

Vaultwarden

Alternative inoffizielle Implementierung des Bitwarden Servers in Rust. Open Source & 100% kostenlos zum selber hosten. Bitwarden Client wird komplett unterstützt und kann problemlos verwendet werden.

- [Übersicht](#)
- [Installation](#)
- [Mail & Send konfigurieren](#)
- [Admin Seite aktivieren](#)

Übersicht

Bei Vaultwarden handelt es sich um eine Implementierung der Community des Bitwarden Servers in Rust. Der Server kann komplett kostenlos selbst gehostet werden z. B. als Docker Container. Der vollständige Code sowie die Dokumentation kann hier eingesehen werden: [Vaultwarden GitHub](#)

Vaultwarden unterstützt die folgenden (Bitwarden-)Features:

- Organisationen
- Ordner zum Gruppieren
- Sammlungen zum Teilen von Passwörtern
- Anhänge und die Funktion *Senden*
- Vault API Unterstützung
- Statische Dateien für Vault Instanz zur Verfügung stellen
- Webseiten Icons API
- Authenticator und 2 Faktor
- YubiKey und Duo
- Notfallzugriff
- Anbindung von Bitwarden Clients
- Weboberfläche (Zugriff ohne Client von jedem Gerät aus)

In allen Bitwarden Clients kann ein Vaultwarden Server als URL hinterlegt werden anstelle eines "richtigen" Bitwarden Servers. Es stehen trotzdem alle Funktionen zur Verfügung.

Tresor

Der Tresor eines Benutzers sieht im Web beispielsweise wie folgt aus.



FILTER



Tresor durchsuchen

- Alle Tresore
 - Mein Tresor
 - CIA
 - FBI
 - Neue Organisation
- Alle Einträge
 - Favoriten
 - Zugangsdaten
 - Karte
 - Identität
 - Sichere Notiz
- Ordner
 - Family
 - Schule
 - Test-Server
 - Webshops
 - Kein Ordner
- Papierkorb

Alle Tresore

Neu

<input type="checkbox"/> Alle	Name	Besitzer	
<input type="checkbox"/>	Amazon	Ich	⋮
<input type="checkbox"/>	AWS	Ich	⋮
<input type="checkbox"/>	Bookstack	Ich	⋮
<input type="checkbox"/>	eBay	Ich	⋮
<input type="checkbox"/>	Mail Account Mr. President	FBI	⋮
<input type="checkbox"/>	Schuldenkonto Trump	CIA	⋮
<input type="checkbox"/>	Twitter/X Account Elon	CIA	⋮

Send

Im Menü *Send* können z. B. Passwörter oder Texte oder ganze Dateien sicher geteilt werden über einen Link samt Passwort sowie Ablaufzeit.



FILTER

Sends suchen

Alle Sends

- Typen
- Text
- Datei

Send

+ Neues Send



Keine aktiven Sends

Verwende Send, um verschlüsselte Informationen sicher mit anderen zu teilen.

+ Neues Send

Werkzeuge

Unter den Werkzeugen steht z. B. ein Passwort Generator zur Auswahl sowie Im- und Exportfunktionen.



- WERKZEUGE
- Generator**
- Daten importieren
- Tresor exportieren

Generator

ho&GwbaCrG!#2LRJR*p7zxA9M#8WYJ

Was möchtest du generieren?

Passwort Benutzername

Passworttyp

Passwort Passphrase

Länge

30

Minimale Passwortlänge

30

Mindestanzahl Ziffern

1

Mindestanzahl Sonderzeichen

1

Optionen

- A-Z
- a-z
- 0-9
- !@#\$\$%^&*
- Mehrdeutige Zeichen vermeiden

Passwort neu generieren

Passwort kopieren



Berichte

Einige besonders interessante Funktionen sind im Reiter Berichte zu finden, womit beispielsweise die Passwörter überprüft werden können, um mögliche Kompromittierungen zu entdecken.



Berichte

Identifiziere und schließe Sicherheitslücken in deinen Online-Konten, indem du auf die Berichte unten klickst.



Kompromittierte Passwörter

Durch Datendiebstahl aufgedeckte Passwörter sind einfache Ziele für Angreifer. Ändere diese Passwörter, um mögliche Einbrüche zu verhindern.



