

Passwörter und Datenträgerverschlüsselung

Starke Passwörter



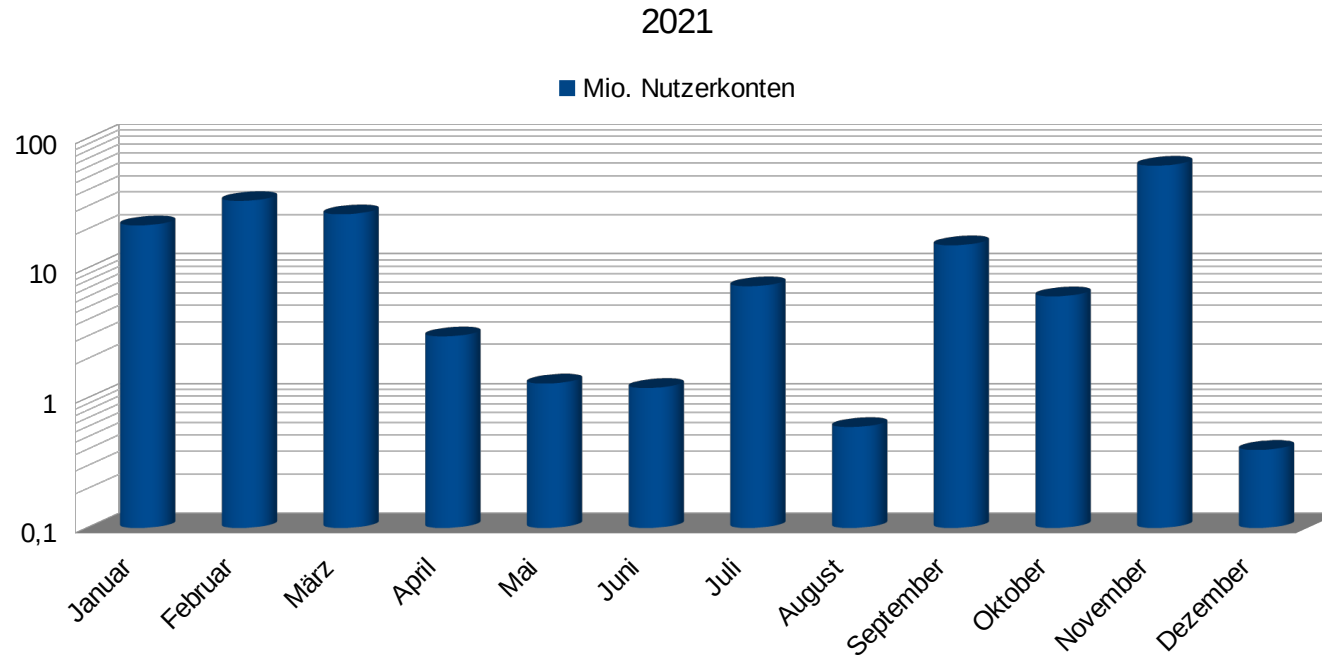
Agenda

- ▶ Notwendigkeit
- ▶ Starke Passwörter
 - ▷ Wie werden Passwörter "geknackt"
 - ▷ Was macht Passwörter stark?
 - ▷ Starke Passwörter selber erzeugen
- ▶ Ein Zweiter Faktor machts noch stärker
- ▶ Passwortverwaltung
- ▶ Praxis

Notwendigkeit von Passphrasen

- ▶ Passwörter/-phrasen = "Schlüssel" zu Daten
- ▶ Gesetzliche Verankerung u.a. Datenschutzgrundverordnung
- ▶ Art. 25 DSGVO: Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen
 - ▷ Gilt insb. bei Verarbeitung personenbezogener Daten --> Art. 4 Nr. 1 DSGVO!
- ▶ Integrität und Vertraulichkeit, Art. 5 Abs. 1 lit. f) DSGVO
 - ▷ Schutz insb. vor unbefugtem Zugriff
 - ▷ Datensicherheit durch technische und organisatorische Maßnahmen, vgl. Art. 28 Abs. 1, Art. 32 Abs. 1 DSGVO

Kompromittierte Nutzerkonten



2021 bislang:
177.967.082

(Quelle: Hasso-Plattner-Institut, <https://sec.hpi.de/ilc/statistics>)

Passwörter Top 10

	Passwort	Häufigkeit (in ‰)
1	123456	8,10
2	123456789	3,89
3	password	1,89
4	qwerty	1,85
5	12345	1,38
6	12345678	1,17
7	111111	1,17
8	qwerty123	1,02
9	1q2w3e	0,97
10	123123	0,85
...	...	...

