White Paper: Sichere Verwaltung von Kennwörtern in Unternehmen mit dem Password Depot Enterprise Server

Einleitung: Vielen Unternehmen fehlt oft ein geeigneter Ort, an dem sie Kennwörter und ähnliche sensible Daten wie Software-Lizenzschlüssel, Kreditkartennummern, PIN- und TAN-Nummern, geheime Notizen usw. sicher speichern können. Mitarbeiter erhalten Kennwörter über unsichere Methoden, beispielsweise erfolgt die Übermittlung per E-Mail, Messenger oder auf Papierzetteln. Daten auf diesem Wege zu aktualisieren und zu verwalten, ist in der Regel sehr aufwendig.

Zweck des Password Depot Enterprise Servers

Password Depot Enterprise Server ermöglicht Teams und Gruppen, ihre Datenbanken zentral zu speichern und zu verwalten. Alle Benutzer greifen auf gemeinsame Datenquellen zu. Dabei können alle dazu autorisierten Clients diese Datenquellen gleichzeitig bearbeiten und ändern.

Damit ist das Problem der manuellen Aktualisierung und Verwaltung von Kennwörtern und Dokumenten an verschiedenen Arbeitsplätzen gelöst.

Durch die zentrale Verwaltung der Einträge müssen einzelne Kennwörter oder Dokumente nicht mehr manuell an einzelne autorisierte Teammitglieder gesendet werden, was eine wichtige Sicherheitslücke schließt.

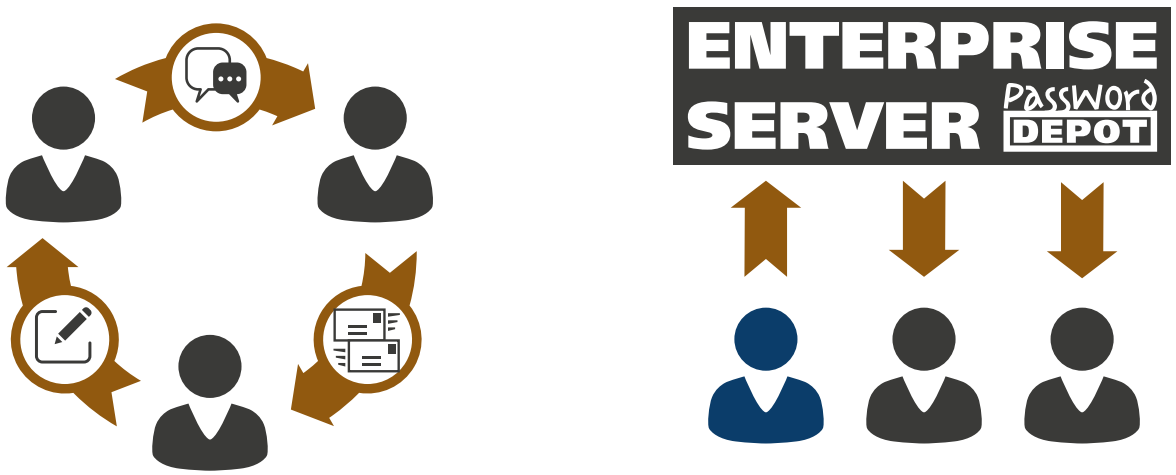

Abbildung 1: In vielen Unternehmen werden Kennwörter nach wie vor per E-Mail oder Messenger ausgetauscht oder auf Zetteln weitergegeben. Mit Password Depot können Kennwörter zentral verwaltet und sicher ausgetauscht werden.

Technischer Hintergrund

Password Depot Enterprise Server läuft als Windows NT-Dienst und ermöglicht die zentrale Speicherung und Verwaltung zahlreicher Datenbanken. Mehrere Benutzer können dabei von verschiedenen PCs und Mobilgeräten gleichzeitig auf Datenbanken zugreifen, indem sie die Passwort Depot Client-Software verwenden.

