



Erklärung

Bestätigung über die durchgeführte betriebliche Aufgabe¹

(Diese Bestätigung ist als Deckblatt online einzureichen, gemeinsam mit dem Report/der Dokumentation.)

Prüfling (vollständige Anschrift und Telefonnummer)	Ausbildungsbetrieb (vollständige Anschrift)
Vorname, Name Robin Helwig	Firma Ashampoo GmbH & Co. KG
Straße, Hausnr. [REDACTED]	Straße, Hausnr. Schafjückenweg 2
PLZ, Ort [REDACTED]	PLZ, Ort 26180 Rastede
Tel.Nr.: [REDACTED]	Tel.Nr.: 04402/9739200

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

Fachinformatiker - Fachrichtung Systemintegration

Bezeichnung der betrieblichen Aufgabe

Einführung eines Backup Systems einer Microsoft 365 Cloud Umgebung

Erklärung des Prüflings

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

Verantwortlicher im Unternehmen

[REDACTED]
selbstständig durchgeführt und die Unterlagen selbstständig zusammengestellt habe.

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

Rastede, 12.05.25
Ort, Datum

[REDACTED]
Unterschrift des Prüflings

Bestätigung des Ausbildungsbetriebes

Wir bestätigen, dass die Angaben des Prüflings richtig sind.

Rastede, 12.05.2025
Ort, Datum

[REDACTED]
Unterschrift des Verantwortlichen, der die Aufgabe betreut hat.

Rastede, 12.05.2025
Ort, Datum

[REDACTED]
Unterschrift des Ausbilders

¹Zur 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.



Oldenburgische
Industrie- und Handelskammer

Abschlussprüfung Sommer 2025

Fachinformatiker für Systemintegration

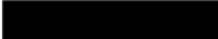
Dokumentation zur betrieblichen Projektarbeit

Einführung eines Backup Systems einer Microsoft 365 Cloud Umgebung

Abgabedatum: Bad Zwischenahn, den 14.05.2025

Robin Helwig



Tel.: 

Ausbildungsbetrieb

Ashampoo GmbH & Co. KG

Schafjückenweg 2

26180 Rastede





Inhalt

Inhalt	I
Abbildungsverzeichnis	III
Tabellenverzeichnis	IV
Abkürzungsverzeichnis	V
1 Einleitung	1
1.1 Projektumfeld	1
1.2 Projektziel	1
1.3 Projektbegründung	1
1.4 Projektschnittstellen	2
1.4.1 Organisatorische Schnittstellen	2
1.4.2 Technische Schnittstellen	2
1.5 Projektabgrenzung	2
2 Projektplanung	3
2.1 Projektphasen	3
2.2 Ressourcenplanung	4
3 Analysephase	5
3.1 Ist-Analyse	5
3.2 Stakeholder Analyse	5
3.3 Wirtschaftlichkeitsanalyse	5
3.3.1 Potenzielle Schadenskosten ohne Backup	6
3.4 Nutzwertanalyse	6
3.4.1 Make or Buy Entscheidung	6
3.4.2 Projektkosten	7
4 Entwurfsphase	7
4.1 Erstellung eines detaillierten Implementierungsplans	7
5 Durchführungsphase	8
5.1 Installation der Software	8
5.2 Hinzufügen der Microsoft 365-Organisation	8
5.3 Auswahl der zu sichernde Dienste	9
5.4 Verbindungs- und Authentifizierungseinstellungen	9
5.5 Registrierung einer Microsoft Azure-Anwendung	9
5.6 Einrichtung eines Auxiliary Backup Accounts	9
5.7 Repository und Backup-Jobs	10
5.7.1 Item-Level Speicherung	10



5.7.2	Snapshot-Basierte Speicherung.....	10
5.7.3	Auswahl und Begründung der Aufbewahrungs-Methode.....	10
5.8	Konfiguration des Backup-Jobs.....	11
5.9	Einrichtung des Self-Service Restore Portals.....	11
5.10	Wiederherstellungstests.....	13
5.11	E-Mail-Benachrichtigungen	13
6	Abnahmephase	13
7	Fazit	14
8	Literaturverzeichnis	15
A.	Anhänge.....	i
A.1.	Stakeholder Analyse.....	i
A.2.	Nutzwertanalyse	ii
A.3.	Gantt-Diagramm	iv
A.4.	Systemdokumentation	v
A.5.	Anwenderdokumentation	ix
A.6.	Größere Wiederherstellungen durch Administratoren	xv



