Tipps und Tricks

- Generator | Passwort und Benutzername
- Berichte | Kontosicherheit
- Notfallzugriff
- Import | Export von Passwörtern

Generator | Passwort und Benutzername

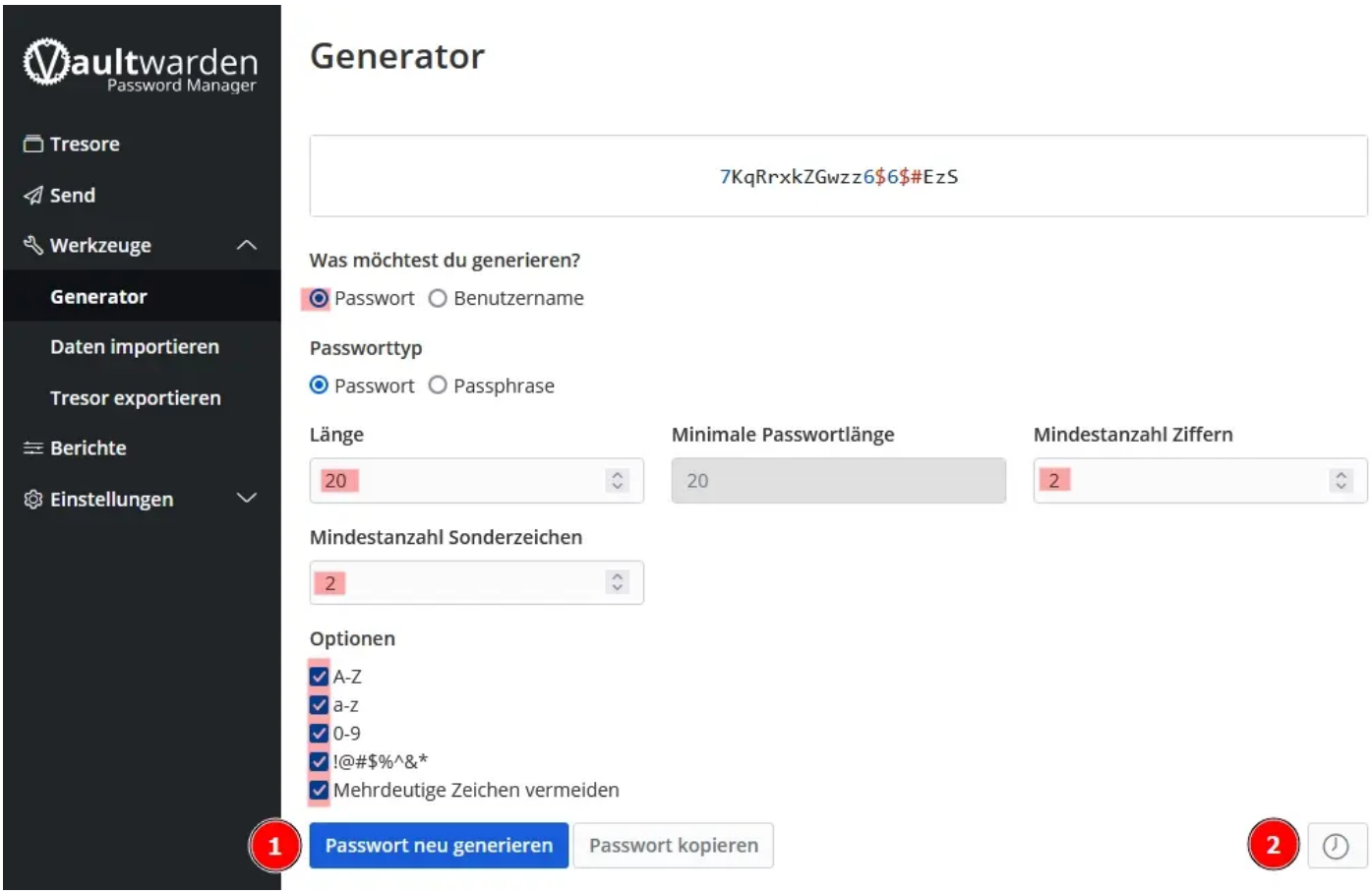
Beim Generator haben wir 2 verschiedenen Optionen zur Auswahl. Einmal den Passwortgenerator der uns sichere und zufällige Passwörter generiert und zweitens einen Benutzernamen Generator der uns zufällige Benutzernamen generiert.

Zum Generator gelangen wir über den Webpasswortmanager oder über die Jeweiligen Apps.

https://icrar.jwebbi.de

Unter **Werkzeuge** -> **Generator**

Passwort



Oben wähle Passwort aus und beim Passworttyp auch.

Wir empfehlen folgende Einstellungen als meidest Einstellungen mehr ist immer besser:

- Länge 20
- Mindestanzahl Ziffern 2
- Mindestanzahl Sonderzeichen 2
- Alle Optionen aktivieren

> Einige Dienste haben Probleme mit zu langen Passwörtern, teilweise müssen diese auch kürzer gewählt werden.

1. Mit **Passwort neu generieren** kannst du und beliebig oft ein neues Passwort erzeugen bis du eins gefunden hast, was du benutzen willst.
2. Hier kannst du alte Generierte Passwörter nachrücken, falls du sie noch einmal benötigst.

Mit **Passwort kopieren** kopierst du das Passwort in deine Zwischenablage

> Der Generator ist auch in der Handy und Desktop App sowie in der Browser Erweiterung zu finden und hat überall die gleichen Funktionen.