Der Server verwendet keine externen Server-Datenbanken, sondern speichert alle eigenen Datenbanken

sowie eigenen Daten zur Konfiguration **ausschließlich lokal und hochverschlüsselt (sogenannte On-Premises-Lösung)**. Die Clients kommunizieren mit dem Server mittels TCP/IP-Protokoll (IPv4/IPv6). Sobald sich ein Client mit dem Server verbindet, wird mittels **ECDH-Protokolls** (Elliptic Curve Diffie-Hellmann) ein sicherer Kanal hergestellt. Anhand des AES-256-Bit-PBKDF-Algorithmus werden alle übertragenen Daten mit einem zeitlimitierten Sitzungsschlüssel verschlüsselt. Somit wird die Methode **Perfect Forward Secrecy** unterstützt.

In öffentlichen Netzwerken können optional auch ein **SSL-Zertifikat** auf dem Server installiert und anschließend SSL/TLS-Protokolle aktiviert werden. Zudem kann der Server-Administrator am Server festlegen, von welcher IP-Adresse sich ein Benutzer anmelden darf, wie oft ein Benutzer ein falsches Kennwort eintippen darf, bevor das Konto gesperrt wird; und er kann für Benutzer festlegen, bis zu welchem Datum sie Zugriff auf eine Datenbank haben.

