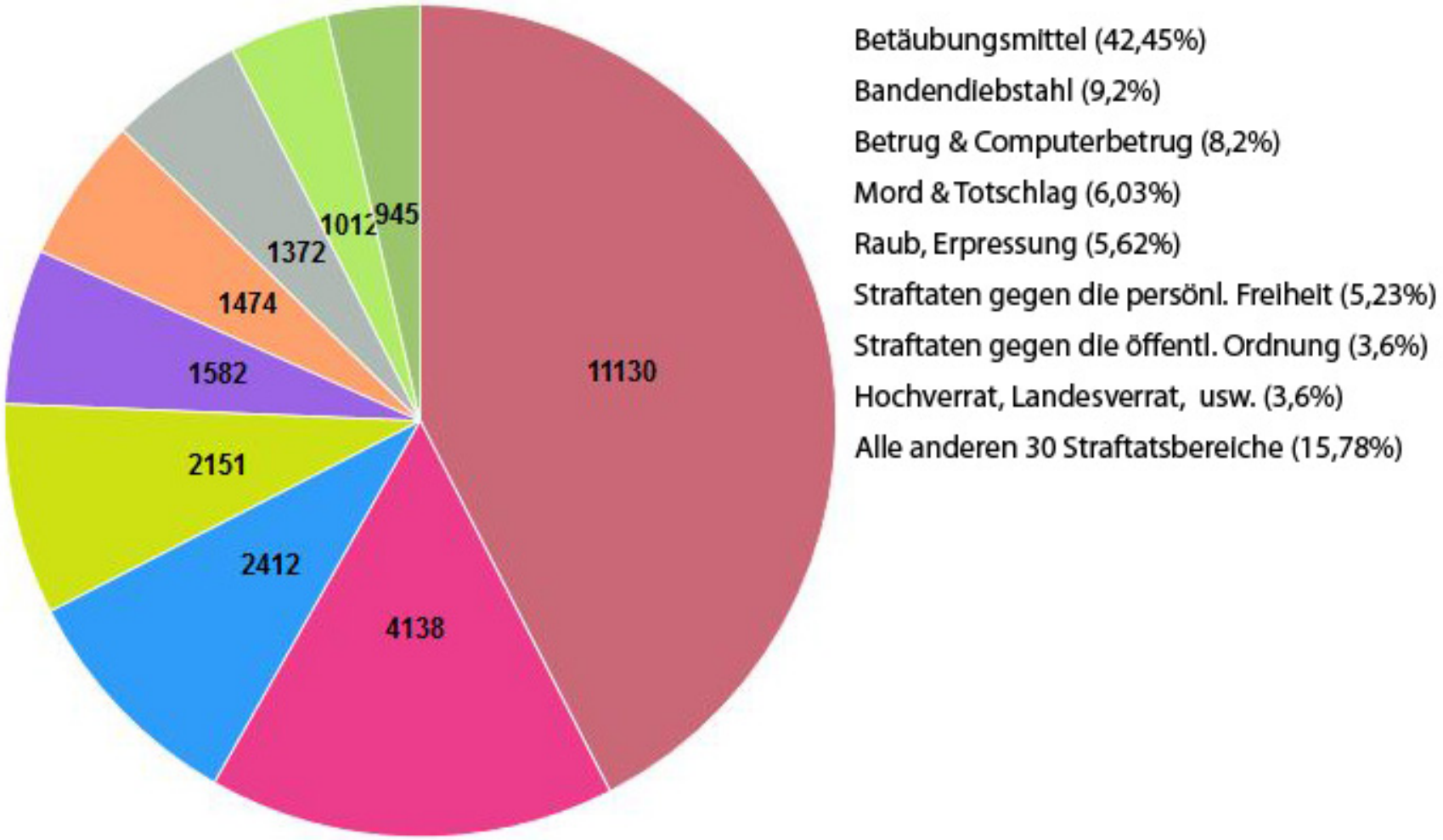
- Standortdaten **aller Mobiltelefonate** bei Beginn des Telefonats (für 4 Wochen)
- Standortdaten bei Beginn einer **mobilen Internetnutzung** (für 4 Wochen)
- Rufnummern, Zeit und Dauer **aller Telefonate** (für 10 Wochen)
- Rufnummern, Sende- und Empfangszeit **aller SMS-Nachrichten** (für 10 Wochen)
- Zugewiesene IP-Adressen **aller Internetnutzer** sowie Zeit und Dauer der Internetnutzung (für 10 Wochen)

VDS Visualisierung

- Balthasar Glättli (Grüne, Schweiz):
  https://apps.opendatacity.de/vds/

- Malte Spitz (Grüne, Deutschland):
  http://www.zeit.de/datenschutz/malte-spitz-vorratsdaten

Telekommunikationsüberwachung 2015 nach Straftatbeständen



Quelle: Netzpolitik.org

VDS: Ausweitung

- Schon vor in Kraft treten des Gesetzes
- Vorratsdaten auch bei Wohnungseinbrüchen abfragen
  - Zusätzlich Funkzellenabfrage

- Kritik:
  Technik erst etablieren, dann ausweiten

Folgen von Massenüberwachung

- Alle Bürger sind Verdächtige
- Schere im Kopf
  - Selbstzensur
- Chilling Effect
  - Angepasstes Verhalten
- Einschränkung vieler Grundrechte
  - Meinungsfreiheit, Briefgeheimnis, Freie Entfaltung der Persönlichkeit

Freie Entfaltung der Persönlichkeit

Grundgesetz, Artikel 2

Auswahl von Überwachungsgesetzen und -maßnahmen 2016

Geheimdienste und Behörden	Gesetze und Gesetzesentwürfe	Politische Forderungen	Privatwirtschaft & Überwachung	Gesetze und -entwürfe Europa	Datenbanken Europa	Gesetze im Ausland
Zitis	Anti-Terror-Gesetz (u.a. Ausweise für SIM)	Ausweitung VDS auf Messenger	Uploadfilter in sozialen Netzwerken	PNR Fluggast-daten	Fluggast-daten PNRDEP	Snoopers Charter UK
ANISKI	BND-Gesetz	Aufweichung Provider-privileg	Yahoo durchsuchte alle E-Mails	Schutz von Geschäfts-geheim-nissen	ADEP	Anti-Terror-Gesetz in Polen
Bund: Höhere Budgets Geheim-dienste	Datenaus-tauschs-verbesserungs gesetz	Gesichts-erkennung bei Video-überwachung	Ausweitung der Video-überwachung	Mehr Europol-Befugnisse + Meldestelle Internet	Reiseregister EET & ETIAS	Ausnahme-zustand in Frankreich
Bayerischer VS: Zugriff auf Vorratsdaten	Videoüberwac hungsver besserungs-gesetz	Verbot von Fake News	US-Wahlkampf: Targeting mit Psychometrie	Eröffnung Europäisches Anti-Terror-Zentrum Dem Haag	Erweiterung Eurodac	Geheimdienst-Gesetz in Niederlande
Mobiler Staats-trojaner	Novelle BDSG	Verlängerung Speicherfrist VDS	Facebook speichert ethnische Zugehörigkeit	EU-Anti-Terror-Richtlinie	Zusammen-legung der „Datentöpfe“	Staatsschutz-gesetz in Österreich

Massenüberwachung durch die NSA

- Stasi vs. NSA Flächenvergleich: https://apps.opendatacity.de/stasi-vs-nsa/

Leseempfehlungen

- https://netzpolitik.org
- Buch: "Die globale Überwachung" (Glenn Greenwald)
- Buch: "Was Google wirklich will" (Thomas Schulz)
- Videos: http://www.alexanderlehmann.net/

- Mittagspause -

Agenda Freitag

von	bis	Titel
10:00	12:00	Vortrag: Einführung, Warum überhaupt Verschlüsselung?
12:00	12:45	- Mittagspause -
12:45	14:00	Digitale Selbstverteidigung I (W10, Passwörter, E-Mail, Datenverschlüsselung)
14:00	14:15	- Pause -
14:15	16:00	Praxisteil
		Open End

"Datenschutzalbtraum" Windows 10

"Datenschutzalbtraum" Windows 10?

