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



Von Holger Fischer

Azubi-Ident-Nr: [redacted]

Umschulungs- und Praktikumsbetrieb:

Umschulung bei:

- TBG Technologie und Bildung GmbH

Praktikum bei:

- Müller & Egerer Bäckerei und Konditorei GmbH
- Mittelständig, Inhabergeführt
- >800 Mitarbeiter
- 66 + Filialen
- Projektort: Zentrale in Rastede Leuchtenburg

Agenda

Vorbereitung

- Passwortmanager
- Zeitrahmen
- Ist und Soll

Auswahl und Entscheidung

- Anforderungen
- Nutzwertanalyse
- Kosten

Durchführung

- Bereitstellung der virtuellen Umgebung
- VM-Erstellung
- Installation und Konfiguration von Docker und Bitwarden

Testphase

- Softwaretest
- Fehlerbehebung
- Änderungen zum Projektziel

Abschluss

- Dokumentation und Übergabe
- Ausblick und Fazit

Vorbereitung

Definition und Vorteile Passwort-Manager

- Software zum Speichern und Abrufen von Passwörtern
- Verschlüsselt in einer Datenbank
- Arbeitet mit Tresoren

- Generell wird zwischen zwei Arten von Managern unterschieden:

online	offline
- Tresor liegt auf einem Server, entweder in der Cloud oder on-premise - Vorteil: Mobiles Zugreifen möglich - Nachteil: Unerlaubtes Erreichen von außen möglich	- Tresor liegt lokal auf Endgerät - Vorteil: Passwörter auch ohne Internet erreichbar - Nachteil: Nur auf dem Endgerät verfügbar

Zeitplanung

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

Ist und Soll

Ist-Analyse

- Keine einheitliche Lösung, Passwörter zu speichern
- Keine internen Passwortrichtlinien
- Änderungen nicht Nachvollziehbar
- Benutzer „vergessen“ oft Kennwörter
- Häufiges Rücksetzen durch Administrator

Soll-Konzept

- Einheitlicher, zentralisierter Passwortspeicher
- Automatische Passwortkontrolle
- SSO + MFA

Auswahl & Entscheidung

Anforderungen

- Verschlüsselung
- Vertrauen in den Softwarehersteller
- Integration mit AD
- Gemeinsame Tresore
- Zentrale Verwaltung durch IT
- Kontrolle bei schwachen Passwörtern
- Für zukünftige Projekte geeignet

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	10
Gesamt		14	65	36	**190**	35	177	32	157

GW = Gewichtung; B = Bewertung; G = Gewichtete Bewertung

1 = „sehr niedrig“; 5 = „sehr hoch“

Kosten

Personalkosten			
Position	**Interner Verrechnungssatz**	**Stunden**	**Gesamt**
Praktikant	30,00 €	40	1.200,00 €
Backup-Admin	50,00 €	1	50,00 €
	Gesamt:	41	**1.250,00 €**