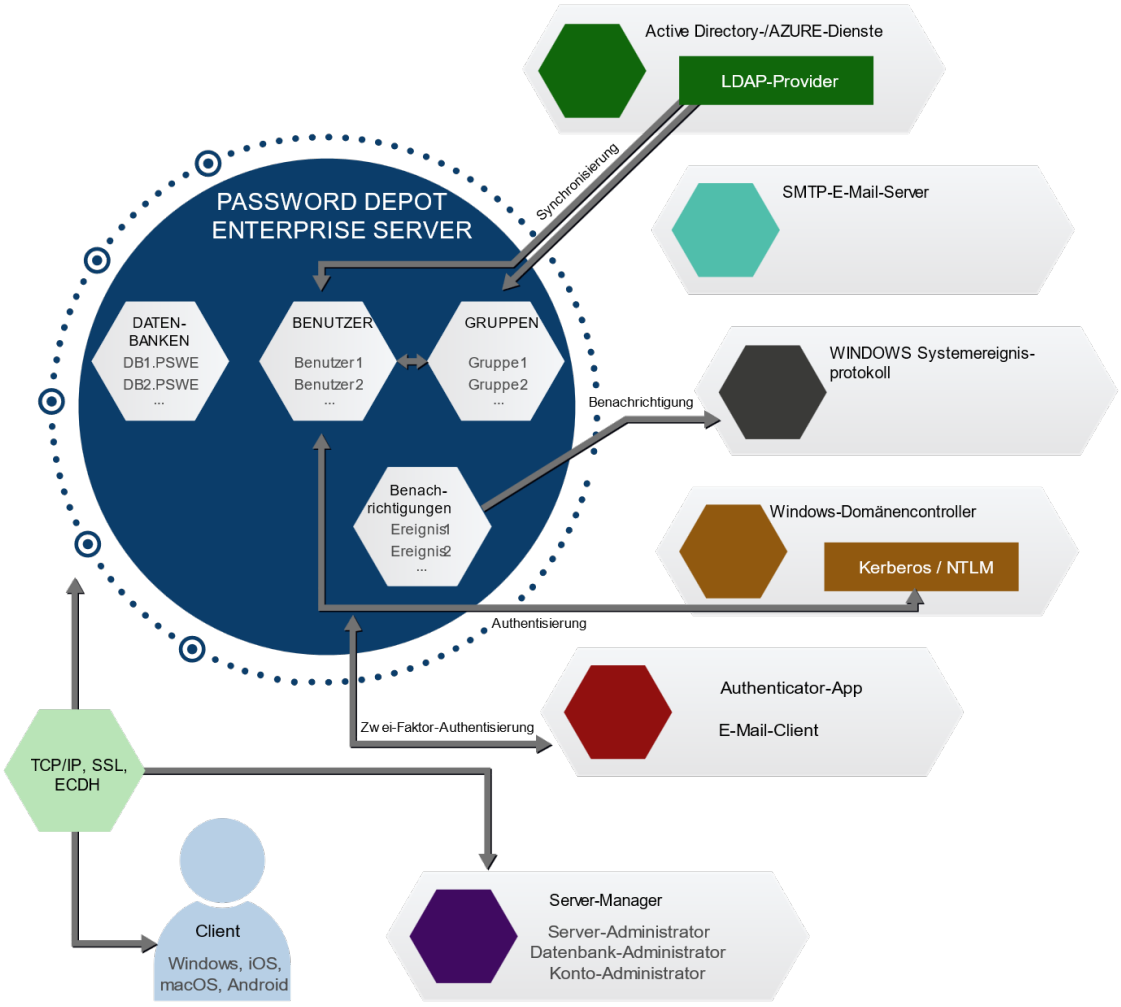

Abbildung 2: Aufbau des Password Depot Enterprise Servers.

Der Password Depot Enterprise Server verwaltet folgende Objektsammlungen: Datenbanken, Benutzer, Gruppen und Benachrichtigungen.

Datenbanken

Jede Datenbank stellt eine PSWE-Datei dar, die alle darin gespeicherten Kennworteinträge beinhaltet. Zusätzlich stehen Ihnen weitere Eintragstypen wie TeamViewer, Remote-Desktopverbindung, Banking, Identität etc. zur Verfügung und es besteht auch die Möglichkeit, Ihrer Datenbank Dokumente hinzuzufügen. Die PSWE-Datenbanken werden mit dem Administrator-Kennwort verschlüsselt und lokal auf dem Server gespeichert. Die Metadaten einer Datenbank definieren dabei die Zugriffsrechte von Benutzern und Gruppen auf die gesamte Datenbank und/oder auf einzelne Kennworteinträge oder Ordner innerhalb einer Datenbank.

Benutzer

Die Benutzer-Sammlung enthält eine Liste der registrierten Clients, Informationen zu deren Eigenschaften sowie Informationen zu deren Authentifizierung. Mit dem Server können für jeden einzelnen Benutzer individuelle Datenbanken angelegt werden, die mit dem speziell für den Benutzer bereitgestellten Master-Kennwort verschlüsselt sind. Diese individuellen Datenbanken enthalten dann auch nur die Einträge, zu deren Verwendung der entsprechende Benutzer berechtigt ist.

Gruppen

Gruppenobjekte dienen dazu, die gleichzeitige Verwaltung mehrerer Benutzer zu vereinfachen: Jeder Benutzer kann entweder Mitglied einer oder auch mehrerer Gruppen sein. Gruppenobjekte können manuell erstellt und geändert oder aus Active Directory importiert und mit dem Enterprise Server automatisch synchronisiert werden.

Benachrichtigungen

Der Password Depot Enterprise Server führt detailliertes Protokoll über aller Benutzeraktionen und Ereignisse, die auf dem Server stattfinden. Zusätzlich ist es möglich, selbst Ereignisse zu definieren, bei denen der Enterprise Server eine Benachrichtigung per E-Mail an den Administrator sendet und einen Eintrag in das Systemereignisprotokoll einfügt. Dazu zählen beispielsweise Versuche, sich mit einem falschen Kennwort anzumelden, der Zugriff auf besonders wichtige Datenbanken oder Kennworteinträge oder das gleichzeitige Löschen mehrerer Einträge etc.

Benutzer-Authentifizierung

Der Enterprise Server speichert keine Kennwörter der Clients und unterstützt die Benutzer-Authentifizierung wie folgt:

- **Standard** (mit Benutzername und Kennwort): Der Server verifiziert Benutzername und Kennwort, indem er Hashwerte speichert.

- **Integrierte Windows-Authentifizierung:** Diese Funktion ermöglicht die Organisation der Single-Sign-On-Methode, wenn authentifizierte Windows-Benutzer nahtlos vom Client aus auf den Server zugreifen sollen.

- **Azure Active Directory.** Benutzer werden über die Anmeldung bei Azure AD mit ihren Anmeldeinformationen und optional anderen Methoden wie Smartcards authentifiziert.

Zusätzlich unterstützt der Enterprise Server die 2-Faktor-Authentifizierung folgendermaßen:

- **TOTP** – Das Time-based One-Time Password-Verfahren in Zusammenarbeit mit einer Vielzahl von Authentifizierungs-Apps wie die Microsoft Authenticator App, Google Authenticator, Authy etc.
- **E-Mail** – Der Server sendet ein zeitlimitiertes Einmalkennwort an die E-Mail-Adresse des Clients.

