bitwarden | Hilfezentrum Artikel

PASSWORD MANAGER > TRESORVERWALTUNG

Tresor-Gesundheits-Berichte

Ansicht im Hilfezentrum:
https://bitwarden.com/help/reports/

Tresor-Gesundheits-Berichte

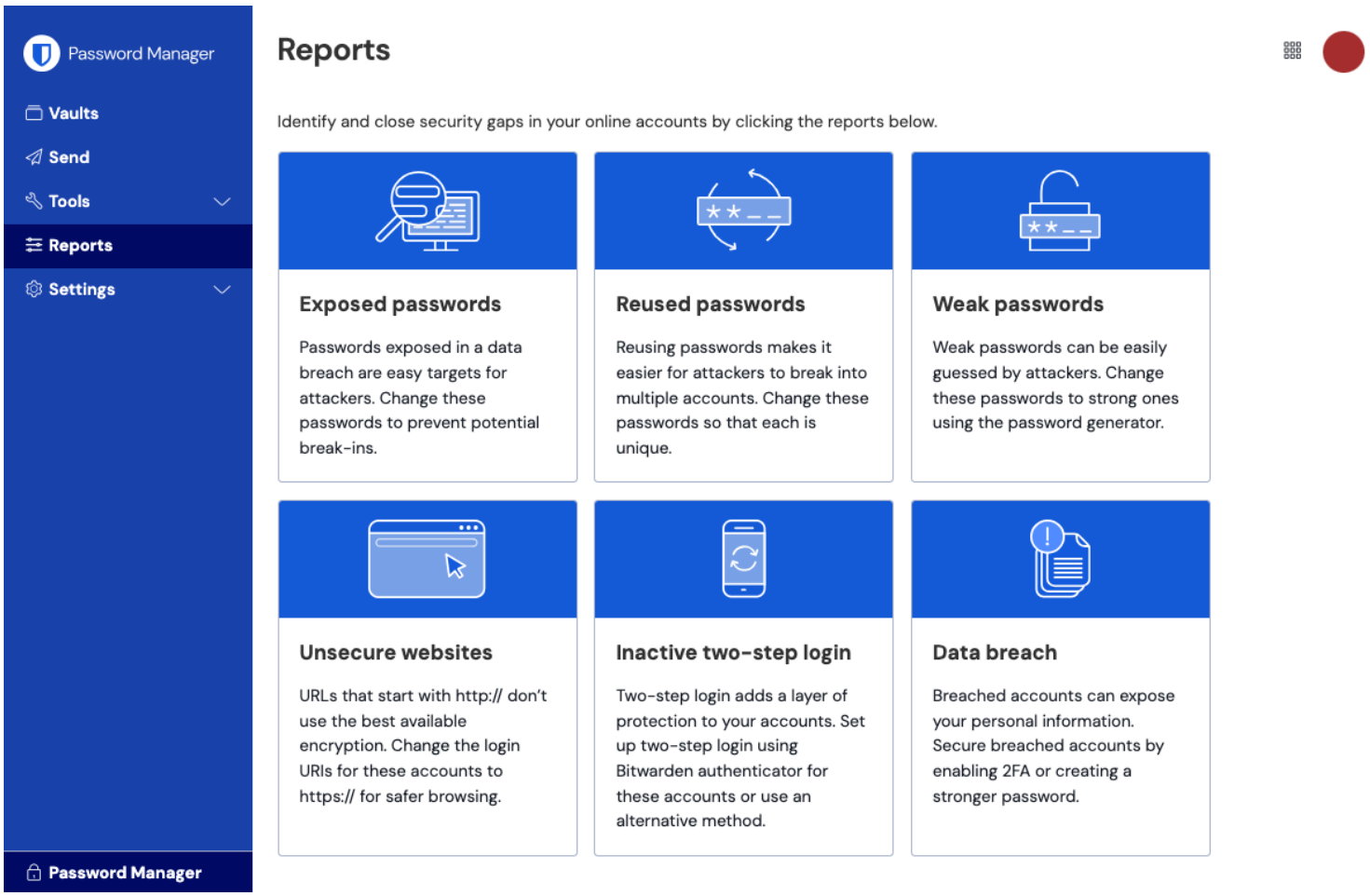
Tresor-Gesundheitsberichte können verwendet werden, um die Sicherheit Ihres individuellen Bitwarden-Tresors oder der Organisationstresor zu bewerten. Berichte, zum Beispiel der Wiederverwendete Passwörter und Schwache Passwörter Bericht, werden lokal auf Ihrem Client ausgeführt. Dies ermöglicht die Identifizierung von anstößigen Einträgen, ohne dass Bitwarden jemals Zugang zu unverschlüsselten Versionen dieser Daten hat.