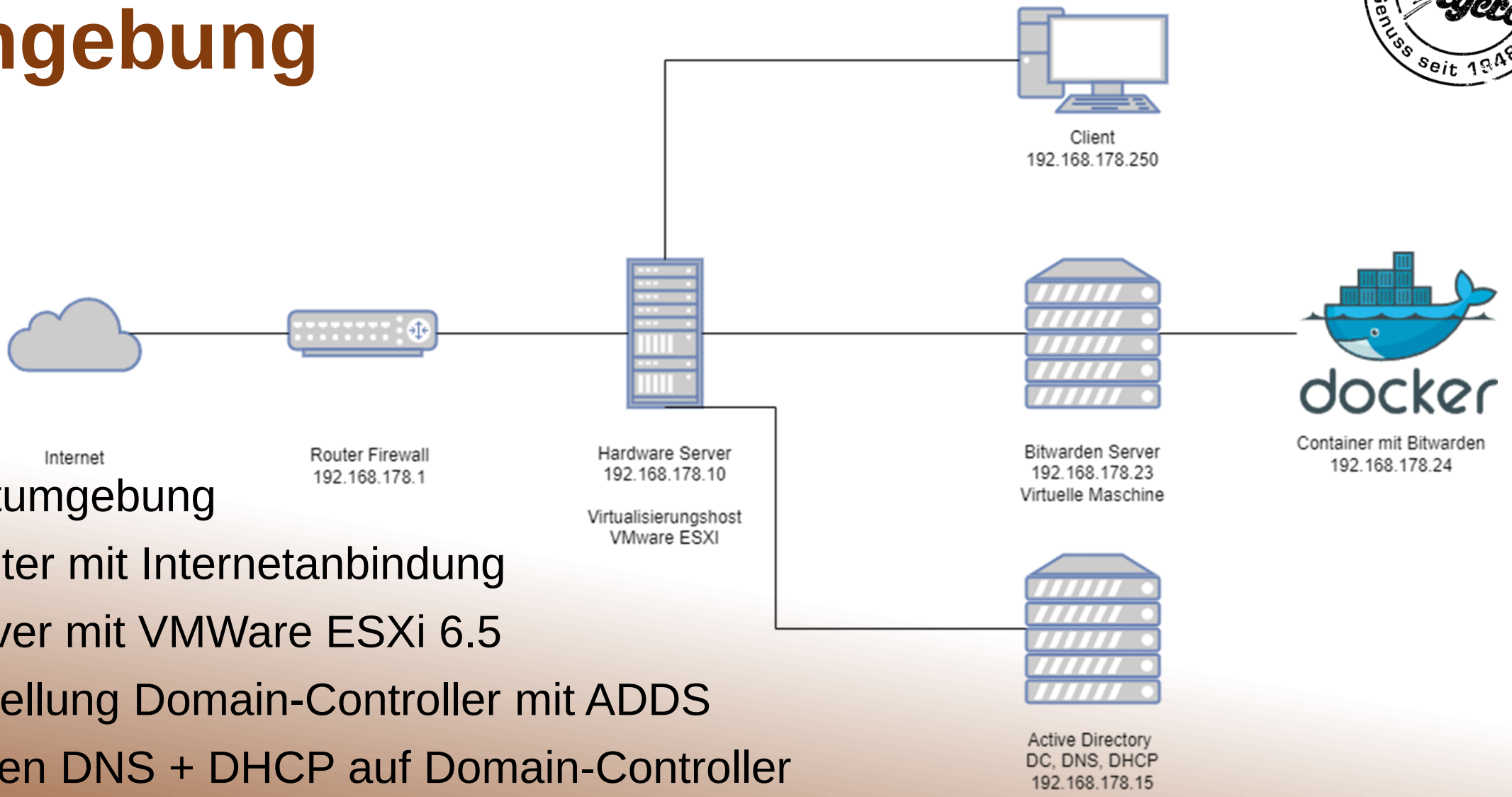
Kosten Server (monatlich)	
Wartung Server	350,00 €
VM (Alle Maschinen)	220,00 €
Gesamt:	**570,00 €**