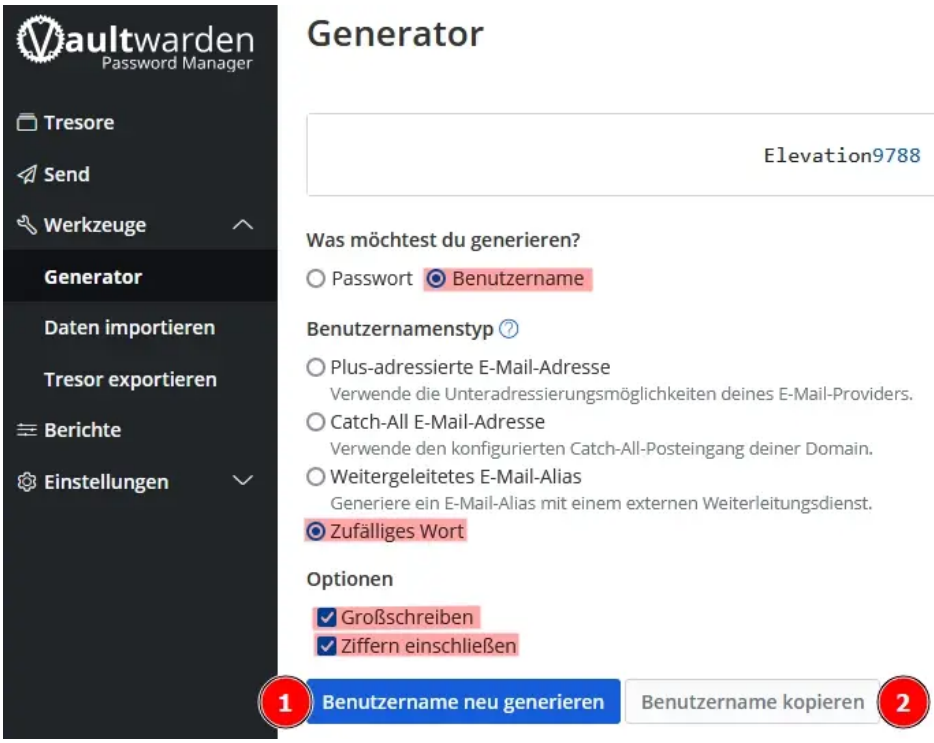
Benutzernamen

Wenn du gerne anonymer im Internet unterwegs seien möchtest und nicht immer den Gleichen Benutzernamen überall haben willst dann ist der Benutzernamen Generator genau das Richtige für dich.

Zum Generator gelangen wir über den Webpasswortmanager oder über die Jeweiligen Apps.

https://icrar.jwebbi.de

Unter **Werkzeuge** -> **Generator**



Oben wähle **Benutzername** aus und **Zufälliges Wort**

Jetzt kannst du noch optional **Großschreiben** und **Ziffern einschließen** auswählen.

Mit **Benutzername neu generieren** kannst du dir so lange Benutzername generieren bist du eine gefunden hast, der dir zusagt. Und mit **Benutzername kopieren** kannst du ihn in deine Zwischenablage kopieren.

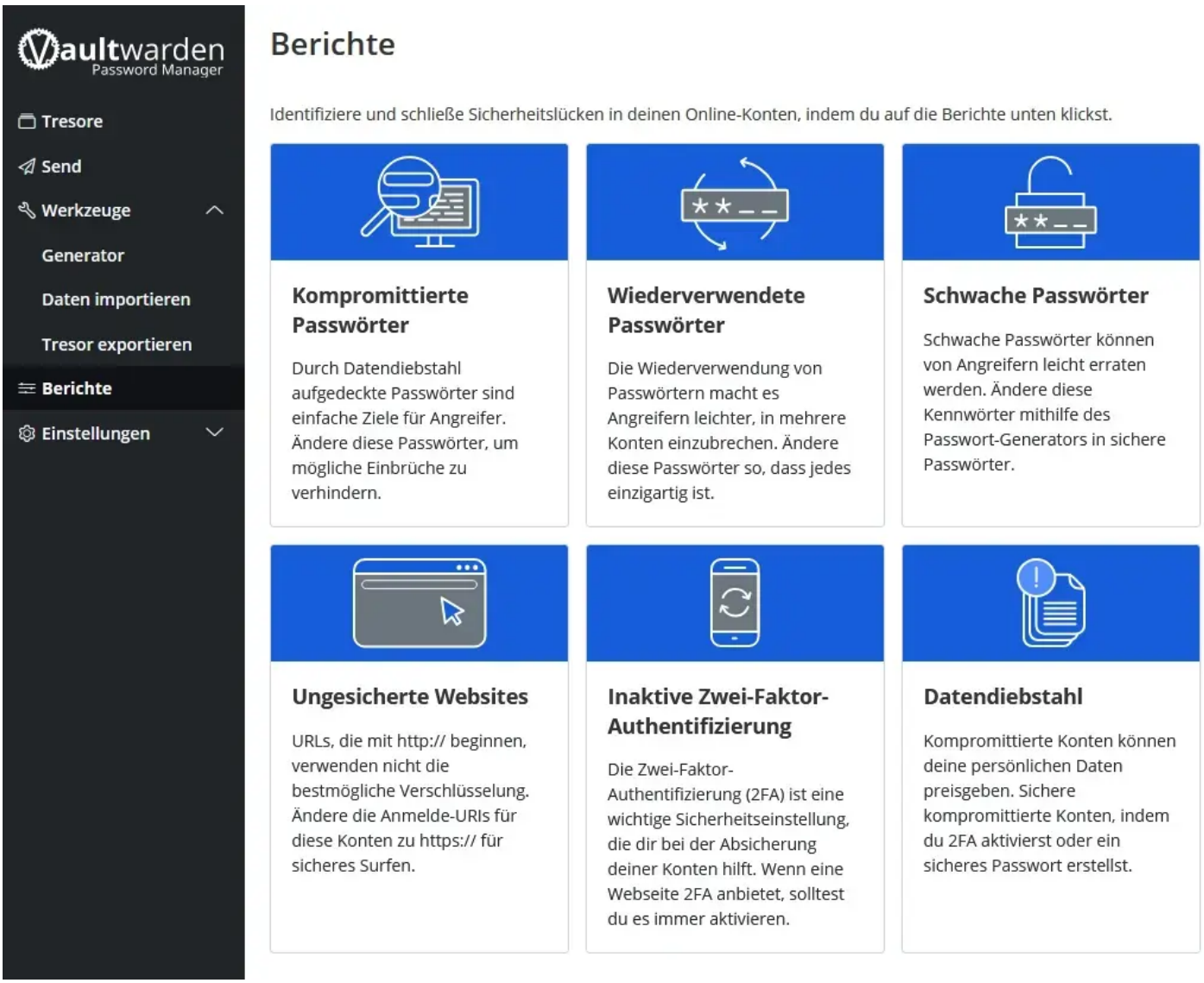
> Der Generator ist auch in der Handy und Desktop App sowie in der Browser Erweiterung zu finden und hat überall die gleichen Funktionen.