- Windows Store mit zahlreichen vorinstallieren Apps
  - z.B. Cloud-Dienst "OneDrive" oder Browser und PDF-Reader "Edge"
- "Sprachassistentin" Cortana
- Systemupgrades, die nur aufgeschoben werden können
  - aktuell "Creators-Update"

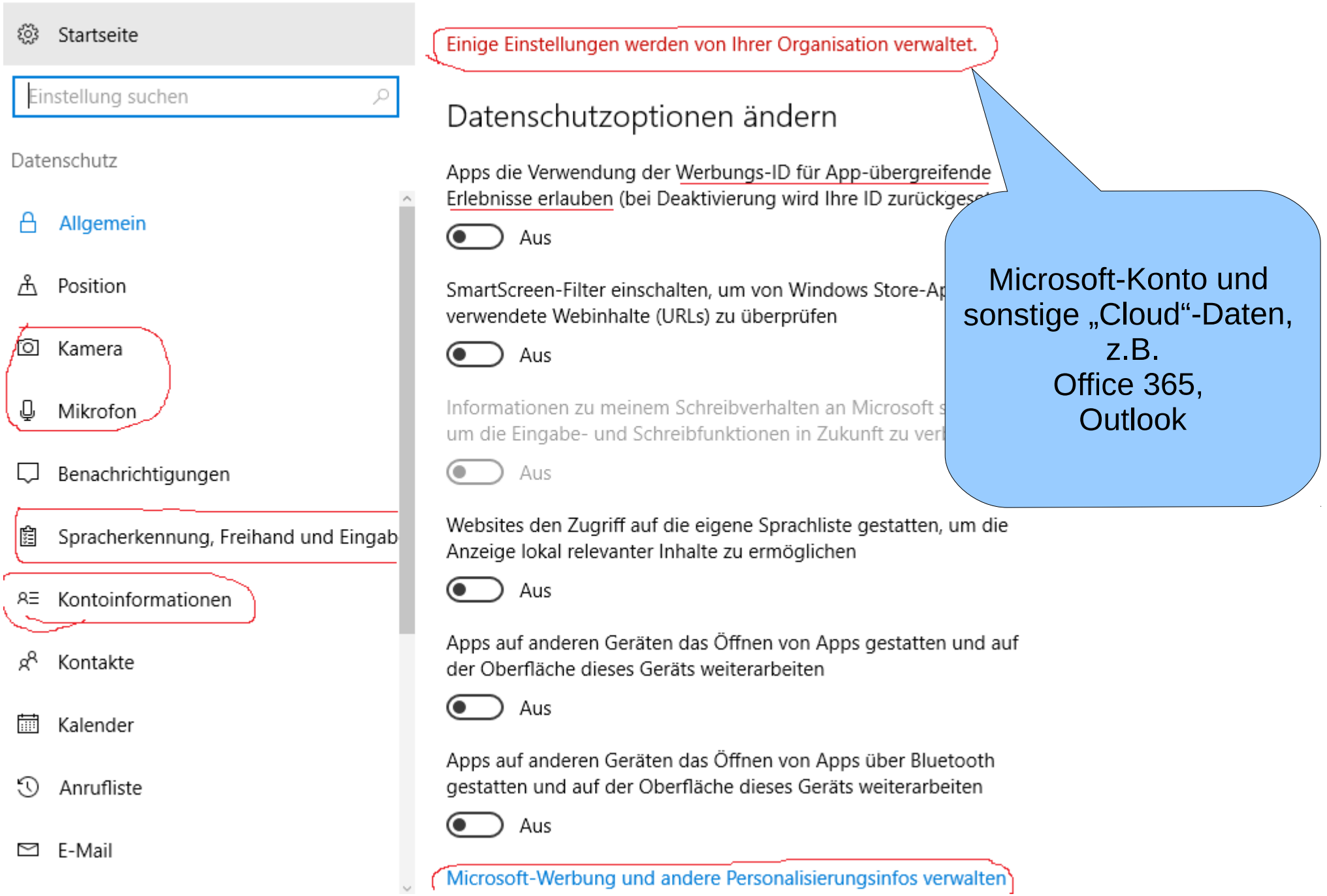
Sammelwut von Windows 10

- Sammelt standardmäßig fleißig Daten und sendet diese an Microsoft
  - Common Data (diagnostic header information)
  - Device, Connectivity and Configuration data
  - Product and Service Usage data
  - Product and Service Performance data
  - Software Setup and Inventory data
  - Content Consumption data
  - Browsing, Search and Query data
  - Inking, Typing, Speech Utterance data
  - Licensing and Purchase data

https://docs.microsoft.com/de-de/windows/configuration/windows-diagnostic-data

Datenschutzerklärung

- "Microsoft erhebt Daten, um effektiv arbeiten und Ihnen die besten Erfahrungen mit unseren Produkten anbieten zu können. Sie stellen einige dieser Daten direkt bereit, beispielsweise wenn Sie ein Microsoft-Konto erstellen, eine Suchanfrage bei Bing einreichen, einen Sprachbefehl an Cortana erteilen, [... können wir] Ihre Interaktion mit unseren Produkten aufzeichnen [...] Wir erhalten ebenfalls Daten von Drittanbietern."
  https://privacy.microsoft.com/de-de/privacystatement
- Zweck der Sammelwut: mit den Daten der eigenen Kunden Geld verdienen!


Startseite
Einstellung suchen
Datenschutz
Allgemein
Position
Kamera
Mikrofon
Benachrichtigungen
Spracherkennung, Freihand und Eingab
Kontoinformationen
Kontakte
Kalender
Anrufliste
E-Mail
Einige Einstellungen werden von Ihrer Organisation verwaltet.
Datenschutzoptionen ändern
Apps die Verwendung der Werbungs-ID für App-übergreifende Erlebnisse erlauben (bei Deaktivierung wird Ihre ID zurückgese
Aus
SmartScreen-Filter einschalten, um von Windows Store-Ap verwendete Webinhalte (URLs) zu überprüfen
Aus
Informationen zu meinem Schreibverhalten an Microsoft s um die Eingabe- und Schreibfunktionen in Zukunft zu verb
Aus
Websites den Zugriff auf die eigene Sprachliste gestatten, um die Anzeige lokal relevanter Inhalte zu ermöglichen
Aus
Apps auf anderen Geräten das Öffnen von Apps gestatten und auf der Oberfläche dieses Geräts weiterarbeiten
Aus
Apps auf anderen Geräten das Öffnen von Apps über Bluetooth gestatten und auf der Oberfläche dieses Geräts weiterarbeiten
Aus
Microsoft-Werbung und andere Personalisierungsinfos verwalten
Microsoft-Konto und sonstige „Cloud“-Daten, z.B. Office 365, Outlook

Wo kann ich weitere Informationen zu Werbung auf Microsoft-Websites und -Apps erhalten?

Microsoft arbeitet mit Partnern wie AOL, AppNexus und anderen dritten Dienstanbietern zusammen, um angepasste Inhalte bereitzustellen und Werbung auf MSN, Outlook.com und anderen Websites und Apps anzuzeigen. Microsoft übermittelt auch Suchanzeigen an Bing und unsere Konsortialsuchpartner. Weitere Informationen zu den Datenschutzpraktiken von Microsoft erhalten Sie hier: hier. Mehr Informationen zu interessenbezogener Werbung von AOL und AppNexus finden Sie in deren Datenschutzbestimmungen: AOL und AppNexus.

Welche Optionen stehen bei interessenbezogener Werbung zur Verfügung?

