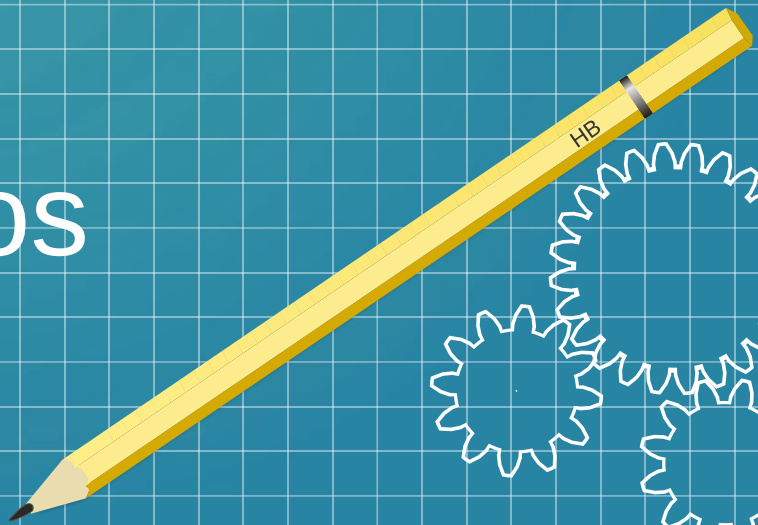
Passwortmanager

statt

Passwortchaos

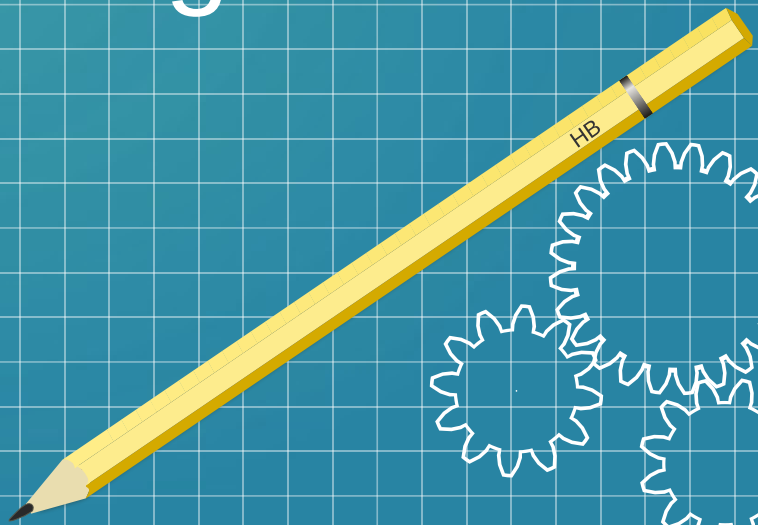


Wer bin ich?

Jürgen Kostzewski

- IT-Projektleiter und
- Open Source-Enthusiast

Warum Passwortmanager?



Das Passwortproblem – Ein Blick in die Realität

„123456“ – Noch immer eines der beliebtesten Passwörter!

- Passwort-Wiederverwendung bei 65% aller Nutzer
  → „Mein Passwort ist doch gut/sicher genug“
- Zettel unter der Tastatur oder Excel-Liste im Klartext
- Cloud-Dienste wie Google Docs als Notlösung
- „Hirn-Overload“: 30+ Accounts, aber nur 3 Passwörter?
  → Kognitive Überlastung

Das Passwortproblem – Ein Blick in die Realität

Wer nutzt noch dasselbe Passwort wie vor 5 Jahren?

