Oldenburgische
Industrie- und Handelskammer

Projektdokumentation



TBG
Technologie & Bildung GmbH

Implementierung eines Passwort-Managers in die bestehende Serverstruktur mit Integration in die bestehende Active Directory auf einer eigenen virtuellen Maschine

Fachinformatiker – Fachrichtung Systemintegration
15.08.2022 – 19.07.2024

Umschüler:

Holger Fischer
Musterstraße 15
12345 Musterhausen

Praktikumsbetrieb:

Müller & Egerer Bäckerei und Konditorei GmbH
An der Brücke 27
26180 Rastede

Vorwort

Die Umschulung zum Fachinformatiker mache ich schulisch in der TBG Technologie & Bildung GmbH in Roffhausen. Zu dieser Maßnahme gehören, neben der Schule, auch 2 Praktika je 3 Monate, die zwischen dem 10.03.2023 - 16.06.2023 und dem 11.12.2023 – 28.03.2024 bei der Müller & Egerer Bäckerei und Konditorei GmbH durchgeführt wurden. In dieser Zeit ist auch das Projekt entstanden.

Real existierende Namen und Systempfade wurden aus datenschutzrechtlichen Gründen und zum Schutz des Betriebes unkenntlich gemacht. Dies hat jedoch keinerlei Einfluss auf das hier beschriebene Projekt.

Des Weiteren verstehen sich alle genannten Preise Netto in Euro, da Müller & Egerer Bäckerei und Konditorei GmbH vorsteuerabzugsberechtigt ist und die Umsatzsteuer einen durchlaufenden Posten darstellt.

Kursiv geschriebene Wörter werden in dem Glossar näher erläutert.

Auf das Erläutern von einfachen Fachbegriffen wird verzichtet, da sich diese Projektdokumentation an fachlich versierte Personen richtet.

Inhaltsverzeichnis

I Abkürzungsverzeichnis i
1. Beschreibung 1
1.1. Persönliche Vorstellung 1
1.2 Praktikumsbetrieb 1
1.3 Projektumfeld 1
1.4 Ziel 1
1.5 Ansprechpartner 1
1.6 Definition Passwort-Manager 2
1.6.1 Vorteile eines Passwort-Managers 2
2. Vorbereitungsphase 3
2.1 Zeitplanung 3
2.2 Ist-Analyse 3
2.3 Soll-Konzept 4
2.4 Vergleich der Passwort-Manager 5
2.5 Kosten pro User-Lizenz 7
2.6 Nutzwertanalyse 7
2.7 Entscheidungsprozess 8
2.7.1 Vergleich 8
2.7.2 Entscheidung 8
3. Hardware und Budget 8
3.1 Hardwareanforderungen vom Hersteller 8
3.2 Personalkosten 8
3.3 Kostenaufstellung 8
4. Installation 9
4.1 VM einrichten 9
4.2 Verbinden mit der Active Directory 9
4.3 Portfreigabe 10
4.4 Docker 10
4.5 Bitwarden 11
4.6 Neustart Installation 11
4.7 Fehler die Behoben wurden und öffnen von Bitwarden 12
4.8 Integration in die AD 12
4.9 Richtlinien 13
4.10 Datensicherung 14
5. Endphase 14

5.1 Testphase 14
5.2 Nach der Testphase/ Ausschau auf die Zukunft 14
6. Abschluss 15
6.1 Rechnung 15
6.2 Soll-Ist-Vergleich Zeitplan 15
6.3 Kundendokumentation 15
6.4 How-To 15
6.5 Fazit 15
II Glossar i
III Anhang ii
Netzwerkplan ii
Vergleich: Online oder on-premise iii
Detaillierte Zeitplanung iii
How-To (Ausschnitt) iv
Kundendokumentation (Auszug) vi
Protokoll Datensicherung viii
Angebot ix
Rechnung xi
Quellen xviii

Abbildungsverzeichnis

Abbildung 1 Synchronisationseinstellungen 13
Abbildung 2 Konfiguration der VM xii
Abbildung 3 Installation Ubuntu xii
Abbildung 4 Umbenennen des Hostname xiii
Abbildung 5 Prüfen des DNS xiii
Abbildung 6 Einfügen und Testen der Kerberus Konfig xiii
Abbildung 7 Integration in AD xiii
Abbildung 8 Integration AD Prüfung xiv
Abbildung 9 Test Installation Docker xiv
Abbildung 10 Installation Bitwarden xv
Abbildung 11 DNS Weiterleitung xvi
Abbildung 12 Portfreigabe Firewall xvi
Abbildung 13 Einrichten Konto xvi
Abbildung 14 Bitwarden Richtlinien Organisation xvii

I Abkürzungsverzeichnis

SSO
Single Sign-on
SSO ermöglicht es, sich mit einem sicheren Anmeldungsverfahren auf mehreren Anwendungen und Websites anzumelden. Die Anwendungen „Vertrauen“, meist über Zertifikate, einem Identitätsanbieter. Sobald eine Person sich dort anmeldet, wird dieses Zertifikat „signiert“ und an den Anwendungsanbieter gesendet. Somit weiß diese dann, dass die Person „identifiziert“ wurde und gibt den Zugriff frei.

MFA
Mehr-Faktor-Authentifizierung
Die MFA erfordert von dem User eine zweite Bestätigung der Identität. Dies kann über eine zweite unabhängige App, per E-Mail oder auch per Handynummer, z. B. mit einem Pin, erfolgen. Dadurch wird es unautorisierten Nutzern schwerer gemacht, sich anzumelden und Zugriff zu diesen teils sensiblen Daten zu erlangen.

SCIM
System for Cross-domain Identity Management
SCIM ist ein offener Standard zur automatisierten Bereitstellung von Benutzerkonten.
Es ermöglicht, per einheitlichem Protokoll, Benutzerinformationen von z. B. der Active Directory zu importieren. Es gibt jedem Feld einen Namen. Z. B. die Straße hat den Feldnamen „Straße“ und jede SCIM-fähige Anwendung kann somit automatisch richtig ausgefüllt werden, egal welche Position welches Feld belegt. Damit ist das Ausfüllen und Importieren von Daten automatisiert und vereinfacht.

VPN
Virtual Private Network
VPN ist eine Netzwerkverbindung, die von anderen nicht einsehbar ist. Sie baut eine direkte „Tunnelverbindung“ mit dem gewünschten Server auf, ohne dass es über andere Anbieter läuft. Wie ein Tunnel in einem Berg. Die VPN ist der Tunnel und der „normale“ Verbindungsaufbau ist ein Weg über den Berg.

MDM
Mobile Device Management
MDM steht für die zentralisierte Verwaltung von mobilen Geräten mit der Möglichkeit der Fernwartung durch einen Administrator.
Eine MDM-Anwendung wie z. B. Miradore oder Intune ist ein Programm, womit der Administrator eine einheitliche Einrichtung für viele Geräte gleichzeitig durchführen kann. Zudem ist damit eine Fernwartung ermöglicht, womit das mobile Gerät aktualisiert oder sogar gesperrt werden kann.

NAS
Network Attached Storage
Ist ein mit dem Netzwerk verbundener Speicher, um Daten zentral zu sichern und zu speichern.

DSGVO
Datenschutzgrundverordnung
Die DSGVO ist eine Regelung der Europäischen Union und beschreibt, wie Unternehmen, mit den persönlichen Daten der Mitarbeiter und Kunden umzugehen haben.

1. Beschreibung

1.1. Persönliche Vorstellung

Im Folgenden stelle ich mich und meinen Praktikumsbetrieb, der mir die Möglichkeit gab das Projekt durchzuführen, vor.

Mein Name ist Holger Fischer, geboren am 01.01.1970 in Musterdorf, und ich wohne derzeit in Musterhausen. Meine schulische Umschulung zum Fachinformatiker – Fachrichtung Systemintegration absolviere ich seit dem 15.08.2022 bei der TBG Technologie & Bildung GmbH (kurz TBG) in Roffhausen.

Mein Praktikum mache ich in der Handwerksbäckerei Müller & Egerer Bäckerei und Konditorei GmbH (kurz M&E) am Zentralstandort in Rastede.

1.2 Praktikumsbetrieb

Die Müller & Egerer Bäckerei und Konditorei GmbH ist ein mittelständisches, inhabergeführtes Handwerksunternehmen in der Lebensmittelindustrie, welches 1948 gegründet wurde. Das Unternehmen beschäftigt mehr als 800 Mitarbeiter, verteilt auf mehr als 65 Filialen, Produktion und Verwaltung.

1.3 Projektumfeld

Das Projekt wird in der Zentrale von M&E in Rastede Leuchtenburg durchgeführt.

1.4 Ziel

Für die Verwaltung ist geplant, einen einheitlichen und für das Unternehmen kontrollierbaren Speicher von Passwörtern einzuführen. Hierfür soll ein Passwort-Manager auf einem dedizierten Server implementiert und in das bestehende System über die Active Directory integriert werden.

Das Ziel ist es, dass alle Mitarbeiter hinsichtlich ihrer Passwörter auf dem gleichen Stand sind. So soll zentral ein Passwortspeicher integriert werden, in dem Mitarbeiter in Gruppen eingeteilt werden, über welche die Berechtigungen des Mitarbeiters zugewiesen werden. Dies wird im Zusammenhang mit der Active Directory umgesetzt, aus der die relevanten Daten übertragen werden. So kann gesagt werden, welcher Mitarbeiter Zugang zu welchen Gruppen zusätzlich zum eigenen Tresor erhalten darf.

Die Verwaltung des Managers und der Zugriffsrechte soll zentral durch die IT-Abteilung erfolgen, die über entsprechende Berechtigungen verfügt.

1.5 Ansprechpartner

TBG:
Herr Michael Schmohl
Olympiastr. 1 (Geb. 1)
26419 Schortens
Telefon [redacted]
E-Mail: [redacted]

M&E:

Herr Rolf Döscher
Position: Leitung IT
[redacted]

1.6 Definition Passwort-Manager

Ein Passwort-Manager, auch bekannt als Kennwort- oder Passwortverwaltung, ist eine Softwareanwendung und Sicherheitsmaßnahme, mit deren Hilfe ein Benutzer Zugangsdaten zentral und verschlüsselt speichern kann. Diese Anwendung automatisiert den Prozess der Passwortverwaltung und spart letztendlich die Zeit des Passwortsuchens, da alles an einem Ort und aktuell ist.

Passwort-Manager arbeiten meist mit verschlüsselten Datenbanken und werden erst auf dem Endgerät des Benutzers entschlüsselt, um höchste Sicherheit für die gespeicherten Daten zu gewährleisten.

Es ähnelt einem Tresor: Man erstellt ein neues Passwort und speichert es in diesem »Tresor« ab. Wenn das Passwort nun benötigt wird, öffnet man den Tresor mit einem Masterpasswort und kopiert den benötigten Inhalt, auch so, dass das Passwort nicht im Klartext angezeigt wird.

Es gibt zwei Arten von Passwortmanagern. Zum einen gibt es die Offline-Variante, bei der der Tresor lokal auf dem Endgerät gespeichert ist und nur von dort aus zugänglich ist. Der Vorteil davon ist, dass die Passwörter auch ohne Internetverbindung verfügbar sind, aber die Passwörter sind nur auf dem einen Gerät verfügbar. Sollte dieses ausfallen und es gibt kein Backup, sind die Daten verloren. Die andere Variante ist die Online-Variante, bei der der Tresor auf einem Server oder in der Cloud gespeichert wird. Der Vorteil dabei ist, dass man von überall aus Zugriff darauf hat und dass die Daten auf allen unterstützten Endgeräten synchronisiert werden. Ein Nachteil besteht jedoch darin, dass es anderen auch ermöglicht, Zugriff darauf zu haben, wenn sie das Masterpasswort kennen oder kompromittiert haben.

1.6.1 Vorteile eines Passwort-Managers

Passwortmanager bieten die Funktion eines Passwortgenerators, mit dem sichere und schwer zu erratende Passwörter erstellt werden können. Menschen fallen bei der Erstellung von Passwörtern immer in Muster, selbst wenn sie es nicht beabsichtigen, und diese Muster sind leicht erkennbar. Vor meiner Recherche und Implementierung verwendete ich zum Beispiel Passwörter, die für Dritte, die mich ein wenig kannten, leicht zu knacken waren. So wie mein Lieblingsfußballverein, mein Lieblingstier oder mein Geburtsjahr. Selbst wenn die über eine ausreichende Länge verfügten, war ein Muster leicht zu erkennen.

Selbst wenn eine Person scheinbar "zufällig" auf Tasten auf der Tastatur drückt, entsteht unbewusst ein Muster. Zum Beispiel sieht "PaF438o" auf den ersten Blick zufällig aus, aber bei genauerem Hinsehen erkennt man darin leicht "Premium Aerotec Flugzeug A380". Ein Passwort-Generator hingegen hat solche Probleme nicht. Er generiert Passwörter, die "komplett" zufällig sind.

Die Nutzer eines Passwort-Managers müssen sich nur das Masterpasswort merken, mit dem sie Zugriff auf ihre Passwörter erhalten. Dadurch kann das Masterpasswort schwieriger und länger sein, da es einfacher ist, ein komplexes Passwort zu merken als viele einfache Passwörter. In einem Unternehmen mit Passwortmanager müssen Mitarbeiter ihre geforderten Passwörter nicht mehr aufschreiben und möglicherweise an leicht zugänglichen Orten liegen lassen, was eine erhebliche Sicherheitslücke schließt.