(Quelle: Hasso-Plattner-Institut, <https://sec.hpi.de/ilc/statistics>)

Leaks nach Domäne

	Domäne	Anteil (in %)	Anzahl
1	yahoo.com	17,55	2.377.604.343
2	gmail.com	15,69	2.162.023.545
3	hotmail.com	12,68	178.076.325
4	mail.ru	3,88	525.949.324
5	aol.com	3,70	501.053.015
6	qq.com	2,36	319.302.292
7	rambler.ru	2,09	282.768.921
8	163.com	2,02	2.377.752.580
9	yandex.ru	1,56	211.617.024
10	hotmail.fr	0,84	113.667.731

(Quelle: Hasso-Plattner-Institut, <https://sec.hpi.de/ilc/statistics>)

HPI Identity Leak Checker

- Finde heraus, ob deine Daten im Internet aufzufinden sind

Wurden Ihre Identitätsdaten ausspioniert?

Täglich werden persönliche Identitätsdaten durch kriminelle Cyberangriffe erbeutet. Ein Großteil der gestohlenen Angaben wird anschließend in Internet-Datenbanken veröffentlicht und dient als Grundlage für weitere illegale Handlungen.

Mit dem HPI Identity Leak Checker können Sie mithilfe Ihrer E-Mailadresse prüfen, ob Ihre persönlichen Identitätsdaten bereits im Internet veröffentlicht wurden. Per Datenabgleich wird kontrolliert, ob Ihre E-Mailadresse in Verbindung mit anderen persönlichen Daten (z.B. Telefonnummer, Geburtsdatum oder Adresse) im Internet offengelegt wurde und missbraucht werden könnte.

 Bitte geben Sie hier Ihre E-Mail-Adresse ein.

Die von Ihnen eingegebene E-Mail-Adresse wird lediglich zur Suche in unserer Datenbank und das anschließende Versenden einer Benachrichtigungs-E-Mail benutzt. Sie wird von uns in verschleierter Form gespeichert, um Sie vor E-Mail-Spam zu schützen. Die Weitergabe an Dritte ist dabei ausgeschlossen.

E-Mail-Adresse prüfen!

(Quelle: Hasso-Plattner-Institut,
<https://sec.hpi.de/ilc/search?lang=de>)

Wie werden Passwörter geknackt?

- ▶ Brute Force
 - ▷ alle möglichen Kombinationen ausprobieren
- ▶ Listen / Wörterbuch-Angriffe
 - ▷ alle Wörter aus einer Liste oder einem Wörterbuch ausprobieren
- ▶ Ausnutzen von Fehlern/Schwachstellen
 - ▷ Im Programmcode oder der technischen Umsetzung
 - ▷ Passwörter im Klartext speichern
- ▶ Social Engineering
 - ▷ Phishing, Person austricksen um Passwort zu erfahren
 - ▷ gerne auch durch Facebook, LinkedIn etc.

Wie werden Passwörter geknackt?

▶ Keylogger

- ▷ Schadprogramm auf dem Rechner
- ▷ Liest alle Tastatureingaben mit und sendet diese an Angreifer

▶ Sniffing

- ▷ Abhören/-fangen der über die Netzwerkverbindung übertragenen Daten

▶ Datenbankhack

- ▷ Enthält Anmeldedaten inkl Passwörter
- ▷ Schlechte oder keine Verschlüsselung

Vertiefung: Passwörter knacken durch Bruteforce

- ▶ Ausprobieren verschiedener Zeichenkombinationen in schneller Abfolge
- ▶ Einfacher Algorithmus, weshalb möglichst viele Zeichenkombinationen probiert werden
- ▶ Rechenleistung entscheidend für Anzahl an Berechnungen pro Sekunde/Minute
- ▶ Praxisrelevanz (noch immer) hoch, weil einfach
 - ▷ Häufig kurze Passzeichen und nur solche des Alphabets
 - ▷ Dadurch mögliche Kombinationen drastisch reduziert