Wiederverwendete Passwörter

Die Wiederverwendung von Passwörtern macht es Angreifern leichter, in mehrere Konten einzubrechen. Ändere diese Passwörter so, dass jedes einzigartig ist.



Schwache Passwörter

Schwache Passwörter können von Angreifern leicht erraten werden. Ändere diese Kennwörter mithilfe des Passwort-Generators in sichere Passwörter.



Ungesicherte Websites

URLs, die mit http:// beginnen, verwenden nicht die bestmögliche Verschlüsselung. Ändere die Anmelde-URIs für diese Konten zu https:// für sicheres Surfen.



Inaktive Zwei-Faktor- Authentifizierung

Die Zwei-Faktor-Authentifizierung (2FA) ist eine wichtige Sicherheitseinstellung, die dir bei der Absicherung deiner Konten hilft. Wenn eine Webseite 2FA anbietet, solltest du es immer aktivieren.



Datendiebstahl

Kompromittierte Konten können deine persönlichen Daten preisgeben. Sichere kompromittierte Konten, indem du 2FA aktivierst oder ein sicheres Passwort erstellst.

Organisationen

In diesem Menü können neue Organisationen erstellt und bestehende verwaltet werden. Für jede Organisation lassen sich Mitglieder samt Berechtigungen einstellen sowie Richtlinien für die Mitglieder festlegen wie z. B. 2FA erzwingen.



FILTER



Sammlung durchsuche

- Alle Einträge
- Zugangsdaten
- Karte
- Identität
- Sichere Notiz
- Sammlungen**
- Nicht zugeordnet
- Standardsammlung
- Papierkorb

CIA tresor

Neu

<input type="checkbox"/> Alle	Name	Berechtigung	
<input type="checkbox"/>	Nicht zugeordnet	-	
<input type="checkbox"/>	Standardsammlung	Darf bearbeiten	

Installation

Die Installation des Vaultwarden Servers ist mit Docker schnell erledigt.

So würde z. B. folgende Docker Compose Datei bereits ausreichend sein, um eine funktionierende Instanz bereitzustellen.

```
pass:
  image: vaultwarden/server
  container_name: vaultwarden
  environment:
    - TZ=Europe/Berlin
  volumes:
    - /pfad/zu/vaultwarden/data:/data
  ports:
    - 80:80
  restart: unless-stopped
```

Um die Docker Compose Konfiguration auszuführen, kann am besten in das Verzeichnis der YAML Datei gewechselt werden. Danach wird je nach gewählter Installation `sudo docker-compose up -d` oder `sudo docker compose up -d` (keine Bindestrich zwischen docker und compose) eingegeben, um die Standard Konfiguration `docker-compose.yml` zu starten. Compose erstellt dann die gewünschten Container mit den angegebenen Optionen. Sollten die Container bereits mit dieser Compose Konfiguration erstellt worden sein, so werden die Container in dieser neu erstellt, dessen Konfiguration geändert wurde.

Nach einigen Sekunden ist die Weboberfläche von Vaultwarden unter `http://Server-IP` erreichbar.

Da Vaultwarden besonders sensible Daten wie eben Passwörter, Kreditkarteninformationen usw. speichert, sollte die Weboberfläche unbedingt mit HTTPS abgesichert werden. Die Entwickler selbst empfehlen einen Reverse Proxy, bieten jedoch auch eine eigene HTTPS Funktion über Rocket an: [Vaultwarden HTTPS](#)

Beim Aufruf der Seite erscheint das Login/Registrierungsfenster. Je nach weiterer Konfiguration (z. B. deaktivierter Registrierung) sieht diese etwas anders aus.



Sie müssen sich anmelden oder ein neues Konto erstellen, um auf den Tresor zugreifen zu können.

E-Mail-Adresse (erforderlich)

⊗ Eingabe ist erforderlich.

E-Mail-Adresse merken

Fortsetzen

Neu hier? [Konto erstellen](#)

Vaultwarden Web
Version 2024.1.2

A modified version of the Bitwarden® Web Vault for Vaultwarden (an unofficial rewrite of the Bitwarden® server).
Vaultwarden is not associated with the Bitwarden® project nor Bitwarden Inc.

Mail & Send konfigurieren

Für einige Funktionen wie z. B. das Senden von Passwörtern / Geheimnissen ist ein E-Mail Konto samt SMTP-Server anzugeben.