Darüber hinaus sorgt der AES-256-Bit-Verschlüsselungsstandard, den führende Passwortmanager verwenden, für Sicherheit. Dieser Standard wurde vom US-Militär als Standard etabliert und gilt derzeit als "unknackbar". Ein moderner Quantencomputer bräuchte länger, als das Universum existiert, oder die Sonne Brennstoff hat, um die Verschlüsselung zu knacken. Es gibt theoretische Angriffsmöglichkeiten, die aber in der Praxis nicht durchgeführt werden können, da die Bedingungen nicht vorherrschen oder die Dauer „nur“ um ein paar Tausend Jahre verkürzt wird. Die einzige, heutige Möglichkeit, die Passwörter zu kompromittieren, ist ein Brute-Force-Angriff, um das Passwort direkt herauszufinden. Voraussetzung für die Sicherheit dort ist, dass man ein Passwort mit einer Kombination aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen, ohne einfache Muster wie Buchstabenkombinationen (z. B. QWERTZ) oder Zahlenreihen (z. B. 1234) oder Wörtern (z. B. Haus, Maus) verwendet. Die Länge des Passworts spielt ebenfalls eine wichtige Rolle. Ein 14-stelliges Passwort ist sicherer als ein 5-stelliges Passwort.

Ein solches sicheres Passwort kann einfach und automatisch mit einem Passwort-Generator erstellt werden und bietet somit vollständige Sicherheit.

2. Vorbereitungsphase

2.1 Zeitplanung

Für die Durchführung des Projekts sind 40 Stunden eingeplant und wurden wie folgt aufgeteilt:

Aufgabe	Zeit in h
Analyse	**5**
Planung/Konzeptionierung	**7**
Durchführung	**16**
Testphase	**3**
Abschluss	**9**
Gesamt	**40**

Eine ausführliche Aufteilung befindet sich im Anhang in Detaillierte *Zeitplanung*.

2.2 Ist-Analyse

Zurzeit gibt es keine einheitliche Lösung in der Zentrale um Passwörter zu speichern. Aktuell werden Passwörter von jedem Mitarbeiter unterschiedlich abgespeichert. Einige, wie z.B. in der IT-Abteilung benutzten KeePass, andere schreiben sich die Passwörter in eine Textdatei oder auf einem Zettel auf.
Die Passwörter sind in der Active Directory hinterlegt. Sollte ein Mitarbeiter das Unternehmen verlassen, wird sein Benutzter Konto gesperrt und nach einiger Zeit gelöscht. Damit ist es dem Mitarbeiter nicht mehr möglich sich mit seinen Anmeldedaten anzumelden. Aber die Shared-Mailbox steht ohne weitere Authentifizierung zur Verfügung und es sind lediglich Freigaben erforderlich.
Sollten böswillige Dritte Zugang zum System erlangen, könnten Unternehmen erhebliche Konsequenzen erwarten. Von einem möglichen Ausfall der IT-Infrastruktur von bis zu wenigen Tagen, was zu bedeutenden Einschränkungen des Geschäftsbetriebs führen könnte, bis hin zum Verlust der wirtschaftlichen Existenz, abhängig von der Menge der kompromittierten Daten.

Jeder Mitarbeiter in der Verwaltung benutzt im Durchschnitt 10 Anwendungen, die Passwörter erfordern und wahrscheinlich verwendet er für mehrere Konten dasselbe Passwort, welches er möglicherweise auch im privaten Bereich benutzt. Viele Mitarbeiter verwenden zusätzlich ihre M&E-E-Mail-Adresse auch privat. Wenn in einem solchen Fall die Zugangsdaten kompromittiert werden, haben Dritte Zugriff auf viele geschäftskritische Anwendungen des

Unternehmens. Oft werden die Passwörter sogar auf Papier notiert oder in einfachen Word-Dateien gespeichert, was sie leicht zugänglich macht, sobald jemand Zugriff auf die Computer bekommt.

Ein weiteres Problem besteht bei Änderungen von Passwörtern. Wenn diese verändert werden, werden die Kollegen, die damit arbeiten, per Teams oder Mail darauf hingewiesen. Danach steht jeder Mitarbeiter selbst in der Verantwortung, dass er die Passwörter aktuell hält. Dies führt aber häufig zu Problemen, da diese oft nicht mehr auf dem aktuellen Stand sind. Somit ist ein reibungsloses Arbeiten nur schwer möglich.
Das Unternehmen besitzt einen Server-Cluster, auf den die verschieden Dienste per virtueller Maschine laufen. Die Mitarbeiter greifen vom internen Firmennetz auf diese Dienste zu. Die Mitarbeiter, die im Homeoffice arbeiten greifen per VPN auf das interne Netz zu, damit gesichert ist, dass keine Person von außen Zugriff auf die Server hat.
Die Backups werden einmal täglich in 3 Formen ausgeführt. Zum einen auf einer extra dafür gestellten NAS, einer externen Festplatte und in der Cloud.
Das Internet wird mittel Sophos-Router verteilt.
Da nur geplant ist, die Zentrale mit dem Passwortmanager auszustatten, werden die Filialen und ihre Mitarbeiter außen vorgelassen.

Das Projekt wird in einer eigens dafür erstellten Umgebung installiert und getestet und später in der Produktivumgebung umgesetzt, was nicht mehr in der Projektphase passiert.
Diese Testumgebung beinhaltet eine Microsoft Active Directory mit eigener DNS und einem DHCP auf der AD-VM (siehe *Netzwerkplan*)

2.3 Soll-Konzept

In Zukunft sollen die Passwörter zentral auf einem dedizierten Server für alle Mitarbeiter gespeichert werden. Die Verwaltung und Steuerung dieser Zugangsdaten sollen von der IT-Abteilung übernommen werden. Hierfür werden sogenannte Tresore verwendet, in denen den einzelnen Benutzergruppen Zugriffsrechte zugewiesen werden. Diese Zugriffsrechte ermöglichen es, zu steuern, wer wann und wie auf welche Passwörter zugreifen kann. Die Verwaltung dieser Gruppen soll über das Active Directory erfolgen und von dort in den Manager integriert werden.

Des Weiteren soll die IT bei Sicherheitsverstößen wie beispielsweise unsicheren Passwörtern oder Sicherheitslücken automatisch benachrichtigt werden, um schnell und gezielt darauf reagieren zu können.

Beim Ausscheiden eines Mitarbeiters wird über der Active Directory der Benutzer deaktiviert. Der Passwortmanager soll dann die Zugriffsrechte für die Passwörter automatisch entfernen. Wenn Passwörter geändert werden, sollen diese automatisch in den entsprechenden Benutzergruppen synchronisiert werden. Dadurch soll Zeit eingespart werden, da nicht mehr jeder einzelne Mitarbeiter darüber informiert werden muss, dass sich das Passwort geändert hat. Und die Sicherheit soll somit erhöht werden, da Änderungen nicht mehr per z.B. E-Mail verschickt werden.
Um die Aktivitäten auf den jeweiligen Zugangsdaten zu kontrollieren, soll der Passwortmanager ungewöhnliche Aktivitäten loggen und der IT-Abteilung melden.

Für erhöhte Sicherheit soll der Passwort-Manager eine *Zwei-Faktor-Authentifizierung (2FA)* unterstützen. Dadurch soll gewährleistet werden, dass sich Mitarbeiter in der Verwaltung nur in Verbindung mit ihren dienstlichen Mobilgeräten, die in den jeweiligen Konten hinterlegt sind, anmelden können. Dies stellt sicher, dass nur autorisierte Personen Zugriff erhalten.

Zusätzlich soll die *Single Sign-On-Funktion (SSO)* vorhanden sein. Dadurch kann sich ein Mitarbeiter morgens einmal bei einem vertrauenswürdigen Anbieter anmelden und wird danach automatisch und sicher an unterstützten Websites angemeldet. Dies erleichtert den Arbeitsablauf und spart Zeit, da der Mitarbeiter nicht mehrfach seine Zugangsdaten eingeben und suchen muss.

Da das Unternehmen M&E unter anderem das *Apple-Ökosystem* nutzt, benötigt der zukünftige Passwort-Manager eine entsprechende App aus dem App Store für die vorhandenen Geräte, denn bei Arbeitsantritt bekommen viele Mitarbeiter für ihre Zeit im Unternehmen ein iPad gestellt. Viele Mitarbeiter in der Verwaltung erhalten zusätzlich dazu noch ein iPhone als Arbeitshandy. Dies ist allerdings keinen Bestandteil meines Projektes und wird nur bei der Auswahl eine Rolle spielen.
Für dieses Projekt ist geplant, dass jeder mit einem MS365-Business-Premium-Account auch ein Bitwarden-Konto bekommen soll.

Für das Projekt muss noch geklärt werden, ob der Passwort-Manager als *On-Premise*- oder Cloud-Lösung eingesetzt werden soll. Allerdings wird aufgrund der aktuellen IT-Strategie eine *On-Premise*-Lösung bevorzugt. In diesem Fall muss eine neue virtuelle Maschine (VM) eingerichtet werden und den bisher bestehenden Maschinen hinzugefügt werden. Eine wesentliche Voraussetzung ist außerdem die Integration in das Active Directory, da darüber die Benutzerverwaltung erfolgt. (*Netzwerkplan*)

2.4 Vergleich der Passwort-Manager

Bei der Recherche und Benutzung von neuen Programmen ist es von entscheidender Bedeutung, dem ausgewählten Unternehmen einen Vertrauensvorschuss zu geben. Besonders bei Anwendungen, die etwas so Wichtiges wie die Verwaltung und den Schutz von Passwörtern übernehmen, ist es unerlässlich, sicherzustellen, dass alles in bester Ordnung ist und man ohne große Bedenken die jeweilige Anwendung in Anspruch nehmen kann.

Mir war es wichtig, wie bereits erwähnt, dass der Passwort-Manager über einen Passwort-Generator verfügt. Darüber hinaus muss der Manager in der Lage sein, leicht zu erratende oder bereits geleakte sowie doppelte Passwörter zu erkennen und zu melden, die von Kollegen verwendet werden. Dadurch soll verhindert werden, dass bei einem Sicherheitsvorfall weitere Anwendungen kompromittiert werden und Sicherheitslücken so schnell wie möglich geschlossen werden. Aufgrund der Serverpolitik des Unternehmens M&E wäre es von großem Vorteil, wenn diese systemrelevante Anwendung die Möglichkeit des *On-Premise*-Hostings bietet. Sollte dies nicht der Fall sein, muss geprüft werden, wo sich bei der Cloud-Lösung der Serverstandort befindet, um den jeweiligen Datenschutzbestimmungen gerecht zu werden.
Die Sicherheit der Daten der Mitarbeiter ist von großer Bedeutung. Daher ist eine *Zwei-Faktor-Authentifizierung (2FA)* unerlässlich. Dadurch kann sichergestellt werden, dass tatsächlich die jeweilige Person versucht sich anzumelden, und keine unberechtigten Dritten Zugriff erhalten.

LastPass

Während meiner Recherche stieß ich auf einen Sicherheitsvorfall, der im August 2022 stattfand und Folgen im Dezember hatte. Im August wurde der Quellcode von LastPass von einem Geschäftslaptop gestohlen. Im Dezember nutzten Dritte diesen Quellcode, um dadurch Zugriff auf eine große Menge an Kundendaten zu erlangen. Bedauerlicherweise schaffte es LastPass damals nicht, offen und transparent mit ihren Kunden über die begangenen Fehler zu kommunizieren. Dies hat mein Vertrauen in das Unternehmen stark beeinträchtigt und war somit ein Ausschlusskriterium für mich.

Zum Ende der Recherche und auf Anfrage von meinen Kollegen sind folgende Anwendungen in die engere Auswahl gefallen:

KeePass2

KeePass2 ist eine kostenlose *Open-Source*-Freeware, die als Desktopanwendung verfügbar ist. Es bietet wie andere Passwortmanager auch einen Passwortgenerator. Im Wesentlichen handelt es sich bei KeePass um eine verschlüsselte Excel-Liste, die grafisch angepasst wurde. Für individuelle Nutzer mit einem Gerät ist diese Offline-Lösung gut geeignet. Allerdings hilft sie Unternehmen weniger. Sie ermöglicht nur einen Benutzer und bietet keine Möglichkeit, weitere Benutzer oder Unterkonten, ohne den Kauf kostenpflichtiger Erweiterungen hinzuzufügen. Die Daten werden lokal auf dem genutzten Endgerät gespeichert und können daher nicht auf einem Server liegen und von externen Standorten über mehrere Endgeräte verwendet werden. Darüber hinaus besteht durch diesen einen Nutzer entweder die Möglichkeit, alle Daten preiszugeben oder keine Daten herauszugeben. Da es sich um eine Freeware handelt, gibt es vom Hersteller auch keinen aktiven Support.

