

Cryptocafé

Digitale Selbstverteidigung für Einsteigerinnen und Einsteiger

Christian Widmann

digital**courage** e.V., Ortsgruppe München

Ablauf

- ▶ Einleitung
 - ▶ Digitale Mündigkeit
 - ▶ Digitale Selbstverteidigung gegen ...
 - ▶ Dinge, die wir sofort gemeinsam umsetzen können
 - ▶ Am Wochenende könnte ich ...
 - ▶ Bis Juni kann ich sogar ...
 - ▶ Dreamline: „schwarzer Gürtel“ bis zum Jahresende
-
- ▶ Fragen, fragen, fragen. :-)

Disclaimer

▶ **Es gibt keine 100%-ige Sicherheit**

- ▶ Unbekannte Softwarefehler
- ▶ Falsches Nutzungsverhalten
- ▶ Aufwand des Angreifenden
- ▶ fehlende Updates
- ▶ ...

▶ Keine Beratung zu individueller Überwachung!

▶ „Nerdgespräche“ im Anschluss

▶ Fokus auf freier OpenSource Software

▶ Offener Quellcode, d.h. überprüfbar

▶ Freie Verbreitung und Veränderung

Digitalcourage e.V.

- ▶ Gegründet 1987
- ▶ Bürgerrechte, Datenschutz
- ▶ Engagement für eine lebenswerte Welt im digitalen Zeitalter und eine lebendige Demokratie
- ▶ Technik und Politik kritisch erkunden und menschenwürdig gestalten
- ▶ gemeinnützig, **finanziert sich durch private Spenden** und lebt durch die Arbeit vieler Freiwilliger



Fabian Kurz (CC-BY 2.0)

- ▶ Sitz: Bielefeld
- ▶ Ortsgruppen: Berlin, Bielefeld, Braunschweig, Bremen, München

Digitale Mündigkeit



CC BY SA 2.0

Digitale Mündigkeit

- ▶ Wenn du nichts bezahlst, bist du die Ressource, die ausgebeutet wird, um sie zu einem Produkt für die Werbeindustrie zu formen.



CC BY SA 4.0

Digitale Mündigkeit

- ▶ Sapere aude!
- ▶ Habe Mut, dich deines eigenen Verstandes zu bedienen!
- ▶ Immanuel Kant, 1784



I.Kant.

Digitale Mündigkeit

- ▶ Mündig sein bedeutet, Verantwortung für das eigene Leben und für den Fortbestand unserer Gesellschaft zu tragen.
- ▶ Mündigkeit ist Übungssache!
- ▶ Maschinen machen Fehler
- ▶ Algorithmen sind nicht perfekt
- ▶ Abweichung vom „digitalen Zwilling“



I.Kant.

Digitale Selbstverteidigung gegen ...

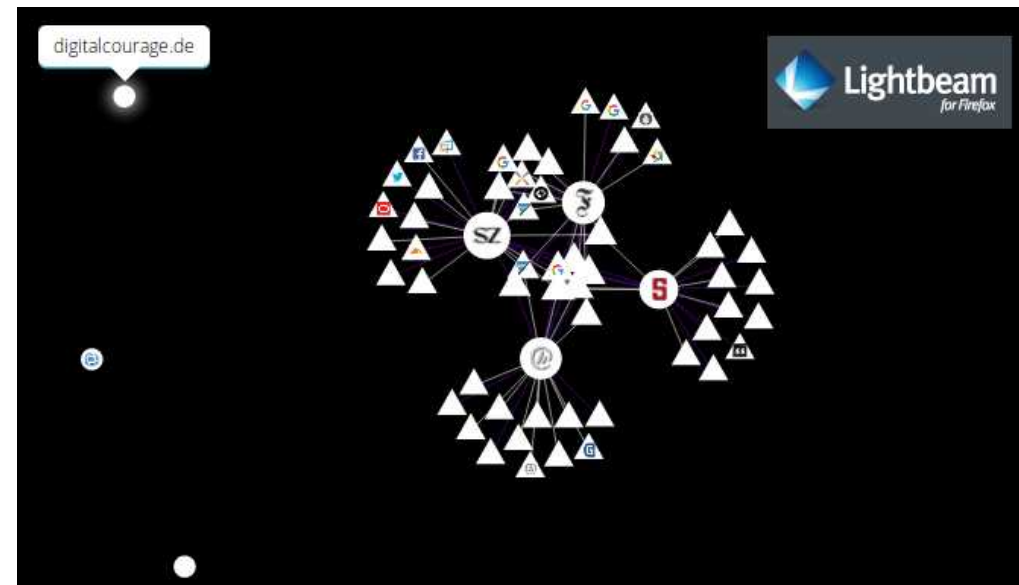
- ▶ (Kommerzielle) Überwachungsindustrie
 - ▶ Personalisierte Werbung
 - ▶ Einfallstor für Schadprogramme
 - ▶ Verlangsamung von Seitenaufrufen & höheres Datenaufkommen
 - ▶ Optische & akustische Zumutung
 - ▶ Personalisierte Profile (Profiling)
 - ▶ Verlust der Souveränität (wer hat welche Daten über mich und setzt sie wie (gegen mich) ein?)
 - ▶ Meist illegal, Verstoß gegen DSGVO
 - ▶ Bedrohung der Menschenrechte und Demokratie
- ▶ Große Digitalunternehmen (Google, Amazon, Facebook, Apple, Microsoft – GAFAM)
 - ▶ Kampf um Aufmerksamkeit, Microtargeting
- ▶ „Vendor-Lockin“: Netzwerkeffekt
- ▶ Ziel: Rückerlangung der digitalen Souveränität



Digitale Selbstverteidigung gegen ...

