bitwarden | Hilfezentrum Artikel

SICHERHEIT

Whitepaper zur Sicherheit bei Bitwarden

Ansicht im Hilfezentrum:
https://bitwarden.com/help/bitwarden-security-white-paper/

Whitepaper zur Sicherheit bei Bitwarden

Überblick über das Sicherheits- und Compliance-Programm von Bitwarden

Mit dem Anstieg der Telearbeit und der Internetnutzung auf einem Höchststand ist die Nachfrage nach der Erstellung und Pflege von Dutzenden (wenn nicht Hunderten) von Online-Konten mit Zugangsdaten und Passwörtern enorm.

Sicherheitsexperten empfehlen, dass Sie für jedes Konto, das Sie erstellen, ein anderes, zufällig generiertes Passwort verwenden. Aber wie verwalten Sie all diese Passwörter? Und wie pflegt man eine gute Passwort-Hygiene in einer Organisation?

Effektives Passwort-Management ist eine stark untergenutzte Ressource im Enterprise. Im 2020 Under the Hoodie Bericht von Rapid7 wird darauf hingewiesen, dass das Passwort-Management und sekundäre Kontrollen wie die Zwei-Faktor-Authentifizierung "schwerwiegend fehlen, was zu 'leichten' Kompromissen führt." Das Wiederverwenden oder Teilen von Passwörtern auf unsichere Weise macht das Enterprise verwundbar.

Um Veränderungen in einer Organisation herbeizuführen, müssen Sicherheits- und IT-Teams die Mitarbeiter über die besten Praktiken aufklären. In Bezug auf die Passwortverwaltung ist eine der einfachsten Möglichkeiten, gute Passworthygiene zu fördern und zu unterstützen, die Bereitstellung einer Passwort-Manager-Lösung in Ihrem Arbeitsplatz.

Bitwarden ist der einfachste und sicherste Weg, all Ihre Zugangsdaten, Passwörter und andere sensible Informationen zu speichern, während sie bequem zwischen all Ihren Geräten synchronisiert werden.

Bitwarden bietet die Werkzeuge, um Ihre Passwörter zu erstellen, zu speichern und zu teilen, während die höchste Sicherheitsstufe gewährleistet wird.

Die Lösung, Software, Infrastruktur und Sicherheitsprozesse von Bitwarden wurden von Grund auf mit einem mehrschichtigen, verteidigungstiefen Ansatz konzipiert. Das Bitwarden-Sicherheits- und Compliance-Programm basiert auf dem ISO27001-Informationssicherheits-Managementsystem (ISMS). Wir haben Richtlinien festgelegt, die unsere Sicherheitsrichtlinien und -prozesse regeln und aktualisieren unser Sicherheitsprogramm kontinuierlich, um es mit den geltenden gesetzlichen, branchenspezifischen und regulatorischen Anforderungen für die Dienstleistungen, die wir Ihnen im Rahmen unserer Servicevereinbarungsbedingungen anbieten, in Einklang zu bringen.

Bitwarden entspricht branchenüblichen Anwendungssicherheitsrichtlinien, die ein spezielles Sicherheitsingenieursteam beinhalten und regelmäßige Überprüfungen des Anwendungsquellcodes und der IT-Infrastruktur umfassen, um Sicherheitslücken zu erkennen, zu validieren und zu beheben.

Dieses Weißbuch bietet einen Überblick über die Sicherheitsprinzipien von Bitwarden sowie Links zu zusätzlichen Dokumenten, die in bestimmten Bereichen mehr Details liefern.

Bitwarden Sicherheitsprinzipien

Benutzerschutz der Daten

Bitwarden nutzt die folgenden Sicherheitsmaßnahmen, um Benutzerdaten zu schützen.

End-to-End-Verschlüsselung: Sperren Sie Ihre Passwörter und privaten Informationen mit End-to-End-AES-CBC-256-Bit-Verschlüsselung, Salted Hashing und PBKDF2 SHA-256. Alle kryptografischen Schlüssel werden vom Client auf Ihren Geräten generiert und verwaltet, und alle Verschlüsselungen werden lokal durchgeführt. Sehen Sie mehr Details im Abschnitt zur Passwort-Hashing-Ableitung.

Zero-Knowledge-Verschlüsselung: Bitwarden-Teammitglieder können Ihre Passwörter nicht sehen. Ihre Daten bleiben Ende-zu-Ende verschlüsselt mit Ihrer individuellen E-Mail-Adresse und Ihrem Master-Passwort. Wir speichern niemals und können nicht auf Ihr Master-Passwort oder Ihre kryptografischen Schlüssel zugreifen.

> **Note**
>
> Mit der Mitte 2021 veröffentlichten Version der Passwort-Zurücksetzung durch Administratoren wurde ein neues öffentliches/privates RSA-Schlüsselpaar für alle Organisationen eingeführt. Der private Schlüssel wird zusätzlich mit dem bereits vorhandenen symmetrischen Schlüssel der Organisation verschlüsselt, bevor er gespeichert wird. Das Schlüsselpaar wird bei der Erstellung einer neuen Organisation oder bei einer bestehenden Organisation durch den Client erzeugt und verschlüsselt, und zwar durch:
>
> - Navigation zum Fenster Verwalten → Personen.
> - Updates von Elementen im Fenster Einstellungen → Meine Organisation.
> - Upgrades von einem Organisationstyp zu einem anderen.

Sichere Passwortfreigabe: Bitwarden ermöglicht die sichere Freigabe und Verwaltung sensibler Daten mit Benutzern im gesamten Unternehmen. Eine Kombination aus asymmetrischer und symmetrischer Verschlüsselung schützt sensible Informationen, während sie geteilt werden.

Open-Source und verfügbarer Quellcode:
Der Quellcode für alle Bitwarden-Softwareprodukte wird auf GitHub gehostet und wir laden jeden ein, den Bitwarden-Code zu überprüfen, zu prüfen und dazu beizutragen. Der Quellcode von Bitwarden wird von renommierten Sicherheitsprüfungsfirmen von Drittanbietern sowie unabhängigen Sicherheitsforschern geprüft. Darüber hinaus ruft das Bitwarden Schwachstellen Offenlegungsprogramm die Hilfe der Hacker-Community bei HackerOne auf, um Bitwarden sicherer zu machen.

Datenschutz durch Design: Bitwarden speichert alle Ihre Anmeldungen in einem verschlüsselten Tresor, der auf allen Ihren Geräten synchronisiert wird. Da es vollständig verschlüsselt ist, bevor es Ihr Gerät überhaupt verlässt, haben nur Sie Zugang zu Ihren Daten. Nicht einmal das Team bei Bitwarden kann Ihre Daten lesen (selbst wenn wir wollten). Ihre Daten sind versiegelt mit AES-CBC 256-Bit-Verschlüsselung, gesalzenem Hashing und PBKDF2 SHA-256.

Sicherheitsprüfung & Compliance: Open Source und von Drittanbietern geprüft, entspricht Bitwarden den AICPA SOC2 Typ 2 / Privacy Shield, GDPR und CCPA Vorschriften.

Master-Passwort

Der Datenschutz der Benutzerdaten in Bitwarden beginnt in dem Moment, in dem ein Benutzer ein Konto und ein Master-Passwort erstellt. Wir empfehlen dringend, während des Onboarding-Prozesses ein starkes Master-Passwort zu verwenden. Bitwarden enthält einen Passwort-Stärke-Messer als Leitfaden, der die Gesamtstärke des eingegebenen Master-Passworts bewertet und anzeigt, um ein starkes Master-Passwort zu fördern.

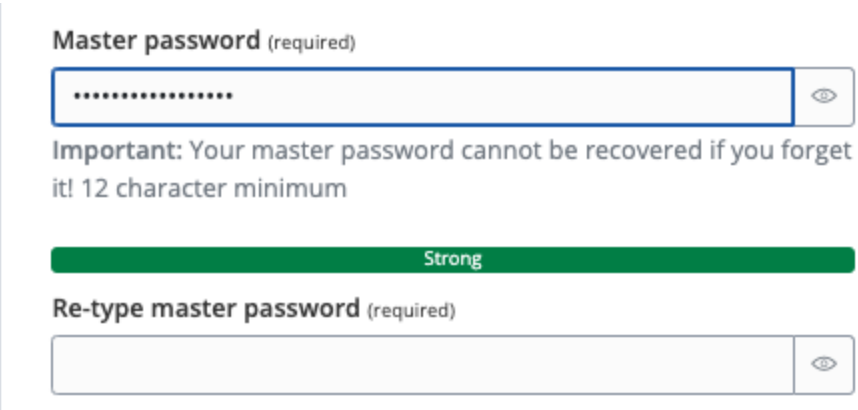

Abbildung: Erstellen eines Bitwarden-Kontos

Wenn Sie versuchen, sich mit einem schwachen Passwort anzumelden, wird Bitwarden Sie darauf hinweisen, dass das gewählte Master-Passwort schwach ist. Wenn Sie ein Bitwarden-Konto erstellen, haben Sie auch die Möglichkeit, bekannte Datendiebstähle für das Master-Passwort mit HIBP zu überprüfen.

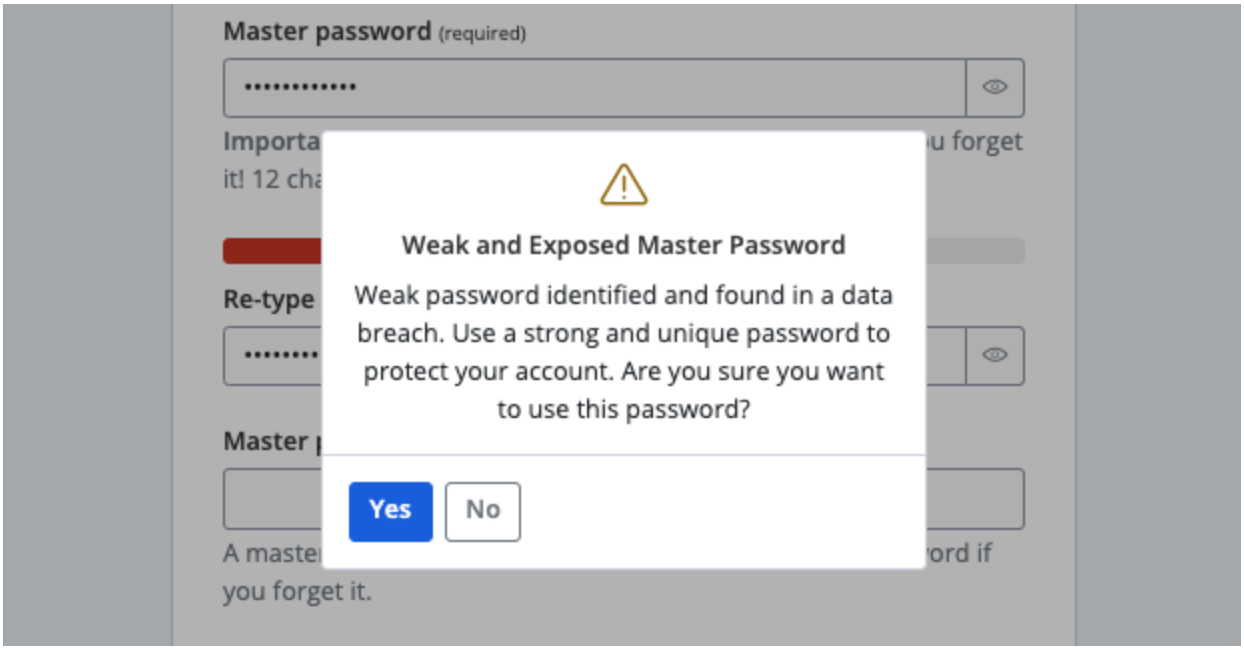

Abbildung: Warnung vor schwachem Master-Passwort

Die Verwendung eines starken Master-Passworts ist zu Ihrem eigenen Sicherheitsvorteil, da es das Token ist, das Sie verwenden, um auf Ihren sicheren Tresor zuzugreifen, in dem Ihre sensiblen Einträge gespeichert sind. Sie sind verantwortlich für die Sicherheit Ihres Kontos, während Sie den Bitwarden-Dienst nutzen. Wir bieten zusätzliche Maßnahmen, wie die Zwei-Schritt-Zugangsdaten, um Ihnen bei der Aufrechterhaltung der Sicherheit Ihres Kontos zu helfen, aber der Inhalt Ihres Kontos und seine Sicherheit liegen bei Ihnen.