Bitwarden

Bitwarden bietet für Unternehmen zwei interessante Versionen an: die Teams-Version für 3 $ pro Lizenz und die Enterprise-Version für 5 $ pro Lizenz pro Monat. Beide Versionen sind als Desktop-Anwendung, Web-App, Browser-Erweiterung und als offizielle App im App Store für mobile Geräte verfügbar.
Die Enterprise-Version von Bitwarden bietet einige zusätzliche Funktionen, darunter die Unterstützung von SCIM (System for Cross-domain Identity Management) und SSO (Single Sign-On) an. Der wichtigste Vorteil dieser Version besteht jedoch darin, dass der Passwort-Manager on-premise gehostet werden kann und somit nur von M&E steuerbar ist.
Wie auch die anderen Passwort-Manager verfügt Bitwarden über einen Passwort-Generator, eine Passwortüberwachung und ein Aktivitätenprotokoll. Bitwarden ist gegenüber anderen Passwort-Managern kostengünstiger und bietet den zusätzlichen Vorteil, dass es Open-Source ist. Dies bedeutet, dass der Quellcode eingesehen und bei Bedarf auch angepasst werden kann.

1password

Das kanadische Unternehmen 1Password bietet seine Business-Version für 7,99 $ pro Lizenz an. Dabei stellt es eine Desktop-App, eine Web-App, eine Browser-Erweiterung und eine App im App Store zur Verfügung.
Neben den grundlegenden Funktionen wie dem Passwort-Generator und dem Aktivitätenprotokoll bietet 1Password auch eine Passwortüberwachung an. Für das Teilen von Passwörtern besteht die Möglichkeit, diese direkt an die E-Mail-Adresse des Empfängers zu binden, so dass nur der Besitzer dieser E-Mail-Adresse Zugriff erhält.
Ein besonderes Merkmal von 1Password ist der Reisemodus. Wenn dieser aktiviert ist, werden die Tresore vorübergehend aus der App entfernt. Dies erhöht die Sicherheit für Unternehmen, insbesondere während Reisen oder in Situationen, in denen der Zugriff auf die Tresore vorübergehend eingeschränkt werden soll.
Im Vergleich zu den anderen vorgestellten Passwort-Managern ist 1Password eher teuer. Allerdings bietet es den Vorteil, dass Unternehmen den Serverstandort wählen können. Zur Auswahl stehen die AWS-Server in den USA, Kanada oder der EU in Frankfurt.

Dashlane

Dashlane bietet zwei interessante Versionen für M&E an: die Teams-Version für 5 € pro Lizenz pro Monat und die Business-Version für 8 € pro Lizenz. Die Franzosen stellen eine App im App Store sowie eine Web-App und eine Browser-Erweiterung zur Verfügung.

Die Business-Version von Dashlane bietet im Vergleich zur Teams-Version den zusätzlichen Vorteil von SCIM (System for Cross-Domain Identity Management) und SSO (Single Sign-On). Diese Funktionen erleichtern die Verwaltung von Benutzern und ermöglichen einen nahtlosen Zugriff auf unterstützende Anwendungen.
Neben dem Passwort-Generator und dem Aktivitätenprotokoll, das Warnungen bei Sicherheitsverletzungen und Schwachstellen bietet, hat Dashlane einen weiteren Vorteil: Die Möglichkeit, ein VPN zu aktivieren. Diese Funktion ermöglicht eine sichere Verbindung zum Internet und schützt die Daten vor unerwünschten Zugriffen. Für M&E ist diese Funktion jedoch nicht relevant, da das Unternehmen bereits VPN-Verbindungen nutzt.

Es gibt zwei Möglichkeiten die Software zu betreiben. Zum einen in einer Cloud und zum anderen als on-premise Lösung. Einen Vergleich zwischen den beiden Lösungen befindet sich im Anhang *(siehe Vergleich: Online oder* on-premise*)*

2.5 Kosten pro User-Lizenz

Im Folgenden, ist ein Vergleich der Einzellizenzkosten der Passwortmanager.

Zeitraum	KeePass2	Bitwarden	1password	Dashlane
Pro Monat	0,00 €	4,59 €	7,43 €	8,00 €
1 Jahr	0,00 €	55,08 €	89,16 €	96,00 €
2 Jahre	0,00 €	110,16 €	178,32 €	192,00 €
5 Jahre	0,00 €	275,40 €	445,80 €	480,00 €

Die Preise sind von den jeweiligen Internetseiten (Stand 12/2023). Die Dollarbeträge wurden in Euro umgerechnet.

2.6 Nutzwertanalyse

Anforderung	**GW**	**KeePass2**		**Bitwarden**		**1password**		**Dashlane**	
		B	**G**	**B**	**G**	**B**	**G**	**B**	**G**
Vertrauen	5	4	20	4	20	4	20	4	20
Passwortgenerator	4	5	20	5	20	5	20	5	20
Identifizieren von schwachen Passwörtern, (Wiederholungen, Verletzungen)	5	0	0	5	25	5	25	5	25
Browser Plug-In	2	0	0	4	8	4	8	5	10
Passwort teilen	5	0	0	3	15	4	20	3	15
IOS APP	5	0	0	4	20	4	20	4	20
2FA	5	0	0	5	25	5	25	5	25
Verschlüsselter Speicherplatz	1	0	0	4	4	4	4	4	4
Serverstandort online – in welchem Land steht dieser	4	0	0	2	8	5	20	2	8
Möglichkeit des *on-premise* Hosting	5	0	0	5	25	0	0	0	0
Kosten	5	5	25	4	20	3	15	2	1
Gesamt		14	65	36	**190**	35	177	32	157

GW = Gewichtung; B = Bewertung; G = Gewichtete Bewertung
1 = „sehr niedrig“; 5 = „sehr hoch“

2.7 Entscheidungsprozess

2.7.1 Vergleich

Es lässt sich feststellen, dass bis auf KeePass2 alle anderen Passwortmanager den grundlegenden Anforderungen entsprechen. Sie alle bieten einen Passwortgenerator an, der es den Mitarbeitern ermöglicht, sichere Passwörter zu generieren und somit die Sicherheit zu gewährleisten.
Insgesamt bietet Bitwarden mit seinem *On-Premise*-Hosting-Ansatz einen klaren Vorteil für Unternehmen wie M&E, die die volle Kontrolle über ihre Daten in systemrelevanten Anwendungen wünschen.

2.7.2 Entscheidung

Wie der Entscheidungsmatrix zu entnehmen, fiel die Entscheidung auf Bitwarden.
Die Firma Müller & Egerer präferiert eine *on-premise* Lösung, wenn möglich. Und Bitwarden ist der einzige Manager mit dieser Möglichkeit. Alle wichtigen Punkte, wie *2FA, SSO* oder auch *SCIM* sind vorhanden. Zudem ist es möglich den Manager in die Active Directory zu integrieren und somit kann in der IT wie bisher gearbeitet werden.
Es wurde nach Absprache entschieden, die Software auf einer virtuellen Maschine mit Linux zu installieren.

3. Hardware und Budget

3.1 Hardwareanforderungen vom Hersteller

	Minimum	Empfohlen
Prozessor	X64, 1.4GHz	X64, 2GHz Dual Core
Arbeitsspeicher	2 GB	4+ GB
Speicher	12 GB	25 GB
Docker Version	Engine 19+ and Compose 1.24+	Engine 19+ and Compose 1.24+

Außerdem zwingend nötig ist die Möglichkeit zur verschachtelten Virtualisierung. Wichtig ist außerdem die Möglichkeit, eine Ausnahme in die Firewall zu bauen.

3.2 Personalkosten

Die Personalkosten werden in Relation der aufgebrachten Arbeitsstunden und dem Stundenlohn berechnet.

Position	Interner Verrechnungssatz	Stunden	Gesamt
Praktikant	30,00 €	40	1.200,00 €
Backup-Admin	50,00 €	1	50,00 €
	Gesamt:	**36**	**1.250,00 €**

3.3 Kostenaufstellung

Kosten Server (monatlich)	
Wartung Server	350,00 €
VM (Alle Maschinen)	220,00 €
Gesamt:	**570,00 €**

Lizenzkosten (monatlich)	
Anzahl der Lizenzen	115,00 €
Einzelkosten (Projektpreis)	3,33 €
Gesamt:	**383,33 €**

Die Endkosten der Lizenzen hat sich aufgrund eines Zwischenhändlers verändert.
(Siehe *Angebot*.)

Gesamtkosten	
Personalkosten	1.250,00 €
Kosten Server	570,00 €
Lizenzkosten	383,33 €
Projektkosten gesamt 1. Monat	**2.203,00 €**

4. Installation

Alle virtuellen Maschinen befinden sich auf einem für das Projekt bereitgestellten Computer auf dem VMware ESXI 6.5 läuft und bereits vorinstalliert war. Dazu wurde eine FritzBox als Router bereitgestellt.
Zur Vorbereitung auf das Projekt wurde eine eigene Umgebung aufgebaut mit einem Windows Server 2019 auf der eine Active Directory mit einem DNS und DHCP läuft. Auf diese Vorbereitung für das Projekt wird, da es für das Projekt keinen Bestandteil hat, nicht weiter darauf eingegangen.

4.1 VM einrichten

Zu Beginn der Installation richten wir auf dem VMware ESXi einen neuen virtuellen Computer ein (siehe *Netzwerkplan*). Diesem Computer geben wir den Namen "bitwarden-Server". Dabei wählen wir das Gastbetriebssystem als Linux und die Version Ubuntu Linux. Anschließend wählen wir den Speicher aus, wobei wir uns für den Datastore "VM" entscheiden, die sämtlichen virtuellen Maschinen speichert (*Abbildung 2 Konfiguration der VM*).
Nachdem wir so vorgegangen sind, gelangen wir zu den Einstellungen, in denen wir die Anzahl der CPU-Kerne auf zwei setzen. Ebenso wichtig ist die Festlegung des Arbeitsspeichers auf 6 GB und die Bereitstellung einer Festplattenkapazität von 60 GB. Um Ubuntu auf der neuen virtuellen Maschine zu installieren, wählen wir die Installationsdatei unter den CD-/DVD-Medien aus, die sich auf Datastore1 befindet. Eine entscheidende Einstellung für unsere spezifische Maschine ist unter dem Punkt "CPU" die Hardwarevirtualisierung, die es ermöglicht, Docker zu betreiben. Diese Einstellung entspricht dem Aktivieren der Virtualisierung im BIOS

Anschließend starten wir die neue virtuelle Maschine, die nun mit der Vorbereitung der Installation von Ubuntu beginnt. Dort wählen wir die Sprache aus und gehen auf „Weiter“. Nach der obligatorischen Auswahl der Tastatursprache können wir festlegen, welche Art von Installation durchgeführt werden soll. Da wir den Server ausschließlich für Docker und den Passwortmanager benötigen, reicht eine minimale Installation aus. Um den Installationsprozess zu beschleunigen, aktivieren wir die Option für automatische Aktualisierungen während der Installation. Dann wird das Speichermedium formatiert, um die Dateistruktur für das Betriebssystem anzulegen und die eigentliche Installation beginnt.

Nach der erfolgreichen Installation von Ubuntu richten wir einen lokalen Benutzer namens "bitwarden" ein. Für zukünftige Zwecke generieren wir außerdem ein Passwort für den Root-Benutzer. (*Abbildung 3 Installation Ubuntu*).

4.2 Verbinden mit der Active Directory

Um eine Verbindung mit der Active Directory vom Windows Server herzustellen, müssen wir die entsprechenden Dienste installieren. Dazu verwenden wir den Terminal und schauen uns mit *hostnamectl* unseren Static-Hostname an. Damit wir den Server-Client in die AD integrieren können, ändern wir diesen neu in *Clientname.Domain* indem wir den Befehl *hostnamectl set hostname* benutzen (*Abbildung 4 Umbenennen des Hostname*). Danach schauen wir noch einmal, dass unser neuer Name übernommen wurde. Damit es in Zukunft keine Probleme gibt checken wir mit *timedatectl* das der NTP-Service aktiviert ist. Als nächstes schauen wir, das der Server den richtigen DNS hat. Dies schauen wir mit *resolvectl* nach. Dort muss dann das DNS von der Active Directory stehen, in unserem Fall ist das auch gleichzeitig der Domain-Controller (*Abbildung 5 Prüfen des DNS*).

Nachdem wir alles getestet haben, installieren wir den SSSD herunter, der uns den Zugriff auf andere Provider erlaubt. Dies erreichen wir mit dem Befehl *apt install sssd-ad sssd-tools realmd adcli*. Haben wir das installiert, schauen wir mit *realm -v discover dh.test* ob wir die Domain finden können. Danach erstellen wir einen Befehlscode für den Kerberus, der uns erlaubt der Active Directory beizutreten (*Abbildung 6 Einfügen und Testen der Kerberus Konfig*).
Haben wir all das gemacht, ist es Zeit, der Domain beizutreten. Das machen wir mit dem Befehl *realm join -v DH-Test*. Da wir keinen bestimmten Nutzer angegeben haben will er das Passwort vom Administrator der Domain haben. Damit sind wir Mitglied der Domain. Zum Schluss testen wir den Status der Domain und sehen, dass wir nun ein Kerberos Mitglied sind. Außerdem testen wir mit einem Ping zu Domain Controller, das die Verbindung stimmt und alles läuft und melden uns mit einem User der Domain an *(Abbildung 8 Integration AD Prüfung*).

4.3 Portfreigabe

Als nächsten Schritt müssen wir bestimmte Ports für diese virtuelle Maschine freigeben. Dazu greifen wir in unserem Fall auf die Firewall über die Adresse https://192.168.178.1 zu und navigieren zu den Internet-Einstellungen für Freigaben. Dort finden wir eine Liste aller bisherigen Freigaben.