Wenns schiefgeht – Datenpannen & Leaks

Wenn Dein Passwort plötzlich öffentlich ist

- LinkedIn-Passwort-Leak aus 2012

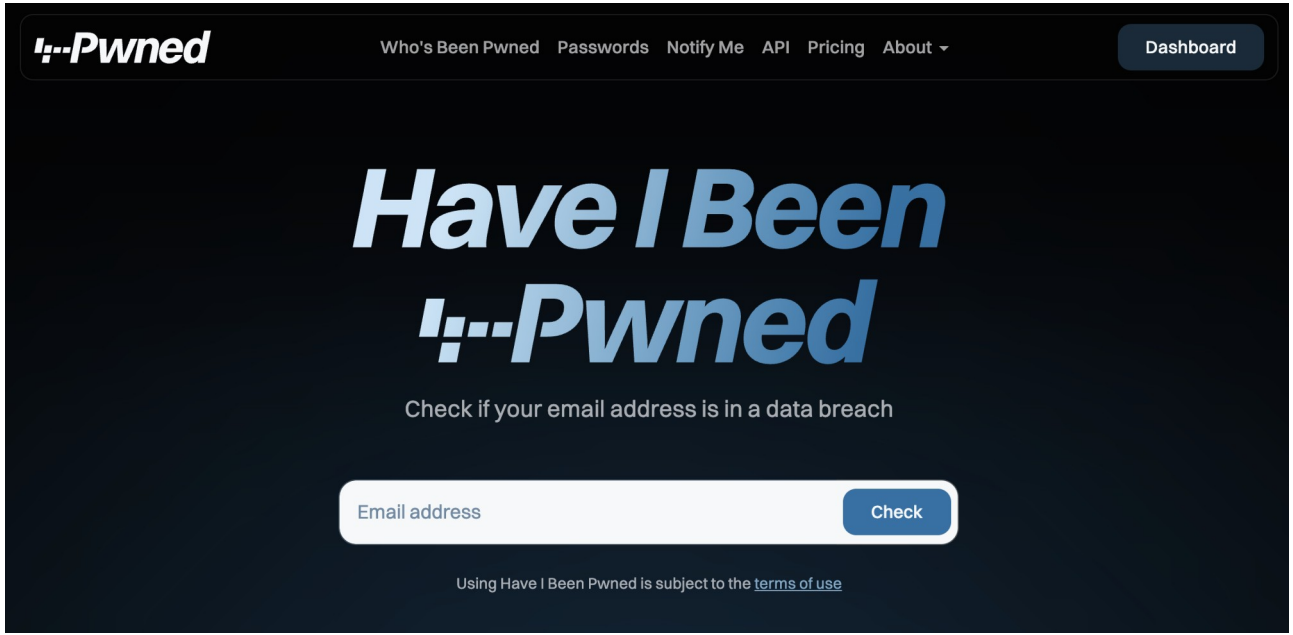
  Im Datenleck von 2012 wurden Passwörter von rd. 6,5 Millionen Nutzerkonten gestohlen.

- Veröffentlichung Facebook-Anmeldedaten in 2019

  Rund 267 Millionen Facebook-Anmeldedaten wurden im Darknet veröffentlicht.