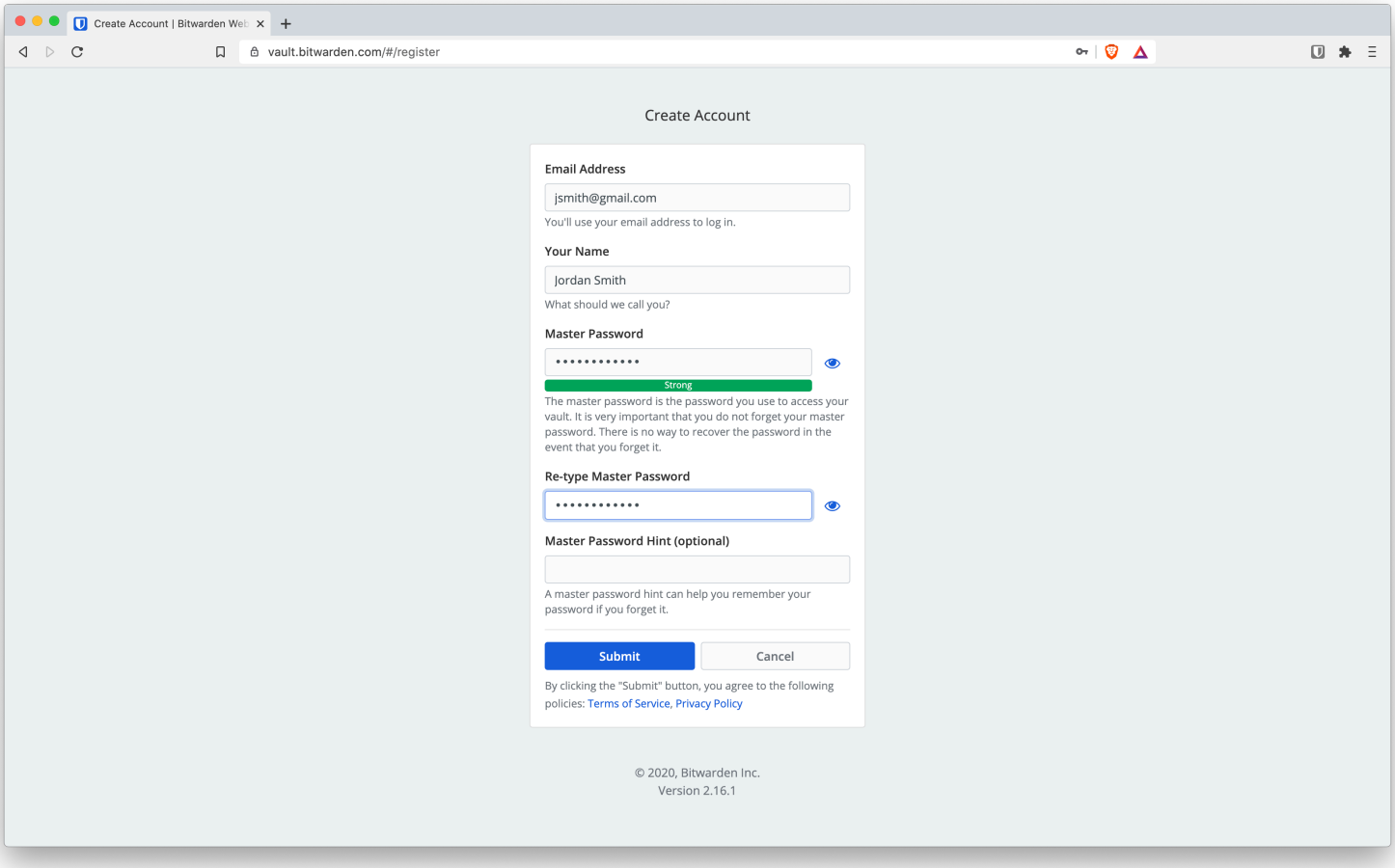

Abbildung: Setzen Sie ein starkes Master-Passwort

Weiterlesen: Fünf beste Praktiken für Passwort-Management und 3 Tipps vom NIST, um Ihre Passwörter sicher zu halten

Nützliche Werkzeuge: Bitwarden Passwortstärke-Testwerkzeug und Bitwarden Passwort-Generator

Es ist sehr wichtig, dass Sie Ihr Master-Passwort niemals vergessen. Das Master-Passwort wird nach Gebrauch aus dem Speicher gelöscht und niemals über das Internet an Bitwarden-Server übertragen, daher gibt es keine Möglichkeit, das Passwort wiederherzustellen, falls Sie es vergessen.

Das bedeutet auch, dass niemand aus dem Bitwarden-Team jemals Ihre echten Daten sehen, lesen oder rückentwickeln kann. Ihre Daten sind vollständig verschlüsselt und/oder gehasht, bevor sie jemals Ihr lokales Gerät verlassen. Dies ist ein kritischer Schritt, den Bitwarden unternimmt, um Sie und Ihre Daten zu schützen.

Nachdem Sie Ihr Konto erstellt und Ihr Master-Passwort festgelegt haben, generiert Bitwarden als nächstes mehrere Schlüssel, die zum Schutz der Daten Ihres Kontos verwendet werden.

ⓘ Note

Mitte 2021 führte Bitwarden die Kontowiederherstellung für Enterprise-Pläne ein. Mit dieser Option haben Benutzer und Organisationen die Möglichkeit, eine neue Richtlinie umzusetzen, die Administratoren und Eigentümern erlaubt, Passwörter für Benutzer zurückzusetzen.

Überblick über den Hashing-, Schlüsselableitungs- und Verschlüsselungsprozess des Master-Passworts

Benutzerkonto Erstellung

Wenn das Formular zur Kontoerstellung abgesendet wird, verwendet Bitwarden die Passwortbasierte Schlüsselableitungsfunktion 2 (PBKDF2) mit 600.000 Iterationsrunden, um das Master-Passwort des Benutzers mit einem Salt der E-Mail-Adresse des Benutzers zu strecken. Der resultierende gesalzene Wert ist der 256-Bit-Master-Schlüssel. Der Master-Schlüssel wird zusätzlich auf 512 Bit Länge gestreckt, indem die HMAC-basierte Extract-and-Expand-Schlüsselableitungsfunktion (HKDF) verwendet wird. Der Master-Schlüssel und der gestreckte Master-Schlüssel werden niemals auf Bitwarden-Servern gespeichert oder dorthin übertragen.

> **Note**
> In der Version 2023.2.0 hat Bitwarden Argon2id als alternative Option zu PBKDF2 hinzugefügt. Erfahren Sie mehr.

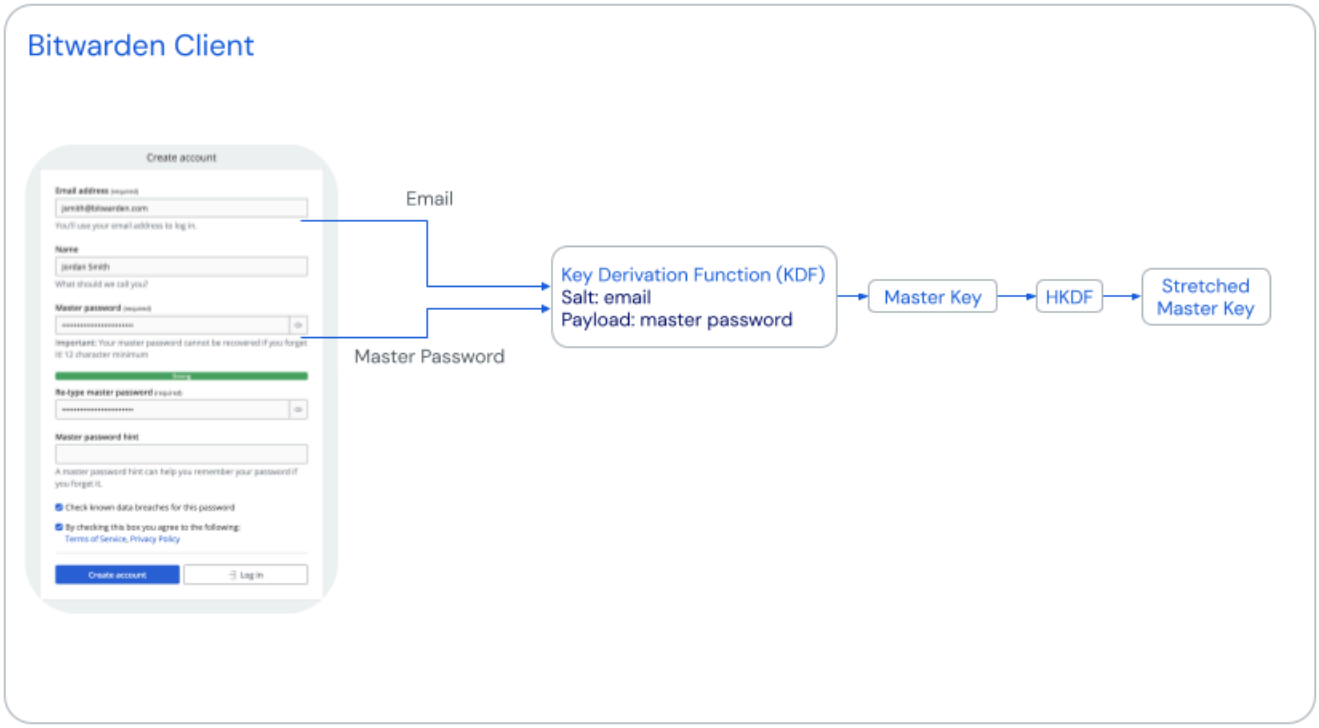

Abbildung: Passwortbasierte Schlüsselableitung

Darüber hinaus wird ein 512-Bit-Symmetrischer Schlüssel und ein Initialisierungsvektor mit einem kryptographisch sicheren pseudozufälligen Nummer Generator (CSPRNG) generiert. Der symmetrische Schlüssel wird mit AES-256-Bit-Verschlüsselung unter Verwendung des gestreckten Master-Schlüssels und des Initialisierungsvektors verschlüsselt. Der resultierende Schlüssel wird als geschützter symmetrischer Schlüssel bezeichnet. Der geschützte symmetrische Schlüssel ist der Hauptschlüssel, der mit dem Benutzer verbunden ist und bei der Kontoerstellung an den Server gesendet wird, und der bei der Synchronisation an die Bitwarden Client-Apps zurückgesendet wird.

