Dokumentation zur betrieblichen Projektarbeit

Einführung eines zentralen Passwortmanager

Jana Okrey
Fachinformatik/ Systemintegration

Ashampoo GmbH & CO. KG.
Schafjückenweg 2,
26180 Rastede

Eidesstattliche Erklärung

IHK Oldenburgische Industrie- und Handelskammer

Eidesstattliche Erklärung

Bestätigung über die durchgeführte betriebliche Aufgabe[1]
(Diese Bestätigung ist als Deckblatt online einzureichen, gemeinsam mit dem Report/der Dokumentation.)

Prüfling (vollständige Anschrift und Telefonnummer)	**Ausbildungsbetrieb (vollständige Anschrift)**
Vorname, Name Jana Okrey	Firma Ashampoo GmbH & Co. KG
Straße, Hausnr. [redacted]	Straße, Hausnr. Schafjückenweg 2
PLZ, Ort [redacted]	PLZ, Ort 26180 Rastede
Tel.Nr.: [redacted]	Tel.Nr.: [redacted]

Hinweis vorab: Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung männlicher und weiblicher Sprachformen verzichtet. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.

Ausbildungsberuf

Fachinformatik für Systemintegration

Bezeichnung der betrieblichen Aufgabe

Einführung eines zentralen Passwortmanager

Eidesstattliche Erklärung des Prüflings

Hiermit versichere ich, dass ich die betriebliche Aufgabe unter der Betreuung von

Verantwortlicher im Unternehmen

Jan Iben

selbstständig durchgeführt und die Unterlagen selbstständig zusammengestellt habe.

Dokumente und Textpassagen, die ich nicht selbstständig erstellt habe, sind von mir gekennzeichnet.

[redacted] 10.05.2022 [redacted]

Ort, Datum

Bestätigung des Ausbildungsbetriebes

Wir bestätigen, dass die Angaben des Prüflings richtig sind.

[redacted] 10.05.2022 [redacted]

Ort, Datum Unterschrift des Verantwortlichen, der die Aufgabe betreut hat.

[redacted] 10.05.2022 [redacted]

Ort, Datum Unterschrift des Ausbilders

[1] Zur Vereinfachung wird einheitlich der Begriff „betriebliche Aufgabe" verwendet. Gemeint sind die Fachaufgabe/die Projektarbeit/der betrieblicher Auftrag. Die unterschiedlichen Bezeichnungen entstehen durch die verschiedenen Berufe, die eine Aufgabe online einstellen.

Formblatt

Projektbezeichnung
Einführung eines zentralen Passwortmanager

Persönliche Daten
Jana Okrey
[redacted]

Ausbildungsbetrieb
Ashampoo GmbH & CO. KG.
Schafjückenweg 2
26180 Rastede

Projektverantwortliche*r
Jana Okrey
[redacted]

Inhaltsverzeichnis

Inhalt

Abbildungsverzeichnis

Tabellenverzeichnis

1. Initiierungsphase

Im Rahmen der Ausbildung zur Fachinformatikerin für Systemintegration führe ich in diesem Dokument, das nachfolgend erläuterte IHK-Abschlussprojekt durch. Durch die Dokumentation des Projekts sollen die damit verbundenen Geschäftsprozesse und Handlungsprozesse betrachtet werden.

1.1. Projektziel

Das Ziel des Projekts ist es, einen den Anforderungen des Kunden entsprechenden Passwortmanager auszuwählen und einzuführen. Grund dafür ist die Ablösung des lokal gehosteten Passwortmanagers, der nur von wenigen Abteilungen genutzt wird. Durch den Austausch der Systeme wird eine einheitliche Nutzung eines Passwortmanagers im Unternehmen angestrebt. Dadurch soll eine sichere Verwaltung der Firmenpasswörter geregelt sein, da mehr als 80 % aller Datendiebstähle auf schwache Passwörter zurückzuführen sind.

1.2. Projektumfeld

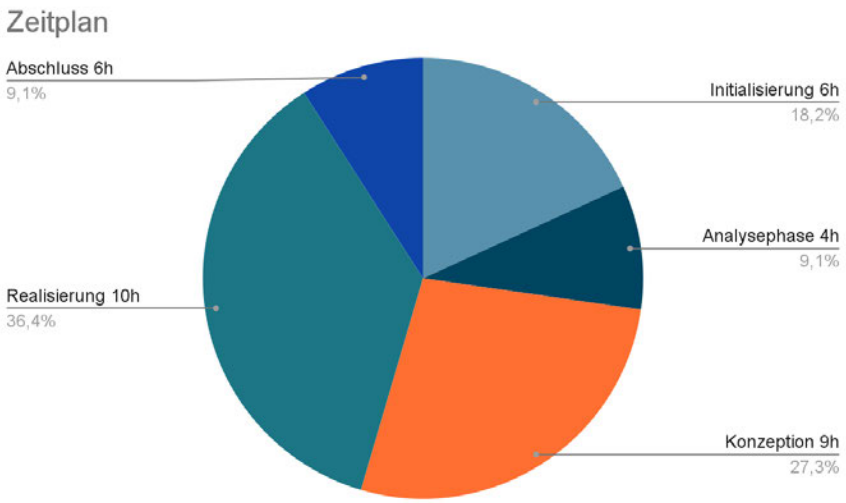
Der Auftraggeber und Ausbildungsbetrieb ist die Ashampoo GmbH und CO. KG mit Sitz in Rastede. Das 1999 gegründete mittelständische Unternehmen entwickelt und vertreibt weltweit über das Internet Softwareprodukte. Die Firma Ashampoo gehört zur //CRASH Unternehmensgruppe, in der momentan 120 Mitarbeiter*innen beschäftigt sind. Die Organisationsform des Unternehmens entspricht der Matrixorganisation, um möglichst kunden- und prozessorientiert zu arbeiten. Für jedes Softwareprodukt gibt es einzelne Teams, die aus verschiedenen Abteilungen zusammengestellt werden. Die Abteilungen sind: Buchhaltung, Vertrieb, Marketing, Design, Entwicklung und die Administration.

1.3. Projektabgrenzung

Das beschriebene Projekt umfasst die Evaluierung und die Einführung des neuen Passwort-Management-Systems. Für die Evaluierung werden die Anforderungen der Unternehmung zusammengestellt. Anhand dieser Auswertung wird ein passendes Produkt herausgesucht. Die Einführung des Systems umfasst die Vorplanung und Vorkonfiguration sowie die Migration der Daten aus dem alten Passwortmanagement-System. Zum Projekt gehört nicht der Austausch bestehender unsicherer Passwörter, sowie die Einrichtung der Multi Faktor Austenitisierung (MFA) für alle Accounts.

1.4. Projektablauf

Das Projekt gliedert sich in vier Phasen. Das folgende Diagramm bietet eine grobe Übersicht der zeitlichen Planung der Projektphasen:



(Abbildung A: Projektphasen mit Zeiteinteilung)

Eine detaillierte Zeitplanung ist dem Anhang zu entnehmen (V, Aufgabenplanung, detailliert).

1.5. Stakeholder Management

Durch das Stakeholder Management ermittelt der Prüfling die Bedürfnisse der wichtigsten Interessensgruppen, um diese bei der Projektplanung und der Projektdurchführung zu berücksichtigen. Dadurch sollen mögliche Gefahren vom Projekt abgewendet werden. Um die Mitarbeiter einschätzen zu können, wird eine Umfrage erstellt, in der erfragt wird, ob die Mitarbeiter bereits einen Passwort-Manager nutzen und wenn ja, welchen. Was sie von Passwort-Managern halten oder ob sie noch gar keine Berührungspunkte mit einem Passwort-Manager hatten.

Die Stakeholder werden in folgende Gruppen eingeteilt:

Die betroffenen Stakeholder: Mitarbeiter die den Passwortmanager nutzen. Hier ist es wichtig vor Projektplanung ihre Bedürfnisse abzufragen. Die einzelnen Mitarbeiter können unterschiedlich zu einem neuen Passwort-Management-Tool stehen. Daher ist es wichtig, die Mitarbeiter in verschiedene Gruppen einzuteilen. Die Befürworter, benötigen keine besondere Behandlung. Die Skeptiker hingegen müssen sensibilisiert werden. Die Gruppe, die sich schwer mit Veränderungen anfreundet, benötigt Hilfe bei der Einarbeitung. Durch gezielte Umfragen können die Mitarbeiter in die Gruppen eingeordnet werden und dementsprechend behandelt werden.

Die IT-Abteilung wird die neue Software verwalten müssen und wirkt direkt an der Umsetzung mit, daher gehören sie zu den beteiligten Stakeholdern. Da die Abteilung ein großes Interesse daran hegt, die Unternehmensdaten zu schützen sind sie der Umsetzung des Projekts sehr positiv zugestimmt.

Des Weiteren gibt es noch die Gruppe an Steakholdern, die weder betroffen oder beteiligt sind, aber dennoch bestreben auf das Projekt einzuwirken. Dazu gehört in diesem Fall die Geschäftsführung. Sie ist wie die IT-Abteilung einzuordnen, dennoch haben sie den finanziellen Rahmen mehr im Blick, weshalb bei ihnen für ein kostspieliges Tool eventuell Überzeugungsarbeit geleistet werden muss.

