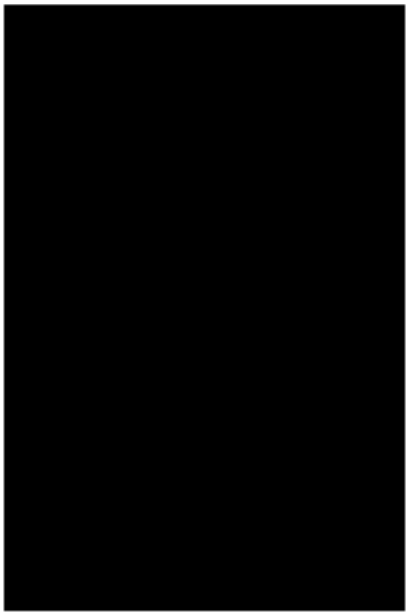
Implementierung eines zentralen Passwort-Management-Systems

Abschlussprojekt Sommer 2024

Fachinformatiker für Systemintegration



Prüfungsteilnehmer: Michael Becker



Geburtsdatum:

Geburtsort:

Ausbildungsbetrieb:

Projektbetreuer:

[redacted]

Inhaltsverzeichnis

1 Einleitung 1
2 Ausgangssituation 1
2.1 Der Ausbildungsbetrieb 1
2.2 Auslöser des Projektes 1
2.3 Ist-Analyse 2
3 Konzeptionsphase 2
3.1 Anforderungen an den Passwortmanager 2
3.2 Marktanalyse 3
3.2.1 Bitwarden 3
3.2.2 Keeper Security 3
3.2.3 1password 3
3.2.4 Passbolt 3
3.2.5 Password Depot 3
3.3 Kostenvergleich der Produkte 3
3.4 Nutzwertanalyse 4
3.5 Kostenkalkulation 6
3.5.1 Personalkosten 6
3.5.2 Stromkosten 6
3.5.3 Lizenzkosten 6
3.6 Kosten bei Schadensfall 7
3.7 Planung der Serverinstallation 7
3.8 Planung der Netzwerkkonfiguration 8
3.9 Planung der Client Konfiguration 8
3.10 Rechtekonzept 9
3.11 Zeitplanung 9
4 Durchführung 10
4.1 Installation der Virtuellen Maschine 10
4.2 Konfiguration der VM 10
4.3 Installation des Password Depot Servers 10
4.4 Konfiguration des Password Depot Servers 10
4.5 Serverrichtlinien 11
4.5.1 Konfiguration der Passwortrichtlinien 11
4.5.2 Standardberechtigungen 11
4.5.3 Einträge 12
4.6 Clientsicherheitsrichtlinien 12
4.6.1 Kennwortrichtlinien 12
4.6.2 Programmoptionen 12

4.6.3 Richtlinien für Aktionen 12
4.6.4 Richtlinien für erlaubte Speicherorte 12
4.7 Installation der Datenbanken des Password Depot Servers 12
4.8 Gruppen anlegen 12
4.9 Benutzer anlegen 12
4.10 Konfiguration der Datenbankberechtigungen 12
4.11 Passwörter importieren 13
4.12 Migration der Umgebung 13
4.13 Einrichtung des Zertifikates 13
4.14 Firewall Regel 13
5 Testphase 13
5.1 Test der Anmeldung an den Server 13
5.2 Funktionstest des Password Depot 14
6 Abschluss 14
6.1 Soll ist Abgleich 14
6.2 Abgleich der Zeitplanung 15
6.3 Lizenzkostenabgleich 15
6.4 Übergabe des Projektes 15
6.5 Fazit 16

Tabellenverzeichnis

Tabelle 1: Nutzwertanalyse 5
Tabelle 2: Personalkosten 6
Tabelle 3: Zeitplanung 9
Tabelle 4: Lizenzkosten Passbolt und Bitwarden II
Tabelle 5: Lizenzkosten Password Depot II
Tabelle 6: Kosten eines Arbeitsplatzes 2023 II
Tabelle 7: Stromkostenberechnung III
Tabelle 8: Lizenzkostenberechnung III
Tabelle 9: Kosten bei Schadensfall IV

Abbildungsverzeichnis

Abbildung 1: Kosten Zeitvergleich 4
Abbildung 2: Password Depot Logo 6
Abbildung 3: Konzept 8
Abbildung 4: Konfiguration der Standardberechtigungen 11
Abbildung 5: Zeitplanungsabgleich 15
Abbildung 6: Stromkosten III
Abbildung 7: Konfiguration der VM IV
Abbildung 8: Allgemeine Konfiguration IV
Abbildung 9: Konfiguration der Verbindungen V
Abbildung 10: Sicherung der Config-Datei V
Abbildung 11: Erweiterte Servereinstellungen VI

Abbildung 12: Konfiguration des TOTP VI
Abbildung 13: Konfiguration der Passwortrichtlinien VII
Abbildung 14: Konfiguration der Einträge VII
Abbildung 15: Konfiguration der Client Passwortrichtlinien VIII
Abbildung 16: Konfiguration der Programmoptionen der Clients VIII
Abbildung 17: Konfiguration der Aktionen der Clients VIII
Abbildung 18: Konfiguration der Client Speicherorte IX
Abbildung 19: Password Depot Angebot IX

Anhangsverzeichnis

I. Quellenverzeichnis I
II. Glossar I
III. Anhang II
A. Lizenzkosten Passbolt und Bitwarden II
B. Lizenzkosten Password Depot II
C. Kosten eines Arbeitsplatzes 2023 II
D. Stromkosten III
E. Stromkostenberechnung III
F. Lizenzkostenberechnung III
G. Kosten bei Schadensfall IV
H. Konfiguration der VM IV
I. Allgemeine Konfiguration IV
J. Konfiguration der Verbindungen V
K. Sicherung der Config-Datei V
L. Erweiterte Servereinstellungen VI
M. Konfiguration des TOTP VI
N. Konfiguration der Passwortrichtlinien VII
O. Konfiguration der Einträge VII
P. Konfiguration der Client Passwortrichtlinien VIII
Q. Konfiguration der Programmoptionen der Clients VIII
R. Konfiguration der Aktionen der Clients VIII
S. Konfiguration der Client Speicherorte IX
T. Password Depot Angebot IX
U. Betriebsdokumentation X
V. Kundendokumentation XVI

[redacted]

1 Einleitung

In dieser Dokumentation für mein IHK-Abschlussprojekt zum Fachinformatiker für Systemintegration werde ich alle Tätigkeiten erläutern, welche ich für die Durchsetzung des Projektes ausgeführt habe.

Aufgrund von internen Umstellungen ist der Projektbetreuer nicht mehr [redacted] sondern [redacted]

Aus Gründen der besseren Lesbarkeit wurde auf die gleichzeitige Verwendung der Sprachformen männlich, weiblich und divers verzichtet. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.

Abkürzungen und Fachbegriffe werden im Text Gold formatiert und können im Glossar nachgeschlagen werden.

Verweise auf Belege und Darstellungen im Anhang werden im Text mit hochgestellten Verweisen in folgender Notation dargestellt: [Anh.0;S.0]

2 Ausgangssituation

2.1 Der Ausbildungsbetrieb

[redacted]

2.2 Auslöser des Projektes

Aktuell verwendet die [redacted] das den Passwortmanager KeePass. Da dieser leider keine Rechteverwaltung unterstützt, sind alle Kennwörter in einer allgemeinen Datenbank gespeichert. In der Datenbank kann nur eine Person gleichzeitig arbeiten. Dies erschwert die Arbeit der Kollegen mit dem derzeitigen Produkt. Alle personenbezogenen Passwörter werden in eigenen Passwortmanagern oder in eigenen Dateien wie zum Beispiel eine Word-Datei gespeichert. Daraus ergibt sich die Situation, dass jeder Mitarbeiter Zugriff auf alle Passwörter hat, auch wenn diese nicht zu seinem Zuständigkeitsbereich gehören. Außerdem stellt dies ein erhebliches Sicherheitsrisiko dar, da ein Fremder die komplette Systemkontrolle erlangen kann, wenn er das Passwort bekommen sollte. Des Weiteren muss das Masterpasswort aus Gründen der IT-Sicherheit regelmäßig geändert werden, wenn ein Mitarbeiter der [redacted] das Unternehmen verlässt.

Um dieses Problem zu beheben, soll ein zentral verwalteter Passwortmanager implementiert werden, welcher die Funktion einer Benutzerverwaltung besitzt.

[redacted]

2.3 Ist-Analyse

Wie im vorherigen Abschnitt erwähnt, werden die Passwörter in einer KeePass-Datei gespeichert, auf die jeder Mitarbeiter Zugriff hat. Bei Betrachtung des Passwortmanagers ist aufgefallen, dass viele Passwörter nicht aktuell sind und es keine generelle Struktur der Passwörter gibt. Dies führt zu langer Suche der Passwörter. Dadurch, dass das derzeitige Produkt keine Benutzer- und Rechteverwaltung besitzt, haben Praktikanten und Auszubildende keinen Zugriff auf die Datenbank. Dadurch ist die Verwaltung der Kennwörter für Auszubildende und Praktikanten umständlich. Die gleichzeitige Bearbeitung der Datenbank ist ebenfalls nicht möglich.

In der [redacted] verfügen wir über ein eigenes On-Premises Rechenzentrum mit Fujitsu Primergy RX2540 M5 Servern. Die Server sind ausgestattet mit zwei Intel Xeon Silver 4214R Prozessoren, 512 GB Arbeitsspeicher und 20 TB Festplattenspeicher. Jeder Server wird in einem RAID 5 Verbund betrieben. Auf den Servern ist ein Bare Metall Hypervisor im Einsatz mit einem ESXi-Betriebssystem. Für die Virtualisierung wird die Managementplattform VMware vSphere genutzt. Die Server werden in Clustern betrieben. Zudem werden alle Server mit kontinuierlichen Backups gesichert.

3 Konzeptionsphase

3.1 Anforderungen an den Passwortmanager

Am Ende des Projektes soll ein zentrales Passwortmanagementsystem vorhanden sein, welches alle arbeitsrelevanten Passwörter speichert.

Nach einem Meeting zur Bedarfsermittlung des Projektes mit den Administratoren wurden folgende Punkte festgestellt, die der Passwortmanager beinhalten muss:

- Der Dienst muss von jedem Arbeitsplatz der Administratoren erreichbar sein, da es sonst zur Arbeitsunterbrechung führen kann.
- Aufgrund des hohen Stellenwertes für den Betrieb muss der Service mit kontinuierlichen Backups gesichert werden.
- Der Service muss ein Rechtemanagement enthalten, mit dem man sowohl Gruppenrechte als auch einzelne Benutzerrechte vergeben kann, um Zugriffe der Mitarbeiter klar zu definieren.
- Um potenzielle Angriffe zu verhindern, wird der Passwortmanager mit einer sicheren und personalisierten Authentifizierungsmethode gesichert.
- Außerdem muss das System im Stande sein, dem Stand der Technik entsprechenden Passwörter zu generieren.
- Das Produkt muss selbst eine On-Premises-Lösung sein, um die eigene Datenhoheit zu gewähren und keine Ausfallzeiten durch Verschuldung des Providers zu erleiden.
- Eine weitere Anforderung muss sein, dass die Passwörter und Daten, die im Passwortmanager hinterlegt werden, verschlüsselt gespeichert und übertragen werden.
- Der Passwortmanager muss mit dem Windowsbetriebssystem kompatibel sein, da die Arbeitsgeräte mit Windows betrieben werden.
- Um dafür zu sorgen, dass alle Dienste eine hohe Passwortsicherheit haben, ist es wichtig, dass Passwortrichtlinien erstellt werden können.

Diese Anforderungen müssen für das Produkt gegeben sein, damit es als Passwortmanager infrage kommt.

3.2 Marktanalyse

Nach einer Produktrecherche im Internet wurden fünf Produkte zum Vergleich gefunden. Diese werden auf die Anforderungen des Soll-Konzeptes überprüft. Im Folgenden werden die Produkte Bitwarden, Keeper Security, 1password, Passbolt und Password Depot überprüft.

3.2.1 Bitwarden

Bitwarden ist ein Open Source Passwort Manager, der sowohl in der Cloud als auch selbst gehostet werden kann. Nach Recherche auf der Webseite von Bitwarden konnte festgestellt werden, dass nur die Unternehmensversion den Anforderungen des Projektes entspricht, da diese Version selbst gehostet werden kann.

3.2.2 Keeper Security

Keeper Security ist ein Passwortmanager für Unternehmen. Nach ausführlicher Recherche ist dieser Passwortmanager kein geeigneter Kandidat für das Projekt, da es keine On-Premises Version gibt.

3.2.3 1password

1password ist ein vom kanadischen Unternehmen AgileBits Inc. entwickelter Passwortmanager. Die Recherche ergab, dass dieses Produkt den Anforderungen des Projektes nicht entspricht, da es für 1Password keine On-Premises Version gibt.

3.2.4 Passbolt

Passbolt ist ein Open Source Passwort Manager. Er kann sowohl in der Cloud mit Sitz in Luxemburg betrieben werden oder aber On-Premises selbst gehostet werden. Der Passwortmanager lässt sich sogar auf einem Raspberry Pi betreiben. Die Recherche der Produktwebseite ergab, dass sich das Produkt als potenzieller Kandidat für dieses Projekt eignet. Da in der kostenlosen Version von Passbolt keine Passwortrichtlinien erstellt werden können, müssen wir die kostenpflichtige Version in Betracht ziehen.

3.2.5 Password Depot

Password Depot ist ein in Deutschland entwickelter Passwort Manager von der Firma Acebit. Er ist nur als On-Premises Version zu erhalten, sodass er ausschließlich selbst gehostet werden kann.

3.3 Kostenvergleich der Produkte

Im jetzigen Schritt vergleiche ich die Kosten der oben genannten Produkte. Da alle Produkte pro Benutzer zu zahlen sind, wurde eine Benutzeranzahl von 30 gewählt, um alle Mitarbeiter und künftige Praktikanten und Azubis in den Passwortmanager mit aufnehmen zu können. Als nächstes wurden die Kosten der Passwortmanager recherchiert.

