Lernlabor: Digital privat bleiben

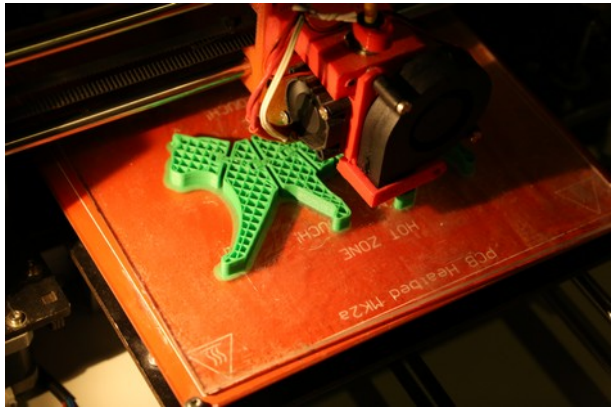
z-Labor Zwickau e.V. in Kooperation mit

WHZ Westsächsische Hochschule Zwickau
Hochschule für Mobilität

19.03.2025

z-Labor e.V.

- gemeinnütziger Hackspace
- Chaostreff in der Kulturweberei Zwickau
- für technikbegeisterte Lebewesen



Wer sind wir?

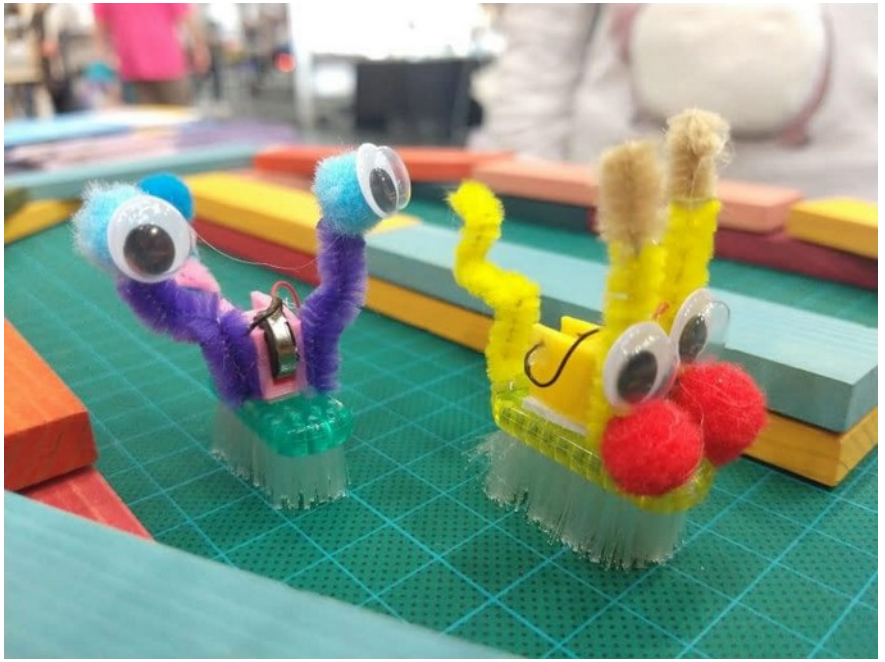
Themen/Projekte

- Wir mögen Elektronik, Netzwerktechnik und Programmierung, (Kunst-)Handwerk, Siebdruck, 3D-Druck und (Analog-)Fotografie, Musikinstrumente, Birds, Isopoden
- Es gibt Lötstationen, eine Holz- und Metallwerkstatt sowie ein Fotolabor
- Chemie-Ecke mit Kunstharzen, Utensilien zur Leiterplattenherstellung und Fotochemie sind vorhanden

Wer sind wir?

Themen

- Wir lieben Freie Software (meist)
- veranstalten Workshops, Spiele- und Filmabende sowie Löt- und Bastelworkshops für Kinder und alle anderen



Wer sind wir?

Räumlichkeiten des z-Labors

Wer sind wir?

Was machen wir sonst so

Computertruhe e. V.

freifunk.net

Wer sind wir?

Kontakt

- Öffentlicher Treff **Donnerstags ab 19 Uhr**
  Seilerstraße 1, Haus C, Box 39, 08056 Zwickau
- **Per Mail:**
  info@z-labor.space
- **Webseite:**
  https://www.z-labor.space
- **Matrix:**
  https://matrix.to/#/#public:z-labor.space
- **Mastodon**
  https://chaos.social/@zLabor
- **Codeberg**
  https://codeberg.org/z-labor

Nichts zu verbergen?

Referentin: exe
z-Labor Zwickau e.V.

Nichts zu verbergen?

Keine Woche ohne Pannen

USA: Falsch konfigurierter Server legt sensible Daten von Pflegekräften offen

Ein falsch konfigurierter Cloudspeicher ermöglichte den Zugriff auf Daten von zehntausenden Pflegefachkräften, die eine App zur Schichtenbesetzung nutzten.

12.03.2025 10:56 Uhr 22 | heise Security

Datenleck im Ludwigsburger Klinikum: Fast 200 Patienten betroffen

von **Philipp Schneider** | 14.03.2025, 05:00 Uhr

IT-SICHERHEITSLÜCKE

Datenleck D-Trust: Auch Zahnärzte und Justiz betroffen

10. Februar 2025, 12:17 Uhr

19.10.2009 14:37

Unbekannte lesen mit

Datenpanne bei Google Docs

Sicherheitsleck bei Google Docs: Laut einem Fernsehbericht werden bei Googles Dienst "Text und Tabellen" Dokumente freigegeben, die eigentlich privat bleiben sollten.

Nichts zu verbergen?

Datenpannen, Hackerangriffe, Überwachungsskandale

Disney-Fans aufgepasst: Phishing-Mail an Streaming-Kunden im Umlauf

Artikel von Annika Danielmeier • 4Tage • 2 Minuten Lesezeit

Smartphone-Sicherheit

Banking-Trojaner boomen – Angriffe haben sich verdreifacht

04. März 2025, 08:06

Einschüchterungs-Masche

FBI warnt vor Ransomware-Erpressung per Brief

Cyber-Erpresser, die ihre Forderungen per normaler Briefpost an die vermeintlich betroffenen Firmen schicken? Klingt merkwürdig und ist es auch: Das FBI rät zur Vorsicht.

07.03.2025, 14.30 Uhr

Datenleck-Such-Website Have I Been Pwned um 284 Millionen Accounts aufgestockt

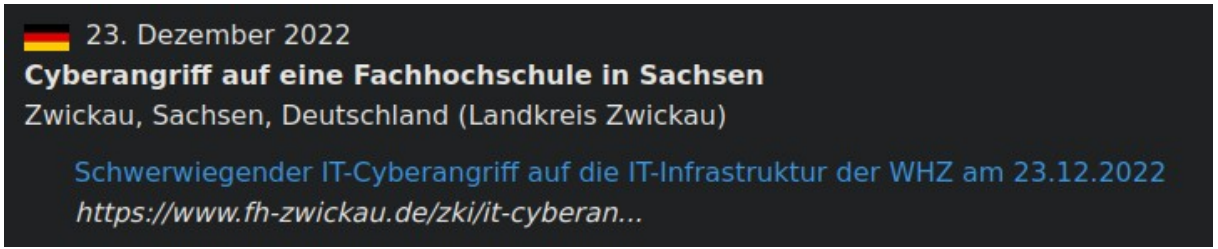
Im Telegram-Kanal ALIEN TXTBASE wurden von Infostealer-Malware erbeute Mailadressen und Passwörter geteilt. Diese Daten sind nun in HIBP integriert.

26.02.2025 | heise Security

Nichts zu verbergen?