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

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

Durchführung

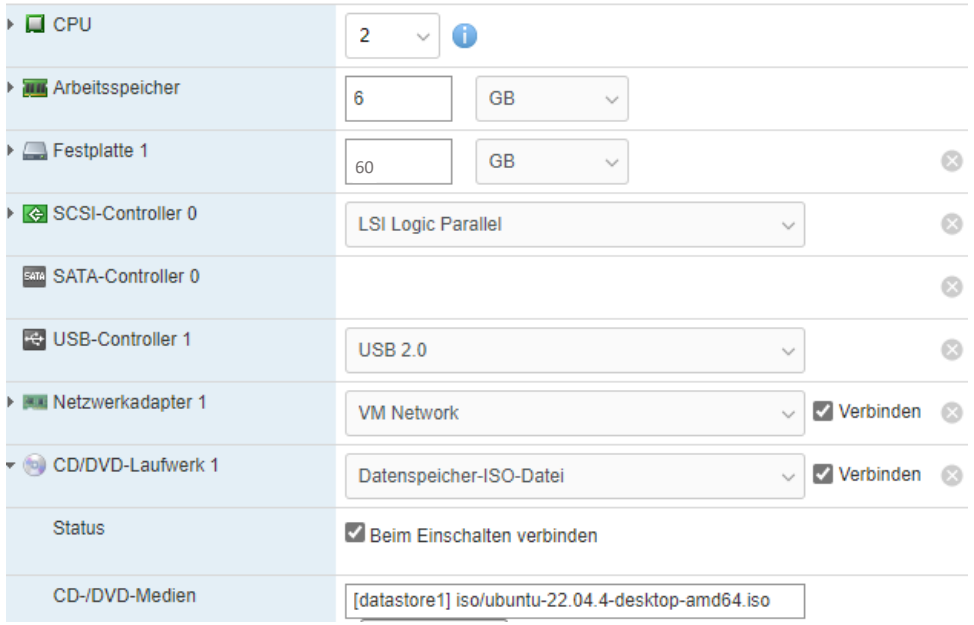
Umgebung



- Testumgebung
- Router mit Internetanbindung
- Server mit VMWare ESXi 6.5
- Erstellung Domain-Controller mit ADDS
- Rollen DNS + DHCP auf Domain-Controller

VM Erstellung

- Linux
- Ubuntu LTS 22.04
- Specs:
  - 6 GB RAM
  - 2 Cores
  - 60 GB Speicher



- Hardware Virtualisierung aktivieren für Docker Container



- Nach der Initialisierung Standard-Installation und Konfiguration des Ubuntu Betriebssystems.

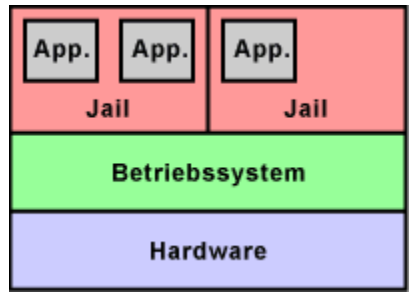
Integration in ADDS

- Hostname ändern, FQDN, (hostnamectl *hostname.domainname*)
- NTP-Service aktivieren (timedatectl)
- DNS-Einstellungen prüfen
- SSSD installieren
- Kerberus-Befehl
- Testen der Namensauflösung und Verbindung
- Beitreten (realm join –v)
- Firewall Portfreigabe

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

Docker

- Was ist Docker:
  - Tool zur Bereitstellung & Verwaltung von Containern
  - Betriebssystem Virtualisierung



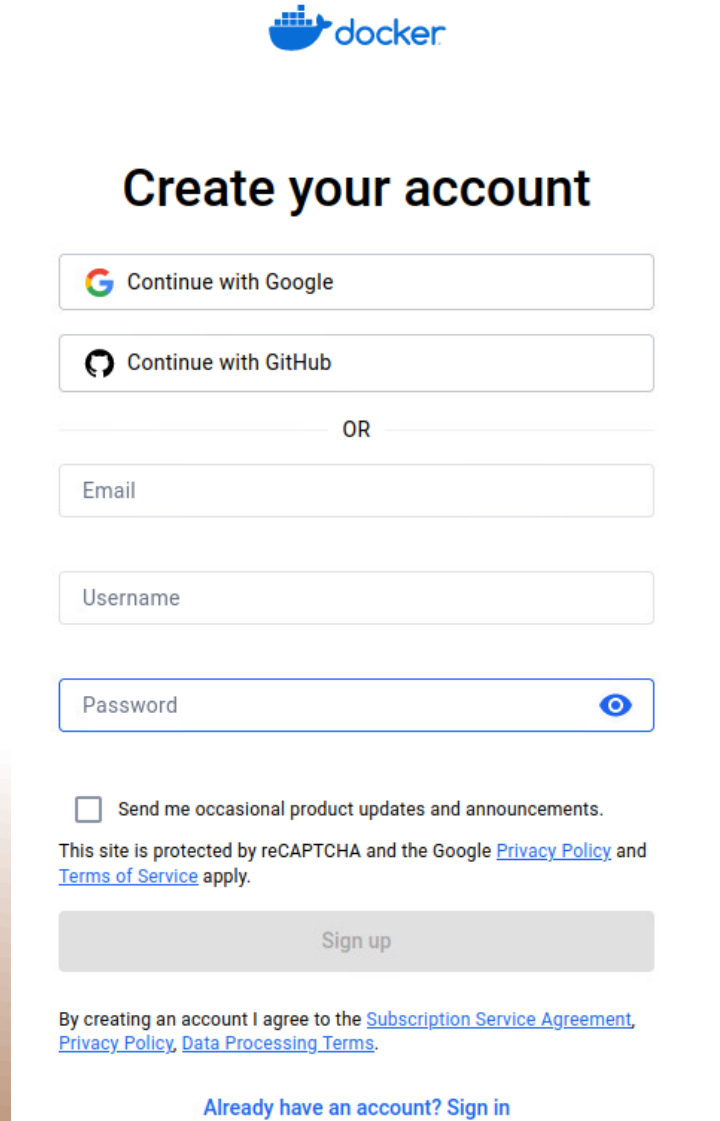
- Warum Docker:
  - Bitwarden wurde auf Dockerbasis erstellt
  - Leichtere Dokumentation und Anleitung
  - Optimiert, da auf „einem“ System