Anschließend wählen wir die Option "Gerät für Freigaben hinzufügen" und selektieren unsere virtuelle Maschine. Dann klicken wir auf "Neue Freigabe". Ein Pop-Up-Fenster öffnet sich, in dem wir "http-Server" als Anwendung auswählen und sicherstellen, dass das Häkchen bei "Freigabe aktiviert" gesetzt ist. Diesen Vorgang wiederholen wir für den HTTPS-Server. Zum Abschluss bestätigen wir die Einstellungen durch Klicken auf "Übernehmen".

4.4 Docker

Docker ist eine Open-Source Container-Technologie, mit der Linux-Container erstellt werden können. Die Bitwarden Technologie ist so konfiguriert, dass eine einfache Installation auch für Anfänger gewährleistet ist. Damit dieses in einfachen Schritten erklärt werden kann baut diese auf der Docker Technologie auf, da diese immer gleich ist.
Nach der Freigabe der Ports kommen wir zur Vorbereitung der Docker-Installation. Zunächst aktivieren wir KVM mit dem Befehl `sudo apt -y install bridge-utils cpu-checker libvirt-clients libvirt-daemon qemu qemu-kvm` und überprüfen dann mit `kvm-ok` die Funktionalität. Anschließend installieren wir GNOME mit `sudo apt install gnome-terminal` und führen dann eine Aktualisierung aller Pakete durch.

Nach Abschluss dieser Schritte laden wir Docker mithilfe des APT-Repositorys herunter und überprüfen seine Funktionstüchtigkeit. Nachdem alles einwandfrei läuft, führen wir erneut eine Aktualisierung aller Pakete durch.

Als nächstes wechseln wir in den Downloadordner und installieren Docker Desktop. Während dieses Vorgangs kann eine Fehlermeldung auftreten, die den Zugriff verhindert. Da es sich jedoch um eine Installationsdatei handelt, ist dies normal und erfordert keine weitere Beachtung.

Nachdem wir alle Schritte durchgeführt haben, starten wir Docker Desktop. Dadurch öffnet sich die grafische Oberfläche von Docker. Wir akzeptieren die Servicevereinbarungen und erstellen ein Docker-Konto. (Hinweis: Zunächst funktioniert die Installation ohne Konto nicht.) Nach erfolgreicher Anmeldung mit E-Mail, Benutzername und Passwort starten wir Docker. Anschließend führen wir zur Sicherheit einen Neustart des Systems durch.

Nach dem Neustart erstellen wir im Root-Verzeichnis einen neuen Ordner namens "Bitwarden". Hierfür müssen wir dem Benutzer Root mit `sudo` Root-Rechte geben. Nach der Erstellung vergeben wir die Berechtigungen mit `777`. Wichtig: Die Vergabe von Berechtigungen mit `777` wurde hier aus Gründen der Einfachheit für das Projekt verwendet und sollte in einer produktiven Arbeitsumgebung niemals so erfolgen. In einer Produktivumgebung empfehle ich eine Berechtigungsverteilung von 750 (*Abbildung 9 Test Installation Docker*).

4.5 Bitwarden

Nachdem wir den Bitwarden-Installer von der offiziellen Webseite heruntergeladen haben, installieren wir diesen im zuvor erstellten Ordner im Root-Verzeichnis.

Anschließend beginnen wir mit der Einrichtung von Bitwarden. Zuerst wird die Domäne abgefragt, auf die wir zukünftig über einen Browser darauf zugreifen werden. In unserem Fall lautet die Domäne bitwarden.mueller-egerer.de. (Anmerkung: Ein Fehler wurde gemacht, indem nur mueller-egerer.de eingegeben wurde, was dazu führte, dass die Webseite immer auf die Firmenwebseite weitergeleitet wurde, selbst mit einer Weiterleitung konnte das Problem nicht behoben werden). Danach wird gefragt, ob ein SSL (TLS) Zertifikat generiert werden soll. In diesem Fall wird darauf verzichtet.

Anschließend tritt eine Fehlermeldung auf die besagt, dass Docker Compose nicht installiert ist. Wir holen dies mit `sudo apt install docker-compose` nach und überprüfen es mit `docker-compose -version`. Außerdem dürfen wir nicht vergessen, die Berechtigung für `/run/docker.sock` mit dem chmod-Befehl auf 777 zu setzen. Da zuvor kein Docker-Konto angelegt wurde, wird dies nun nachgeholt.

Des Weiteren müssen wir eine Freigabe für Docker erstellen, damit es auf die Dateien und Ordner zugreifen kann. Dazu gehen wir in die Einstellungen unter den Ressourcen auf "File sharing" und geben dort den Ordner `/opt/Bitwarden` ein. Abschließend speichern wir die Einstellungen und starten die virtuelle Maschine neu. (Hinweis: Die Berechtigungen vom Ordner werden vererbt).

4.6 Neustart Installation

Nachdem wir die Installation neu gestartet haben, geben wir erneut den Domainnamen ein, bitwarden.mueller-egerer.de. Danach wählen wir bei der Zertifikatgenerierung für die Projektumgebung die Option Nein aus. Als nächstes legen wir fest, wie die Datenbank heißen soll, beispielsweise "mebitwarden". Anschließend geben wir unsere Installations-ID und den Key ein (*Abbildung 10 Installation Bitwarden*).

Als nächstes werden wir nach unserer Region gefragt, wobei die Auswahl zwischen EU und US liegt. Hier müssen wir sicherstellen, dass wir die Region auswählen, die dem Key entspricht. In diesem Fall ist es US.

Da wir zuvor angegeben haben, dass wir kein Zertifikat besitzen und auch keines von Let's Encrypt generieren lassen möchten, werden wir nun gefragt, ob wir eines selbst generieren möchten. Für unser Projekt wählen wir Ja und lassen es automatisch generieren.

Damit ist die Installation abgeschlossen. Nach einem kurzen Überprüfen der Berechtigungen der Verzeichnisse starten wir Bitwarden mit `./bitwarden.st start`. Während des Startvorgangs muss das Passwort für Docker noch einmal eingegeben werden.

4.7 Fehler die Behoben wurden und öffnen von Bitwarden

Nachdem die Installation abgeschlossen war, traten einige Fehler auf, die behoben werden mussten:

1. **SMTP-Einrichtung mit Editor:** Für die Funktionalität von Bitwarden muss in der global.override.env die SMTP-Einstellungen angepasst werden. Dies ist dazu notwendig, weil damit eine no-reply-Adresse erstellt wird, die für z.B. Einladungen verwendet wird.
2. **Einrichtung der DNS-Weiterleitung:** Um auf den Manager im Browser zugreifen zu können, musste eine Weiterleitung im DNS eingerichtet werden, die auf die IP-Adresse des Servers zeigt (*Abbildung 11 DNS Weiterleitung*).
3. **Fehler beim Start von Docker:** Es gab einen Fehler, der besagte, dass der SQL-Server (der bei der Installation von Bitwarden mit Installiert wurde), wo die Daten gespeichert werden zu wenig Arbeitsspeicher hatte. Dies lag daran, dass Docker nicht auf den gesamten verfügbaren Speicher zugreifen konnte. Unter den Docker-Einstellungen im Bereich Ressource -> Advanced wurde festgestellt, dass Docker nur 1,9 GB Arbeitsspeicher zur Verfügung hatte. Dieser Wert wurde auf 6 GB erhöht.
4. **Probleme mit Docker und der Internetverbindung:** Bitwarden benötigt eine stabile Internetverbindung, um reibungslos zu funktionieren und darauf zuzugreifen. In den Docker-Einstellungen unter Ressourcen -> Netzwerk wurde festgestellt, dass die IP-Adresse mit der Subnetzmaske in CIDR-Schreibweise nicht mit dem eigenen Netz übereinstimmte.
5. **Ports:** Nach der vorigen Anpassung stellte sich heraus, dass die zuvor freigegebenen Ports für Bitwarden von Docker verwendet wurden. Um dieses Problem zu umgehen, wurden in configurations-Datei von Bitwarden neue Ports für Bitwarden auf 4444 für http und 5555 für https festgelegt. Diese Ports mussten auch in der Firewall freigegeben werden (*Abbildung 12 Portfreigabe Firewall*).

Nachdem alle Einstellungen vorgenommen wurden, wurde Bitwarden neu aktualisiert, um sicherzustellen, dass alle Änderungen übernommen wurden. Anschließend wurde Bitwarden neu gestartet.

Nach den durchgeführten Anpassungen rufen wir im Browser den Manager unter https://bitwarden.mueller-egerer.de auf und melden uns mit dem zuvor beim SMTP-Einrichten hinterlegten Konto an. Nach der erfolgreichen Anmeldung richten wir eine neue Organisation ein.

Hierbei geben wir den Namen der Organisation sowie die Rechnungs-E-Mail-Adresse an. Anschließend werden wir nach der Art der Organisation gefragt. In unserem Fall wählen wir "Unternehmen" aus. Des Weiteren müssen wir die gewünschte Benutzeranzahl und die Zahlungsinformationen angeben.

4.8 Integration in die AD

Für die Synchronisation mit der Active Directory benötigen wir die Directory Connector App von Bitwarden.
Dort melden wir uns mit der ID und dem Code, den wir von Bitwarden bekommen haben als wir uns als Unternehmen registriert haben, an.
Dort gehen wir in die Einstellungen und geben nochmals den Server-Hostname, die Ports und den Pfad der Active Directory an. Zudem geben wir noch den Namen und das Passwort an, mit welchem der Connector sich an der Directory registriert.
Danach kommen wir zu den Synchronisationsoptionen. Diese befinden sich auch auf der Einstellungsseite.

Wir setzten die Intervall-Zeit auf das Minimum von 5 Minuten und sagen, das gesperrte Nutzer nicht mit synchronisiert werden. Außerdem erlauben wir das Überschreiben von vorhandenen Benutzerdaten. In Zukunft kann auch noch eingestellt werden, dass nur bestimmte Nutzer oder Gruppen synchronisiert werden sollen.

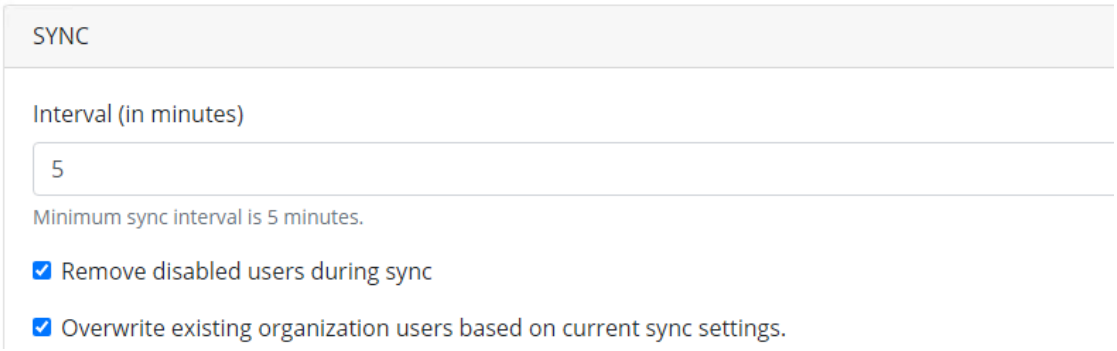


Abbildung 1 Synchronisationseinstellungen

4.9 Richtlinien

Nachdem wir die Organisation erstellt und mit der AD verbunden haben, öffnet sich im Browser automatisch die Admin-Konsole. Dort navigieren wir zu den Einstellungen und dann zu den Richtlinien, wo wir alle relevanten Einstellungen für die Organisation vornehmen können.

1. **Zwei-Faktor-Authentifizierung aktivieren:** Zuerst aktivieren wir die Zwei-Faktor-Authentifizierung, um sicherzustellen, dass sich kein Mitglied ohne zusätzliche Verifizierung anmelden kann.
2. **Richtlinien für das Masterpasswort festlegen:** Wir bearbeiten die Richtlinien für das Masterpasswort der einzelnen Mitglieder und legen fest, dass es mindestens 12 Zeichen lang sein muss und eine starke Komplexität aufweisen muss. Wir erlauben alle gängigen Sonderzeichen.
3. **Kontowiederherstellungsverwaltung konfigurieren:** Wir erlauben den Administratoren die Möglichkeit, das Masterpasswort zurückzusetzen, wenn ein Mitarbeiter es vergisst.
4. **Passwort-Generator aktivieren:** Da der Passwort-Generator Pflicht wird, aktivieren wir diesen und legen fest, dass Mitarbeiter Passwörter mit mindestens 12 Zeichen, darunter mindestens 2 Ziffern und Sonderzeichen, verwenden müssen.
5. **Verbot mehrerer Organisationen pro Mitarbeiter:** Aus Sicherheitsgründen verbieten wir per Richtlinie, dass ein Mitarbeiter mehr als einer Organisation beitreten kann.
6. **Einstellungen für SEND und persönlicher Tresor:** Wir erlauben die Nutzung des persönlichen Tresors und von SEND, legen jedoch fest, dass die E-Mail-Adresse beim SEND nicht versteckt werden darf.
7. **Tresor-Timeout festlegen:** Wir wollen, dass ein Mitarbeiter nach maximal 4 Stunden Inaktivität automatisch abgemeldet wird.
8. **Auto-Ausfüllen aktivieren:** Um sicherzustellen, dass der Mitarbeiter den Manager tatsächlich verwendet und weil es die Arbeitet erleichtert, aktivieren wir das Auto-Ausfüllen.