Vertiefung: Passwörter knacken durch Social Engineering

- ▶ Umfassende Analyse des Umfelds des Opfers
 - ▷ Suche und Analyse aller Seiten bzw. Profile
 - ▷ Automatisches scannen von Social Media Seiten
 - ▷ Auswertung von Fotos und Texten – auch Autokennzeichen
 - ▷ Gezielte Suche nach typischen Informationen wie Name, Adresse, Geburtsdaten von Familienmitgliedern und Namen der Haustiere

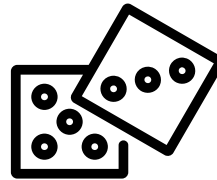


Was macht ein Passwort stark

- ▶ Geheimhaltung



- ▶ Zufall



- ▶ Länge

Geheimhaltung: gar nicht so einfach...



▶ Abhören / Abfilmen

- ▷ Keylogger, Überwachungskameras, Handys anderer Leute, Staatstrojaner, unverschlüsselte Emails (Google), der Blick von Hinten über die Schulter - "Shoulder-Surfing"

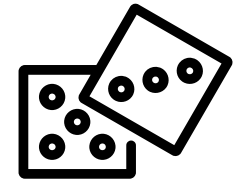
▶ Schlechte Verstecke

- ▷ Post-Its, Schreibtischunterseiten, Zettel in der Geldbörse, Cloudspeicher, Klartextdateien

▶ Social Engineering

- ▷ Liebe Menschen: Kolleg:innen, Freunde, Familie, Vorgesetzte, vorgebliche Vorgesetzte
- ▷ Nicht so liebe Menschen: Erpressung, Schmerzandrohung

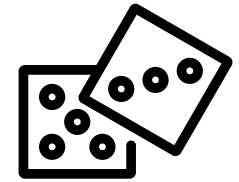
Die Macht des Zufalls - Entropie



- ▶ Der Mensch ist nicht gut darin, sich zufällige Worte auszudenken
- ▶ Verknüpfung von Sinneseindrücken und Vorstellung unter Einbeziehung bereits gelernten --> Prozess = Denken
- ▶ Problem: das menschliche Gehirn assoziiert immer
- ▶ Beispiel auf der folgenden Folie



Die Macht des Zufalls - Entropie



- ▶ Situation
 - ▷ Jemand sitzt am Schreibtisch im Arbeitszimmer und isst dabei eine Melone
 - ▷ Im Arbeitszimmer befinden sich viele Bürogegenstände; auf dem Tisch stehen zB ein Locher und ein Hefter, sowie Stifte und der PC
- ▶ "Spontan und zufällig ausgedachtes Passwort" durch aneinanderreihung von Worten
 - ▷ **HausLocherTasteMeloneHefter**
 - ▷ Gehirn hat Gegenstände aus der konkreten Situation verknüpft
- ▶ Wörterbuchangriff möglich, da alle Wörter in einem handelsüblichen Wörterbuch stehen

Passwort vs Passphrase

- ▶ Passwort = wenige Zeichen (oftmals ≤ 6)
- ▶ Passphrase = aneinanderreihung von vielen Zeichen ($\neq$ Wörter)
 - ▷ Ziel: Angreifer zu möglichst vielen Rateversuchen zwingen
 - ▷ Stärke Passphrasen = mehr Anzahl möglicher Kombinationen
- ▶ Merkmale einer guten Passphrase
 - ▷ Auf die Länge kommt es an!
 - ▷ Länge durch viele Zeichen (Länge, z.B. 16+)
 - ▷ Aus einem großen Alphabet (Zeichenvorrat: Ziffern, Groß-/Kleinbuchstaben), Zahlen, Sonderzeichen
 - ▷ Zufällig ausgewählt (nicht: selbst ausgedacht)