Auf dieser Seite können Sie angeben, dass Sie keine interessenbezogene Werbung mehr von Microsoft empfangen möchten.

Zudem können Sie auf den folgenden Websites angeben, dass Sie keine interessenbezogene Werbung mehr von allen selbstregulierten Mitgliedern, einschließlich Microsoft, AOL, AppNexus und Anzeigennetzwerken von Drittanbietern, erhalten möchten:

- In den USA: Digital Advertising Alliance (DAA)
- In Europa: European Interactive Digital Advertising Alliance (EDAA)
- In Kanada: Ad Choices: Digital Advertising Alliance of Canada (DAAC)

Sie können die interessenbezogene Werbung in Windows-Apps steuern, indem Sie die Option Werbe-ID in den Windows-Einstellungen deaktivieren.

Personalisierte Werbung in diesem Browser

OFF

Überprüfen Sie die Einstellung „Personalisierte Werbung" für diesen Webbrowser.

Erfahren Sie mehr

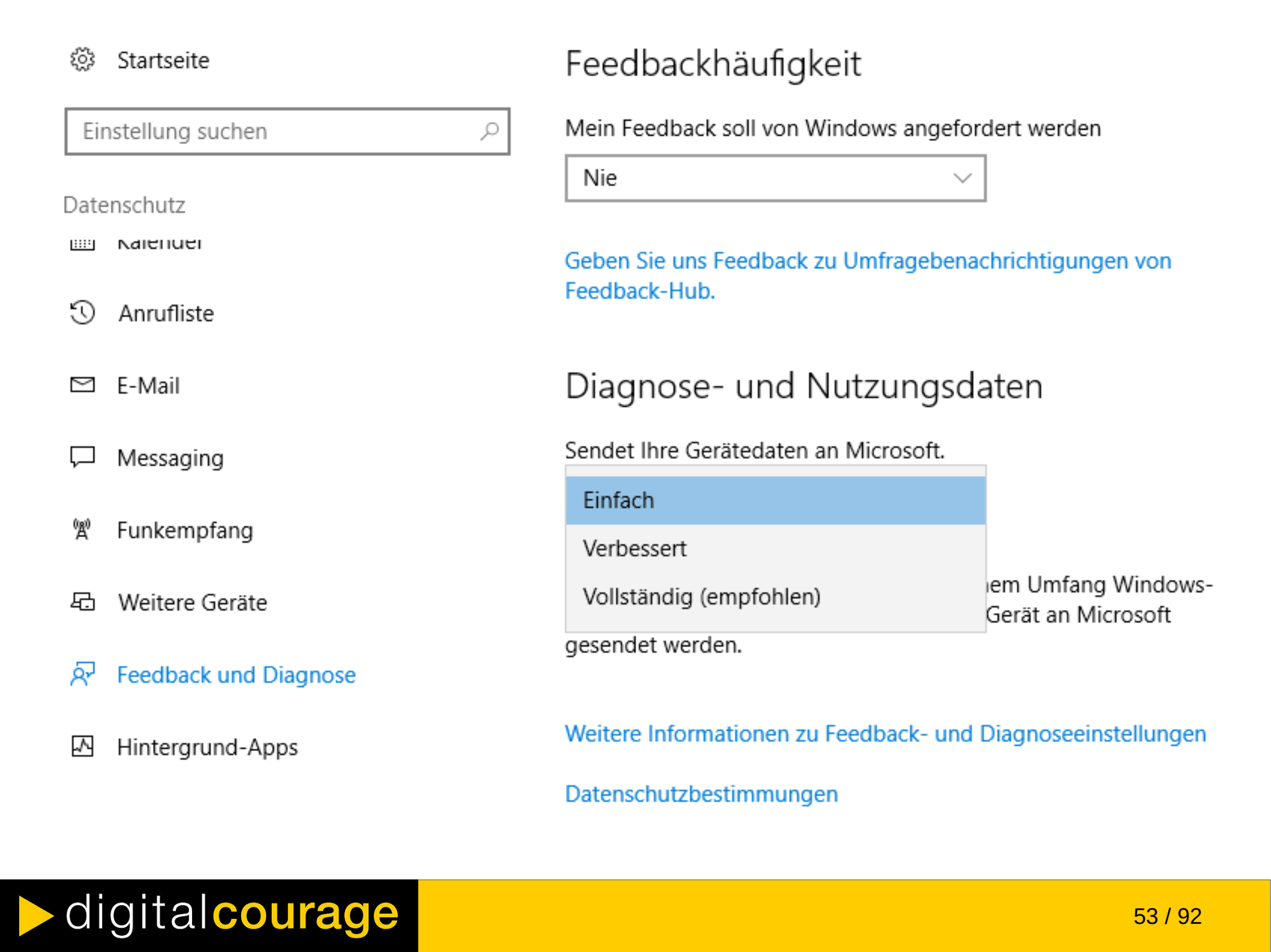
Beim Verwenden meines Microsoft-Kontos immer personalisierte Werbung anzeigen

OFF Zum Ändern anmelden...

Überprüfen Sie die Einstellung „Personalisierte Werbung". Sie gilt, wenn Sie sich auf einem Computer oder Gerät mit Ihrem Microsoft-Konto anmelden. Dies gilt auch für Windows, Windows Phone, Xbox und andere Geräte.

"Datenschutzalbtraum" Windows 10!

- Sammelwut lässt sich nur schwer verhindern
- Selbst wenn man in den Datenschutzeinstellungen das Senden sämtlicher Daten deaktiviert, werden dennoch Daten gesendet
- Als generelle Regel sollte gelten: Dienste, die Ihr nicht brauchet oder deren Aktionen Ihr nicht versteht, sollten deaktiviert werden


Startseite
Einstellung suchen
Datenschutz
Kalender
Anrufliste
E-Mail
Messaging
Funkempfang
Weitere Geräte
Feedback und Diagnose
Hintergrund-Apps
Feedbackhäufigkeit
Mein Feedback soll von Windows angefordert werden
Nie
Geben Sie uns Feedback zu Umfragebenachrichtigungen von Feedback-Hub.
Diagnose- und Nutzungsdaten
Sendet Ihre Gerätedaten an Microsoft.
Einfach
Verbessert
Vollständig (empfohlen)
em Umfang Windows-
Gerät an Microsoft
gesendet werden.
Weitere Informationen zu Feedback- und Diagnoseeinstellungen
Datenschutzbestimmungen

Diagnose- und Nutzungsdaten = Vollständig

- Bei der Einstellung "Vollständig" sendet Win10 u.a. die folgenden Daten an Microsoft:
  - Daten über App-Verwendung (z.B. welche Apps, Nutzungsdauer und Reaktionszeit)
  - Browser-Nutzung, einschließlich Browserverlauf und Suchbegriffe
  - Teilweise Freihand- und Tastatureingaben (lt. Microsoft werden alle personenbezogenen Daten entfernt)
  - "Erweiterte Fehlerberichterstattung, die den Speicherstatus des Geräts bei einem System- oder App-Absturz umfasst. Dabei können unbeabsichtigt Teile der Datei übermittelt werden, die Sie beim Auftreten des Problems verwendet haben."
  - Datenweitergabe an OEM-Partner (z.B. Fehlerberichte)

Schutz gegen den "Datenschutzalbtraum"

- Was könnt Ihr dagegen tun?
- Keine Tools oder 1-Click-Lösungen (z.B. O&O ShutUp10, DoNotSpy10)
- Einfach und nutzerfreundlich
  - Paper vom AKIF – Orientierungshilfe zur datenarmen Konfiguration von Windows 10, abrufbar unter: https://www.it-sicherheit.mpg.de/Orientierungshilfe_Windows10.pdf
- Übergangslösung: So lang wie möglich bei einer älteren Windows-Version bleiben
- Auf Linux umsteigen; Windows nur noch für Programme nutzen, die unter Linux nicht laufen

Literaturempfehlung

- Arbeitskreis Informationssicherheit der deutschen Forschungseinrichtungen (AKIF) der Max-Planck-Gesellschaft, Orientierungshilfe zur datenarmen Konfiguration von Windows 10; Stand: 06.12.2016; abrufbar unter: https://www.it-sicherheit.mpg.de/Orientierungshilfe_Windows10.pdf
- Mike Kuketz, Windows 10: Dem Konntrollverlust entgegenwirken; Stand: 28. März 2017; abrufbar unter https://www.kuketz-blog.de/windows-10-dem-kontrollverlust-entgegenwirken/
- Datenschutzerklärung von Microsoft; Stand: März 2017; abrufbar unter https://privacy.microsoft.com/de-de/privacystatement

Sichere Passwörter

Sichere Passwörter (1)

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.

