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

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

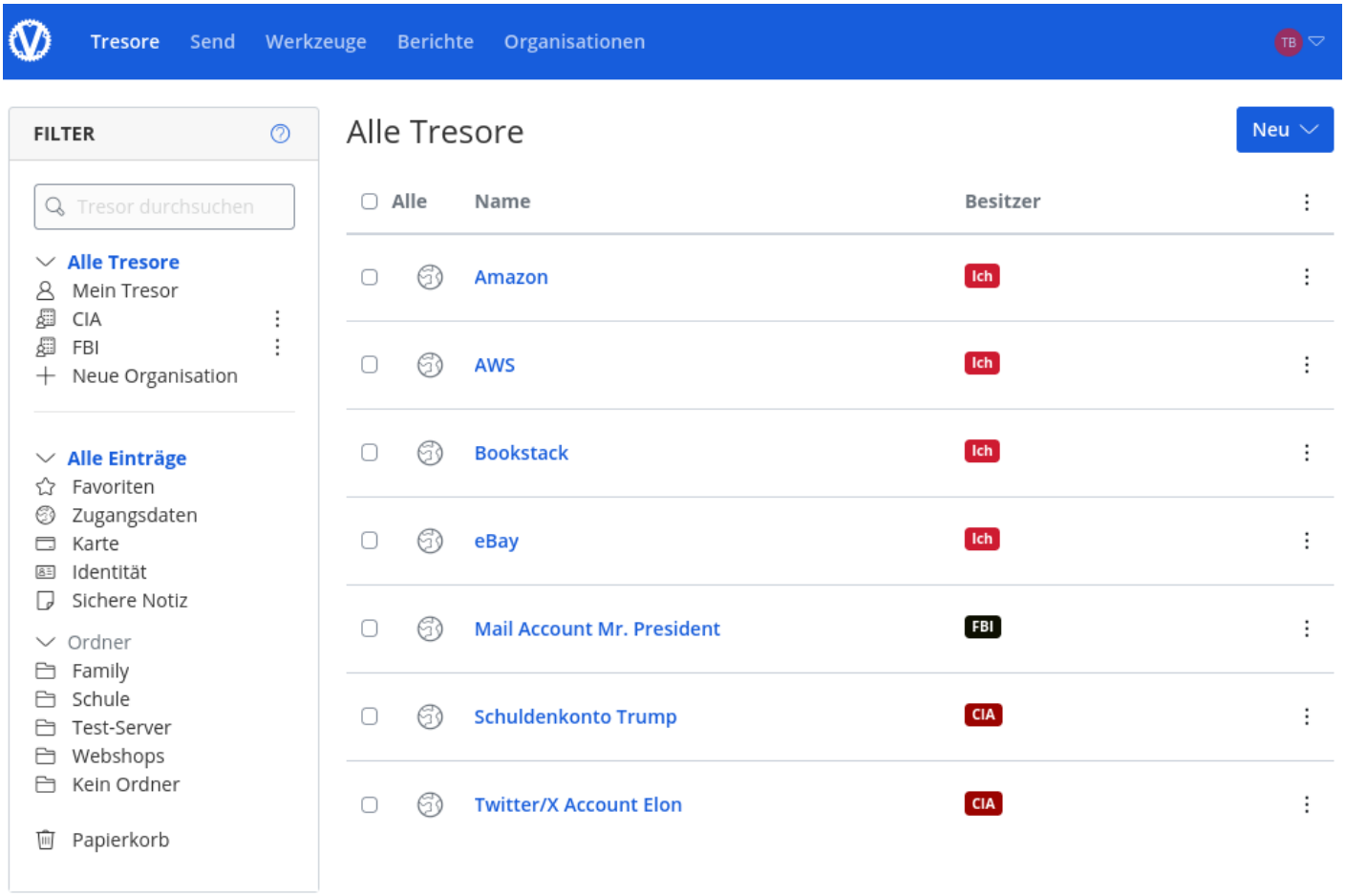
Vaultwarden unterstützt die folgenden (Bitwarden-)Features:

- 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.