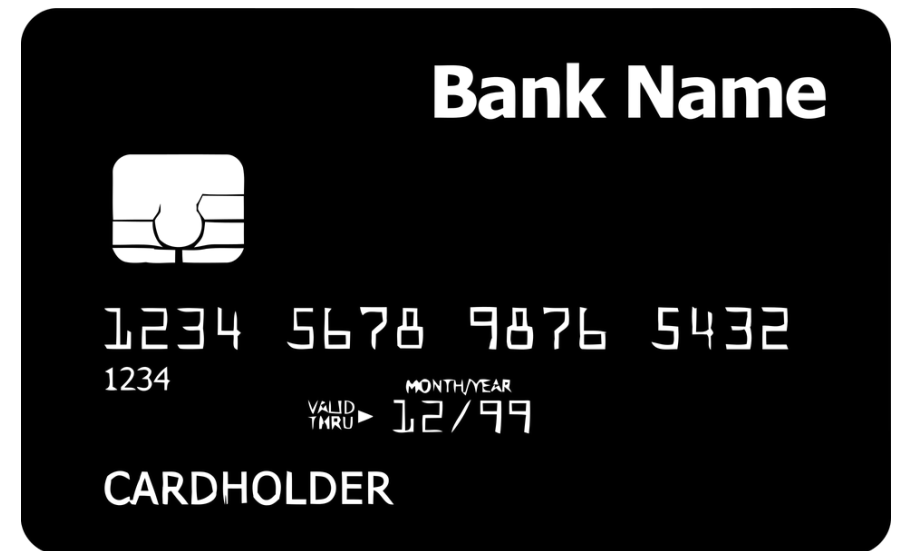
Starkes Passwort erzeugen

- ▶ Länge + Zufall = entscheidend!
- ▶ Passwort "auswürfeln"
 - ▷ Diceware
 - ▷ Würfellisten (Link am Ende des Passwortteils)
 - ▷ UAVM-3nKAEclSKDMa/WhT2En9

Zwei-Faktor-Authentisierung



Kombination zweier unterschiedlicher und insbesondere unabhängiger Komponenten (Faktoren).



Funktionsweise

- ▶ Teilprozesse eines Anmeldevorgangs welche zusammengesetzt werden (im Sprachgebrauch synonym)
 - ▷ Fehlen = Anmeldevorgang nicht erfolgreich
- ▶ Authentisierung
 - ▷ Benutzer:in meldet sich mittels eindeutiger Informationen an einem System an (zB Passwort oder Chipkarte)
- ▶ Authentifizierung
 - ▷ System überprüft Gültigkeit der Anmeldedaten und "erkennt" Benutzer:in

Funktionsweise

- ▶ Elemente
 - ▷ Besitz (z.B. Chipkarte, TAN-Generator, physischer Schlüssel)
 - ▷ Geheimes Wissen (z.B. Passphrase, PIN, TAN)
 - ▷ Biometrie (z.B. Fingerabdruck, Retina, menschliche Gang, Stimme)
- ▶ Keine zwingende Verschiedenheit, aber idR getrennte Übertragungskanäle
- ▶ In Stufen hintereinander geschaltet oder in Kombination miteinander
- ▶ https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Zwei-Faktor-Authentisierung/zwei-faktor-authentisierung_node.html

Arten

- ▶ TAN (Transaktionsnummer)/OTP-Systeme (One-Time-Passwort)
 - ▷ Einmalkennwort, dass zeit- oder ereignisbasiert stets neu generiert wird und zusätzlich übermittelt werden kann
 - ▷ Früher: Papierlisten (iTAN)
 - ▷ Heute: TAN-Generatoren (Hardware) bzw. Authenticator Apps (Software)
 - ▷ Teilw. auch unter Einbeziehung von Transaktionsdaten (Kontonummer und Betrag); eTAN, Chip TAN
- ▶ TAN als SMS (mTAN, smsTAN)
 - ▷ Achtung: Niemals dasselbe Gerät für Log-In und TAN nutzen
 - ▷ Zweiter Faktor fällt weg!

Arten

- ▶ Kryptographische Token, gemeint "Schlüssel"
- ▶ Speicherung eines privaten kryptographischen Schlüssel
 - ▷ Softwarezertifikat (bekannt von ELSTER)
 - ▷ Hardware auf einer Chipkarte (HBCI, Signaturkarten) oder einem speziellen USB-Stick/NFC-Token (FIDO/U2F) -> Nitro-/Yubikey
- ▶ Biometrische Systeme: Überprüfung des Vorhandenseins von zuvor erfassten körperlichen Merkmalen (Fingerabdruck, Gesicht, Retina).
 - ▷ Normalerweise nicht Geheim (Sichtbarkeit des eigenen Gesichts) --> Lebenderkennung
 - ▷ Problem: Lässt sich schwer/gar nicht ändern

Wie erschwert man das Knacken eines Passwords?