Server-Verwaltung

Das Softwarepaket beinhaltet für die Serveradministration ein spezielles Tool, und zwar den Server-Manager. Der Zugriff auf diesen kann in insgesamt fünf verschiedenen Kategorien erfolgen:

- **Super-Administrator:** Das Hauptkonto für die Serververwaltung und Rechtevergabe. Nach der ersten Installation wird ihm der Benutzername *admin* und das Kennwort *admin* zugeordnet. Aus Sicherheitsgründen müssen diese Standard-Zugangsdaten so schnell wie möglich geändert werden.
- **Server-Administrator:** Ein Server-Administrator hat die gleichen Rechte wie der Super-Administrator. Er besitzt Vollzugriff auf den Enterprise Server und den Server-Manager, kann auf alle Datenbanken, Benutzer, Gruppen, Benachrichtigungen und das Protokoll zugreifen und zusätzlich auch den Server verwalten und konfigurieren.
- **Datenbank-Administrator:** Dieser kann auf dem Server neue Datenbanken erstellen und anderen Benutzern auf solche Datenbanken den Zugriff gewähren oder entziehen. Er kann ebenso die Rechteverwaltung für solche Datenbanken vornehmen. Ein Datenbank-Administrator kann nicht auf andere Serverbereiche, wie beispielsweise Benutzer oder Gruppen, zugreifen oder das Serverprotokoll lesen bzw. den Server konfigurieren.
- **Konto-Administrator:** Dieser kann Benutzer und Gruppen auf dem Server verwalten und in diesem Zusammenhang beispielsweise dem Server auch neue Benutzer und Gruppen hinzufügen oder solche löschen.
- **Active-Directory-Verwalter:** Diese Server-Rolle ermöglicht Benutzern, Vorgänge bezüglich der AD-Synchronisation durchzuführen.
- **Ereignisprotokoll-Leser:** Benutzer haben Zugriff auf die Protokolle des Servers.

Über den Server-Manager können obige Benutzer in Ihren jeweiligen Rollen den Server verwalten und verschiedene Aufgaben ausführen, darunter:

- Installieren und Entfernen von Datenbanken auf dem Server.
- Hinzufügen und Ändern von Benutzern und Gruppen.
- Vergabe von Zugriffsrechten auf Datenbanken (und optional auch auf einzelne Einträge und Ordner) an definierte Benutzer oder Gruppen.
- Definieren von allgemeinen und dateibasierten Sicherheitsrichtlinien (Regeln zur Komplexität der Kennwörter, Rechte zum Drucken, Exportieren, Speichern einer Kopie usw.).
- Erstellen und Verwalten von Warnungen zu bestimmten Ereignissen.
- Generieren verschiedener Berichte (Datenbank-Bericht/Benutzerbericht).
- Anzeigen und Exportieren von Serverprotokollen.
- Active Directory-Synchronisation

- Azure-Synchronisation

Active Directory-Integration

Password Depot Enterprise Server vereinfacht die Benutzerverwaltung, indem Benutzerkonten und -gruppen aus dem Active Directory einer Windows NT-Domäne importiert werden können. Benutzer, die aus Active Directory importiert wurden, können dann über ihre Windows-Domänenkonten und -Kennwörter auf den Server zugreifen. Die Synchronisation dieser Benutzer und Clients zwischen dem Server und Active Directory kann manuell oder automatisch nach einem festgelegten Zeitplan erfolgen.

Azure Active Directory-Integration

Wie bei einem lokalen Active Directory können mit Password Depot Enterprise Server Benutzer und Gruppen aus einem oder mehreren Azure-Verzeichnissen importiert und synchronisiert werden. Diese importierten Benutzer können dann auf dem Server über die Anmeldung am Azure AD in einem integrierten Browserfenster authentifiziert werden.

