Poznajemy Vaultwardena

Opowieść i mapa książki.

- Vaultwarden: sejf na hasła, który trzymamy u siebie

Vaultwarden: sejf na hasła, który trzymamy u siebie

Poziom: podstawy **Dotyczy: Vaultwarden 1.37** **Czas: ~15 min**

Ta strona otwiera książkę o Vaultwardenie: skąd wziął się pomysł na własny sejf na hasła, czym Vaultwarden różni się od oficjalnego serwera Bitwardena i dlaczego Zielona w ogóle takiego sejfu potrzebowała.

Skróty użyte na tej stronie (2)

Skrót	Co znaczy
API	Application Programming Interface: sposób, w jaki programy rozmawiają ze sobą
IT	Information Technology: dział albo praca związana z komputerami i infrastrukturą firmy

Skąd się wzięło

Pojęcie: menedżer haseł. Program, który zamiast człowieka pamięta hasła do wszystkich kont, przechowuje je w zaszyfrowanej bazie odblokowywanej jednym hasłem głównym i sam wypełnia formularze logowania w przeglądarce albo w aplikacji.

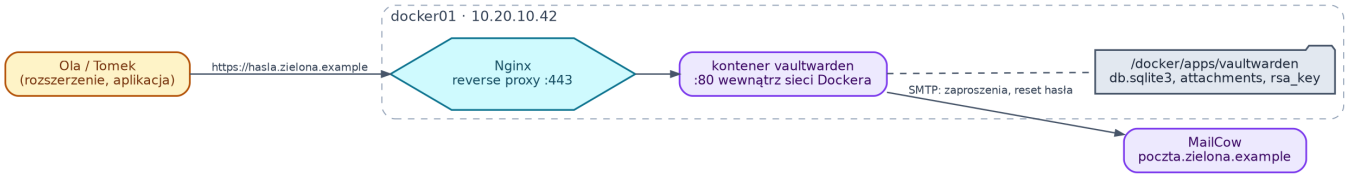
Pojęcie: Bitwarden. Menedżer haseł uruchomiony w 2016 roku, dostępny jako aplikacje na komputery, telefony i rozszerzenia przeglądarek, z częścią serwerową udostępnioną jako otwarty kod. Kod serwera Bitwardena stoi w większości na licencji AGPLv3, ale kilka katalogów z funkcjami dla dużych organizacji objęto osobną, zamkniętą licencją firmy Bitwarden. Postawienie własnego, w pełni oficjalnego serwera Bitwardena wymaga więc albo pominięcia tych fragmentów, albo zgody na ich licencję, a do tego oficjalny serwer, napisany w C# i .NET, jest zestawem kilkunastu osobnych usług: potrzebuje więcej pamięci i mocy obliczeniowej niż mała firma zwykle chce poświęcić na sam sejf haseł.

> **Pojęcie: Vaultwarden.** Niezależna implementacja serwera Bitwardena, napisana od zera w języku Rust przez dani-garcię w 2018 roku, pod pierwotną nazwą `bitwarden_rs`. Rozmawia z tymi samymi aplikacjami klienckimi co oficjalny Bitwarden (rozszerzeniem przeglądarki, aplikacją mobilną, aplikacją na komputer), bo odtwarza to samo API, ale mieści się w jednym, niewielkim pliku wykonywalnym i jednym kontenerze, bez osobnej bazy danych, kolejki wiadomości i kilku mikrousług obok.

W 2020 roku firma Bitwarden poprosiła autora o usunięcie swojej nazwy handlowej z nazwy projektu. Zamiast `bitwarden_rs` projekt przyjął nazwę Vaultwarden: `vault`, czyli sejf, i `warden`, czyli strażnik, zostawiając samo słowo Bitwarden markom, którym firma jest właścicielem. Sam projekt zostaje wolnym oprogramowaniem na licencji AGPLv3 niezależnie od tej zmiany nazwy, a Zielona korzysta właśnie z niego.