Berichte | Kontosicherheit

Um zu dein berichten zu gelangen, melde dich im Web Passwortmanager an:

https://icrar.jwebbi.de

Die Berichte vom Passwortmanager sind extrem nützlich, um mögliche Schwachstellen in seinen Logins zu finden. Identifiziere und schließe Sicherheitslücken in deinen Online-Konten, indem du auf die Berichte unten klickst.

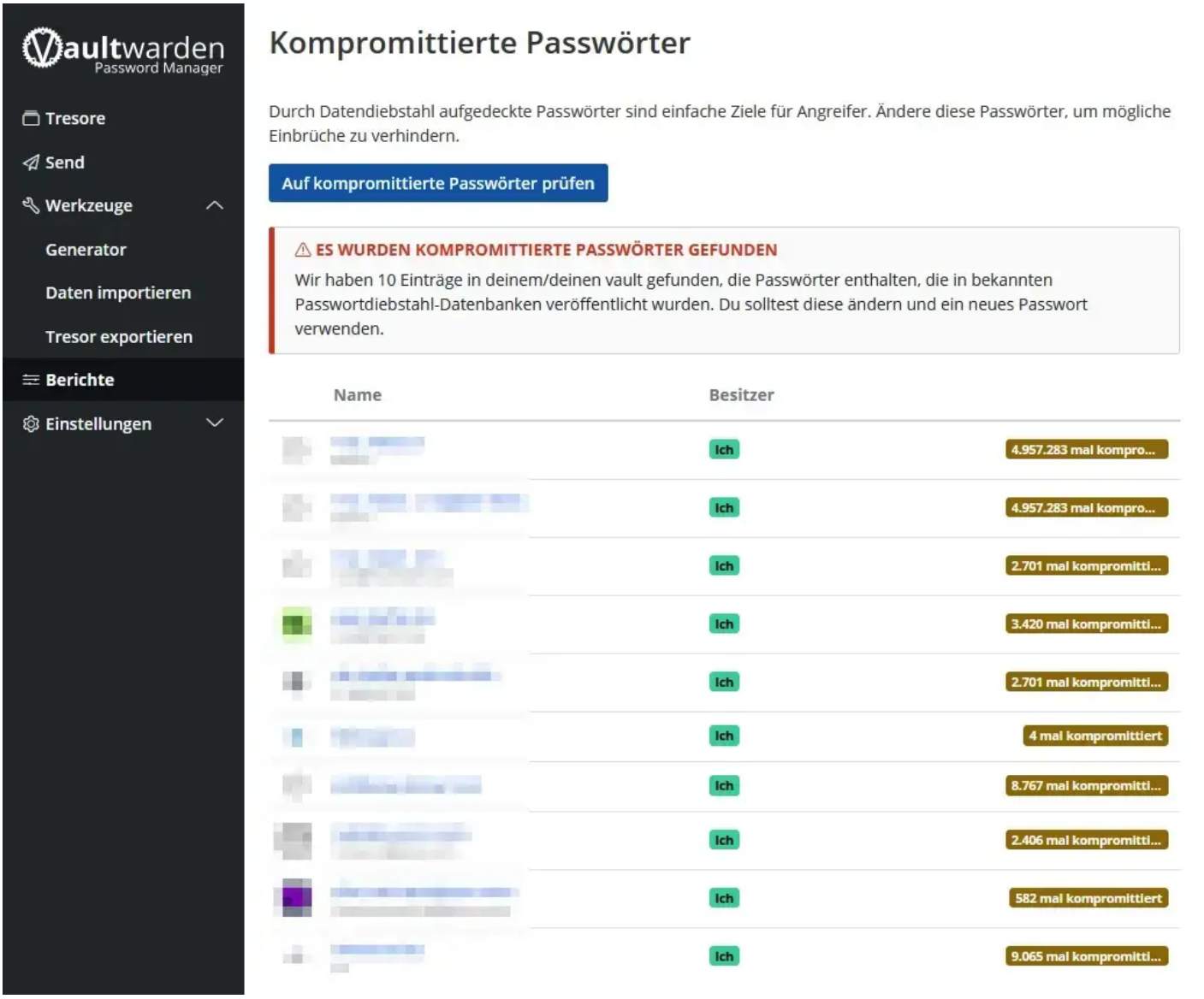


Hier hast du 6 verschiedenen Check zur Auswahl, wir werden jeden Check durchgehen und genau angucken.

