

Leistungsbeschreibung ITSR ManagedPass

Vorbemerkung

Unterschieden zwischen den verschiedenen Paketen (Basis, Standard und Premium) sind explizit deklariert. Alle anderen Punkte gelten für alle drei Pakete. Es wird nach Anzahl der Nutzer, welche im vergangenen Monat ein Konto aufwiesen, abgerechnet. Die Mindest-Vertragslaufzeit beläuft sich auf 12 Monate. Sollte nicht innerhalb der Kündigungsfrist von 3 Monaten zum Vertragsablaufdatum gekündigt werden, verlängert sich der Vertrag automatisch um 12 Monate.

Voraussetzungen

Um eine reibungslose und zuverlässige Betreuung dieses Konzeptes gewährleisten zu können, setzen wir Folgendes beim Kunden voraus:

1. Der administrative Zugriff auf den Domäne Controller des Kunden muss gewährleistet sein.
2. Ein Kennwort-Konzept, welches Ablagestruktur, Berechtigungsstruktur sowie eine Benutzerliste bestehend aus Vorname, Nachname und E-Mail Adresse, beinhaltet.

1. Rechenzentrumsbasierte Datenhaltung und -verarbeitung

Der zentrale Kennwortspeicher wird in einem Rechenzentrum in der Bundesrepublik Deutschland bereitgestellt. Daten werden via „https“ übermittelt. Die Infrastruktur, Lizenzen und Betriebskosten, welche für die Bereitstellung erforderlich sind, sind enthalten.

Auf den Kennwortspeicher kann über eine browserbasierte Web-Oberfläche, über eine Mobile App (Für Android ab Version 5.0, für iOS ab Version 13.0) oder ein Browser-Plugin (Verfügbar für Mozilla Firefox, Google Chrome und Microsoft Edge) zugegriffen werden.

2. Verschlüsselung

Für die Verschlüsselung der im Kennwortsafe gespeicherten Kennwörter wird zusätzlich ein Unternehmensschlüssel erzeugt, mit dem die im Kennwortspeicher gesicherten Kennwörter codiert werden. Gesicherte Kennwörter können nur mit Hilfe des Unternehmensschlüssels ausgelesen und entschlüsselt werden. Ausgenommen davon sind Kennwörter, die der Auftragnehmer für administrative Konten erhält, welche für die Erfüllung der Managed Services und Wartungsverträge benötigt werden.

3. Web-Zugriff auf einen zentralen Kennwortspeicher für Unternehmenskennwörter

Der Kennwortspeicher ermöglicht das Hinterlegen von Unternehmenskennwörtern. Diese werden von einem vom Kunden zu benennenden Nutzer zentral verwaltet und können von allen Nutzern des Unternehmens eingesehen werden.

4. Web-Zugriff auf einen zentralen Kennwortspeicher für die persönlichen Kennwörter der Mitarbeiter

Der Kennwortspeicher ermöglicht das Hinterlegen von persönlichen Kennwörtern. Dies sind Kennwörter, die von dem Nutzer selbst hinterlegt, verwaltet und nur von ihm eingesehen werden können.

5. Bereitstellung einer 2-Faktor-Authentifizierung (2FA/MFA)

Der Auftragnehmer stellt dem Kunden eine 2FA-Methode zur Anmeldung an dem Kennwortspeicher zur Verfügung. Dem Nutzer wird bei der ersten Anmeldung die Möglichkeit gegeben, zwischen den Optionen E-Mail, SMS oder einer mobilen Authentifizierungsapp für das Smartphone zu wählen.

Bei jedem Anmeldeprozess an dem Kennwortspeicher muss der Nutzer neben seinem Benutzernamen und Kennwort zusätzlich eine zeitlich limitierte Zahlenkombination eingeben. Die Übermittlung dieser erfolgt über E-Mail, SMS oder Authentifizierungsapp.

6. Zurücksetzen des Zugangs zum Kennwortspeicher

Sollte einem Nutzer das Anmelden am Kennwortspeicher nicht mehr möglich sein, so muss dieser den Auftragnehmer kontaktieren. Der Auftragnehmer kann auf Anfrage ein neues Kennwort bereitstellen, bzw. etwaige Anmeldeprobleme lösen.