- ▶ Google weiß mehr als uns lieb ist
 - ▶ Suchanfragen
 - ▶ Analytics
 - ▶ Fonts
 - ▶ Maps
 - ▶ Android
 - ▶ Gmail
 - ▶ ...

- ▶ Sichtbarmachung: Lightbeam





DATA GATHERED SINCE FEB 07 2021
YOU HAVE VISITED 4 SITES
YOU HAVE CONNECTED WITH 158 THIRD PARTY SITES

TRACKING PROTECTION OFF

VISUALIZATION

Graph

DATA

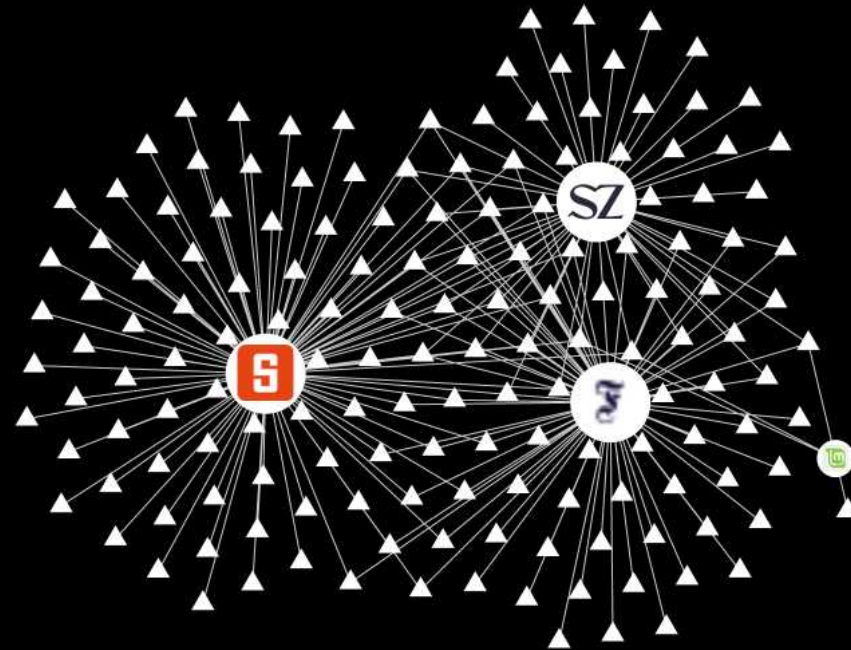
Save Data

Reset Data

Give Us Feedback

Recent Site

GRAPH VIEW





DATA GATHERED SINCE: FEB 07 2021
YOU HAVE VISITED: 3 SITES
YOU HAVE CONNECTED WITH: 11 THIRD PARTY SITES

TRACKING PROTECTION OFF

VISUALIZATION

Graph

Recent Site

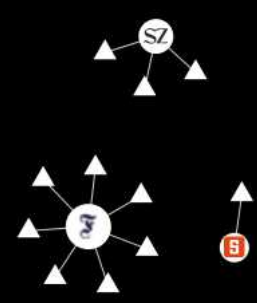
GRAPH VIEW

DATA

Save Data

Reset Data

[Give Us Feedback](#)



Sofortmaßnahmen

- ▶ Browser wechseln: Mozilla Firefox
 - ▶ <https://www.mozilla.org/de/firefox/new/>
- ▶ Mobil: Fennec, Bromite oder iCab Mobile (iOS).
- ▶ Addons (Einstellungen → Addons):
 - ▶ uBlock origin: Web filter (Werbung, Schriftarten u.v.m.)
 - ▶ Noscript: JavaScript blocker



Sofortmaßnahmen

- ▶ Firefox Einstellungen:
 - ▶ Startseite: abschalten von externen Inhalten
 - ▶ Suche: Startpage, Duckduckgo, Metager, Searx, ...
 - ▶ Datenschutz & Sicherheit: Streng
 - ▶ **Cookies von Drittanbietern und den ganzen Rest blockieren**
 - ▶ „Do Not Track“ Information immer senden
 - ▶ **Cookies und Website-Daten beim Beenden löschen**
 - ▶ Chronik benutzerdefiniert anlegen und löschen beim Beenden



In Einstellungen suchen

- Allgemein
- Startseite
- Suche
- Datenschutz & Sicherheit
- Sync

https://www.startpage.com/

Aktuelle Seite verwenden | Lesezeichen verwenden...