docker

Docker Installation

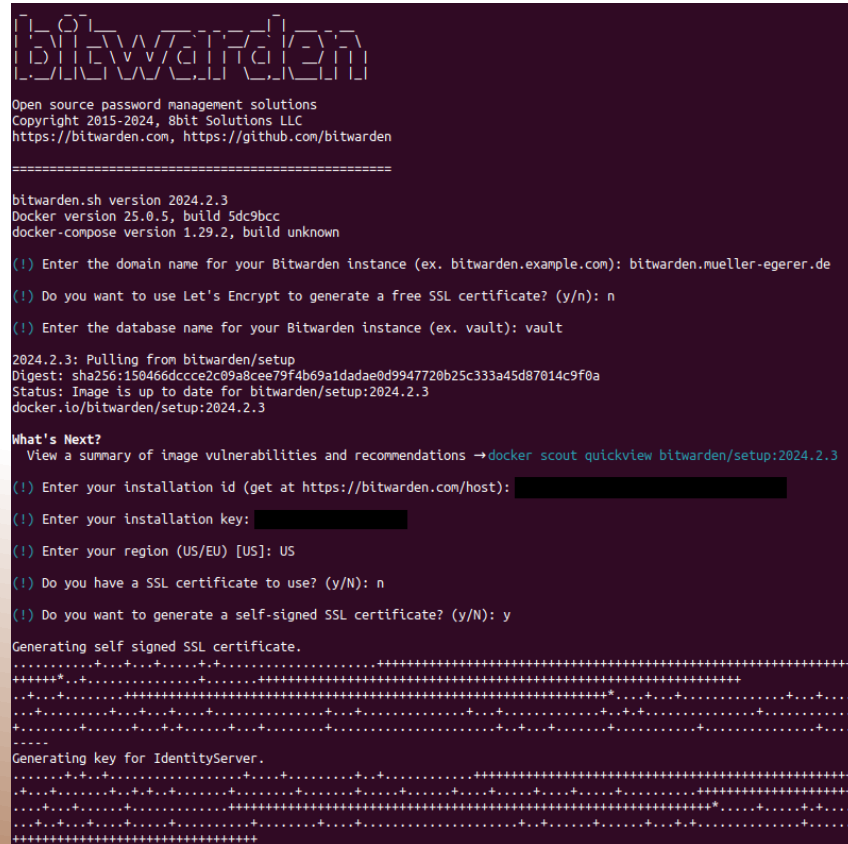
- KVM aktivieren und testen
- Gnome installieren
- Docker herunterladen + installieren (apt-get)
- Starten und neues Konto einrichten