Ein asymmetrischer Schlüssel wird auch generiert (RSA-Schlüsselpaar), wenn der Benutzer sein Konto registriert. Das generierte RSA-Schlüsselpaar wird verwendet, wenn und sobald der Benutzer eine Organisation erstellt, die erstellt und verwendet werden kann, um Daten zwischen Benutzern zu teilen. Für weitere Informationen, siehe Daten zwischen Benutzern teilen.

Ein Hash des Master-Passworts wird ebenfalls mit PBKDF-SHA256 generiert, mit einer Nutzlast des Master-Schlüssels und einem Salz des Master-Passworts. Der Hash des Master-Passworts wird bei der Erstellung des Kontos und bei den Zugangsdaten an den Server gesendet und zur Authentifizierung des Benutzerkontos verwendet. Sobald der Server erreicht ist, wird der Master-Passwort-Hash erneut mit PBKDF2-SHA256 und einem zufälligen Salt sowie 600.000 Iterationen gehasht. Eine Übersicht über den Passwort-Hashing-, Schlüsselableitungs- und Verschlüsselungsprozess wird unten gezeigt.

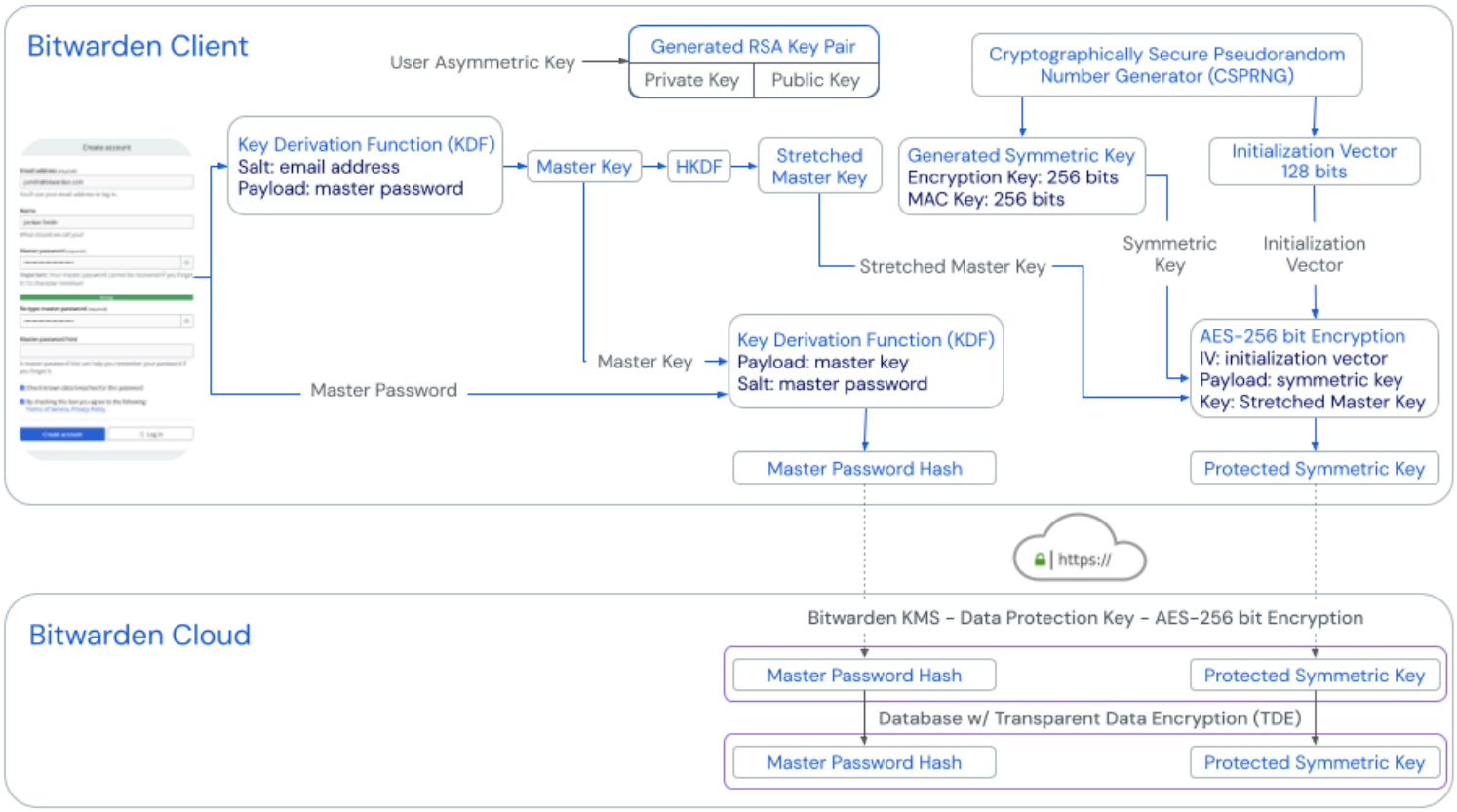

Abbildung: Übersicht über die verschiedenen Schlüssel, die bei der Registrierung eines neuen Bitwarden-Kontos erzeugt werden

Benutzer Zugangsdaten | Benutzer Authentifizierung | Zugang zu Benutzer Tresor Daten

Sie müssen zunächst Ihre E-Mail-Adresse und Ihr Master-Passwort eingeben, um sich bei Ihrem Bitwarden-Konto anzumelden .

Als nächstes verwendet Bitwarden die Password-Based Key Derivation Function 2 (PBKDF2) mit einem Standard von 600.000 Iterationsrunden, um Ihr Master-Passwort mit einem Salz Ihrer E-Mail-Adresse zu strecken. Der resultierende gesalzene Wert ist der 256-Bit-Master-Schlüssel. Ein Hash des Master-Schlüssels wird bei der Erstellung und den Zugangsdaten des Kontos an den Server gesendet und zur Authentifizierung des Benutzerkontos verwendet.

> **ⓘ Note**
>
> In der Version 2023.2.0 hat Bitwarden Argon2id als alternative Option zu PBKDF2 hinzugefügt. Erfahren Sie mehr.

Der Master-Schlüssel wird zusätzlich auf 512 Bit Länge gestreckt, indem die HMAC-basierte Extract-and-Expand-Schlüsselableitungsfunktion (HKDF) verwendet wird. Der geschützte symmetrische Schlüssel wird mit dem gestreckten Master-Schlüssel entschlüsselt. Der symmetrische Schlüssel wird verwendet, um Einträge im Tresor zu entschlüsseln. Die Entschlüsselung erfolgt vollständig auf dem Bitwarden Client, da Ihr Master-Passwort oder gestreckter Master-Schlüssel niemals auf Bitwarden-Servern gespeichert oder dorthin übertragen wird.