Nachdem alle Einstellungen vorgenommen wurden, folgt der Import der Daten. Wir nehmen zum Testen die Daten, die in der IT-Abteilung im KeePass gespeichert wurden. Dazu gehen wir in den alten Manager, in diesem Fall KeePass, und wählen in der oberen Leiste die Option "Export" aus. Nach Eingabe des Masterpassworts und Auswahl des Exportformats, speichern wir die Datei. Zurück im Browser navigieren wir zu den Einstellungen und wählen die Option "Daten Importieren". Hier wählen wir den Speicherort der Importdatei, die Zielsammlung und das Dateiformat aus und führen dann den Importvorgang durch (*Abbildung 14 Bitwarden Richtlinien Organisation*).

4.10 Datensicherung

Bitwarden führt regelmäßige Backups durch. Jede Nacht wird automatisch ein Backup des *sql*-Containers erstellt. Diese Backups werden über einen Zeitraum von 30 Tagen archiviert. Dadurch besteht die Möglichkeit, auf frühere Versionen der Datenbanken zurückzugreifen, falls dies erforderlich sein sollte.

Zusätzlich zu den Backups von Bitwarden sichert der Backup-Administrator die virtuellen Maschinen mittels Altaro. Dabei werden die VMs einmal täglich in dreifacher Form gesichert, um mehrere Sicherungen zur Verfügung zu haben. Die Sicherung der Maschinen erfolgt auf unterschiedlichen Speichermedien, um die Daten bestmöglich zu schützen.

Eine Kopie der Backups wird auf dem hauseigenen *NAS* gespeichert. Damit können Sicherungen schnell wiederhergestellt werden. Des Weiteren werden die Backups zusätzlich in einer nicht zu ändernden Cloud (Immutable) gespeichert, womit eine externe Sicherung gewährleistet ist. Dies bietet einen zusätzlichen Schutz, falls es lokal zu Problemen kommen sollte. Darüber hinaus erfolgt eine lokale Speicherung der Backups auf einer Festplatte, die speziell für diesen Zweck eingesetzt wird.

Durch diese umfassende Backup-Strategie wird sichergestellt, dass die Daten bei so gut wie jedem Problem gesichert und wiederherstellbar sind. Die automatisierten Backups, die langfristige Aufbewahrung der Daten und die Verwendung unterschiedlicher Speicherorte tragen dazu bei, dass, wenn es zu einem Systemausfall oder einem unvorhergesehenen Ereignis kommen sollte, die Daten problemlos wiederhergestellt werden können.

Für die virtuelle Maschine, auf der der Passwort-Manager steht, beauftrage ich den Backup-Administrator von M&E., die neue VM in die bisherige Backup-Strategie zu integrieren.
Nach erfolgreicher Datensicherung bitte ich um ein Sicherungsprotokoll, in dem dokumentiert ist, dass das Backup ordnungsgemäß durchlaufen ist und eine Wiederherstellung im Test erfolgreich war.

5. Endphase

5.1 Testphase

Nach der erfolgreichen Installation und Konfiguration der Passwort-Manager-Software beginnt die Testphase, um sicherzustellen, dass alles reibungslos funktioniert.
Sollte der Test ein Erfolg werden, wird die Software in die Arbeitsumgebung integriert und zunächst in der IT ausgerollt und gründlich getestet. Dabei wird geprüft, ob alle Funktionen wie geplant laufen und es zu keiner Beeinträchtigung für die Kollegen bei der Arbeit durch fehlende oder fehlerhafte Passwörter kommt.

5.2 Nach der Testphase/ Ausschau auf die Zukunft

Nach Abschluss der Testphase in der IT-Abteilung erfolgt die Installation des Passwort-Managers auf den Geräten der anderen Abteilungen im Unternehmen.

Geplant, aber nicht mehr Bestandteil meines Projektes aufgrund mangelnder Zeit:

1- Für die mobilen Geräte wird die Installation der Bitwarden-App über das *Mobile Device Management (MDM)* Intune eingerichtet. Dies geschieht mithilfe der vorab erstellten Profile, in denen die entsprechenden Einstellungen und Konfigurationen enthalten sind.

2- Für die Laptops und Computer erfolgt die Installation schrittweise über Microsofts *Intune*. Dort wird wie in Intune in den einzelnen Profilen angewiesen, dass der Passwort-Manager heruntergeladen und installiert werden soll.

3- Parallel dazu wird im betriebsinternen Portal Intratool, in Teams und per Mail ein Handout veröffentlicht, das über den Passwort-Manager, seine Funktionen, Bedienung und den Grund für seine Einführung informiert. Dadurch erhalten die Mitarbeiter eine umfassende Anleitung und können sich so über den Passwort-Manager informieren.

6. Abschluss

6.1 Rechnung

Die Berechnung der Personalkosten basiert auf dem internen Stundensatz von ME. Versorgungskosten wie Strom, Wasser und Gas sind in dem Stundensatz mit inbegriffen. Die erstellte Rechnung ist im Anhang beigefügt. (Rechnung)

6.2 Soll-Ist-Vergleich Zeitplan

Während der Projektdurchführung haben sich einige Zeiten der Schritte verändert. Die Gesamtstundenzahl hat sich nicht verändert. Eine tabellarische Aufstellung der Zeiten ist im Anhang beigefügt. (Detaillierte *Zeitplanung*)

6.3 Kundendokumentation

Im Verlaufe des Projektes wurde eine Kundendokumentation angefertigt. Ein Ausschnitt dieser befindet sich im Anhang (*Kundendokumentation*).

6.4 How-To

Eine Erklärung, wie sich die Mitarbeiter anmelden können und die größten Funktionen, habe ich in einem How-To geschrieben und befindet sich als Ausschnitt im Anhang. (*How-To* (*Ausschnitt*))

6.5 Fazit

Das Thema Passwörter im Internet ist äußerst sensibel und kann schnell zu Verwirrung und Angst führen. Ein kleiner Fehler kann bereits dazu führen, dass unbefugte Personen Zugang zu sensiblen Daten erhalten. Gleichzeitig ist es auch ein Thema, das oft vernachlässigt wird, und man vergisst, wie häufig man beispielsweise dasselbe Passwort verwendet.

Abschließend kann mein Projekt als erfolgreich bewertet werden, auch wenn das Thema Passwörter niemals endgültig abgeschlossen sein wird. Ich möchte mich bei allen Beteiligten und insbesondere der Geschäftsleitung von Müller & Egerer für die Möglichkeit bedanken, ein solches Projekt durchzuführen. Ich bin gespannt, wie die Kollegen die neue Anwendung, die in Zukunft Bestandteil ihrer Arbeit ist, aufnehmen, und freue mich auf Ihr Feedback.

Dieses Thema war nicht nur für das Projekt selbst, sondern für mich persönlich und meinen Bekanntenkreis eine wichtige Erfahrung und Bereicherung.

II Glossar

On-premise

On-premise gehostete Server sind Server, die vor Ort auf der eigenen Hardware gehostet werden.

Open-Source

Als Open-Source bezeichnet man eine Software, deren Quellcode frei einsichtbar ist und Nutzern die Möglichkeit gibt, diesen frei zu verwenden, zu ändern oder zu verteilen. Der Vorteil dabei ist, dass jemand Versiertes prüfen kann, was genau in dem Programm passiert, oder ihn gegebenenfalls so zu ändern, dass dieser besser an den User oder der Firma angepasst ist.

Apple-Ökosystem

Das Apple-Ökosystem ist die kollektive Nutzung von Apple-Hard- und Software, die miteinander funktionieren und untereinander interagieren. Es umfasst verschiedene Apple-Geräte und Gerätearten, z.B. iPhone, iPad, MacBook etc.
Ein gutes Beispiel ist die Bearbeitung einer Notiz: Man startet unterwegs auf dem iPhone eine neue Notiz und fängt an dort etwas zu schreiben. Zuhause auf dem MacBook wird diese synchronisiert, so dass ohne Unterbrechung von dem iPhone auf das MacBook gewechselt werden kann und ein nahtloses Arbeiten möglich ist.

haveibeenpwned

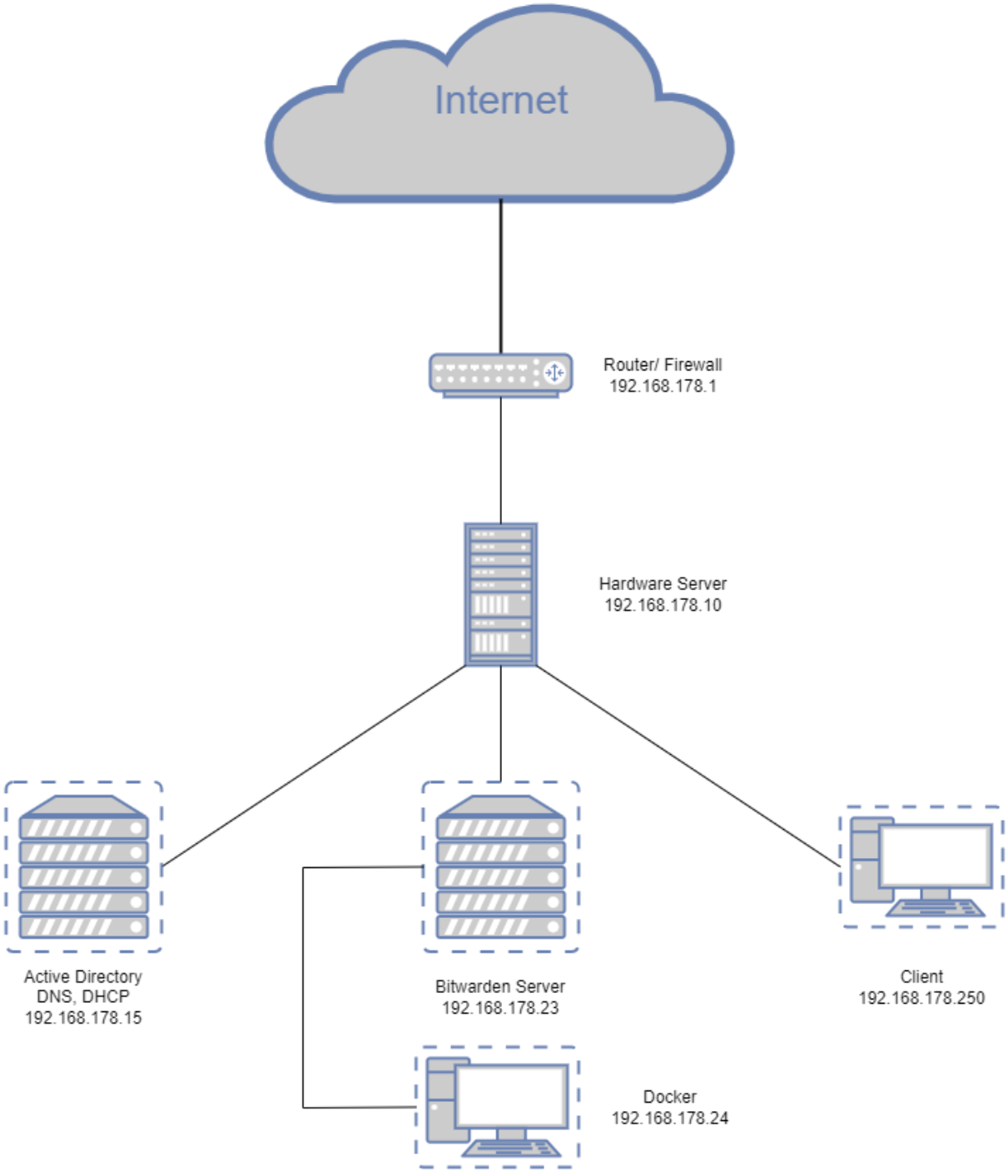
haveibeenpwned ist eine Website, auf der Personen mit ihrer E-Mail oder Handynummer überprüfen können, ob ihre persönlichen Daten durch Datenleaks kompromittiert wurden.
Dafür greift es auf eine Vielzahl von so genannten Datenbankdumps und Paste-Bins zu, wo geleakte Konten zu finden sind, und sucht diese nach den entsprechenden E-Mails oder Nummern durch.

Intune

Intune ist ein von Microsoft veröffentlichter End-Point-Manager, der eine cloudbasierte App- und Geräteverwaltung ermöglicht.

III Anhang

Netzwerkplan



Vergleich: Online oder on-premise

Online (Cloud beim Anbieter)	On-premise (in der eigenen Umgebung)
Der Server wird von dem jeweiligen Unternehmen bereitgestellt.	Es muss ein Server/ Platz auf einem Server bereitgestellt werden.
Bei Ausfall des Systems wird das automatisch repariert/gewechselt. Der Anbieter versucht, dass dieses nahtlos passiert.	Bei Ausfall des Systems muss dies selbst repariert werden.
Die Wartungen und Updates bedürfen keiner eigenen Arbeit und der Anbieter kümmert sich um einen reibungslosen Ablauf.	Bei Wartungen und Updates muss ein Mitarbeiter aktiv eingesetzt werden und sie müssen selbst integriert werden.
Die Kosten für das Betreiben und Instandhalten sind meist in den monatlichen Kosten mit eingerechnet.	Es fallen Kosten für eigene Server, Wartung, IT-Personal, Energiekosten etc. an.
Man ist auf den Anbieter angewiesen. Wenn der die Cloud schließt, besteht keine Möglichkeit, die Daten weiter dort laufen zu lassen und es kann sein, dass es zu einem Datenverlust kommt.	Es muss darauf geachtet werden, dass die Daten Datenschutzgerecht (DSGVO, BDSG) verschlüsselt sind.
Sollte das Internet ausfallen, hat man keinen Zugriff auf die Anwendung	Sollte das Internet ausfallen, kann man trotzdem lokal auf den Server zugreifen.