https://de.wikipedia.org/wiki/Liste_von_Datendiebst%C3%A4hlen

Wenns schiefgeht – Datenpannen & Leaks



https://haveibeenpwned.com/

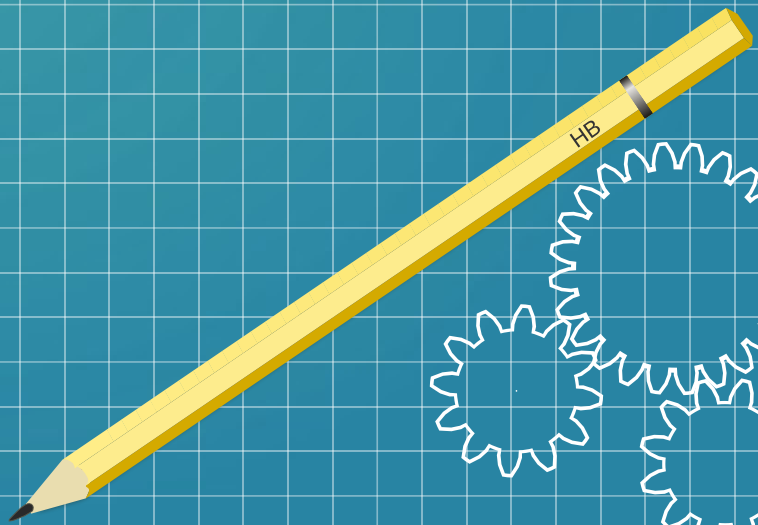
Die Lösung: Passwortmanager

Ein Tresor für deine digitalen Schlüssel

- Zentral, verschlüsselt, überall dabei
- Nur ein Masterpasswort merken – der Rest ist sicher gespeichert
- Generierung starker, individueller Passwörter
- Verfügbarkeit auf Desktop, Browser, Smartphone
- Sicherheit durch Zero-Knowledge-Prinzip

Ein Passwortmanager ist keine Option mehr, sondern Voraussetzung für digitale Sicherheit!

Marktüberblick



Marktüberblick kommerzielle Anbieter (Auswahl)

Überblick Open Source-Lösungen (Auswahl)

Vor- und Nachteile

Kategorie	Open Source	Kommerziell
Kosten	Meisten kostenfrei (Self-Hosting)	Meist Abo-basiert (monatlich/jährlich)
Transparenz	Open Source (auditierbar)	Closed Source (Vertrauen nötig)
Self-Hosting	Möglich (z.B. Vaultwarden)	Meist nicht vorgesehen
Support	Community-gestützt	Professioneller Support, SLAs möglich
Sicherheit	Hängt von Setup und Nutzung ab	Meist Audits & Zertifizierungen
Updates	Von Community abhängig	Regelmäßige Updates, klare Roadmaps

Fazit

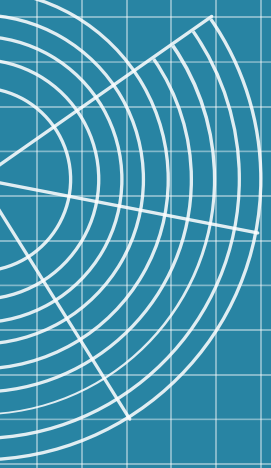
Open Source

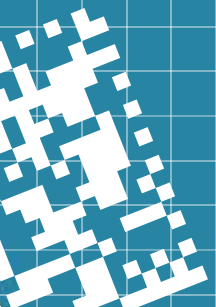
Ideal für Self-Hoster, Datenschutz-Enthusiasten und Techniker

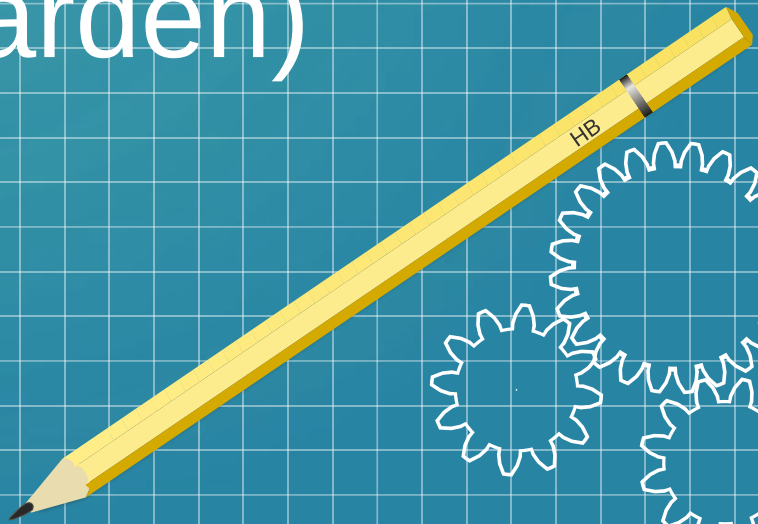
Kommerziell

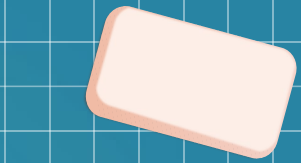
Gut für Einsteiger und Firmen, die bequeme, wartungsfreie Lösungen suchen.