Steht dieser zur Verfügung, am besten ein eigenes Postfach für Vaultwarden erstellen.

Danach die Docker Compose Konfiguration wie folgt erweitern.

```
environment:
  - SENDS_ALLOWED=true
  - SMTP_HOST=smtp.beispiel.de
  - SMTP_FROM=vaultwarden@beispiel.de
  - SMTP_FROM_NAME=Vaultwarden
  - SMTP_SECURITY=starttls
  - SMTP_PORT=465
  - SMTP_USERNAME=vaultwarden
  - SMTP_PASSWORD=EinRichtigStarkes20+ZeichenPasswort
#   - SMTP_TRUSTSERVER=true
```

Die Option *SENDS_ALLOWED* aktiviert die Funktion zum Senden von Passwörtern / Geheimnissen. Alle anderen Optionen, die mit *SMTP_* beginnen, konfigurieren die Einstellungen für den E-Mails Server sowie das Postfach.

Die Option *SMTP_TRUSTSERVER* wurde auskommentiert. Sofern es einen Zertifikatsfehler gibt, z. B. weil ein selbst signiertes Zertifikat verwendet wird, kann die Zertifikatsprüfung deaktiviert werden, indem diese Option aktiviert wird (Raute entfernen). Dies stellt jedoch eine Sicherheitsgefährdung dar und sollte nicht verwendet werden. Es sei denn, die Container sind direkt über den Host miteinander verbunden und kommunizieren nur Docker Intern.

Anschließend wie gewohnt die Compose Konfiguration neu laden und die Container neu erstellen lassen.

Um die Docker Compose Konfiguration auszuführen, kann am besten in das Verzeichnis der YAML Datei gewechselt werden. Danach wird je nach gewählter Installation `sudo docker-compose up -d` oder `sudo docker compose up -d` (keine Bindestrich zwischen docker und compose) eingegeben, um die Standard Konfiguration `docker-compose.yml` zu starten. Compose erstellt dann die gewünschten Container mit den angegebenen Optionen. Sollten die Container bereits mit dieser Compose Konfiguration erstellt worden sein, so werden die Container in dieser neu erstellt, dessen Konfiguration geändert wurde.

Admin Seite aktivieren

Wenn gewünscht, kann eine Admin Seite aktiviert werden, über die sich Benutzer einladen, verwalten und löschen lassen.

Die Admin Seite wird über einen sog. Admin Token abgesichert. Mit diesem Token kann die Adminoberfläche geöffnet werden. Der Token kann eine beliebige Zeichenkette sein. Diese sollte möglichst lang sein, gut geschützt und geheim gehalten werden.

Die Aktivierung erfolgt durch eine zusätzliche Environment Variable in der Compose Konfiguration.

```
environment:  
  - ADMIN_TOKEN=hier_der_extra_lange_laaaange_token
```

Anschließend wie gewohnt die Compose Konfiguration neu laden und die Container neu erstellen lassen.

Um die Docker Compose Konfiguration auszuführen, kann am besten in das Verzeichnis der YAML Datei gewechselt werden. Danach wird je nach gewählter Installation `sudo docker-compose up -d` oder `sudo docker compose up -d` (keine Bindestrich zwischen docker und compose) eingegeben, um die Standard Konfiguration `docker-compose.yml` zu starten. Compose erstellt dann die gewünschten Container mit den angegebenen Optionen. Sollten die Container bereits mit dieser Compose Konfiguration erstellt worden sein, so werden die Container in dieser neu erstellt, dessen Konfiguration geändert wurde.

Danach ist ein neuer Unterordner in der URL verfügbar: <http://Server-IP/admin>

Auf der neuen Seite können auch alle Einstellungen am Server geändert werden, die bisher über die Docker Compose Konfiguration geändert wurden, wie z. B. SMTP-Server.

Configuration

NOTE: The settings here override the environment variables. Once saved, it's recommended to stop setting them to avoid confusion. This does not apply to the read-only section, which can only be set via environment variables. Settings which are overridden are shown with a yellow colored background .

General settings

Advanced settings

Yubikey settings

Global Duo settings (Note that users can override them)

SMTP Email Settings

Email 2FA Settings

Read-Only Config

Backup Database

Save

Reset defaults