Detaillierte Zeitplanung

Während der Umsetzung des Projekts haben sich die zeitlichen Abläufe verändert. Einige Schritte sind schneller als geplant und andere haben länger gebraucht. Die Endzeit hat sich jedoch nicht verändert. Die Änderungen sind farblich markiert.

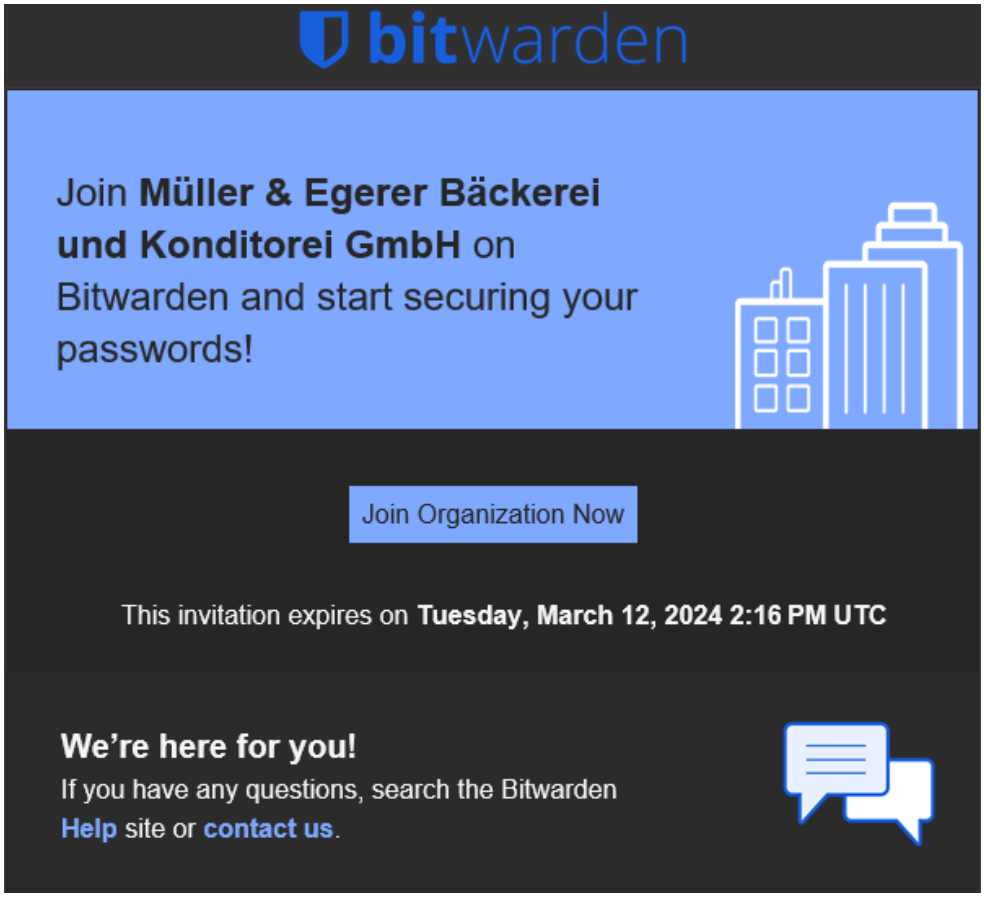
Aufgabe	Planung	Ist	Diff.
Analyse	**5,0**	**5,0**	**0,0**
• Ist- und Sollanalyse	3,0	3,0	0,0
• Schnittstellenfindung/ Vorgespräch	2,0	2,0	0,0
Planung/Konzeptionierung	**7,0**	**6,5**	**- 0,5**
• Recherche und Vergleich von Anwendungen	2,5	3,0	+ 0,5
• Kosten-Nutzen-Analyse	1,5	1,5	0,0
• Recherche der MFA-Apps	1,0	0,5	- 0,5
• Vorstellen der Softwareprodukte für Passwortmanager und MFA	1,0	1,0	0,0
• Entscheidungsfindung/ Genehmigung durch Kunden	1,0	0,5	- 0,5
Durchführung	**16,0**	**14,5**	**- 1,5**
• Erstellung der VM/Serverinstallation	4,0	4,0	0,0
• Netzwerkkonfiguration/Integration Verzeichnis Dienst	2,0	2,5	+ 0,5
• Installation und Konfiguration der Passwortmanager-Software	5,0	7,0	+ 2,0
• Installation Passwortmanager auf den Test-Clients	2,5	1,0	- 1,5
• Installation MFA auf Mobilgeräten	2,5	0,0	- 2,5
Testphase	**3,0**	**5,0**	**+ 2,0**
• Testen der Software mit MFA-Authentifizierung	2,0	1,0	- 1,0
• Fehlerbeseitigung	1,0	4,0	+ 3,0
Abschluss	**9,0**	**9,0**	**0,0**
• Rechnungserstellung	1,0	1,0	0,0
• Vorstellung/Übergabe	1,0	1,0	0,0
• Erstellung eines How-To's	2,0	2,0	0,0
• Erstellung Kundendokumentation	5,0	5,0	0,0
Gesamt	**40**	**40**	

Die Zeiten sind in Stunden.

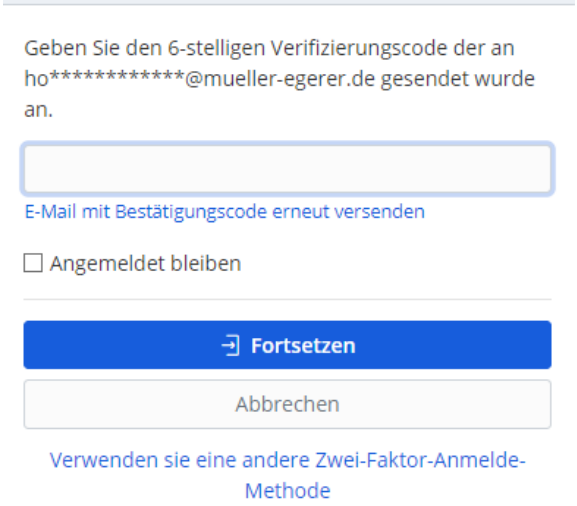
How-To (Ausschnitt)

Einrichten von Bitwarden

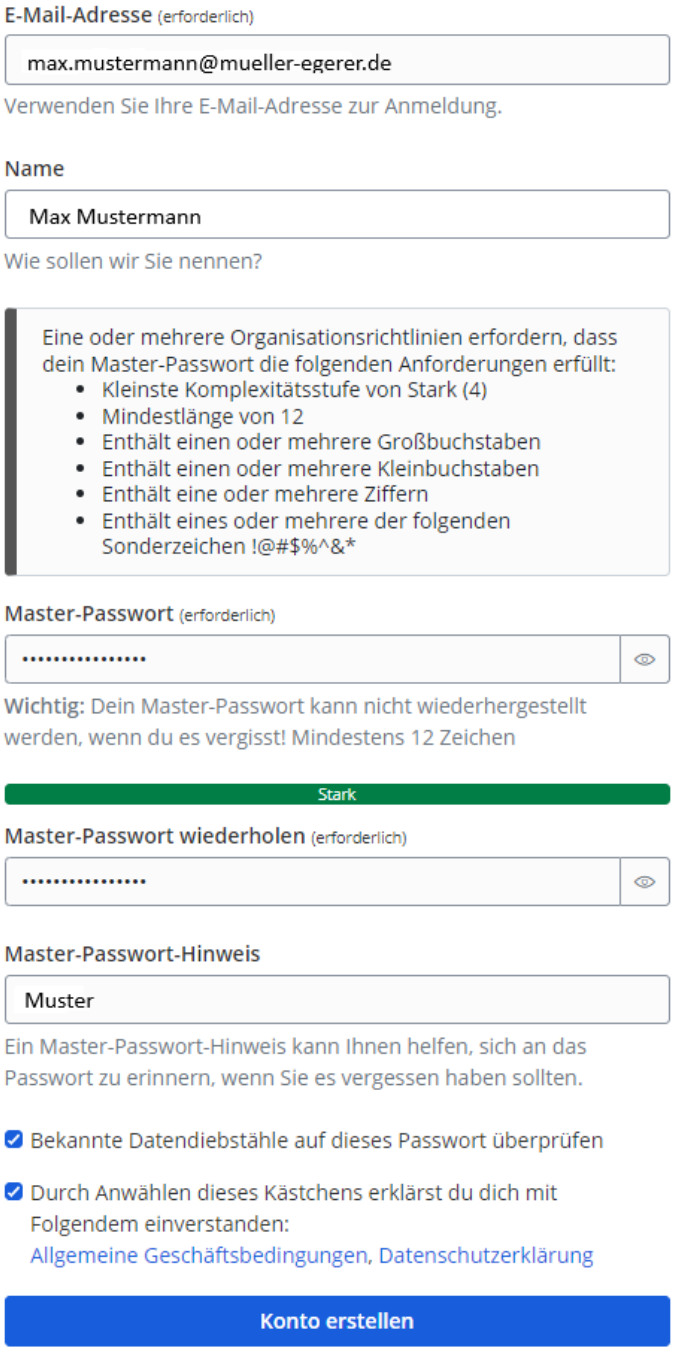
Öffne den Link der E-Mail.



Danach bekommt ihr per Email eine Nachricht von Bitwarden mit eurem Verifizierungscode.



Danach braucht ihr, wenn ihr noch kein Bitwarden-Konto mit der E-Mail-Adresse erstellt habt, ein solches. Hier ist wie ihr es anlegt.



Es gibt mehrere Möglichkeiten, auf den Passwortmanager zuzugreifen. Jetzt direkt nach der Registrierung zu sehen, haben wir den sogenannten Bitwarden Web Vault, der unter " https://bitwarden.mueller-egerer.de/“ zu öffnen ist.

Wichtig: Ihr müsst entweder in der Firma sein oder, wenn ihr von außerhalb, z. B. von Zuhause aus arbeitet, unbedingt den VPN anschalten, da sonst die Internetseite nicht gefunden werden kann.

Kundendokumentation (Auszug)

Kundendokumentation

Für die:

Müller & Egerer Bäckerei und Konditorei GmbH

Implementierung eines Passwort-Managers in die bestehende Serverstruktur
Integration in die bestehende Active Directory auf einer eigenen Virtuellen Maschine

Erstellt von Holger Fischer

Einleitung:
Diese Dokumentation fasst die Implementierung eines Passwortmanagers zusammen.

Projektplanung
Für die Implementierung dieses Projekts wurden 40 Stunden benötigt und wurde wie folgt aufgeteilt:

Projektphasen	Zeit in h
Analyse	5
Planung/Konzeptionierung	7
Durchführung	16
Testphase	3
Abschluss	9
Gesamt	**40**

Software, die benötigt wurde:
- VMWare ESXI 6.5
- Ubuntu 23.10
- Docker
- Bitwarden
- Bitwarden Directory Connector App

Durchführung:
Für das Projekt wurde auf dem VMware ESXI Server eine Virtuelle Maschine mit 6 GB RAM und 60 GB Festplattenspeicher erstellt. Auf dieser Maschine wurde Ubuntu 23.10 installiert und konfiguriert. Nach der Installation wurde ein Benutzer Namens „Bitwarden“ eingerichtet. Danach wurde diese Virtuelle Maschine in die bestehende Active Directory „me“ implementiert.

Es wurde Docker installiert und eingerichtet. Danach folgte das Installieren und Testen von Bitwarden. Nach erfolgreichem Test wurde ein Administratorkonto für Bitwarden erstellt und angemeldet.

In Bitwarden wurde die Organisation Müller & Egerer erstellt. Die Richtlinien für die Mitarbeiter wurde dem Wunsch nach angepasst und für Testzwecke wurden Passwörter der IT von Keepass importiert.
Die Active Directory wurde mit Bitwarden mithilfe der Directory Connector App synchronisiert. Es wurde die Funktionalität getestet und für die bevorstehende Testphase wurden die Mitarbeiter der IT-Abteilung eingeladen.

Mit dem Mitarbeiter der IT wurde die Einladung überprüft und gemeinsam ein Konto erstellt und die einzelnen Funktionen besprochen und getestet.

Nun erfolgt eine 3-monatige Testphase nach der Entschieden wird diese Software zu behalten oder eine andere auszuwählen.

Weitere Informationen:
IP-Adressen:
Die IP-Adressen wurden automatisch vom DHCP vergeben und hinterher reserviert.