Top-Angriffsarten

- Malware, Phishing, Spoofing, DDoS, Ransomware, Spionage
- 9 von 10 Unternehmen betroffen
- Ransomware as a service
- 37c3: Hirne Hacken (Linus Neumann)



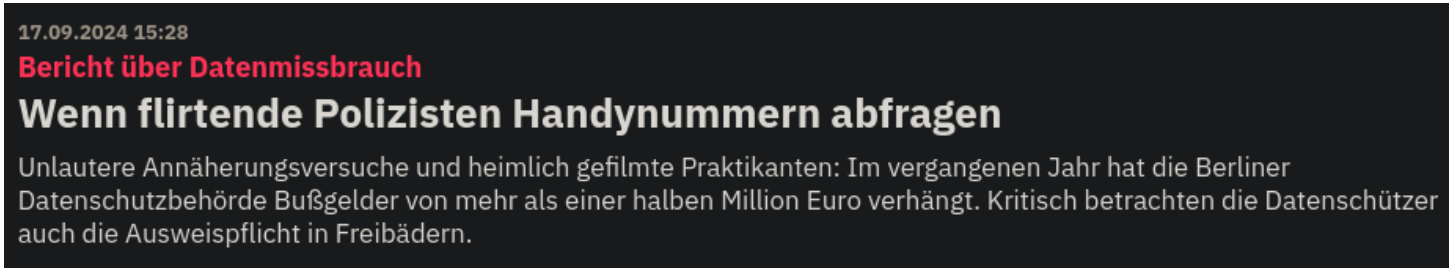
Cloud-Act der USA

- erlaubt US-Behörden den Zugriff auf im Ausland gespeicherte Daten
- europäische Dienste bevorzugen

Problemgewehr G36

Geheimdienst MAD sollte kritische Journalisten ausspähen

Geheime Akten über das G36 beschreiben eine brisante Kumpanei: Verteidigungsministerium und Hersteller wollten den Geheimdienst MAD dazu bringen, negative Berichte über das Bundeswehrgewehr zu verhindern. Im Visier waren auch Journalisten von SPIEGEL und SPIEGEL ONLINE.



17.09.2024 15:28

Bericht über Datenmissbrauch

Wenn flirtende Polizisten Handynummern abfragen

Unlautere Annäherungsversuche und heimlich gefilmte Praktikanten: Im vergangenen Jahr hat die Berliner Datenschutzbehörde Bußgelder von mehr als einer halben Million Euro verhängt. Kritisch betrachten die Datenschützer auch die Ausweispflicht in Freibädern.

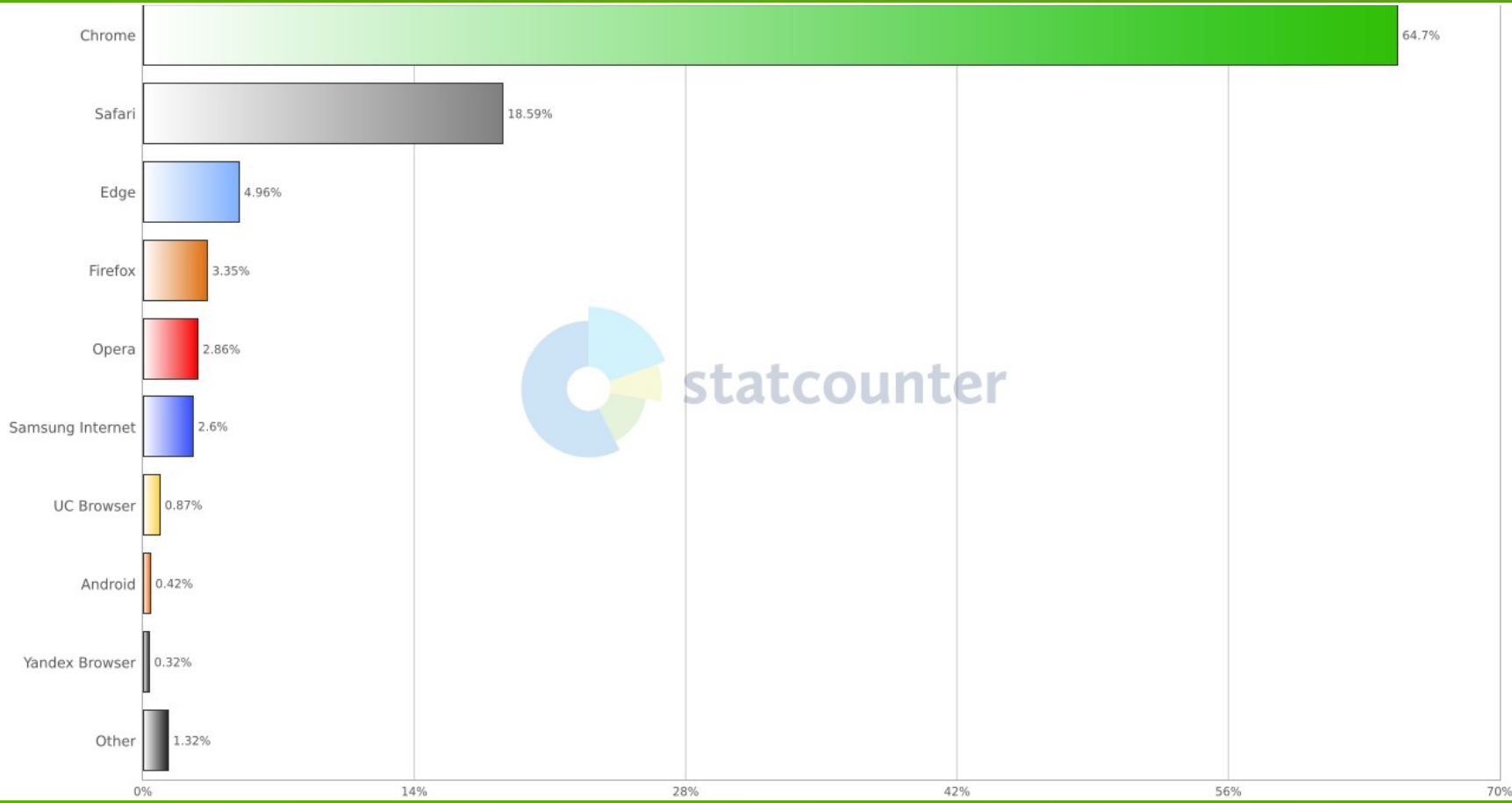
Nichts zu verbergen?

Freie Software

- freie Software, die für alle zugänglich, replizierbar und veränderbar ist
- Quellcode ist offen und frei für jeden einsehbar
- Schwachstellen fallen häufiger auf
- gute Standards werden etabliert
- **bekannte FOSS-Software:**
  - Wordpress
  - Gimp
  - Firefox
  - Android

Webbrowser

Übersicht [1]