Neue Tabs

Firefox-Startseite (Standard)

Inhalte des Firefox-Startbildschirms

Wählen Sie, welche Inhalte auf Ihrem Firefox-Startbildschirm angezeigt werden sollen.

- Internetsuche**
- Wichtige Seiten**
Die von Ihnen am meisten besuchten Websites 1 Zeile
- Empfohlen von Pocket** [Wie es funktioniert](#)
Besondere Inhalte aus dem ganzen Internet, ausgewählt von Pocket
 - Gesponserte Inhalte
- Überblick**
Eine Auswahl von Websites, die Sie gespeichert oder besucht haben 1 Zeile
 - Besuchte Seiten
 - Lesezeichen
 - Neueste Downloads
 - Bei Pocket gespeicherte Seiten
- Kurzinformationen**
Neuigkeiten von Mozilla und Firefox

- Erweiterungen & Themes
- Hilfe für Firefox

⚙ Allgemein

🏠 Startseite

🔍 Suche

🔒 **Datenschutz & Sicherheit**

🔄 Synchronisation

🦊 Mehr von Mozilla

📦 Erweiterungen & Themes

❓ Hilfe für Firefox

Browser-Datenschutz

Verbesserter Schutz vor Aktivitätenverfolgung



Skripte zur Aktivitätenverfolgung folgen Ihnen und sammeln Informationen über Ihre Internet-Gewohnheiten und Interessen. Firefox blockiert viele dieser Skripte zur Aktivitätenverfolgung und andere böswillige Skripte. [Weitere Informationen](#)

[Ausnahmen verwalten...](#)

Standard

Ausgewogen zwischen Schutz und Leistung. Seiten laden normal.

Streng

Stärkerer Schutz, einige Websites oder mancher Inhalt funktioniert eventuell nicht.

Firefox blockiert Folgendes:

- Skripte zur Aktivitätenverfolgung durch soziale Netzwerke
- Seitenübergreifende Cookies in allen Fenstern
- Inhalte zur Aktivitätenverfolgung in allen Fenstern
- Heimliche Digitalwährungsberechner (Krypto-Miner)
- Identifizierer (Fingerprinter)

⚠ Achtung!

Diese Einstellung kann dazu führen, dass einige Websites nicht korrekt Inhalte anzeigen oder funktionieren. Wenn eine Website defekt zu sein scheint, können Sie den Schutz vor Aktivitätenverfolgung für diese Website deaktivieren, um alle Inhalte zu laden. [Weitere Informationen](#)

In Einstellungen suchen

- Allgemein
- Startseite
- Suche
- Datenschutz & Sicherheit**
- Sync

Websites eine "Do Not Track"-Information senden, dass die eigenen Aktivitäten nicht verfolgt werden sollen
[Weitere Informationen](#)

Immer
 Nur wenn Firefox bekannte Elemente zur Aktivitätenverfolgung blockieren soll

Cookies und Website-Daten
Die gespeicherten Cookies, Website-Daten und der Cache belegen derzeit 1,1 GB Speicherplatz. [Weitere Informationen](#)

Cookies und Website-Daten beim Beenden von Firefox löschen

Zugangsdaten und Passwörter

Fragen, ob Zugangsdaten und Passwörter für Websites gespeichert werden sollen

Zugangsdaten und Passwörter automatisch ausfüllen
 Starke Passwörter erzeugen und vorschlagen
 Alarme für Passwörter, deren Websites von einem Datenleck betroffen waren [Weitere Informationen](#)

Hauptpasswort verwenden [Weitere Informationen](#)
Früher bekannt als Master-Passwort

Chronik
Firefox wird eine Chronik nach benutzerdefinierten Einstellungen anlegen

Immer den Privaten Modus verwenden

Besuchte Seiten und Download-Chronik speichern
 Eingegebene Suchbegriffe und Formulare Daten speichern
 Die Chronik löschen, wenn Firefox geschlossen wird

Daten entfernen...
Daten verwalten...
Ausnahmen verwalten...
Ausnahmen...
Gespeicherte Zugangsdaten...
Hauptpasswort ändern...
Chronik leeren...
Einstellungen...

Einstellungen für das Löschen der Chronik

Wenn Firefox beendet wird, folgende Daten automatisch löschen:

Chronik

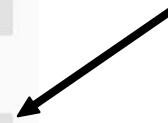
Besuchte Seiten & Download-Chronik
 Aktive Logins
 Eingegebene Suchbegriffe & Formulare Daten

