WEIHRICH
INFORMATIK

Passwörter zentral, sicher und einfach aufbewahren

In der immer weiter digitalisierten Welt verfügt jede Person über eine immer grösser werdende Zahl an Benutzerkonten: Zugangsdaten mit Benutzernamen und Passwort für den Arbeitsplatz, den privaten PC, das eBanking, den Internet-Shop oder die Vereinshomepage. Häufig nutzen Anwenderinnen und Anwender für diese Benutzerkonten identische Zugangsdaten. Diese Tatsache führt unweigerlich dazu, dass einem Angreifer bei der Offenlegung nur eines Benutzerkontos praktisch alle Türen offenstehen. Auch werden Passwörter immer noch häufig in einfachen Word- oder Excel-Dateien oder als Outlook-Notizen unverschlüsselt abgelegt. Bei Ferienvertretungen, oder wenn andere Personen dieselben Zugangsdaten verwenden, werden diese sensiblen Informationen als Kopie weitergegeben.

Diese unbefriedigende Situation kann grundsätzlich dadurch wesentlich verbessert werden, wenn für jedes Benutzerkonto ein individuelles Passwort festgelegt wird. Jedoch ist dies oft nur schwer möglich, da bei der Vielzahl an Benutzerkonten ohne technische Hilfsmittel leicht der Überblick verloren geht. Mit einem modernen Passwortmanager kann mittels des integrierten Passwortgenerators zudem sichergestellt werden, dass die verwendeten Passwörter heutigen Anforderungen entsprechen und einzigartig sind.

Weihrich Informatik bietet Ihnen zur modernen Passwortverwaltung zwei Optionen an. Das «Password Depot» eignet sich am besten für Geschäftsumgebungen, bei denen ein lokales Active Directory zur Verfügung steht und die Nutzer sich zentral über das Active Directory anmelden. Ebenso eignet sich das «Password Depot» hervorragend für Remote Desktop Umgebungen (RDP) und für die Regelung der Zugriffsmöglichkeiten über Sicherheitsgruppen. Alle Informationen sind zentral und verschlüsselt abgelegt, der Zugriff und Veränderungen werden protokolliert und der Zugang kann jederzeit und sehr individuell angepasst werden.

Für Unternehmen und Privatpersonen, welche nicht über eine zentrale Serverinfrastruktur verfügen, oder weit verteilt in Homeoffice Umgebungen arbeiten, eignet sich die cloudbasierte Lösung «Bitwarden» am besten. Der Zugriff auf die Passwörter ist weltweit von allen Geräten sowie webbasiert möglich.

Beide Lösungen garantieren eine sichere Verwaltung Ihrer Passwörter. Ihre Passwörter befinden sich niemals unverschlüsselt auf einem Server, die Entschlüsselung Ihrer Passwörter erfolgt immer lokal auf Ihrem Gerät.

	Password Depot	**Bitwarden (Teams)**
Datenhaltung	On-Prem Server	Cloud
Zugriff	Lokal (inkl. RDS)	weltweit
Verschlüsselung	AES-256 Bit	AES-256 Bit/Web
AD-Integration	✓	o
2-FA	✓	✓ (inkl. DUO)
Benutzergruppen	✓	✓
Teilen im Team	✓	✓
2-FA im PW Manager	✓	✓
Benutzerdefinierte Rollen	✓	x
Mobiler App Zugriff	eingeschränkt	✓
Zeitlich beschr. Zugriff	✓	x