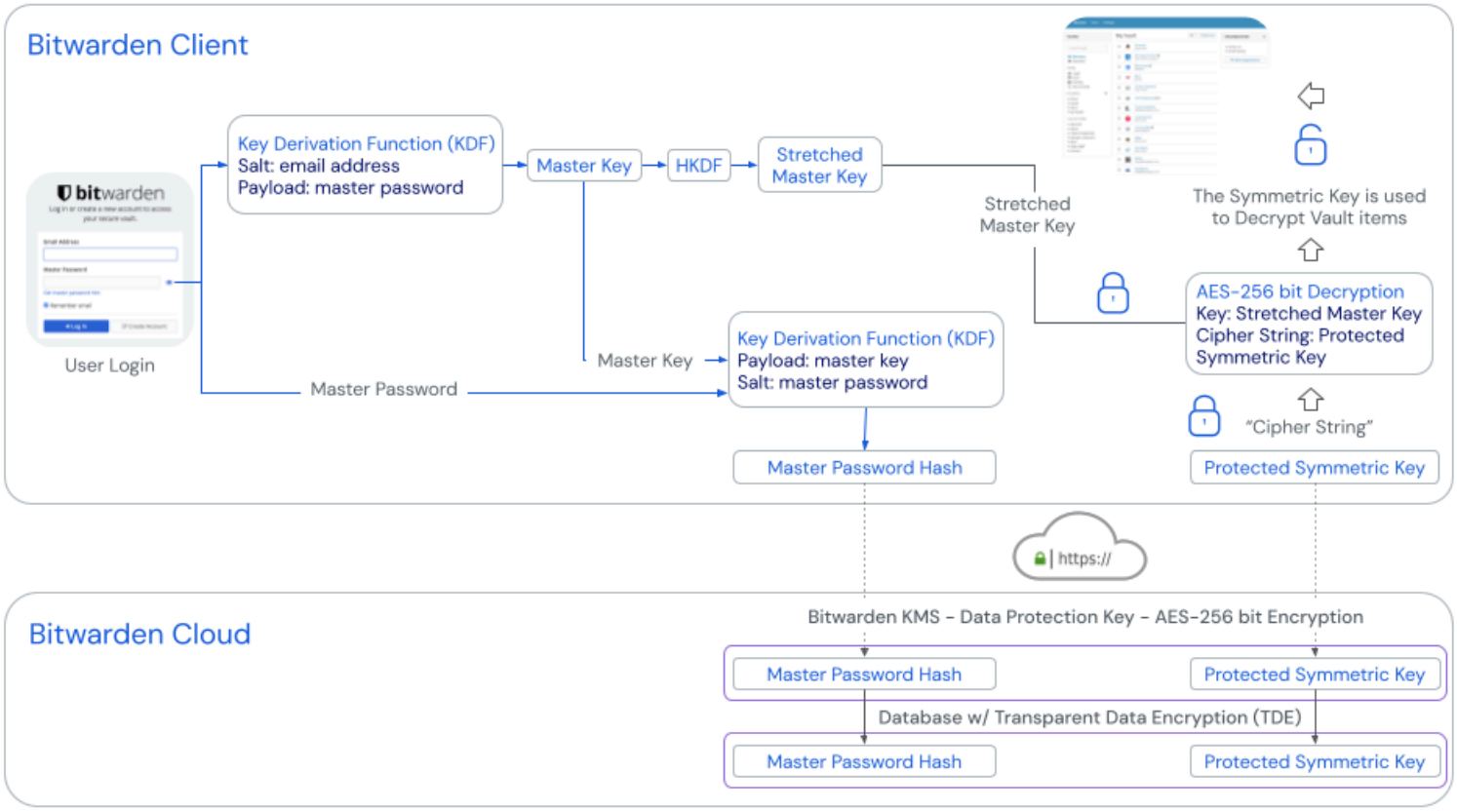

Abbildung: Übersicht über die Benutzeranmeldung

Wir speichern das Master-Passwort nicht lokal oder im Speicher auf dem Bitwarden Client. Ihr Verschlüsselungsschlüssel (Symmetrischer Schlüssel) wird im Speicher gehalten, während die App entsperrt ist. Dies wird benötigt, um Daten in Ihrem Tresor zu entschlüsseln. Wenn der Tresor gesperrt ist, werden diese Daten aus dem Speicher gelöscht. Nach einer bestimmten Zeit der Inaktivität auf dem Sperrbildschirm laden wir die Anwendungsprozesse neu, um sicherzustellen, dass auch alle übrig gebliebenen verwalteten Speicheradressen gelöscht werden. Wir tun unser Bestes, um sicherzustellen, dass alle Daten, die möglicherweise im Speicher für die Funktion der Anwendung vorhanden sind, nur so lange im Speicher gehalten werden, wie Sie sie benötigen und dass der Speicher immer dann bereinigt wird, wenn die Anwendung gesperrt ist. Wir betrachten die Anwendung als völlig sicher, während sie in einem gesperrten Zustand ist.

Zusätzlicher Benutzerdatenschutz bei Aktivierung der Zwei-Schritte-Zugangsdaten

Die Zwei-Schritt-Anmeldung (auch als Zwei-Faktor-Authentifizierung oder 2FA bezeichnet) ist eine zusätzliche Sicherheitsebene für Ihr Konto, die sicherstellen soll, dass Sie die **einzige** Person sind, die auf Ihr Konto zugreifen kann, selbst wenn jemand Ihr Master-Passwort entdecken sollte.

Als beste Vorgehensweise empfehlen wir allen Benutzern, die zweistufige Anmeldung in ihrem Bitwarden-Konto zu aktivieren und zu verwenden. Wenn die Zwei-Schritt-Zugangsdaten aktiviert sind, müssen Sie einen zusätzlichen Schritt durchführen, wenn Sie sich bei Bitwarden anmelden (zusätzlich zu Ihrem Master-Passwort). Standardmäßig werden Sie aufgefordert, diesen zweiten Schritt jedes Mal abzuschließen, es gibt jedoch eine Aufforderung "Mich merken", die Ihren 2FA-Status speichert, sodass Sie sich das nächste Mal auf diesem speziellen Gerät bis zu 30 Tage lang ohne 2FA anmelden können.

Notiz: Wenn Sie Ihr Master-Passwort ändern oder Sitzungen deautorisieren, müssen Sie die 2FA-Authentifizierung erneut durchführen, unabhängig davon, ob Sie zuvor "Remember Me" ausgewählt haben oder nicht.

Bitwarden unterstützt die zweistufige Anmeldung mit den folgenden Methoden:

Kostenlose Pläne

- Die Verwendung einer Authenticator-App (zum Beispiel, 2FAS, Ravio oder Aegis)
- FIDO2 WebAuthn (jeder FIDO2 WebAuthn zertifizierte Schlüssel)
- E-Mail

Premium-Funktionen - enthalten als Teil der Family-, Teams- und Enterprise-Pläne

- Duo Sicherheit mit Duo Push, SMS, Telefonanruf und U2F Sicherheitsschlüsseln
- YubiKey (jedes Gerät der 4/5 Serie oder YubiKey NEO/NFC)

Sie können mehrere Methoden zur zweistufigen Anmeldung aktivieren. Wenn Sie mehrere zweistufige Anmeldemethoden aktiviert haben, ist die Reihenfolge der bevorzugten Standardmethode, die beim Anmelden angezeigt wird, wie folgt: FIDO U2F > YubiKey > Duo > Authenticator App > E-Mail-Adresse. Sie können jedoch während der Eingabe Ihrer Zugangsdaten manuell zu jeder Methode wechseln und diese verwenden.

Es ist sehr wichtig, dass Sie Ihre zweistufigen Zugangsdaten-Wiederherstellungscodes niemals verlieren. Bitwarden bietet ein Sicherheitsmodell zum Schutz des Kontos, das keine Unterstützung für Benutzer bietet, die ihr Master-Passwort oder die Wiederherstellungscodes für die zweistufigen Zugangsdaten verlieren. Wenn Sie die Zwei-Schritt-Zugangsdaten für Ihr Konto aktiviert haben und den Zugang zu Ihren Wiederherstellungscodes für die Zwei-Schritt-Zugangsdaten verlieren, können Sie sich nicht bei Ihrem Bitwarden-Konto anmelden.

> **ⓘ Note**
>
> Mitte 2021 führte Bitwarden die Kontowiederherstellung für Enterprise-Pläne ein. Mit dieser Option haben Benutzer und Organisationen die Möglichkeit, eine neue Richtlinie umzusetzen, die Administratoren und Eigentümern erlaubt, Passwörter für Benutzer zurückzusetzen.

Benutzerpasswort ändern

Ihr Master-Passwort kann nur vom Web-Tresor geändert werden. Für spezifische Schritte, wie Sie Ihr Benutzerpasswort ändern können, sehen Sie sich diesen Bitwarden Hilfe Artikel an.

Erneuern Sie den Verschlüsselungsschlüssel Ihres Kontos

Während einer Passwortänderungsoperation haben Sie auch die Möglichkeit, den Verschlüsselungsschlüssel Ihres Kontos zu erneuern (ändern). Es ist eine gute Idee, den Verschlüsselungsschlüssel zu erneuern, wenn Sie glauben, dass Ihr vorheriges Master-Passwort kompromittiert wurde oder dass die Daten Ihres Bitwarden-Tresors von einem Ihrer Geräte gestohlen wurden.

> **⚠ Warning**
>
> Das Rotieren des Verschlüsselungsschlüssels Ihres Kontos ist ein sensibler Vorgang, weshalb es keine Standardoption ist. Eine Schlüsselrotation beinhaltet die Generierung eines neuen, zufälligen Verschlüsselungsschlüssels für Ihr Konto und das erneute Verschlüsseln aller Tresor-Daten mit diesem neuen Schlüssel. Weitere Details finden Sie in diesem Artikel in Bitwardens Hilfe-Center.

Datenschutz bei der Übertragung

Bitwarden nimmt die Sicherheit sehr ernst, wenn es um den Umgang mit Ihren sensiblen Daten geht. Ihre Daten werden niemals an die Bitwarden Cloud gesendet, ohne zuerst auf Ihrem lokalen Gerät verschlüsselt zu werden.

Darüber hinaus verwendet Bitwarden TLS/SSL, um die Kommunikation zwischen Bitwarden-Clients und Benutzergeräten zur Bitwarden-Cloud zu sichern. Die TLS-Implementierung von Bitwarden verwendet 2048-Bit-X.509-Zertifikate für die Server-Authentifizierung und den Schlüsselaustausch sowie eine starke Verschlüsselungssuite für die Massenverschlüsselung. Unsere Server sind so konfiguriert, dass sie schwache Verschlüsselungsalgorithmen und Protokolle ablehnen.

Bitwarden implementiert auch HTTP-Sicherheitsheader wie HTTP Strict Transport Security (HSTS), die alle Verbindungen dazu zwingen, TLS zu verwenden. Diese zusätzliche Schutzschicht mit HSTS verringert die Risiken von Downgrade-Angriffen und Fehlkonfigurationen.

Datenschutz im Ruhezustand

Bitwarden verschlüsselt und/oder hashiert Ihre Daten immer auf Ihrem lokalen Gerät, bevor sie zur Synchronisation an die Cloud-Server gesendet werden. Die Bitwarden-Server werden nur zum Speichern und Synchronisieren verschlüsselter Tresor-Daten verwendet. Es ist nicht möglich, Ihre unverschlüsselten Daten von den Bitwarden Cloud-Servern zu erhalten. Insbesondere verwendet Bitwarden die AES 256-Bit-Verschlüsselung sowie PBKDF-SHA256, um Ihre Daten zu sichern.

AES ist ein Standard in der Kryptographie und wird von der US-Regierung und anderen Regierungsbehörden auf der ganzen Welt zum Schutz von streng geheimen Daten verwendet. Mit einer ordnungsgemäßen Implementierung und einem starken Verschlüsselungsschlüssel (Ihr Master-Passwort) gilt AES als unknackbar.

PBKDF-SHA256 wird verwendet, um den Verschlüsselungsschlüssel aus Ihrem Master-Passwort abzuleiten. Dann wird dieser Schlüssel gesalzen und gehasht zur Authentifizierung mit den Bitwarden-Servern. Die standardmäßig verwendete Iterationsanzahl mit PBKDF2 beträgt 600.001 Iterationen auf dem Client (diese Client-seitige Iterationsanzahl kann in Ihren Kontoeinstellungen konfiguriert werden) und dann zusätzliche 100.000 Iterationen, wenn sie auf unseren Servern gespeichert wird (für insgesamt 700.001 Iterationen standardmäßig).

> **Note**
>
> In der Version 2023.2.0 hat Bitwarden Argon2id als alternative Option zu PBKDF2 hinzugefügt. Erfahren Sie mehr.

Einige verschlüsselte Daten, einschließlich des geschützten symmetrischen Schlüssels eines Benutzers und des Master-Passwort-Hashs, werden auch transparent von der Anwendung verschlüsselt, wenn sie sich in Ruhe befinden, was bedeutet, dass sie verschlüsselt und wieder entschlüsselt werden, wenn sie in die Bitwarden-Datenbank ein- und ausfließen.

Bitwarden verwendet zusätzlich Azure transparente Datenverschlüsselung (TDE), um gegen die Bedrohung durch bösartige Offline-Aktivitäten zu schützen, indem es eine Echtzeit-Verschlüsselung und Entschlüsselung der Datenbank, zugehöriger Backups und Transaktionsprotokolldateien im Ruhezustand durchführt.

Erfahren Sie mehr: Wie End-to-End-Verschlüsselung den Weg für Zero Knowledge ebnet und Welche Verschlüsselung verwendet wird

Melden Sie sich mit Passschlüsseln an und halten Sie eine Ende-zu-Ende-Verschlüsselung aufrecht.