Bitwarden ist nur im Abo-Modell zu bekommen. Da nur die Unternehmensversion von Bitwarden infrage kommt, betragen die Kosten 6,00 $ pro Monat pro Benutzer. Rechnet man dies in Euro um und rechnet dieses hoch auf Jahreskosten, ergeben sich Kosten in Höhe von 2.023,20 € pro Jahr. [Anh.A; S. II]

Da die kostenlose Version von Passbolt den Anforderungen des Projektes nicht entspricht, muss die kostenpflichtige Version verglichen werden. Die Kosten in dieser Version liegen bei 135,00 € pro Monat pro Benutzer. Die Jahreskosten dieses Produktes belaufen sich dadurch auf 1.620,00 €. [Anh.A; S.II]

Password Depot hat einmalige Kosten von 2.658,00 € für eine Lizenz für 30 Nutzer. Um unseren Server auf dem neusten Stand der Sicherheitsupdates zu bringen, müssen wir für diesen Server Supportkosten bezahlen. Der Support von Password Depot beläuft sich auf 30 % der Lizenzkosten im ersten Jahr und senkt sich bis zum dritten Jahr auf einen Betrag von

[redacted]

25 % der Lizenzkosten. Die Supportkosten werden jährlich gezahlt. Dies ergibt Supportkosten von 797,40 € im ersten Jahr, im zweiten Jahr sind es 730,95 € und ab dem dritten Jahr zahlt man Supportkosten in Höhe von 664,50 € pro Jahr. [Anh.B;S.II]

Um diese Kosten nun miteinander zu vergleichen, habe ich einen Kosten Zeitvergleich erstellt.

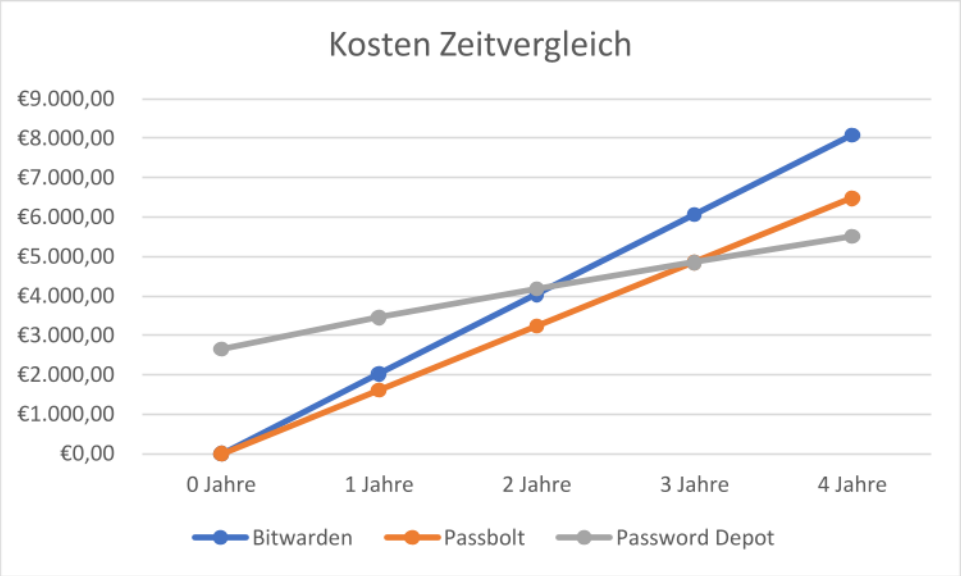


Abbildung 1: Kosten Zeitvergleich

Password Depot ist im ersten Jahr das unrentabelste Produkt aufgrund der hohen Anschaffungskosten der Lizenz. Ab dem dritten Jahr ist Password Depot jedoch am rentabelsten im Vergleich mit Bitwarden und Passbolt, da die Supportkosten deutlich geringer sind als die Abokosten der anderen Produkte. Dadurch ist Password Depot das kostengünstigste Produkt, da die Schul-IT vorhat, den Passwortmanager so lange zu nutzen wie möglich.

3.4 Nutzwertanalyse

Um eine fundierte Entscheidung treffen zu können, habe ich mich dafür entschieden, eine Nutzwertanalyse mit den im vorherigen Schritt genannten Produkten zu erstellen. Die ausgewählten Kriterien für die Nutzwertanalyse wurden in einem Meeting mit dem Abteilungsleiter und den Fachteamleitern besprochen und festgelegt. Die Kriterien erläutere ich im nächsten Abschnitt.

Jährliche Kosten: Jährliche Kosten, die anfallen, werden durch die Lizenzierung inklusive Support berechnet. Dieses Kriterium wird mit einer hohen Gewichtung bewertet, da die IT nur ein begrenztes jährliches Budget hat.

Anpassbare Benutzeranzahl: Im Falle eines Wachstums der IT sollte man die Benutzeranzahl des Passwortmanagers anpassen können. Da die [redacted] kaum noch Zuwachs benötigt, wird dadurch die Benutzeranzahl kaum noch verändert werden. Aus diesem Grund hat dieses Kriterium eine niedrige Gewichtung.

Mehrfaktor Authentifizierung: Damit der Passwortmanager eine hohe Sicherheit aufweist, ist es wichtig, dass die Zugriffe auf das System mit einem zweiten Faktor abgesichert werden. Aufgrund des hohen Stellenwertes dieses Dienstes für die IT-Sicherheit wird dieses Kriterium mit einer hohen Gewichtung bewertet.

[redacted]

Passwörter und Passwortordner teilen: Um das Arbeiten der Abteilungen miteinander zu vereinfachen, ist es manchmal von Nöten, dass die Zugriffe kurzzeitig geteilt werden. Da die Passwörter nur selten mit Mitarbeitern geteilt werden müssen, wird dieses Kriterium niedrig gewichtet.

Speicherung von Lizenzen, Kreditkarten etc.: Da wir viele Lizenzen für unsere Systeme haben und wir keine verschlüsselte Speicherungslösung dafür besitzen, ist es von Vorteil, wenn wir dies auch im Passwortmanager tun können. Da dies die IT-Sicherheit steigert, hat dieses Kriterium eine hohe Gewichtung.

Externe Datenbank nötig: In diesem Punkt wird geguckt, ob der Passwortmanager die Datenbanken selbst erzeugen kann oder eine externe Datenbank dafür installiert werden muss. Da dieses Kriterium nur einen geringen Unterschied im Arbeitsaufwand bietet, wird es niedrig gewichtet.

Passkey **Kompatibilität:** Passkeys sind eine von der FIDO Alliance entwickelte passwortlose Anmeldemöglichkeit. Um den Passkey zu nutzen, wird ein asymmetrisches Schlüsselpaar erzeugt. Der private Schlüssel wird auf dem Gerät gespeichert und der öffentliche Schlüssel wird auf dem Server gespeichert. Ein Klick auf die Fläche Passwortlose Anmeldung startet den Anmeldevorgang. Nach der Eingabe eines Pins oder einer biometrischen Authentifizierung wird der Anmeldevorgang vollendet. Da diese Anmeldemöglichkeit noch kaum verbreitet und recht neu ist, wird dieses Kriterium niedrig gewichtet.

Die in der Soll-Konzept genannten Kriterien werden nicht in die Nutzwertanalyse miteinbezogen, da diese schon vorab überprüft wurden und ein sofortiges Ausschlusskriterium sind für das Produkt.

		Passbolt		Bitwarden		Password Deport	
Kriterium	**Gewichtung**	**Punkte**	**gewichtet**	**Punkte**	**gewichtet**	**Punkte**	**gewichtet**
Jährliche Kosten	30	0,5	15	0	0	1	30
Anpassbare Benutzeranzahl	10	1	10	1	10	1	10
Mehrfaktor Authentifizierung	25	1	25	1	25	1	25
Passwörter teilen	15	1	15	1	15	1	15
Speicherung von Lizenzen etc.	5	0	0	0,5	2,5	1	5
Externe Datenbank nötig	5	0	0	0	0	1	5
Passkey Kompatibilität	10	0	0	1	10	0	0
Ergebnis	100		65		62,5		90

Tabelle 1: Nutzwertanalyse

Die Punktevergabe der Nutzwertanalyse sieht wie folgt aus: Bei 1 Punkt wurde das Kriterium im vollen Umfang erfüllt, 0 Punkte gab es, wenn das Produkt das Kriterium nicht erfüllt hat und 0,5 Punkte gab es, wenn das Kriterium mit einem Manko versehen war. Bitwarden hat bei dem Kriterium „Speicherung von Lizenzen, Kreditkarten etc.“ nur 0,5 Punkte erhalten, da man ein Feld für Lizenzen oder ähnliches erst selbst anlegen muss, bevor man es benutzen kann, wohingegen Password Depot schon vorgefertigte Felder dafür zur Verfügung stellt und zusätzlich die Option bietet, eigene Datenfelder anzulegen. Die Kosten hingegen wurden anhand der Wirtschaftlichkeit verglichen. Dies führt dazu, dass das wirtschaftlichste Produkt die volle Punktzahl bekommen hat und die anderen nach Platzierung weniger Punkte bekommen haben.

Das Ergebnis der Nutzwertanalyse ist, dass Password Depot das Produkt für dieses Projekt wird. Dies ist hauptsächlich durch den Preis und die integrierte Datenbank der Fall.

[redacted]

Die Nutzwertanalyse habe ich meinem Bereichsleiter vorgestellt und er hat dies für erfolgreich angesehen. Dadurch haben wir das Produkt Password Depot bei der Finanzabteilung in Auftrag gegeben.



Abbildung 2: Password Depot Logo

3.5 Kostenkalkulation

Im folgenden Abschnitt werde ich die entstehenden Kosten des Projektes aufzeigen. Diese werde ich in die drei Abschnitte Personalkosten, Serverbetriebskosten und Lizenzkosten unterteilt.

3.5.1 Personalkosten

Im Folgenden wurden die Personalkosten des Projektes berechnet. Die angegebenen Personalkosten inklusive Gemein-, Sach- und IT-Kosten sind in der Tabelle „Kosten eines Arbeitsplatzes 2023“ zu finden. [Anh.C;S.II]

Da die Stelle eines Administrators bei der [redacted] mit der Entgeltgruppe 10 bewertet wird, betragen die Kosten 64,11 € pro Stunde. Die Kosten eines Auszubildenden betragen 24,39 € pro Stunde. Der Arbeitsumfang des Auszubildenden beträgt 40 Stunden und es werden geschätzt 3 Stunden eines Administrators gebraucht.

	Stunden	Stundenlohn	Gesamtlohn
Auszubildender 3. Lehrjahr	40	24,39 €	975,60 €
Angestellter nach TVöD 10	3	64,11 €	67,11 €
Gesamt			1.042,71 €

Tabelle 2: Personalkosten

Dadurch ergeben sich Gesamtpersonalkosten von 1.042,71 €.

3.5.2 Stromkosten

Die Fujitsu-Server haben einen durchschnittlichen Stromverbrauch von ca. 260 Watt pro Stunde. Laut dem Hersteller braucht der Password Depot Server mindesten 8 GB RAM. Wenn einer VM durchschnittlich 8 GB RAM zugewiesen würden, dann würde man damit maximal 63 VMs auf dem Hardwareserver betreiben können. Dies ergibt bei einer VM einen durchschnittlichen Stromverbrauch von ca. 4,13 Watt pro Stunde. Bei einem Strompreis von 0,26 €/kWh [Anh.D;S.III] entspricht dies 9,40 € pro Jahr. [Anh.E;S.III]

3.5.3 Lizenzkosten

Die Lizenzkosten des Password Depot Servers können wir aus der vorher schon genutzten Tabelle entnehmen. Für die Password Depot Clients werden keine zusätzlichen Lizenzen benötigt, da die Lizenz des Servers eine unbegrenzte Clientanzahl zulässt.

Der Password Depot Server benötigt vor der Installation noch ein Betriebssystem. Auf der Herstellerseite ist zu finden, dass der Password Depot Server nur auf Windows Server Betriebssystemen oder Windows Client Betriebssystemen zu installieren ist. Da die Kosten von einer Windows Server 2022 Lizenz bei ungefähr 6.000,00 € liegen und die Kosten einer Windows 10 Pro Edition bei ungefähr 50,00 € liegen, wird für dieses Projekt eine Windows 10 Pro Edition beschafft.

[redacted]

Das ergibt Lizenzkosten von 4.900,85 €. [Anh.F;S.III]

3.6 Kosten bei Schadensfall

Im folgenden Schritt stelle ich den voraussichtlichen wirtschaftlichen Schaden, den [redacted] und [redacted] nehmen würden, wenn ein Fremder sich Zugriff durch einen Mitarbeiter auf die Keepass-Datei verschaffen würde.

Wenn das Masterpasswort der Keepass-Datei gestohlen werden würde, dann hätte man Zugang zu allen unseren Systemen. Dadurch könnten die Server, die Netzwerke und die Workstations [redacted] beispielsweise durch einen Verschlüsselungstrojaner kompromittiert werden. Eine mögliche Folge wäre der Stillstand [redacted] Der Unterricht würde auch beeinträchtigt werden, da sehr viele Lehrer auf einen digitalen Unterricht vorbereitet sind und alle ihre Unterlagen digital auf den [redacted] Servern speichern. Dadurch müsste unsere Netzwerkumgebung von [redacted] neu implementiert werden. Die ca. 7000 Endgeräte in den [redacted] die von uns verwaltet werden, müssten alle neu konfiguriert werden. Außerdem müsste das [redacted] Rechenzentrum an Hand von Backups wiederhergestellt werden.

Für die Wiederherstellung aller Systeme müssten alle 27 [redacted] Mitarbeiter eingesetzt werden. Dies würde ca. 3 Monate lang dauern. Dadurch ergeben sich ca. 13 Arbeitswochen. Pro Woche arbeitet ein Administrator 39 Stunden. Dadurch ergibt sich über die Monate eine Arbeitszeit von 507 Stunden pro Mitarbeiter. Dies würde einen Gesamtstundensatz von 13689 Stunden ergeben, um alle Systeme wiederherzustellen. Bei einem durchschnittlichen Stundenlohn von 64,11 € würde dies Gesamtarbeitskosten von 877.601,79 € entsprechen. [Anh.G;S.IV]

Die Schätzwerte gehen von einem kleinen Schadensmaß aus. Im Falle des Cyberangriffes auf den Landkreis Anhalt-Bitterfeld der sich am 09.07.2021 ereignete, hatte der Landkreis einen Schaden von 2,5 Mio. Euro erlitten. Für den Wiederaufbau der IT Systeme benötigte der Landkreis ungefähr ein Jahr. In unserem Schätzungsbeispiel wurden nur die verursachten Personalkosten der Administratoren bei einem kleinen Schadensausmaß bemessen. Die Kosten für neue Hardware und andere Personalkosten wurden nicht betrachtet.