1.6. Erstellung eines Projektauftrags

Im Anschluss der Projektinitialisierung wird der Projektauftrag erstellt. Hier werden die wichtigsten Informationen und Ziele festgehalten, sowie die initialen Risiken, kritische Erfolgsfaktoren und die Projektabgrenzung. Der Projektauftrag ist dem Anhang zu entnehmen (B. Projektauftrag).

1.7. Abweichung vom Projektantrag

Die Abweichung vom Projektantrag, die hier beschrieben wird, beeinflusst einzig die Projektphasen und die Zeitplanung. Inhaltlich findet keine Abweichung vom Projekt statt.

Der Prüfling bewertet die einzelnen Projektphasen zeitlich neu. Die Analysephase beträgt nun 4 Stunden, da die Analyse der Ist-Situation zum größten Teil aus Mitarbeiterumfragen besteht, die erstellt und ausgewertet werden müssen. Dafür wird für die Projektrealisierung nur noch mit 10 Stunden geplant, da der Prüfling die Vorbereitung der Projektdokumentation aus der Realisierungsphase herausnimmt und komplett in die Abschlussphase schiebt. Für den Projektabschluss werden daher 6 Stunden eingeplant.

2. Analysephase

2.1. Durchführung Ist-Analyse

Die derzeitige IT-Infrastruktur für die Sicherung von Passwörtern besteht aus dem Passwortmanager “Password Depot”, der von drei Abteilungen genutzt wird.

2.1.1. Funktionsanalyse

Die Software läuft clientseitig und sichert die Kennwortdateien auf einem Enterprise Server der als On Premises-Lösung gehostet wird. Der Datenaustausch zwischen dem Enterprise Server und den Clients wird durch AES-265-Bit verschlüsselt. Die Client-Server-Verbindung erfolgt über TCP/IP (IPv4/IPv6). Zurzeit wird das Password Depot von drei Abteilungen genutzt. Die Buchhaltung, Administration und Geschäftsführung verfügen über eine Passwort Datenbank. Die GUI des Password Depots ist relativ unübersichtlich und eher tabellenartig. Während der Einspielung von Updates ist der Zugriff auf die Passwörter eingeschränkt. Der administrative Aufwand ist relativ hoch, da nicht nur der Server aktualisiert werden muss, sondern auch alle Clients.

2.1.2. Prozessanalyse

Durch die Corona Epidemie wurde vermehrt aus dem Homeoffice gearbeitet. Die Arbeit mit dem Password Depot aus dem Homeoffice bedingt eine ständige VPN-Verbindung zum Firmennetzwerk, um mit dem Passwortmanager arbeiten zu können. Ohne Netzwerkverbindung bleibt nur der Zugriff auf eine offline Datei der Datenbank, die auf dem Client zwischengespeichert wird. Dadurch konnten Passwortänderungen aus dem Homeoffice nicht vollzogen werden. Abteilungen, die das Password Depot nicht nutzten, können Kennwörter nicht zentral speichern. In Krankheitsfällen gibt es daher oft das Problem, dass auf benötigte Passwörter nicht zugegriffen werden kann. Passwörter werden meist digital unverschlüsselt weitergegeben, da es keine einheitliche Möglichkeit gibt, Passwörter einfach sicher verschlüsselt weiterzugeben. Einige Abteilungen nutzen eigene Passwort-Management-Tools, schreiben ihre Kennwörter handschriftlich auf oder nutzten nur ein Kennwort, welches sie dann nicht speichern müssen. Dieses Nutzerverhalten stellt ein hohes Sicherheitsrisiko dar.

2.2. Durchführung Soll-Analyse

Im Anschluss an die Ist-Analyse folgt die Ausarbeitung des Soll-Zustands. Damit die Anforderungen der verschiedenen Zielgruppen herausgearbeitet werden können, wurden die verschiedenen Stakeholder Gruppen befragt.

Die derzeitige Verwaltung der Passwörter des Unternehmens stellt ein hohes Sicherheitsrisiko dar, dass möglichst schnell beseitigt werden muss. Unternehmens- und Kundendaten sollten bestmöglich geschützt werden. Im schlimmsten Fall können Passwörter durch Datenbank Leaks ins Internet gelangen und “Bad Boys” können sich ins Firmennetz einwählen, da Mitarbeiter immer das gleiche Passwort auch bei anderen Webapplikationen verwenden. Hinzu kommt, dass sich die Funktionalität des derzeitig eingesetzten Tools mit der Zeit weiterhin verschlechtert. Daher ist eine zeitnahe Projektumsetzung von starker Dringlichkeit. Um das Sicherheitsrisiko zu mindern, soll ein neuer Passwortmanager eingeführt werden, der von allen Mitarbeitern im Unternehmen genutzt wird. Die neu eingesetzte Lösung soll Passwörter sicher speichern und verwalten können. Des Weiteren sollen Zahlungsdaten sicher verwahrt werden. Ein wichtiges neues Feature, das die Software erfüllen muss, ist die Möglichkeit Kennwörter sicher an andere Mitarbeiter weitergeben zu können. Die vorhandenen Passwortdatenbanken sollen in das neue System migriert werden. Dafür soll die neue Software einfache Importwege bieten, damit der Import möglichst schnell vollzogen werden kann. Wichtig ist eine leichte Bedienbarkeit des Tools mit einer einfachen und klaren GUI. Der Passwortmanager soll auch von außerhalb erreicht werden können das bedeutet, dass der Zugriff nicht aus dem internen Netz beschränkt werden soll. Die Software soll dem Mitarbeiter die Möglichkeit bieten schnell randomisierte Passwörter zu erstellen. Da die Allgemeinheit schnell dazu neigt auf Standardpasswörter wie “Passwort” oder dem eigenen Namen zurückzugreifen. Um dieses Verhalten möglichst einschränken zu können soll der Passwortmanager über Richtlinien verfügen, die auf Nutzergruppen angewendet werden können. Im Unternehmen müssen auch Lizenzen und Zertifikate verwaltet werden, daher sollte die neue Software auch die Speicherung dieser anbieten.

Nach der Ausarbeitung des Soll-Konzepts, in dem alle Anforderungen gesammelt wurden, geht das Projekt in die Konzeptphase über.

3. Konzeptphase

3.1. Evaluation eines geeigneten Passwortmanagers

Innerhalb der Phase wird durch Auswertung technischer und wirtschaftlicher Kundenanforderungen ermittelt, welche Software als passende Lösung in Frage kommt. Der ausgewählte Passwort-Manager wird dem Projektauftraggeber vorgestellt. Anschließend werden Ressourcen und Arbeitspakete für das Projekt geplant.

3.1.1. Technische Anforderungen

Durch die Stakeholder Gruppen wurden folgende Anforderungen ermittelt:

- Passwörter sicher speichern
- SSL/TSL Verschlüsselung
- AES 256-bit Verschlüsselung
- Passwörter werden lokal gespeichert
- Multi-Faktor-Authentifizierung
- Detaillierte Richtlinienverwaltung
- Benutzer und Gruppenstrukturen
- Speicherungen von Lizenzen, Zahlungsdaten und Zertifikate
- einfache Benutzeroberfläche
- einfache Import und Exportmöglichkeiten
- Passwörter einfach generieren zu lassen
- Passwörter sicher teilen
- Zugriff übers Internet
- Cloud-Dienst

3.1.2. Wirtschaftlichkeitsanalyse

Für die Wirtschaftlichkeitsbewertung sind die Anschaffungskosten, die Personalkosten für die Umsetzung und die laufenden Kosten zu berücksichtigen. Direkte Anschaffungskosten bestehen nicht, da die Software als Abo-Modell bezahlt wird. Die monatlichen Abonnement-Kosten zählen zu den laufenden Kosten. Diese ergeben sich aus den Lizenzkosten pro Mitarbeiter und die Personalkosten für Administration der neuen Software. Demgegenüber steht die Schließung eines Sicherheitsrisikos. Die geringe Passwortsicherheit stellt ein Risiko für Unternehmensdaten dar. In diesem Fall ist es schwierig einen genauen Ertrag zu ermitteln. Durch den Verlust von Firmendaten würde eine sehr hohe Schadenssumme entstehen. Daher ist es erstrebenswert, die bestmögliche Lösung herauszuarbeiten. Die Kostenzusage erfolgt durch den Projektauftraggeber.