Live-Demo
(am Beispiel Bitwarden)

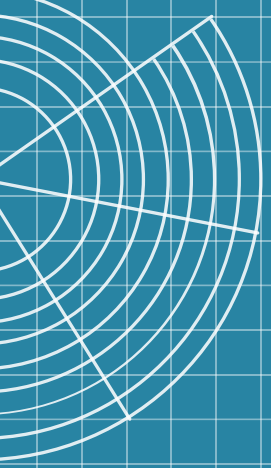


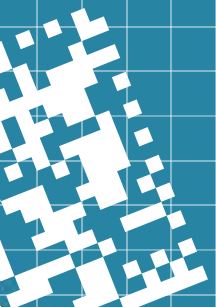


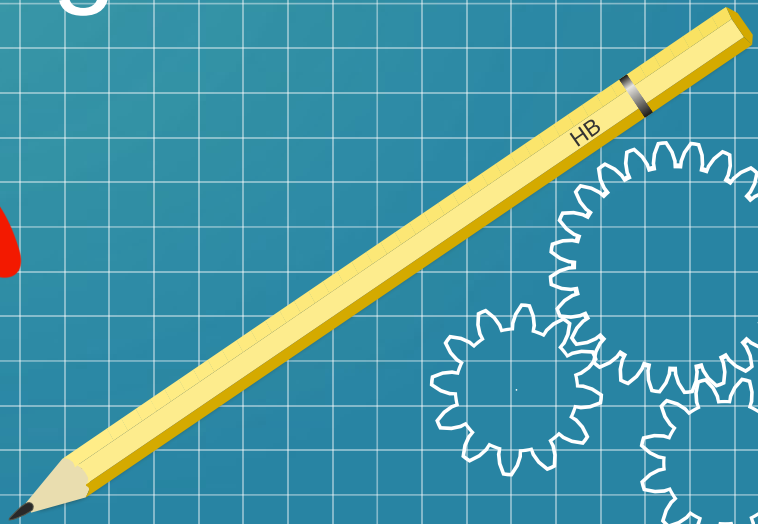




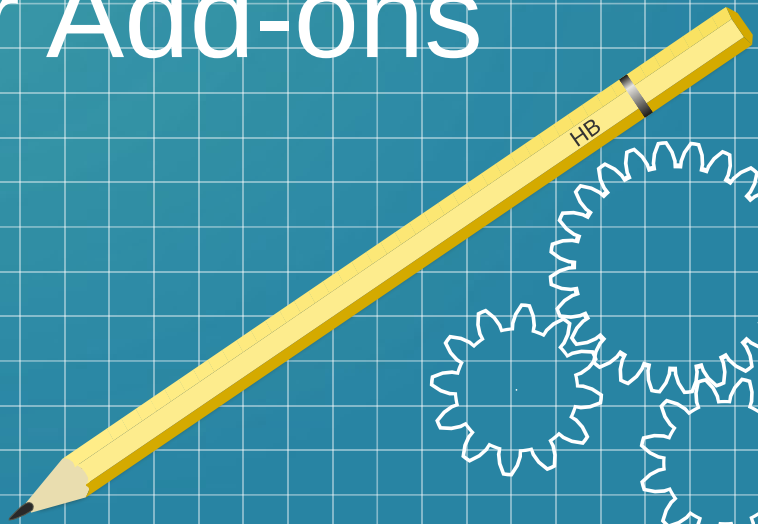
Vaultwarden kurz vorgestellt







Clickjacking-Angriff bei Autofill in Browser Add-ons



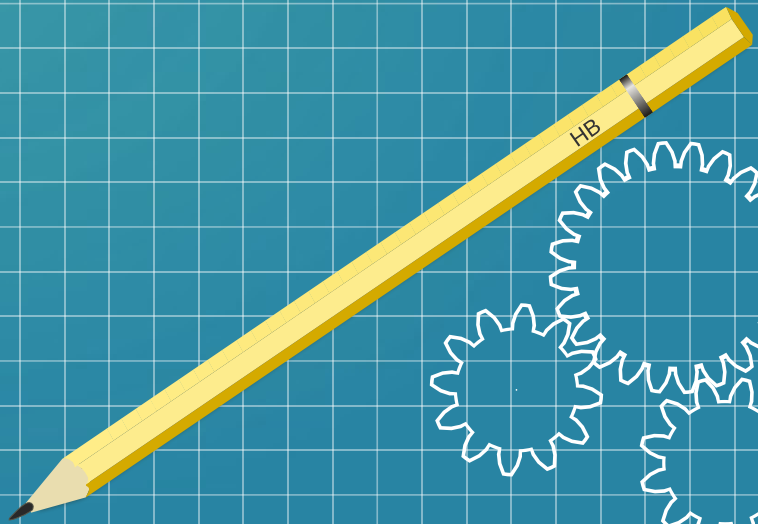
Das Wichtigste in Kürze

- Auf der DEF CON 33 stellte der Security-Forscher Marek Tóth einen Clickjacking-Angriff vor, der Autofill-In Browser-Add-ons ausnutzt.
- Der Angriff nutzt unsichtbare Overlays oder manipulierte DOM-Elemente, sodass ein Nutzer-Klick (z.B. auf „Cookies akzeptieren“) ungewollt das Autofill auslöst – und Anmeldedaten oder Kreditkarteninformationen an Angreifer verschickt werden.

Was kann ich tun?

- Nicht in Panik ausbrechen!
- Passwort-Manager regelmäßig updaten.
- Auto-Ausfüllen in Formularfelder abschalten.