Cookies
 Cache

Daten

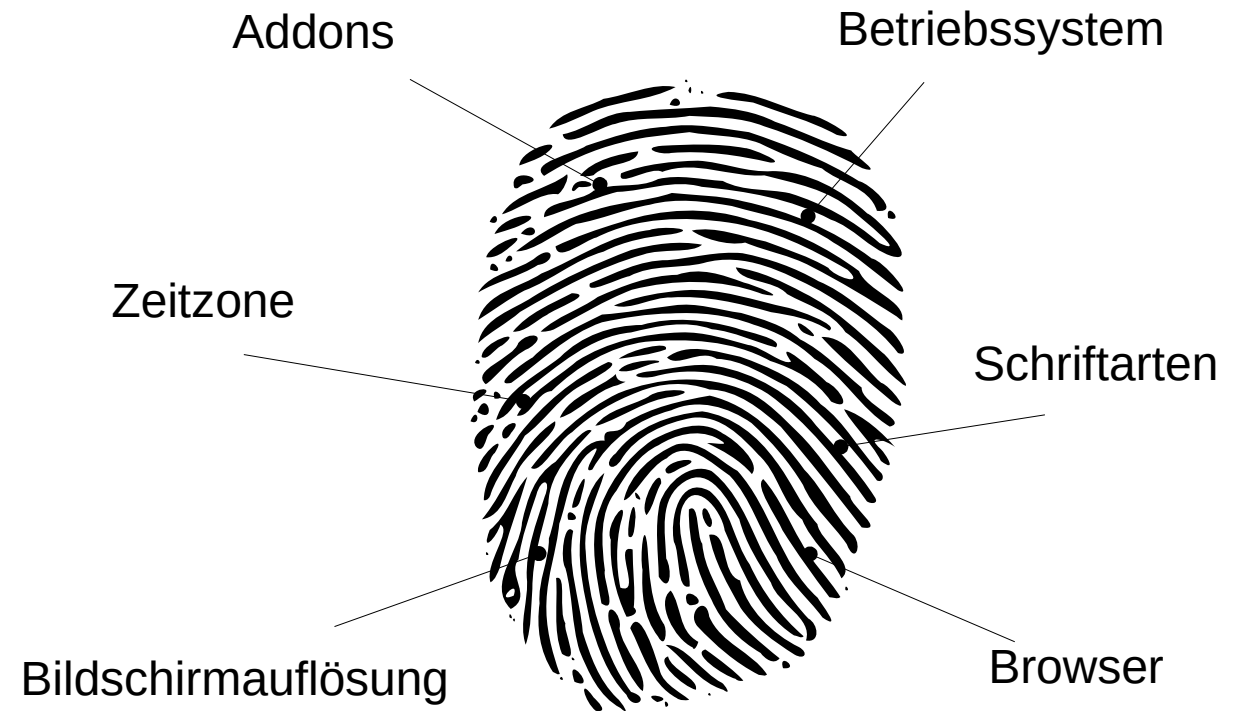
Website-Einstellungen
 Offline-Website-Daten

Hilfe Abbrechen **OK**



Sofortmaßnahmen

- ▶ Browser Fingerprint:
 - ▶ Mehrere Eigenschaften zusammen ergeben ein genaueres Profil
 - ▶ <https://coveryourtracks.eff.org/>
- ▶ Schutz:
 - ▶ Javascript blockieren
 - ▶ „einheitliche“ Browser nutzen, z.B. TOR Browser, Safari
 - ▶ Mehrere verschiedene Browser nutzen
- ▶ Mobil: Advertising ID
 - ▶ Eindeutige Kennung über Apps hinweg ermöglicht detaillierte Überwachung
 - ▶ Regelmäßig zurücksetzen
 - ▶ Alternative Betriebssysteme ohne ID nutzen, z.B. LineageOS

