PASSWORD MANAGER > KLUISBEHEER

Kluis gezondheidsrapporten

Kluis gezondheidsrapporten

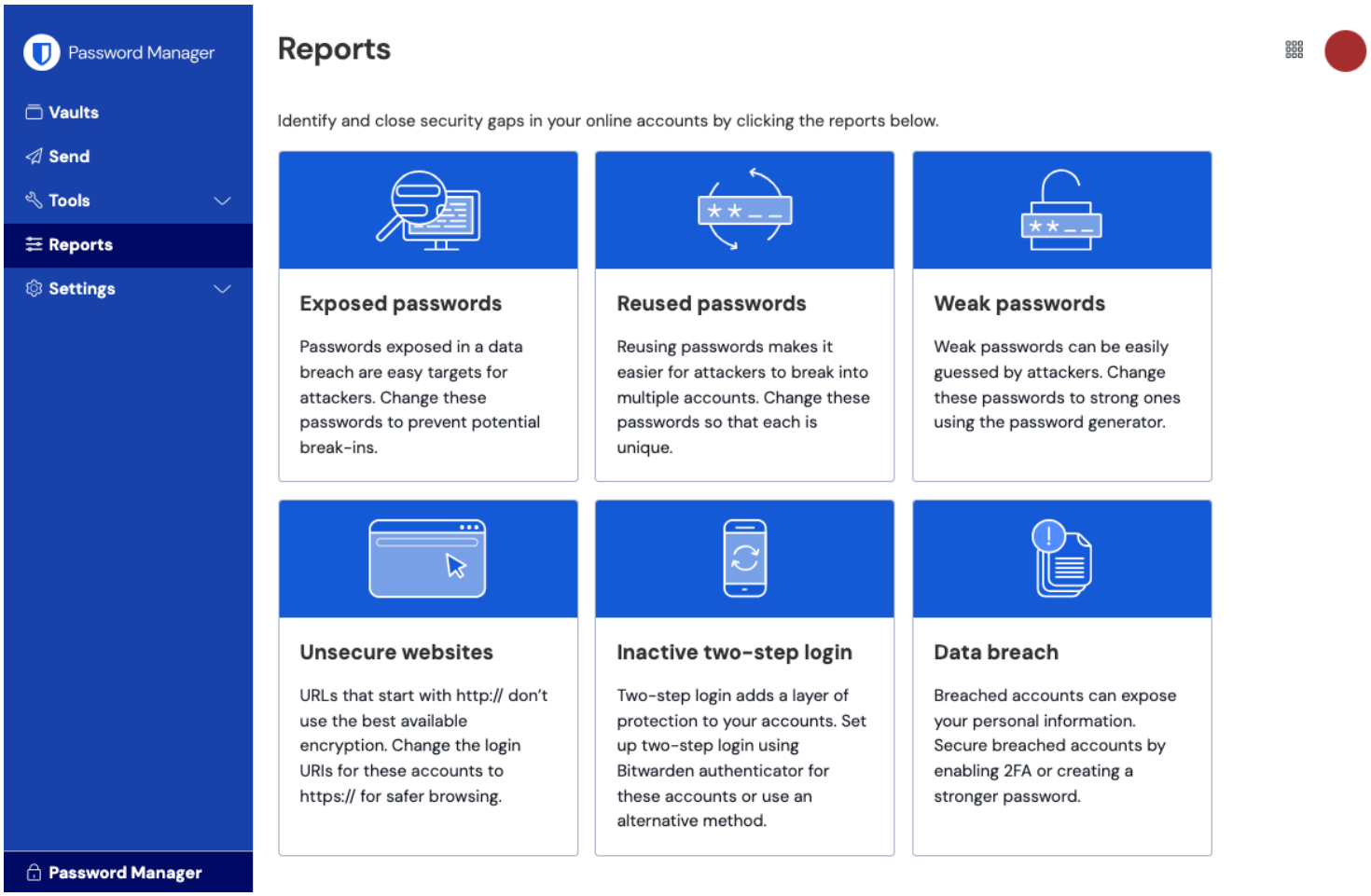
Rapporten over de gezondheid van kluizen kunnen worden gebruikt om de veiligheid van uw Bitwarden-kluis voor individuen of organisaties te evalueren. Rapporten, bijvoorbeeld het rapport Hergebruikte wachtwoorden en Zwakke wachtwoorden, worden lokaal op je client uitgevoerd. Hierdoor kunnen overtredende items worden geïdentificeerd, zonder dat Bitwarden ooit toegang heeft tot onversleutelde versies van deze gegevens.