Browser Marktanteile

Dezember 2023

Quelle: StatCounter Global Stats

Webbrowser

Übersicht [2] Web Engines

Blink/Chromium

Webkit

Gecko

Webbrowser

Übersicht [3] Privatsphäre Funktionen

Browser	Datenschutzfreundlich	Schutz vor Tracking/Fingerprinting	Sicherheit	Website-Kompatibilität	Bemerkung
Brave (Desktop/Mobil)	nach Konfigurations-anpassung	Hoch, aufgrund diverser Techniken[1 2 3] und integriertem Blocker (adblock-rust)	Site-Isolation, Sandboxing-Maßnahmen auf dem Desktop und Mobil	hoch	Aufgeblasener Funktionsumfang, Kompromiss zwischen Sicherheit und Datenschutz
Firefox (Desktop/Mobil)	nach Konfigurations-anpassung	Gut, aufgrund diverser Techniken[4 5 6]	Site-Isolation auf dem Desktop, unter Android keine Site-Isolation, sondern lediglich App-Sandboxing	hoch	Wie auch Brave erst nach Konfigurationsanpassung datenschutzfreundlich, sicherheitstechnisch besteht Nachholbedarf
LibreWolf (Desktop)	als Grundeinstellung	Hoch, aufgrund diverser Techniken[4 5] in Kombination mit RFP[7] (Fallback auf FFP[6]) und integriertem Blocker (uBlock Origin)	Site-Isolation, verzögerte Bereitstellung von (Sicherheits-)Updates	gut, teilweise Probleme aufgrund RFP	Datenschutzfreundlich und hoher Trackingschutz, sofern ResistFingerprinting (RFP) aktiviert bleibt, Updates verzögert, für Durchschnittsnutzer ungeeignet
Tor-Browser (Desktop/Mobil)	als Grundeinstellung	Bester Schutz, da alle Nutzer des Tor-Browsers einheitlich erscheinen	Site-Isolation auf dem Desktop, unter Android keine Site-Isolation, sondern lediglich App-Sandboxing	noch okay, leider viele Captcha-Abfragen	Bester Schutz gegen User-Tracking, sofern keine Anpassungen in der about:config oder den Browsereinstellungen vorgenommen werden, für Durchschnittsnutzer ungeeignet
Mullvad-Browser (Desktop)	als Grundeinstellung	Bester Schutz (sofern VPN aktiv), da alle Nutzer des Mullvad-Browsers einheitlich erscheinen	Site-Isolation auf dem Desktop	gut, teilweise Probleme aufgrund RFP	Bester Schutz gegen User-Tracking, sofern keine Anpassungen in der about:config oder den Browsereinstellungen vorgenommen werden, für Durchschnittsnutzer ungeeignet, für hohen Tracking-Schutz muss VPN aktiv sein
Fennec (Mobil)	als Grundeinstellung	Gut, aufgrund diverser Techniken[4 5 6]	Keine Site-Isolation unter Android, sondern lediglich OS-Sandboxing, verzögerte Bereitstellung von (Sicherheits-)Updates	hoch	Datenschutzfreundlicher Firefox-Fork für Android, ähnliche Usability wie mit dem Original, leider Updates verzögert
Mull (eingestellt) IronFox (Mobil)	als Grundeinstellung	Hoch, aufgrund diverser Techniken[4 5] in Kombination mit RFP[7] (Fallback auf FFP[6])	Keine Site-Isolation unter Android, sondern lediglich App-Sandboxing	gut, teilweise Probleme aufgrund RFP	Datenschutzfreundlich und hoher Trackingschutz, sofern ResistFingerprinting (RFP) aktiviert bleibt, zeitnahe Updates, für Durchschnittsnutzer ungeeignet
Vanadium (Mobil)	als Grundeinstellung	Gering, Content-Blocker ausbaufähig	Höchste Sicherheit, Site-Isolation und zusätzliche Maßnahmen wie Control Flow Integrity (CFI) oder SSP-Konfiguration	hoch	Gehärteter Browser für höchste Sicherheitsansprüche, Nachholbedarf bei Anti-Tracking-Maßnahmen, nur für GrapheneOS verfügbar

Quelle: https://www.kuketz-blog.de/sichere-und-datenschutzfreundliche-browser-meine-empfehlungen-teil-1/

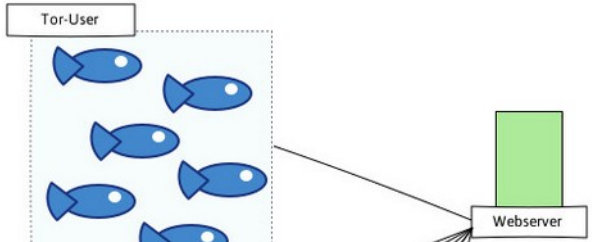
Der Tor Browser

Tor

Tor-Browser für sensible Recherchen und Kommunikation

- anonymes Surfen
- Anfragen werden verschlüsselt über drei ständig wechselnde Server geroutet
- ursprüngliche IP des Users wird verschleiert

- Spiegel:
  kxenegnp5vjtzfifupdaibxckguzitxyuqo2qoyj5riumorb54l3zdqd.onion



Quelle (Fische): https://www.kuketz-blog.de/vanadium-sichere-und-datenschutzfreundliche-android-browser-teil-6/

Datenarm surfen und leben

Suchmaschine & Add-Blocker

- Startpage
- Duckduckgo
- Open Street Map

- uBlock Origin

Open Source

Weitere Empfehlungen

- Nextcloud
- terminplaner.dfn.de
- Jitsi Meet, BBB
- Hedgedoc, Cryptpad
- Mastodon
- Mumble

HedgeDoc

Nextcloud

Open Source

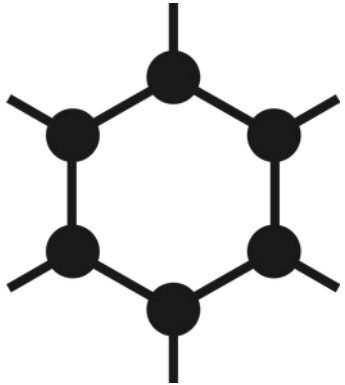
Weitere Empfehlungen 2

- VS Codium
- Joplin
- Darktable
- Inkscape
- Supertuxkart
- Smarttube

Datenschutz auf Mobilgeräten

Betriebssysteme

- Android: grundsätzlich freie Software
- aber: starke Abhängigkeit von Google & OEM
- Graphene OS
- Lineage OS
- MicroG, OpenGapps
- F-Droid-Store



- Signal
- Matrix mit Element / Schildichat

E-Mail

"E-Mail" was ist das?

- Asynchrones Kommunikationsmedium
- Neben dem WWW immer noch einer der wichtigsten Dienste im Internet

	2015	2016	2017	2018	2019
Worldwide Email Accounts (M)	**4,353**	**4,626**	**4,920**	**5,243**	**5,594**
%Growth		*6%*	*6%*	*7%*	*7%*
Worldwide Email Users* (M)	**2,586**	**2,672**	**2,760**	**2,849**	**2,943**
% Growth		*3%*	*3%*	*3%*	*3%*
Average Accounts Per User	1.7	1.7	1.8	1.8	1.9

Table 1: Worldwide Email Accounts and User Forecast (M), 2015–2019

Referent: zMa

E-Mail

Warum immer noch? [1]

...oder warum wir nicht davon los kommen.

...oder warum wir nicht davon los kommen.

- Höchster Verbreitungsgrad unter den persönlichen elektronischen Kommunikationsdiensten
- Sowohl im privaten als auch geschäftlichen Bereich akzeptiert
- Authentifikation für viele weitere Dienste/Plattformen erfordern häufig eine Email-Adresse

- Erweiterbar
  - Neben plain Text auch html möglich
  - Anhänge mit beliebigen Dateien

- Geräte/Betriebssystem unabhängig
  - Computer
  - Smartphones
  - Alarmanlagen/Türschlösser
  - Geräte der Netzwerkinfrastruktur wie Router und Switche
  - Glühlampen
  - Sextoys

...oder warum wir nicht davon los kommen
und warum wir das auch nicht sollten.

Dezentralität

- Keine zentrale Infrastruktur wie bei weit verbreiteten Instant-Messengern oder großen Plattformen im WWW
- Jeder kann einen eigenen Mailserver betreiben ohne bei jemandem um Erlaubnis zu fragen

E-Mail

Was läuft schief?

- Transport ist nicht zwingend und nicht automatisch verschlüsselt
- Mails liegen auf den Servern im Klartext vor
- Fehlender Integritäts- und Authentizitätsnachweis
- Durch Erweiterungen (z.B. html) anfällig für Angriffe
- Freemail-Anbieter verkaufen Nutzerdaten
- Häufigster Weg für Kontaktaufnahme mit betrügerischer Absicht
  → Phishing

Phishing:
der Versuch Dritter, sich persönliche Informationen oder Zugänge vom rechtmäßigen Inhaber zu erschleichen.

Warum? → $$$$$

- Jährlicher Umsatz durch Erpressung im digitalen Raum 30 Mrd. USD
- Jährlicher Umsatz durch Drogenhandel 32 Mrd. USD
- 90% der „Cybervorfälle“ auf Faktor Mensch zurückzuführen

Wie?

- Massen-Phishing-E-Mails
- Spear-Phishing
- SMS-Phishing oder Smishing
- Voice Phishing oder Vishing
- Social-Media-Phishing

Einschüchterungs-Masche

FBI warnt vor Ransomware-Erpressung per Brief

Cyber-Erpresser, die ihre Forderungen per normaler Briefpost an die vermeintlich betroffenen Firmen schicken? Klingt merkwürdig und ist es auch: Das FBI rät zur Vorsicht.

07.03.2025, 14.30 Uhr

Was kann ich machen?