WEIHRICH
INFORMATIK

Password Depot Enterprise - die Funktionen in der Übersicht

Funktion	Beschreibung
Gemeinsame Team-Datenbanken	Nutzen Sie die Datenbanken gemeinsam mit den berechtigten Team-Mitgliedern.
Abteilungen und Gruppen	Unterteilen Sie Ihre Benutzer übersichtlich in Abteilungen und Gruppen.
Detailliertes Rechtemanagement	Weisen Sie Zugriffsrechte auf Datenbanken, Ordnern in den Datenbanken oder einzelne Einträge zu.
Höchste Sicherheit	Client/Server-Kommunikation mit ephemeren Schlüsseln und Perfect Forward Secrecy (PFS).
Verschlüsselte Verbindung (AES 256 Bit)	Der Datenaustausch zwischen dem Enterprise Server und den Clients ist immer mit AES 256 Bit verschlüsselt.
Active Directory	Verknüpfen Sie den Enterprise Server optional mit Ihrer bestehenden Active Directory-Struktur.
Azure Active Directory	Verknüpfen Sie den Enterprise Server optional mit Ihrer bestehenden Azure Active Directory-Struktur.
Hochverfügbarkeit	Serverspiegelung für die Hochverfügbarkeit des Servers, für das unterbrechnungsfreie Arbeiten bei Serverausfällen.
Zwei-Faktor-Authentisierung (2FA)	Anmeldung der Clients oder des Server-Managers am Server optional über 2FA (TOTP oder E-Mail).
Datensatz-Historie	Protokollieren Sie die Änderung eines einzelnen Datensatzes.
Rollenbasierter Zugriff	Weisen Sie Administratoren einen rollenbasierten Zugriff auf den Server-Manager zu.
REST Api	Greifen Sie auf den Enterprise Server aus Ihren eigenen Anwendungen heraus zu.
Benachrichtigungssystem	Lassen Sie sich über Ereignisse, wie z. B. den Zugriff auf einen Eintrag, informieren.
Zertifikate und SSL/TLS-Verbindung	Installieren Sie optional Zertifikate und verwenden Sie eine SSL/TLS-Verbindung.
Zugriff auf Server-Manager	Greifen Sie auf den Server-Manager von lokal oder remote über TCP/IP zu.
Terminalserver	Nahtlose, sessionbasierte Zusammenarbeit mit Terminalservern.
Mobile Geräte	Greifen Sie neben der PC- und Mac-Edition auch mit nativen Apps für iOS und Android auf den Server zu.
Web-Interface	Greifen Sie auf Ihren Server über das Web-Interface zu. Das Web-Interface erhalten Sie im Quelltext.
Single Sign-On (SSO)	Optionale Unterstützung der integrierten Windows-Authentifizierung (Single Sign-On) für Active Directory-Benutzer.
Passwort-Richtlinien	Definieren Sie unternehmensweite Passwortrichtlinien.
Lokale Richtlinien	Legen Sie lokale Richtlinien für Ihre Clients fest, wie z. B. die verfügbaren Speicherorte (Cloud, Lokal etc.) und andere lokale Einstellungen und Optionen.
Zugriff zeitlich begrenzen	Legen Sie den Zeitrahmen fest, für den ein Benutzer Zugriff gewährt bekommt.
Kennwörter verbergen	Optional können Sie Einträge so schützen, dass Benutzer sie verwenden, jedoch nicht sehen können.
Daten optional offline nutzen	Erlauben Sie es den Benutzern optional, die Datenbanken auch im Offline-Modus zu verwenden.
Siegel-Funktionalität	Versiegeln Sie optional Einträge, um Benutzern Zugriff auf einen Eintrag zu gewähren. Greift der Benutzer im Bedarfsfall auf den Eintrag zu, so bricht er das Siegel und Sie werden darüber informiert, dass er den Eintrag genutzt hat.
Teilen von Daten durch Benutzer	Erlauben Sie optional Ihren Benutzern direkt über den Client (ohne Zugriff auf den Server Manager), ihre Daten mit anderen Benutzern zu teilen und optional zu versiegeln.
Automatische Backups	Erzeugen Sie automatische Backups auf beliebigen Speicherorten.
Reporting	Detailliertes Reporting über wichtige Ereignisse.
Logs im RFC 5424-Format	Alle Aktivitäten des Servers und der Benutzer werden protokolliert und können optional per UDP an externe Protokollserver zur revisionssicheren Verarbeitung und Speicherung gesendet werden.
Datenimport und -export	Importieren oder exportieren Sie Ihre Datenbanken über den Client.
Effektive Berechtigungen	Lassen Sie sich die effektiven Berechtigungen der Benutzer für einzelne Ordner oder Einträge anzeigen.
Datenbank-Assistenten	Automatische Erzeugung neuer Datenbanken oder Zuweisung bestehender zu Benutzern und Gruppen.

Bitwarden - die Funktionen in der Übersicht

	Teams	Enterprise
Zentrale Funktionen von Bitwarden	✓	✓
Premium-Funktionen für Benutzer	✓	✓
Unbegrenzt viele Benutzer	✓	✓
Unbegrenztes Teilen durch Sammlungen	✓	✓
API-Zugang	✓	✓
Ereignis- und Prüfungsprotokolle	✓	✓
Organization Two-Step Login via Duo	✓	✓
Benutzergruppen	✓	✓
Directory Connector	✓	✓
SCIM-Unterstützung	-	✓
Benutzerdefinierte Rollen	-	✓
Richtlinien für Unternehmen	-	✓
SSO-Integration↗	-	✓
Kostenloser Familien-Tarif für alle Nutzer	-	✓
Passwortwiederherstellung durch Administrator	-	✓
Option, Bitwarden selbst zu hosten	-	✓

https://www.password-depot.de/ / https://bitwarden.com