----------**Projektantrag**----------

Ausgangssituation

Bei der Firma XYZ wird zurzeit der Passwort-Tresor KeePass für die Verwaltung und Speicherung firmeninterner Passwörter eingesetzt. Diese Lösung ist zwar weit verbreitet, erfüllt jedoch nicht mehr die aktuellen Sicherheits- und Unternehmensanforderungen. Insbesondere fehlen zentrale Verwaltungsfunktionen, eine klare rollenbasierte Rechtevergabe sowie eine benutzerfreundliche Oberfläche, die den Umgang mit Passwörtern erleichtert. In der Praxis führt dies dazu, dass Mitarbeiter Passwörter weiterhin unsicher speichern oder weitergeben, beispielsweise auf Papier, in Word-Dokumenten oder sogar über Kommunikationsplattformen wie Microsoft Teams. Dieses Vorgehen stellt ein erhebliches Sicherheitsrisiko dar, da unverschlüsselt abgelegte Zugangsdaten leicht kompromittiert werden können und damit nicht nur die IT-Sicherheit, sondern auch die Einhaltung von unternehmensinternen Richtlinien und gesetzlichen Vorgaben gefährdet ist.

Projektziel

Das Ziel dieses Projekts ist die Einrichtung einer Testinstanz eines zentralen Passwort-Tresors auf einem internen Server. Mit dieser Lösung soll erreicht werden, dass Passwörter verschlüsselt gespeichert werden, dass Benutzer und Administratoren über ein rollenbasiertes Rechtesystem verwaltet werden können und dass die Bedienung so benutzerfreundlich gestaltet ist, dass eine breite Akzeptanz bei den Mitarbeitern entsteht. Im Rahmen der Umsetzung werden rund zehn Benutzer aus der bestehenden KeePass-Lösung in das neue System migriert. Dabei werden die vorhandenen Passwörter übernommen, sodass die Testbenutzer ihre Arbeitsweise unmittelbar erproben können. Die Testinstanz wird dabei parallel zur bestehenden KeePass-Umgebung betrieben, um den laufenden Betrieb nicht zu unterbrechen. Ein endgültiger Umstieg auf die neue Plattform erfolgt erst zu einem späteren Zeitpunkt in einem separaten Projekt, sobald die Testphase erfolgreich abgeschlossen wurde und alle Anforderungen erfüllt sind. Der Projekterfolg lässt sich daran messen, dass die eingerichtete Testinstanz funktionsfähig in Betrieb genommen wird, dass sich alle zehn vorgesehenen Benutzer erfolgreich anmelden können, ihre Passwörter in der neuen Plattform nutzen und verwalten, und dass Einladungs- und Benachrichtigungs-E-Mails zuverlässig verschickt werden.

Umfeldbedingungen

Das Projekt wird als internes Teilprojekt bei der Firma XYZ durchgeführt. Die benötigten Serverressourcen sowie die Testbenutzer werden durch die interne IT-Abteilung bereitgestellt. Konkret wird hierfür ein virtueller Server auf Basis der bestehenden vSphere-Umgebung eingerichtet. Der Passwort-Tresor benötigt eine Datenbank, beispielsweise auf Basis von MariaDB, in der die Passwörter verschlüsselt gespeichert werden, sowie einen Webserver wie nginx, der den Benutzern den Zugriff über eine

Weboberfläche ermöglicht. Für die Zustellung von Einladungen und Benachrichtigungen ist ein SMTP-Server erforderlich, der in die Lösung integriert wird. Zusätzlich ist eine funktionierende Zeit-Synchronisation über NTP notwendig. Ebenso werden SSL/TLS-Zertifikate zur Absicherung der Kommunikation über HTTPS benötigt. Schließlich

spielen Sicherheitsaspekte wie die Konfiguration einer Firewall und die Absicherung der Datenbank eine wichtige Rolle, um den Schutz der Testinstanz zu gewährleisten und ein realistisches Abbild der späteren Produktivumgebung zu schaffen. Nicht Bestandteil des Projekts sind hingegen eine langfristige Betreuung, die Wartung der Lösung im laufenden Betrieb sowie die Implementierung einer Backup-Strategie. Diese Themen werden erst in einem nachgelagerten, produktiven Projekt betrachtet.

Projektphasen / Zeitplanung

Informationen: 10 Stunden
- Anforderungen prüfen (System, Software, Sicherheit und Verfügbarkeit)
- Nach geeigneter Software suchen
- Angebote einholen
- Entscheidungsmatrix erstellen
- Entscheidungsmatrix präsentieren & Auswahl treffen

Planung: 6 Stunden
- Handbuch der gewählten Software lesen
- Abhängigkeiten recherchieren
- Sicherheitsrisiken ermitteln
- Machbarkeit der Software-Implementierung prüfen
- Datenspeicherort planen
- Zeitplan für die Durchführung erstellen

Durchführung: 13 Stunden
- Datenspeicherort festlegen
- Server bereitstellen
- Abhängigkeiten installieren
- Software installieren
- Benutzer (ca. 10) anlegen
- Rechte vergeben
- Bestehende Passwörter migrieren

Kontrolle: 11 Stunden
- Funktionstest & Sicherheitstest durchführen
- Praxistest mit mehreren Usern
- Feedback einholen & analysieren
- Anpassungen auf Basis des Feedbacks durchführen
- Projektdokumentation erstellen

40 / 40 Stunden