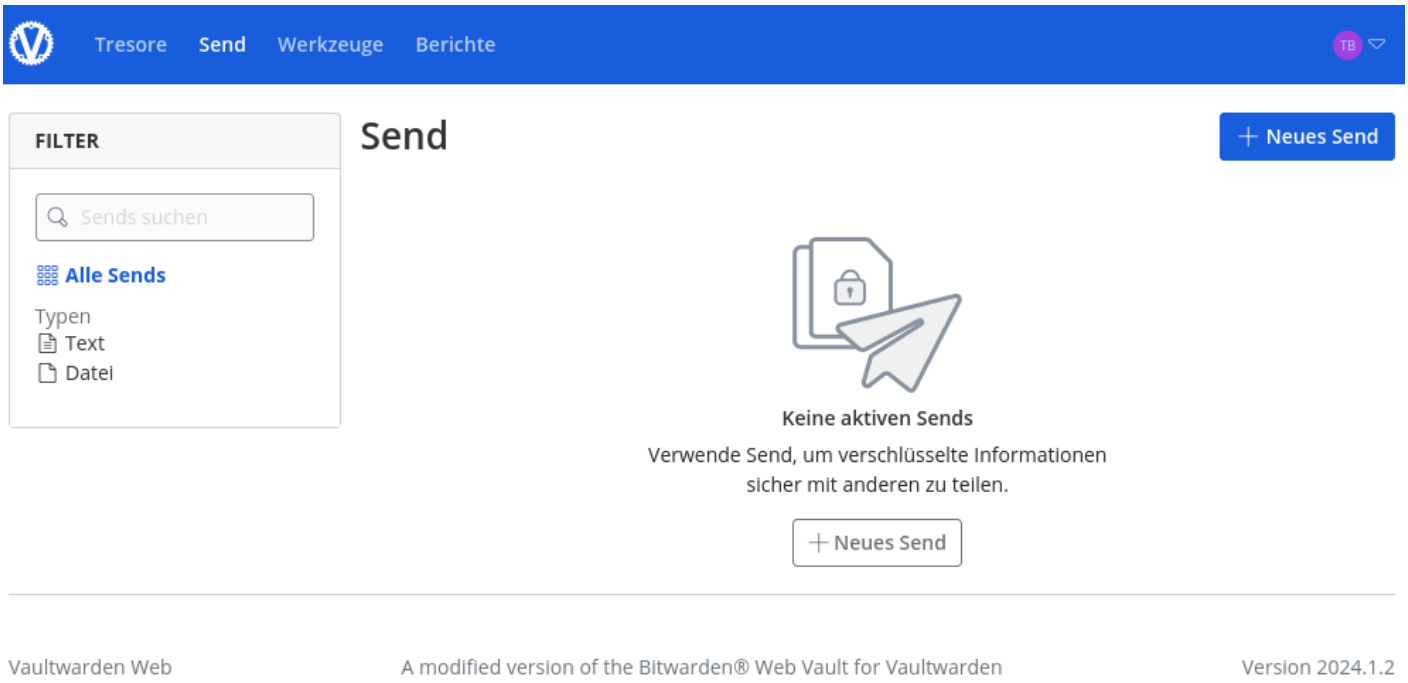
Tresor

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



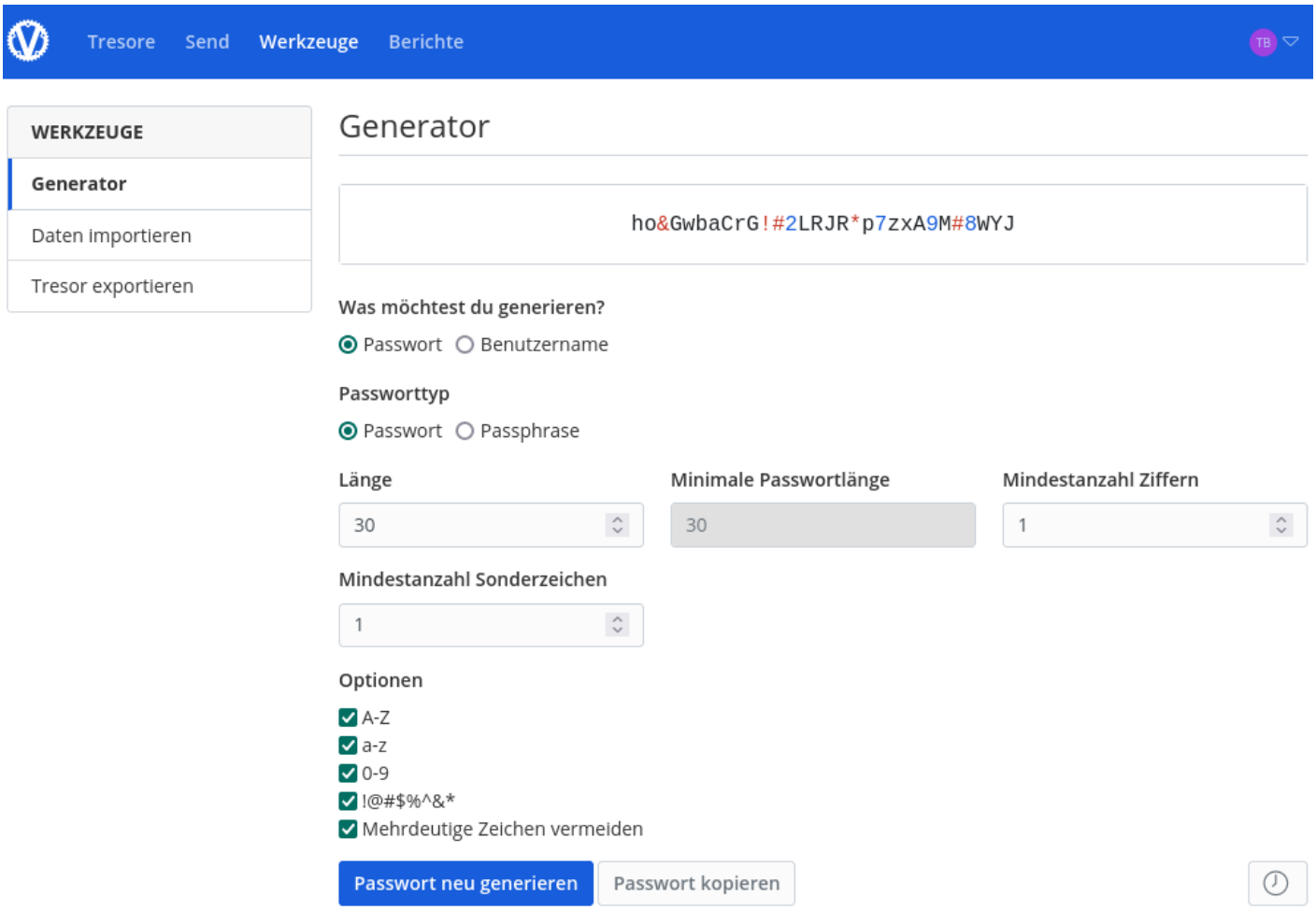
Send

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



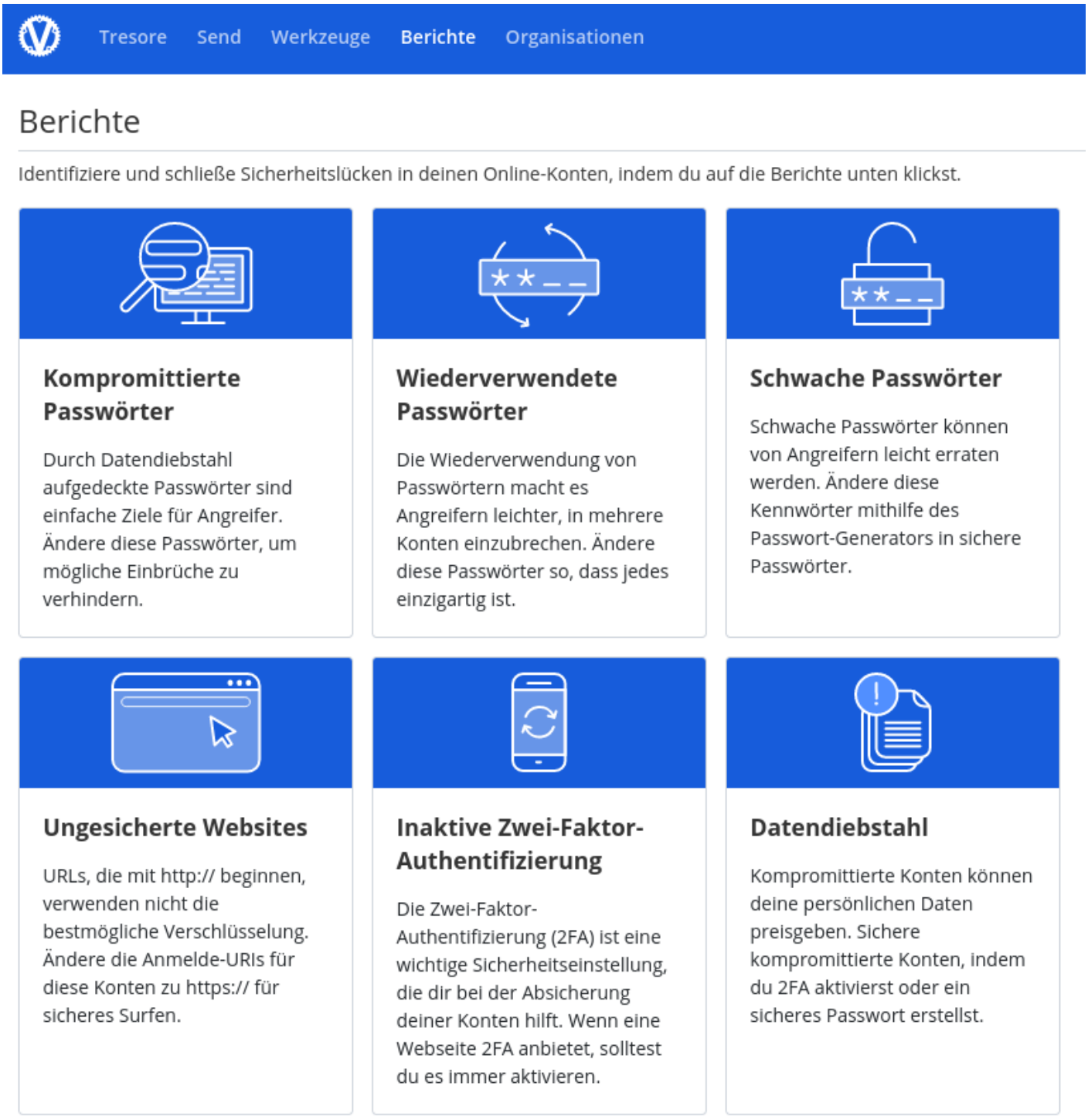
Werkzeuge

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