Sichere Passwörter (2)

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 Passwort verwenden
  - Keine Wörter aus dem persönlichen Umfeld verwenden (Namen, Geburtsdaten etc.)
- Social Engineering
  - Niemandem das Passwort verraten!

Brute-Force-Angriffe und Passwortlänge

Nutzung von Kleinbuchstaben (26 Zeichen)

Zeichen	Kombinationen	Sekunden	Stunden	Jahre
1	26			
2	676			
3	17576			
4	456976			
5	11881376			
6	308915776	0.14		
7	8031810176	3.83		
8	208827064576	100		
9	5429503678976	2590		
10	141167095653376	67344	18.71	
11	3670344486987776	1750948	486.37	
12	95428956661682180	45524643	12645.73	1.44
13	2481152873203736600	1183640714	328789.09	37.53
14	64509974703297150000	30774658570	8548516.27	975.86
15	$1.67725934228572 6 \times 10^{21}$	800141122825	222261423.01	25372.31

Quelle: http://www.1pw.de/brute-force.html (Rechengeschwindigkeit: 2096204400 Schlüssel pro Sekunde (Keys/sec))

Brute-Force-Angriffe und Passwortlänge

Nutzung von Groß-, Kleinbuchstaben und Zahlen (62 Zeichen)

Zeichen	Kombinationen	Sekunden	Stunden	Jahre
1	62			
2	3844			
3	238328			
4	14776336			
5	916132832			
6	56800235584	27		
7	3521614606208	1680		
8	218340105584896	104160	28.93	
9	13537086546263552	6457904	1793.86	
10	839299365868340200	400390041	111219.46	12.70
11	52036560683837100000	24824182548	6895606.26	787.17
12	$3.2262667623979 \times 10^{21}$	1539099317985	427527588.33	48804.52
13	$2.000285392686698 \times 10^{23}$	95424157715092	26506710476.41	3025880.19
14	$1.2401769434657528 \times 10^{25}$	5916297778335704	1643416049537.70	187604571.87
15	$7.689097049487666 \times 10^{26}$	3668104622568136 30	101891795071337.12	11631483455.63

Quelle: http://www.1pw.de/brute-force.html (Rechengeschwindigkeit: 2096204400 Schlüssel pro Sekunde (Keys/sec))

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

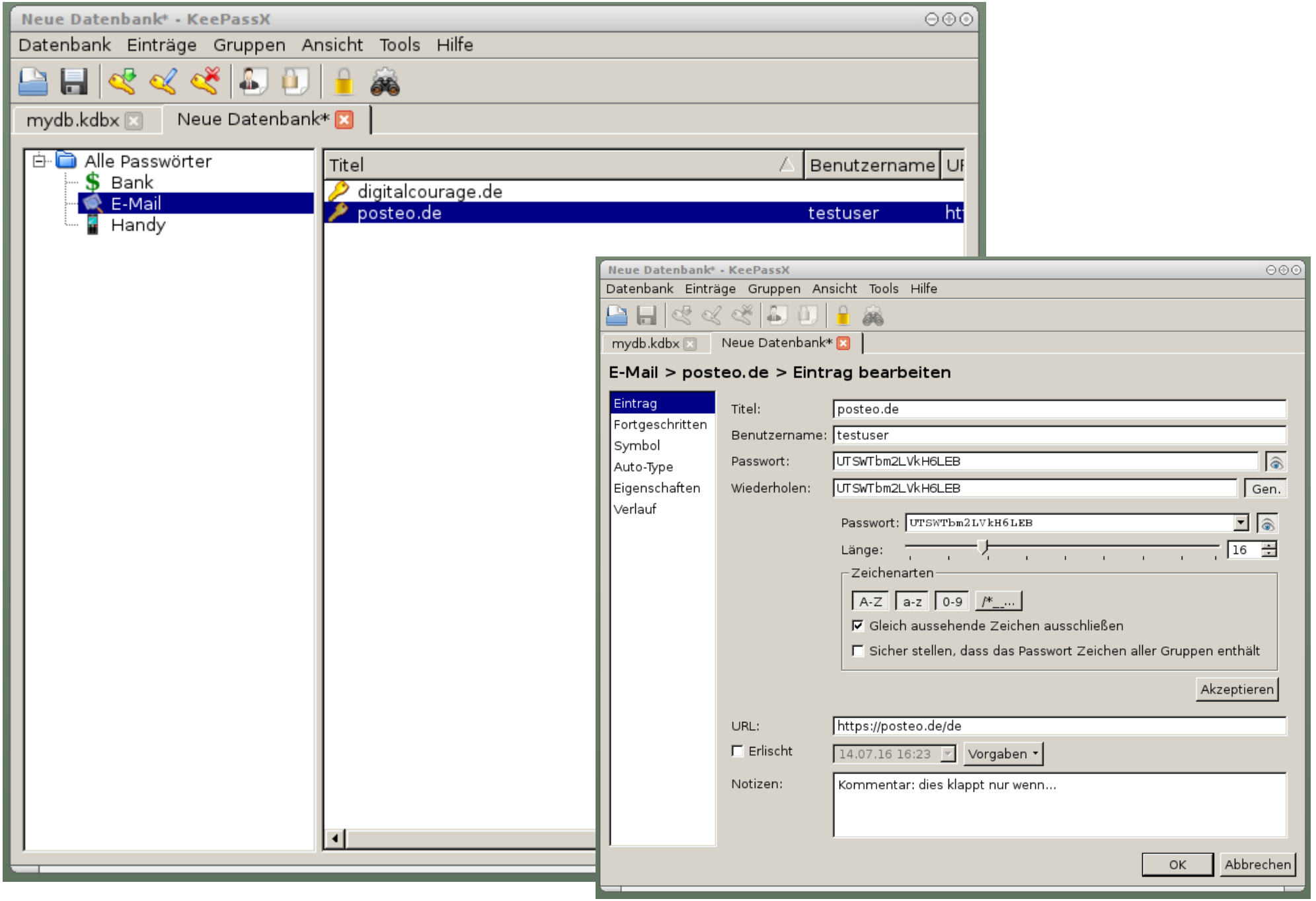
Software: **KeePassX**

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
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

Videoempfehlung

- Um das eben erklärte zu wiederholen, seht Euch bitte das Video von Alexander Lehmann " Passwörter Einfach Erklärt" an; abrufbar unter: https://vimeo.com/138839266