3.7 Planung der Serverinstallation

Der Password Depot Server wird auf einer Virtualisierungsumgebung installiert. Dadurch können die Hardware Ressourcen besser genutzt werden als auf einem einzelnen Hardwareserver. Es wird unsere vorhandene Typ-1-Hypervisor VSphere Umgebung genutzt, da dieser im Gegensatz zu einem Typ-2-Hypervisor eine höhere Performance und eine schnellere Rechenleistung aufweist, da ein Typ 1 Hypervisor kein Betriebssystem zwischen dem Hypervisor und der Hardware benötigt. Da der Password Depot Server nur auf einem Windows Betriebssystem installiert werden kann, wird dieses auf dem Hypervisor in einer virtuellen Maschine installiert, wodurch ein virtueller Server Client simuliert wird. Die VM wird erst in einer Testumgebung installiert und dann in die Live Umgebung migriert. Für die Zugänge der VSphere Umgebung und der Migration der Server aus der Testumgebung in die Liveumgebung ist der Server Administrator zuständig.

In der VM wird eine Datenbank durch den Password Depot Server erstellt. Diese wird mit AES 256 Bit symmetrisch verschlüsselt.

Um eine mit TLS verschlüsselte Kommunikation gewährleisten zu können, muss der Server ein Stammzertifikat und ein Serverzertifikat installieren. Dadurch wird ein Schlüsselpaar für das Stammzertifikat und ein Schlüsselpaar für das Serverzertifikat erstellt. Jedes Schlüsselpaar besteht aus einem öffentlichen und einem privaten Schlüssel. Wenn eine

Nachricht mit dem öffentlichen Schlüssel verschlüsselt wird, kann die Nachricht mit dem Privatem Schlüssel entschlüsselt werden. Der öffentliche Schlüssel des Stammzertifikates muss auf den Clients installiert werden.

3.8 Planung der Netzwerkkonfiguration

Der Server wird in dem internen Servernetz verortet sein. Die IP der VM wird mit 10.0.1.230/24 und das dazugehörige Gateway wird mit 10.0.1.254/24 konfiguriert. Damit die Administratoren den Server erreichen können, wird eine Firewall Regel eingerichtet. Um den Server aus dem Administratorennetzwerk zu erreichen, muss eine Firewall Regel erstellt werden. Diese Regel lässt Pakete aus dem Administratoren Netzwerk 10.0.2.0/24 mit dem Port 25027 auf die IP Adresse 10.0.1.230/24 zu. Diese Regel erstellt der Firewall Administrator. Damit die Administratoren auch von außerhalb des Administratoren Netzwerkes auf den Server zugreifen können, wird die vorhandene End-to-Site VPN Umgebung der [redacted] benutzt. Dadurch wird der Datenverkehr verschlüsselt vom Gerät des Administrators bis zum Administratoren Netzwerk übertragen. Für das VPN Netzwerk wird eine Firewall Regel für den Zugriff auf den Server vom Firewall Administrator erstellt.

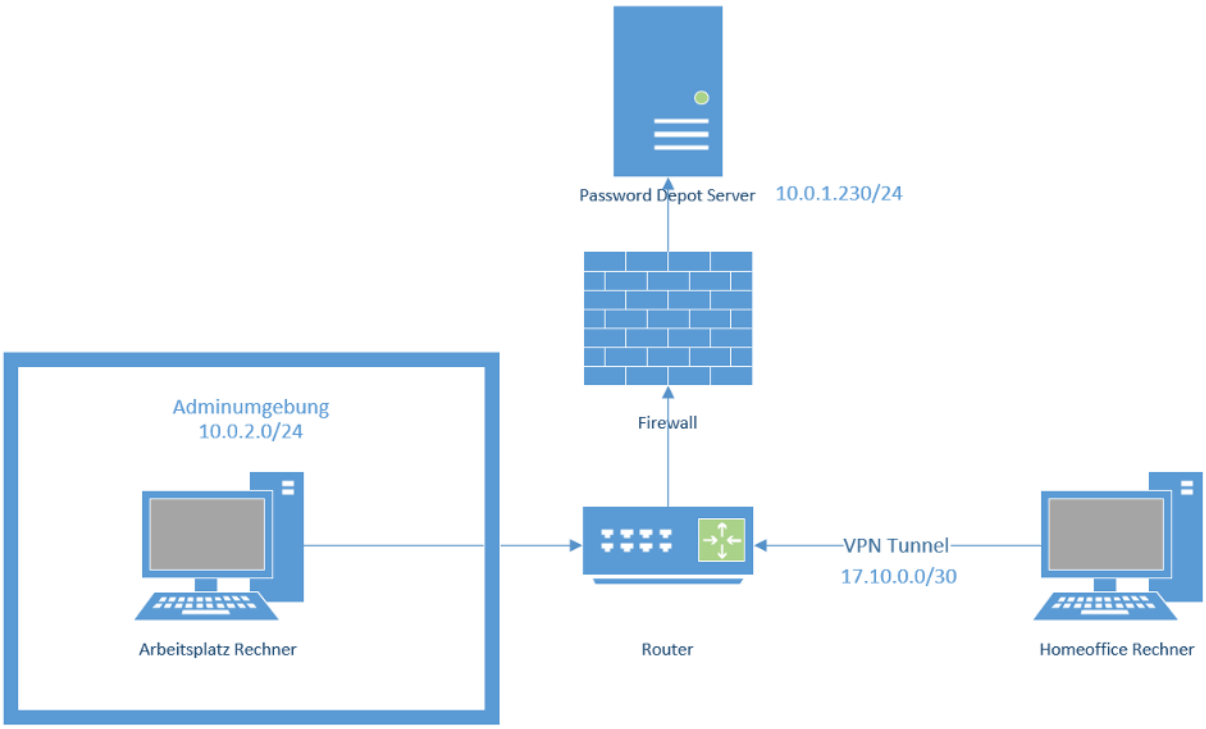


Abbildung 3: Konzept

3.9 Planung der Client Konfiguration

Damit die konfigurierten Richtlinien auf den Clients genutzt werden können, müssen die Passwort Depot Corporate Edition Clients auf jedem Administratoren PC installiert werden. Anhand dieses Clients werden die Endgeräte auf den Server zugreifen können.

Um eine sichere Anmeldemöglichkeit zu gewähren, wird ein zweiter Faktor mit einem TOTP hinzugefügt. Dies ist ein Schutz gegen Bruteforce Angriffe. Bruteforce Angriffe versuchen alle möglichen Passwortkombinationen aus, um sich in den Account des Benutzers einloggen zu können. Durch den TOTP muss, wenn das Passwort herausgefunden wurde, immer noch ein zweites sechsstelliges Einmalpasswort eingegeben werden. Dieses Passwort ändert sich nach einer kurzen Zeitspanne.

[redacted]

3.10 Rechtekonzept

Das Rechtekonzept wird anhand der vorhandenen Bereiche unterteilt. Die vorhandenen Bereiche sind Netzwerkteam, Service Desk und UEM. Darunter haben wir noch kleinere Einzelbereiche.

Der Servicedesk wird in die jeweiligen Standorte unterteilt. Diese lauten: Zentraler Servicedesk, [redacted]

Das Fachteam UEM wird in Web-Services, Client Management und Identity Management eingeteilt.

Das Netzwerkteam wird in Netzwerk Management, Server Management und IT-Sicherheit unterteilt.

Für jeden Bereich wir eine Datenbank erstellt. Die Mitarbeiter werden den Einzelbereichen zugeordnet und werden auf diesen und auf den dazugehörigen Teambereich Zugriff erhalten.

Azubis und Praktikanten werden nur mit Einverständnis des Teamleiters einer Gruppe zugeordnet für die Dauer der Ausbildung im jeweiligen Bereich.

Zudem bekommt jeder einzelne Mitarbeiter einen eigenen privaten Mitarbeiter Speicherbereich.

3.11 Zeitplanung

Um die Installation und Konfiguration des Passwortmanagers und die damit entstehenden Tests und Dokumentation effizient zu bearbeiten, haben die Durchführungsphase und die Testphase teilweise fließende Übergänge.

Tätigkeit	***Stunden***
Analyse der Ausgangssituation	1,5
Ist Analyse	1,5
Konzeptionsphase	*11,5*
Erstellung des Soll Konzeptes	2
Erstellung des Anforderungskatalogs	2,5
Produktvergleich	3
Nutzwertanalyse	1,5
Kostenkalkulation	2,5
Realisierungsphase	*15*
Installation des Passwort-Management-Systems	2,5
Konfiguration des Systems	3
Benutzerrichtlinien	3
Benutzer anlegen	1,5
Migration von alten Passwörtern	2
Test der alten Umgebung	3
Abschlussphase	*12*
Soll-Ist-Abgleich	2
Erstellung einer Betriebsdokumentation	3
Erstellung einer Anwenderdokumentation	2
Roll-out und Projektabschluss	5
Gesamtzeit	*40*

Tabelle 3: Zeitplanung

In der folgenden Abbildung ist die Zeitplanung des Projektes aufgelistet.

[redacted]

4 Durchführung

4.1 Installation der Virtuellen Maschine

Die virtuelle Maschine wurde in unserer Testumgebung erstellt. Die Ressourcen, die benötigt werden, um den Server zum Laufen zu bringen, hat der Hersteller der Software auf seiner Webseite mit Minimalanforderungen beschrieben. Um eine gute Performance des Passwortmanagers zu gewähren, werde ich etwas mehr als die Minimalanforderungen benutzen [Anh.H;S.IV]. Falls die zugewiesenen Ressourcen zu viel oder zu wenig sein sollten, können diese im nach hinein angepasst werden.

4.2 Konfiguration der VM

Erst mal muss das Windowsbetriebssystem installiert werden. Im Zuge dessen wird ein starkes Passwort für den Server generiert, um die Sicherheit zu garantieren. Dies wird anhand des online Passwortgenerators von Password Depot generiert. Dieser Passwortgenerator wird auch im Produkt vorhanden sein. Für die Passwortgenerierung werden alle Zeichen erlaubt sein, Groß- und Kleinschreibung, Zahlen, Sonderzeichen und eine Mindestlänge von 20 Zeichen werden zur Generierung konfiguriert.

Als nächstes muss die IP der VM hinzugefügt werden, dadurch wird erst mal eine freie IP in unserem IP Bereich gesucht und diese dann der Windows VM hinzugefügt. Das lokale Gateway wird hinzugefügt, damit die VM erreichbar ist. Nach erfolgreichem Test des Pings von einem Test Client zum Server konnte ich weiter verfahren.

4.3 Installation des Password Depot Servers

Nachdem die Einrichtung der VM fertig ist, fangen wir mit der Installation des Password Depot Servers an. Die Installation erfolgt durch eine exe Datei. Bei der Installation wird der Speicherort des Servers angegeben. Außerdem wird nach einer kurzen Abfrage automatisch eine Firewall-Regel für Windows erstellt.

Hier wird nur geguckt, dass sowohl der Server als auch der Servermanager installiert wird. Ein starkes Passwort wird erstellt und im derzeitigen Passwortmanager Keepass kurzzeitig festgehalten.

Als nächstes versuche ich mich als Test am Server anzumelden. Dafür muss ich beim Server die IP-Adresse des Servers oder die Localhost Adresse eintragen, da der Servermanager auf der gleichen VM ist wie der Server selbst. Danach wird ich mit dem vorgegeben Passwortdaten angemeldet.

Als Nächstes wird das Passwort des Systemadministrators geändert, mit einem zufällig generierten Passwort des Passwortmanagers. Dies geschieht, indem man auf dem Server auf die zu verwaltenden Benutzer zugreift und dort vom Benutzer „Admin“ das Passwort ändert.

4.4 Konfiguration des Password Depot Servers

Damit wir den Passwortmanager benutzen können, werden wir erst mal die generellen Optionen des Servers konfiguriert. Bei den Serveroptionen werden wir das Internetprotokoll auf nur IPv4 beschränken, da wir im Unternehmen IPv6 nicht nutzen. Als nächstes wird die Einstellung TLS verwenden aktiviert [Anh.I;S.IV]. Das Zertifikat wird in einem späteren Schritt installiert.

Die Authentifizierung wird auf „Zugangsdaten (Konto und Kennwort)“ eingestellt und die unterstützen Clients wird nur der Corporate Edition für Windows sein. Da nur die Corporate Edition die Clientsicherheitsrichtlinien erzwingen kann, wird nur diese aktiviert. Zusätzlich werden neue Verbindungen, wenn man schon eingeloggt ist, unterbunden. Zusätzlich wird der

[redacted]

Client bei Inaktivität nach 60 Minuten getrennt. Dadurch wird die Datenbank lokal geschlossen und der Benutzer wird abgemeldet. [Anh.J;S.V]

Die Protokolldatei soll wöchentlich erstellt werden. Um Speicher zu sparen, werden nur die letzten 30 Protokolldateien gespeichert.

Als Absicherung der Konfigurationen wird die Config-Datei jeden Tag mit einer Kopie gesichert. Es werden nur 80 Maximal gespeichert und alle gesicherten Config-Dateien, die älter als einen Monat sind, werden gelöscht. [Anh.K;S.V]

Die eingestellte Bearbeitungszeit der Einträge wird auf 5 Minuten gesetzt. Die automatische Erzeugung einer privaten Datenbank eines neuen Benutzers und die Löschung der privaten Datenbank eines gelöschten Benutzers werden aktiviert. Zusätzlich werden die maximal fehlgeschlagenen Anmeldeversuche auf sieben gesetzt. [Anh.L;S.VI]

Als nächstes wird die Zwei Faktor Authentifizierung aktiviert. Die Option, dass die Geräte gemerkt werden, wird ausgeschaltet und die TOTP-Funktion wird eingeschaltet, sodass der Token per Authenticator App auf dem Diensthandy generiert wird. Im Abschnitt 4.5.1 Konfiguration der Passwortrichtlinien wird dies genauer erläutert. [Anh.M;S.VI]

4.5 Serverrichtlinien

4.5.1 Konfiguration der Passwortrichtlinien

Als nächstes werden die Passwortrichtlinien konfiguriert. Diese Richtlinien werden bei der Benutzung des Passwortgenerators strikt eingehalten und können dort nicht vereinfacht werden. Die Passwortrichtlinien werden auf eine Mindestgröße von 16 Zeichen gesetzt. Die Passwörter müssen mindestens ein Kleinbuchstabe, ein Großbuchstabe, ein Sonderzeichen und eine Zahl beinhalten. Zusätzlich wird die Überprüfung der Kennwörter auf Wörterbuchangriffe aktiviert. Ein Wörterbuchangriff ist eine abgewandelte Form eines Brute-Force-Angriffes. Wörterbuchangriffe probieren alle möglichen Passwörter von Passwortlisten aus. In diesen Listen stehen z. B. Passwörter wie Passwort, 1234 oder Namen. Durch den Filter werden diese Passwörter auf diese Listen überprüft. [Anh.N;S.VII]

Falls ein selbsterstelltes Passwort dieser Richtlinie nicht entspricht, wird der Benutzer darauf hingewiesen. Der Benutzer kann dieses Passwort jedoch speichern, um auch Passwortrichtlinien von BIOS oder einigen Webseiten zu entsprechen, welche z. B. nicht alle Zeichen oder eine Maximallänge für das Passwort voraussetzen.