3.1.3. Auswahl von geeigneten Systemen

Nach der Ermittlung der technischen und wirtschaftlichen Anforderungen recherchiert der Prüfling anhand der Erkenntnisse nach geeigneten Softwarelösungen. Auf dem Markt existieren sehr viele Anbieter, ein großer Teil konnte bereits vorher ausgeschlossen werden, da sie keine Cloud Lösung anbieten. Zur näheren Auswahl stehen Keeper, LastPass und Dashlane.
Die ausgewählten Produkte sind genau auf die Kriterien zu prüfen, die zu Beginn durch den Prüfling ermittelt wurden: SSL/TSL Verschlüsselung für eine sichere Datenübertragung, Verschlüsselung der sensiblen Daten nach AES 256-bit Verschlüsselung, da dieser Algorithmus allgemein als nicht zu brechen gilt und auch von Banken und dem US-Militär zur Verschlüsslung eingesetzt

wird, Multi-Faktor-Authentifizierung, um den Zugriff vor Cyberangriffen zu schützen, Richtlinienverwaltung, um zugeschnittene Sicherheitsrichtlinien für verschiedene Personen und Abteilungen erstellen zu können, einfache Bedienbarkeit, damit auch Computerlaien ihre Passwörter einfach verwalten können. Die Informationen zu den einzelnen Lösungen wurden über die Webseiten der einzelnen Hersteller recherchiert. Zusätzlich wurde von allen Programmen eine Testversion heruntergeladen, um den Passwortmanager ausgiebig zu testen.

„Keeper“, ein Passwortmanager des Herstellers Keeper Security Inc., wird als Software as a Service (SaaS) Passwortmanager angeboten. Keeper bietet alle Funktionalitäten, um die vorher definierten Anforderungen zu erfüllen. Jedoch ist die Benutzeroberfläche im Vergleich weniger übersichtlich gestaltet. Zudem erfordert die Speicherung von Lizenzen, Zahlungsdaten und Zertifikaten mehr Aufwand, da es keine Vorlagen gibt und die Formulare individuell angelegt werden müssen. Der Preis beträgt je Benutzer 6,50€ pro Monat.

Eine weitere Lösung bietet LogMeIn mit ihrem Passwortmanager „LastPass“. Dieser konnte alle funktionalen Anforderungen erfüllen und überzeugt mit einer sehr übersichtlichen und klaren Benutzeroberfläche. Die Richtlinienverwaltung ist sehr detailliert und individuell anpassbar. LastPass bietet jeden Enterprise User eine kostenlose LastPass Family Lizenz für den privaten Gebrauch. Der private Account kann mit dem geschäftlichen Account verknüpft werden, was ein großer Bonus für den Mitarbeiter darstellt. Preistechnisch schneidet LastPass am besten ab. Der Preis liegt bei 5,70€ im Monat.

Zuletzt folgt die Lösung von Dashlane Inc.,
ihr gleichnamiger Passwortmanager erfüllt ebenso fast alle Anforderungen. Leider gibt es kein Formular, um Softwarelizenzen zu speichern. Preislich ist Dashlane am teuersten.

3.1.4. Auswertung

Die Passwortmanager unterscheiden sich nur geringfügig. Sie erfüllen fast alle die vorher definierten Kriterien. Bei der detaillierten Richtlinienverwaltung konnte sich LastPass durchsetzen. Im Vergleich bietet LastPass eine viel detailliertere Richtlinienverwaltung. Richtlinien können auf einzelne Benutzer oder Gruppen angewendet werden, sodass bei Abteilungen wie der Buchhaltung oder der IT-Administration schärfere Richtlinien greifen als bei anderen. Dazu gibt es eine sehr große Auswahl an einstellbaren Richtlinien. LastPass bietet ebenso als einziger Passwortmanager die Möglichkeit, Softwarelizenzen zu speichern, ohne vorher ein eigenes Formular erstellen zu müssen. Die in Punkt 3.1.3 ermittelten Passwortmanager werden in nachfolgender Nutzwertanalyse (Tabelle Ⅰ) miteinander verglichen. Die Entscheidung über die Gewichtung der in 3.1.3 genannten Kriterien trifft der Prüfling. Erfüllt ein System die Anforderungen in vollem Umfang werden maximal fünf Punkte vergeben.

Kriterium	Gewichtung	Keeper	LastPass	Dashlane
Passwörter sicher speichern		x	x	x
SSL/TSL Verschlüsselung		X	X	x
AES 256-bit Verschlüsselung		x	X	x
Multi-Faktor-Authentifizierung		x	x	x
Passwörter lokal speichern Zero Knowledge-Prinzip		x	x	x
Sicherheit	30%	5 | 1,5	5 | 1,5	5 | 1,5
Detaillierte Richtlinienverwaltung		nicht detailliert genug	x	nicht detailliert genug
Benutzer und Gruppenstrukturen		x	x	x
Verwaltung	25%	2 | 0,5	5 | 1,25	3 | 0,75
Speicherungen von Lizenzen, Zahlungsdaten und Zertifikate		Felder selbst anlegbar	x	Kein Formular für Softwarelizenzen
Einfache Import und Exportmöglichkeiten		x	x	x
Passwörter einfach generieren zu lassen		x	x	x
Passwörter und Passwort Ordner sicher teilen		x	x	x
Zugriff übers Internet		x	x	x
Anbindung ans Aktiv Directory		x	x	x
Funktionalität	20%	3 | 0,6	5 | 1	4 | 0,8
Einfache Benutzeroberfläche			x	
Bedienbarkeit	15%	2 | 0,3	4 | 0,6	3 | 0,45
Cloud-Dienst		x	x	x
Preis pro Monat je Benutzer		6,50€	5,70€	8€
Kosten	10%	4 | 0,4	5 | 0,5	2 | 0,2
Gesamt	100%	3,3	4,4	3,7

(Tabelle I Nutzwertanalyse)

Entsprechend dem Resultat der Nutzwertanalyse spricht der Prüfling gegenüber dem Projektauftraggeber, Herrn Duden, die Produktempfehlung für LastPass aus. Dieser wurde zugestimmt.

3.2. Planung von Arbeitspaketen für die Realisierung

Im Anschluss beginnt der Prüfling zu planen, welche Schritte im Rahmen der Realisierungsphase anfallen (Siehe Tabelle VI). Als erstes geht es um den Kauf und die Einrichtung. Anschließend wird für alle Admin-Team-Mitglieder ein Account erstellt, damit diese das Programm bereits kennenlernen können, um Mitarbeiter nach dem Rollout direkt unterstützen zu können. In einem Meeting mit dem Admin-Team und CTO werden die möglichen Richtlinieneinstellungen besprochen und diskutiert. Die Ergebnisse werden in einem Besprechung Protokoll festgehalten und anschließend zur Einstellung der Richtlinien herangezogen. Das Meeting-Protokoll befindet sich im Anhang. Um herauszufinden welche Passwortmanager bisweilen im Unternehmen genutzt werden, wurde eine Umfrage erstellt. Aus den Ergebnissen werden Informationen für spätere Anleitungen gesammelt, um den Mitarbeitern Export Anleitungen für ihre alten Passwortmanager zur Verfügung zu stellen. Darauf erfolgt der Export der Passwortdatenbanken des Passwort Depots, welches von drei Abteilungen im Unternehmen genutzt und von der IT-Abteilung verwaltet wurde. Anschließend werden Anleitungen im Unternehmens-Wiki Confluence erstellt. In den Artikeln wird LastPass vorgestellt, die Einrichtung erklärt, eine Funktionsübersicht gegeben, die Handhabung mit dem Passwort Managers erläutert und die oben bereits erwähnten Export Anleitungen bereitgestellt. Danach erfolgt der Systemtest innerhalb der IT-Abteilung. Sie nutzen den Passwortmanager im Geschäftsalltag und prüfen, ob alle Eigenschaften nach dem Export funktionieren. Nach dem erfolgreichen Systemtest erfolgt der erste Rollout an die Buchhaltung. Diese Abteilung wird getrennt von den übrigen Abteilungen an den Passwortmanager herangeführt, da diese Abteilung eine individuelle Betreuung von der IT-Abteilung benötigt. Anschließend erfolgt der Rollout an alle weiteren Mitarbeiter. Um ihnen den Passwort-Manager vorzustellen, wird ein Blog-Post veröffentlicht. Nachdem alle Mitarbeiter ihren Account eingerichtet haben, werden die Abteilungen als Gruppen abgebildet, um diese einfacher verwalten zu können. Im Zuge dessen wird die Benutzerliste kontrolliert, ob auch alle Mitarbeiter ihren Account eingerichtet haben. Anschließend ist die Realisierungsphase abgeschlossen. Eine tabellarische Auflistung aller Aufgaben mit Zeiteinschätzung ist dem Anhang zu entnehmen (VI, Planung Arbeitspakete Realisierungsphase).

3.3. Ressourcenplanung

An dieser Stelle erfolgt durch den Prüfling eine Planung aller Ressourcen, die für eine erfolgreiche Umsetzung des Projektes erforderlich ist.

3.3.1. Personalplanung

Das Projekt ist für einen Zeitraum von 35 Arbeitsstunden von denen 100% vom Prüfling umgesetzt werden. Bei einem Stundensatz des Prüflings in Höhe von 40€ brutto, entspricht die Dienstleistung der Projektumsetzung 1.400€ brutto.

3.3.2. Sachmittelplanung

Verwendete Sachmittel sind zum einen folgende Hardware: Das Notebook des Prüflings, der über das betriebsinterne WLAN einen Internetbrowsers nutzt, um den Passwortmanager einzurichten. Für die Migration der Passwörter wird die Software Password Depot und die Tabellenkalkulationssoftware Excel genutzt, um die generierten CSV Dateien anzupassen. Um alle Mitarbeiter über die neue Software zu informieren, wird ein Blogpost über die Wiki Software Atlassen Confluence erstellt. Für die Festlegung der Sicherheitsrichtlinien wird ein Meeting Raum genutzt, das sich das Admin Team mit dem CTO zusammenzusetzen kann.