1. Kompromittierte Passwörter

Dieser Bericht überprüft, ob eines deiner gespeicherten Passwörter in bekannten Datenlecks veröffentlicht wurde. Solche Passwörter sind besonders anfällig, da Angreifer sie aus öffentlich zugänglichen Datenbanken entnehmen können. Wenn ein Passwort als kompromittiert markiert wird, solltest du es sofort ändern. Nutze dabei ein starkes, einzigartiges Passwort, das du mit dem integrierten Passwort-Generator erstellen kannst.

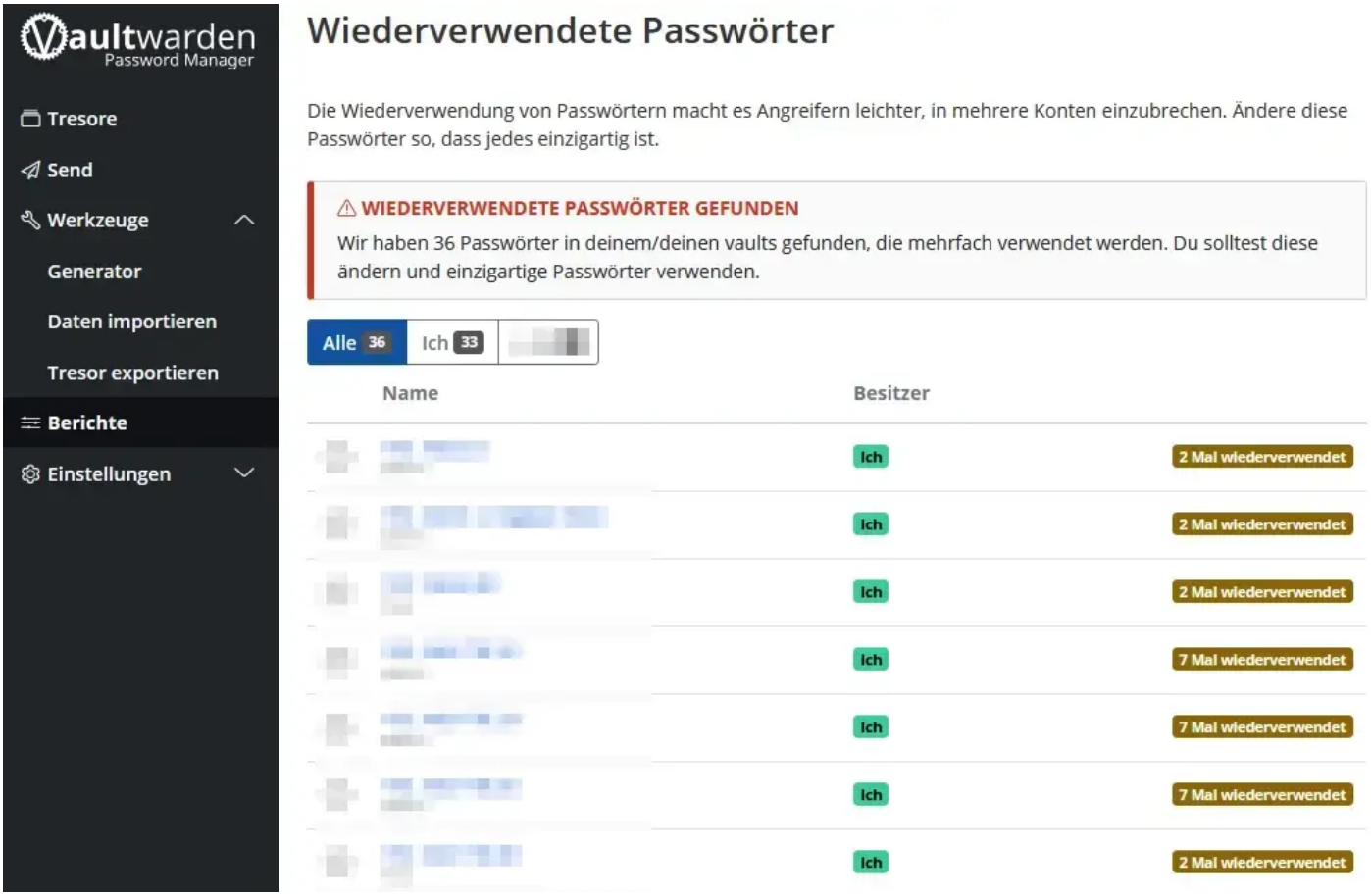
> Durch Datendiebstahl aufgedeckte Passwörter sind einfache Ziele für Angreifer. Ändere diese Passwörter, um mögliche Einbrüche zu verhindern.



2. Wiederverwendete Passwörter

Die Wiederverwendung desselben Passworts für mehrere Konten ist riskant. Wenn ein Konto gehackt wird, können Angreifer leicht auf andere Konten zugreifen, die dasselbe Passwort verwenden. Dieser Bericht zeigt dir, welche Passwörter mehrfach verwendet werden. Du solltest für jedes Konto ein individuelles Passwort erstellen, um dieses Risiko zu minimieren.