> **Note**
>
> De meeste gezondheidsrapporten over gegevensinbreuken zijn alleen beschikbaar voor premium gebruikers, inclusief leden van betaalde organisaties (families, teams of bedrijven), maar het rapport over gegevensinbreuken is gratis voor alle gebruikers.

Een rapport bekijken

Om een gezondheidsrapport van een kluis uit te voeren voor uw **individuele kluis**:

1. Log in op de webapp en selecteer **Rapporten** in de navigatie:



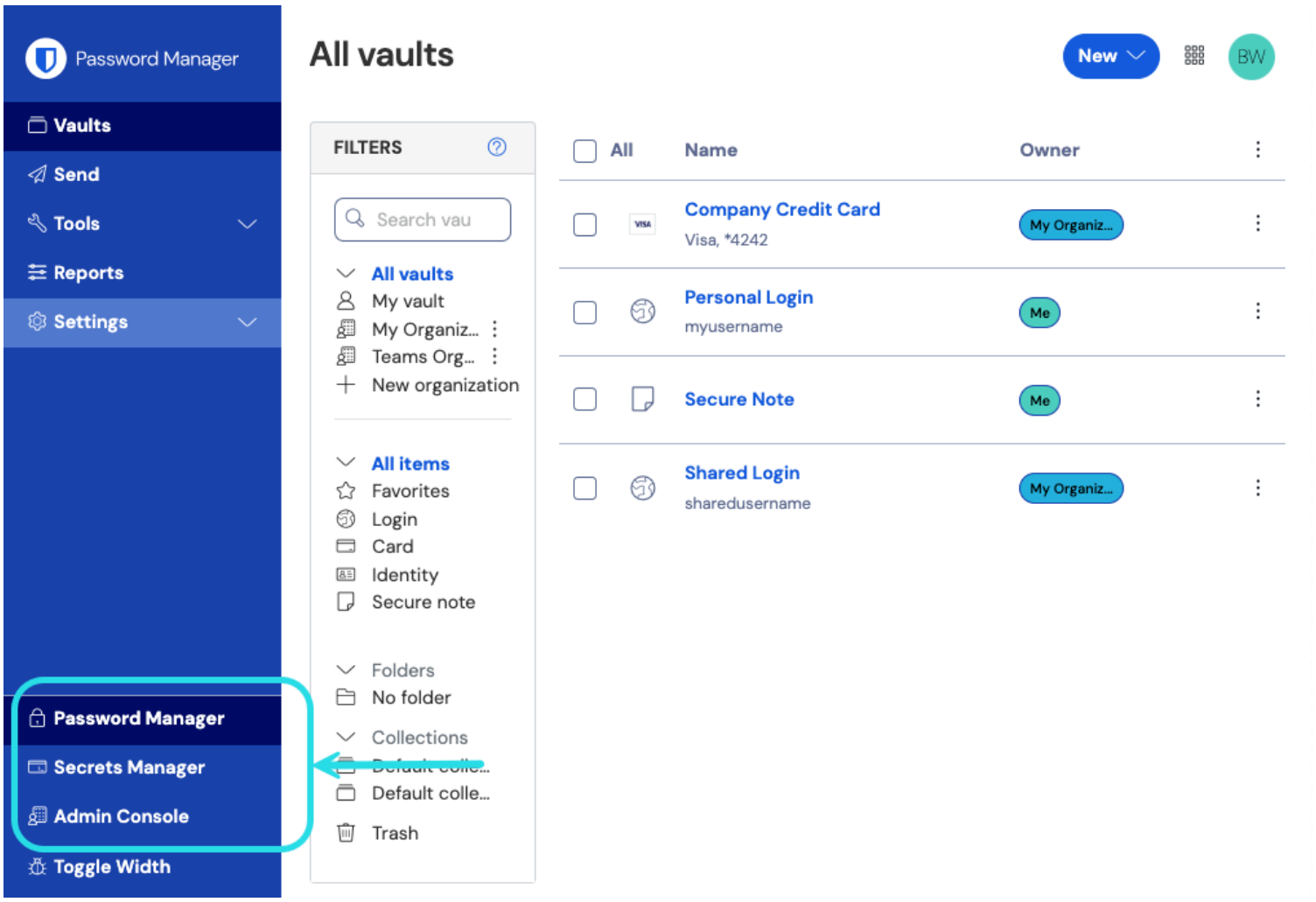
Pagina met rapporten

2. Kies een rapport om uit te voeren.

Om een gezondheidsrapport over de kluis van uw **organisatie** uit te voeren:

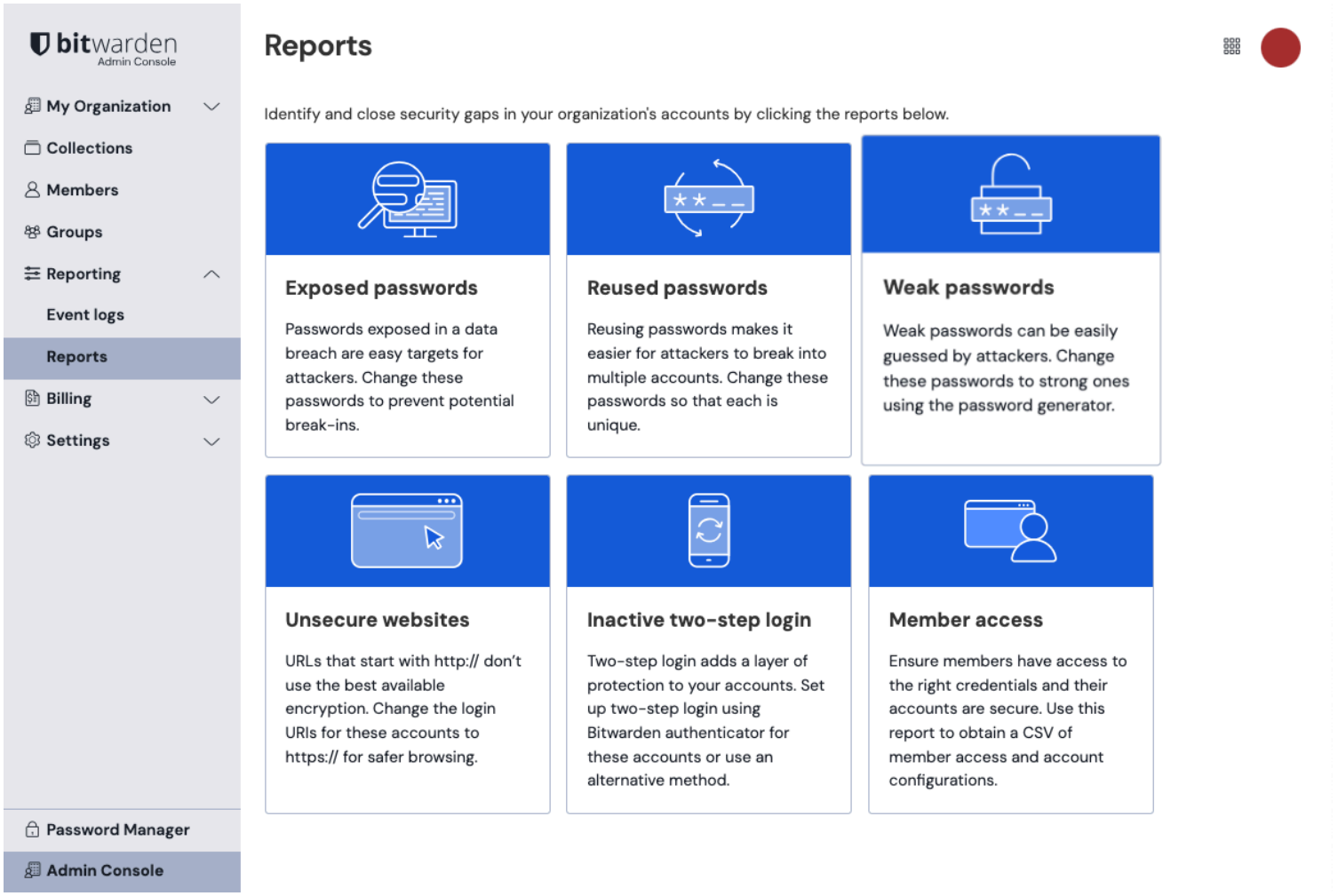
1. Log in op de Bitwarden webapp.

2. Open de beheerconsole met de productswitcher (⊞):



Product switcher

3. Selecteer in je organisatie **Rapportage** → **Rapporten** in de navigatie



Rapporten van organisaties

4. Kies een rapport om uit te voeren.

Beschikbare rapporten

Blootgestelde wachtwoorden

Het rapport Blootgestelde wachtwoorden identificeert wachtwoorden die zijn blootgelegd in bekende datalekken die openbaar zijn gemaakt of zijn verkocht op het dark web door hackers.

Dit rapport gebruikt een vertrouwde webservice om de eerste vijf cijfers van de hash van al je wachtwoorden te zoeken in een database met bekende gelekte wachtwoorden. De lijst met overeenkomende hashes wordt dan lokaal vergeleken met de volledige hash van je wachtwoorden. Die vergelijking wordt alleen lokaal uitgevoerd om je k-anonimiteit te bewaren.