3.3.3. Terminplanung

Nach Angabe der IHK Oldenburg ist das Projekt im Zeitraum vom 15.02 - 15.04.2022 durchzuführen. Innerhalb des IT-Abteilung einigt man sich auf einen Projektzeitraum von Montag dem 21.02 bis Montag, dem 28.02.2022. Dabei bestehen folgende relevante Termine. Donnerstag der 24.02 wird nicht als Arbeitstag genutzt, da sich der Prüfling in der Berufsschule befindet.

Phase	Datum
Analyse	21.02,22.02
Konzeption	22.2, 23.02
Realisierung	23.02-25.02
Abschluss	28.02

(Tabelle II Terminplanung)

3.3.4. Kostenplanung

Der letzte Schritt der Konzeptphase besteht aus der Erstellung einer Übersicht der Gesamtkosten für die Durchführung des Projektes. Dabei fallen die in den Punkten 3.1.3 und 3.3.1 errechneten Anschaffungs- und laufenden Kosten sowie der Dienstleistungsaufwand an. Da es sich bei den Lizenzen für LastPass um ein Abo-Modell handelt, werden hier zur Kalkulation die Lizenzkosten für ein Jahr berechnet.

Artikel	Menge	Stückpreis*	Gesamt
LastPass Lizenz p.A.	70	68,4€	4.788€
Stundenlohn Prüfling	35	40€	1.400€
Summe*			6.188€

(Tabelle III Kostenkalkulation)

4. Realisierungsphase

In der Realisierungsphase wird die geplante Einführung des Passwortmanagers durchgeführt. Die Umsetzung ist nach der Migration der vorhandenen Passwort Datenbanken und Einrichtung aller Mitarbeiter Accounts abgeschlossen. Vor der Einrichtung der Mitarbeiter Accounts wird ein Blogpost veröffentlicht, um alle Mitarbeiter über den neuen Passwortmanager zu informieren. In dem Blogartikel sind die erstellten Anleitungen verlinkt.

4.1. Vorbereitung der Einführung

Die Umsetzung des Projektes beginnt am Montag, den 21.02.2022. Folgend werden die Schritte der Realisierungsphase, die für die Einführung des Passwort Managers benötigt werden, beschrieben.

4.2. Einrichtung der Umgebung

Als ersten Schritt der Realisierungsphase kauft der Prüfling die nötigen Lizenzen ein. Anschließend konfiguriert er die LastPass Enterprise Umgebung. Dazu hinterlegt er alle nötigen Daten (Unternehmensdaten, Zahlungsinformationen, Benachrichtigung-Möglichkeiten) im Admin Portal.

4.3. Konfiguration des neuen Systems

Als nächstes beginnt der Prüfling das System zu konfigurieren. Da es sich um einen Passwortmanager handelt, müssen einige Sicherheitseinstellung getroffen werden. Dazu initiiert der Prüfling ein Meeting mit dem gesamten Admin Team und CTO.

4.3.1. Richtlinien des Passwort Managers festlegen

In dem Meeting werden die möglichen LastPass Richtlinien besprochen. Der Passwortmanager bietet hier sehr viele Einstellungsmöglichkeiten. Damit sich alle Teilnehmer auf das Meeting vorbereiten können, erstellt der Prüfling einen Confluence Eintrag in dem betriebsinternen Wiki mit allen wichtigen Informationen und listet die zu besprechenden Richtlinien auf. Eine wichtige Entscheidung betrifft die Aktiv Directory Integration. In dem Meeting wurde entschieden LastPass unabhängig vom Aktiv Directory zu verwalten, um die Passwörter getrennt vom restlichen System zu verwahren. [redacted] Alle weiteren Entscheidungen können aus den Anlagen entnommen werden (siehe Anlage C. Meeting Protokoll).

4.3.2. Einstellung der Richtlinien

Nach dem Meeting konfiguriert der Prüfling alle besprochenen Richtlinien. Dazu meldet er sich im Admin Bereich an und wählt unter Einstellungen “Richtlinien”. Um die Arbeit sorgfältig durchzuführen, geht der Prüfling alle 90 Richtlinien noch einmal einzeln durch und stellt alle Richtlinien entsprechend ein.

4.3.3 Migration der Passwörter aus dem alten System

Als nächstes folgt der zeitaufwendigste Schritt der Realisierungsphase, die Migration der Passwortdatenbanken aus dem alten System. Für die Migration sind drei Passwortdatenbanken vorgesehen. Die Datenbank der Administration, Geschäftsführung und die der Buchhaltung. Für die Migration wird aus dem Password Depot eine CSV-Datei erstellt, die anschließend wieder in LastPass importiert werden kann. Bei dem Export der CSV-Datei stellt sich die erste Schwierigkeit heraus. Die Passwortdatenbank kann nicht gesamt importiert werden, sondern muss Ordner für Ordner heruntergeladen werden. Die CSV-Dateien sind nicht verschlüsselt, weshalb sie sehr vertraulich behandelt werden müssen. In LastPass kann die Quelle der Passwörter ausgewählt werden, wodurch die Passwörter ganz einfach importiert werden können, indem die zuvor heruntergeladene CSV-Datei einfach wieder hochgeladen wird. Nach dem ersten Import stellt sich heraus, dass die Passwörter nicht fehlerfrei importiert wurden. Daher wurde als zweiter Schritt probiert, die Passwörter über die CSV-Vorlage von LastPass zu importieren. Die Vorlage beinhaltete eine vorgegebene Reihenfolge, wie die Daten angegeben werden müssen (URL, User Name, Password, Extra, Name, Grouping, Fav).

Dabei stellte sich heraus, dass leere Felder die mit “” angegeben wurden, nicht erkannt worden sind und somit alle Informationen in einem falschen Feld landeten. Daher wurde entschieden, nach dem Import aller drei Passwortdatenbanken, die gesamten Passwörter einmal abzugleichen und die fehlerhaft importierten Passwörter einmalig händisch anzupassen. Da die händische Konfiguration nicht eingeplant war, wird die eingeplante Zeit von einer Stunde pro Datenbank überschritten, sodass die Passwort-Migration rund fünf Stunden dauert.

4.4. Qualitätssicherung vor Inbetriebnahme

Nach der Konfiguration wird die Software vor dem Rollout innerhalb der Admin Abteilung getestet. Um einen möglichst großen Testzeitraum nutzen zu können, ohne das Projekt in die Länge zu ziehen, beginnt der Test bereits am Mittwoch, den 23.02.2022 nach der Migration der Passwortdatenbank der Admin-Abteilung.

4.4.1. Testphase in Admin Abteilung (Systemtest)

Nachdem die Passwortdatenbank der IT-Abteilung importiert und alle Richtlinien eingestellt wurden, soll die Umgebung innerhalb des Teams getestet werden, bevor die Software an alle Mitarbeiter ausgerollt wird. In der Testphase werden kontinuierlich weitere Anpassungen durchgeführt, um das Handling für die End User am angenehmsten zu gestalten. Dazu gehört zu einem die Abbildung der Struktur der vorher importierten Passwort Datenbanken. Diese wurden versucht 1:1 wieder in LastPass abzubilden, damit die User ihre Passwörter leicht wiederfinden. Des Weiteren wurde die Richtlinie, die einen zwingt, das Masterpasswort nach Browser Schließung wieder einzugeben deaktiviert. Da die Mitglieder der Admin-Abteilung feststellen, dass sie den Browser mehrfach am Tag schließen und somit wiederholt gezwungen waren das Master Passwort einzugeben.

4.4.2. Anleitung vorbereiten

Vor Beginn der Realisierungsphase wurde eine Umfrage an die Mitarbeiter geschickt, um herauszufinden, welche Passwortmanager einzelne Mitarbeiter nutzen. Für die meistgenutzten Passwortmanager wurden Anleitungen erstellt denen erklärt wird, wie die Passwörter exportiert und wieder in LastPass importiert werden können. Der Prüfling konnte bei den Testimporten, den vorherigen Fehler, der bei dem Import aus dem Password Depot auftrat, ausschließen. Um alle Mitarbeiter möglichst erfolgreich abzuholen, wurden nicht nur Anleitungen für die Importe, sondern ein kleines Wiki mit allen wichtigen Informationen erstellt. Der erste Teil des kleinen Wikis ist die Aufklärung, warum LastPass im Unternehmen eingeführt wird, um die Passwortsicherheit im Unternehmen zu steigern, da dies eines der größten Sicherheitsrisiken darstellt. Anschließend folgt die Anleitung zur Account Einrichtung, in der die nächsten Schritte nach dem Empfangen der

Einladungsmail beschrieben werden. Die nächsten Seiten beschreiben alle Funktionen: Wie werden neue Passwörter und Ordner angelegt, wie funktioniert das Freigabecenter, die Einrichtung der Multifaktor Authentisierung und die Einbindung eines verknüpften privaten Kontos. LastPass Enterprise Kunden können privat “LastPass Family” umsonst nutzen. Die privaten Konten können mit dem Business Account verknüpft werden, dadurch kann aus dem Business Konto auf die privaten Passwörter zugegriffen werden, ohne dass die Konten vermischt werden. Einige Auszüge aus dem erstellten Wiki befinden sich im Anhang (siehe Anhang F. Anleitungsartikel).