- KVM = Kernel-based Virtual Machine



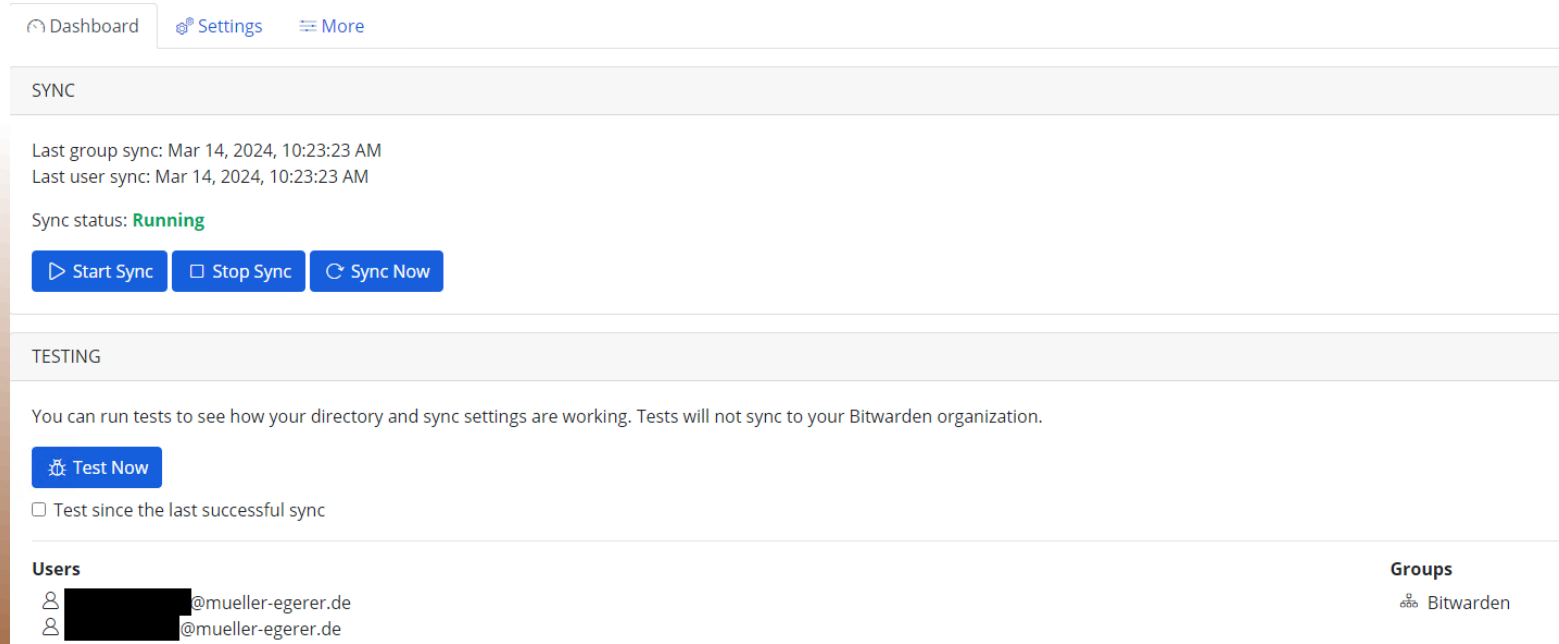
Bitwarden

- Herunterladen + Installieren (apt-get)
- Konfiguration:
  - Domainname (bitwarden.mueller-egerer.de)
  - Online Zertifikatgenerierung Let´s Encrypt (nein)
  - Name der Datenbank
  - Installations-ID + Key
  - Zertifikatserstellung
    - Selfgeneratet SSL certificat – nur Testumgebung!