> **Note**
>
> Die meisten Berichte über die Gesundheit des Tresors sind nur für Premium-Benutzer verfügbar, einschließlich Mitgliedern von bezahlten Organisationen (Families, Teams oder Enterprise), aber der Bericht über den Datendiebstahl ist für alle Benutzer kostenlos.

Einen Bericht ansehen

Um einen Gesundheitsbericht für Ihren **persönlichen Tresor** auszuführen:

1. Melden Sie sich bei der Web-App an und wählen Sie **Berichte** aus der Navigation:



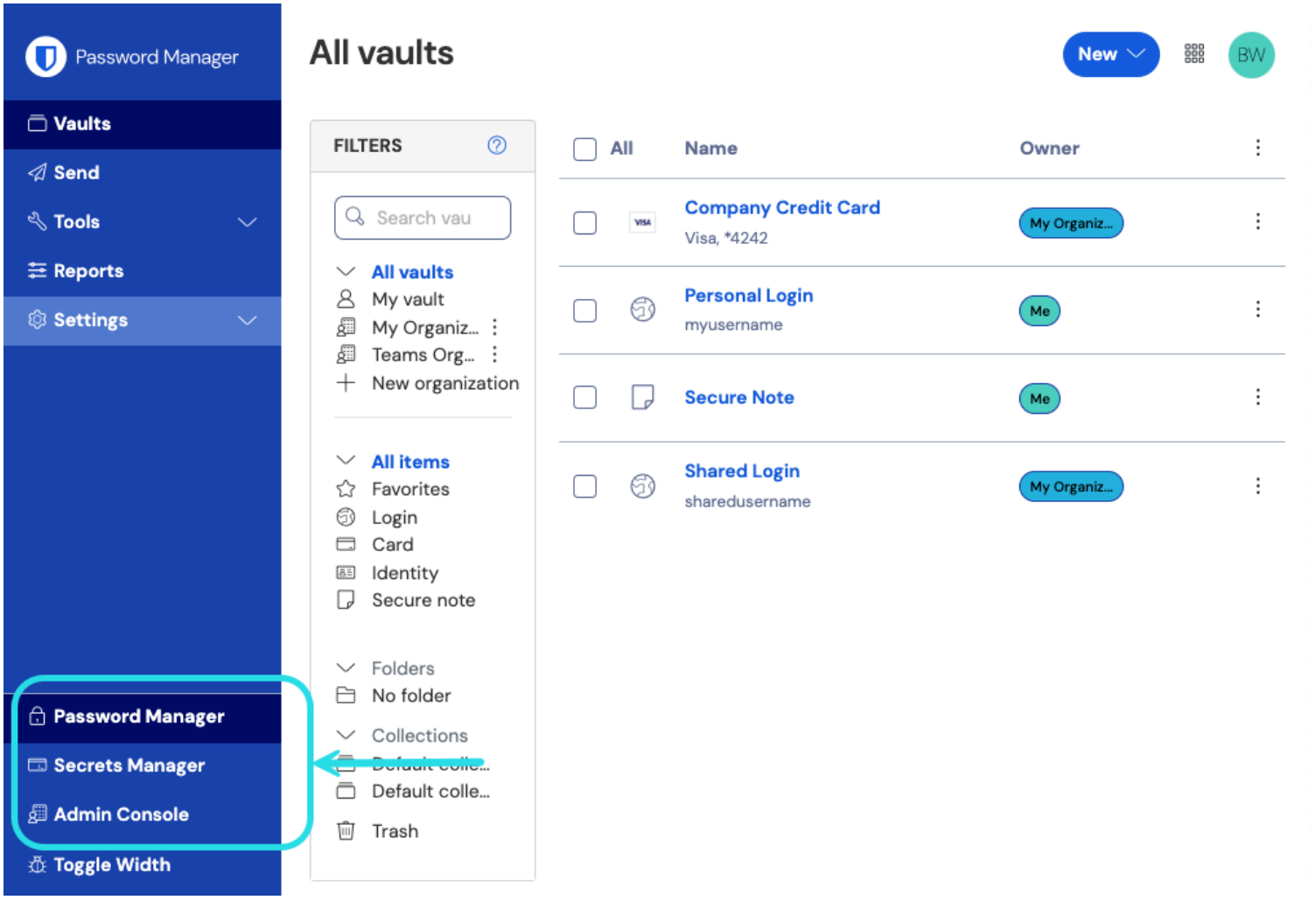
Berichtsseite

2. Wählen Sie einen Bericht zum Ausführen.

Um einen Gesundheitsbericht für Ihren **Organisationstresor** auszuführen:

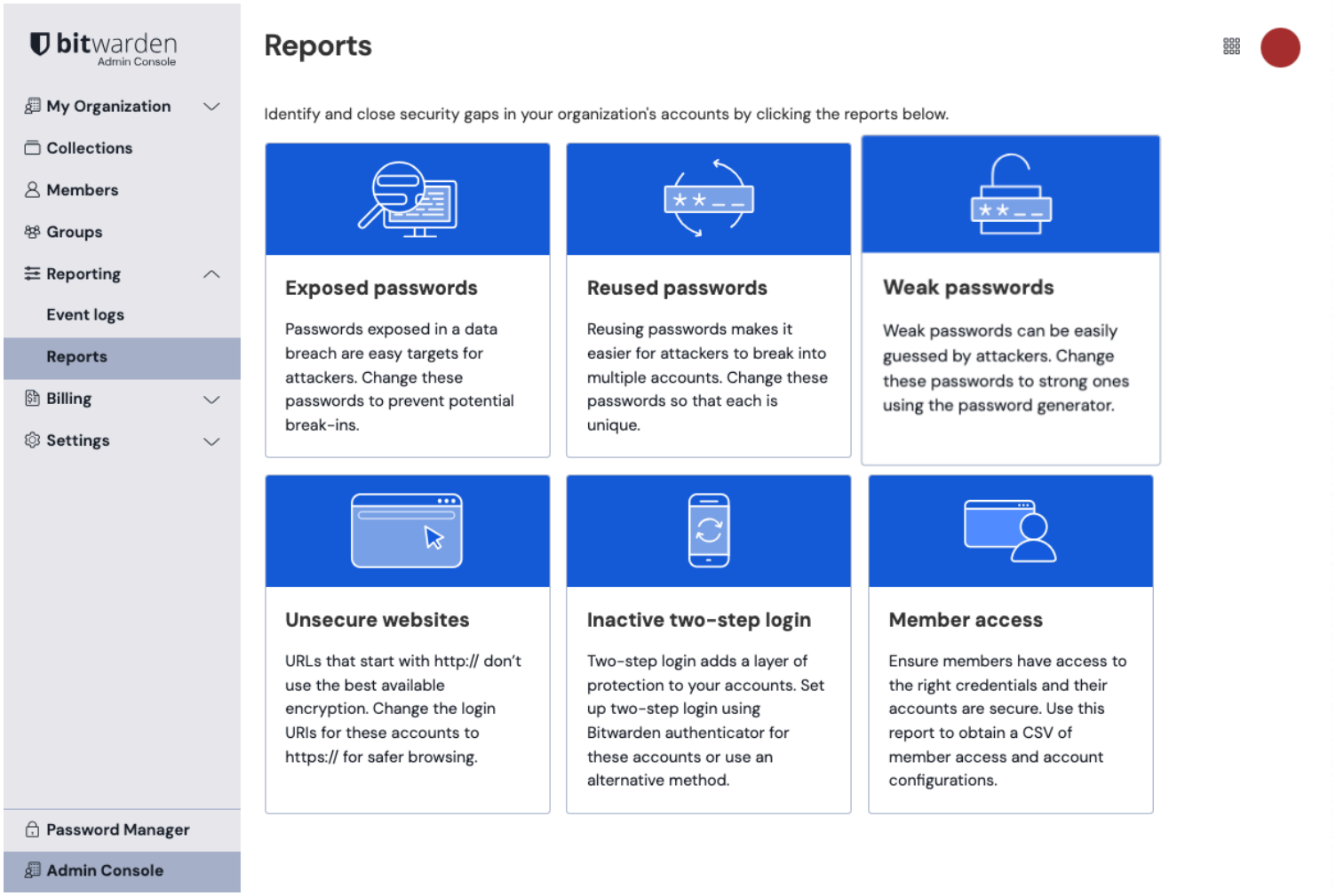
1. Melden Sie sich bei der Bitwarden-Web-App an.