4.5.2 Standardberechtigungen

Die Standartserverberechtigungen werden wie in der folgenden Abbildung gesetzt.

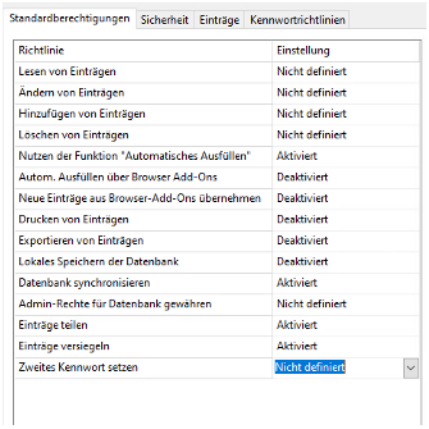


Abbildung 4: Konfiguration der Standardberechtigungen

[redacted]

Die Einstellung deaktiviert bedeutet, dass für alle Datenbanken und für alle Benutzer diese Richtlinie deaktiviert ist. Diese können nicht im nach hinein bei den Benutzer- und Datenbankrichtlinien vergeben werden. Nicht definiert bedeutet, dass die Einstellungen später in den Gruppen- und Benutzerrichtlinien eingestellt werden können. Aktiviert wird nur die Funktion automatisch ausfüllen. Diese ist für alle Benutzer und jede Datenbank damit aktiviert.

4.5.3 Einträge

Da dieser Passwortmanager nur für die IT ist, werden Eintragsdaten wie Kreditkarte, Identität und Banking deaktiviert. Diese Eintragstypen beinhalten nur Daten, welche zur Finanzabteilung gehören und nichts mit unserer zu tun hat. [Anh.O;S.VII]

4.6 Clientsicherheitsrichtlinien

Das Erzwingen der Client Sicherheitsrichtlinien wird eingeschaltet. Da dies nur für Clients der Corporate Edition gilt, wurden alle anderen Clientversionen im vorherigen Schritt deaktiviert.

4.6.1 Kennwortrichtlinien

Diese Passwortrichtlinien gelten nur für die Masterpasswörter der Datenbanken. Dieses Passwort ist das jeweilige Benutzerpasswort für den Passwortmanager. Die Passwörter werden eine Mindestlänge haben von 16 Zeichen und müssen ein Sonderzeichen, eine Zahl und einen Klein- und einen Großbuchstaben beinhalten. Die Kennwörter müssen alle 90 geändert werden und die letzten 12 Kennwörter können nicht verwendet werden. [Anh.P;S.VIII]

4.6.2 Programmoptionen

Für die Programmoptionen wurden alle nicht relevanten Einstellungen deaktiviert. [Anh.Q;S.VIII]

4.6.3 Richtlinien für Aktionen

Die Richtlinien für Daten in die Zwischenablage kopieren, externe Dateien entschlüsseln, interne Dateien verschlüsseln, externe Dateien vollständig löschen, TANs verwenden und zweite Passwörter einstellen, werden aktiviert. Der Rest wird deaktiviert. [Anh.R;S.VIII]

4.6.4 Richtlinien für erlaubte Speicherorte

Hier wird eingestellt, auf was die Datenbanken gespeichert werden. Aus Sicherheitsgründen wurde nur die Einstellung auf dem Password Depot Enterprise Server aktiviert. Alle anderen werden deaktiviert. [Anh.S;S.IX]

4.7 Installation der Datenbanken des Password Depot Servers

Als nächstes brauchen wir eine Datenbank, um die Daten zu speichern. Diese kann man ganz leicht auf dem Password Depot Server erstellen, da dieses im Password Depot Server integriert ist. Für jeden Bereich wird eine Datenbank erstellt.

4.8 Gruppen anlegen

Die Gruppen werden nach Konzept angefertigt. Auszubildende und Praktikanten werden keiner Gruppe zugeordnet, da jeder Azubi in einem anderen Bereich eingesetzt wird.

4.9 Benutzer anlegen

Allen Mitarbeitern werden Benutzer angelegt. Es wird darauf geachtet, dass die Option „Benutzer muss das Kennwort bei der nächsten Anmeldung ändern“ eingestellt wird. Bei der Erstellung werden direkt die Zuordnungen der Gruppen angegeben.

4.10 Konfiguration der Datenbankberechtigungen

Die Berechtigungen der Gruppen werden den Datenbanken zugeordnet. Azubis und Praktikanten werden den Abteilungen mit nur Leseberechtigung zugeteilt, sofern dies vom Abteilungsleiter genehmigt wurde.

[redacted]

4.11 Passwörter importieren

Um die Passwörter vom alten Passwortmanager Keepass in unser neues System zu übernehmen, müssen wir zuerst eine CSV Datei aus der Datenbank kreieren. Dafür wird die verschlüsselte Datenbank auf die Server VM übertragen. Dort wird der Keepass-Client installiert, um die Datenbank anhand des Masterpasswortes zu entschlüsseln und eine CSV Datei zu erstellen. Nach dem Import wird die CSV Datei gelöscht und der Keepass-Client deinstalliert.

Um den Import und der Passwörter und die Einordnung der Passwörter auf die jeweiligen Datenbanken zu verrichten, wird ein Administrator Benutzer angelegt. Dieser Benutzer wird für diese Tätigkeit auf alle nicht privaten Datenbanken Zugriff erhalten. Dieser Benutzer wird nach dieser Tätigkeit wieder gelöscht. Dies muss gemacht werden, da der Serveradministrator keinen Zugriff auf die Passwortdaten hat.

Nach dem Import werden die Passwörter den jeweiligen Datenbanken zugeordnet.

4.12 Migration der Umgebung

Nach der anstehenden Testphase wird das Projekt in die Live-Umgebung migriert. Dies wurde an den zuständigen Server Administrator übergeben. Im Anschluss werden die IP-Bereiche nach dem in der Planungsphase erstellten Konzept eingetragen.

4.13 Einrichtung des Zertifikates

Um den Passwortmanager abzusichern, wird noch ein Zertifikat erstellt. Da der Passwortmanager ein eigenes Zertifikat erstellen kann, wird dieses gemacht. Dadurch werden ein Stammzertifikat und ein Serverzertifikat erstellt.

4.14 Firewall Regel

Der Firewall Administrator wird die im Konzept genannte Firewall Regel einrichten.

5 Testphase

Um einen zufriedenstellenden Betrieb sicherzustellen, welcher gleichzeitig alle zuvor beschriebenen Anforderungen abdeckt, werden in einer Testphase die in der Durchführungsphase beschriebenen Konfigurationen getestet. Die meisten Tests wurden zeitnah nach der Konfiguration getätigt.

5.1 Test der Anmeldung an den Server

Ein Testgerät wird mit einem Password Depot Corporate Edition Client installiert. Mit diesem wird die Verbindung des Clients zum Server getestet. Zusätzlich wird ein Testbenutzer erstellt, um sich mit einem Benutzer anmelden zu können. Bevor wir uns anmelden können, wird der öffentliche Schlüssel des Stammzertifikates installiert. Dann wird mit dem Testbenutzer eine Verbindung aufgebaut. Bei der Erstanmeldung wird die Änderung des Passwortes gefordert. Zusätzlich wird getestet, ob ein Passwort, das nicht den Richtlinien entspricht, verwendet werden kann. Wird ein Passwort eingegeben, das nicht den Richtlinien entspricht, kommt eine Fehlermeldung und es wird noch mal gefordert, das Passwort zu ändern. Als nächstes muss ein zweiter Faktor mit einer TOTP Authenticator App erstellt werden. Die Änderung des Passwortes und die Einrichtung des TOTP kann nicht übersprungen werden.

Danach wird versucht, sich von einem zweiten Gerät mit dem gleichen Benutzer anzumelden. Dazu werden vorher der Client und das Zertifikat installiert. Danach wird die Verbindung getestet. Es erscheint eine Fehlermeldung, dass dieses Konto bereits angemeldet ist und die Verbindung wird nicht gewährt.

[redacted]

Als nächstes wird die Verbindung mit einem vermeintlich inkompatiblen Password Depot Client versucht. Wie erwartet gibt dies eine Fehlermeldung aus, dass dies nicht die richtige Clientversion ist und die Anmeldung deswegen fehlschlägt.

Danach wird getestet, ob die Sperre des Benutzers nach sieben fehlgeschlagenen Anmeldeversuchen eingetragen wird. Beim achten fehlgeschlagenen Anmeldeversuch kommt ein Fehler, dass das Konto gesperrt wurde.

5.2 Funktionstest des Password Depot

Beim Erstellen des Testbenutzers wird darauf geachtet, ob die persönliche Datenbank automatisch erzeugt wird. Sie wird direkt beim Erstellen des Benutzers erzeugt und angezeigt. Auch beim Löschen des Benutzers wird die persönliche Datenbank mitgelöscht.

Für den nächsten Test wird ein den Richtlinien nicht entsprechendes Passwort in einer Datenbank erstellt. Beim Klick auf speichern wird ein Warnhinweis angezeigt, dass dieses Passwort nicht den Richtlinien entspricht.

Die Funktion der Berechtigung des Benutzers wurde getestet. Es wurde auch getestet, ob die Gruppenrechte auf den Benutzer übertragen werden. Beide Tests waren erfolgreich.

Alle Tests der Testphase sind durchlaufen. Daraus wird gefolgert, dass der Passwortmanager für den Livebetrieb bereit ist.

6 Abschluss

6.1 Soll ist Abgleich

Die Anforderung, von jedem Arbeitsplatz erreichbar zu sein, wurde durch die Portfreigabe zum Administratorennetzwerk und zum VPN Netzwerk geschaffen.

Durch die Rechteverwaltung des neuen Servers ist es möglich, die Zugriffe der Mitarbeiter klar zu definieren, konnte ein weiteres Kriterium erfolgreich erfüllt werden.

Die Sicherheit bei der Anmeldung wurde durch das Installieren der Zertifikate und das Einrichten des zweiten Faktors auf die Clients erreicht.

Der Passwortgenerator des Servers funktioniert und generiert Passwörter nach Vorgabe. Auch dieser erfüllt das Kriterium.

Auch die Anforderung, das System On-Premises zu hosten, wird erfüllt, da der Server auf unserer Hardware gehostet wird.

Die Verschlüsselung der Daten und der Datenübertragung ist ein wichtiges Kriterium. Die Verschlüsselung der Datenbank erfolgt durch die AES 256 Bit Verschlüsselung und die verschlüsselte Kommunikation wird durch die TLS Verbindung verschlüsselt.

Da nur Windows Geräte im Einsatz der [redacted] sind, wurde darauf geachtet, dass die Clients des Password Depot mit Windows kompatibel sind.

Die Passwortrichtlinien können durch den Server gesteuert werden. Leider können diese nicht für jedes Passwort als Pflicht gesetzt werden, sondern nur für die Password Depot Zugangsdaten. Mit der Warnung bei einer Passworterstellung außerhalb der Richtlinien werden die Mitarbeiter gewarnt, ein schwaches Passwort zu erstellen.

Die VSphere Umgebung sorgt für kontinuierliche Backups des Systems.

Hiermit wurde festgestellt, dass alle Anforderungen an das System erfüllt wurden.

[redacted]

6.2 Abgleich der Zeitplanung

In der folgenden Abbildung ist die Zeitplanung des Projektes aufgelistet, wie sie geplant war und wie die Zeitplanung bei der tatsächlichen Durchführung des Projektes war. Die sich veränderten Zeiten sind **fett in rot** markiert.

Tätigkeit	***geplante Stunden***	***reale Stunden***
Analyse der Ausgangssituation	1,5	1,5
Ist Analyse	1,5	1,5
Konzeptionsphase	***11,5***	***12,5***
Erstellung des Soll Konzeptes	2	2
Erstellung des Anforderungskatalogs	2,5	2,5
Produktvergleich	3	3
Nutzwertanalyse	1,5	1,5
Kostenkalkulation	**2,5**	**3,5**
Realisierungsphase	***15***	***14***
Installation des Passwort-Management-Systems	2,5	2,5
Konfiguration des Systems	**3**	**2**
Benutzerrichtlinien	3	3
Benutzer anlegen	1,5	1,5
Migration von alten Passwörtern	2	2
Test der alten Umgebung	3	3
Abschlussphase	*12*	*12*
Soll-Ist-Abgleich	2	2
Erstellung einer Betriebsdokumentation	3	3
Erstellung einer Anwenderdokumentation	2	2
Roll-out und Projektabschluss	5	5
Gesamtzeit	*40*	*40*

Abbildung 5: Zeitplanungsabgleich

In der Konzeptionsphase hat die Kostenberechnung etwas länger gedauert als geplant, doch durch die simple Konfiguration des Systems konnte diese Zeit dort wieder aufgeholt werden. Die Zeitplanung konnte sehr gut eingehalten werden.

6.3 Lizenzkostenabgleich

In der Produktbeschaffung ist aufgefallen, dass der Password Depot Server deutlich geringere Kosten verursachte als gedacht. Der Grund dafür liegt darin, dass wir eine öffentliche Organisation sind und von Acebit einen Sondertarif bekommen. Dadurch sind die Kosten deutlich geringer ausgefallen als geplant. Die Kosten des Password Depot Servers liegen damit bei 2.910,51 € [Anh.T;S.IX]. Da die Serverlizenz voraussichtlich 4.900,35 € gekostet hätte, macht dies einen Unterschied von 1.989,84 €. Dadurch ist die Serverlizenz günstiger als in der Planung angedacht.