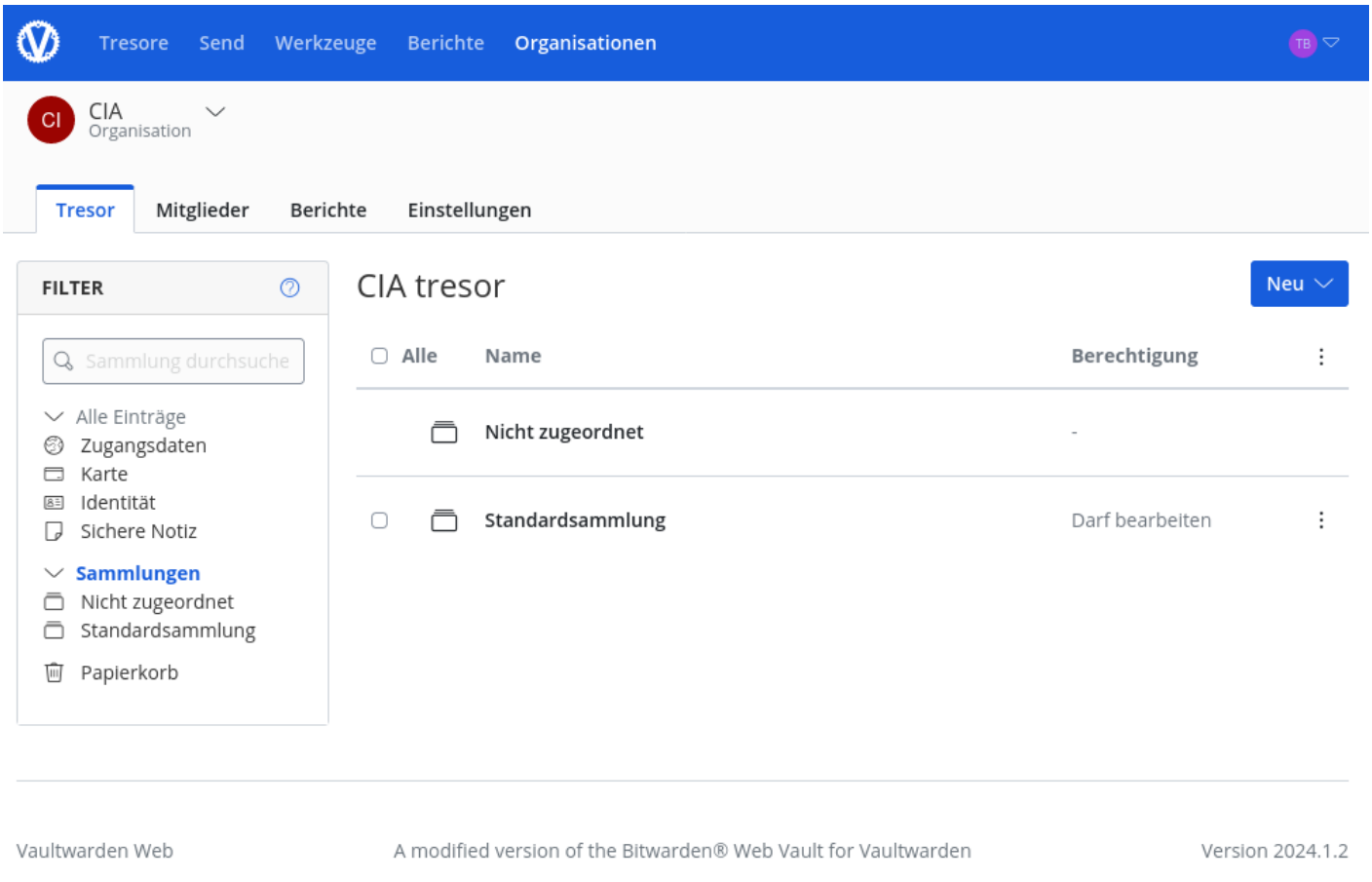
Berichte

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



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.


Tresore
Send
Werkzeuge
Berichte
Organisationen
TB
CI
CIA
Organisation
Tresor
Mitglieder
Berichte
Einstellungen
FILTER
Sammlung durchsuche
Alle Einträge
Zugangsdaten
Karte
Identität
Sichere Notiz
Sammlungen
Nicht zugeordnet
Standardsammlung
Papierkorb
CIA tresor
Neu
Alle
Name
Berechtigung
Nicht zugeordnet
-
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 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 angegeben 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.

Vaultwarden

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

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 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 angegeben 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.