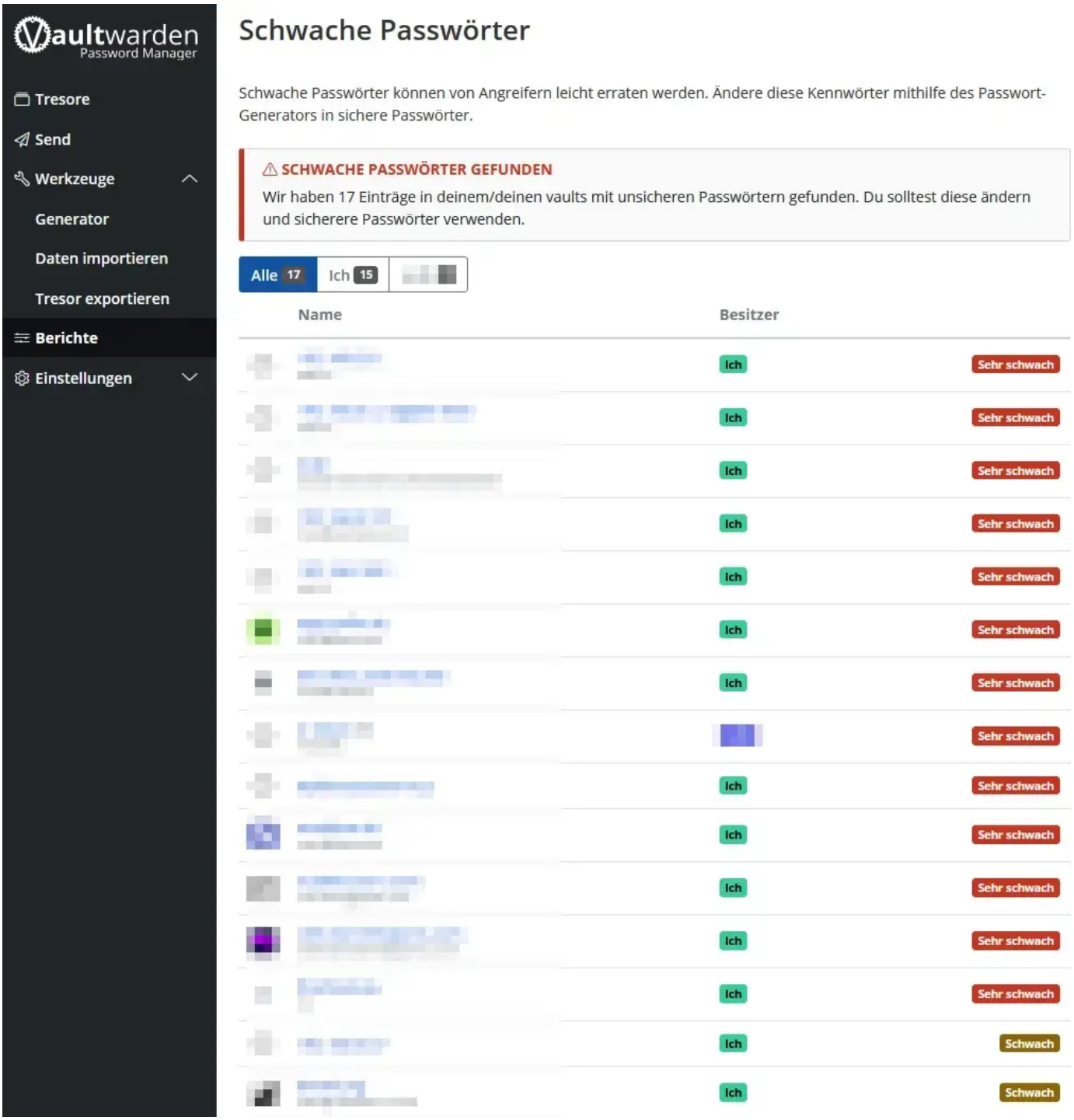
> Die Wiederverwendung von Passwörtern macht es Angreifern leichter, in mehrere Konten einzubrechen. Ändere diese Passwörter so, dass jedes einzigartig ist.



3. Schwache Passwörter

Schwache Passwörter sind leicht zu erraten, insbesondere wenn sie einfache Muster, Wörter oder Zahlenfolgen enthalten. Der Bericht identifiziert solche Passwörter und hilft dir, sie durch sicherere Alternativen zu ersetzen. Ein starkes Passwort sollte mindestens 14 Zeichen lang sein und eine Kombination aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen enthalten.