2. Öffnen Sie die Administrator-Konsole mit dem Produktwechsler (⊞):



Produktwechsler

3. In Ihrer Organisation, wählen Sie **Berichterstattung** → **Berichte** aus der Navigation aus.



Organisationsberichte

4. Wählen Sie einen Bericht zum Ausführen aus.

Verfügbare Berichte

Bericht über kompromittierte Passwörter

Der Bericht über kompromittierte Passwörter identifiziert Passwörter, die in bekannten Datendiebstählen aufgedeckt wurden, die öffentlich veröffentlicht oder von Hackern im Darknet verkauft wurden.

Dieser Bericht verwendet einen vertrauenswürdigen Webdienst, um die ersten fünf Ziffern des Hashs aller Ihrer Passwörter in einer Datenbank bekannter durchgesickerter Passwörter zu suchen. Die zurückgegebene übereinstimmende Liste von Hashes wird dann lokal mit dem vollständigen Hash Ihres Passworts verglichen. Dieser Vergleich wird nur lokal durchgeführt, um Ihre k-Anonymität zu wahren.

Sobald identifiziert, sollten Sie ein neues Passwort für betroffene Konten oder Dienste erstellen.

Tip

Warum die ersten fünf Ziffern von Passwort-Hashes verwenden?

Wenn der Bericht mit Ihren tatsächlichen Passwörtern durchgeführt wurde, spielt es keine Rolle, ob sie offengelegt wurden oder nicht, Sie würden ihn freiwillig an den Dienst weitergeben. Das Ergebnis dieses Berichts bedeutet möglicherweise nicht, dass Ihr Konto kompromittiert wurde, sondern dass Sie ein Passwort verwenden, das in diesen Datenbanken mit exponierten Passwörtern gefunden wurde. Sie sollten jedoch die Verwendung von durchgesickerten und nicht eindeutigen Passwörtern vermeiden.

Bericht über wiederverwendete Passwörter

Der Bericht über wiederverwendete Passwörter identifiziert nicht eindeutige Passwörter in Ihrem Tresor. Die Wiederverwendung des gleichen Passworts für mehrere Dienste kann Hackern ermöglichen, leichter Zugang zu mehr Ihrer Online-Konten zu erhalten, wenn ein Dienst gehackt wird.