7. Protokollierung der Zugriffsnutzung von Benutzerkennwörtern

Der Auftragnehmer protokolliert die Berechtigungen der Nutzer sowie die Zugriffe auf Unternehmenskennwörter. Die Aufbewahrung dieser Protokolle erfolgt über einen Zeitraum von 180 Tagen.

Der Kunde kann den Auftragnehmer mit der Bereitstellung eines Berichts für einen Nutzer beauftragen.

Inhalte:

- Änderungen an Kennworteinträgen (Titel des Eintrags, Nutzer, Datum und Uhrzeit der Änderung)
- Zugriffe auf den Kennwortspeicher und auf die jeweiligen Unternehmenspasswörter durch den Nutzer (Titel des Eintrags, Nutzer, Datum und Uhrzeit der Änderung)
- Zugriffsberechtigungen der Nutzer (Nutzer, Titel des Eintrags)

Bei Überschreitung von mehr als einem Bericht pro Benutzer pro Jahr erfolgt eine Abrechnung von 25 EUR pro weiteren Bericht.

8. Durchführung einer Datensicherung der Unternehmenskennwörter

Um bei versehentlich gelöschten Unternehmenskennwörtern eine Wiederherstellung von einzelnen oder allen Kennwörtern durchführen zu können wird alle sieben Tage eine Datensicherung der Unternehmenskennwörter und der administrativen Zugangsdaten als verschlüsselte ZIP-Datei auf einen vom Kunden zu benennenden Windows-Server durchgeführt. Die persönlichen Kennwörter der Nutzer werden nicht gesichert.

9. Durchführung der Kennwortänderungen für Admin-Konten

Administrative Zugangsdaten, wie bspw. Ein Domänen-Administratorkonto, sind durch ihre Privilegien besonders sensibel. Entsprechend der Rotations-Zyklen (Standard-Paket: alle 90 Tage; Premium-Paket: alle 30-Tage) werden die Kennwörter der vom Auftragnehmer verwalteten administrativen Kennwörter im Kundennetzwerk des Verzeichnisdienstes (Active Directory, AzureAD) regelmäßig geändert. Das aktualisierte Kennwort wird im Unternehmenskennwortspeicher gespeichert.

10. Bereitstellung von Zugriffs- und Änderungsberichten von Kennwörtern für Auditierungen

Im Rahmen von Compliance-Anforderungen und Auditierungen sind Protokolle der Zugriffsberechtigungen und Zugriffsnutzung von Benutzern erforderlich. Der Auftragnehmer stellt auf Anforderung (max. vier Berichte pro Jahr pro Kunde) Berichte für die im Kennwortspeicher verwalteten Unternehmenskennwörter mit folgenden Informationen zur Verfügung:

- Kennwortänderungen
- Kennwortkomplexität
- Zugriffe auf den Kennwort-Safe und auf die jeweiligen Unternehmenskennwörter durch die Nutzer
- Zugriffsberechtigungen der Nutzer
- Zugriffe des Dienstleisters auf die Kennwörter der von ihm verwalteten administrativen Zugänge des Kunden

11. Bereitstellung eines Berichts über schwache Kennwörter

Der Auftragnehmer sendet dem Kunden eine Auflistung aller schwachen Unternehmenskennwörter per E-Mail zu. Die Auflistung enthält die Art des Kennworts, Beschreibung, Benutzernamen und eine vom Kennwortspeicher vorgenommene Einschätzung zur Kennwortstärke.

12. Durchführung von Kennwortänderungen von Benutzerkonten

Auf Anforderung des Kunden übernimmt der Auftraggeber bis zu 3 Kennwortänderungen pro Halbjahr pro Benutzer. Voraussetzung für die Kennwortänderungen ist, dass der Auftragnehmer einen administrativen Zugang für das Zielsystem mit der Berechtigung zur Kennwortänderung der Benutzerkonten erhält. Jede weitere Änderung wird mit 50 EUR pauschal berechnet.

Die Leistung umfasst:

- Kennwortänderung und -reset auf Anfrage
- Aktualisieren des Kennworteintrags im Kennwortspeicher
- Vergabe der Zugriffsberechtigungen im Kennwortspeicher an vom Kunden definierte Nutzer (bei gemeinsam genutzten Zugangsdaten)

Auch bei regelmäßigen Kennwortänderungen bleibt ein Risiko, dass Dritte Zugangsdaten ausspionieren und missbrauchen können.