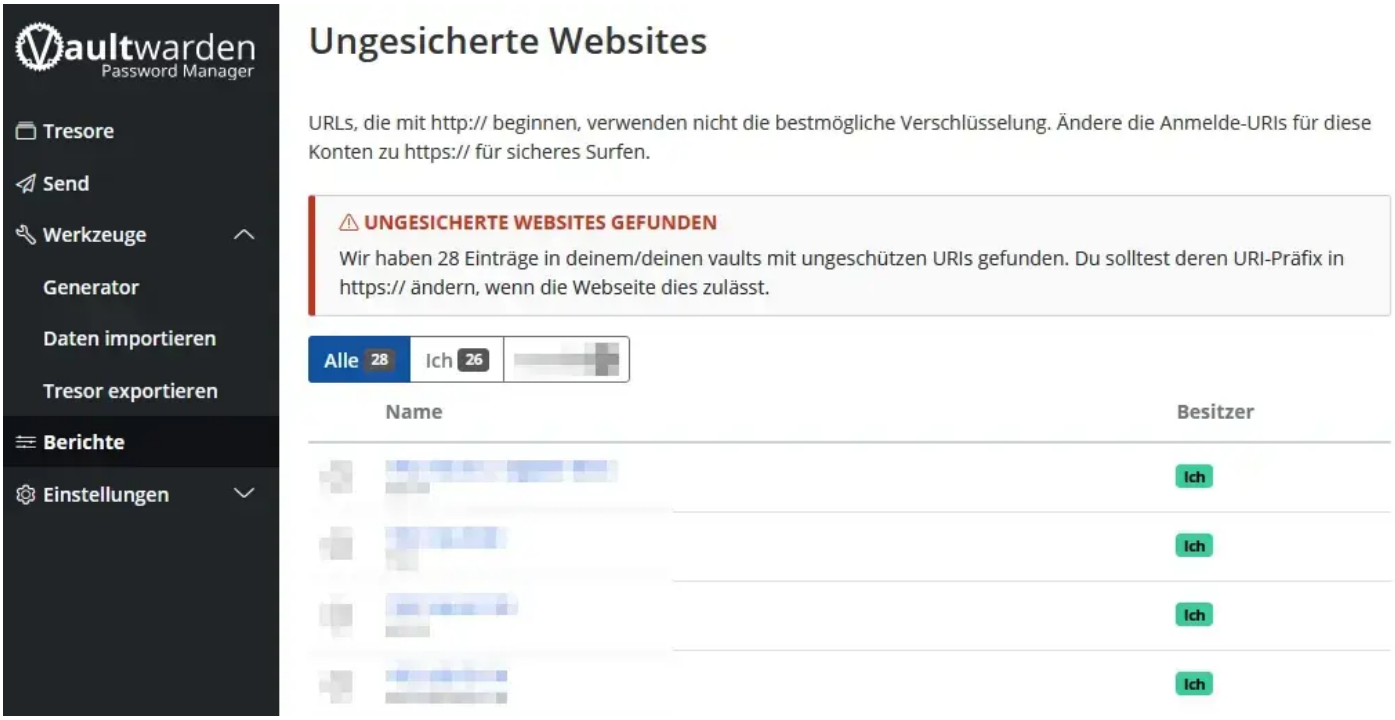
> Schwache Passwörter können von Angreifern leicht erraten werden. Ändere diese Kennwörter mithilfe des Passwort-Generators in sichere Passwörter.



4. Ungesicherte Websites

Websites, die mit "http://" beginnen, verwenden keine verschlüsselte Verbindung. Das bedeutet, dass Daten, die du auf diesen Seiten eingibst, wie Passwörter oder persönliche Informationen, von Dritten abgefangen werden können. Der Bericht zeigt dir, welche URLs in deinem Tresor unsicher sind. Du solltest diese auf "https://" aktualisieren oder die Website meiden, falls keine sichere Verbindung verfügbar ist.

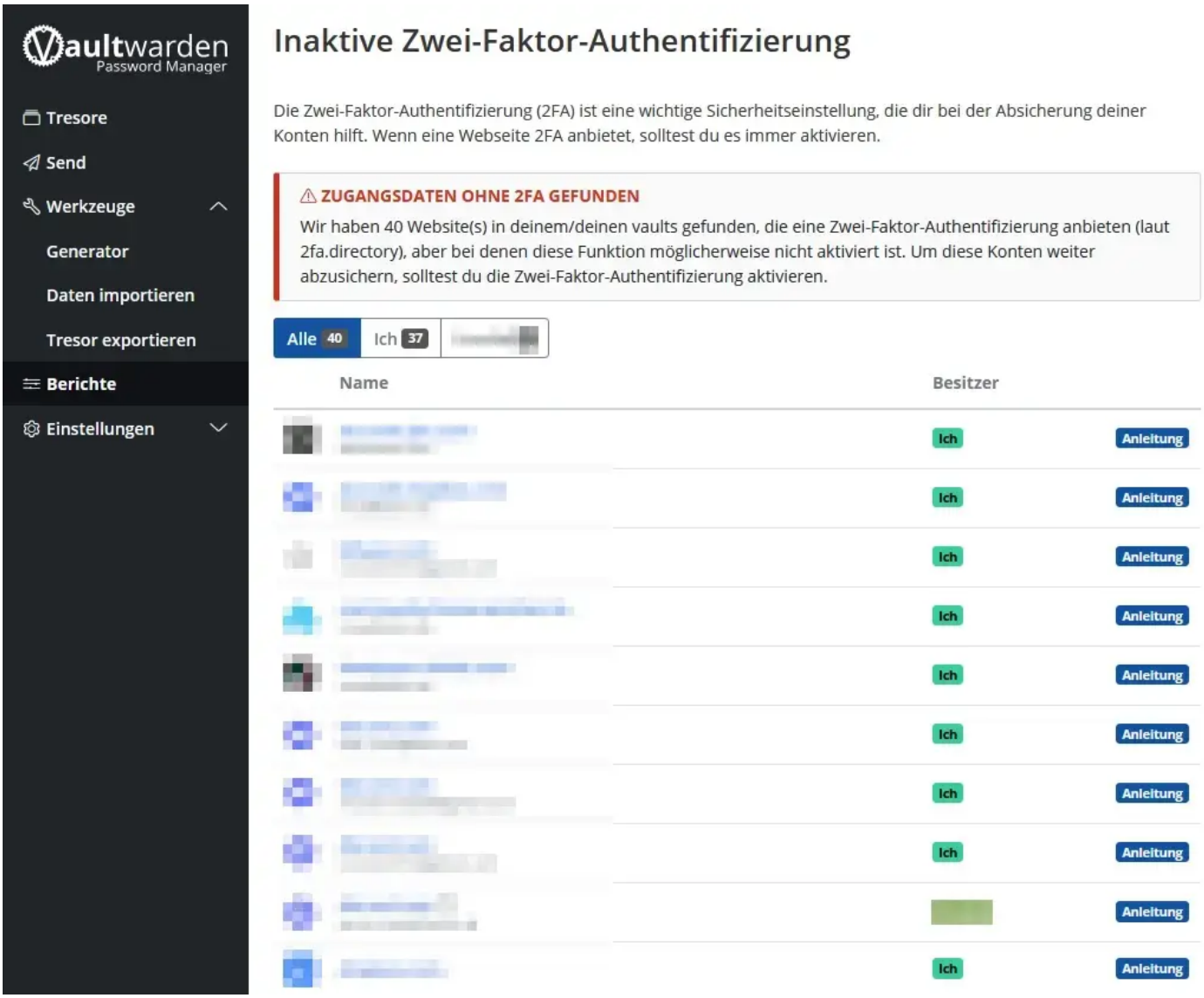
URLs, die mit http:// beginnen, verwenden nicht die bestmögliche Verschlüsselung. Ändere die Anmelde-URIs für diese Konten zu https:// für sicheres Surfen.