▶ Brute Force

- ▷ Länge = je länger, desto besser
- ▷ Verschiedene Zeichentypen (Groß- und Kleinbuchstaben, Zahlen, Sonderzeichen)

▶ Listen / Wörterbuch-Angriffe

- ▷ Keine einzelnen Wörter als Passwort verwenden
- ▷ Keine Wörter aus dem persönlichen Umfeld verwenden (Namen, Geburtsdaten etc.)

▶ Social Engineering

- ▷ **Niemandem das Passwort verraten!**

Fortsetzung: Wie erschwert man das Knacken eines Passworts?

▶ Keylogger

- ▷ Keine (Schad-)Software aus dubiosen Quellen herunterladen
- ▷ Keine Anhänge von unbekannten Absendern öffnen

▶ Sniffing

- ▷ Möglichst in öffentlichen/fremden WLAN-Netzen keine Passwörter eingeben
- ▷ Ausschließlich HTTPS-Verschlüsselung benutzen

Niemanden das Passwort verraten

- ▶ ... ist oftmals gar nicht so leicht



(Quelle: Jimmy Kimmel – What is Your Password? -2016:
<https://yewtu.be/watch?v=opRMrEfAlil>)

Weitere nützliche Tipps

- ▶ Initial-Passwörter umgehend bei Erstanmeldung ändern
- ▶ Anzeigen der Buchstaben bei der Eingabe von Passwörtern deaktivieren
- ▶ Achtung bei "Sicherheitsfragen". Kann jemand die Antwort durch soziale Netzwerke/Social Engineering in Erfahrung bringen?
- ▶ **Für jeden Dienst ein eigenes Passwort nutzen**
- ▶ Alte Passwörter nicht noch einmal verwenden

How-To: Starke Passwörter merken?!