Neben dem Master-Passwort können Benutzer wählen, ihren Tresor mit einem Passwort zu entsperren. Dieser Prozess nutzt einen führenden Standard und eine Erweiterung für WebAuthn, die als pseudo-zufällige Funktion oder PRF bezeichnet wird, welche Schlüsselmaterial von einem Authentifikator bezieht. Mit PRF werden abgeleitete Schlüssel bei der Verschlüsselung und Entschlüsselung von Daten verwendet, die im Bitwarden Passwort-Manager Tresor und Bitwarden Secrets Manager gespeichert sind, wobei eine durchgängige, Null-Wissen-Verschlüsselung aufrechterhalten wird.

Wenn ein Passschlüssel zur Anmeldung bei Bitwarden registriert ist:

1. Ein **öffentlicher und privater Schlüsselpaar-Passkey** wird vom Authenticator über die WebAuth API generiert. Dieses Schlüsselpaar bildet per Definition Ihren Passschlüssel.

2. Ein **PRF symmetrischer Schlüssel** wird vom Authenticator über die PRF-Erweiterung der WebAuthn API generiert. Dieser Schlüssel wird aus einem **internen Geheimnis** abgeleitet, das einzigartig für Ihren Passschlüssel ist, und einem von Bitwarden bereitgestellten **Salt**.

3. Ein **PRF öffentliches und privates Schlüsselpaar** wird vom Bitwarden Client generiert. Der PRF-öffentliche Schlüssel verschlüsselt Ihren **Konto-Verschlüsselungsschlüssel**, auf den Ihr Client Zugriff haben wird, indem er angemeldet und entsperrt ist, und der resultierende **PRF-verschlüsselte Konto-Verschlüsselungsschlüssel** wird an den Server gesendet.

4. Der **PRF-Privatschlüssel** wird mit dem **PRF-Symmetrischen Schlüssel** verschlüsselt (siehe Schritt 2) und der resultierende **PRF-verschlüsselte Privatschlüssel** wird an den Server gesendet.

5. Ihr Client sendet Daten an Bitwarden-Server, um einen neuen Passkey-Credential-Datensatz für Ihr Konto zu erstellen. Wenn Ihr Passwort bei der Unterstützung für die Verschlüsselung und Entschlüsselung des Tresors registriert ist, enthält dieser Datensatz:
   - Der Passwortname
   - Der öffentliche Passkey
   - Der PRF öffentlicher Schlüssel
   - Der PRF-verschlüsselte Konto-Verschlüsselungsschlüssel
   - Der PRF-verschlüsselte private Schlüssel

Ihr privater Passkey, der zur Authentifizierung benötigt wird, verlässt den Client nur in einem verschlüsselten Format.

Wenn ein Passschlüssel verwendet wird, um sich anzumelden und insbesondere Ihre Tresor Daten zu entschlüsseln:

1. Mit der Verwendung von WebAuthn API öffentlicher Schlüsselkryptographie wird Ihre Authentifizierungsanforderung behauptet und bestätigt.

2. Ihr **PRF-verschlüsselter Kontoverschlüsselungsschlüssel** und **PRF-verschlüsselter privater Schlüssel** werden vom Server an Ihren Client gesendet.

3. Unter Verwendung des gleichen von Bitwarden bereitgestellten **Salz** und des für Ihren Passschlüssel einzigartigen **internen Geheimnisses** wird der **PRF-Symmetrischer Schlüssel** lokal neu erstellt.

4. Der **PRF-Symmetrischer Schlüssel** wird verwendet, um Ihren **PRF-verschlüsselten privaten Schlüssel** zu entschlüsseln, was zu Ihrem **PRF-privaten Schlüssel** führt.

5. Der **PRF-Privatschlüssel** wird verwendet, um Ihren **PRF-verschlüsselten Konto-Verschlüsselungsschlüssel** zu entschlüsseln, was zu Ihrem **Konto-Verschlüsselungsschlüssel** führt. Ihr Kontoschlüssel wird verwendet, um Ihre Tresordaten zu entschlüsseln.

Wie Einträge im Tresor gesichert werden

Alle Informationen (Zugangsdaten, Karten, Identitäten, Notizen), die mit Ihren gespeicherten Tresor-Daten verbunden sind, sind durch eine Ende-zu-Ende-Verschlüsselung geschützt. Einträge, die Sie in Ihrem Bitwarden Tresor speichern möchten, werden zuerst mit einem Eintrag namens Cipher-Objekt gespeichert. Chiffrierobjekte werden mit Ihrem generierten symmetrischen Schlüssel verschlüsselt, der nur durch Entschlüsselung Ihres geschützten symmetrischen Schlüssels mit Ihrem gestreckten Master-Schlüssel bekannt sein kann. Diese Verschlüsselung und Entschlüsselung erfolgen vollständig auf dem Bitwarden Client, da Ihr Master-Passwort oder gestreckter Master-Schlüssel niemals auf Bitwarden-Servern gespeichert oder übertragen wird.

Tresor-Gesundheits-Berichte

Alle kostenpflichtigen Bitwarden-Pläne beinhalten Tresor-Gesundheitsberichte sowohl für Einzelpersonen als auch für Organisationen.

Für einzelne Tresore haben Einzelpersonen Zugang zu folgendem:

- Bericht über kompromittierte Passwörter
- Bericht über wiederverwendete Passwörter
- Bericht über schwache Passwörter
- Bericht über unsichere Websites
- Inaktiver 2FA Bericht
- Bericht über Datendiebstahl

Für Geschäftsanwender existiert ein ähnlicher Satz von Berichten für Einträge im Organisationstresor.

Lesen Sie mehr: Tresor Gesundheit Berichte

Für weitere Informationen zu Bitwarden Ereignisprotokollen und externer Berichterstattung, siehe Ereignisprotokolle.

Import von Passwörtern und anderen Geheimnissen in Bitwarden

Sie können Ihre Daten ganz einfach aus über 40 verschiedenen Diensten, einschließlich aller beliebten Passwort-Manager-Anwendungen, in Bitwarden importieren. Die vollständige Liste der unterstützten Anwendungen und einige zusätzliche Informationen, einschließlich der Fehlerbehebungsschritte für den Import Ihrer Daten in Bitwarden, sind in Bitwarden Hilfezentrum dokumentiert.

Wenn Sie Ihre Seiten aus dem LastPass.com Web Tresor exportieren, beziehen Sie sich bitte auf die spezifischen Informationen in dieser Hilfe Notiz Importieren Sie Ihre Daten von LastPass.

Daten zwischen Benutzern teilen

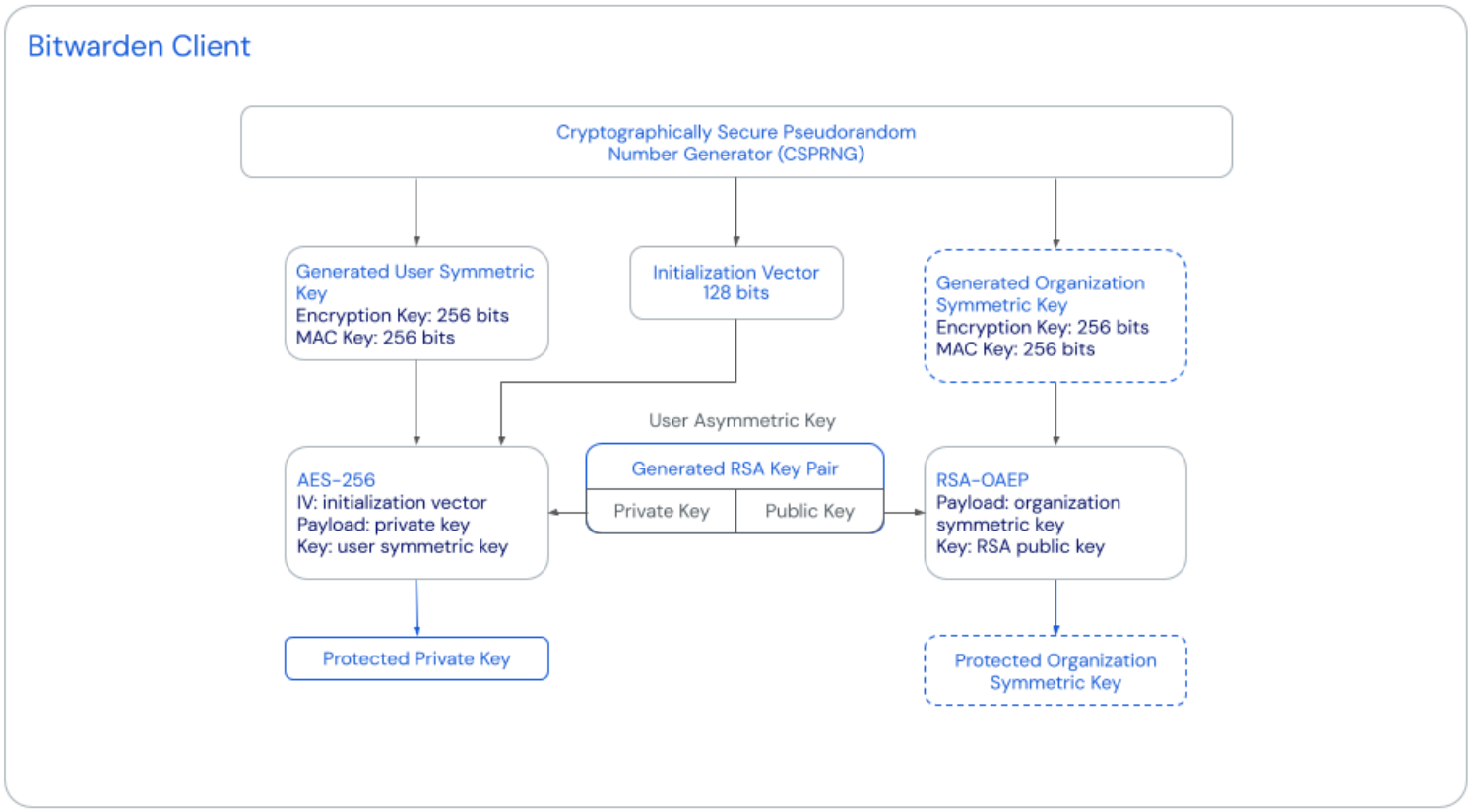

Abbildung: Symmetrischer Schlüssel der Organisation und asymmetrischer Schlüssel des Benutzers, die das RSA-Schlüsselpaar bilden

Zusammenarbeit ist einer der führenden Vorteile bei der Verwendung eines Passwort-Managers. Um das Teilen zu ermöglichen, müssen Sie zuerst eine Organisation erstellen. Eine Bitwarden Organisation ist eine Einheit, die Benutzer zusammenbringt, die Einträge teilen möchten. Eine Organisation könnte eine Familie, ein Team, ein Unternehmen oder jede andere Art von Gruppe sein, die den Wunsch hat, Daten zu teilen.