- Die Übereinstimmungserkennungsmethode spezifischer als „Basisdomäne“ gestalten.
- Die automatische Tresorsperre (Automatische Sperrung nach X Minuten) möglichst kurz halten.

Sicherheit und Best Practices



So nutzt Du Passwortmanger richtig

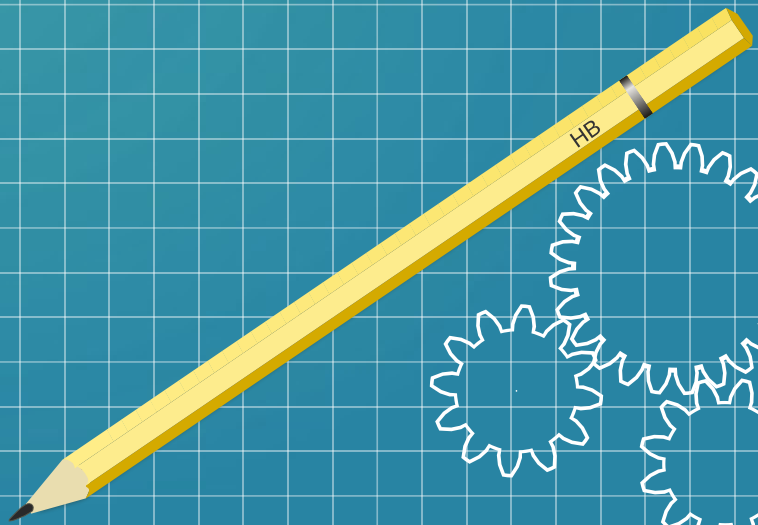
- Ein starkes Masterpasswort wählen
  → mindestens 12-16 Zeichen
  → gerne auch einen ganzen Satz; z.B.:
  „Sch!ldkröt3n planen die Weltherrschaft langsam.“
- Zwei-Faktor-Authentifizierung (2FA) aktivieren
- Für jeden Dienst ein eigenes Passwort
  → der Passwortmanager generiert sie automatisch!
- Keine Passwort-Exporte unverschlüsselt speichern
- Regelmäßige Backups machen (bei Self-Hosting)
- Geräte absichern (PIN, Festplattenverschlüsselung)

Bonus-Tipp

Passwortmanager sind wie Zahnbürsten:

Du brauchst sie mehrfach täglich, sie sollten gut gepflegt sein und du solltest sie mit niemanden teilen!

Fragen und Antworten



Vielen Dank für Eure Aufmerksamkeit