- Phishing erkennen lernen
- Angemessen mit Phishing-Nachrichten umgehen
- Wahrscheinlichkeit für den Eingang von Phishing-Nachrichten klein halten und Wahrscheinlichkeit der Erkennung erhöhen

Phishing erkennen lernen

Technische Merkmale:

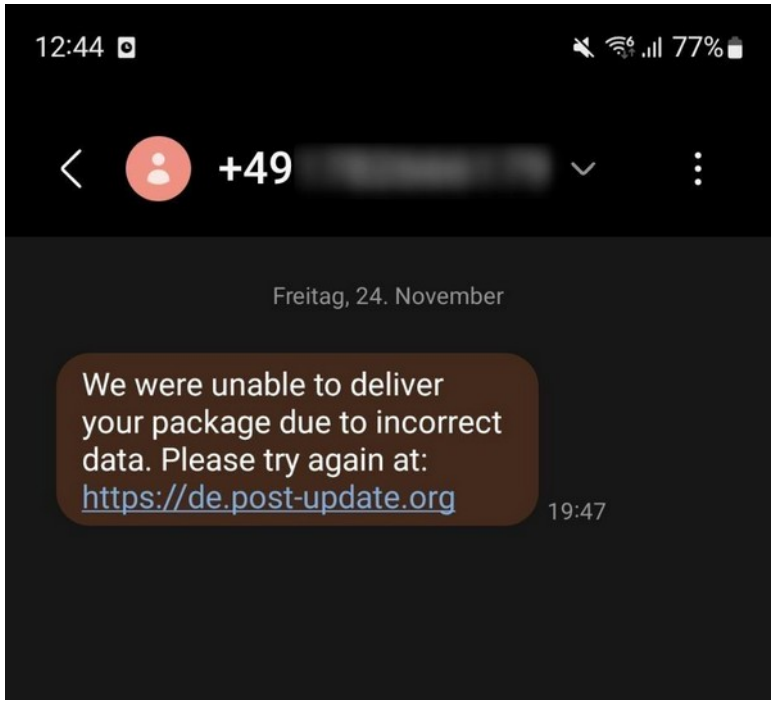
- Falsche Domainnamen
  - https://securitycheck-paypal.com
- Typo-squatting
  - beratung@sparkasse-zwlckau.de
  - www.sporkasse-zwickau.de
- Link Verschleierung
  - www.sparkasse-zwickau.de/kontoübersicht/

Phishing erkennen lernen

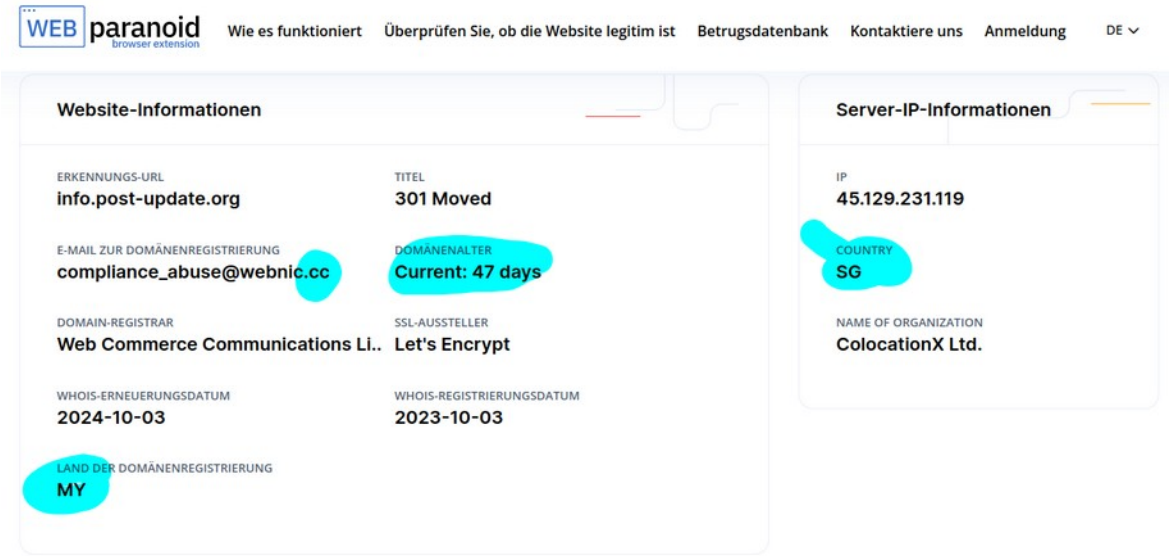
Soziale Merkmale:

- Autorität
- Sympathie
- Hilfsbereitschaft
- Konsistenz
- Knappheit

Eingang per SMS oder Messenger



https://de.post-update.org/e/authID=DuDu/tracking.php?sessionid=27i+ehg+63darezj091bc8foX+D3OgH++8a+afuwMb+erzL4gE1rZGJwkSFC95KYIT7B6+p+2SzeP526z98192#



Phishing → E-Mail

Kann man da nichts machen?

- sparsam beim Verteilen von Mailadressen/Telefonnummern sein
- Wegwerfadressen verwenden
- mehrere kontextbezogene Email-Aliase verwenden
  - bank.mustermann@mailbox.org
  - facebook.mustermann@mailbox.org
  - familie.mustermann@mailbox.org

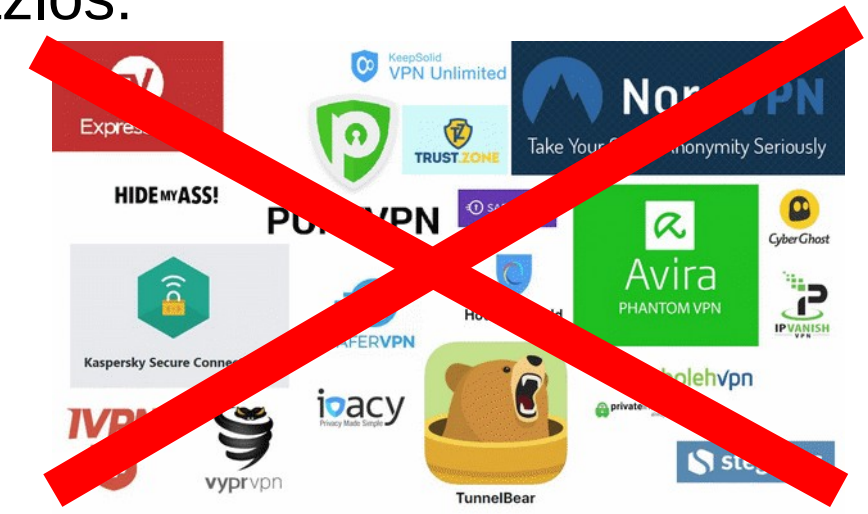
- Vertrauenswürdige Mailanbieter nutzen
  - https://mailbox.org
  - https://posteo.de
  - https://disroot.org/en (spendenfinanziert)
  - ~~https://proton.me~~
- 2FA für Mailkonto aktivieren
- Login/Benutzername ≠ Email-Adresse
- Mail Client statt Webmailer
  - Mozilla Thunderbird

VPN

Alles sicher dank VPN?

Für folgende Zwecke ist ein VPN nutzlos:

- Erzielen von Anonymität
- Schutz vor Hacking, Cyber-Bedrohungen und/oder Identitätsdiebstahl
- Verschleierung des GPS-Standorts (bspw. Mobilgerät)
- Schutz von Passwörtern
- Verhindern, dass Microsoft, Google oder Facebook private Daten sammelt
- Verhinderung unerwünschter Profilerstellung/Tracking durch soziale Netzwerke, Suchmaschinen oder andere Dienstleister
- Vermeidung von Daten-Leaks, bei der Nutzung von Online-Diensten



https://www.kuketz-blog.de/brauchst-du-wirklich-ein-vpn/

Ein vertrauenswürdiges VPN kann für folgende Fälle sinnvoll sein:

- Verbesserung der Sicherheit in unsicheren/nicht vertrauenswürdigen öffentlichen Netzwerken (Cafés, Zügen usw.) durch Prävention vor Man-in-the-Middle-Angriffen
- Umgehung von Zensur oder geografischen Sperren (Geoblocking) von Websites und Inhalten
- Verschlüsselung der Kommunikation, damit dein Internetanbieter oder Mobilfunkbetreiber die Online-Aktivitäten nicht überwachen oder aufzeichnen kann
- Verschlüsselung der DNS-Anfragen, sodass der Internetanbieter oder Mobilfunkanbieter die besuchte Domains nicht protokollieren kann
- Verbergen/Maskieren der IP-Adresse vor den Websites und Servern, die du besuchst
- Getunnelte Verbindung nach Hause und/oder zum Arbeitgeber, um auf Dienste zuzugreifen, die nicht direkt aus dem Internet erreichbar sind

https://www.kuketz-blog.de/brauchst-du-wirklich-ein-vpn/

VPN aber richtig:

- Selbst machen
- oder einen einigermaßen vertrauenswürdigen Dienstleister finden
    - https://mullvad.net/


THE SECURITY
OF ALL MY ACCOUNTS
THAT
ONE PASSWORD

Praktische Maßnahmen

Passwortsicherheit

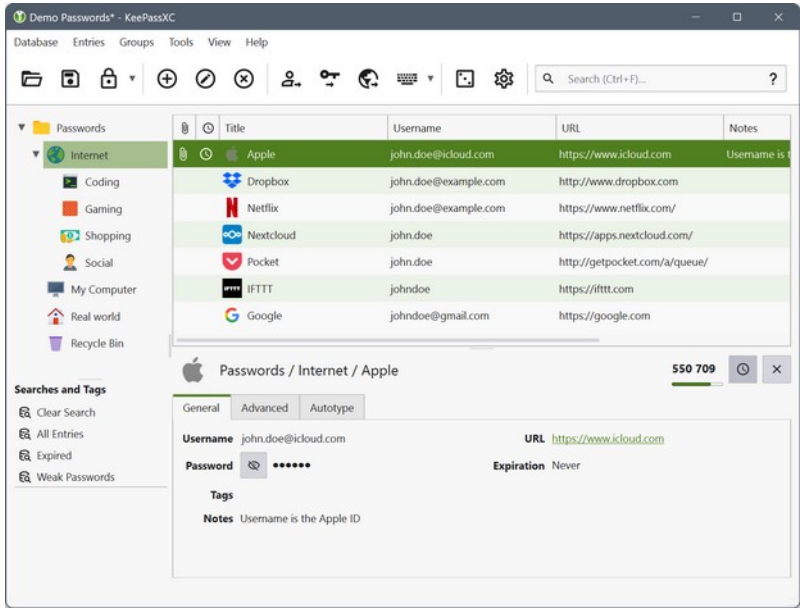
- Grundlage für Verschlüsselung (und Authentifizierung) ist ein sicheres Passwort
- Ziel eines Passworts: Viel Entropie ($E = \log_2(R^L)$)
  - Lang (Exponent = L) und mit Groß- und Kleinschreibung, Zahlen und Sonderzeichen (Basis = R)
  - Schwer zu erraten (für Mensch und Maschine)
    - Nicht in bekannten Datensätzen enthalten
    - Enthält keine persönlichen Informationen
    - Hält Brute Force Angriffen stand

- Status quo bei vielen: schlechte Passwörter und häufig wiederverwendet
  - Bei extrem vielen Diensten angemeldet (Email, Banking, Onlineshops, Foren, Videostreaming, etc.)
  - Ideal: jede Plattform eigene Logindaten, da Plattformen häufig nicht sorgsam mit Daten umgehen
  - Irrglaube: häufig rotierende Passwörter erhöhen relevant die Sicherheit
- Aber: Man kann sich unmöglich hunderte Passwörter merken
- Mögliche Lösungen:
  - Passkeys
  - Wir würfeln uns für jeden Login ein Passwort und speichern es ab

Praktische Maßnahmen

Passwortmanager

- Sicherer Tresor für eure Passwörter
- Ein sicheres Masterpasswort wird benötigt, mit diesen werden individuelle Logins verschlüsselt gespeichert
- Jeder Login kann sicheres, eindeutiges, zufälliges Passwort haben ohne, dass diese gemerkt werden müssen
- Kriterien zur Auswahl:
  - Open Source und etabliert
  - Negativbeispiel LastPass
- Beispiele: KeePassXC & Bitwarden



Livedemo – KeepassXC

- Freie Software
  - Bewährt
- Komplett lokal

Praktische Maßnahmen

Passwortmanager - Zugriff von mehreren Geräten

- Möglichkeiten zum Verteilen der Datenbank auf mehreren Geräten
  - USB-Stick / Sd-Karte
  - Lokaler Netzwerkspeicher und gemeinsame Dateifreigabe
  - Cloudspeicher
- Nachteile KeePassXC
  - Login nur mit Passwort oder Schlüsseldatei
  - Funktioniert nicht auf Mobilgeräten (Jedoch mit einer der vielen anderen Anwendungen)

→ Weitere Empfehlung ohne diese Nachteile: Bitwarden

bitwarden

Livedemo – Bitwarden

- Einfacher Sync zwischen Geräten
- Selfhosting möglich
- Freie Software

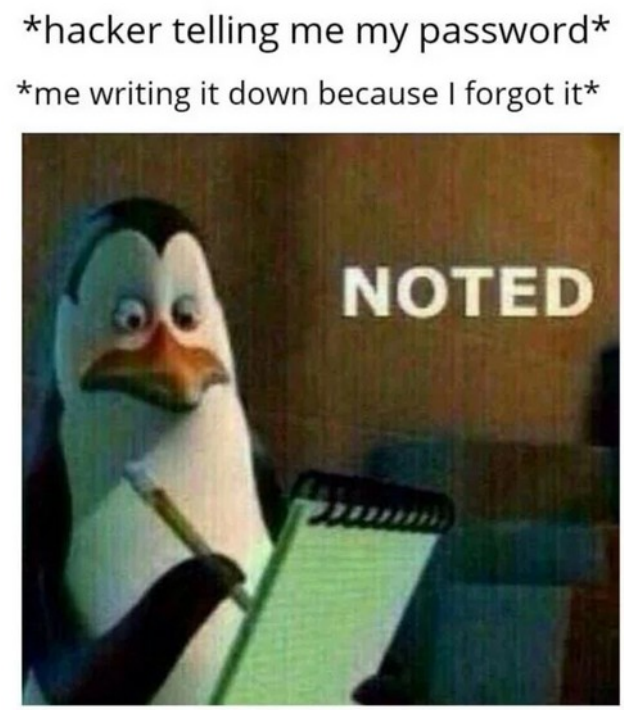
Praktische Maßnahmen

Absicherung gegen Passwortdiebstahl

- Plattformen gehen häufig sehr schlecht mit Daten um → Angreifer tragen Logindaten der Nutzer aus Datenbanken (oder zumindest die Hashes davon)
- Wie finde ich raus, ob ich gehackt wurde?
  - https://haveibeenpwned.com/
  - Benachrichtigung anhand Email-Adresse möglich

Was kann man dagegen tun?

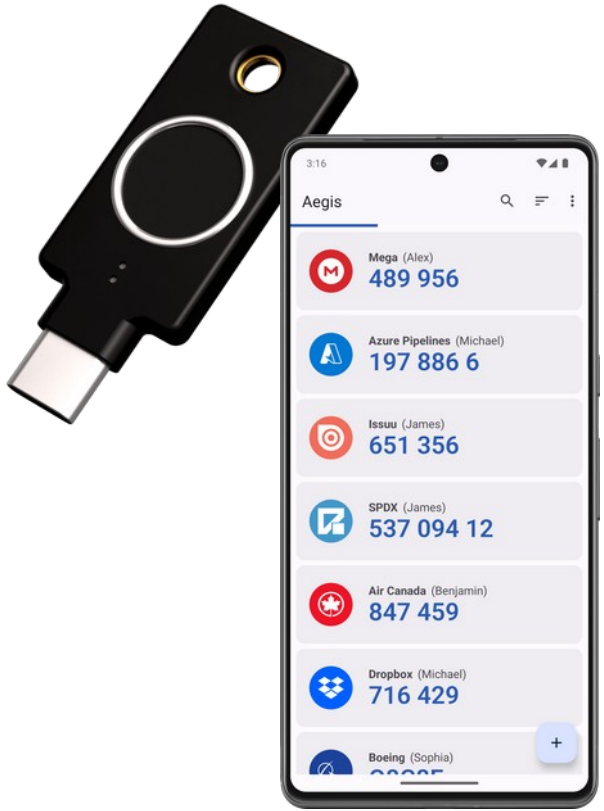
- 2FA = nur das Passwort reicht nicht



Praktische Maßnahmen

Zwei Faktor Authentifizierung - Übersicht

- Mögliche Varianten
  - TAN-Listen
  - SMS mit Einmalcodes
  - Hardware-Token bspw. Yubikey
  - Biometrie (Fingerabdruck, Gesichtsscan)
  - Authenticator App für TOTP (Zeitbasierte Einmal-Passwörter)



Empfehlungen

- Android: Aegis

- iOS: Bitwarden Auth.