Ein einzelnes Benutzerkonto kann viele verschiedene Organisationen erstellen und/oder diesen angehören, was es Ihnen ermöglicht, Ihre Einträge von einem einzigen Konto aus zu verwalten.

Sie können eine neue Bitwarden Organisation vom Web Tresor aus erstellen oder einen Administrator einer bestehenden Organisation bitten, Ihnen eine Einladung zu senden.

Wenn Sie eine Organisation erstellen

Wenn Sie eine Organisation erstellen, wird ein symmetrischer Organisationsschlüssel mit einem kryptographisch sicheren pseudozufälligen Nummer Generator (CSPRNG) generiert. Dieser symmetrische Schlüssel der Organisation wird verwendet, um die vom Tresor der Organisation gehaltenen Daten zu entschlüsseln. Daher erfordert das Teilen von Daten mit Mitgliedern der Organisation einen sicheren Zugang dazu. Der rohe symmetrische Organisationsschlüssel wird niemals auf Bitwarden-Servern gespeichert.

Sobald der symmetrische Schlüssel der Organisation generiert ist, wird RSA-OAEP verwendet, um den symmetrischen Schlüssel der Organisation mit dem RSA-öffentlichen Schlüssel des Erstellers der Organisation zu verschlüsseln. Ein RSA-Schlüsselpaar wird für jeden Benutzer bei der Kontoerstellung generiert, unabhängig davon, ob er ein Mitglied der Organisation ist oder nicht, so dass dieser Schlüssel bereits vor der Gründung der Organisation existieren wird.

> **Note**
> Der RSA-Privatschlüssel, dessen Verwendung unten beschrieben wird, wird verschlüsselt mit dem Verschlüsselungsschlüssel des Benutzerkontos gespeichert, daher müssen Benutzer vollständig angemeldet sein, um darauf zugreifen zu können.

Der resultierende Wert dieser Operation wird als geschützter symmetrischer Schlüssel der Organisation bezeichnet und an die Bitwarden-Server gesendet.

Wenn der Ersteller der Organisation oder ein beliebiges Mitglied der Organisation sich in ihr Konto anmeldet, verwendet die Client-Anwendung den entschlüsselten RSA-Privatschlüssel, um den geschützten symmetrischen Schlüssel der Organisation zu entschlüsseln, was zum symmetrischen Schlüssel der Organisation führt. Unter Verwendung des symmetrischen Schlüssels der Organisation werden die Daten des organisationseigenen Tresors lokal entschlüsselt.

Wenn Benutzer einer Organisation beitreten

Der Prozess für nachfolgende Benutzer, die einer Organisation beitreten, ist ziemlich ähnlich, jedoch sind einige Unterschiede bemerkenswert.

Zuerst bestätigt ein etabliertes Mitglied der Organisation, speziell jemand mit der Berechtigung, andere Benutzer einzuführen, den Benutzer zur Organisation. Dieses etablierte Mitglied hat aufgrund der Tatsache, dass es sich bereits in sein Konto angemeldet und den in dem vorherigen Abschnitt beschriebenen Entschlüsselungsprozess der Organisationsdaten durchlaufen hat, Zugang zum entschlüsselten symmetrischen Schlüssel der Organisation.

Also, wenn der neue Benutzer bestätigt ist, stellt der Client des etablierten Mitglieds eine Verbindung zu den Bitwarden-Servern her, ruft den RSA-öffentlichen Schlüssel des neuen Benutzers ab, der zum Zeitpunkt der Kontoerstellung auf den Bitwarden-Servern gespeichert ist, und verschlüsselt den entschlüsselten symmetrischen Schlüssel der Organisation damit. Dies führt zu einem neuen geschützten symmetrischen Schlüssel der Organisation, der an die Bitwarden-Server gesendet und für das neue Mitglied gespeichert wird.

> **Note**
> Jeder geschützte symmetrische Schlüssel der Organisation ist einzigartig für seinen Benutzer, aber jeder wird zu demselben erforderlichen symmetrischen Schlüssel der Organisation entschlüsselt, wenn er mit dem spezifischen RSA-Privatschlüssel seines Benutzers entschlüsselt wird.

Wenn der neue Benutzer sich in sein Konto anmeldet, verwendet die Client-Anwendung den entschlüsselten RSA-Privatschlüssel, um den neuen geschützten Organisationssymmetrischen Schlüssel zu entschlüsseln, was zum Organisationssymmetrischen Schlüssel führt. Unter Verwendung des symmetrischen Schlüssels der Organisation werden die Daten des organisationseigenen Tresors lokal entschlüsselt.

Weiterlesen: Was sind Organisationen?

Zugriffskontrollen und Verwalten von Bitwarden-Sammlungen

Wenn die Nutzung von Bitwarden in Ihrer Organisation wächst, ist es hilfreich, Benutzer zu haben, die Sammlungen unabhängig verwalten können, ohne Zugang zu allem im organisatorischen Tresor zu benötigen.

Das Verwalten von Sammlungen und Gruppen ist eine einfache Möglichkeit, den Zugriff auf Tresor-Einträge in Bitwarden zu trennen, zu gewähren oder zu begrenzen, wodurch die Sichtbarkeit von Ressourcen für Benutzer kontrolliert wird.

Eine vollständige Liste der Rollen und Zugriffskontrollen ist im Abschnitt Benutzertypen und Zugriffskontrolle des Bitwarden Hilfezentrums dokumentiert.

Weiterlesen: Über Sammlungen

Ereignisprotokolle

Ereignisprotokolle enthalten zeitgestempelte, detaillierte Informationen darüber, welche Aktionen oder Änderungen innerhalb einer Organisation stattgefunden haben. Diese Protokolle sind hilfreich bei der Untersuchung von Änderungen in Anmeldeinformationen oder Konfigurationen und sehr nützlich für die Untersuchung von Audit-Trails und zur Fehlerbehebung.

Zusätzliche Informationen zu Ereignisprotokollen sind im Bitwarden Hilfezentrum dokumentiert. Ereignisprotokolle sind nur für Teams und Business Pläne verfügbar.

Um mehr Daten zu sammeln, können Pläne mit API-Zugriff die Bitwarden API nutzen. API-Antworten enthalten den Typ des Ereignisses und relevante Daten.

SIEM-Integration und externe Systeme

Für Security Information und Event Management (SIEM) Systeme wie Splunk, beim Export von Daten aus Bitwarden, kann eine Kombination von Daten aus der API und CLI verwendet werden, um Daten zu sammeln.

Dieser Prozess wird in der Notiz des Hilfezentrums zu **Ereignisprotokollen der Organisation** unter SIEM und Integrationen externer Systeme beschrieben.

Kontoschutz und Vermeidung von Sperrungen

Heute bietet Bitwarden für Basic, Premium, Families und Teams Pläne, Kontoschutz mit einem Sicherheitsmodell an, das keinen Support für Benutzer bietet, die ihre Passwörter oder zweistufige Zugangsdaten Wiederherstellungscodes verlieren.

Bitwarden kann Benutzerpasswörter nicht zurücksetzen, noch kann Bitwarden die zweistufige Anmeldung deaktivieren, wenn sie auf Ihrem Konto aktiviert wurde. Eigentümer oder Administratoren von Families- und Teams-Konten können Benutzerpasswörter nicht zurücksetzen. Siehe den nächsten Abschnitt für Details zu Enterprise-Plänen.

> ⚠ **Warning**
>
> Benutzer, die ihr Master-Passwort oder ihren Wiederherstellungscode für die zweistufige Anmeldung verlieren, müssen ihr Konto löschen und neu beginnen.

Um diese potenziellen Probleme zu mildern, empfiehlt Bitwarden Folgendes zum Schutz des Kontos und zur Vermeidung von Sperrungen.

Master-Passwort
Identifizieren Sie eine Möglichkeit, wie Sie Ihr Master-Passwort behalten und wiederherstellen können, sollten Sie es vergessen. Dies könnte beinhalten, es niederzuschreiben und es in einem Safe oder an einem sicheren Ort zu platzieren.

Verwenden Sie einen Hinweis für das Master-Passwort
Wenn hilfreich, verwenden Sie den Hinweis zum Master-Passwort, der von Bitwarden bei der Anmeldung bereitgestellt wurde. Oder richten Sie jederzeit einen Hinweis über die Einstellungen im Web-Tresor ein.

Organisationsverwaltung
Für Organisationen, haben Sie mehrere Administratoren, die auf die Organisation zugreifen und sie verwalten können.

Zwei-Schritt-Zugangsdaten Wiederherstellungscode
Wenn Sie sich entscheiden oder von Ihrer Organisation dazu aufgefordert werden, eine Zwei-Schritt-Anmeldung einzurichten, stellen Sie sicher, dass Sie auf Ihren Wiederherstellungscode zugreifen und diesen an einem ebenso sicheren Ort wie Ihr Master-Passwort aufbewahren.

Kontowiederherstellung in Enterprise-Plänen

Mitte 2021 führte Bitwarden die Kontowiederherstellung für Enterprise-Pläne ein. Mit dieser Option haben Benutzer und Organisationen die Möglichkeit, eine neue Richtlinie umzusetzen, die Administratoren und Eigentümern erlaubt, Passwörter für Benutzer zurückzusetzen.

Bitwarden Cloud-Plattform und Webanwendungssicherheit

Übersicht über die Bitwarden-Architektur

Bitwarden verarbeitet und speichert alle Daten sicher in der Microsoft Azure Cloud mit Diensten, die vom Team bei Microsoft verwaltet werden. Da Bitwarden nur Dienstleistungen von Azure nutzt, gibt es keine Serverinfrastruktur zu verwalten und zu warten. Alle Verfügbarkeits-, Skalierbarkeits- und Sicherheitsaktualisierungen, Patches und Garantien werden von Microsoft und ihrer Cloud-Infrastruktur unterstützt.

Sicherheitsaktualisierungen und Patching

Das Team bei Microsoft verwaltet OS-Patching auf zwei Ebenen, den physischen Servern und den Gast-Virtual Machines (VMs), die die Azure App Service Ressourcen ausführen. Beide werden monatlich aktualisiert, was dem monatlichen Microsoft Patch Tuesday Zeitplan entspricht. Diese Aktualisierungen werden automatisch angewendet, auf eine Weise, die die hohe Verfügbarkeit von Azure-Diensten gemäß SLA garantiert.