4.5. Rollout

Nach Abschluss der Systemkonfiguration und Vorbereitung der Anleitungsartikel kann der Prüfling mit der Planung des Rollouts beginnen. Dazu teilt er die Mitarbeiter in zwei Gruppen ein.

4.5.1. Buchhaltung

Der Rollout an die Buchhaltung erfolgt vor dem Rollout an die übrigen Mitarbeiter. Im Zuge des Stakeholder Management ordnete der Prüfung die Buchhaltung in die Gruppe ein, die Hilfestellung bei der Einarbeitung in das Tool benötigt. Daher bekommen sie einen kleinen Workshop und werden persönlich an die neue Software herangeführt. Der Prüfling beginnt am Freitag, den 25.02.2022 mit dem Rollout und sendet allen Mitarbeitern der Buchhaltung den Einladungslink über das LastPass-Admin-Center. Nach dem Workshop wird kontrolliert, ob alle Accounts erfolgreich angelegt worden sind. Der Rollout an die Buchhaltung dient als finaler Test, der kontrolliert begleitet wird. Nicht vorhersehbare Ereignisse können vor dem Rollout an alle weiteren Mitarbeiter ausgeschlossen werden. Die Einführung der Buchhaltung in LastPass verlief reibungslos. Die Accounts konnten alle problemlos eingerichtet werden.

4.5.2. Alle Mitarbeiter

Durch den erfolgreichen Rollout an die Buchhaltung, werden alle weiteren Mitarbeiter in einem Zuge zu LastPass eingeladen. Der Prüfling wählt diese Variante, da bei dem Rollout an die Buchhaltung wenig Fehlerpotential erkannt wurde. Daher werden keine großen Mengen an Zwischenfällen, die im Service Desk auflaufen erwartet. Bevor die Einladungen versendet werden, erstellt der Prüfling einen Blogpost und kündigt den Rollout von LastPass zu 12 Uhr an. Dazu verlinkt er die vorher erstellten Anleitungsartikel zur Einrichtung und Handhabung. Die Einladungen werden über das Admin-Center verschickt. Nach der Versendung prüft der Prüfling, ob alle Mitarbeiter einbezogen worden sind. Sobald alle Mitarbeiter ihren Account erstellt haben, erstellt der Prüfling Gruppen für die einzelnen Abteilungen, um diese einfacher administrieren zu können. Nach der Überprüfung, dass alle Mitarbeiter ihren Account aktiviert haben, ist der Rollout abgeschlossen.

4.6. Qualitätssicherung nach Einführung

Im Anschluss testet der Prüfling alle Funktionen. Dabei fällt auf, dass die Mitarbeiter nur mit E-Mailadresse anstatt mit Vor- und Nachnamen angezeigt werden. Daher werden diese händisch nachgetragen, um die Mitarbeiter leichter zuordnen zu können. Durch mehrere Mitarbeiter Gespräche konnte der Prüfling die ersten Erfahrungen der Mitarbeiter mit LastPass in Erfahrung bringen. Das Feedback war bis auf die Kritik des langen Masterpasswortes sehr positiv. Die Qualitätssicherung findet bei diesem Projekt kontinuierlich statt, da das Tool vom Admin-Team selbst genutzt wird. Sobald Unregelmäßigkeiten auftreten, kann sofort eingegriffen werden. Um weiter Feedback von den restlichen Anwendern zu erhalten, ist eine weitere Umfrage nach 3 Monaten Nutzung geplant.

5. Abschlussphase

In der letzten Phase des Projekts behandelt der Prüfling einen Vergleich der Ist- und der gewünschten Soll Situation. Die Projektdokumentation wird erstellt und ein Abschlussgespräch mit dem Auftraggeber wird geführt.

5.1. Abgleich/ Ist-/ Soll Situation

Die herbeigeführte Ist-Situation wird mit dem Projekt-Soll verglichen. Dazu werden die geplanten und die in Anspruch genommene Zeit verglichen:

Projektphase	Soll-Stunden	Ist-Stunden	Differenz
Initialisierung	6	5	-1
Analyse	4	4	
Konzeption	9	9	-1
Realisierung	10	12	+2
Abschluss	6	6	
Gesamt	35	35	0

(Tabelle IV Zeitvergleich Ist-/ Soll Situation)

Das Projekt konnte innerhalb der geplanten Zeit von 35 Stunden durchgeführt werden. Dennoch konnten drei Zeitabweichungen festgestellt werden. Die Initialisierungsphase und Konzeptionsphase konnten schneller abgeschlossen werden. Die Initiierungsphase wurde leicht überschätzt, der Prüfling hielt das Stakeholder Management für umfangreicher. Die Konzeption konnte schneller abgeschlossen werden, da der Passwortmanager LastPass ein sehr umfangreiches Wiki für die Einrichtung bereitstellt, daher konnte die Planung der Arbeitspaketen sehr rasch abgeschlossen werden. Dafür verlängerte sich die Realisierungsphase durch die Komplikationen mit dem Import der Passwortdatenbanken aus dem Password Depot. Die händische Nacharbeit, um alle importierten Einträge abzugleichen, kostete zwei zusätzliche Stunden. Insgesamt gleichen sich die Zeitabweichungen aus, daher weichen die geplanten Kosten nicht ab.

5.2. Abnahme

In einem Abschlussgespräch mit dem Projektauftraggeber wird das Projekt abgenommen. Der Prüfling präsentiert dem Auftraggeber das fertige Projektergebnis. Da der Projektauftraggeber seit dem Rollout innerhalb des Admin Team bereits mit der Software arbeitet, ist keine weitere Einführung von Nöten. Der Prüfling erläutert auch die Ergebnisse aus dem Abgleich der Ist-/ Soll Situation. Auftraggeber und Prüfling sind sich einig, dass das Projektziel aus organisatorischer, wirtschaftlicher und technischer Sicht als erreicht gilt. Mit der Übergabe der Projektdokumentation ist die letzte Projektphase abgeschlossen.

6. Fazit

Nachfolgend zieht der Prüfling ein persönliches Fazit. Das Projekt wird reflektiert und ein Ausblick wird gegeben.

6.1. Lesson Learned

Im Zuge des Projekts konnte der Prüfling elementare Erfahrungen in Bezug auf Prozesse im Projektmanagement, als auch aus fachlicher Sicht sammeln. Wichtig war die Vorarbeit in der Initialisierung und Konzeptphase. Die Mitarbeiter wurden früh im Thema abgeholt und in einzelnen Gruppen einbezogen, sodass es nach Projektdurchführung sehr positives Feedback gab. Es wurde bewusst auf ein hybrides Projekt gesetzt. Das Projekt wurde nach dem klassischen Projektmanagement geplant. Die Einführung lief jedoch zum Teil agil. Durch die frühe Einführung der Software in der Admin-Abteilung, konnten viele Stolpersteine für das große Rollout bereits beseitigt werden. Gleichzeitig wurden die Teammitglieder bereits im Umgang mit der Software geschult und Mitarbeitern konnte später schnell Hilfe angeboten werden. Für den Import der Passwörter hätte der Prüfling mehr Zeit einplanen müssen. Der Import, der auf den ersten Blick einfach wirkte,

nahm im Endeffekt in der Realisierung mehr Zeit in Anspruch als geplant. Wären in der Initialisierung und Konzeptionsphase nicht Zeit eingespart worden, hätte sich der Projektabschluss zeitlich verschoben. Bei unbekannten Aufgaben, mit neuen Systemen, sollte in Zukunft nicht so knapp kalkuliert werden. Im späteren Austausch im Admin-Team berichteten Kollegen von ähnlichen Erfahrungen mit Import Tools. Meist endet es in händischer Nachkonfiguration, besonders bei so großen Datenmengen. Insgesamt war es ein sehr interessantes Projekt. Ein Unternehmens Passwortmanager wird für sehr sensible und zu schützende Daten eingesetzt, daher muss er mit Bedacht ausgewählt werden und ein breites Spektrum an Sicherheitsmerkmalen und Datenschutzauflagen erfüllen.

6.2. Ausblick

Die Firma Ashampoo verfügt durch die erfolgreiche Projektumsetzung über einen zentralen Passwortmanager, der von allen Mitarbeitern im Unternehmen genutzt wird. Dadurch konnte die Passwortsicherheit schon erheblich gesteigert werden. Das Sicherheit Dashboard in LastPass bietet einen Überblick über die gewählte Passwortstärke der Mitarbeiter. Diese liegt kurz nach Umsetzung bei 60%. Jeder vierte Mitarbeiter verwendet Passwörter wieder. Daher ist es zukünftig das Ziel, die Passwortstärke zu steigern, indem randomisierten Passwörter nur einmalig genutzt werden.