5. Inaktive Zwei-Faktor-Authentifizierung (2FA)

Die Zwei-Faktor-Authentifizierung fügt eine zusätzliche Sicherheitsebene hinzu, indem sie neben dem Passwort einen zweiten Faktor wie einen Code oder eine biometrische Bestätigung erfordert. Der Bericht zeigt dir, bei welchen deiner gespeicherten Konten 2FA nicht aktiviert ist. Wenn verfügbar, solltest du 2FA aktivieren, um deine Konten besser zu schützen.

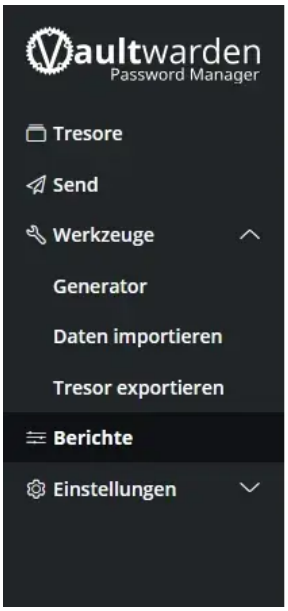
Die Zwei-Faktor-Authentifizierung (2FA) ist eine wichtige Sicherheitseinstellung, die dir bei der Absicherung deiner Konten hilft. Wenn eine Webseite 2FA anbietet, solltest du es immer aktivieren.



6. Datendiebstahl

Dieser Bericht überprüft, ob eines deiner Konten in einem Datenleck kompromittiert wurde. Wenn ein Konto betroffen ist, solltest du sofort das Passwort ändern und, falls noch nicht geschehen, 2FA aktivieren. Dies hilft, den Schaden zu begrenzen und zukünftige Angriffe zu verhindern.

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



Datendiebstahl

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

Benutzername

[redacted]

Prüfen Sie alle Benutzernamen und E-Mail-Adressen, die Sie verwenden.

Auf Datendiebstähle prüfen

GUTE NEUIGKEITEN

[redacted] wurde in keinem der bekannten Datendiebstahlvorfällen gefunden.

Zurück zu den Berichten

Notfallzugriff

Logge dich im Passwortmanager ein: https://icrar.jwebbi.de

Der Bitwarden-Notfallzugriff ist eine Funktion, die es ermöglicht, einer vertrauenswürdigen Person Zugriff auf deinen Bitwarden-Tresor zu gewähren, falls du selbst nicht mehr darauf zugreifen kannst (z. B. bei Krankheit oder anderen Notfällen). So funktioniert es:

1. **Einrichtung des Notfallzugriffs**:
   - Du wählst eine oder mehrere Personen aus, denen du vertraust (z. B. Familienmitglieder oder enge Freunde).
   - Diese Personen müssen ein Bitwarden-Konto haben.
   - Du legst fest, welche Berechtigungen diese Person erhält und wie lange sie warten muss, bevor sie Zugriff erhält (z. B. 1 Tag, 7 Tage).
2. **Freigabeprozess**:
   - Wenn die vertrauenswürdige Person Zugriff benötigt, kann sie eine Anfrage stellen.
   - Du wirst über diese Anfrage benachrichtigt und kannst sie entweder genehmigen oder ablehnen.
   - Wenn du nicht innerhalb der festgelegten Wartezeit reagierst, erhält die Person automatisch Zugriff.
3. **Sicherheit**:
   - Der Zugriff ist verschlüsselt und sicher. Die Person erhält nur Zugriff, wenn die Bedingungen erfüllt sind.
   - Du kannst den Notfallzugriff jederzeit widerrufen, falls du deine Meinung änderst.

Vorteil: Der Notfallzugriff stellt sicher, dass wichtige Passwörter und Daten nicht verloren gehen, selbst wenn du sie selbst nicht mehr verwalten kannst.

Das ist besonders nützlich für den Fall, dass jemand nach deinem Tod oder in einer Notsituation auf deine Konten zugreifen muss.