Weiterlesen: Patching in Azure App Service oder SLA für App Service

Für detaillierte Informationen darüber, wie Aktualisierungen angewendet werden, lesen Sie hier

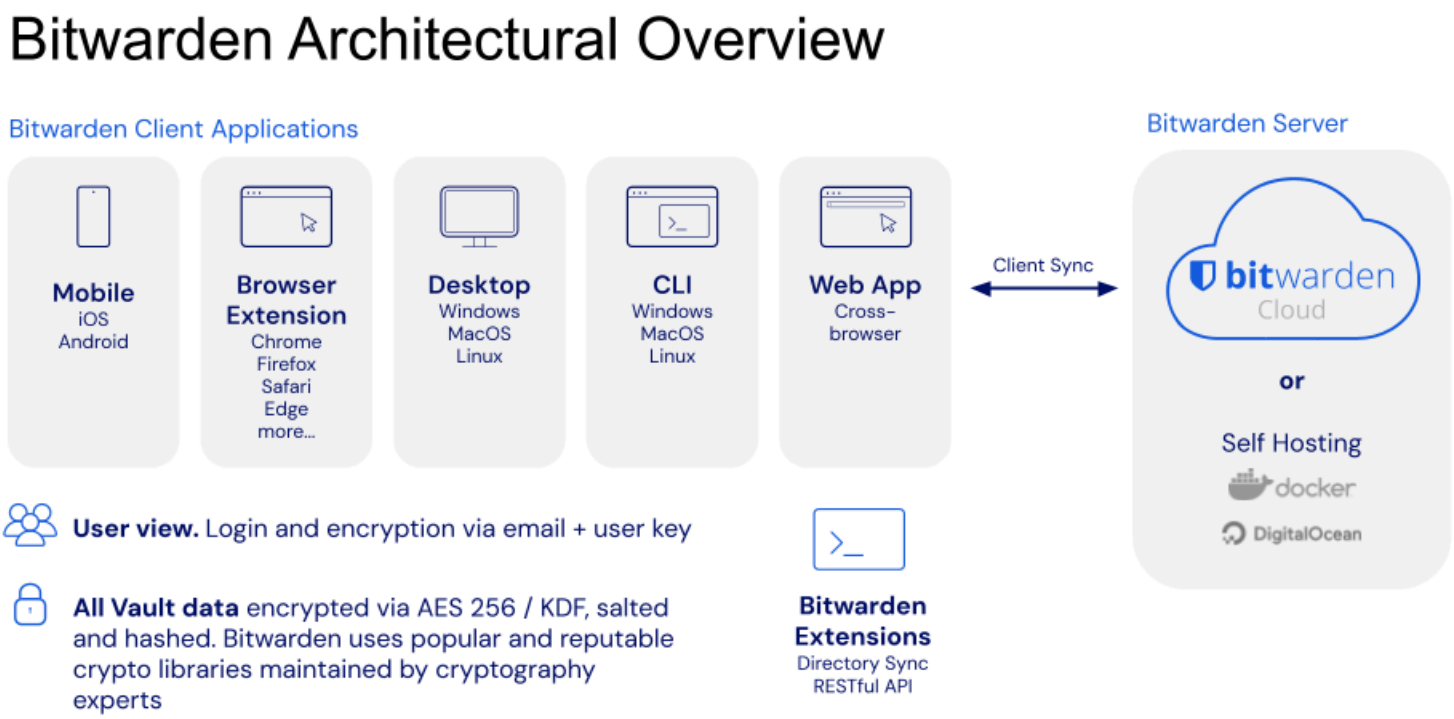

Abbildung: Ein Überblick über Bitwardens Architektur

Bitwarden Zugriffskontrollen

Bitwarden-Mitarbeiter haben eine bedeutende Ausbildung und Expertise für den Typ von Daten, Systemen und Informationsressourcen, die sie entwerfen, architektieren, implementieren, verwalten, unterstützen und mit denen sie interagieren.

Bitwarden folgt einem etablierten Onboarding-Prozess, um sicherzustellen, dass der entsprechende Zugriffslevel zugewiesen und aufrechterhalten wird. Bitwarden hat Zugriffsebenen festgelegt, die für jede Rolle angemessen sind. Alle Anfragen, einschließlich aller Zugriffsänderungsanfragen, müssen vom Manager überprüft und genehmigt werden. Bitwarden folgt einer Richtlinie mit minimalen Berechtigungen, die den Mitarbeitern das Mindestmaß an Zugang gewährt, das zur Erfüllung ihrer Aufgaben erforderlich ist. Bitwarden folgt einem etablierten Off-Boarding-Prozess über Bitwarden Human Resources, der bei Beendigung alle Zugriffsrechte widerruft.

Software-Lebenszyklus und Änderungsverwaltung

Bitwarden bewertet Änderungen an der Plattform, Anwendungen und Produktionsinfrastruktur, um Risiken zu minimieren, und solche Änderungen werden gemäß den Standardbetriebsverfahren bei Bitwarden implementiert.

Änderungsanforderungs-Einträge werden basierend auf der Roadmap geplant und zu diesem Zeitpunkt an die Technikabteilung übermittelt. Die Ingenieurabteilung wird ihre Kapazität überprüfen und bewerten und den Aufwand für jeden Änderungsantrag Eintrag einschätzen. Nach Überprüfung und Bewertung werden sie formulieren, woran sie für eine bestimmte Veröffentlichung arbeiten werden. Der CTO gibt Details zur Veröffentlichung über Kommunikationskanäle und Management-Meetings bekannt und der Entwicklungslebenszyklus für diese Veröffentlichung beginnt.

Hochrangiger Entwicklungs-, Freigabe-, Test- und Genehmigungsprozess:

- Entwickeln, Bauen und Iterieren mit Pull-Anfragen in GitHub
- Bringen Sie die Funktionen zu einem Punkt, an dem sie testbar sind.
- Die Ingenieurwissenschaften führen funktionale Tests der Funktion und/ oder des Produkts durch, während sie entwickelt und gebaut werden.
- Die Erstellung von Unit-Tests ist automatisiert als Teil der Bitwarden Continuous Integration (CI) Pipelines.
- Einige Tests werden auch vom Kundenerfolgsteam durchgeführt
- Der Direktor der Technik unterstützt bei der Überprüfung und hilft, den Prozess zu formalisieren, einschließlich der Aktualisierung der Dokumentation.
- CTO gibt endgültige Go / No-Go-Freigabe

Teilnahme an Meetings: Um eine erfolgreiche Überprüfung, Genehmigung, Umsetzung und Schließung von Änderungsanfragen zu gewährleisten, sollte jeder Kernmitarbeiter des Betriebs- und IT-Dienstes während des Meetings zur Überprüfung und Diskussion der Änderungsanfrage vertreten sein.

Notfalleinsätze / Hotfixes erhalten eine eskalierte Priorität und die Überprüfung und Genehmigung der Änderung wird von einem Manager oder Direktor vor der Durchführung der Änderung erhalten und wird anschließend überprüft, kommuniziert und während des nächsten geplanten Änderungstreffens geschlossen. Dies ist normalerweise bei einem Serviceausfall, Systemausfall oder in einer dringenden Ausfallsverhinderungssituation der Fall.

Kontrolle von Produktionssystemen

Bitwarden unterhält dokumentierte Handbücher für alle Produktionssysteme, die die Bereitstellung, Aktualisierung und Fehlerbehebungsprozesse abdecken. Umfangreiche Warnungen sind eingerichtet, um zu benachrichtigen und zu eskalieren, im Falle von Problemen.

Basis-Konfigurationen
Bitwarden verarbeitet und speichert alle Daten sicher in der Microsoft Azure Cloud mit Diensten, die vom Team bei Microsoft verwaltet werden. Da Bitwarden nur Dienstleistungen von Azure nutzt, gibt es keine Serverinfrastruktur zu verwalten und zu warten. Alle Verfügbarkeits-, Skalierbarkeits- und Sicherheitsaktualisierungen und Garantien werden von Microsoft und ihrer Cloud-Infrastruktur unterstützt.

Azure Service Konfigurationen werden von Bitwarden genutzt, um sicherzustellen, dass Anwendungen auf wiederholbare und konsistente Weise konfiguriert und bereitgestellt werden.

Bitwarden Plattform Schlüsselverwaltungsverfahren

Schlüssel und andere Geheimnisse, die von der Bitwarden-Plattform selbst genutzt werden, beinhalten Anmeldedaten für die Bitwarden Cloud-Anbieter Konten. Alle solche Schlüssel werden generiert, sicher gespeichert und bei Bedarf erneuert, in Übereinstimmung mit branchenüblichen Praktiken. Bitwarden verwendet einen internen Bitwarden-Tresor zur sicheren Speicherung und Sicherung von sensiblen Schlüsseln oder anderen Geheimnissen, die von der Bitwarden-Plattform genutzt werden. Der Zugriff auf den Bitwarden Tresor nutzt Benutzertypen und Zugriffskontrolle.

Datentypen und Datenaufbewahrung

Bitwarden verarbeitet zwei Arten von Benutzerdaten, um den Bitwarden-Service zu liefern: (i) Tresor Daten und (ii) Verwaltungsdaten.

(i) Tresor Daten

Tresor Daten beinhalten alle Informationen, die in Konten zum Bitwarden-Dienst gespeichert sind und können persönliche Informationen enthalten. Wenn wir den Bitwarden Service für Sie hosten, werden wir Tresor Daten hosten. Die Daten im Tresor werden mit sicheren kryptographischen Schlüsseln verschlüsselt, die unter Ihrer Kontrolle stehen. Bitwarden kann nicht auf Tresor Daten zugreifen.

Datenaufbewahrung von Tresor-Daten: Sie können jederzeit Tresor-Daten hinzufügen, ändern und löschen.

(ii) Verwaltungsdaten

Bitwarden erhält persönliche Informationen in Verbindung mit Ihrer Kontoerstellung, Nutzung des Bitwarden-Dienstes und Support sowie Zahlungen für den Bitwarden-Dienst, wie Namen, E-Mail-Adressen, Telefon- und andere Kontaktinformationen für Benutzer des Bitwarden-Dienstes und die Anzahl der Einträge in Ihrem Bitwarden-Dienstkonto ("Verwaltungsdaten"). Bitwarden verwendet administrative Daten, um Ihnen den Bitwarden-Service zur Verfügung zu stellen. Wir behalten administrative Daten so lange, wie Sie Kunde von Bitwarden sind und wie es das Gesetz vorschreibt. Wenn Sie Ihre Beziehung zu Bitwarden beenden, werden wir Ihre persönlichen Informationen gemäß unseren Datenhaltungsrichtlinien löschen.

Wenn Sie die Seite nutzen oder mit uns kommunizieren (z.B. über E-Mail-Adresse), werden Sie bestimmte persönliche Informationen bereitstellen und Bitwarden wird diese in einer Sammlung erfassen, wie zum Beispiel:

- Name
- Firmenname und Adresse
- Geschäftliche Telefonnummer
- E-Mail-Adresse
- IP-Adresse und andere Online-Kennungen
- Jede Kundenbewertung, die Sie uns die Erlaubnis gegeben haben zu teilen.
- Informationen, die Sie den interaktiven Bereichen der Website zur Verfügung stellen, wie ausfüllbare Formulare oder Textfelder, Schulungen, Webinare oder Veranstaltungsanmeldungen.
- Informationen über das Gerät, das Sie verwenden, einschließlich des Hardwaremodells, des Betriebssystems und der Version, eindeutiger Gerätekennungen, Netzwerkinformationen, IP-Adresse und/oder Bitwarden Service Informationen beim Interagieren mit der Site.