Lizenzierung

Bei Password Depot werden Enterprise Server und Clients als Paket lizenziert und zusammen verkauft. Die erworbenen Lizenzen sind Named Licences, die immer nur von einem Benutzer, jedoch auf beliebig vielen Computern und Betriebssystemen installiert und verwendet werden dürfen. Darüber hinaus kann eine Lizenz in allen verfügbaren lokalisierten Sprachen genutzt werden. Dies gilt auch bei Verwendung eines Terminalservers.

Für die Lizenzierung muss in einem ersten Schritt die Anzahl der Benutzer definiert werden, die der Administrator am Server anlegen möchte. Auf dem Enterprise Server selbst kann immer nur maximal die Anzahl an Benutzern eingerichtet werden, die auch lizenziert wurden.

Reicht das Anlegen von bis zu maximal drei Benutzern aus, so kann der Server kostenlos heruntergeladen und genutzt werden.

Wenn am Enterprise Server mehr als drei Benutzer angelegt werden müssen, ist es notwendig, eine Serverlizenz zu erwerben. Diese ist ab fünf Benutzern zu Staffelpreisen bis zu einer unbegrenzten Anzahl von Benutzern erhältlich.

Softwarewartung und Verlängerung

Mit dem Kauf einer Lizenz können Sie optional auch eine ein-, zwei- oder dreijährige Softwarewartung bei Kauf erwerben. Diese wird automatisch um ein weiteres Jahr verlängert, sofern Sie der Verlängerung nicht widersprechen. Sie werden 60 Tage vor der Verlängerung per E-Mail über die anstehende Verlängerung informiert.

Updates und Upgrades erhalten Sie, sofern Sie eine gültige Softwarewartung besitzen.

Wenn Sie Ihre Softwarewartung nicht verlängert haben, so können Sie keine weiteren Updates und Upgrades mehr beziehen. Ihre vorliegende Version können Sie jedoch weiterhin zeitlich unbegrenzt nutzen. Sie können anschließend zu einem beliebigen späteren Zeitpunkt ein Upgrade Ihrer Lizenzen erwerben oder Ihre Softwarewartung rückwirkend verlängern.

Client-Modul

AceBIT entwickelt und pflegt die entsprechende Client-Software für den Zugriff auf den Password Depot Enterprise Server für alle wichtigen Betriebssysteme - MS Windows, Mac OS X, iOS und Android. Auch ein Web-Client ist inzwischen verfügbar.

Corporate Edition

Die Corporate Edition des Clients ist eine angepasste Edition des Standard-Clients, die es ermöglicht, nicht nur allgemeine Richtlinien für Datenbanken auf dem Server, sondern für alle Datenbanken und sogar für das gesamte Programmumfeld festzulegen. Hierzu zählen beispielsweise, dass der Server-Administrator die Programmoptionen des Clients weitgehend definieren, das Speichern auf Cloud-Diensten aktivieren oder deaktivieren, das Drucken und Exportieren verwalten kann usw.

DS-GVO und Datenschutz

Bei Password Depot und Password Depot Enterprise Server handelt es sich um eine sichere und datenschutzfreundliche **sogenannte On-Premises oder On-Prem Funktionsweise – Made in Germany**. Das heißt: Nach Bearbeitung Ihres Auftrags und dem Download Ihrer Kopie(n) gibt es unsererseits keinerlei Beeinflussung oder Abschöpfung Ihrer Daten bzw. keinen Zugriff auf Ihre Daten. Diese sind standardmäßig **bei Ihnen selbst lokal gespeichert** – und nicht bei uns oder auf einer Cloud einer Drittpartei, die womöglich darüber hinaus noch in einem anderen Land unter anderer Rechtsprechung ansässig sein könnte.

Anders ausgedrückt: Unser Verständnis ist, dass wir als AceBIT GmbH bei der Bestellung und Bereitstellung von Password Depot – bei Vertragsschluss – „Verantwortliche“ im Sinne der DS-GVO sind, gemäß Art. 4 Nr. 7.

Fazit

Password Depot Enterprise Server unterstützt Unternehmen bei der Verwaltung von Kennwörtern im gesamten Unternehmen und erhöht dadurch die Sicherheit und Produktivität erheblich. Die Aktualisierung der Kennwörter erfolgt auf dem Server, sodass alle autorisierten Teammitglieder ohne manuelle Benachrichtigung darauf zugreifen können.