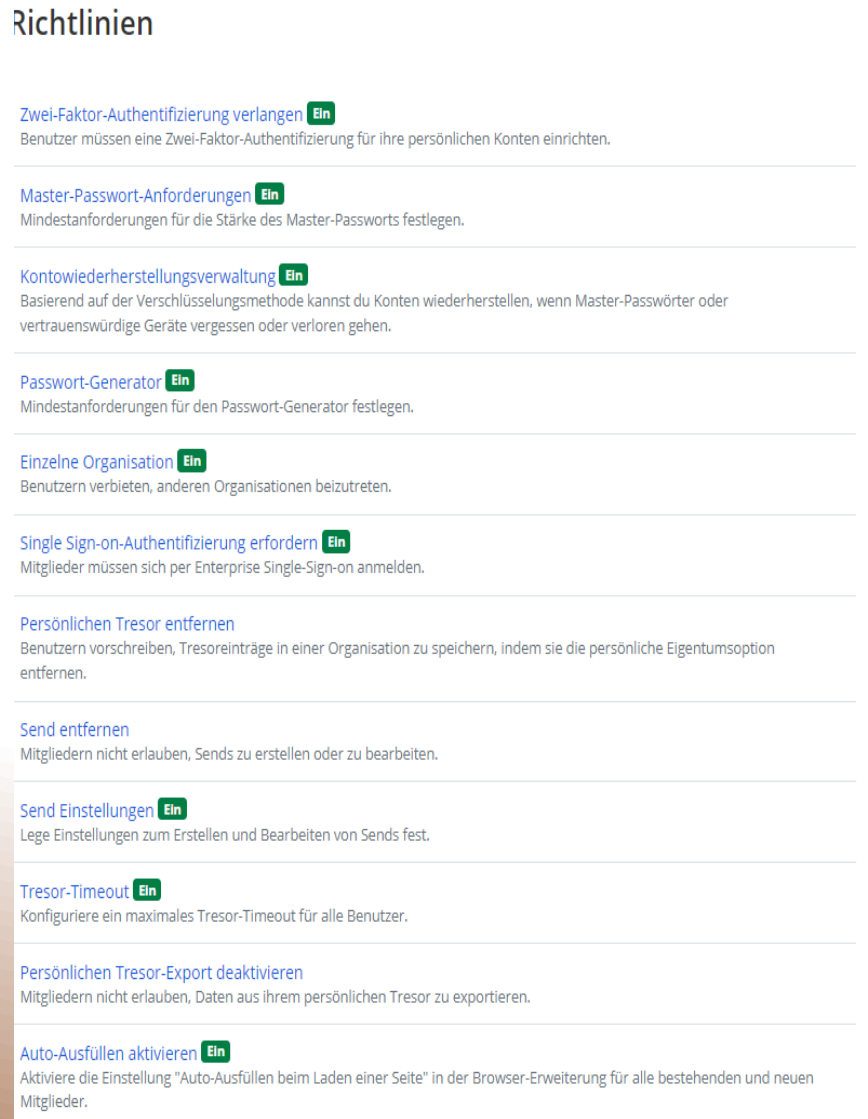
AD Integration Bitwarden

- Directory Connector App
- Anmelden
- Server Hostname, Ports, Pfad und Anmeldedaten
- Synchronisationsoptionen