Eenmaal geïdentificeerd, moet je een nieuw wachtwoord aanmaken voor de accounts of services die in overtreding zijn.

> **Tip**
>
> Waarom de eerste vijf cijfers van wachtwoord-hashes gebruiken?
>
> Als het rapport werd uitgevoerd met je echte wachtwoorden, maakt het niet uit of ze al dan niet blootgesteld zijn, je lekt ze vrijwillig naar de service. Het resultaat van dit rapport hoeft niet te betekenen dat uw account is gecompromitteerd, maar eerder dat u een wachtwoord gebruikt dat is gevonden in deze databases met blootgestelde wachtwoorden. U moet echter het gebruik van gelekte en niet-unieke wachtwoorden vermijden.

Hergebruikte wachtwoorden

Het rapport Hergebruikte wachtwoorden identificeert niet-unieke wachtwoorden in je kluis. Door hetzelfde wachtwoord te hergebruiken voor meerdere diensten kunnen hackers gemakkelijk toegang krijgen tot meer van je online accounts wanneer één dienst is gekraakt.

Eenmaal geïdentificeerd, moet je een uniek wachtwoord aanmaken voor beledigende accounts of services.

Rapport over zwakke wachtwoorden

Het rapport Zwakke wachtwoorden identificeert zwakke wachtwoorden die gemakkelijk kunnen worden geraden door hackers en geautomatiseerde tools die worden gebruikt om wachtwoorden te kraken, gesorteerd op ernst van de zwakte. Dit rapport gebruikt zxcvbn voor het analyseren van de wachtwoordsterkte.

Zodra dit is vastgesteld, moet u de Bitwarden-wachtwoordgenerator gebruiken om een sterk wachtwoord te maken voor de beledigende accounts of services.

Rapport onbeveiligde websites

Het rapport Unsecured Websites identificeert aanmeldingsitems die onbeveiligde `(http://)` schema's gebruiken in URI's. Het is veel veiliger om `https://` te gebruiken om communicatie te versleutelen met TLS/SSL. Zie URI's gebruiken voor meer informatie.

Zodra dit is vastgesteld, moet u de overtredende URI's wijzigen van `http://` in `https://.`

Inactief 2FA-verslag

Het Inactief 2FA-rapport identificeert aanmeldingsitems waarbij:

- Authenticatie met twee factoren (2FA) via TOTP is beschikbaar via de service
- U hebt geen TOTP-authenticatiesleutel opgeslagen

Twee-factor authenticatie (2FA) is een belangrijke beveiligingsstap die helpt om je accounts te beveiligen. Als een website dit aanbiedt, moet je 2FA altijd inschakelen. Overtredende items worden geïdentificeerd door URI-gegevens te vergelijken met gegevens van https://2fa.directory/.

Zodra dit is vastgesteld, stelt u 2FA in via de hyperlink `Instructies` voor elk overtredend item:

Rapport Instructies

Rapport gegevensinbreuk (alleen individuele kluizen)

Het rapport over gegevensinbreuken identificeert gecompromitteerde gegevens (e-mailadressen, wachtwoorden, creditcards, DoB en meer) in bekende inbreuken met behulp van een service genaamd Have I Been Pwned (HIBP).

Wanneer u een Bitwarden-account aanmaakt, hebt u de optie om dit rapport uit te voeren op uw hoofdwachtwoord voordat u besluit het te gebruiken. Om dit rapport uit te voeren, wordt een hash van je hoofdwachtwoord naar HIBP gestuurd en vergeleken met opgeslagen blootgestelde hashes. Uw hoofdwachtwoord zelf wordt nooit vrijgegeven door Bitwarden.

Een "inbreuk" wordt door HIBP gedefinieerd als "een incident waarbij gegevens onbedoeld worden blootgelegd in een kwetsbaar systeem, meestal als gevolg van ontoereikende toegangscontroles of zwakke plekken in de beveiliging van de software". Raadpleeg voor meer informatie de documentatie met veelgestelde vragen van HIBP.

ⓘ Note

Als u Bitwarden zelf host, moet u, om het datalekrapport in uw exemplaar uit te voeren, een HIBP-abonnementssleutel kopen waarmee u de API kunt aanroepen, die u hier kunt verkrijgen.

Zodra u de sleutel hebt, opent u uw `./bwdata/env/global.override.env` en VERVANGT u de placeholders voor `globalSettings__hibpApiKey` met uw gekochte API-sleutel:

```bash
globalSettings__hibpApiKey=REPLACE
```

Zie Configureer omgevingsvariabelen voor meer informatie.