See my
password
on the back
side

KeePassXC

<https://keepassxc.org/>

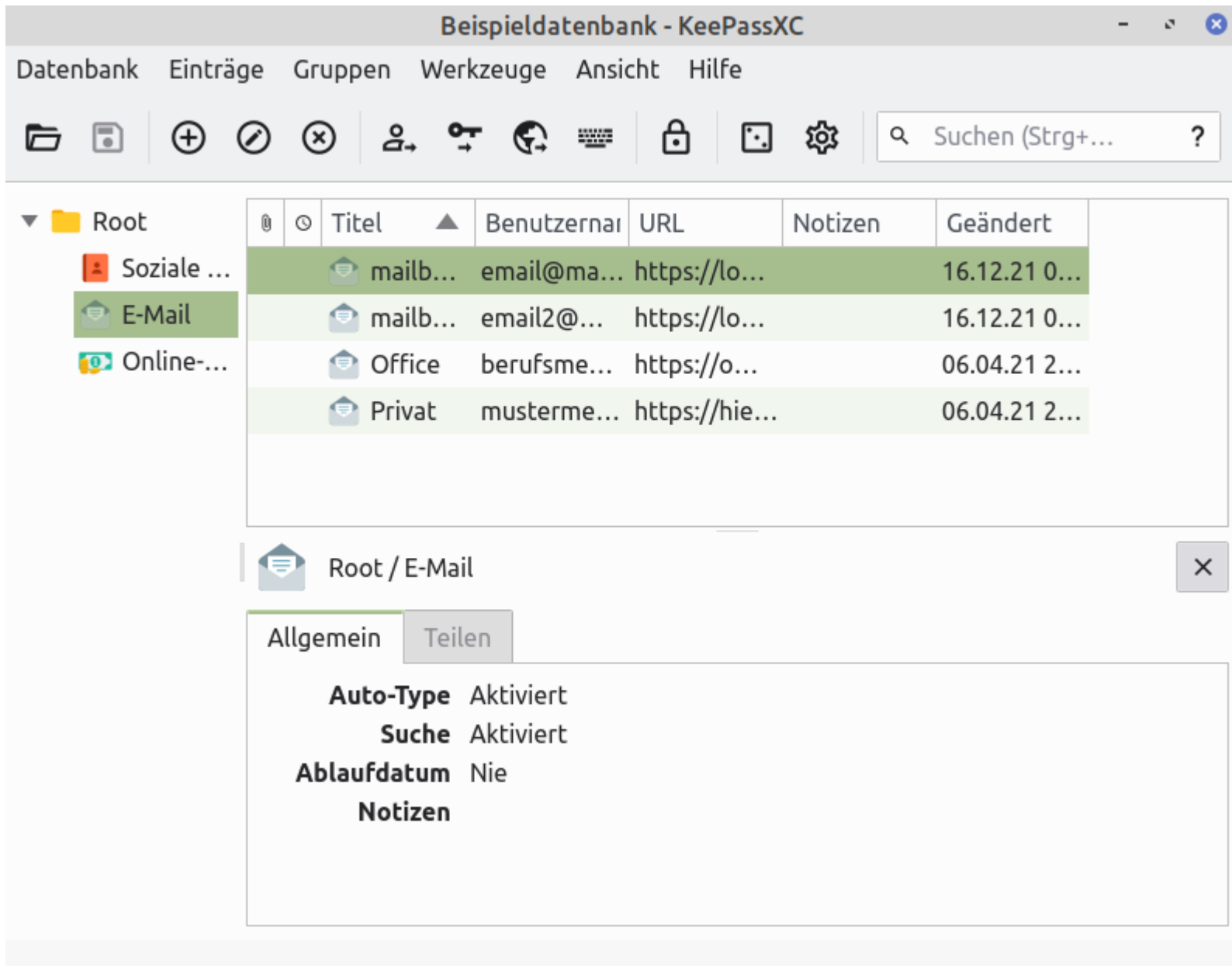
Vorteile

- ▶ Freie Software
- ▶ Viele Plattformen
 - ▷ Win, Linux, Mac
- ▶ 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*

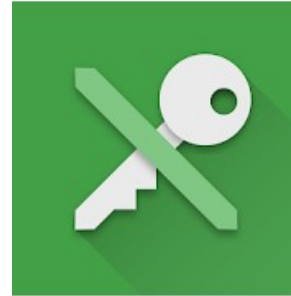




KeePass als App

KeePassDX

- ▷ Kompatibel mit KeePassXC
- ▷ F-Droid
- ▷ Play Store



Keepass2Android Password Safe

- ▷ Kompatibel mit KeePassXC
- ▷ Nur Play Store

Starkes Hauptpasswort finden: Würfeln und Passwortliste

- ▶ Passwörter würfeln mithilfe einer Passwortliste
- ▶ Warum? → Entropie!
- ▶ Vorteil: nur dieses Passwort muss man sich merken
 - ▷ Haupt-/Masterpasswort
- ▶ Tipp: mind. 6 Wörter würfeln



How-To: Masterpasswort würfeln

▶ Zubehör

- ▷ Wortliste mit deren Hilfe sich die Passphrase würfeln lässt (Link am Ende des Passwortteils)
- ▷ 6-seitiger Würfel

▶ Funktionsweise

- ▷ Je Wort wird 5 Mal gewürfelt und die Zahlen notiert
- ▷ Dieses wird mind. 6 Mal durchgeführt (also $6 * 5 = 30$)
- ▷ Alle Worte hintereinander geschrieben (ohne Leerzeichen), ergeben die Passphrase
- ▷ Die Passphrase muss man sich merken und kann als Hauptpasswort für die Passwortdatenbank dienen

Wozu diene 00000000 als Passcode?

- ▶ Möglichkeit A: Türcode zum Serverraum des CERN
- ▶ Möglichkeit B: Startcode der US-Atomraketen
- ▶ Möglichkeit C: Geheim-Vorwahl der Telekom, um kostenlos Telefonieren zu können
- ▶ Möglichkeit D: Erste Faxnummer der Bundespost, die Helmut Schmidt als Bundeskanzler genutzt hat

Launch-Code US-Atomraketen

- ▶ Passcode für die Atomraketen der USA von 1962 - 1977

00000000

- Hinweis: Es ist umstritten, ob der Code wirklich niemals während der Zeit geändert wurde.
- Quelle:
<https://www.heise.de/security/meldung/00000000-Passwort-fuer-US-Atomraketen-2060077.html>

– Ende Passwörter –