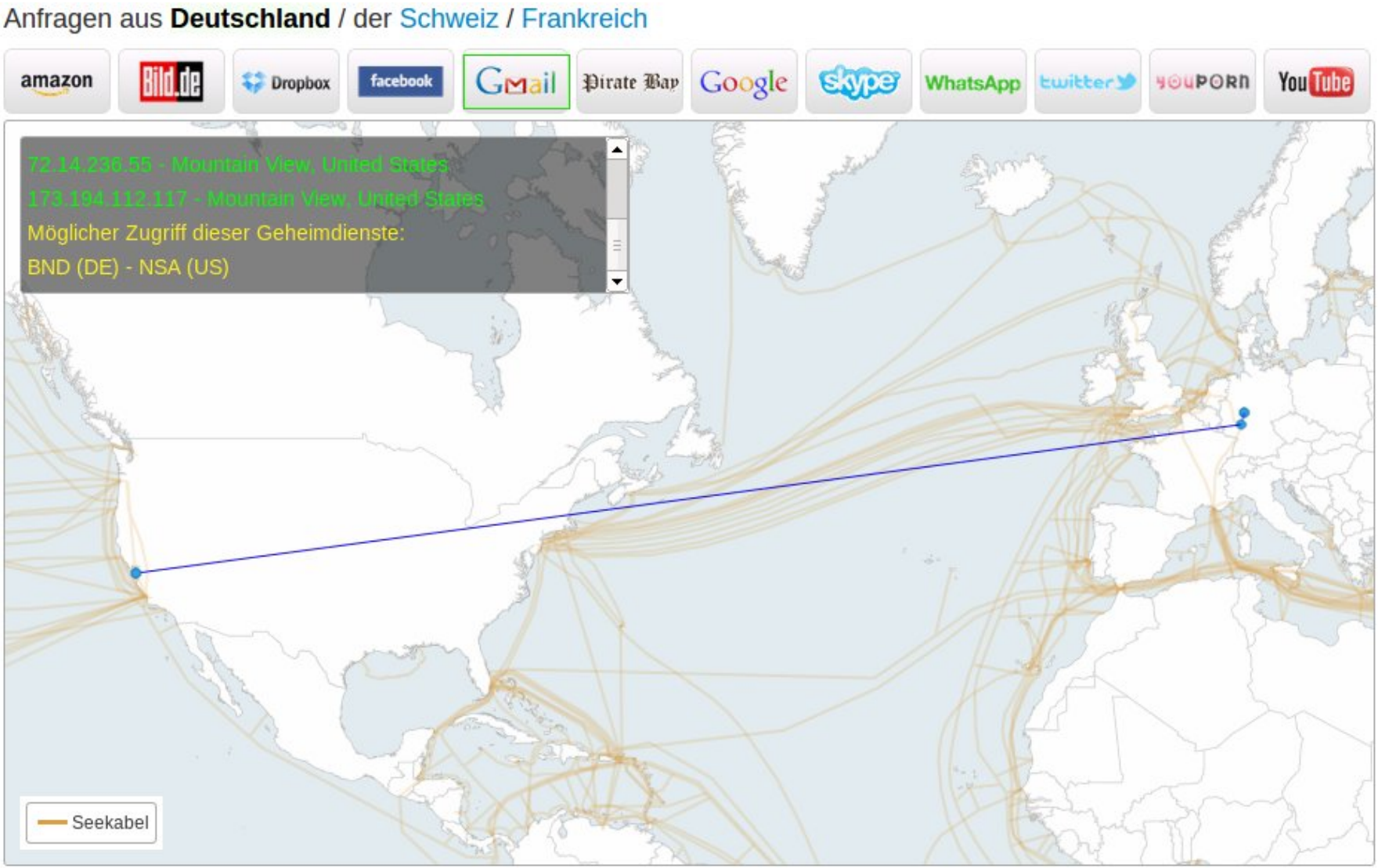
Exkurs: Freie Software

- Freiheit 0: Die Freiheit, das Programm auszuführen, wie man möchte, für *jeden Zweck.*
- Freiheit 1: Die Freiheit, die Funktionsweise des Programms zu untersuchen und eigenen Bedürfnissen der Datenverarbeitung anzupassen.
- Freiheit 2: Die Freiheit, das Programm weiterzuverbreiten und damit seinen Mitmenschen zu helfen.
- Freiheit 3: Die Freiheit, das Programm zu verbessern und diese Verbesserungen der Öffentlichkeit freizugeben, damit die gesamte Gemeinschaft davon profitiert.

⇒ Viel mehr als Open Source (offenlegen der Quelltexte)

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

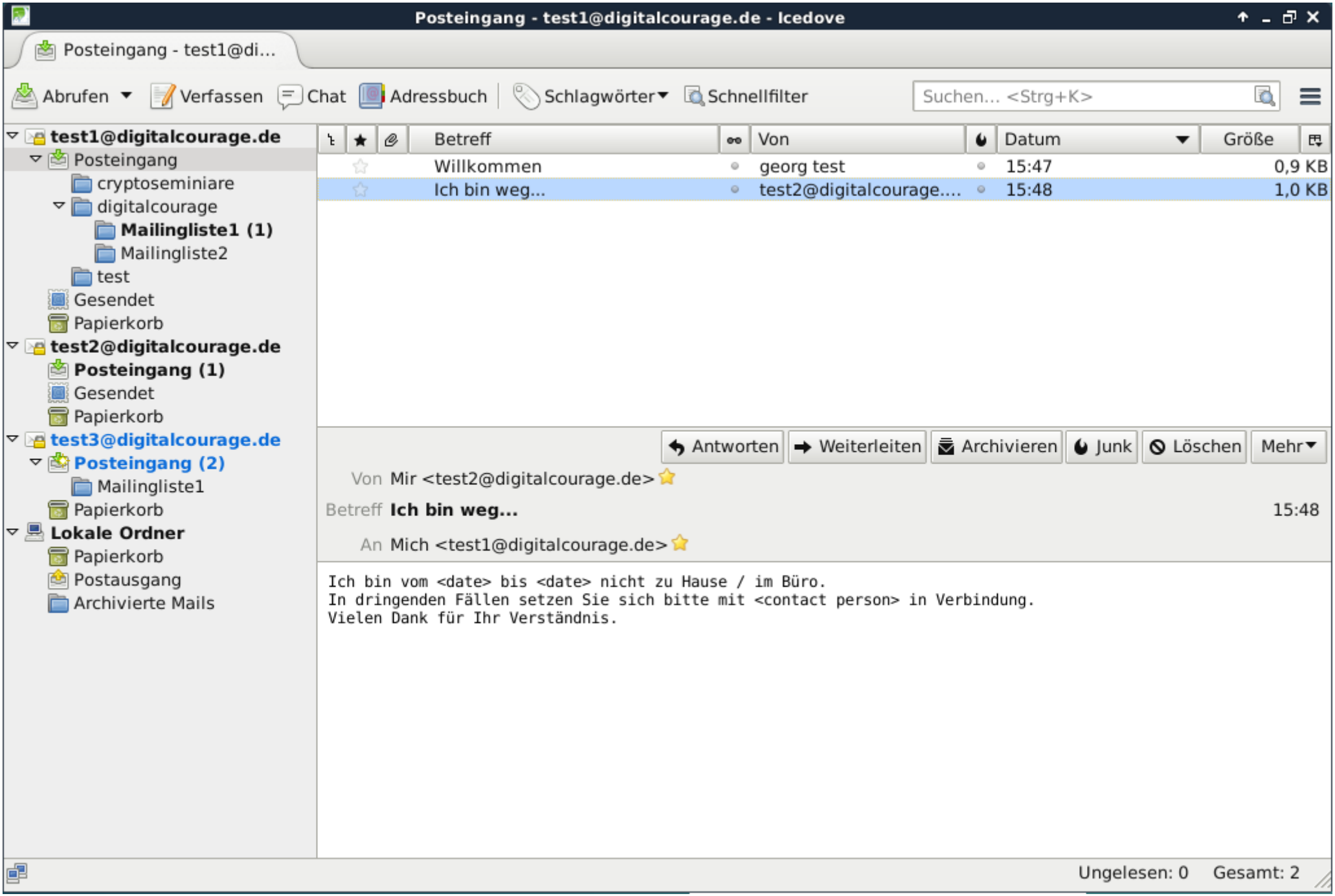
- Standort in Deutschland
- Datensparsamkeit
- Keine Inhaltsanalyse
- Keine Werbung
- Anonyme Nutzung möglich
- Datenschutz hat Priorität

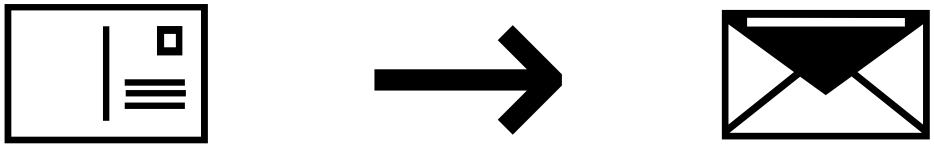
Nachteile

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

E-Mail-Client

- 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



"Privacy is the right to a free mind."