- Wenn Sie mit der Bitwarden Community interagieren oder an einer Schulung teilnehmen, sich für eine Prüfung oder Veranstaltung anmelden, können wir biografische Informationen und den Inhalt, den Sie teilen, in unserer Sammlung erfassen.

- Informationen, die über Cookies, Pixel-Tags, Protokolle oder ähnliche Technologien gesammelt wurden.

Bitte beziehen Sie sich auf die Bitwarden Datenschutzrichtlinien für zusätzliche Informationen.

Protokollierung, Überwachung und Alarm-Benachrichtigung

Bitwarden unterhält dokumentierte Handbücher für alle Produktionssysteme, die Bereitstellung, Aktualisierung und Fehlerbehebungsprozesse abdecken. Umfangreiche Warnungen sind eingerichtet, um zu benachrichtigen und zu eskalieren, im Falle von Problemen. Eine Kombination aus manueller und automatisierter Überwachung der Bitwarden Cloud-Infrastruktur bietet eine umfassende und detaillierte Ansicht der Systemgesundheit sowie proaktive Warnungen in Bereichen von Bedenken. Probleme werden schnell aufgedeckt, damit unser Infrastruktur-Team effektiv reagieren und Probleme mit minimaler Unterbrechung mildern kann.

Geschäftskontinuität / Katastrophenwiederherstellung

Bitwarden verwendet eine vollständige Palette von Disaster-Recovery- und Business-Continuity-Praktiken von Microsoft Azure, die in die Bitwarden Cloud integriert sind. Dies beinhaltet Hochverfügbarkeit und Backup-Dienste für unsere Anwendungs- und Datenbankebenen.

Bedrohungsprävention und Reaktion

Bitwarden führt regelmäßig Schwachstellenbewertungen durch. Wir nutzen Drittanbieter-Tools und externe Dienste, einschließlich: OWASP ZAP, Mozilla Observatory, OpenVAS und andere werden für interne Bewertungen verwendet.

Bitwarden verwendet Cloudflare, um eine WAF am Rand zu bieten, besseren DDoS-Schutz, verteilt
Verfügbarkeit und Zwischenspeicherung. Bitwarden verwendet auch Proxies innerhalb von Cloudflare für eine bessere Netzwerksicherheit und
Leistung seiner Dienstleistungen und Websites.

Bitwarden ist Open-Source-Software. All unser Quellcode ist auf GitHub gehostet und steht jedem zur freien Überprüfung zur Verfügung. Der Quellcode von Bitwarden wird von renommierten Drittanbieter-Sicherheitsprüfungsfirmen sowie unabhängigen Sicherheitsforschern geprüft. Darüber hinaus ruft das Bitwarden Schwachstellen Offenlegungsprogramm die Hilfe der Hacker-Community bei HackerOne auf, um Bitwarden sicherer zu machen.

Prüfbarkeit und Einhaltung

Das Bitwarden-Sicherheits- und Compliance-Programm basiert auf dem ISO27001-Informationssicherheits-Managementsystem (ISMS). Wir haben Richtlinien festgelegt, die unsere Sicherheitsrichtlinien und -prozesse regeln und aktualisieren unser Sicherheitsprogramm kontinuierlich, um es mit den geltenden gesetzlichen, branchenspezifischen und regulatorischen Anforderungen für die Dienstleistungen, die wir Ihnen im Rahmen unserer Nutzungsbedingungen anbieten, in Einklang zu bringen.

Bitwarden entspricht branchenüblichen Anwendungssicherheitsrichtlinien, die ein spezielles Sicherheitstechnikerteam beinhalten und regelmäßige Überprüfungen des Anwendungsquellcodes und der IT-Infrastruktur umfassen, um Sicherheitslücken zu erkennen, zu validieren und zu beheben.

Externe Sicherheitsüberprüfungen

Sicherheitsüberprüfungen und Bewertungen von Anwendungen und/oder der Plattform durch Drittanbieter werden mindestens einmal pro Jahr durchgeführt.

Zertifizierungen

Die Zertifizierungen von Bitwarden beinhalten:

- SOC2 Typ II (jährlich erneuert)

- SOC3 (jährlich erneuert)

Laut der AICPA ist die Verwendung des SOC 2 Typ II Berichts eingeschränkt. Für Anfragen zum SOC 2 Bericht, bitte kontaktieren Sie uns.

Weiterlesen: Bitwarden erreicht SOC2-Zertifizierung

Der SOC 3 Bericht bietet eine Zusammenfassung des SOC 2 Berichts, die öffentlich verteilt werden kann. Laut der AICPA ist SOC 3 der SOC für den Bericht der Dienstleistungsorganisationen über die Vertrauensdienstkriterien zur allgemeinen Verwendung.
Bitwarden macht eine Kopie unseres SOC 3 Berichts hier verfügbar.

Diese SOC-Zertifizierungen repräsentieren einen Aspekt unseres Engagements zur Sicherung der Sicherheit und Privatsphäre unserer Kunden und zur Einhaltung strenger Standards. Bitwarden führt auch regelmäßige Audits unserer Netzwerksicherheit und Code-Integrität durch.

Lesen Sie mehr: Die Sicherheitsprüfung von Bitwarden für 2020 ist abgeschlossen und Bitwarden schließt die Sicherheitsprüfung durch einen Drittanbieter ab

HTTP-Sicherheitsheader

Bitwarden nutzt HTTP-Sicherheitsheader als zusätzliche Schutzebene für die Bitwarden-Webanwendung und Kommunikation. Zum Beispiel erzwingt HTTP Strict Transport Security (HSTS) die Verwendung von TLS für alle Verbindungen, was die Risiken von Downgrade-Angriffen und Fehlkonfigurationen mindert. Content-Security-Policy-Header bieten weiteren Schutz vor Injection-Angriffen, wie zum Beispiel Cross-Site-Scripting (XSS). Darüber hinaus implementiert Bitwarden X-Frame-Optionen: SAMEORIGIN, um sich gegen Clickjacking zu verteidigen.

Überblick über Bedrohungsmodell und Angriffsflächenanalyse

Bitwarden folgt einem risikobasierten Ansatz zur Gestaltung sicherer Dienste und Systeme, der Bedrohungsmodellierung und Angriffsflächenanalyse umfasst, um Bedrohungen zu identifizieren und Maßnahmen zu deren Abwehr zu entwickeln. Die Risiko- und Bedrohungsmodellierungsanalyse erstreckt sich auf alle Bereiche der Bitwarden-Plattform, einschließlich der Kernanwendung des Bitwarden Cloud Servers und der Bitwarden-Clients wie Mobile, Desktop, Webanwendung, Browser und/oder Kommandozeilen-Schnittstellen.

Bitwarden Clients

Benutzer interagieren hauptsächlich mit Bitwarden über unsere Client-Anwendungen wie Mobile, Desktop, Webanwendung, Browser und/oder Kommandozeilen-Schnittstellen. Die Sicherheit dieser Geräte, Arbeitsstationen und Webbrowser ist entscheidend, denn wenn eines oder mehrere dieser Geräte kompromittiert werden, könnte ein Angreifer in der Lage sein, Malware wie einen Keylogger zu installieren, der alle auf diesen Geräten eingegebenen Informationen erfassen würde, einschließlich aller Ihrer Passwörter und Geheimnisse. Sie als Endbenutzer und/oder Geräte-Eigentümer sind dafür verantwortlich, sicherzustellen, dass Ihre Geräte gesichert sind und vor nicht autorisiertem Zugriff geschützt sind.

HTTPS TLS und Web Browser Crypto Ende-zu-Ende-Verschlüsselung

Der Bitwarden Web-Client läuft in Ihrem Web-Browser. Die Authentizität und Integrität des Bitwarden Web-Clients hängen von der Integrität der HTTPS TLS-Verbindung ab, über die er geliefert wird. Ein Angreifer, der in der Lage ist, den Verkehr zu manipulieren, der den Web-Client liefert, könnte dem Benutzer einen bösartigen Client liefern.

Webbrowser-Angriffe sind eine der beliebtesten Methoden für Angreifer und Cyberkriminelle, um Malware zu injizieren oder Schaden anzurichten. Angriffsvektoren auf den Web-Browser könnten beinhalten:

- Ein Element der **Social Engineering, wie Phishing,**, um das Opfer zu täuschen und zu überreden, eine Aktion zu unternehmen, die die Sicherheit ihrer Benutzergeheimnisse und ihres Kontos gefährdet.

- **Webbrowser-Angriffe und Browsererweiterungen/Add-On-Exploits:** Eine bösartige Erweiterung, die darauf ausgelegt ist, Benutzergeheimnisse abzufangen, während diese auf der Tastatur eingegeben werden.

- **Angriffe auf Webanwendungen über den Browser:** Clickjacking, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF).

Bitwarden nutzt HTTP-Sicherheitsheader als zusätzliche Schutzebene für die Bitwarden-Webanwendung und -Kommunikation.

Code-Bewertungen

Bitwarden ist ein Open-Source-Passwort-Manager. All unser Quellcode wird auf GitHub gehostet und ist öffentlich zur Überprüfung verfügbar. Der Quellcode von Bitwarden wurde und wird weiterhin jährlich von renommierten Drittanbieter-Sicherheitsprüfungsfirmen sowie unabhängigen Sicherheitsforschern geprüft. Darüber hinaus ruft das Bitwarden-Schwachstellenoffenlegungsprogramm die Hilfe der Hacker-Community bei HackerOne auf, um Bitwarden sicherer zu machen.

Lies mehr:

- Bitwarden Sicherheits-FAQs
- Bitwarden Bedrohungsprävention und Reaktion
- Bitwarden Sicherheits- und Compliance-Bewertungen, Überprüfungen, Schwachstellen-Scans, PenTesting

Schlussfolgerung

Diese Übersicht über das Bitwarden-Sicherheits- und Compliance-Programm wird Ihnen zur Überprüfung angeboten. Die Lösung, Software, Infrastruktur und Sicherheitsprozesse von Bitwarden wurden von Grund auf mit einem mehrschichtigen, verteidigungstiefen Ansatz konzipiert.

Das Bitwarden-Sicherheits- und Compliance-Programm basiert auf dem ISO27001 Informationssicherheits-Managementsystem (ISMS). Wir haben Richtlinien festgelegt, die unsere Sicherheitsrichtlinien und -prozesse regeln und aktualisieren unser Sicherheitsprogramm kontinuierlich, um es mit den geltenden gesetzlichen, branchenspezifischen und regulatorischen Anforderungen für die Dienstleistungen, die wir Ihnen im Rahmen unseres Dienstleistungsvertrags anbieten, in Einklang zu bringen.

Wenn Sie Fragen haben, bitte kontaktieren Sie uns.