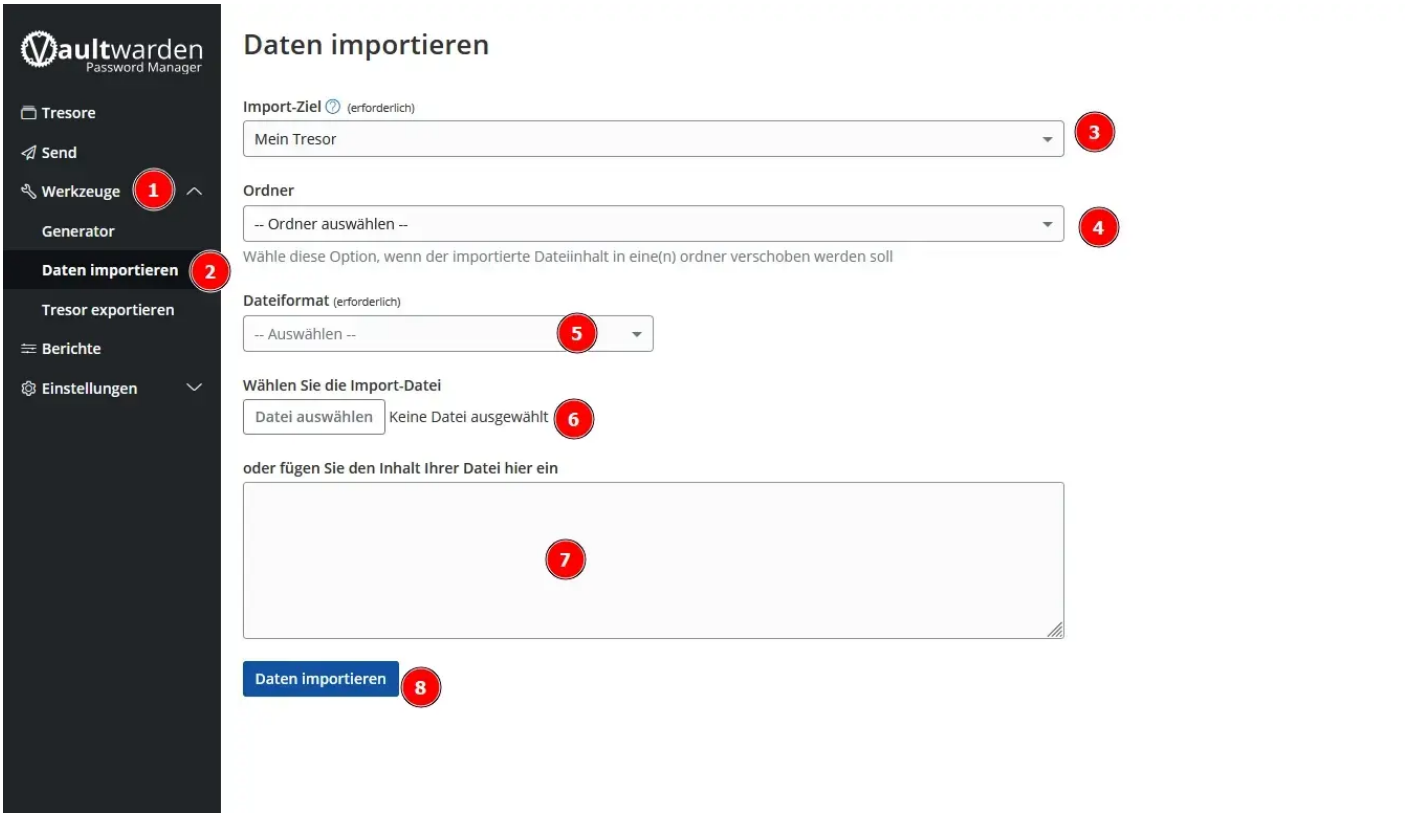
Import | Export von Passwörtern

Import in deinen Passwortmanager

Mit dem Import kannst du deine Passwörter aus einem anderen Passwortmanager in deinem neuen importieren.

Um zum Import zu gelangen, melde dich im Web Passwortmanager an:

https://icrar.jwebbi.de



Die Importfunktion findest du unter **Werkzeuge** -> **Dateien importieren**

Hier hast du jetzt mehrere Sachen zur Auswahl, die du einstellen kannst.

3. Hier kannst du festlegen, wohin du deine Passwörter importieren möchtest. Wenn du Organisationen benutzt hast du diese zur Auswahl.

4. **Optional** Hier kannst du einen Ordner auswählen, in den die Passwörter importiert wer denn sollen.

5. Hier wählst du aus welchem Passwortmanager du die Daten exportiert hast.

6. Dann wählst du hier die exportierte Datei aus deinem alten Passwortmanager aus.

7. Falls du keine Datei, sondern nur Text für den Export bekommen hast, kannst du ihn hier einfügen.

8. Starte jetzt das Importieren mit einem Klick auf Daten importieren

> Es gibt viele verschiedene unterstützte Passwortmanager für den Import wie du die daten, aus denen exportieren kannst, erfährst du beim, Anbieter deines alten Passwortmanagers.

Einige sind auch beispielhaft in der offiziellen Dokumentation erklärt: https://bitwarden.com/de-de/help/import-data/

Export aus deinem Passwortmanager

> Exportiere deine Passwörter nur, wenn du zu einem anderen Passwortmanager wechselst. Teilen diesen Export mit niemandem, da er alle deine Passwörter unverschlüsselt enthält!

> Es werden nur persönliche Tresoreinträge exportiert, die mit Deinem Konto verbunden sind. Tresoreinträge der Organisation werden nicht berücksichtigt. Es werden nur Informationen der Tresoreinträge exportiert. Diese enthalten nicht die zugehörigen Anhänge.

Um zum Export zu gelangen, melde dich im Web Passwortmanager an:

https://icrar.jwebbi.de

Die Exportfunktion findest du unter **Werkzeuge** -> **Tresor exportieren**

1. Hier kannst du auswählen in welchem Dateiformat du deine Passwörter exportieren möchtest.
2. Wenn du das für dich passen Format ausgewählt hast, klicke auf Format Bestätigen und du musst noch einmal dein Masterpasswort eingeben

Jetzt kannst du den gesamten Inhalt deines Passwortmanagers herrunterladen.

> Dieser Export enthält deine Tresor-Daten in einem unverschlüsseltem Format. Du solltest die Datei daher nicht über unsichere Kanäle (z.B. E-Mail) versenden oder speichern. Lösche die Datei sofort nach ihrer Verwendung.