13. Einmalige Einrichtungsgebühr

Mit der Einrichtungsgebühr ist die Ersteinrichtung des Kennwortspeichers gemäß dem vom Kunden bereitzustellenden Kennwort-Konzept abgegolten. Nicht enthalten ist die Installation eines Browser-Plugins sowie das Einrichten einer mobilen App auf dem Smartphone der Benutzer. Ebenso nicht enthalten ist das Befüllen des Kennwortspeichers, also bspw. Das Abspeichern von Kennwörtern der Benutzer.

14. Durchführung einer Kennwortänderung eines Windows-Dienste-Kontos alle 90 Tage

Windows-Dienste-Konten sind administrative Zugänge, die von Systemen und Anwendungen benötigt werden. Diese unterliegen denselben Risiken wie menschliche Administratorkonten. Aufgrund ihrer Interdependenzen mit Systemen kann es daher bei einer Rotation zu einer kurzfristigen Dienste-Unterbrechung kommen. Der Kunde informiert den Auftragnehmer über Dienste-Konten, für die diese Unterbrechungszeit kritisch sein könnte, um einen Zeitpunkt zu vereinbaren, zu dem die Änderung erfolgen kann.

15. Bereitstellung einer Kennwort-zurücksetzen-Funktion für Benutzer

Der Auftragnehmer stellt dem Kunden eine Smartphone App (Android ab Version 5.0 und iOS ab Version 13) bereit, mit der der Nutzer das Kennwort für sein persönliches Windows-Anmeldekonto zurücksetzen kann.

Der Nutzer erhält initial eine E-Mail mit einem QR-Code, welchen er mittels der vom Auftragnehmer gestellten Smartphone-App scannen muss. Sollte der Nutzer sein Kennwort zur Anmeldung am Windows-Client des Kunden vergessen haben, so kann er die Smartphone App nutzen, um sein Kennwort selbstständig zurückzusetzen.

Voraussetzung ist, dass der Auftragnehmer administrativen Zugriff auf den Verzeichnisdienst (Active Directory) hat.

16. Einmalige Übernahme von Kennwörtern aus einem anderen Kennwort-Safe

Vorhandene Kennwörter des Kunden werden auf Wunsch und gemäß technischer Machbarkeit in die bereitgestellten Unternehmenskennwortspeicher importiert. Eine grundsätzliche technische Machbarkeit besteht bei Importvorgängen aus den Quellen Microsoft Excel und KeePass. Eine Prüfung und Durchführung eines Imports von Bestandsdaten aus anderen Quellen kann der Kunde beim Auftragnehmer jederzeit beauftragen. Die Abrechnung erfolgt gemäß Ziffer 18.

17. Stundensatz für weitere Leistungen

Der Stundensatz für die Erbringung von Dienstleistungen wie technische Hilfestellung, Fehleranalyse, Lösungserarbeitung, Umsetzung und Dokumentation im Servicezeitraum von Mo-Fr 8-17 Uhr gilt gemäß Leistungsbroschüre. Die Abrechnung erfolgt im 15 Minuten Takt. Etwaige Fahrtkosten werden mit EUR 0,80€ pro Entfernungskilometer berechnet. Die Anfahrtszeit wird mit dem vorgenannten Stundensatz abgerechnet, bzw. mit dem Stundenkontingent verrechnet. Die Rückfahrtzeit wird nicht berechnet. Ein Fernzugriff auf die Kundensysteme erspart dem Kunden die Fahrtkosten, die Zeit wird wie zuvor genannt abgerechnet. Außerhalb der Servicezeiten werden 50% Zuschlag (zwischen 17-8 Uhr) bzw. 100% Zuschlag (sonn- und feiertags) berechnet.

18. Gültigkeit Servicebedingungen

Nachrangig zu den Regelungen dieser Leistungsbeschreibung gelten die Servicebedingungen in der jeweils aktuellen Version. Außerdem gelten nachrangig für die eingesetzten Softwareprodukte die Lizenz- und Nutzungsbedingungen der jeweiligen Hersteller.