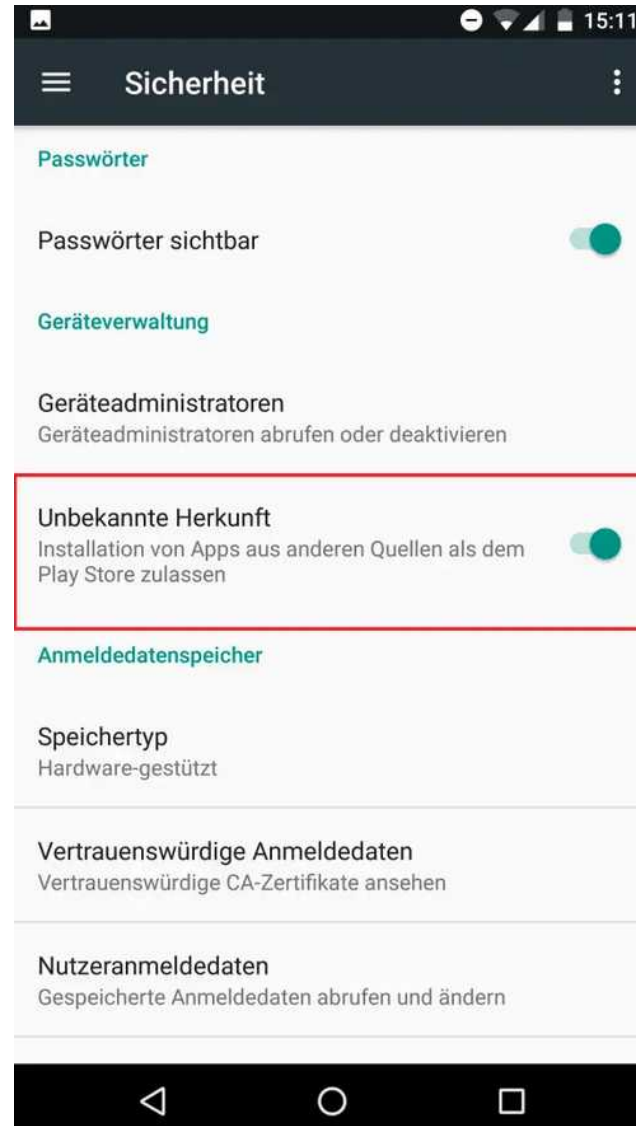


Von Wilfredor - Eigenes Werk, CC BY-SA 3.0

Sofortmaßnahmen

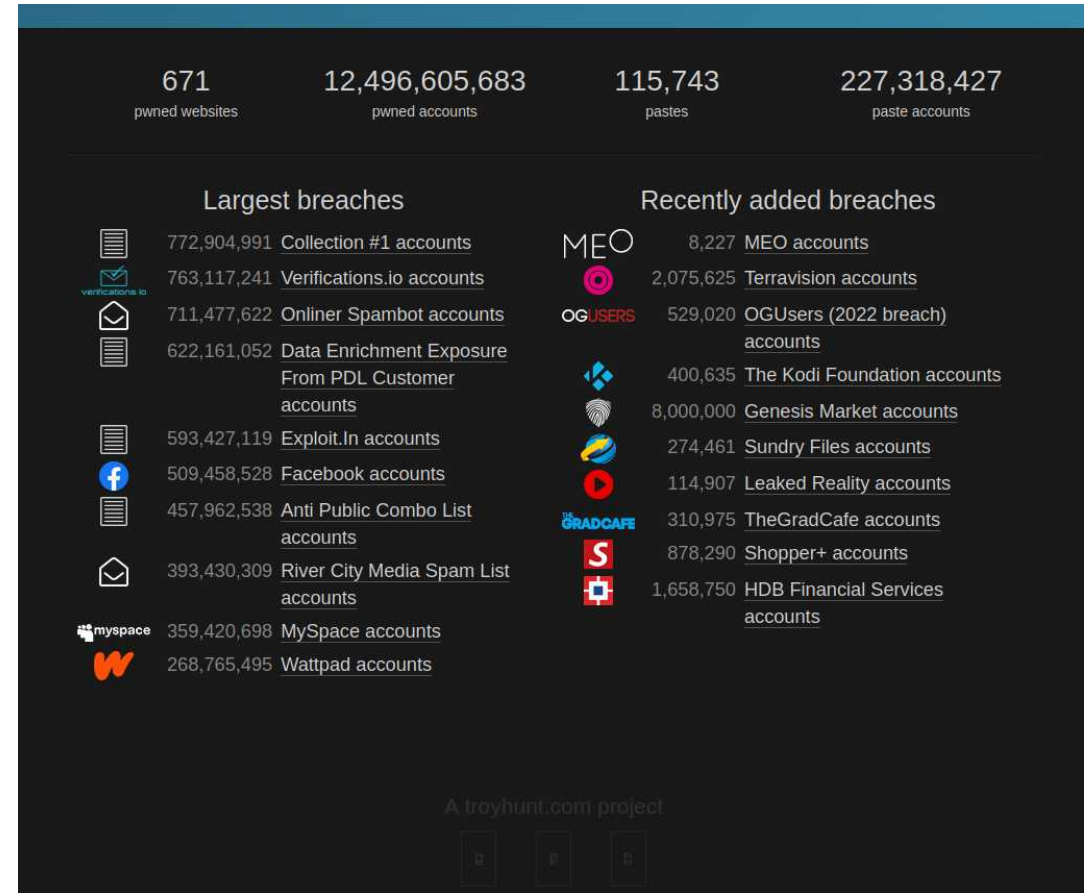
- ▶ Problem an Apps von Apple/Google/Microsoft Stores:
 - ▶ Sehr viele bauen auf vorhandener Funktionalität auf und beinhalten Tracker (z.B. Facebook SDK in 42 %)
 - ▶ Permanentes Ausbeuten von Daten (Account?)
- ▶ Lösung: F-Droid (nur Android)
 - ▶ Nur Freie Open Source Software ohne Tracker
 - ▶ <https://f-droid.org/de/>
 - ▶ „Apps aus unbekannter Herkunft“ erlauben
 - ▶ Liste mit Empfehlungen: <https://digitalcourage.de/digitale-selbstverteidigung/freie-apps-fuer-das-befreite-smartphone>





Am Wochenende könnte ich ...

- ▶ ... meine Passwortstrategie überarbeiten!
- ▶ Über 12 Mrd. Nutzerkonten betroffen, bestimmt auch Du!
- ▶ <https://haveibeenpwned.com>
- ▶ Eigene Email eingeben und herausfinden, ob eigene Zugangsdaten in Vergangenheit bereits leaked wurden.



Am Wochenende könnte ich ...