7. Verzeichnisse

7.1. Literaturverzeichnis

Handbuch Password Depot
https://www.password-depot.de/dokumentation/Handbuch-Password-Depot-Enterprise-Server-16.pdf

Website LastPass:
https://www.lastpass.com/de
https://www.lastpass.com/de/solutions/enterprise-password-management
https://www.lastpass.com/de/pricing

Website Keeper
https://www.keepersecurity.com/de_DE/
https://www.keepersecurity.com/de_DE/enterprise.html
keepersecurity.com/de_DE/pricing.html?t=e

Website Dashlane
https://www.dashlane.com/de/
https://www.dashlane.com/de/business
https://www.dashlane.com/de/business/pricing

Einrichtung LastPass Enterprise
https://support.logmeininc.com/de/lastpass/help/get-started-as-a-lastpass-enterprise-user-lp010051
https://support.logmeininc.com/de/lastpass/help/how-to-add-enterprise-users-lp010044

7.2. Anhangsverzeichnis

(Tabelle V Aufgabenplanung, detailliert)

Phase / Vorgang	veranschlagte Zeit in Std.
Initialisierungsphase	6
Projektziel ermitteln	1
Projektabgrenzung	0,5
Projektablauf	1
Stakeholder Management	3
Projektauftrag	0,5
Analysephase	4
Durchführung Ist-Analyse	2
Durchführung Soll-Analyse	2
Konzeptphase	9
Klärung der technischen Anforderungen	1
Wirtschaftlichkeitsanalyse	1
Auswahl geeigneter Systeme	2
Auswertung	1
Planung von Arbeitspaketen	1

Ressourcenplanung	0,5
Personalplanung	0,5
Sachmittelplanung	0,5
Terminplanung	1
Kostenplanung	0,5
Realisierungsphase	10
Vorbereitung	1
Migration der Passwörter	3
Konfiguration des Systems	2
Qualitätssicherung (Systemtest)	parallel
Anleitungen erstellen	3
Qualitätssicherung nach Einführung	1
Abschlussphase	6
Abgleich/ Ist-/ Sollsituation	0,5
Erstellung der Projektdokumentation	5
Abnahme	0,5
Gesamt	35

(Anhang B Projektauftrag)

Projektname:	ITZ-1278
Projektauftrag:	Einführung eines webbasierten Passwortmanager für die gesamte Unternehmung
Ausgangslage:	Ein Passwortmanager für wenige Abteilungen, der nur intern genutzt werden kann.
Projektziele:	1. Konfiguration der neuen Software 2. Einrichtung der Benutzeraccounts für alle Mitarbeiter 3. Import der bestehenden Passwörter in das neue Tool
Abgrenzung:	Austausch bestehender unsicherer Passwörter Einrichtung der MFA für alle Accounts
Termine	Projektstart: 21.02.2022 Projektabschluss am 28.02.2022
Personalaufwand	35 Arbeitsstunden eines Azubis
Projektkosten	Kostenrahmen von 6.500€
Projektrisiken	Ablehnung der Nutzung, keine Verhaltensänderung der Mitarbeiter
Auftraggeber	Hauke Duden
Projektleiter	Jana Okrey
Sonstige Beteiligte:	/
Unterschrift Auftraggeber	
Unterschrift Projektmanagerin	

(Tabelle VI Planung Arbeitspakete Realisierungsphase)

Nr.	Arbeitspaket	Zeit in h
	Vorbereitung der Einrichtung	1
1	LastPass Enterprise kaufen	0,25
2	LastPass Umgebung einrichten	0,5
3	Admin Abteilung zu LastPass einladen	0,25
4	System Konfiguration	4,5
5	Meeting Richtlinien Einstellungen	1
6	Richtlinien einstellen	0,5
9	Import/ Export Passwort Datenbank via CSV Datei - Admin Abteilung - Buchhaltung - Geschäftsführung	3
	Qualitätssicherung	2,5
10	Testphase in der Admin Abteilung (Systemtest)	parallel
11	Mitarbeiter Umfrage welche Passwortmanager genutzt werden erstellen, verschicken und auswerten	0,5
12	Anleitung für LastPass erstellen - Vorstellung, Funktionen, Sharing, Einrichtung, MFA - Migration aus alten Passwort Managern (Aus Umfrage)	2
	Rollout	2
14	Roll Out Buchhaltung, und Einführungsworkshop	0,5
15	Roll Out an alle Mitarbeiter - Blogpost, um Mitarbeiter abzuholen	1
16	Gruppen anlegen, Benutzer Überprüfung	0,5

(Anhang C Meeting Protokoll)

LastPass Policy
Datum: 23.02.2022
Teilnehmer

- Stephan Schuchardt
- Jan Iben
- Mario Stolz
- Hauke Duden
- Jana Okrey

[redacted]

Folgende Richtlinie sollen besprochen werden:

- [redacted]
- [redacted]
- [redacted]
- [redacted]

Richtlinie	JIB	MST	SSH	HDU	JOK	Ergebnis
[redacted]	[redacted]		[redacted]			[redacted]
[redacted]	[redacted]		[redacted]			[redacted]
[redacted]	[redacted]		[redacted]			[redacted]
[redacted]	[redacted]		[redacted]			[redacted]

[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

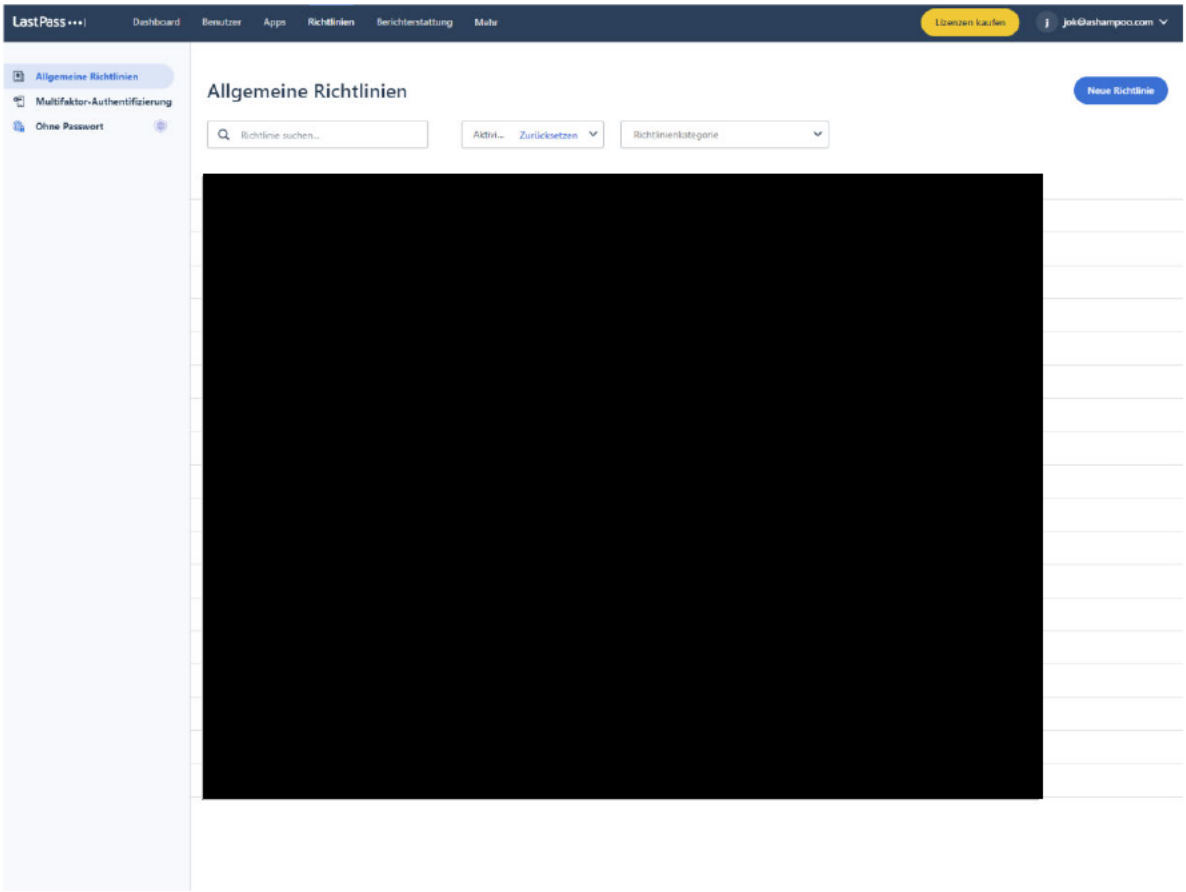
Info bezüglich AD:

Das AD wird nur für die automatische Einrichtung/Löschung/Deaktivierung von Accounts verwendet. Das AD-Passwort ist NICHT das Master Passwort des Users — das muss in jedem Fall manuell gesetzt werden und wird separat verwaltet. Es werden dann automatisch entsprechende Einladungs-Emails versendet.