6.4 Übergabe des Projektes

Die Kundendokumentation [Anh.Fehler! Verweisquelle konnte nicht gefunden werden.;S.Fehler! Textmarke nicht definiert.] für die Administratoren und die Betriebsdokumentation [Anh.U;S.X] für den Systemadministrator des Password Depot Servers werden dem Abteilungsleiter der [redacted] übergeben. Mit dem Abteilungsleiter wurde besprochen, dass die Administratoren den Client und die Zertifikate selbstständig installieren. Ebenfalls wurde ein weiteres Vorgehen des Projektes besprochen, da ich dieses nicht weiter administrieren werde, muss sich ein geeigneter Administrator durch eine Stellenausschreibung finden. Das Administratorpasswort wird für den Nachfolger in unserem Tresor hinterlegt.

6.5 Fazit

Das Projekt war insgesamt ein Erfolg. Die Serverinfrastruktur konnte erfolgreich eingerichtet und konfiguriert werden. Die Testphase wurde auch mit Erfolg durchgeführt und hat keine Probleme feststellen können. Durch dieses Projekt ist die Passwortverwaltung deutlich komfortabler für die Bereiche und die IT-Sicherheit des Unternehmens hat dadurch zugenommen. Eine Schwierigkeit des Projektes war, die Zeitplanung realistisch zu erstellen. Daraus konnte ich lernen, dass vor allem die Planung mehr Zeit in Anspruch nimmt, als ich es vorher gedacht hatte. Außerdem konnte das Projekt sehr gut umgesetzt werden. Das Produkt war eine sehr gute Wahl, da die Konfiguration und die Anwendung sehr intuitiv und leicht zu bedienen sind. Alle Konfigurationen sind sehr leicht einzustellen, da dies meistens nur einen Klick auf die Einstellung benötigt und andere auch keine komplexen Befehle benötigen. Auch die Bedienung des Password Depot Clients ist sehr intuitiv. Zusätzlich ist es eine sehr komfortable Sache, dass der Client über eine Schnellauswahlleiste verfügt. Da diese so klein ist, bemerkt man kaum, dass diese etwas vom Bildschirm verdeckt. Der Client kann dadurch effizient für die Arbeit genutzt werden.

[redacted]

I. Quellenverzeichnis

[redacted]

https://bitwarden.com/de-de/pricing/business/

https://www.keepersecurity.com/de_DE/pricing/business-and-enterprise.html

https://1password.com/de

https://www.passbolt.com/pricing/pro

https://www.password-depot.de/de/produkt/geschaeftlich/funktionen-server.htm

https://www.password-depot.de/de/produkt/geschaeftlich/lizenzierung.htm

https://www.password-depot.de/de/preise/bestellen-server.htm

https://www.ndr.de/nachrichten/info/Strompreis-aktuell-So-viel-kosten-die-Kilowattstunden,strompreis182.html#:~:text=26%2C5%20Cent%20kostet%20Neukunden,zur%20Vorwoche%20nahezu%20gleich%20geblieben.

https://kommunalwiki.boell.de/index.php/Cyberangriff_auf_Landkreis_Anhalt-Bitterfeld_2021

https://www.password-depot.de/de/dokumentation/onlinehilfe-enterprise-server/introduction-de.htm

https://www.password-depot.de/de/dokumentation/dokumentation.htm

https://www.password-depot.de/de/ressourcen/passwort-generator.htm

II. Glossar

A

AES
Advanced Encryption Standard ..... *Eine Verschlüsselung als Blockchiffre*

B

BZTG ..... *Bildungszentrum für Technik und Gestaltung*

E

ESXi
Elastic Sky X integrated ..... *Hypervisor, welcher direkt auf der Hardware installiert wird.*

K

KeePass ..... *Kennwortverwaltungssoftware*

P

Passkey ..... *Passwortlose Anmeldemethode*

T

TLS
Transport Layer Security ..... *Verschlüsselungsprotokoll zur Datenübertragung*
TOTP

[redacted]

Time-based one-time password ..... *Verfahren zur Erzeugung von zeitlich limitierten Einmalpasswörtern*

U

UEM..... *Unified Endpoint Management*

III. Anhang

A. Lizenzkosten Passbolt und Bitwarden

Produkt	Bitwarden	Passbolt
Kosten pro Benutzer	6$	
Kosten in Euro	5,62 €	
Preis bei 30 Benutzern	168,60 €	135,00 €
Preis pro Jahr	2.023,20 €	1620,00 €

Tabelle 4: Lizenzkosten Passbolt und Bitwarden

B. Lizenzkosten Password Depot

Produkt	Password Depot
Einmalige Kosten	2.658,00 €
Supportkosten Jahr 1	797,40 €
Supportkosten Jahr 2	730,95 €
Supportkosten Jahr 3	664,50 €

Tabelle 5: Lizenzkosten Password Depot

C. Kosten eines Arbeitsplatzes 2023

Kosten eines Arbeitsplatzes 2023

Beschäftigte (ohne Sozial- und Erziehungsdienst)

Entgelt-gruppe	durchschnittl. Arbeitgeber-Personal-kosten	Verwaltungs-gemeinkosten 20 %	Sachkosten	IT-Kosten	KoAP (p.a.)	KoAP (p. Std.) 1.590 Std./p.a.
Azubis	24.276 €	4.810 €	6.250 €	3.450 €	38.786 €	24,39 €
03	48.008 €	9.602 €	6.250 €	3.450 €	67.309 €	42,33 €
04	51.495 €	10.299 €	6.250 €	3.450 €	71.494 €	44,96 €
05	54.350 €	10.870 €	6.250 €	3.450 €	74.920 €	47,12 €
06	55.754 €	11.151 €	6.250 €	3.450 €	76.605 €	48,18 €
07	55.396 €	11.079 €	6.250 €	3.450 €	76.175 €	47,91 €
08	58.295 €	11.659 €	6.250 €	3.450 €	79.654 €	50,10 €
09a	66.119 €	13.224 €	6.250 €	3.450 €	89.043 €	56,00 €
09b	68.435 €	13.687 €	6.250 €	3.450 €	91.822 €	57,75 €
09c	71.804 €	14.361 €	6.250 €	3.450 €	95.865 €	60,29 €
10	76.856 €	15.371 €	6.250 €	3.450 €	101.927 €	64,11 €
11	80.925 €	16.185 €	6.250 €	3.450 €	106.810 €	67,18 €
12	95.540 €	19.108 €	6.250 €	3.450 €	124.348 €	78,21 €
13	93.922 €	18.784 €	6.250 €	3.450 €	122.406 €	76,98 €
14	103.623 €	20.725 €	6.250 €	3.450 €	134.047 €	84,31 €
15	111.404 €	22.281 €	6.250 €	3.450 €	143.385 €	90,18 €

Tabelle 6: Kosten eines Arbeitsplatzes 2023

[redacted]

D. Stromkosten

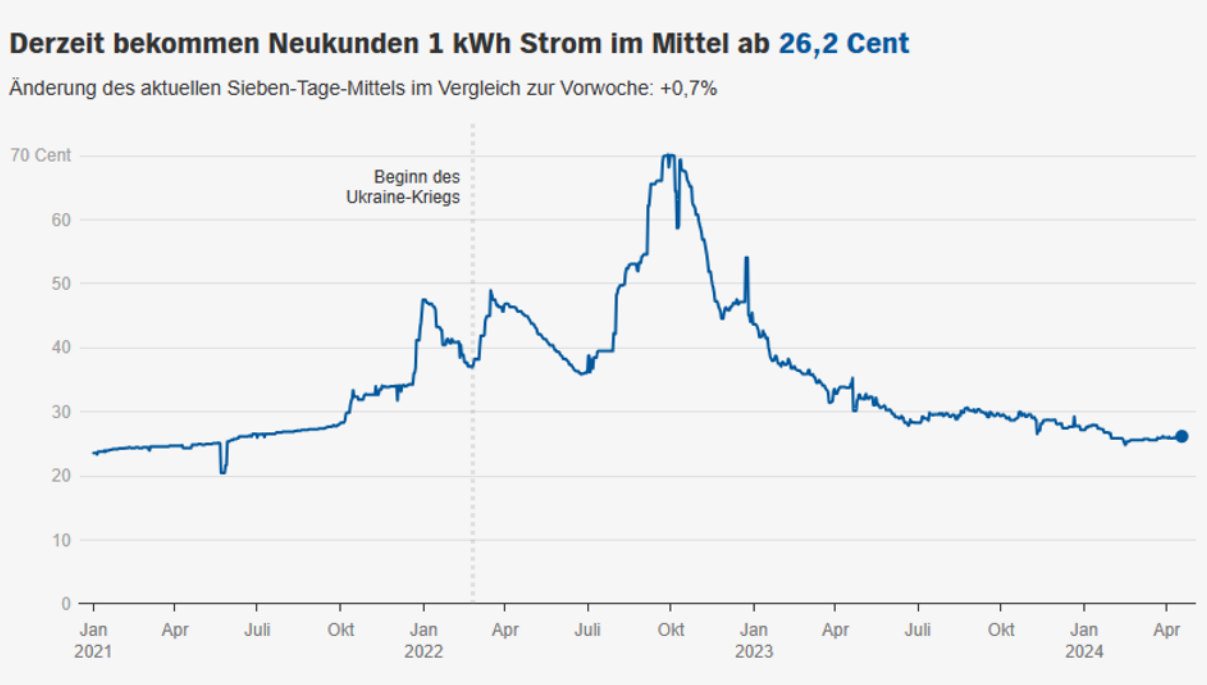


Abbildung 6: Stromkosten

E. Stromkostenberechnung

Stromkosten	**0,26 €/kWh**	**0,00026 €/Wh**
Wattverbrauch	4,13 Wh	0,00107 €
Jahreskosten		9,40 €/Jahr

Tabelle 7: Stromkostenberechnung

F. Lizenzkostenberechnung

	Kosten
Windows 10 Lizenz	50,00 €
Password Depot Server Lizenz	2.658,00 €
Supportkosten 3 Jahre	2.192,85 €
Gesamtkosten	4.900,85 €

Tabelle 8: Lizenzkostenberechnung

[redacted]

G. Kosten bei Schadensfall

	Arbeitszeit in 3 Monaten	Stundenlohn Mitarbeiter
Arbeitszeit pro Mitarbeiter	507 h	
Arbeitszeit gesamt	13.689 h	64,11 €/h
Gesamtkosten		877.601,79 €

Tabelle 9: Kosten bei Schadensfall

H. Konfiguration der VM

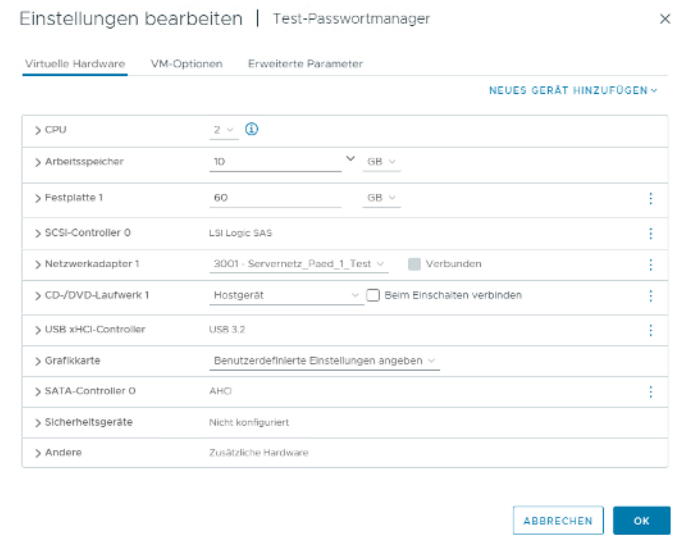


Abbildung 7: Konfiguration der VM

I. Allgemeine Konfiguration

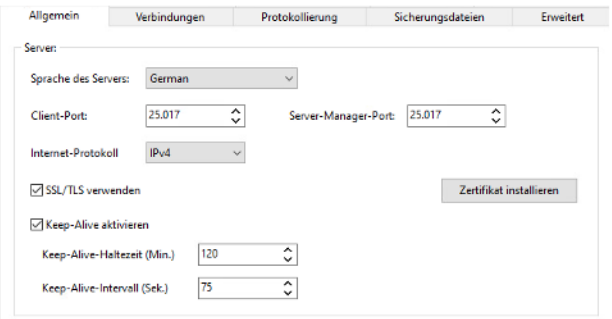


Abbildung 8: Allgemeine Konfiguration

J. Konfiguration der Verbindungen

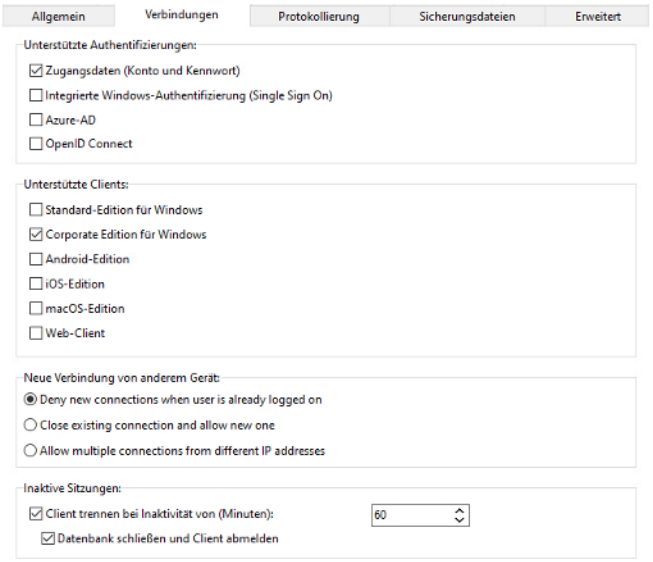


Abbildung 9: Konfiguration der Verbindungen

K. Sicherung der Config-Datei

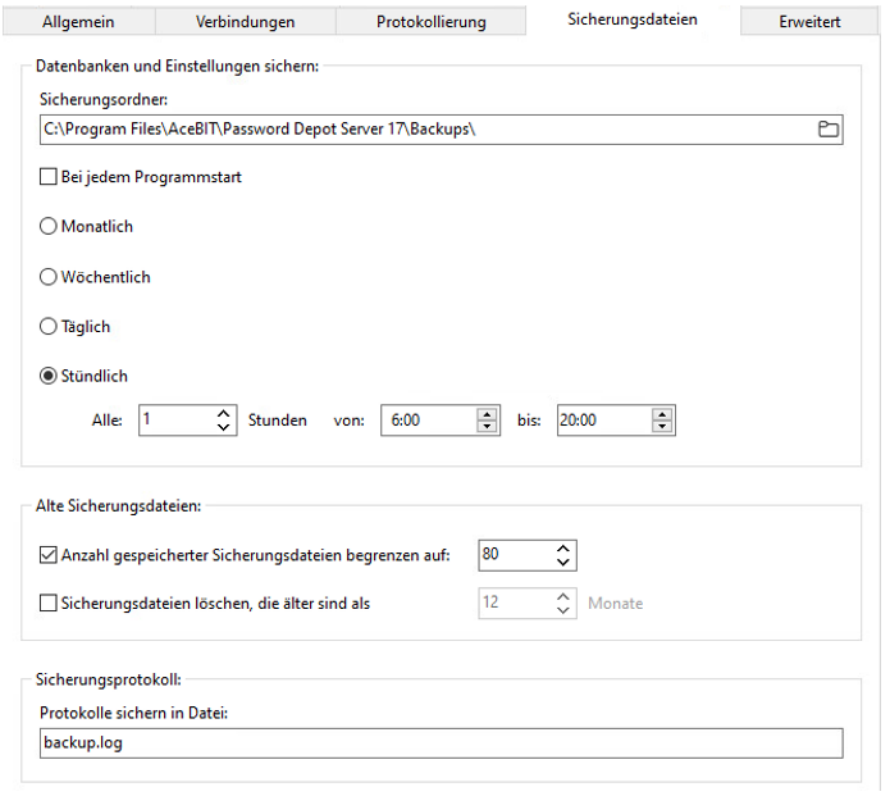


Abbildung 10: Sicherung der Config-Datei

[redacted]