- ▶ Häufigste Passwörter: 123456, qwerty, 123abc, password ...
- ▶ Ausprobieren, ob selbe Zugangsdaten (Email + Passwort) auch bei anderen Diensten funktionieren



Sichere Passwörter

- ▶ *Goldene Regel: Unterschiedliche Passwörter für jeden Zugang (!!!)*
- ▶ Mind. 14 Zeichen, verschiedene Zeichentypen (A-Z, a-z, 0-9, /*~ ...), z.B. `:Rj/T23Sy2KhiqX[^ncR_nk``
- ▶ Lang genug, um Brute Force Angriffen (Ausprobieren aller Kombinationen) stand zu halten
- ▶ **Kein** Bezug zur Person (z.B. Geburtstag, Name des Hundes)
- ▶ **Niemals** im Klartext (unverschlüsselt) weitergeben
- ▶ Passwörter **nicht** direkt neben dem PC aufbewahren



Sichere Passwörter

▶ Merksätze:

Meine Katze hat 7 Leben, davon 5 bereits aufgebraucht und spielt gerne mit Wolle.

→ MKh7L,d5bausgmW.



Alvesgaspar / CC BY-SA

Sichere Passwörter

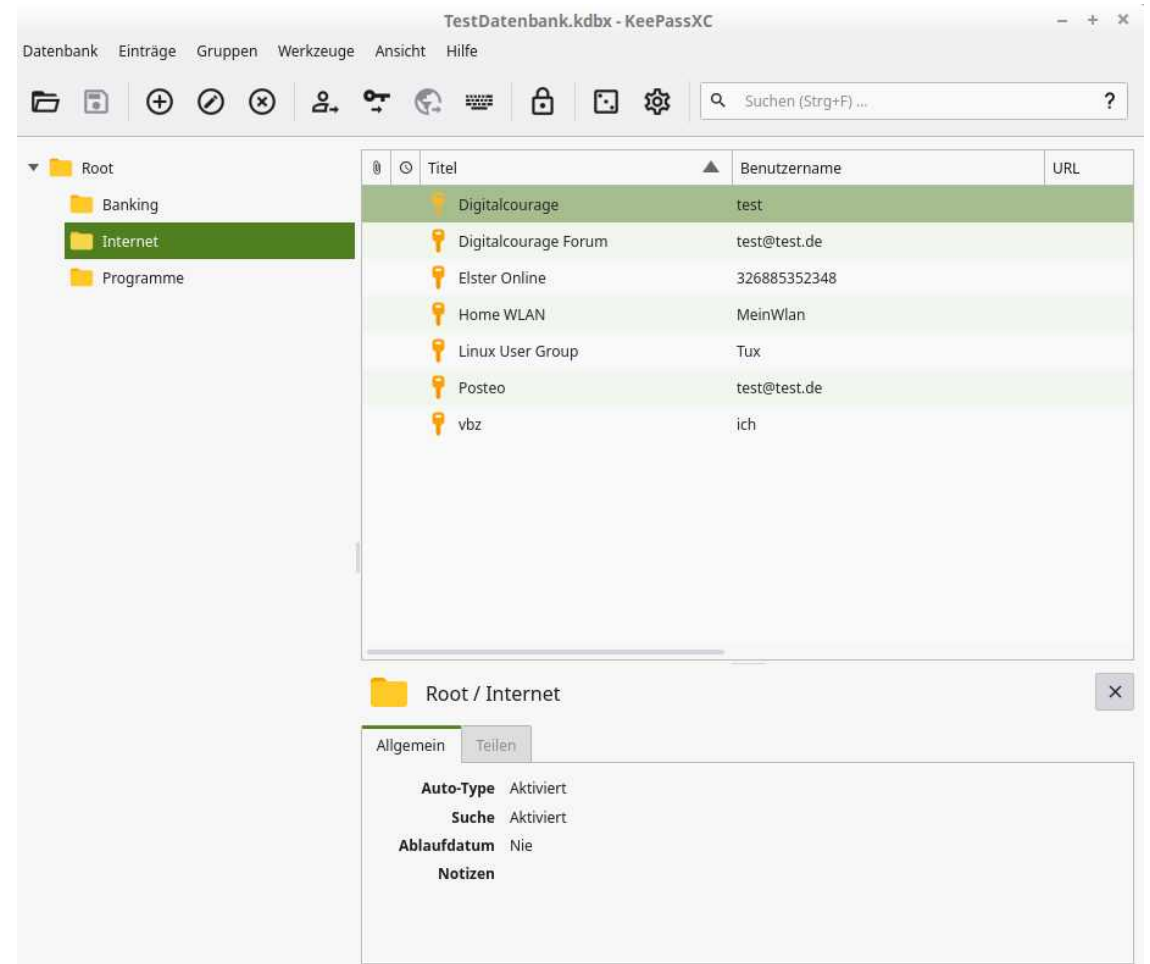
- ▶ Wortreihungen („Würfel“):
 - ▶ Vorhandene Liste mit 66666 Wörtern und Zeichenfolgen:
 - ▶ world.std.com/~reinhold/diceware_german.txt
 - ▶ Einen Würfel fünf Mal würfeln (z.B. 43142), entsprechendes Wort nachschlagen
 - ▶ Das ganze sechs Mal wiederholen