Bitwarden-Server	192.168.178.23
Docker	192.168.178.24

Protokoll Datensicherung

Protokoll Überprüfung Datensicherung

Basisdaten

Virtuelle Maschine	DH-Bitwarden
Betriebssystem	Linux Ubuntu 22.04.
Host	192.168.178.10
Speicherort	\\"Datensicherungsserver"\DH-Bitwarden
Offsite Immutable Storage Wasabi	me-bitwarden-store

Protokolldaten letzten 3 Datensicherungen

Datum	Umfang in GB	Ergebnis onPrem	Offsite
14.03.2024	63	Erfolgreich	Erfolgreich
15.03.2024	7	Erfolgreich	Erfolgreich
18.03.2024	11	Erfolgreich	Erfolgreich

Protokolldaten Rücksicherung mit Überprüfung

Datum	Art der zur Verfügungstellung	Ergebnis
15.03.2024	Aus Sicherung gestartet	Erfolgreich
18.03.2024	Restore gesamte VM	Erfolgreich

Ausgeführt von

Rolf Döscher

Vorname Name



Unterschrift

Rastede, den

Ort, Datum

Angebot

Position 2 ist geschwärzt, da sie nicht zum Projekt gehört.

alphasolid
PASSION TO PERFORM IT

Alphasolid IT GmbH - Boschstr. 15 - 49733 Haren (Ems)

Müller & Egerer Bäckerei Konditorei GmbH
An der Brücke 27
26180 Rastede
Deutschland

Angebots-Nr. AN-2365
Datum 08.03.2024

Angebot AN-2365 - Bitwarden

Sehr geehrte Damen und Herren,

vielen Dank für Ihre Anfrage. Gerne unterbreiten wir Ihnen das gewünschte freibleibende Angebot:

Pos.	Beschreibung	Menge	Einzelpreis	Gesamtpreis
1.	**Bitwarden Enterprise Organization** Per User Advanced functionalities including enterprise policies SSO integration Admin Passwort Reset Self-host Option Hinweis: Der Preis bezieht sich auf ein jährliches Abo. Mindestlaufzeit sind 12 Monate. Wenn nicht 3 Monate vor Ende der Laufzeit schriftlich gekündigt wird, verlängert sich das Abo automatisch um weitere 12 Monate.	115,00 Jährlich	40,00 EUR	4.600,00 EUR
2.	[redacted]		[redacted]	

Alphasolid IT GmbH
Passion to perform IT
Boschstr. 15
49733 Haren (Ems)
Deutschland

Tel.: +49 (0) 5932 5009818
E-Mail: sales@alphasolid.de
Web: https://alphasolid.de

Amtsgericht Osnabrück
HR-Nr.: HRB 213218
USt.-ID: DE321801157
Steuer-Nr.: 53/202/47423
Geschäftsführung: Sascha Bolmer

[redacted]

Pos.	Beschreibung	Menge	Einzelpreis	Gesamtpreis
	Gesamtbetrag netto			[redacted]
	zzgl. Umsatzsteuer 19%			
	Gesamtbetrag brutto			

Lieferbedingungen: Frei Haus
Zahlungsbedingungen: 14 Tage Netto ohne Abzug von Skonto

Für Rückfragen stehen wir Ihnen jederzeit gerne zur Verfügung.
Wir bedanken uns sehr für Ihr Vertrauen.

Mit freundlichen Grüßen
Alphasolid IT GmbH

Es gelten die AGBs der Alphasolid IT GmbH

(https://alphasolid.de/agbs/)

Bitte beachten: Bei Dienstleistungen ohne Pauschale wird der effektiv anfallende Zeitaufwand berechnet.

Bei Arbeiten außerhalb der Regelarbeitszeit von (Montag - Freitag 08:00 - 18:00 Uhr) berechnen wir folgende Aufschläge auf die Dienstleistungen:

Zeit:	**Aufschlag:**
Montag - Freitag; 18:00 – 21:59 Uhr	25%
Montag - Freitag; 22:00 – 23:59 Uhr	50%
Montag - Samstag; 00:00 – 07:59 Uhr	100%
Samstag; 08:00 - 17:59 Uhr	25%
Samstag ab 18:00Uhr, Sonn- & Feiertage	100%

Alphasolid IT GmbH
Passion to perform IT
Boschstr. 15
49733 Haren (Ems)
Deutschland

Tel.: +49 (0) 5932 5009818
E-Mail: sales@alphasolid.de
Web: https://alphasolid.de

Amtsgericht Osnabrück
HR-Nr.: HRB 213218
USt.-ID: DE321801157
Steuer-Nr.: 53/202/47423
Geschäftsführung: Sascha Bolmer

Rechnung

Das ist eine Pro-Forma Rechnung, da es sich um ein Firmeninternes Projekt handelt.

Müller & Egerer - An der Brücke 27 - 26180 Rastede
Müller & Egerer Bäckerei
Konditorei GmbH
An der Brücke 27
26180 Rastede
Deutschland

Datum: 27.03.2024
Rechnungsnummer: 0
Rechnungsdatum entspricht Liefer-/Leistungsdatum

Rechnung

Sehr geehrter Damen und Herren,

Ihre Rechnung vom 27.03.2024

Position	Anzahl	Einheit	Bezeichnung	Einzelpreis	Gesamtpreis
1	40	Stunden	Implementierung eines Passwort-Managers in die bestehende Serverstruktur Integration in die bestehende Active Directory auf einer eigenen Virtuellen Maschine	50,00 €	1200,00 €
				Summe	1200,00 €
				19% MwSt.	228,00 €
				Gesamt	**1200,00 €**

Bitte überweisen Sie den Rechnungsbetrag innerhalb von 14 Tagen auf unser unten genanntes Konto.

Es gelten unsere Allgemeinen Geschäftbedingungen.

Müller & Egerer Bäckerei Konditorei GmbH
An der Brücke 27
26180 Rastede
Deutschland

[redacted]

Ust.-Id.: DE177049120
Registernummer: HRB 120560
Amtsgericht: Oldenburg
Geschäftsführer: Jan-Christoph Egerer
Hilmar Ukena
Webseite: www.mueller-egerer.de

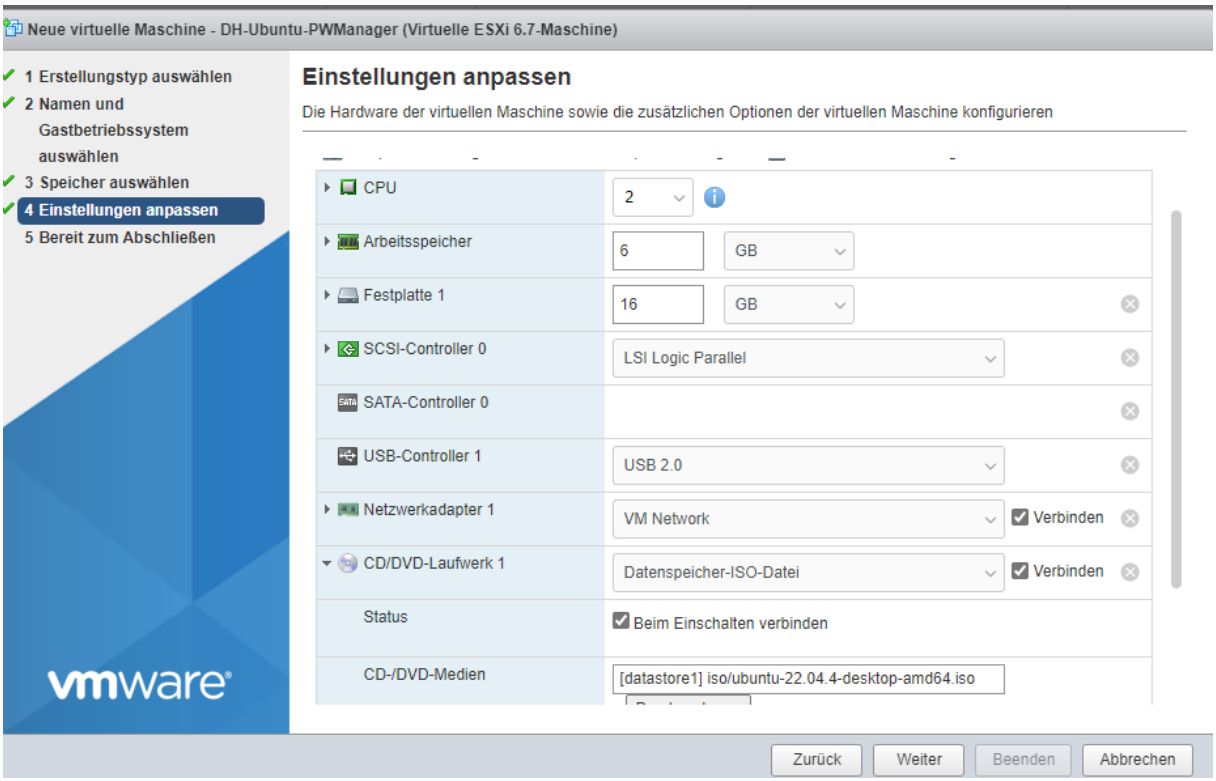


Abbildung 2 Konfiguration der VM

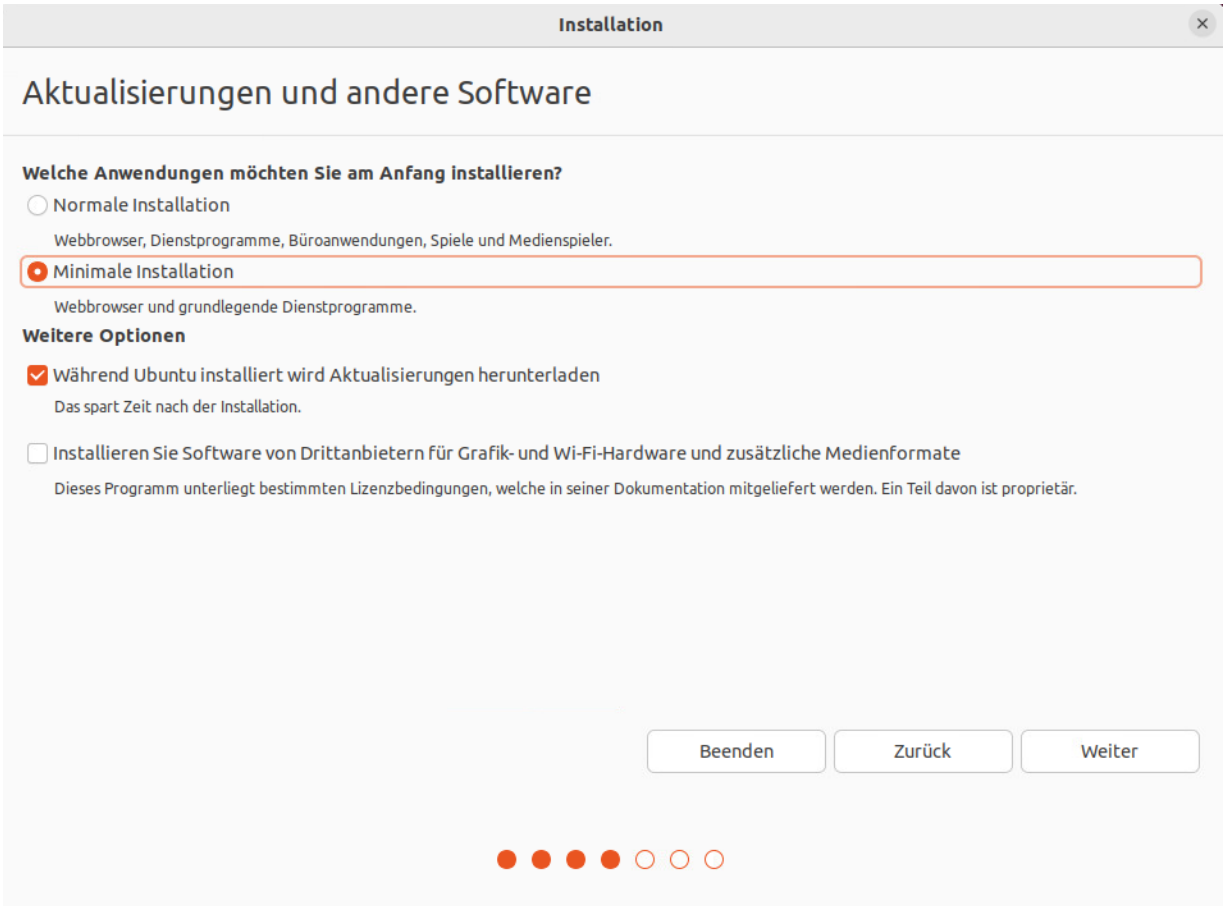


Abbildung 3 Installation Ubuntu

```
root@bitwarden-virtual-machine:~# hostnamectl set-hostname ubuntubw.dh.test
root@bitwarden-virtual-machine:~# hostnamectl
 Static hostname: ubuntubw.dh.test
       Icon name: computer-vm
         Chassis: vm
      Machine ID: e32dbcc5cc794050a14f3bb05f10854d
         Boot ID: 9fcffc101c7b48bfb3542ccb1ff1f5fa
  Virtualization: vmware
Operating System: Ubuntu 22.04.4 LTS
          Kernel: Linux 6.5.0-25-generic
    Architecture: x86-64
 Hardware Vendor: VMware, Inc.
  Hardware Model: VMware Virtual Platform
root@bitwarden-virtual-machine:~# timedatectl
               Local time: Fr 2024-03-15 14:02:55 CET
           Universal time: Fr 2024-03-15 13:02:55 UTC
                 RTC time: Fr 2024-03-15 13:02:55
                Time zone: Europe/Berlin (CET, +0100)
System clock synchronized: yes
              NTP service: active
          RTC in local TZ: no
```