– Edward Snowden

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

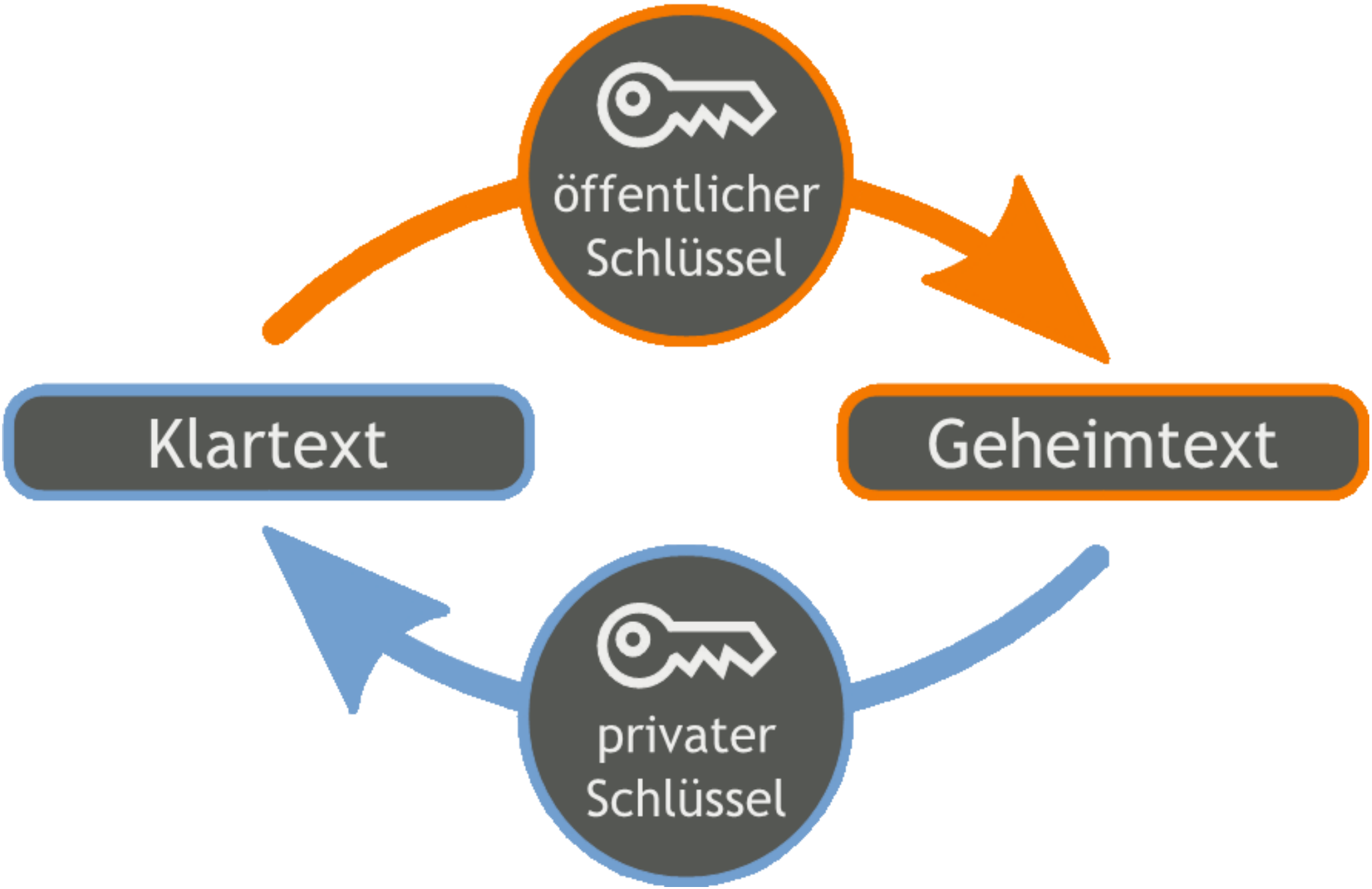
- **Schlüsselpaar:** was **ein** Schlüssel **ver**schlüsselt, muss mit dem **anderen** Schlüssel **ent**schlüsselt werden
- Alle Beteiligten erzeugen ein eigenes Schlüsselpaar

- 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

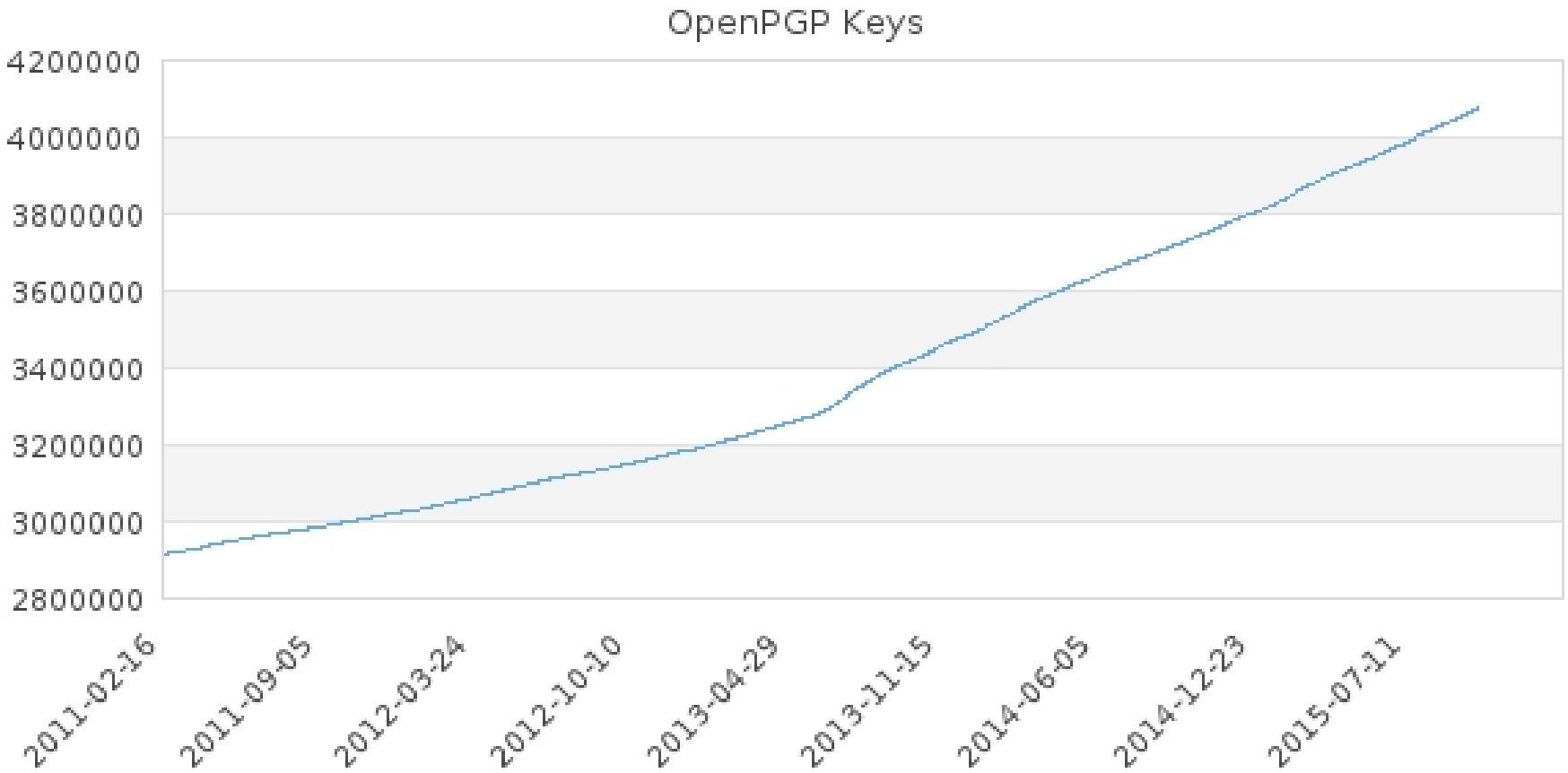
- Es gilt:
  - Absender braucht **öffentlichen Schlüssel der Empfängerin**
  - nur Empfängerin kann (mit ihrem privaten Schlüssel) entschlüsseln