L. Erweiterte Servereinstellungen

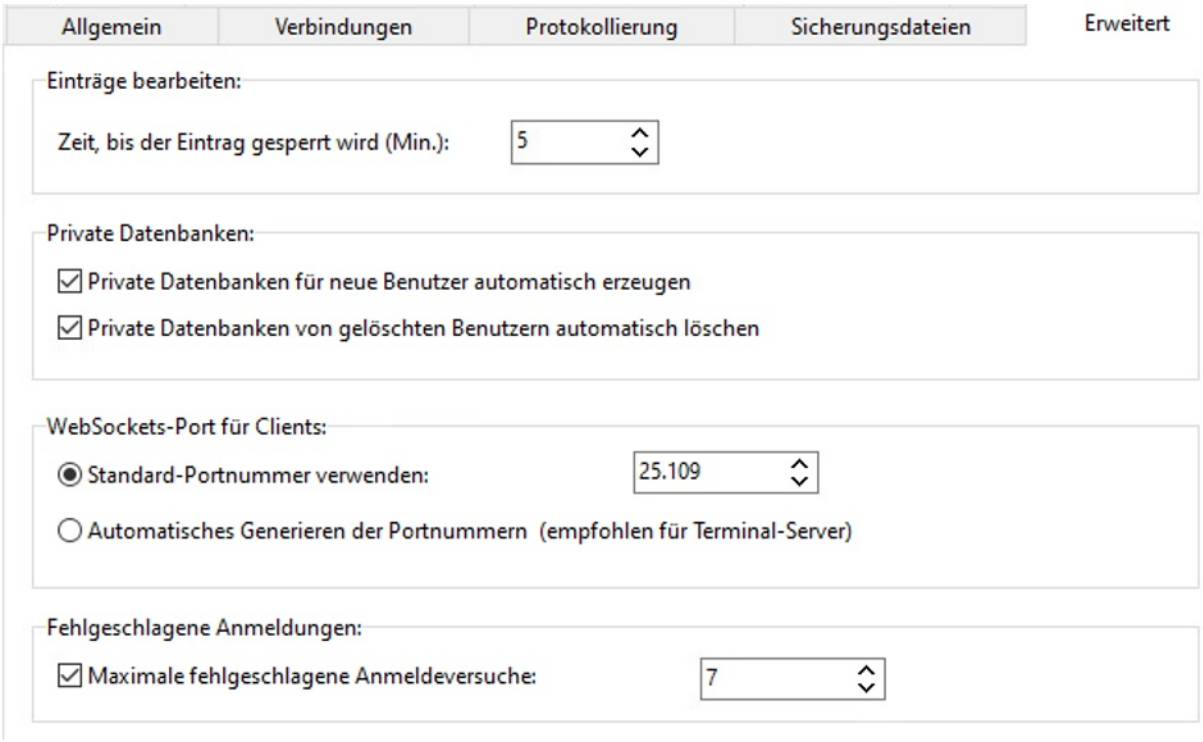


Abbildung 11: Erweiterte Servereinstellungen

M. Konfiguration des TOTP

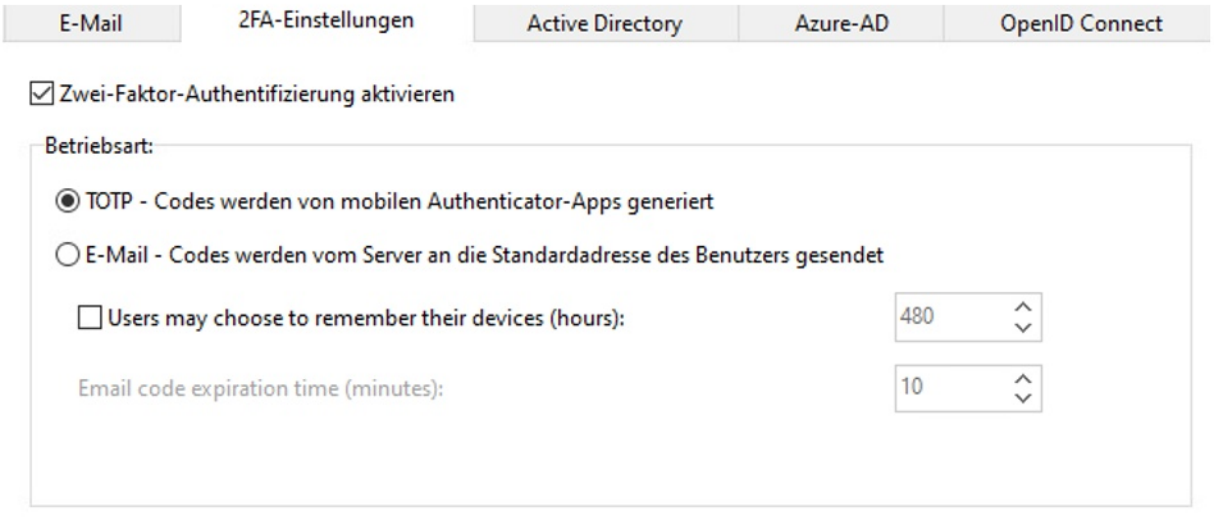


Abbildung 12: Konfiguration des TOTP

[redacted]

N. Konfiguration der Passwortrichtlinien

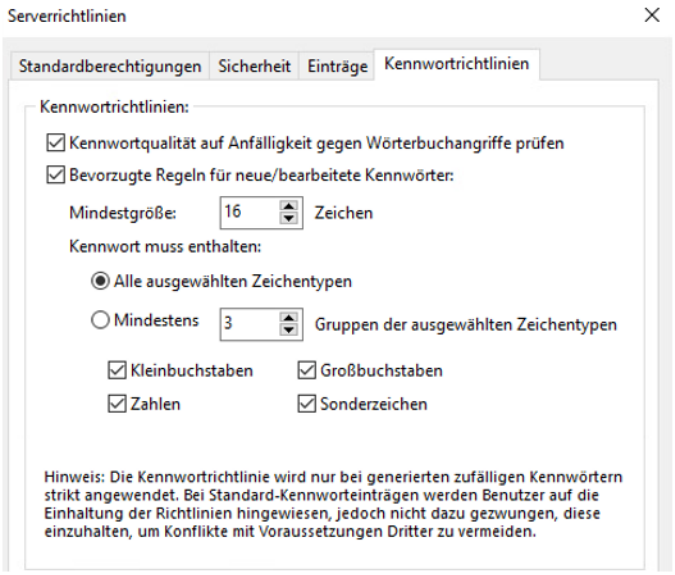


Abbildung 13: Konfiguration der Passwortrichtlinien

O. Konfiguration der Einträge

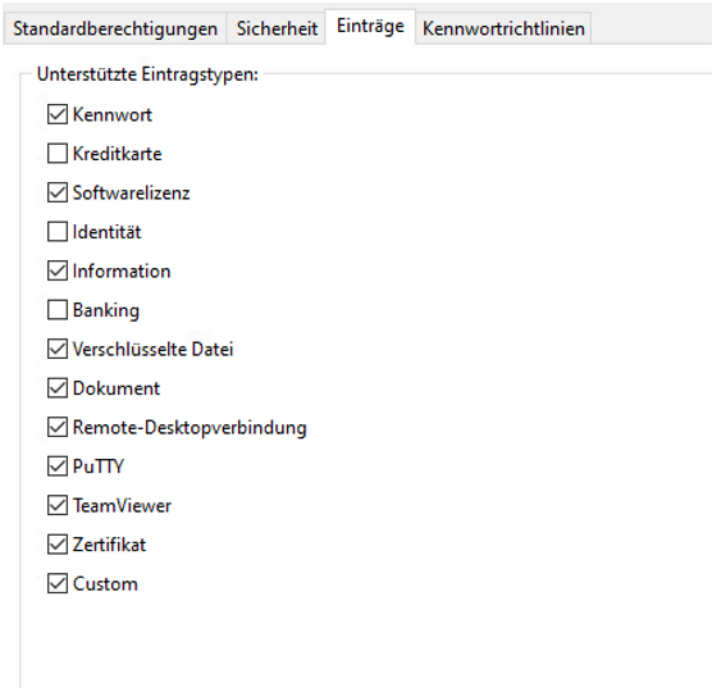


Abbildung 14: Konfiguration der Einträge

[redacted]

P. Konfiguration der Client Passwortrichtlinien

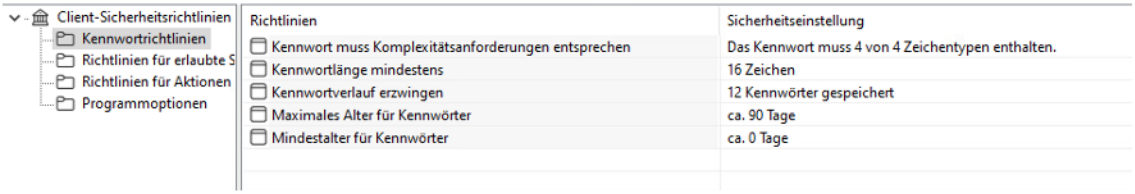


Abbildung 15: Konfiguration der Client Passwortrichtlinien

Q. Konfiguration der Programmoptionen der Clients

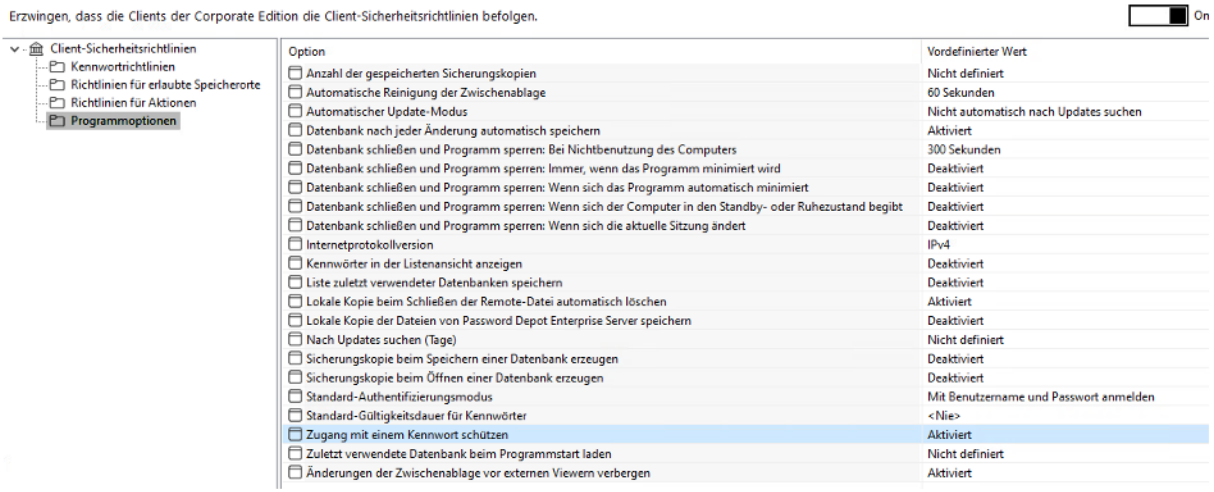


Abbildung 16: Konfiguration der Programmoptionen der Clients

R. Konfiguration der Aktionen der Clients



Abbildung 17: Konfiguration der Aktionen der Clients

[redacted]

S. Konfiguration der Client Speicherorte

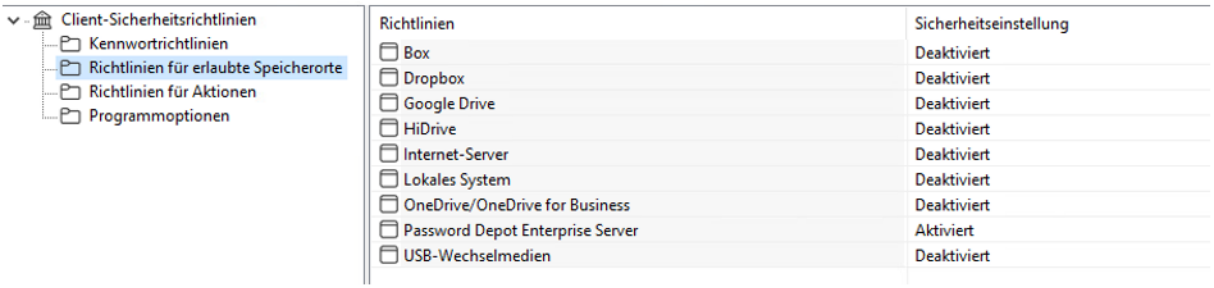


Abbildung 18: Konfiguration der Client Speicherorte

T. Password Depot Angebot

PASSWORD DEPOT BY AceBIT

AceBIT GmbH • Holzhofallee 15 • D-64295 Darmstadt

[redacted]

Angebots-Nr. [redacted]
Datum 28.03.2024

Ihre Kundennummer [redacted]
Ihr Ansprechpartner [redacted]

Angebot Q-23-003798

Pos.	Beschreibung	Menge	Einzelpreis	Gesamtpreis
1.	**Password Depot Enterprise Server 17, 30 Benutzer** In diesem Preis sind alle Clients für alle Betriebssysteme und das Web-Interface enthalten.	1 Stk	2.233,61 EUR	2.233,61 EUR
2.	**Softwarewartung (3 Jahre)** Die Softwarewartung sichert 3 Jahre ab Kaufdatum alle neuen Hauptversionen ohne weitere Kosten zu.	1 Stk	1.842,73 EUR	1.842,73 EUR
	Summe Positionen			4.076,34 EUR
	GOV			40% (1.630,54 EUR)
	Gesamtbetrag netto			2.445,81 EUR
	zzgl. Umsatzsteuer 19%			464,70 EUR
	Gesamtbetrag brutto			**2.910,51 EUR**

Die Gültigkeit dieses Angebotes beträgt 30 Tage. Dieses Angebot wurde automatisch anhand Ihrer Angaben erstellt. Es ist somit freibleibend. Änderungen und Irrtümer vorbehalten.