Abbildung 4 Umbenennen des Hostname

```
root@bitwarden-virtual-machine:~# resolvectl
Global
       Protocols: -LLMNR -mDNS -DNSOverTLS DNSSEC=no/unsupported
resolv.conf mode: stub

Link 2 (ens160)
    Current Scopes: DNS
         Protocols: +DefaultRoute +LLMNR -mDNS -DNSOverTLS DNSSEC=no/unsupported
Current DNS Server: 192.168.178.15
       DNS Servers: 192.168.178.15
        DNS Domain: DH.Test
root@bitwarden-virtual-machine:~#
```

Abbildung 5 Prüfen des DNS

```
root@bitwarden-virtual-machine:~# cat > /etc/krb5.conf <<EOF
[libdefaults]
default_realm = DH.TEST
rdns = false
EOF
root@bitwarden-virtual-machine:~# cat /etc/krb5.conf
[libdefaults]
default_realm = DH.TEST
rdns = false
root@bitwarden-virtual-machine:~#
```

Abbildung 6 Einfügen und Testen der Kerberus Konfig

```
root@bitwarden-virtual-machine:~# realm join -v DH.TEST
 * Resolving: _ldap._tcp.dh.test
 * Performing LDAP DSE lookup on: 192.168.178.15
 * Successfully discovered: DH.Test
Passwort für Administrator:
 * Unconditionally checking packages
 * Resolving required packages
```

Abbildung 7 Integration in AD

```
root@bitwarden-virtual-machine:~# realm -v discover dh.test
 * Resolving: _ldap._tcp.dh.test
 * Performing LDAP DSE lookup on: 192.168.178.15
 * Successfully discovered: DH.Test
DH.Test
  type: kerberos
  realm-name: DH.TEST
  domain-name: dh.test
  configured: kerberos-member
  server-software: active-directory
  client-software: sssd
```

Abbildung 8 Integration AD Prüfung

```
root@ubuntubw:~# sudo docker run hello-world

Hello from Docker!
This message shows that your installation appears to be working correctly.

To generate this message, Docker took the following steps:
 1. The Docker client contacted the Docker daemon.
 2. The Docker daemon pulled the "hello-world" image from the Docker Hub.
    (amd64)
 3. The Docker daemon created a new container from that image which runs the
    executable that produces the output you are currently reading.
 4. The Docker daemon streamed that output to the Docker client, which sent it
    to your terminal.

To try something more ambitious, you can run an Ubuntu container with:
 $ docker run -it ubuntu bash

Share images, automate workflows, and more with a free Docker ID:
 https://hub.docker.com/
```

Abbildung 9 Test Installation Docker

```
bitwarden@bitwarden-Server:/opt/bitwarden$ ./bitwarden.sh install

 _     _ _                          _
| |__ (_) |___      ____ _ _ __ __| | ___ _ __
| '_ \| | __\ \ /\ / / _` | '__/ _` |/ _ \ '_ \
| |_) | | |_ \ V  V / (_| | | | (_| |  __/ | | |
|_.__/|_|\__| \_/\_/ \__,_|_|  \__,_|\___|_| |_|

Open source password management solutions
Copyright 2015-2024, 8bit Solutions LLC
https://bitwarden.com, https://github.com/bitwarden

=====================================================

bitwarden.sh version 2024.2.3
Docker version 25.0.5, build 5dc9bcc
docker-compose version 1.29.2, build unknown

(!) Enter the domain name for your Bitwarden instance (ex. bitwarden.example.com): bitwarden.mueller-egerer.de

(!) Do you want to use Let's Encrypt to generate a free SSL certificate? (y/n): n

(!) Enter the database name for your Bitwarden instance (ex. vault): vault

2024.2.3: Pulling from bitwarden/setup
Digest: sha256:150466dccce2c09a8cee79f4b69a1dadae0d9947720b25c333a45d87014c9f0a
Status: Image is up to date for bitwarden/setup:2024.2.3
docker.io/bitwarden/setup:2024.2.3

What's Next?
  View a summary of image vulnerabilities and recommendations →docker scout quickview bitwarden/setup:2024.2.3

(!) Enter your installation id (get at https://bitwarden.com/host): [redacted]

(!) Enter your installation key: [redacted]

(!) Enter your region (US/EU) [US]: US

(!) Do you have a SSL certificate to use? (y/N): n

(!) Do you want to generate a self-signed SSL certificate? (y/N): y

Generating self signed SSL certificate.
...........+...+...+.....+.+.....................++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*..
++++++*..+...............+.......++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
..+...+........++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*....+...+..............+...+....+...
...+.........+...+...+....+...............+...+..............+...+.............+..+.+...............+................
+........+......+...+.+......+...+........+......................+..+...+.......+...........+...............+.......+
-----
Generating key for IdentityServer.
.......+.+..+..................+....+.........+..+............++++++++++++++++++++++++++++++++++++++++++++++++++++++++
.+...+.......+..+.+..+.......+........+.......+.....+......+....+.....+....+.....+..........++++++++++++++++++++++++++
....+...+......+.............++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*.....+.....+.+.....+..
...+..+...+....+.....+..........+........+....+......................+..+......+......+...+.+..............+..........
++++++++++++++++++++++++++++++++
-----

!!!!!!!!!! WARNING !!!!!!!!!!
You are using an untrusted SSL certificate. This certificate will not be
trusted by Bitwarden client applications. You must add this certificate to
the trusted store on each device or else you will receive errors when trying
to connect to your installation.
```

Abbildung 10 Installation Bitwarden

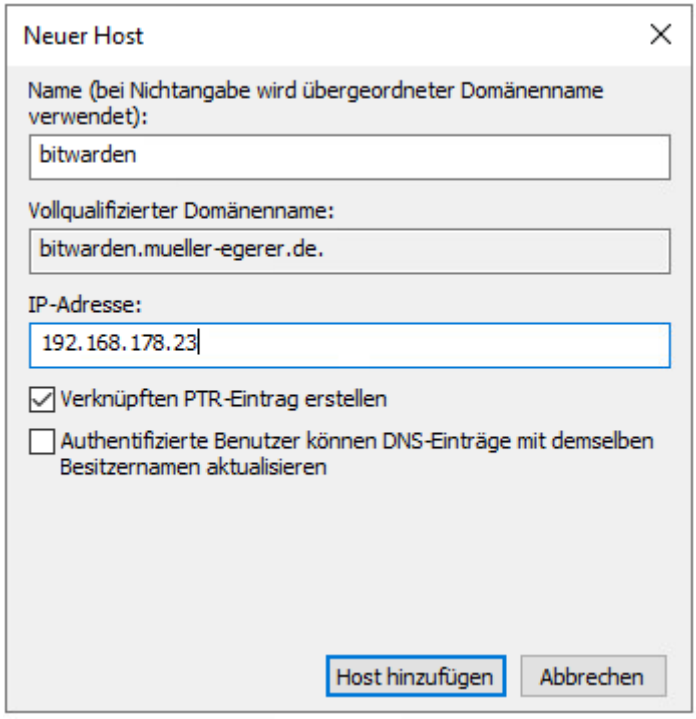


Abbildung 11 DNS Weiterleitung



Gerät / Name	IP-Adresse	Freigaben	Port extern vergeben IPv4	Port extern vergeben IPv6	Selbstständige Portfreigabe
bitwarden-Server	192.168.178.23	HTTP-Server HTTPS-Server HTTP-Server HTTP-Server HTTPS-Server	80 443 8080 4444 5555		0 aktiv

Abbildung 12 Portfreigabe Firewall

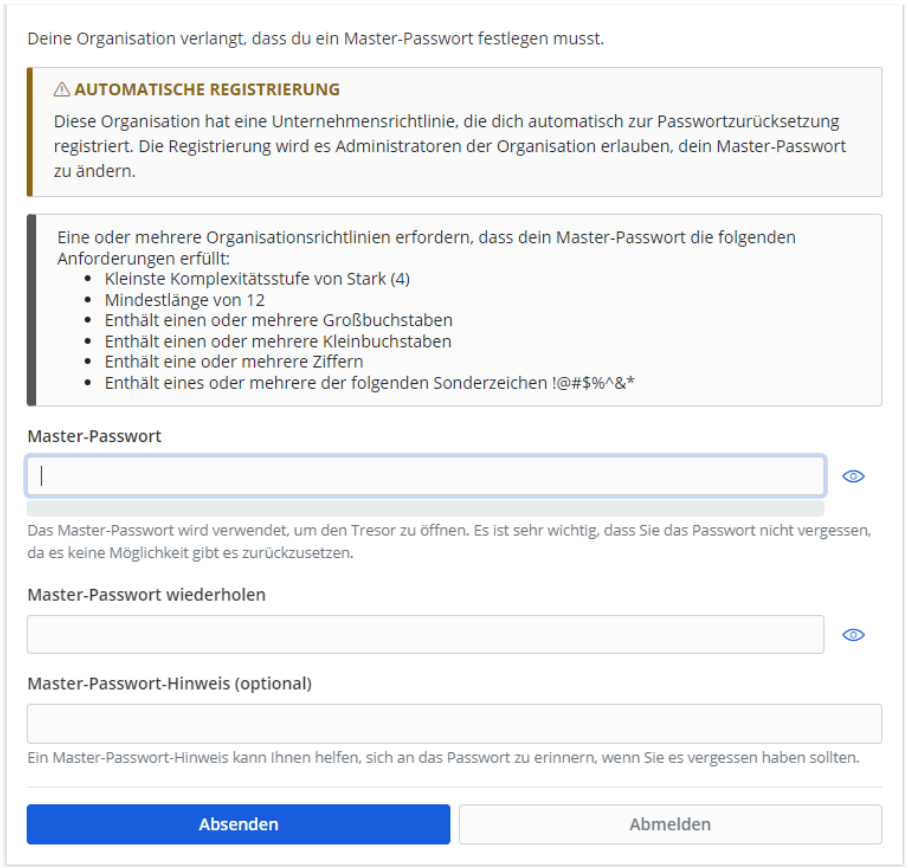


Abbildung 13 Einrichten Konto

Richtlinien

Zwei-Faktor-Authentifizierung verlangen Ein
Benutzer müssen eine Zwei-Faktor-Authentifizierung für ihre persönlichen Konten einrichten.

Master-Passwort-Anforderungen Ein
Mindestanforderungen für die Stärke des Master-Passworts festlegen.

Kontowiederherstellungsverwaltung Ein
Basierend auf der Verschlüsselungsmethode kannst du Konten wiederherstellen, wenn Master-Passwörter oder vertrauenswürdige Geräte vergessen oder verloren gehen.

Passwort-Generator Ein
Mindestanforderungen für den Passwort-Generator festlegen.

Einzelne Organisation Ein
Benutzern verbieten, anderen Organisationen beizutreten.

Single Sign-on-Authentifizierung erfordern Ein
Mitglieder müssen sich per Enterprise Single-Sign-on anmelden.

Persönlichen Tresor entfernen
Benutzern vorschreiben, Tresoreinträge in einer Organisation zu speichern, indem sie die persönliche Eigentumsoption entfernen.

Send entfernen
Mitgliedern nicht erlauben, Sends zu erstellen oder zu bearbeiten.

Send Einstellungen Ein
Lege Einstellungen zum Erstellen und Bearbeiten von Sends fest.

Tresor-Timeout Ein
Konfiguriere ein maximales Tresor-Timeout für alle Benutzer.

Persönlichen Tresor-Export deaktivieren
Mitgliedern nicht erlauben, Daten aus ihrem persönlichen Tresor zu exportieren.

Auto-Ausfüllen aktivieren Ein
Aktiviere die Einstellung "Auto-Ausfüllen beim Laden einer Seite" in der Browser-Erweiterung für alle bestehenden und neuen Mitglieder.

Abbildung 14 Bitwarden Richtlinien Organisation

Quellen

https://unix.stackexchange.com/questions/168794/how-to-get-the-list-of-ports-which-are-free-in-a-unix-server

https://bitwarden.com/help/self-host-an-organization/

https://www.computerweekly.com/de/ratgeber/So-binden-Sie-Ubuntu-Geraete-direkt-an-Active-Directory-an

https://ubuntu.com/desktop/

https://3rdman.de/2019/03/docker-in-windows-server-2019-installieren/

https://www.openkritis.de/it-sicherheitsgesetz/kritis-sektoren.html

https://www.hornetsecurity.com/de/services/365-total-protection-enterprise-backup/

https://de.safetydetectives.com/best-password-managers/1password/

https://support.dashlane.com/hc/de/articles/360013436619

https://1password.com/de/business-pricing

https://de.safetydetectives.com/best-password-managers/enterprise/

https://keepass.info/screenshots.html

https://www.youtube.com/watch?v=AB5UcxBlAiM&ab_channel=RaspberryPiCloud

https://www.experte.de/passwort-manager/lastpass

https://www.dashlane.com/de/pricing

https://de.wizcase.com/password-manager/dashlane/

https://www.proofpoint.com/de/threat-reference/personal-identifiable-information#:~:text=Im%20Prinzip%20kann%20jede%20Information,als%20personenbezogene%20Daten%20betrachtet%20werden.

https://www.bmi.bund.de/DE/themen/verfassung/datenschutz/bundesdatenschutzgesetz/bundesdatenschutzgesetz-node.html

https://www.abmh.de/fhs/crypt/AES2LoopAES/RST_AES.HTML/

https://www.youtube.com/watch?v=b_f0-8CqYKU