Plattform	iOS	iOS	iOS			iOS	iOS
Open-Source	✗	✗	✗	✓	✓	✓	✓
App-Sperre	✓	✓	✓	✓	✓	✓	✓
Seed-Zugriff	✗	✗	✗	✓	✓	✓	✓
Auto-Backup	✓	✓	✓	✓	✓	✓	✓
Verschl. Backup	✗	✓	✓	✓	✓	✓	✓
Trackerfrei	✓	✗	✗	✓	✓	✗	✓

Livedemo – 2FA iOS

Praktische Maßnahmen

Zusammenfassung

- Nutzt lange, gut zu merkende Passwörter!
- Es ist gefährlich, dasselbe Passwort mehrmals zu nutzen
- Nutzt einen Passwortmanager!
- Multi-Faktor Authentifizierung ist Pflicht für kritische Zugänge!

Gerätesicherheit

Agenda

- Was ist damit gemeint?
- Grundsätze der Datensicherheit
- Mögliche Bedrohungszenarien
  (wovor schützen wir uns überhaupt?)
- Daten(träger-)verschlüsselung
- Backups und Clouddienste

Referent: flox, z-Labor e.V.

Gerätesicherheit

Was ist das überhaupt?

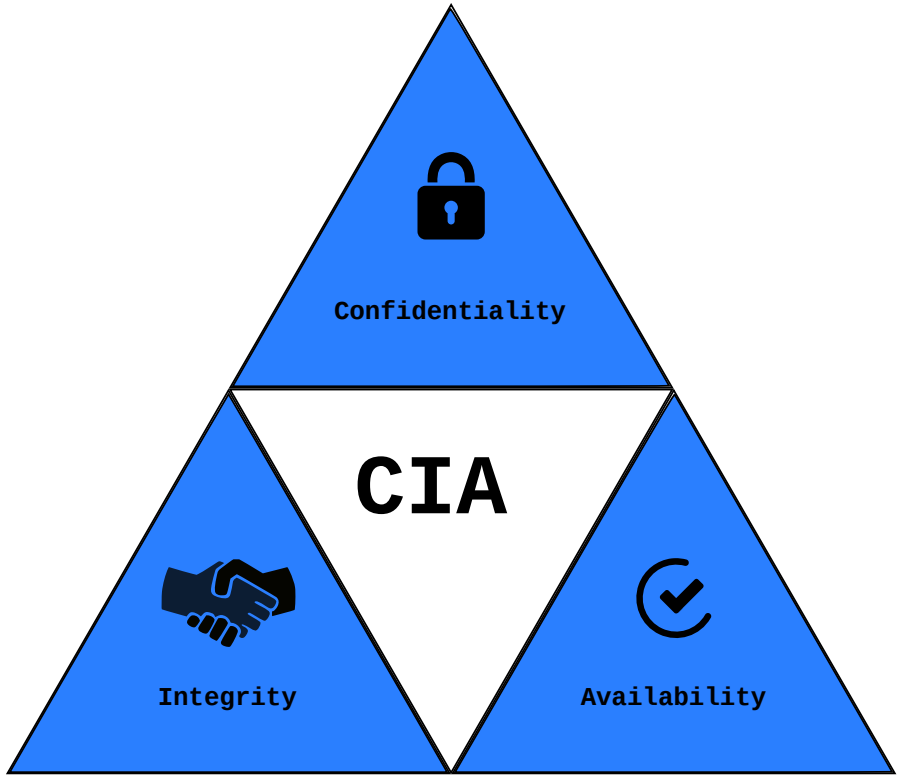
- Möglichkeiten sich vor physischen Faktoren zu schützen
- Sowohl innere und äußere Einflüsse
- Ziel: Datensicherheit gewährleisten auch wenn Gerät ausgeschaltet ist

1. Vertraulichkeit (Confidentiality):
   Sicherstellen, dass nur autorisierte Personen Zugriff auf schützenswerte Daten haben

2. Integrität (Integrity):
   Gewährleistung der Richtigkeit und Vollständigkeit der Daten

3. Verfügbarkeit (Availability):
   Sicherstellung, dass autorisierte Benutzer bei Bedarf zuverlässigen Zugriff auf Daten und Ressourcen haben

> In Summe als CIA-Trade bezeichnet



Beschädigte Speichermedien

Ein Festplattendefekt führt zum Verlust der Forschungen zur Masterarbeit, welche nicht ausreichend gesichert waren.

Verletzte Prinzipien:

- Verfügbarkeit
  Mit fehlenden Daten kannst du deine Arbeit nicht schreiben
- Integrität
  Man kann sich nie sicher sein ob Datenstand vollständig rekonstruierbar

Alchemist-hp (talk) www.pse-mendelejew.de, CC BY-SA 3.0, via Wikimedia Commons

Hinterlassen von Geräten

Vor lauter Stress beim Umsteigen lässt du deinen Laptop mit ungesicherter Arbeit an deiner neusten Geschäftsidee in der Bahn liegen.

Verletzte Prinzipien:

- Verfügbarkeit
  Du musst jetzt nochmal von vorne anfangen
- Vertraulichkeit
  Der unehrliche Finder kann nun beliebig mit deinen privatesten Daten agieren

Brian Penningtron, CC BY 2.0, via flickr

Einreise in Staat

Du reist in einen Staat mit repressiven Regime ein um einen Infoabend zu den Rechten von LGBTQ+-Personen zu halten. Bei der Einreise wird dir dein Laptop als Beweismittel abgenommen.

Verletzte Prinzipien:

- Verfügbarkeit
  Du kannst den Vortrag nun nicht mehr halten weil du keinen Zugriff auf deine Materialien hast
- Vertraulichkeit
  Die Daten auf deinen Laptop machen dich strafrechtlich in diesem Land angreifbar

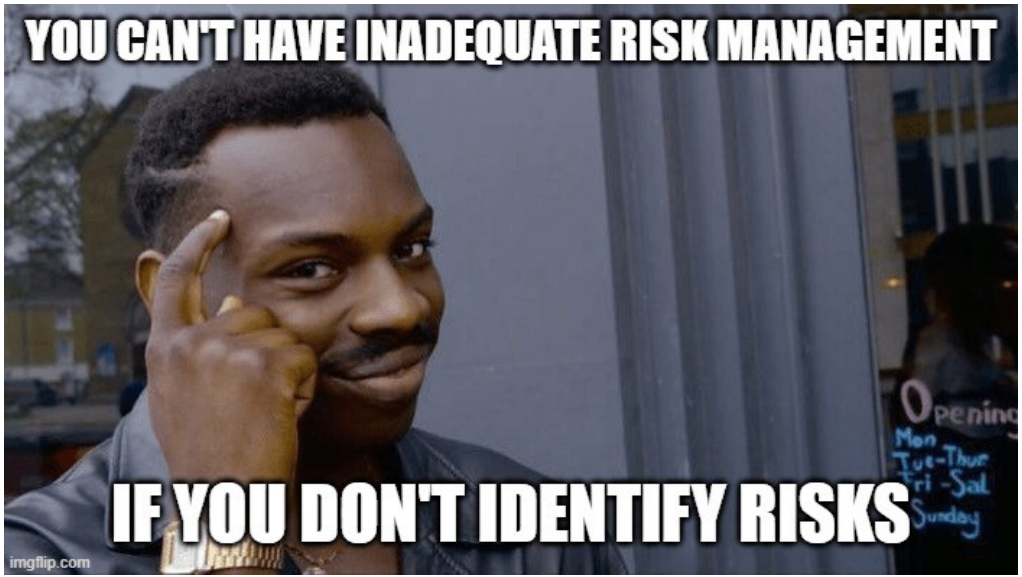
Michael Ball, CC0, via Wikimedia Commons

Gerätesicherheit

Fazit aus Beispielen

- Vertraulichkeit und Verfügbarkeit größte Gefahren für „Privatanwender“
- Beides einfach Lösbar durch