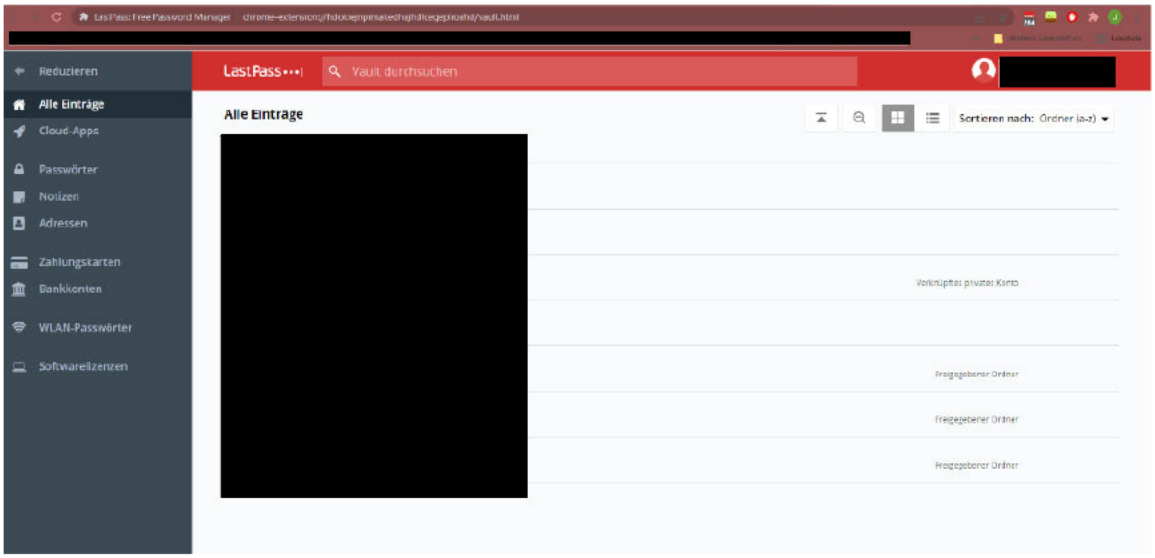
LastPass kann auch als ID-Provider agieren (mit einem höheren Tarif)

Ergebnis: AD-Integration kann anscheinend auf zwei Arten erfolgen: Identity Provider (nur Account Provisionierung) und Federated (Master-Passwort aus AD). Das allgemeine Gefühl im Team ist, dass LastPass unabhängig bleiben sollte und keine der beiden Optionen verwendet wird.

(Abbildung D LastPass Richtlinien)



(Abbildung E LastPass Übersicht Einträge)



Vorstellung

LastPass ist ein webbasierter Passwort-Manager-Online-Dienst.

Nutzen kannst du ihn über das Webinterface oder auch über ein Add On, dass du in deinen Browser integrierst.

Funktionen

Wir nutzen die Enterprise-Version, mit der dir folgende Funktionen zur Verfügung stehen:

- Passwörter sicher speichern
- Passwörter automatisch ausfüllen
- Starke, zufällige Passwörter erstellen
- Digitale Notizen sicher speichern
- Passwörter für Kollegen freigeben

Account Erstellung

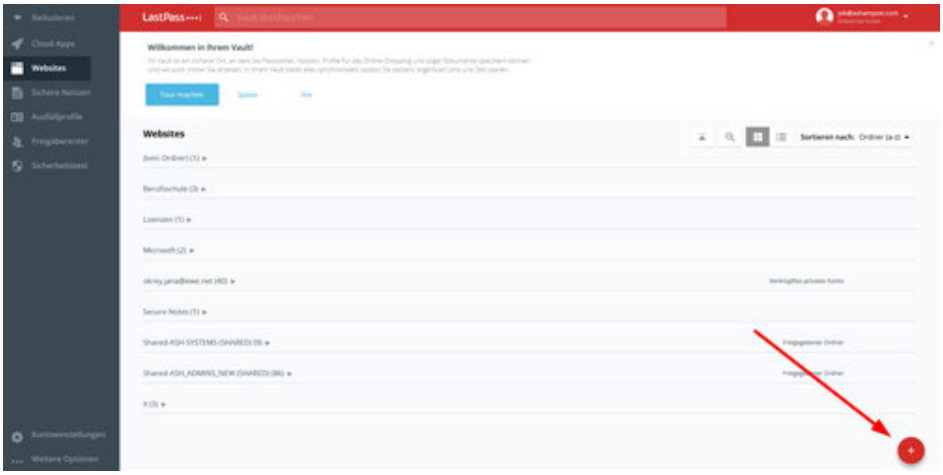
Dein Account wird im Vorfeld angelegt. Um ihn zu aktivieren, bekommst du eine E-Mail.

In der E-Mail wirst du aufgefordert, dein temporäres Masterpasswort zu ändern.
Für dein neues Masterpasswort verwende:

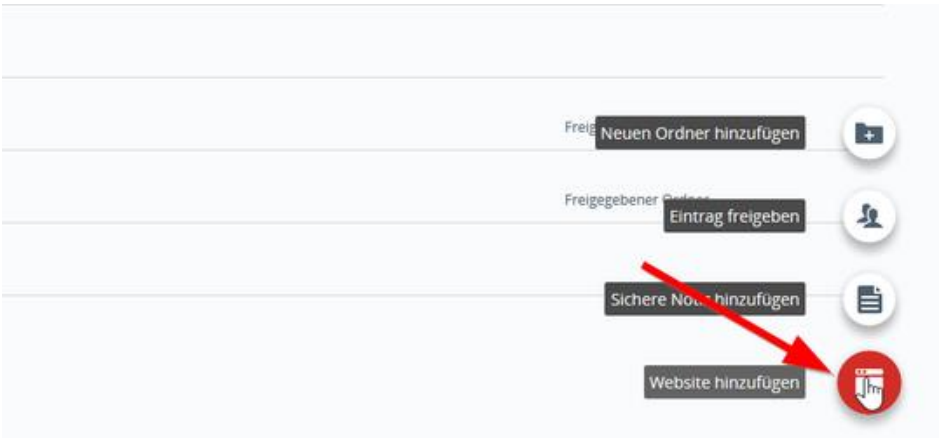
- Mindestens 8 Zeichen.
- Nutze Großbuchstaben, Kleinbuchstaben und Ziffern
- Sonderzeichen kannst du nutzen. Sind aber nicht vorgeschrieben.

Danach ist dein Account eingerichtet.

Ein Passwort speichern



Um ein Passwort zu hinterlegen, bewegst du den Mauszeiger auf den roten Button mit dem "Plus". Dadurch öffnet sich ein neues Auswahlmenü.

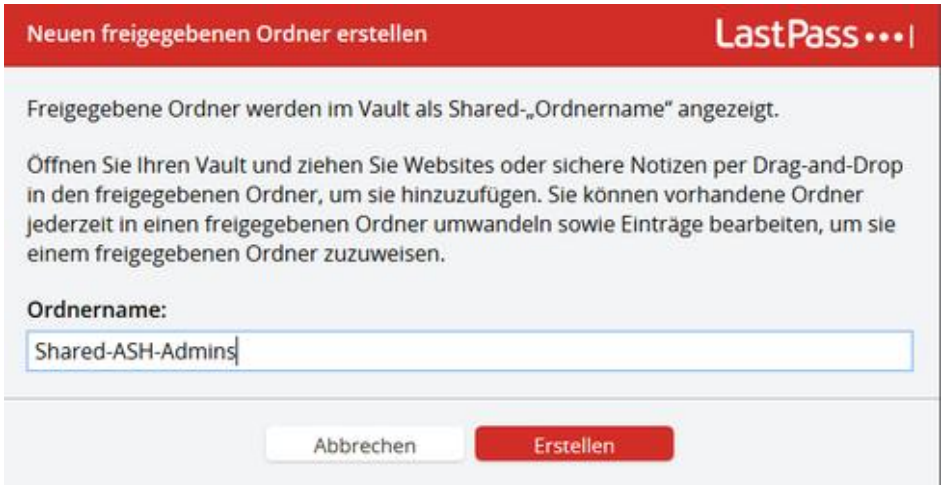


- Hier kannst du neue Ordner erstellen, um deine Passwörter zu organisieren.
- Einzelne Passwörter für einen oder mehrere Kollegen freigeben
- Eine sichere Notiz anlegen
- Eine Website mit einem hinterlegten Passwort speichern

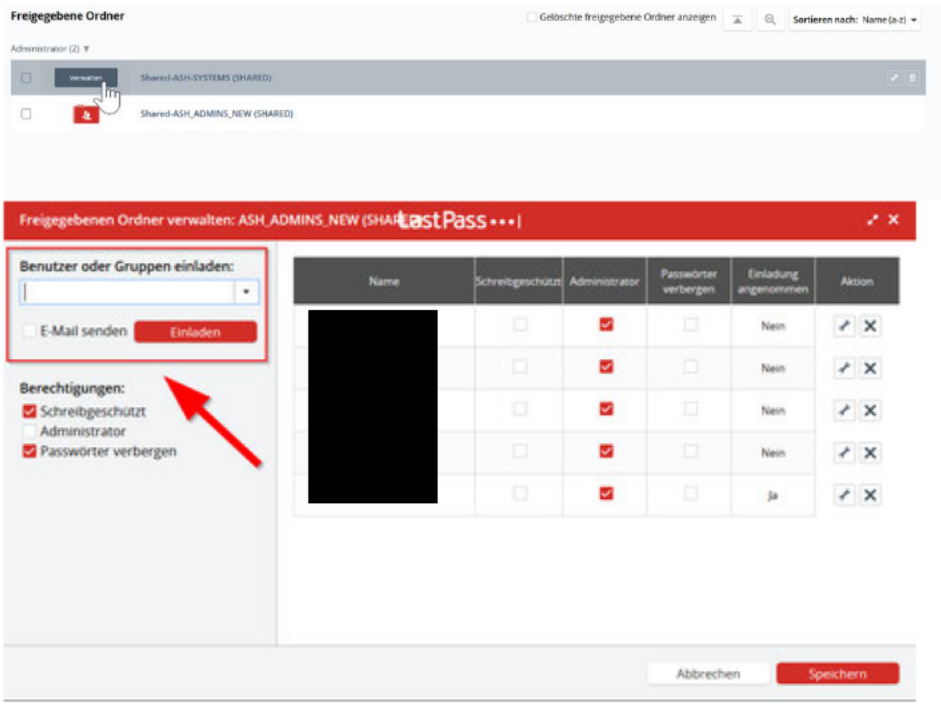
Um ein Passwort zu speichern gehts du auf "Website hinzufügen".