Unternehmensrichtlinien

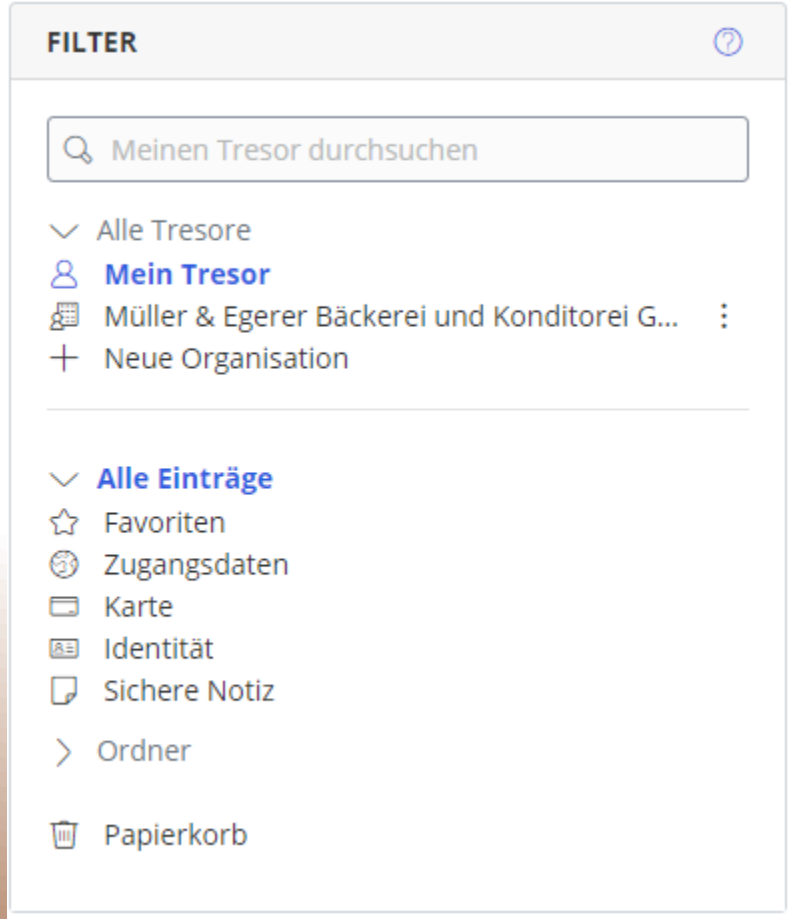
- Zwei-Faktor-Authentifizierung aktivieren
- Richtlinien Masterpasswort
- Passwortgenerator Richtlinien
- Organisationen Mitarbeiter
- SEND & persönlicher Tresor
- Tresor-Timeout
- Auto-Ausfüllen



Testphase

Softwaretest

- Testen der Funktionalität
  - Auto-Ausfüllen
  - Speichern
  - Passwörter finden
  - Schwache Passwörter
  - Ändern der Benutzertimeouts



Was ging schief? / Fehlerbehebung

- Hardware Virtualisierung für VM nicht aktiviert
  - Im Nachhinein die Einstellung aktivieren
- SMTP-Einrichtung
  - Für die NoReply-Adresse musste der SMTP mit den dazugehörigen Daten eingerichtet werden (bitwarden@mueller-egerer.de)
- DNS-Eintrag
  - Damit die zukünftige Adresse im Netzwerk erreicht werden kann, musste der Eintrag eingerichtet werden
- Docker Internetprobleme
  - Docker benötigt eine eigene IP-Adresse

Änderungen zum Projektziel

Im Laufe des Projektes haben sich die Zeiten leicht verändert

Zeit in Stunden	Analyse	Planung	Durchführung	Testphase	Abschluss	Gesamt
Geplant	5,0	7,0	16,0	3,0	9,0	40,0
Durchgeführt	5,0	6,5	14,5	5,0	9,0	40,0
Abweichung		- 0,5	- 1,5	+ 2,0		

Einschränkung Projektumfang:

- Nur Grundkonfiguration für SSO + MFA in Bitwarden durchgeführt
- Integration in Domäne, MDM und Intune erfolgt durch IT-Abteilung

Abschluss

Dokumentation und Übergabe

- Erstellung der Kundendokumentation
- Erstellung eines How-To`s
- Projekt-Übergabe an die IT-Abteilung



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

Ausblick

- Ausrollen in der IT-Abteilung für weitere Tests
- Verbindung mit Mobile Devices
- Nach gründlichen Tests erstes Rollout in der Verwaltung
- Unternehmensweite Integration über MDM/ Intune



Fazit

- Erwerb von Fachkenntnissen im Bereich Linux, Docker und Sicherheit.

- Das Thema Passwörter ist ein sensibles Thema.
- User vergessen, wie oft sie ein Passwort verwendet haben.
- Ein Thema, welches regelmäßige Überprüfung und Auffrischung benötigt.

- Alles in allem kann das Projekt als Erfolg gewertet werden.
- Kundenzufriedenheit

Danke an:

- Müller & Egerer Bäckerei und Konditorei GmbH



- Vielen Dank fürs Zuhören!