43142	merken
15613	boom
22543	ekd
66445	zonen
51615	ragt
32644	hurra

→ merkenboomekdzonenragthurra

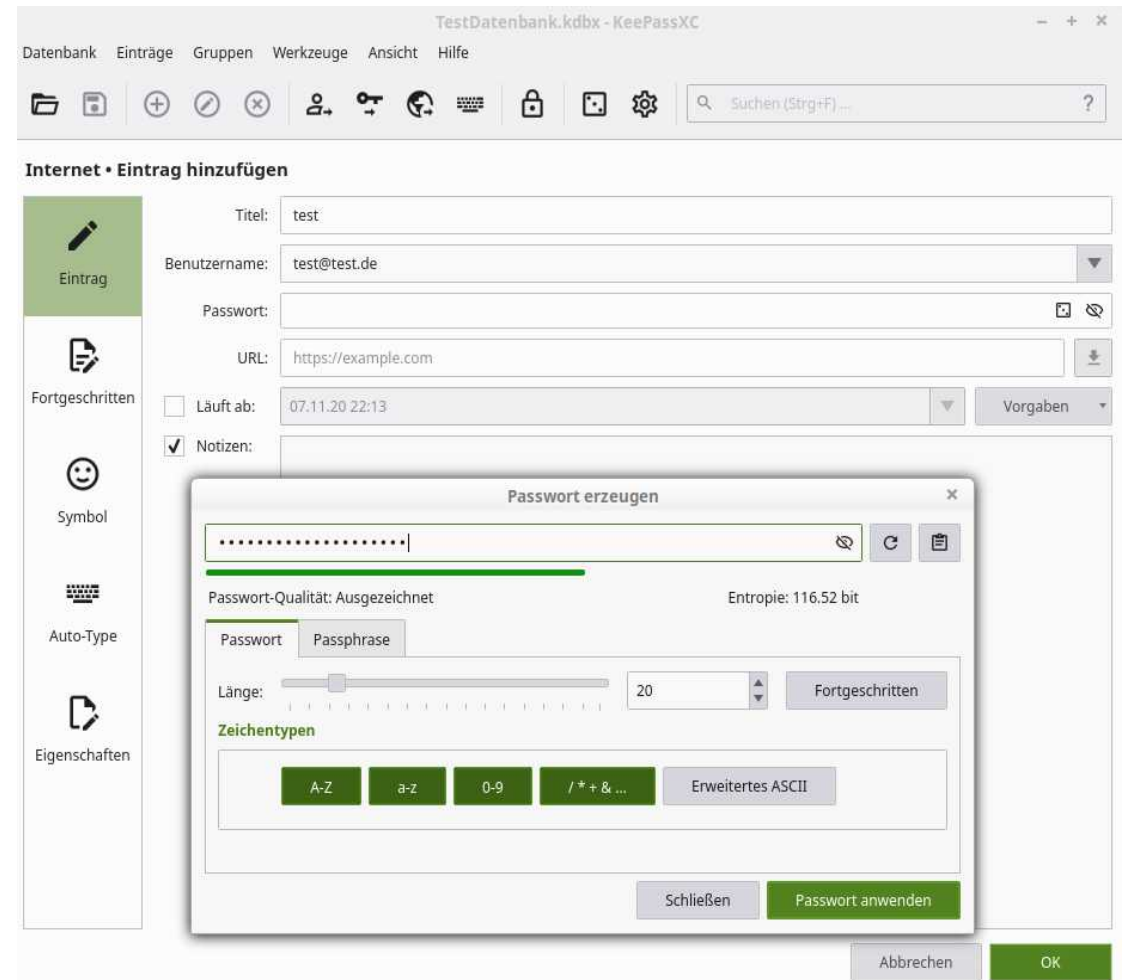
Strategien zum Erstellen und Merken

- ▶ Passwortmanager (z.B. KeePassXC am PC, KeePassDX für Android, KeePassium für iOS)
 - ▶ Ein „Safe“ für alle Passwörter
 - ▶ Verschlüsselte Datei
 - ▶ Sehr starkes Passwort zur Sicherung!
 - ▶ Enthält Passwortgenerator
 - ▶ Produziert sehr starke Passwörter und speichert sie übersichtlich
 - ▶ Leicht zu ändernde Passwörter



Sichere Passwörter

- ▶ Fazit:
 - ▶ Nur 2 sehr starke Passwörter zu merken (Betriebssystem + Passwortsafe)
 - ▶ Restliche sehr starke Passwörter im Passwortsafe verschlüsselt
 - ▶ Unterschiedliche Passwörter für jeden Zugang!



Sicher Passwörter: Zusätzliche Hilfsmittel

- ▶ Automatisches Ausfüllen (bei entsperrtem Safe):
 - ▶ Auto-Type
 - ▶ KeePassXC-Browser
- ▶ Mobil: KeePassDX
 - ▶ Magikeyboard
 - ▶ AutoFill
- ▶ Synchronisation von Endgeräten
 - ▶ Syncthing (auch lokal!)
 - ▶ WebDAV
 - ▶ Achtung:
 - ▶ Müssen alle Passwörter mobil verfügbar sein?
 - ▶ Geräteverschlüsselung + sicherer PIN!



Bis Juni kann ich sogar ...