Abbildung 19: Password Depot Angebot

[redacted]

U. Betriebsdokumentation

Administrator Dokumentation zum Password Depot Server

1.Administrator Kennwort

Das Administratorpasswort für die VM als auch für den Administrator Zugang des Password Depot Servers ist im Tresor [redacted] auf einem Zettel hinterlegt.

2.Servereinstellungen verwalten

Die generellen Einstellungen finden Sie in der oberen rechten Ecke unter „Verwalten“.



Wenn Sie auf „Verwalten“ klicken, bekommen Sie ein Drop-down-Menü, um die generellen Servereinstellungen zu verwalten.

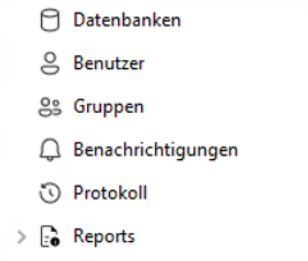
3.Server neustarten

Um den Server neu zu starten, müssen Sie oben rechts auf „Verwalten“ klicken und dann auf „Neu starten“ klicken.

4.Datenbanken Verwalten

4.1 Datenbank erstellen

Um eine Datenbank zu erstellen, klicken Sie auf „Datenbanken“ links in der Spalte.



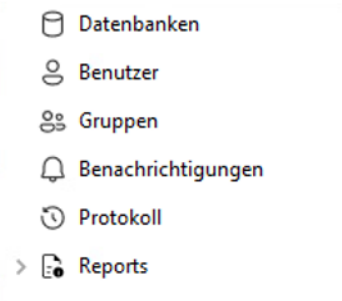
Dann drücken Sie rechts in der Spalte auf „Neue Datenbank“.



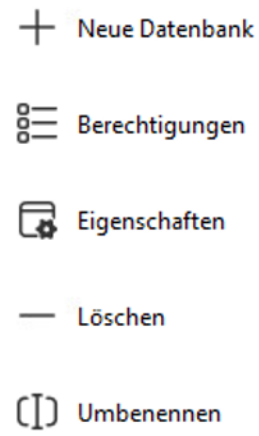
Jetzt klicken Sie auf „Neue Datenbank erzeugen“ geben den Namen der Datenbank in das Feld „Dateiname“ und drücken auf den Knopf „OK“.

4.2 Berechtigungen der Datenbank setzen

Als erstes klicken Sie links in der Spalte auf „Datenbanken“.

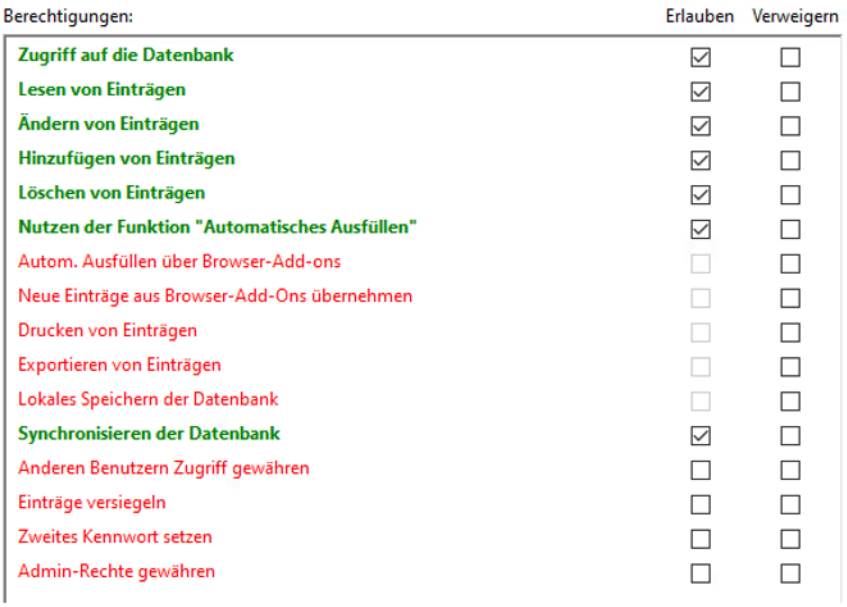


Dann klicken Sie auf die gewünschte Datenbank. Nun klicken Sie in der linken Spalte auf „Berechtigungen“.



Nun klicken Sie rechts auf die Schaltfläche „Neu“, um neue Berechtigungen für die Datenbank zu erstellen.

Nun wählen Sie den Benutzer oder die Gruppe in der Tabelle aus. Rechts können Sie nun die Rechte für den Benutzer oder die Gruppe verwalten.



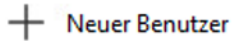
Wenn Sie fertig sind, klicken Sie auf „OK“.

5. Benutzer verwalten

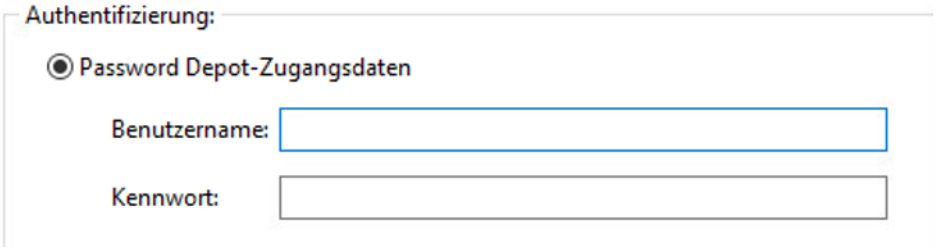
Um die Benutzer zu verwalten, müssen Sie als erstes links auf „Benutzer“ klicken.

5.1 Benutzer anlegen

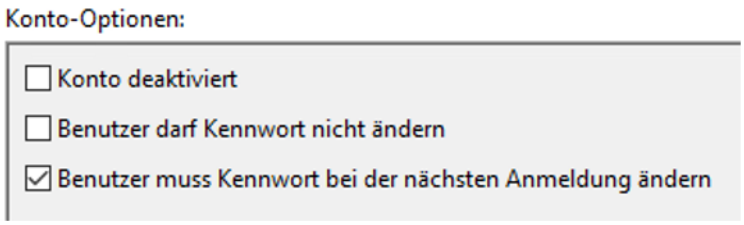
Um einen Benutzer neu anzulegen, klicken Sie rechts auf „Neuer Benutzer“.



Danach klicken Sie im Feld Authentifizierung auf Password Depot-Zugangsdaten und vergeben dem Benutzer einen Benutzernamen und ein Passwort.



Als nächstes setzen Sie unter Konto-Optionen bei dem Kästchen „Benutzer muss Kennwort bei der nächsten Anmeldung ändern“ den Haken.

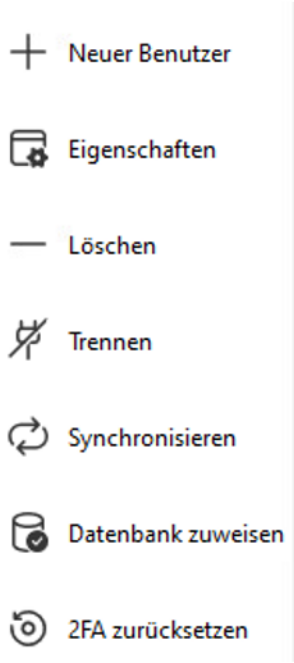


[redacted]

Nun klicken Sie auf die Schaltfläche „OK“ und der Benutzer wird angelegt.

5.2 Benutzer Eigenschaften ändern

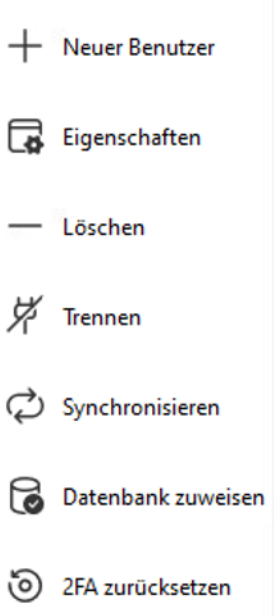
Klicken Sie auf den gewünschten Benutzer. Dann klicken Sie rechts in der Spalte auf Eigenschaften.



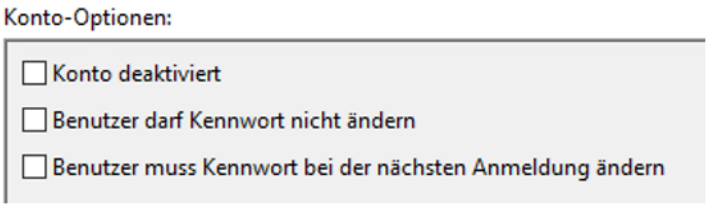
Nun können Sie die Eigenschaften des Benutzers verwalten.

5.3 Konto aktivieren

Klicken Sie auf den Benutzer. Dann klicken Sie rechts in der Spalte auf Eigenschaften.

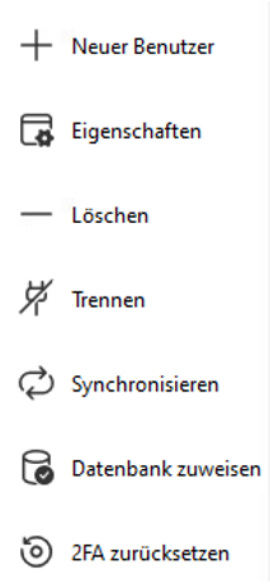


Nun entfernen Sie den Haken bei „Konto deaktiviert“.

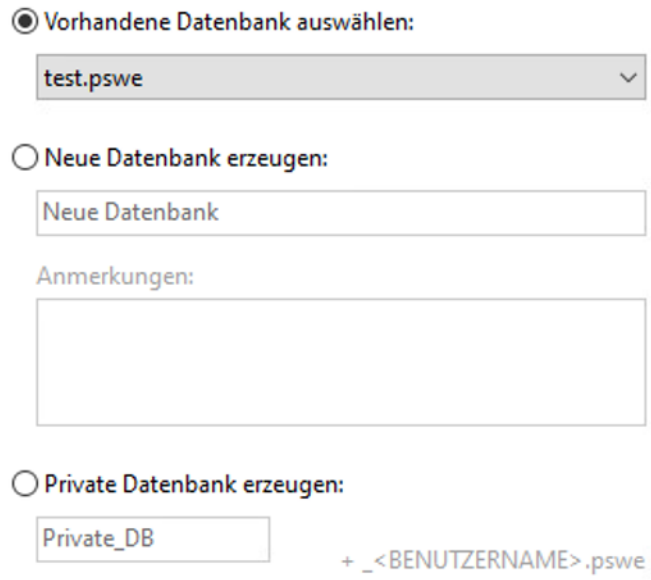


5.4 Datenbank zuweisen

Um den Benutzer eine Datenbank zuzuweisen, klicken Sie auf den jeweiligen Benutzer. Dann klicken Sie rechts in der Spalte auf „Datenbank zuweisen“.



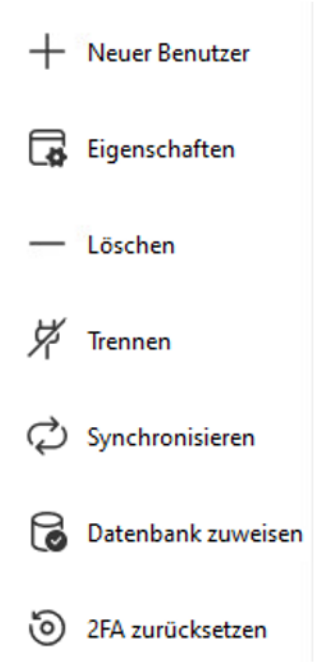
Hier können Sie nun auswählen, ob Sie eine vorhandene Datenbank auswählen wollen, eine neue Datenbank erzeugen wollen oder eine neue private Datenbank erzeugen wollen.



Oben im Reiter können Sie auf „Rechte“ klicken und dort die gewünschten Rechte für die Datenbank setzten. Mit einem Klick auf „OK“ werden die Rechte für die Datenbank gespeichert.

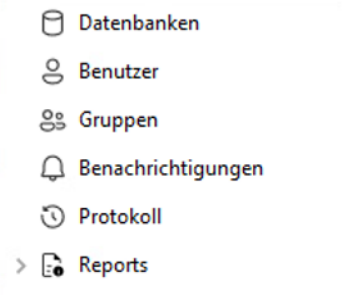
5.5 Benutzer Trennen

Klicken Sie auf den gewünschten Benutzer. Nun klicken Sie rechts in der Spalte auf „Trennen“.



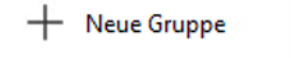
6. Gruppen verwalten

Um die Gruppen zu verwalten, klicken Sie links auf „Gruppen“.



6.1 Neue Gruppe erstellen

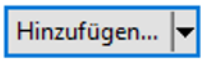
Klicken Sie rechts in der Spalte auf „Neue Gruppe“.



Unter dem Reiter „Allgemein“ können Sie den Namen der Gruppe eingeben.



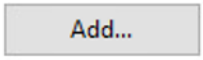
Bei dem Reiter Mitglieder können Sie die Mitglieder hinzufügen, indem Sie unten auf „Hinzufügen…“ klicken.



Nun wählen Sie den Benutzer oder die Gruppe aus und klicken auf „OK“.

Bei Mitglied von können Sie die Gruppen hinzufügen, von der unsere neue Gruppe ein Mitglied wird. Dazu klicken Sie auf die Schaltfläche „Hinzufügen“ und wählen dann die gewünschte Gruppe aus. Dann bestätigen Sie dies mit der Schaltfläche „OK“.

Bei Administrator können Sie die Gruppenadministratoren hinzufügen. Hier klicken Sie auf „Add…“.



Nun wählen Sie den gewünschten Benutzer aus und klicken auf „OK“.

