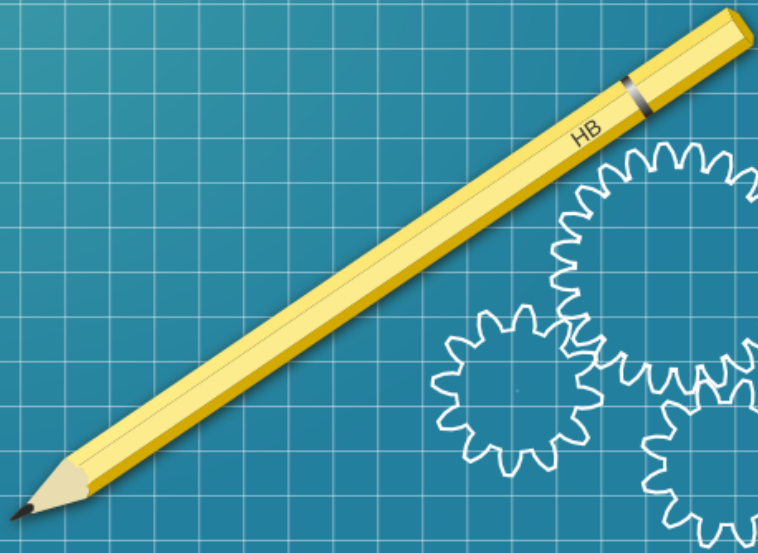
Vaultwarden
Open Source
Selbstgehosteter Passwort Manager

Linux Cafe Vortrag
vom 01.02.2023



Anmerkung zum Vortrag

- Der hier gezeigte Weg ist nur einer von sehr vielen um Vaultwarden zu installieren.
- Für diesen Vortrag habe ich eine Methode gewählt die für eine Installation und auch die Absicherung (Sicherheit) am einfachsten ist.

- **Jegliche Verantwortung bei der Umsetzung auch bei Datenverlust oder Fehlkonfiguration etc. liegt bei dir selbst. Der hier gezeigte Weg wurde nach bestem Wissen und Gewissen zusammengestellt. Die Aktualität, Richtigkeit und Vollständigkeit kann also abweichen!**

  Sei dir dem Risiko also Bewusst und Installiere und nutze Vaultwarden auf eigene Gefahr!

Ablauf des Vortrages

1. Grundwissen über Passwort Manager
2. Praktischer Teil – wir Installieren Vaultwaren zusammen
3. eure Fragen werden beantwortet

Was ist ein Passwort Manager

- Es handelt sich um eine Anwendung, wo Passwörter sicher aufbewahrt werden können.

- Ein Passwort-Manager, auch Kennwort- oder Passwortverwaltung (englisch Password Manager, Password Safe) genannt, ist eine Anwendungssoftware, mit deren Hilfe ein Computer-Benutzer Zugangsdaten und Geheimcodes verschlüsselt speichern, verwalten und verwenden kann. Entsprechende Anwendungsprogramme sind plattformübergreifend für Desktop-Computer und Laptops wie für Smartphones verfügbar.

  Quelle: https://de.wikipedia.org/wiki/Kennwortverwaltung

Warum sollte man einen Passwort Manager verwenden?

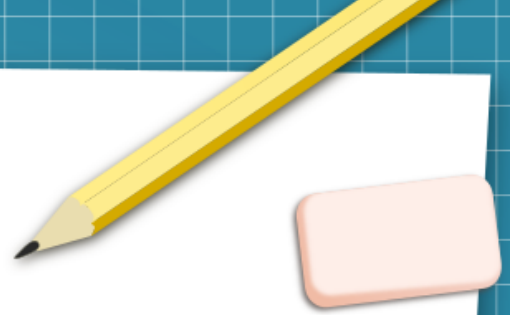
- Es sollte für jede Webseite / Login wo Passwörter verwendet werden ein eigenes individuelles Passwort genutzt werden.
- Wenn immer das gleiche oder ähnliche Passwörter verwendet werden geht man ein großes Risiko ein! Sollten Webseiten Opfer von Hackern werden können so ganz einfach mehrere Webseiten etc. übernommen werden!
- Passwort Manager generieren automatisch für jede Webseite sichere Passwörter ohne das du dir Gedanken über das Passwort machen musst.
- Weitere Infos

  https://de.wikipedia.org/wiki/Kennwortverwaltung

Vorteile eines Passwort Managers

- Man muss sich nur 1 „Master Passwort“ merken um dann auf alle Passwörter Zugriff zu haben
- Passwörter / Logins sind in einer Anwendung gespeichert und nicht auf Zetteln oder Dateien auf einem Endgerät (meistens sogar Unverschlüsselt) abgespeichert.
- Für jede Webseite wird eine eigenes Individuelles Passwort genutzt, was man sich nicht merken muss, da die Verwaltung und Organisation komplett vom Passwort Manager übernommen wird.