Sobald identifiziert, sollten Sie ein einzigartiges Passwort für betroffene Konten oder Dienste erstellen.

Bericht über schwache Passwörter

Der Bericht über schwache Passwörter identifiziert schwache Passwörter, die leicht von Hackern und automatisierten Tools, die zum Knacken von Passwörtern verwendet werden, erraten werden können, sortiert nach Schweregrad der Schwäche. Dieser Bericht verwendet zxcvbn zur Passwortstärkenanalyse.

Sobald identifiziert, sollten Sie den Bitwarden Passwort Generator verwenden, um ein starkes Passwort für betroffene Konten oder Dienste zu generieren.

Bericht über unsichere Websites

Der Bericht über unsichere Websites identifiziert Zugangsdaten-Einträge, die unsichere (`http://`) Schemata in URIs verwenden. Es ist viel sicherer, `https://` zur Verschlüsselung der Kommunikation mit TLS/SSL zu verwenden. Um mehr zu erfahren, sehen Sie URIs verwenden.

Sobald identifiziert, sollten Sie anstößige URIs von `http://` zu `https://` ändern.

Inaktiver 2FA-Bericht

Der Inaktive 2FA-Bericht identifiziert Zugangsdaten-Einträge, bei denen:

- Zwei-Faktor-Authentifizierung (2FA) über TOTP ist vom Service verfügbar.
- Sie haben keinen TOTP-Authentifikator-Schlüssel gespeichert.

Die Zwei-Faktor-Authentifizierung (2FA) ist ein wichtiger Sicherheitsschritt, der hilft, Ihre Konten zu sichern. Wenn eine Website es anbietet, sollten Sie immer 2FA aktivieren. Anstößige Einträge werden identifiziert, indem URI-Daten mit Daten von https://2fa.directory/ abgeglichen werden.

Sobald identifiziert, richten Sie 2FA ein, indem Sie den `Anweisungen` Hyperlink für jeden anstößigen Eintrag verwenden:

Anweisungen für den Bericht

Bericht über Datendiebstahl (nur einzelne Tresore)

Der Bericht über den Datendiebstahl identifiziert kompromittierte Daten (E-Mail-Adressen, Passwörter, Kreditkarten, Geburtsdaten und mehr) in bekannten Verstößen, mit Hilfe eines Dienstes namens Have I Been Pwned (HIBP).

Wenn Sie ein Bitwarden-Konto erstellen, haben Sie die Möglichkeit, diesen Bericht über Ihr Master-Passwort auszuführen, bevor Sie sich entscheiden, es zu verwenden. Um diesen Bericht auszuführen, wird ein Hash Ihres Master-Passworts an HIBP gesendet und mit gespeicherten kompromittierten Hashes verglichen. Ihr Master-Passwort wird von Bitwarden selbst nie kompromittiert.

Ein "Verstoß" wird von HIBP als "ein Vorfall definiert, bei dem Daten unbeabsichtigt in einem anfälligen System kompromittiert werden, normalerweise aufgrund unzureichender Zugriffskontrollen oder Sicherheitsschwächen in der Software". Für weitere Informationen, siehe HIBP's FAQs Dokumentation.

Note

Wenn Sie Bitwarden selbst hosten, müssen Sie, um den Bericht über den Datendiebstahl in Ihrer Instanz auszuführen, einen HIBP-Abonnementschlüssel kaufen, der Sie dazu berechtigt, Anrufe an die API zu tätigen, den Sie hier erhalten.

Sobald Sie den Schlüssel haben, öffnen Sie Ihre `./bwdata/env/global.override.env` und ERSETZEN Sie den Platzhalterwert für `globalSettings__hibpApiKey` mit Ihrem gekauften API-Schlüssel:

```Bash
globalSettings__hibpApiKey=REPLACE
```

Für weitere Informationen, siehe Umgebungsvariablen konfigurieren.