öffentlicher Schlüssel
Klartext
Geheimtext
privater Schlüssel

PGP Public Keys austauschen

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

Verbreitung von PGP



Quelle: https://sks-keyservers.net/status/key_development.php

Digitale Signatur mit PGP

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

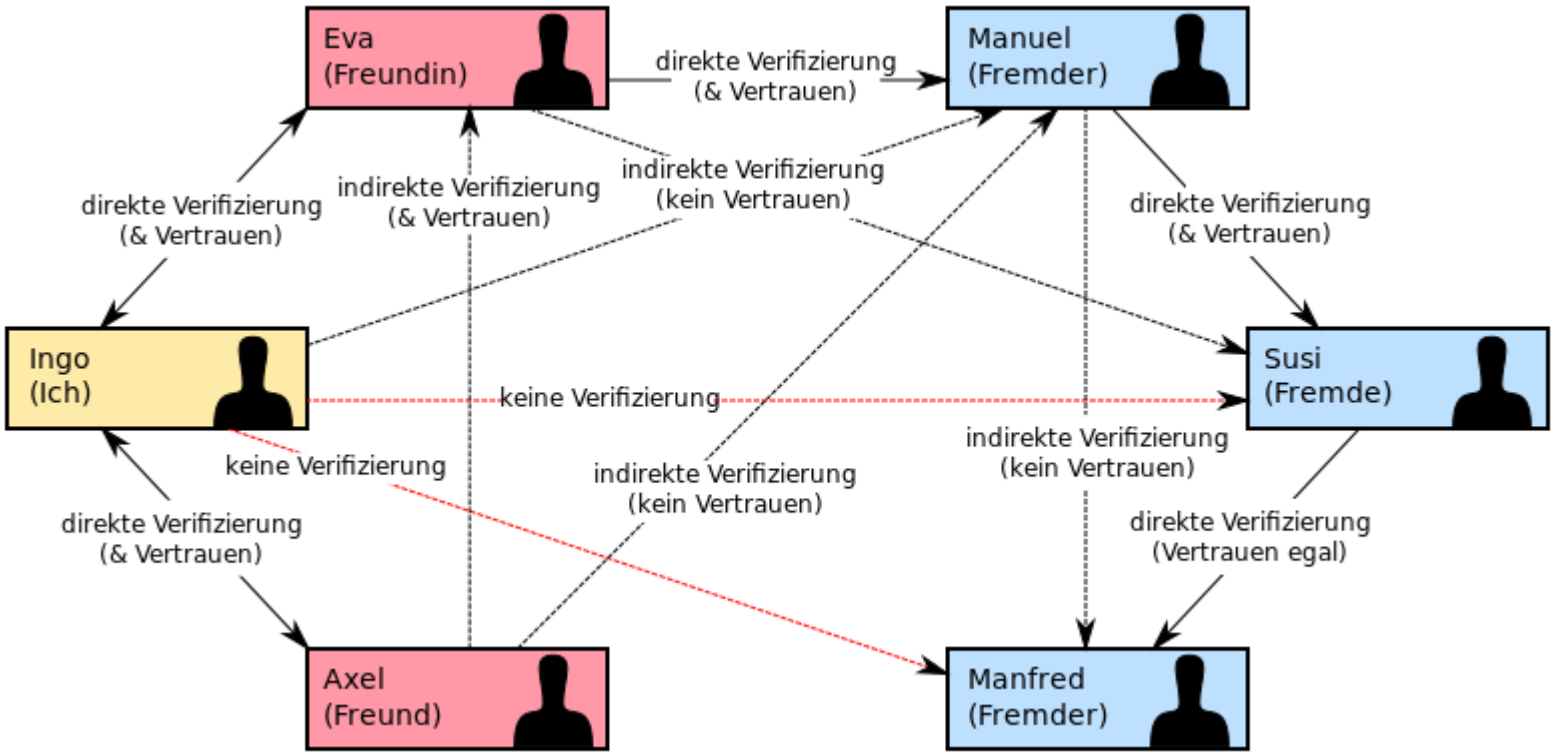
- Auch ohne Verschlüsseln möglich
- Beispiel:

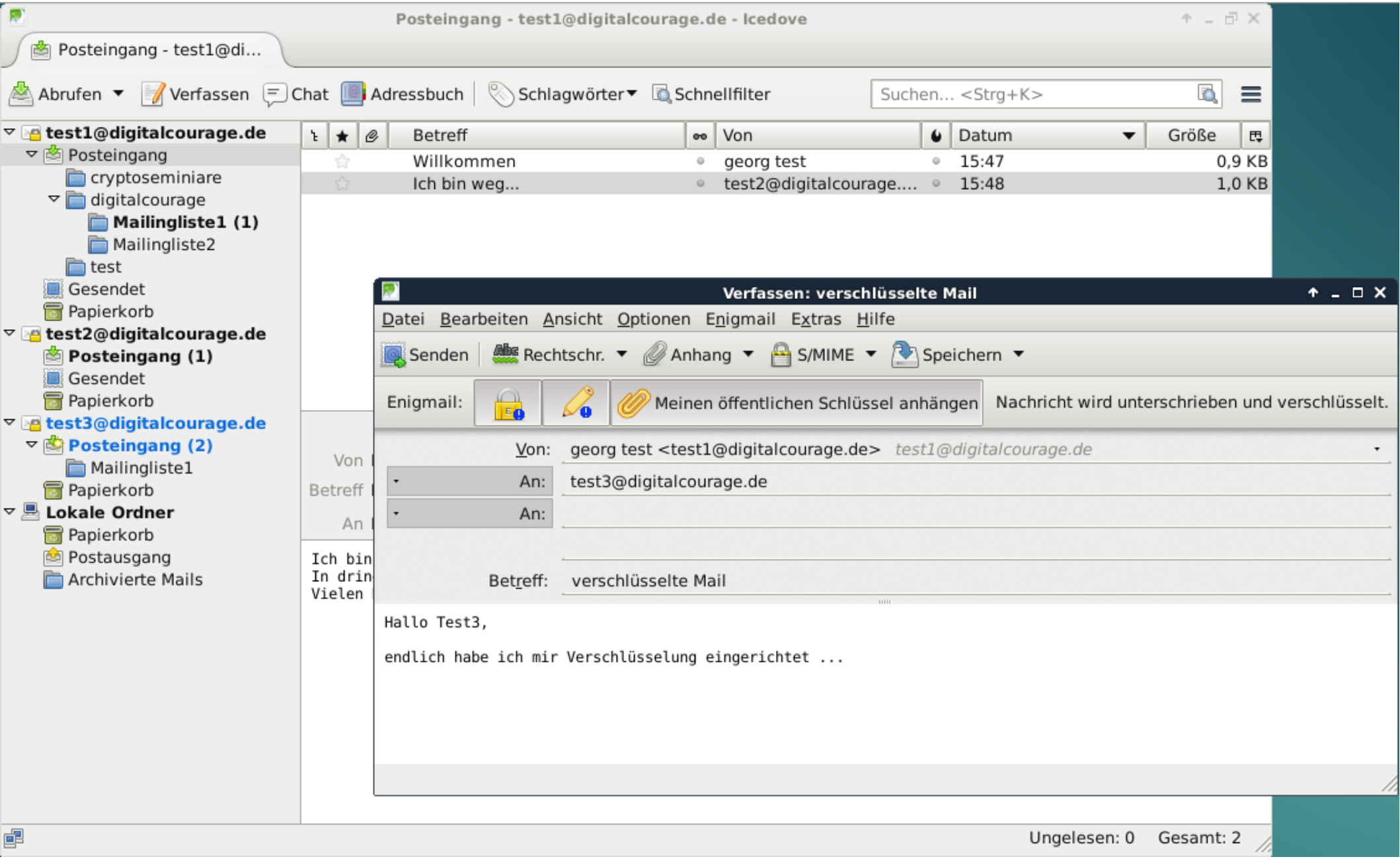
```
-----BEGIN PGP SIGNATURE-----
iQA/AwUBONpOg40d+PaAQUTlEQIc5ACdGkKSzpOrsT0Gvj
3jH9NXD8ZP2IcAn0vj/BHT+qQCtPCtCwO1aQ3Xk/NL=1CZt
-----END PGP SIGNATURE----
```