Ich nutze schon einen Passwort Manager



- Dann hast du bereits jetzt schon eine gute Entscheidung getroffen!
- Es gibt viele Passwort Manager Programme, hier führe ich ein paar auf:

  KeePass - ist ein freies, unter den Bedingungen der GNU General Public License (GPL)

  KeePassX - ist eine Variante von KeePass für Windows, Linux, macOS und OS/2 basierend auf Qt, die nicht mehr weiter entwickelt wird.)

  KeePassXC - (KeePassX Reboot) ist eine plattformübergreifende Abspaltung von KeePassX mit zusätzlichen Features.

  LastPass - ist ein webbasierter Passwortmanager-Online-Dienst des Unternehmens GoTo

  1Password - ist ein Online-Dienst zum Passwort-Management, entwickelt vom kanadischen Unternehmen AgileBits Inc

  Quellen: https://de.wikipedia.org/wiki/Kennwortverwaltung + https://de.wikipedia.org/wiki/KeePass + https://de.wikipedia.org/wiki/LastPass + https://de.wikipedia.org/wiki/1Password

Warum sollte man keine Kommerzielle Lösung nutzen?

- Kommerzielle Lösungen können von einen auf den anderen Tag den Dienst einstellen oder in ein Freemium-Modell umgewandelt werden.

  (Freemium ist ein Geschäftsmodell, bei dem das Basisprodukt gratis angeboten wird, während das Vollprodukt und Erweiterungen kostenpflichtig sind)
- Sind immer Closed Source / Proprietäre Software also nicht Quelloffen (Sicherheit kann nicht unabhängig Bestätigt werden).
- Können Opfer von Hackern werden, zuletzt war dies bei LastPass im Dezember 2022 der Fall!
- Man Vertraut seine Passwörter einer fremden Firma an.
- Man muss vertrauen haben, das Passwörter sicher vor Zugriff durch den Anbieter oder anderer „Dritter“ sind. Würdest du deinen Haustürschlüssel / Schlüssel einer Fremden Person geben?

  Quellen: https://de.wikipedia.org/wiki/Freemium

Vorteile von Vaultwarden

- Passwörter können von überall Abgerufen werden
- Passwörter werden an einer Zentralen Stelle verwaltet / gespeichert
- Passwörter sind auf jedem Endgerät (PC, Laptop, Handy...) immer den gleichen Stand und man muss sich somit nicht Gedanken darum machen auf welchem Endgerät der aktuellste Passwort Stand ist bzw. war!
- Kann zuhause z.B. auf einem Raspberry Pi oder auch Virtualisiert (z.B. Proxmox) installiert und genutzt werden.
- Hat viele Funktionen, die Bitwarden nicht hat, der größte Vorteil ist das der Passwort Manager mit einer Zwei-Faktor-Authentisierung genutzt werden kann (E-Mail, YubiKey, Nitrokey und Solokey)
- Vorhandene Passwort Datenbanken z.B. von KeePass etc. können importiert werden um somit nicht wieder von vorne anfangen zu müssen Passwörter abzuspeichern!

Unterstützte Funktionen

Anmerkung zum Vortrag

- Der hier gezeigte Weg ist nur einer von sehr vielen um Vaultwarden zu installieren.
- Für diesen Vortrag habe ich eine Methode gewählt die für eine Installation und auch die Absicherung (Sicherheit) am einfachsten ist.

- **Jegliche Verantwortung bei der Umsetzung auch bei Datenverlust oder Fehlkonfiguration etc. liegt bei dir selbst. Der hier gezeigte Weg wurde nach bestem Wissen und Gewissen zusammengestellt. Die Aktualität, Richtigkeit und Vollständigkeit kann also abweichen!**

  Sei dir dem Risiko also Bewusst und Installiere und nutze Vaultwarden auf eigene Gefahr!

Praktischer Teil

Was wird für diesen Vortrag benötigt?

- Raspberry Pi z.B. 2er besser ist ein 3er
- SD-Karte
- USB Stick am besten auch ein NAS(Netzwerk Speicher) → beides für Backups
- BalenaEtcher - https://www.balena.io/etcher/
- Raspberry Pi Imager + Raspberry Pi OS Lite
- DynDNS Dienst z.B.: IPv64.net oder noIP.at ...
- Portfreischaltung im Router: Port 80 (HTTP) + 443 (HTTPS) (Vaultwarden ist damit dann von überall erreichbar)

Habt ihr Fragen?