Jak to działa w jednym obrazku

Zespół w Zielonej otwiera sejf haseł przez rozszerzenie przeglądarki albo aplikację, wskazaną na adres `hasla.zielona.example`. Ruch trafia najpierw na Nginksa na `docker01`, opisanego na stronie Reverse proxy i równoważenie obciążenia, a dopiero stamtąd do kontenera Vaultwarden. Sam Vaultwarden trzyma wszystkie dane, hasła, załączniki i klucze szyfrujące, w jednym pliku bazy na dysku kontenera, a wysyłkę zaproszeń i powiadomień zleca serwerowi MailCow, opisanemu w książce o poczcie.



Architektura Vaultwarden w Zielonej: przeglądarka albo aplikacja, Nginx, kontener Vaultwarden, baza na dysku i MailCow do wysyłki poczty (kliknięcie otwiera pełny rozmiar)

Dlaczego Zielona

> **Z ŻYCIA WZIĘTE**
>
> Coroczny audyt. Pan Wojtek przegląda udziały sieciowe w poszukiwaniu czegoś, co powinno dawno zniknąć. Na `\\fs01\Ksiegowosc\Wspolne` znajduje plik `hasla.xlsx`: trzydzieści wierszy z

> nazwami systemów, loginami i hasłami w kolumnie obok, edytowany ostatnio przez cztery różne osoby na przestrzeni dwóch lat. W raporcie z audytu ten jeden plik zajmuje więcej miejsca niż wszystkie pozostałe uwagi razem wzięte.

Plik `hasla.xlsx` to najbardziej rozpowszechniony sposób trzymania haseł w małych i średnich firmach, i najgorszy zarazem. Każdy, kto ma dostęp do udziału, ma dostęp do wszystkich haseł na liście, bez względu na to, czy ich w ogóle potrzebuje. Nikt nie wie, kto plik otwierał, nie ma śladu zmiany hasła po odejściu pracownika, a kopia zapasowa udziału sieciowego to jedyne zabezpieczenie danych, które w rękach niepowołanej osoby wystarczą do zalogowania się wszędzie naraz.

Vaultwarden rozwiązuje ten problem, nie oddając kontroli nad danymi na zewnątrz. Hasła trzymamy na własnym serwerze, w sieci firmowej, tak jak dotychczas plik na udziale, ale każde konto widzi tylko to, do czego dostało dostęp przez organizację i kolekcje, opisane na stronie Pierwsza konfiguracja: panel admina, organizacja i zaproszenia. Odejście pracownika to jedno kliknięcie usuwające konto, a nie zmiana hasła współdzielonego przez cały dział, którą trzeba by rozesłać mailem do wszystkich pozostałych osób.

Mapa tej książki

Książka o Vaultwardenie prowadzi od pierwszej instalacji do codziennej pracy zespołu IT jako administratorów całego sejfu.

Strona	Na jakie pytanie odpowiada
Vaultwarden: sejf na hasła, który trzymamy u siebie	Skąd wziął się Vaultwarden i po co go mamy
Instalacja Vaultwardena w Dockerze	Jak postawić Vaultwardena w kontenerze za reverse proxy z HTTPS
Pierwsza konfiguracja: panel admina, organizacja i zaproszenia	Jak założyć organizację, kolekcje i zaprosić pierwsze osoby
Konta z Active Directory: Directory Connector i SSO	Co Vaultwarden naprawdę potrafi w zestawieniu z domeną
Kopia zapasowa i aktualizacja Vaultwardena	Jak bezpiecznie zrobić kopię bazy i podnieść wersję
Vaultwarden: częste problemy	Co robić, gdy sejf haseł przestaje działać

Powiązane: Reverse proxy i równoważenie obciążenia · Active Directory: konta, grupy, jednostki organizacyjne · MailCow · Vaultwarden: częste problemy

Źródła: github.com/dani-garcia/vaultwarden · github.com/bitwarden/server, plik `LICENSE_FAQ.md` · github.com/dani-garcia/vaultwarden, dyskusja „v1.21.0 release and project rename to Vaultwarden"