V. Kundendokumentation

Anwenderdokumentation

1. Erste Installation

1.1 Client Installation

Als erstes klicken Sie auf folgenden Hyperlink oder geben Sie dieses in die Browser Suchleiste ein.

https://www.password-depot.de/de/download/download-server.htm

Dort klicken Sie bei der Password Depot Client Corporate Edition auf „Herunterladen“. Laden Sie sich nicht den Password Depot Server herunter.

Doppelklicken Sie auf die „pdepot17CE.exe“, um den Client auf dem Rechner zu installieren. Wählen Sie die Sprache „Deutsch“ aus und klicken auf „OK“. Als nächstes akzeptieren Sie die Lizenzvereinbarungen. Danach klicken Sie auf „Weiter“ bis die Schaltfläche „Installieren“ erscheint.

1.2 Zertifikat Installation

Laden Sie sich die Zertifikate PasswordDepot_CA.crt und PasswordDepot_Server.crt herunter, die Ihnen von Ihrem Administrator geschickt wurden.

Nun starten Sie die Eingabeaufforderung mit Administratorrechten. Dort geben Sie den folgenden Befehl ein: certutil -addstore „ROOT“ 20240424_CA.crt

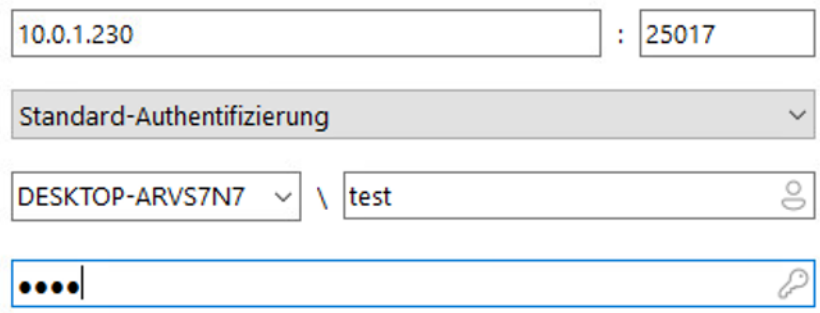
Dieser Befehl installiert das Stammzertifikat.

Um das Serverzertifikat zu installieren, Doppelklicken Sie auf die Datei PasswordDepot_Server.crt klicken sie dann auf „Zertifikat installieren…“. Nun klicken Sie

„Weiter“, bis die Schaltfläche „Fertig stellen“ erscheint und klicken sie auf diesen, um das Zertifikat zu installieren.

1.3 Erstanmeldung

Tragen sie in die Anmeldemaske oben die IP-Adresse des Servers und den Port 25017 ein. Unten tragen Sie ihren Benutzernamen und das Passwort ein, wie in der Abbildung zu sehen ist.

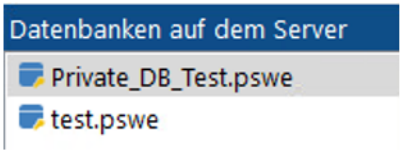


Danach müssen Sie einen TOTP als zweiten Faktor einrichten. Scannen Sie den QR-Code mit der Authentifikator App auf Ihrem Diensthandy. Dann werden Sie aufgefordert, den sechsstelligen PIN einzugeben, den der TOTP erzeugt.

Als nächstes werden Sie aufgefordert, das Passwort zu ändern. Dieses muss mindestens 16 Zeichen lang sein und aus mindestens einer Zahl, einem Sonderzeichen, einem Klein- und einem Großbuchstaben bestehen.

2. Funktion Datenbank switchen

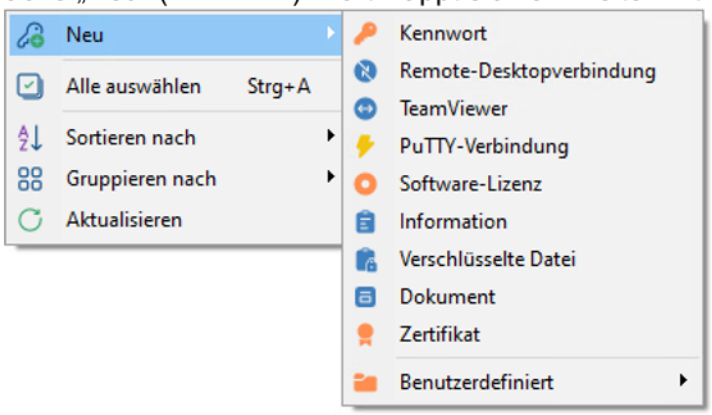
Unten links werden die Datenbanken angezeigt, auf den Ihr Benutzer Zugriff hat.



Die grau hinterlegte Datenbank ist die momentan geöffnete Datenbank. Doppelklick auf eine der Datenbanken wechselt diese.

3. Neuen Eintrag einstellen

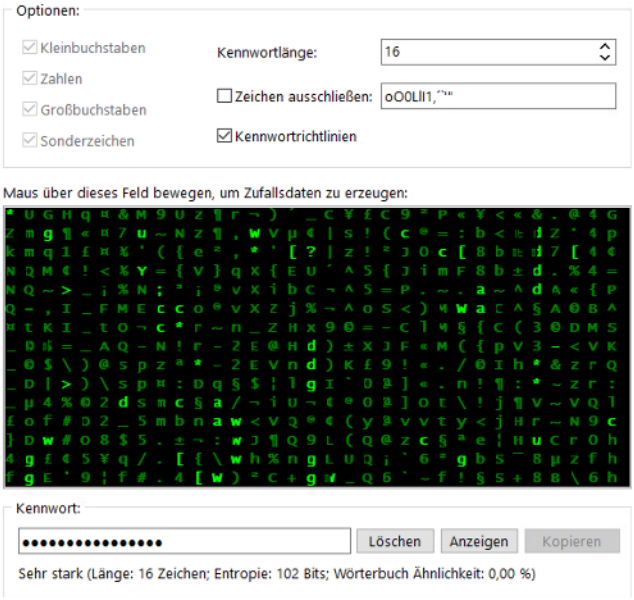
Um einen Eintrag zu erstellen, klicken Sie Rechtsklick auf ein weißes Feld oder auf einen Eintrag und klicken Sie die Schaltfläche „Neu“ (Neu). Dort klappt sich ein Reiter mit



verschiedenen Eintragstypen aus.

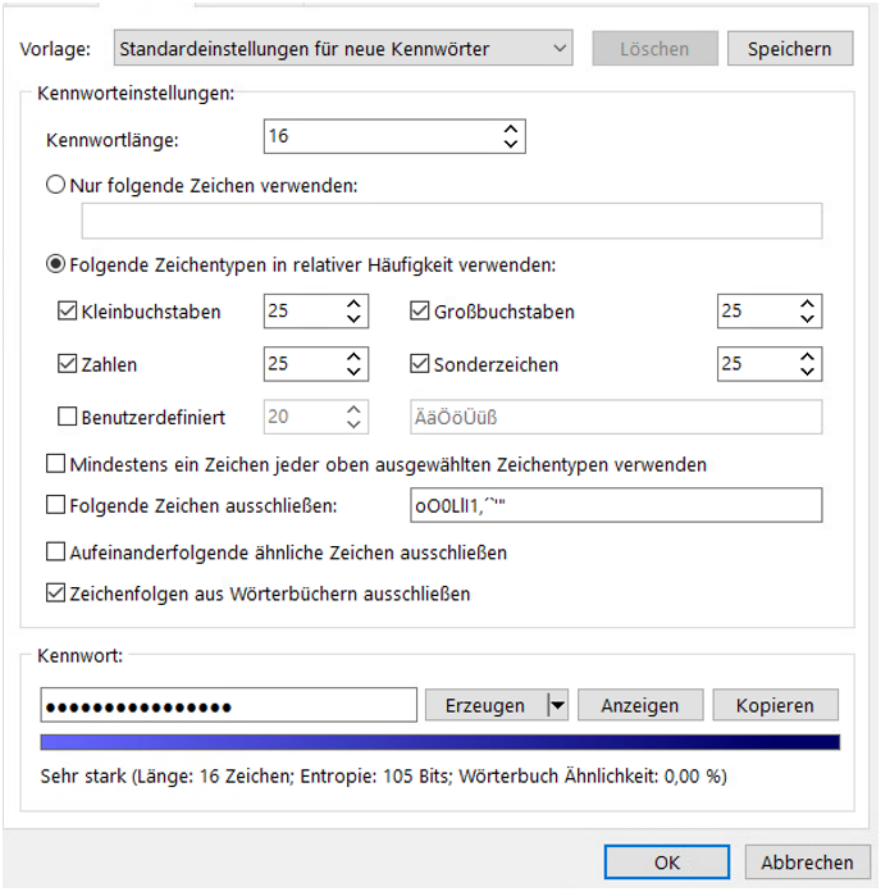
Klicken Sie auf den zu erstellenden Eintrag. Es öffnet sich die Konfiguration des Eintrages. Füllen Sie dieses entsprechend aus. Um den Passwortgenerator aufzurufen, klicken Sie auf dieses Feld am rechten Ende des Passwortfeldes.

Dann öffnet sich der Standardpasswortmanager.



Wenn Sie nun über die sich bewegenden Zeichen mit der Maus bewegen, erstellt der Passwortgenerator ein Passwort.

Sie können jedoch auch den erweiterten Passwortmanager benutzen, indem Sie den Reiter „Erweitert“ auswählen.



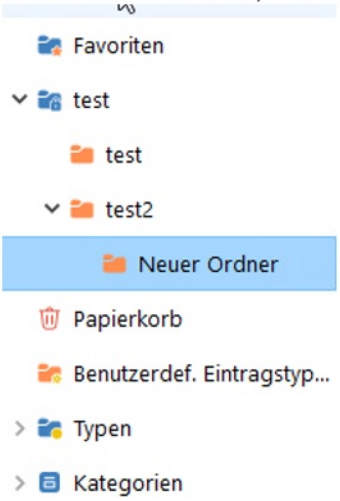
Dort können Sie die eingetragenen Konfigurationen als Vorlage speichern. Dazu klicken Sie nach Eintragen der Konfigurationen oben links auf Speichern. Sie können auch bei dem Drop-down-Menü die Vorlage auswählen, die Sie verwenden möchten.

Wenn Sie unten auf erzeugen klicken, dann wird das neue Passwort erstellt. Beim Klicken auf die Schaltfläche OK wird das Passwort dem Eintrag hinzugefügt.

[redacted]

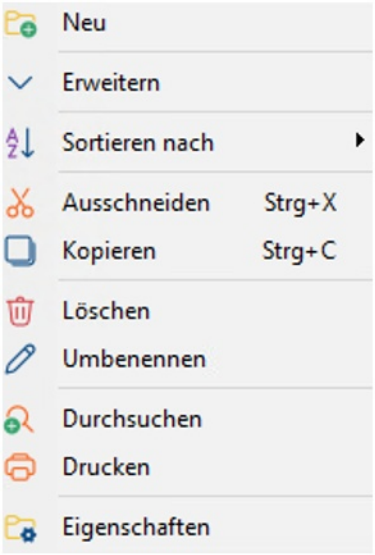
4. Neuen Ordner verwalten

Um die Ordner zu verwalten, müssen Sie auf der rechten Leiste mit den Ordnern Rechtsklick



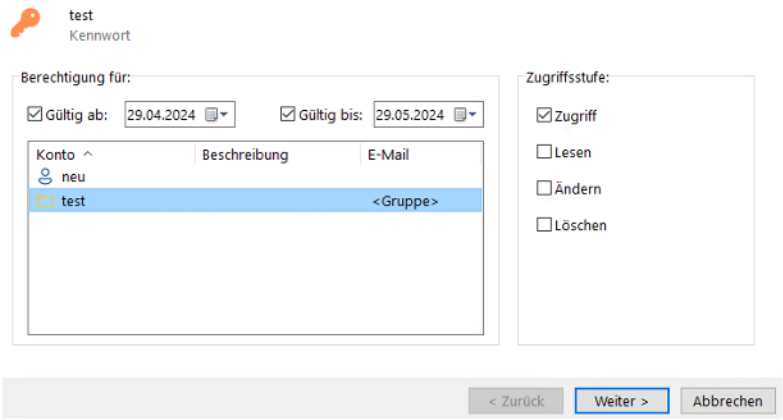
drücken.

Dann erscheint eine Auswahl von Aktionen. Diese sind der nachfolgenden Abbildung zu entnehmen.



5. Einträge teilen

Um einen Eintrag zu teilen, müssen Sie oben auf Eintrag und dann auf Zugriff gewähren, klicken.



Hier können Sie nun einem Benutzer oder einer Gruppe diesen Eintrag zeitlich freischalten. Sie können auf der rechten Seite die Rechte Zugriffsrechte anpassen.

6. Schnellauswahlleiste

Auf der oberen Leiste des Passwortmanagers muss auf dieses Symbol geklickt werden.

Dadurch wird die Anwendung zu einer kleinen Schnellleiste oben am Bildschirmrand. In diesem Zustand wird die Anwendung nicht mehr in der Windows Taskleiste angezeigt. Im nächsten Bild wird die Leiste gezeigt.



Mit einem Klick auf dieses Symbol wird der Client wieder im Ganzen angezeigt.

Durch ein Drop-down-Menü in der Leiste sind die Datenbank, der Ordner und der Eintrag auszuwählen. In der Suchleiste kann man nach einem Passworteintrag suchen.

7. Schellauswahlsymbole

Ein neuer Passworteintrag wird erstellt.

Sorgt dafür, dass man in die Bearbeitungseinstellungen des derzeit ausgewählten Passworteintrages aufruft.

Löscht den ausgewählten Passworteintrag.

Der Benutzername des ausgewählten Eintrages wird in die Zwischenablage kopiert.

Kopiert das Passwort in die Zwischenablage.

[redacted]

 Ein benutzerdefiniertes Feld wird in die Zwischenablage kopiert. Falls es mehr als ein benutzerdefiniertes Feld gibt, wird ein Drop-down-Menü zur Auswahl ausgeklappt.

 Hinterlegte Link beim derzeitigen Eintrag wird im Standardbrowser geöffnet.

 Automatische Ausfüllfunktion. Beim Klicken auf das Feld kommt eine Anweisung, wie dieses zu nutzen ist. Folgen Sie der Anweisung.

 Sperrt den Password Depot Client. In unserer Konfiguration wird man dadurch abgemeldet.

 Minimiert den Passwort Depot Client.

 Meldet den Password Depot Client ab.