  Verschlüsselung und **Backups**

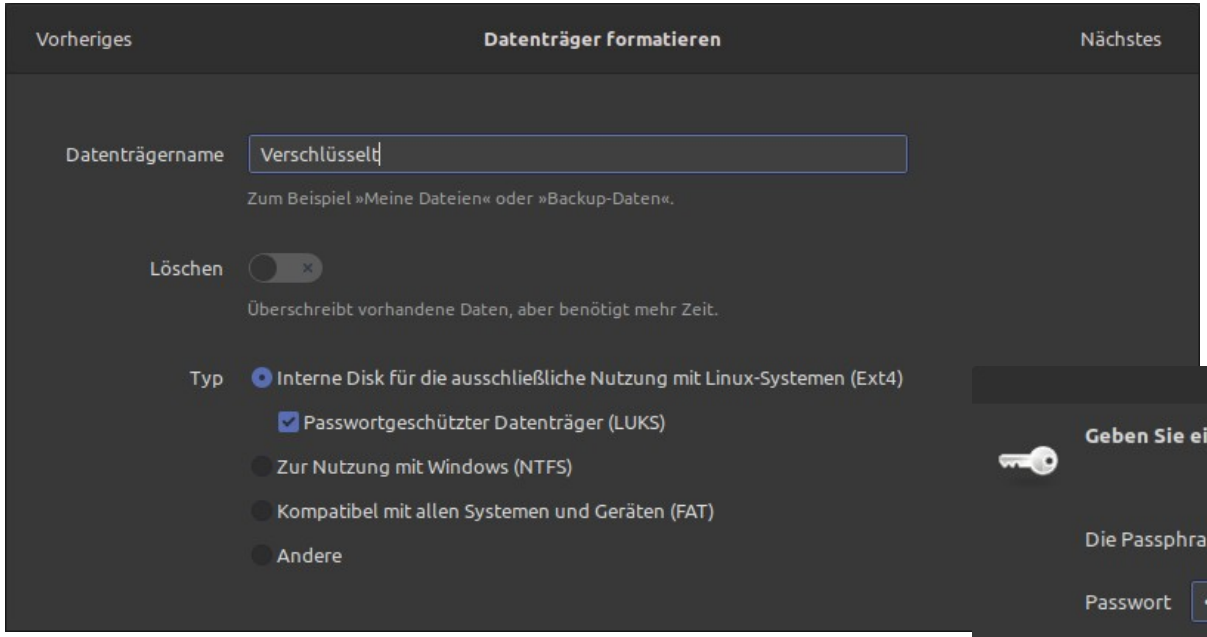


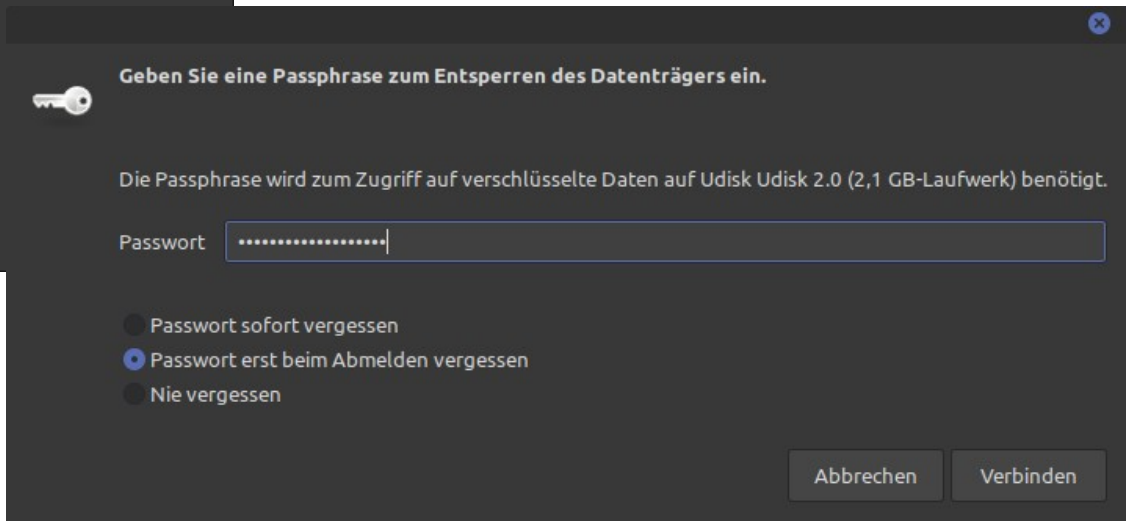
Gerätesicherheit

Was keine wirkliche Sicherheit ist

Gerätesicherheit

Was als Verschlüsselung zählt





Gerätesicherheit

Warum man seine Datenträger verschlüsseln sollte

- **Recht auf informationelle Selbstbestimmung**
  als eine besondere Ausprägung des allgemeinen Persönlichkeitsrechts (GG Art.2)
- **Deine Daten gehören dir!**
  Öffentliche Daten nützen, private Daten schützen!
- **Vor wem?** Vor allen!
- **Daten liegen immer offen auf einem Speicher** -> USB Stick verloren, Laptop geklaut, „Sicherheitscheck“ am Flughafen, Entsorgung von Datenträger
- **Daten:** Bewerbung, Porn, Prüfungsergebnisse, Steuererklärung, Credentials, Code, mehr Porn, Katzenvideos, Millionen-€-Idee, politische Kampfschrift, Familienfotos, ...

Gerätesicherheit

Der Weg zum sicheren Datenträger

- Was kann man alles verschlüsseln?
  - Einzelne Dateien, einzelne Ordner
  - Externe Laufwerke, NAS
  - Teile eines Systems (Home-Partition)
  - Vollverschlüsselung (**full disk encryption**, FDE) (Laptop, stationärer Rechner, Smartphone)

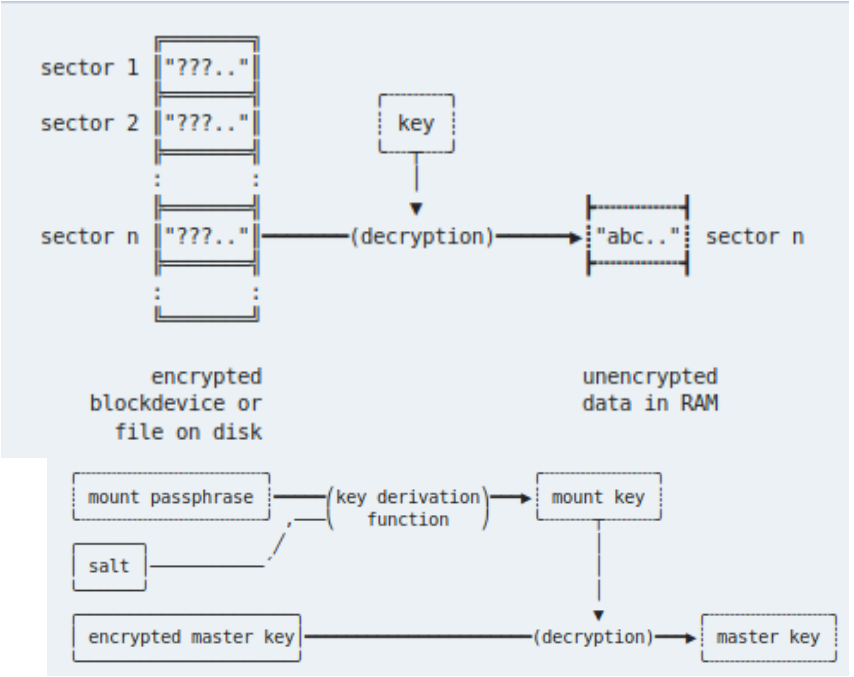
"Memories Stick" by Andrei Lacatusu is licensed under CC BY-NC 4.0

- Hard- vs. Software (Hardware meist teuer und nicht immer besser)
- Wichtig: OPENSOURCE!!!!!!