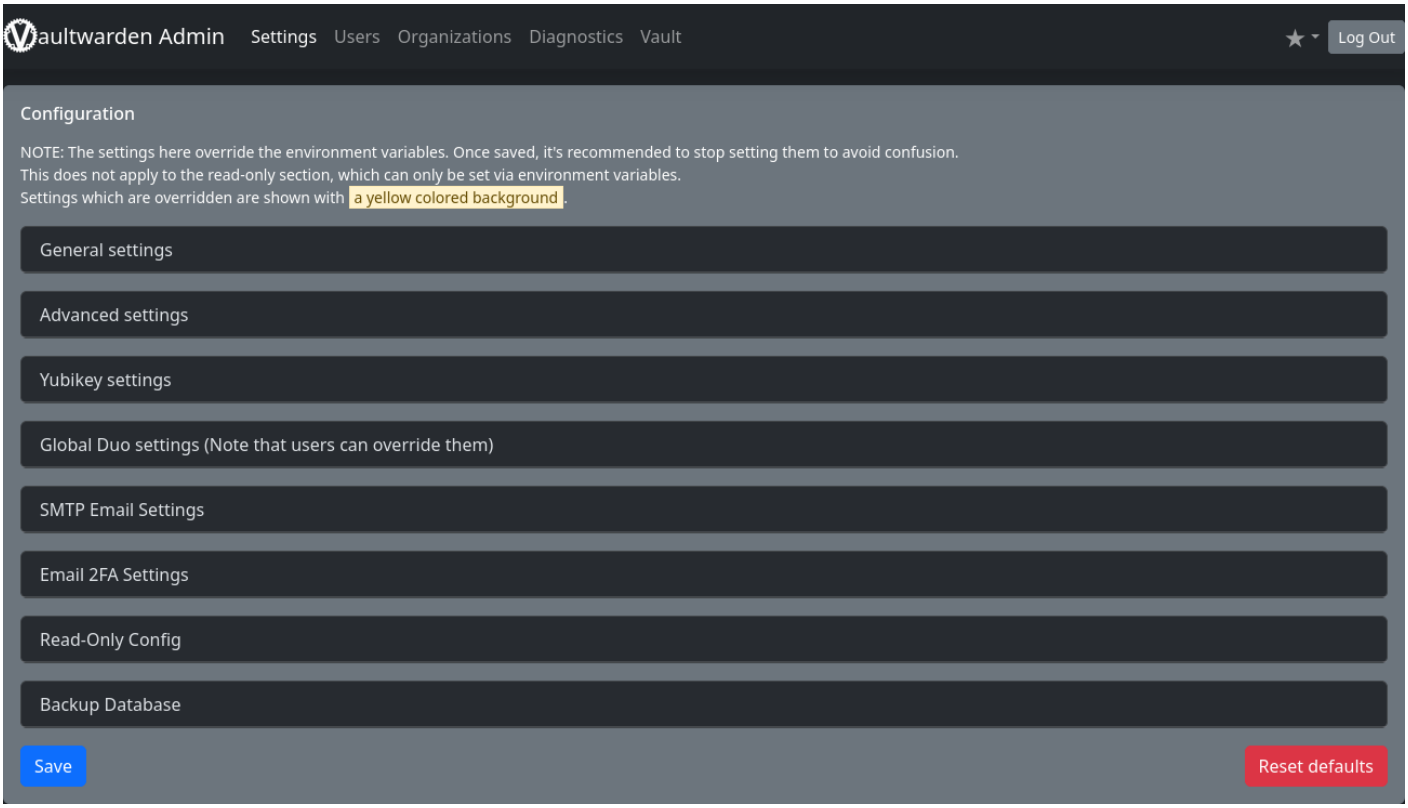
```
    environment:
      - ADMIN_TOKEN=hier_der_extra_lange_laaaange_token
```

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 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 angegeben 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.


Vaultwarden Admin
Settings
Users
Organizations
Diagnostics
Vault
Log Out
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