- ▶ ... meine Kommunikation absichern!
- ▶ E-Mail:
 - ▶ Datenschutzfreundlichen Anbieter wählen (z.B. posteo.de oder mailbox.org)
 - ▶ Auf keinen Fall Freemailer (gmail, gmx, web, freenet, ...)
 - ▶ E-Mails nur noch über einen Client wie Thunderbird schreiben (mobil: K9-Mail)
 - ▶ Ende-zu-Ende Verschlüsselung einrichten, z.B. Thunderbird (mobil: K-9 Mail & OpenKeychain)
 - ▶ <https://digitalcourage.de/digitale-selbstverteidigung/e-mail-verschluesselung>



Bis Juni kann ich sogar ...

- ▶ ... meine Kommunikation absichern!
- ▶ Messenger:
 - ▶ Kompromiss zwischen gutem Datenschutz, Komfort und Verbreitung
 - ▶ Element (Matrix):
 - ▶ Viel Freiheit und Privatsphäre, weniger Verbreitung
 - ▶ Dezentrale Struktur, ähnlich Email
 - ▶ E2E Verschlüsselung nach Signal Standard
 - ▶ Alternativen: XMPP (Jabber), Briar
 - ▶ Signal: hohe Verbreitung und bequeme Einrichtung, allerdings Abstriche im Datenschutz
 - ▶ Telefonnummer zur Identifikation
 - ▶ Adressbuch wird auf zentralen Server hochgeladen
 - ▶ Alternativen: Threema, Wire



Bis Juni kann ich sogar ...

- ▶ ... meine Dienste und Apps überdenken!
- ▶ Navigation:
 - ▶ Osmand, Openstreetmap, openrouteservice, brouter statt GoogleMaps
 - ▶ Öffi oder Transportr statt DB Navigator
- ▶ Terminfinder:
 - ▶ Nuudel statt doodle
- ▶ „Social“ Media:
 - ▶ Mastodon, GNU social und Twidere statt Facebook und Twitter
- ▶ Cloud-Dienste:
 - ▶ Owncube, Nextcloud, SpiderOak, Your Secure Cloud statt Dropbox, Google Drive, OneDrive oder iCloud
- ▶ **Nicht vergessen: Konto bei Google, Facebook etc. löschen ;-)**



▶ digital**courage**

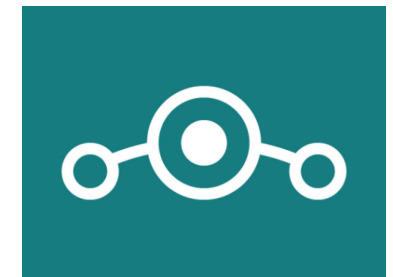
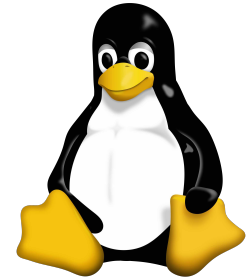
Dreamline: „schwarzer Gürtel“ bis Jahresende



CC-BY-SA 4.0, Oliver Hinzmann

Dreamline: „schwarzer Gürtel“ bis Jahresende

- ▶ Freie Betriebssysteme auf den Geräten installieren:
 - ▶ Mobil: LineageOS
 - ▶ Am PC: Linux (z.B. Ubuntu oder Mint)
- ▶ Unsichere Apps mit Shelter isolieren
- ▶ Ausgehenden Traffic mit Firewall blockieren, z.B. NetGuard, AFWall+
- ▶ Selbst oder mit Kollegen/Freunden eigene Cloud-Dienste hosten („Die Zukunft ist dezentral.“)
- ▶ Spendenliste für verwendete OpenSource Software anlegen
- ▶ Digitalcourage Mitglied werden
- ▶ Digitale Souveränität erlangen und zum Multiplikator werden



Nächste Termine

- ▶ 16. Mai 2023: Cryptocafé @ Verbraucherzentrale Bayern um 18:00 Uhr, Mozartstr. 9, 80336 München
- ▶ Jeden 1. Montag in geraden Monaten (z.B. 05. Juni 2023): digitalcourage @ Radio Lora um 19:00 Uhr
- ▶ Jeden 2. Montag in ungeraden Monaten (z.B. 08. Mai 2023): offenes Treffen der Ortsgruppe um 19:00 Uhr @ Stragula, Bergmannstraße 66, 80339 München

Weiterführende Materialien

- ▶ **digitalcourage** – Digitale Selbstverteidigung
 - ▶ <https://digitalcourage.de/digitale-selbstverteidigung>
- ▶ Anleitungen und Erklärungen für Mobilgeräte
 - ▶ <https://mobilsicher.de>
- ▶ Mike Kuketz – Smartphones & Datenschutz
 - ▶ <https://kuketz-blog.de>
- ▶ Security in a Box – Werkzeuge und Taktiken
 - ▶ <https://securityinabox.org/en/> [EN]
- ▶ My Shadow – Wie funktioniert Tracking?
 - ▶ <https://myshadow.org/> [EN]
- ▶ Surveillance Self-Defense (EFF) – Sicherheitstutorials sortiert nach Anforderungen
 - ▶ <https://ssd.eff.org> [EN]