Einen freigegebenen Ordner erstellen und bearbeiten

Um einen freigegebenen Ordner zu erstellen, klickst du auf den roten Button mit dem "Plus". Dadurch öffnet sich ein neues Fenster.

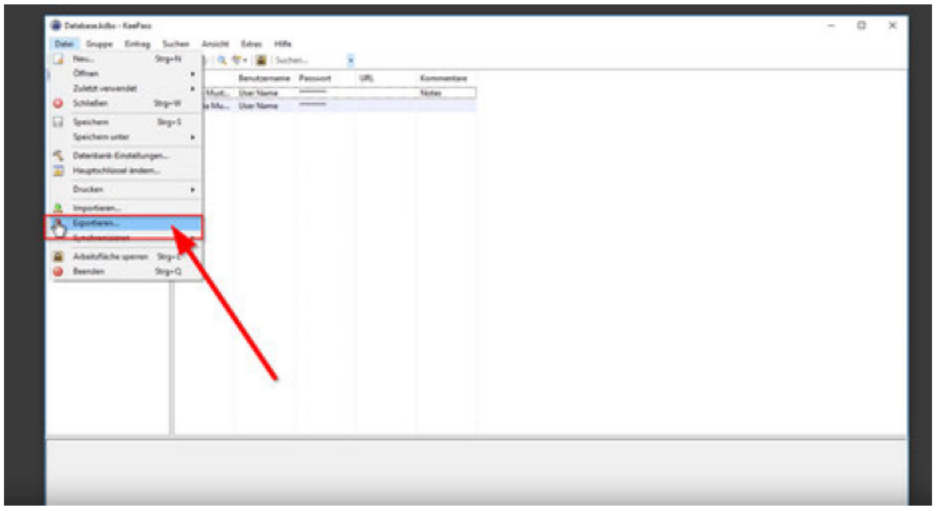


Hier benennst du den Ordner nachfolgenden Schema: ASH-Abteilung (SHARED).

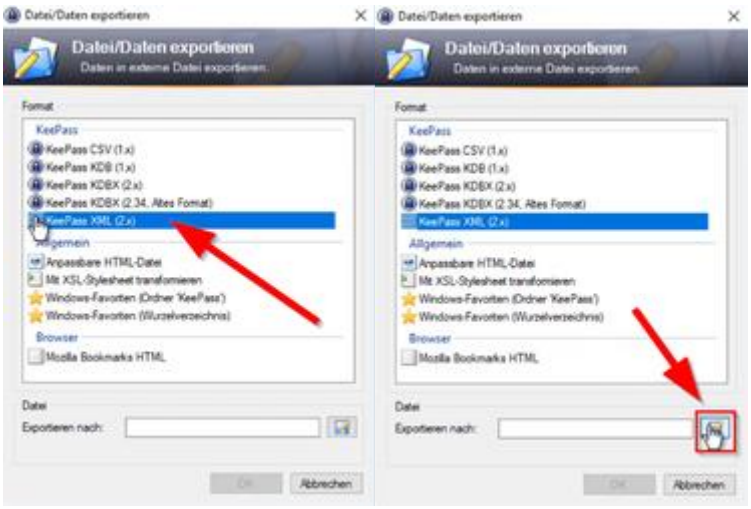


Wenn du die Verwaltung des Ordners öffnest, kannst du die Berechtigungen anpassen, sowie neue Benutzer einladen.

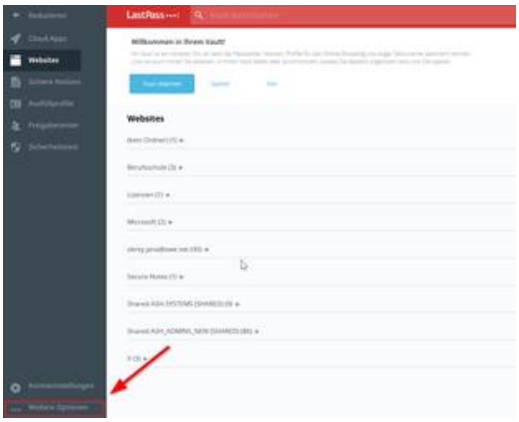
Passwort Import KeePass



Um eine Exportdatei zu erstellen wählst du Datei => Exportieren.

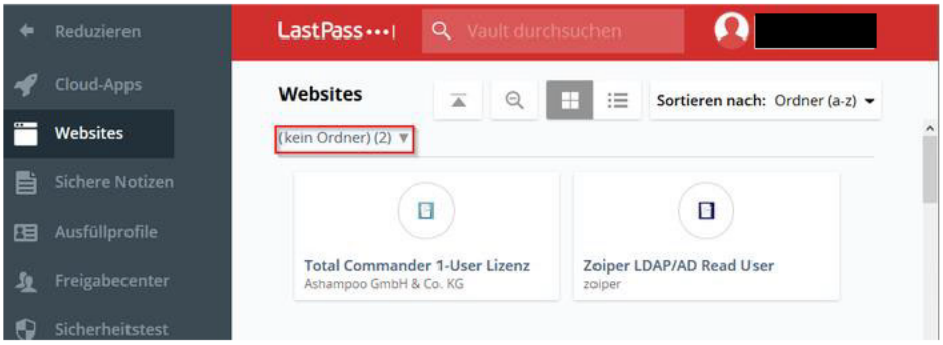


Als Exportformat wählst du XML und anschließend den Speicherort



du deine erstellte Exportdatei in LastPass importieren kannst. Wählst du im Menü "weitere Optionen" => "importieren".

Als nächstes wählst du als Quelle "KeePass", anschließend deine zuvor erstellte Exportdatei und lädst sie hoch.



Die importierten Passwörter findest du unter "Kein Ordner".

(Anhang F Anleitungsartikel)

7.2.1 Glossar

On Premises-Lösung: Software, die im eigenen Netz installiert und betrieben wird.

TCP/IP:
Transmission Control Protokoll: Transport von Datenpaketen in einem dezentralen Netzwerk.
Internet Protokoll: Adressierung und Fragmentierung von Datenpaketen

IPv4: Internet Protokoll Version 4

IPv6: Internet Protokoll Version 6

SSL/TSL Verschlüsselung:
Secure Sockets Layer: Protokoll, welches zwischen dem Webserver und Client arbeitet, um die Datenübertragung zu verschlüsseln.
Transport Layer Security: Protokoll, welches die Datenströme im Internet verschlüsselt, damit sie nur von dem berechtigten Empfänger gelesen werden können.

Software as a Service (SaaS): Softwareanwendungen werden über das Internet als Service angeboten.

Zero Knowledge Prinzip: Service Provider wissen nichts über die Dateien, die auf ihren Servern gespeichert sind. Sie werden verschlüsselt gespeichert und auf dem Server nicht entschlüsselt.

Confluence: Ist ein Tool von Atlassian in dem Teams Zusammenarbeiten können. Dynamische Seiten bieten einen Ort zum Erstellen, Erfassen und Zusammenarbeiten für Projekte oder zum Sammeln von Ideen.

Aktiv Directory: Verzeichnisdienst von Microsoft Windows, in einer hierarchischen Datenbank werden Geräte, Ressourcen und Einstellungen verwaltet. Es gehört zu den zentralen Komponenten, um Windows Basierte Netzwerke zu verwalten.

CSV-Datei: Dateityp, der in Excel erstellt wird. Informationen werden durch Kommata getrennt.

Rollout: Austausch/ Einführung von Software.

Service Desk: Auch Helpdesk genannt, ist eine Anlaufstelle für Kunden oder internen Mitarbeitern, um Informationen oder Unterstützung im Bereich der IT zu bekommen.

7.2.2 Abkürzungsverzeichnis

IHK: Industrie und Handelskammer

MFA: Multifaktor Authentisierung

GUI: Graphical User Interface, Grafische Benutzeroberfläche: Anwendungssoftware wird mittels grafischer Symbole und Steuerelemente bedienbar gemacht.

VPN: Virtual Private Network

CTO: Chief Technical Officer