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

Web of Trust




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

Dateiverschlüsselung

Warum überhaupt verschlüsseln?

- Genereller Schutz sensibler und vertraulicher Daten
  - Bei Verlust/Diebstahl des Laptops oder USB-Stick
  - Jeder der personenbezogene Daten speichert
- Weil Ihr ein Grundrecht auf digitale Intimsphäre habt!
  - Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme
  - sog. IT-Grundrecht, Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG

Dateiverschlüsselung

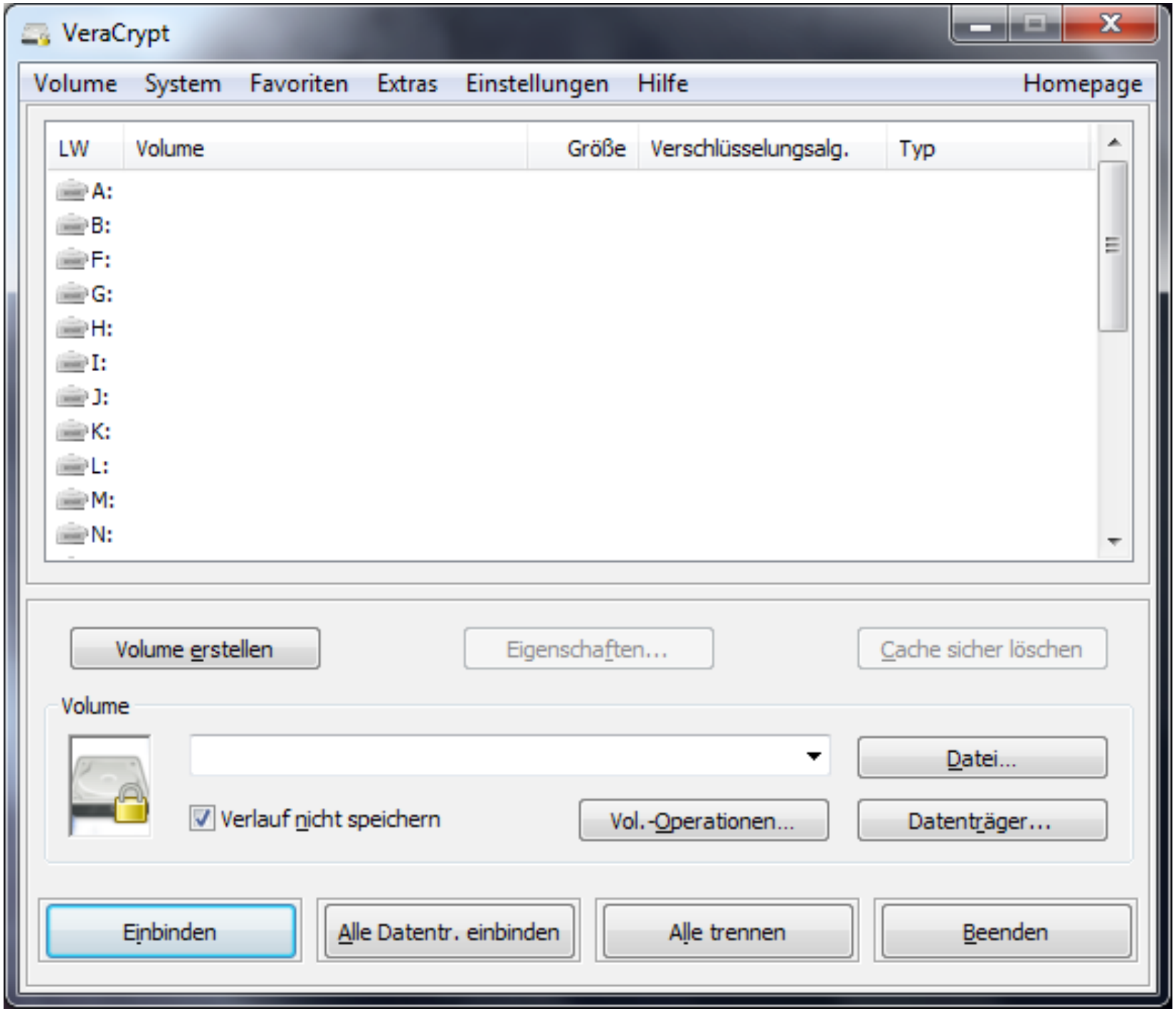
- Software: **VeraCrypt**
  - Software zur Dateiverschlüsselung
  - Quelloffen und auf allen gängigen Plattformen verfügbar
  - Freie Software

- Warum VeraCrypt?
  - Weil Windows-Verschlüsselung "BitLocker" vermutlich von Geheimdiensten geknackt werden kann

Über VeraCrypt (1)

Was kann ich mit VeraCrypt verschlüsseln?

- Container (verschlüsselte Ordner)
- Datenträger:
  - Festplatten/SSDs
  - CDs, DVDs... (Container)
  - USB-Sticks
  - ...
- Systempartition


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

Über VeraCrypt (2)

Vorteile

- Quelloffen, freie Software
- Nachvollziehbare Änderungen am Code
- Plattformübergreifend
- Auf USB-Stick transportierbar
- Unabhängiger Audit

Nachteile

- Komfortverlust
- Passwortverlust = Datenverlust

Umgang mit VeraCrypt

- Was will ich verschlüsseln?
- Sicheres Passwort wählen
- Adminrechte notwendig
- Vorsicht bei fremden Geräten!
- Generell: Benutzerhandbuch zu VeraCrypt lesen

➔ Größtes Sicherheitsrisiko ist fast immer der Nutzer!

Alternativen

- **dm-crypt** (Teil des Linux-Kernels ab Version 2.6)
  - z.B. Ubuntu und Mint erlauben Systemverschlüsselung bei Installation
- **7-Zip**: freie Software, unterstützt AES256-Verschlüsselung für 7z-Archive

- Nicht vertrauenswürdig, da nicht quelloffen:
  - Windows: **BitLocker** (ab Vista, nur bei teuren Windows-Versionen)
  - MacOS: **FileVault**
  - Zahllose weitere kommerzielle Produkte

Rechtliches

- Deutschland: Kein Zwang zur Herausgabe eines Passworts/Schlüssels bei möglicher Selbstbelastung
- Vorsicht im Ausland:
  - Großbritannien: Pflicht zur Herausgabe (→ RIPA), auch Beugehaft möglich!
  - USA: Ein- und Ausreise mit verschlüsselten Datenträgern problematisch