Gerätesicherheit

Einschub: Technische Realisierung

- Ursprung: Ganz langer Schlüssel (Master Key, viel Entropie)
- Daten werden in Blöcke geteilt (erlaubt wahlfreien Zugriff, meist von Datenträger vorgegeben)
- Schlüssel wird mit Blocknummer mathematisch zu Blockschlüssel erweitert → keine gleichen Passwörter für verschiedene Blöcke
- Blöcke werden bei Lesen „live“ entschlüsselt, bei Schreiben „live“ verschlüsselt
  → Es landen nie unverschlüsselte Daten auf Platte
- Langer Schlüssel kann sich niemand merken → Header mit verschlüsselten Master, erlauben Passwortänderung ohne Neuverschlüsselung des Laufwerkes



Quelle: ArchWiki (https://wiki.archlinux.org/index.php/Encryption)

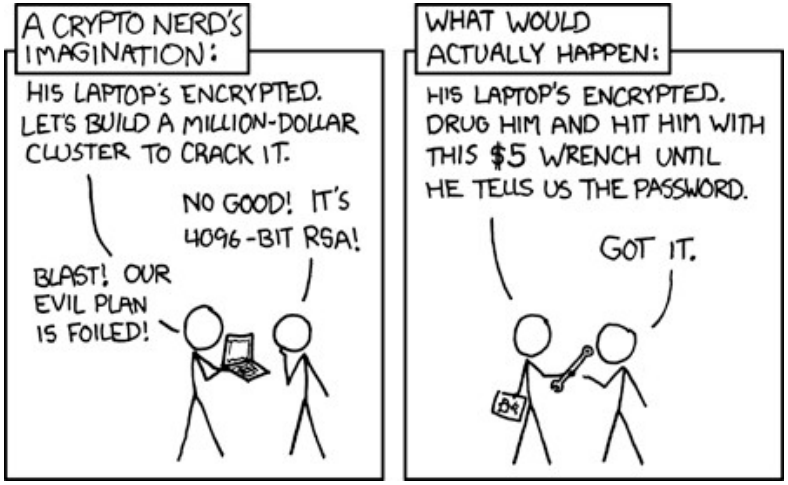
Gerätesicherheit

Wie man wirklich sicher unterwegs ist

- Verwendung sicherer Verschlüsselungsalgorithmen (Namedropping: AES, Argon2)
- Sicheres Passwort (dazu später mehr)
- Mehrere Layer der Sicherheit (Passwörter können ausgespäht werden) → Hardware-Token als zweiter Faktor
- Schützt nicht vor allen möglichen Attacken (Entwendung eingeschaltener Systeme, cold boot und andere physische Angriffe, Schadsoftware)

  → Vorsicht & Verstand sind nie falsch am Platz

  → Datenträgerverschlüsselung primär als physischer Schutz (Offline-Schutz) der Daten



https://imgs.xkcd.com/comics/security.png

Gerätesicherheit

Tools unter Linux

- Linux erlaubt größte Freiheit bei Konfiguration
- Vollverschlüsselung schon im Bootprozess
- Tools plattformunabhängig verfügbar
  - LUKS / dm-crypt: transparente Verschlüsselung für ganze Platten
  - Veracrypt: Erlaubt portable Verschlüsselung von Dateien, Ordner, Laufwerke als Programm
- Einfache Einrichtung sowohl für Vollverschlüsselung als auch für Datenträger: jeweils nur 1 Klick

LUKS
Linux Unified Key Setup

VeraCrypt

Gerätesicherheit

Tools unter Windows

- Vollverschlüsselungswerkzeug: Bitlocker
- Für Privatanwender seit Windows 8 verfügbar
- Sowohl automatische Entschlüsselung mit TPM als auch manuell mit Passphrase
- Nicht open source (Sicherheit gegenüber Backdoors nicht prüfbar)
- Nur geringe Anzahl an Verschlüsselungsmethoden implementiert
- Massive Sicherheitslücken in Kombination mit TPM
- Alternativ: plattformübergreifende Werkzeuge (Veracrypt), diese können allerdings Bootvorgang nicht schützen

Gerätesicherheit

Tools für Mobilgeräte

- Android prinzipiell Open Source, basiert auf Linux-Tools
- unterstützt FDE seit Android 4, seit Android 7 file-based encryption
- Sowohl für internen Speicher als auch SD
- Aber: konkrete Implementation herstellerabhängig, kann im Auslieferungszustand nicht auf Backdoors kontrolliert werden
- Außerdem: diverse Apps für mehr oder minder zweifelhaften Dateischutz (ändern oft nur Dateiendung)
- Ultimative Lösung: **Custom ROM** (Lineage OS, Graphene OS), löst auch Abhängigkeit von Google

Gerätesicherheit

Backups

- Hardwareausfälle häufiger als gedacht

  „Eine Umfrage des Digitalverbands BITKOM ergab, dass ein Fünftel der Befragten bereits Daten wegen eines fehlenden Backups verloren hat“

- Nicht nur Daten sichern, auch über Ernstfall Gedanken machen

Gerätesicherheit

"kalte" Backups

- Klassicher Fall: auf physichen Speichermedium an sicheren Ort
- Bei Oma & Opa, Bankschließfach, …
- Daten gehören zu 100% Nutzer
- Probleme:
  - Manueller Aufwand: je sicherer verwahrt desto seltener wird Backup gemacht
  - Undurchsichtigkeit („wo war jetzt nochmal …“)
  - Hardwarefehler möglich
  - Nicht immer von überall erreichbar

Gerätesicherheit

"kalte" Backups - Tricks und Kniffe

- BSI empfielt midestens zwei Backups an getrennten Orten aufzubewahren
  → Für Privatnutzer kaum umsetzbar außer für ultra wichtige Daten
- Datenträger unbedingt verschlüsseln & Passwort notieren
  („Wie war gleich nochmal das Passwort?“)
- Inkrementelle Backups beschleunigen enorm

  Linux: rsync, Timeshift, duplicati

  Windows: duplicati

Gerätesicherheit

"warme" Backups

- Speicherung auf separater Maschine, welche dauerhaft verfügbar ist
- NAS-Laufwerk, selber gehostete Cloud, Cloud von kommerziellen Anbietern
- Wenn nicht selber gebaut gehören Daten nicht Nutzer

Gerätesicherheit

"warme" Backups - Vor- und Nachteile

Vorteile:

- Ortsunabhängiger Zugriff:
  Daten immer und überall verfügbar
- Automatisierung:
  Clouds bieten sync-Programme an
- Katastrophenschutz:
  Rechenzentren meistens gut geschützt
- Skalierbarkeit:
  Clouds oft flexibel erweiterbar
- Versionierung:
  Alte Versionen werden oft beibehalten

Nachteile:

- Abhängigkeit von Internetverbindung
- Datenschutz und Sicherheit:
  Daten liegen auf fremden Servern
- Laufende Kosten:
  Gebühren / Stromkosten
- Geschwindigkeit:
  Netzwerkanbindung langsamer als USB
- Abhängigkeit von Anbieter:
  Vertragsänderungen, Insolvenz, ...

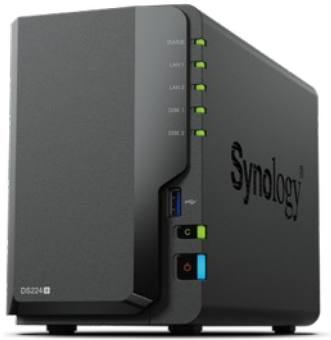
Gerätesicherheit

Eigene Cloud - das Beste aus beiden Welten

- Vorteile des Cloudspeichers ohne die Abhängigkeit
- Möglichkeit 1: Anmieten eines Servers
- Möglichkeit 2: Cloud steht zu Hause, entweder Eigenbau oder fertiges NAS
- Viele Tutorials, gute Möglichkeit Grundlagen Systemadministration zu lernen

HETZNER
SERVER · CLOUD · HOSTING

Nextcloud



Gerätesicherheit

Cloudspeicher: Worauf ist zu achten?

- Für Redundanz sorgen:
  Gleicher Ordner lässt sich auf zwei Dienste synchronisieren
- Verschlüsselung!!!!
  Verschlüsselte Dienste nutzen oder Crypto dazwischen hängen
  Cryptomator, duplicati
- Auch hier wieder wichtig:
  Open Source

Zum Abschluss:

Danke für Ihre Aufmerksamkeit!

Folien & Link-Sammlung

https://docs.z-labor.space/s/dpb2025