Abbildungsverzeichnis

Abbildung 1: Projektphasen im Kuchendiagramm	3
Abbildung 2: Gantt-Diagramm	iv
Abbildung 3: Netzwerktopologie	vii
Abbildung 4: Restore Portal Login	ix
Abbildung 5: Login Microsoft	x
Abbildung 6: Auswahl des Restore Points	x
Abbildung 7: Restore Ordner	x
Abbildung 8: Objektauswahl Restore Portal.....	xi
Abbildung 9: Restore und Restore List	xi
Abbildung 10: Exchange Restore Items.....	xi
Abbildung 11: Restore mode	xii
Abbildung 12: Wiederherstellungsoptionen.....	xii
Abbildung 13: Wiederherstellungsgrund	xii
Abbildung 14: Wiederherstellung Zusammenfassung	xiii
Abbildung 15: Restore Sessions.....	xiii
Abbildung 16: Wiederherstellung über Restore List	xiv
Abbildung 17: User Scope	xiv
Abbildung 18: Zugewiesene restore scopes	xiv
Abbildung 19: Wiederherstellung über Restore Scope	xv
Abbildung 20: Wiederherstellung des Versionsverlaufs	xv
Abbildung 21: Admin Wiederherstellungsauswahl	xvi
Abbildung 22: Admin Mailbox Wiederherstellung	xvi
Abbildung 23: Admin OneDrive Wiederherstellungsoptionen	xvii
Abbildung 24: Admin OneDrive Wiederherstellung	xvii



Tabellenverzeichnis

Tabelle 1: Organisatorische Schnittstellen	2
Tabelle 2: Projektphasen mit Zeiteinteilung.....	3
Tabelle 3: Projektphasen mit Arbeitspaketen	4
Tabelle 4: Projektkosten	7
Tabelle 5: Stakeholder Analyse.....	i
Tabelle 6: Nutzwertanalyse Teil 2	ii
Tabelle 7: Nutzwertanalyse Teil 1	ii
Tabelle 8: Nutzwertanalyse Teil 3	iii
Tabelle 9: Systemkomponenten.....	v
Tabelle 10: Veeam Ports.....	vi
Tabelle 11: Rechte und Rollen	vii
Tabelle 12: Backup Konfiguration	viii
Tabelle 13: Wiederherstellungstests	viii



Abkürzungsverzeichnis

API	Application Programming Interface
EWS	Exchange Web Services
AWS S3	Amazon Web Services Simple Storage Service
DevOps	Development Operations
DNS	Domain Name System
SaaS	Software as a Service
DSGVO	Datenschutzgrundverordnung
VBO365	Veeam Backup for Office 365
ISO	International Organization for Standardization
MS365	Microsoft 365
EnApp	Enterprise Application
AuxBackup	Auxiliary Backup
Auth	Authentication
IP	Internet Protocol
REST	Representational State Transfer
Pfx	Personal Information Exchange
A-Name Record	Address Name Record
VPN	Virtual Private Network
CNAME	Canonical Name Record
URI	Uniform Resource Identifier
SSL	Secure Sockets Layer
OAuth	Open Authorization
HTTPS	Hypertext Transfer Protocol Secure



1 Einleitung

Das Projekt umfasst die Konzeption, Installation und Konfiguration einer Backup-Lösung für Microsoft 365, mit dem Ziel, Unternehmensdaten zuverlässig zu sichern und bei Bedarf gezielt wiederherstellen zu können.

Dabei werden sowohl technische Anforderungen an moderne Datensicherungssysteme berücksichtigt als auch organisatorische und sicherheitsrelevante Aspekte, wie z. B. die Zugriffskontrolle und Aufbewahrungsrichtlinien. Durch die Umsetzung eines realitätsnahen Projekts sollen die im Ausbildungsrahmenplan vermittelten Inhalte praxisorientiert angewendet und vertieft werden.

Das Projekt dient nicht nur der fachlichen Weiterentwicklung, sondern fördert auch die eigenverantwortliche Planung, Durchführung und Dokumentation im Team- und Unternehmenskontext. Die erarbeitete Lösung unterstützt langfristig die IT-Abteilung bei der Sicherstellung der Datenverfügbarkeit und trägt aktiv zur Betriebssicherheit bei.

1.1 Projektumfeld

Die Ashampoo GmbH & Co. KG ist ein Unternehmen, das in der Softwareentwicklung und der Bereitstellung eines Marktplatzes für Software tätig ist.

Die IT-Infrastruktur im Firmengebäude „//CRASH“ wird von der IT-Abteilung der Ashampoo GmbH & Co. KG und der IT-Abteilung der CleverReach GmbH & Co. KG verwaltet. Die IT-Abteilung der Ashampoo GmbH & Co. KG setzt sich aus 4 Mitarbeitern zusammen. Hierzu gehört auch der Prüfling, der gleichzeitig die Projektleitung übernimmt.

Die IT-Abteilung der Ashampoo GmbH & Co. KG kümmert sich um die IT der Ashampoo GmbH & Co. KG (ca. 60 Mitarbeiter), der Personizer GmbH & Co. KG (ca. 13 Mitarbeiter) und der CRASH Group (ca. 25 Mitarbeiter). Die CleverReach GmbH & Co. KG kümmert sich nur um die eigene IT.

1.2 Projektziel

Zur Sicherstellung der Datensicherheit und -verfügbarkeit plant die Ashampoo GmbH & Co. KG die Einführung eines zuverlässigen Backup-Systems für Microsoft 365. Dabei sollen sämtliche relevanten Dienste wie OneDrive, SharePoint, Exchange Online und Microsoft Teams in die Backup-Strategie einbezogen werden. Ziel ist es, die Wiederherstellbarkeit von Daten auch nach versehentlichem Löschen, Cyberangriffen oder anderen Vorfällen wie menschlichem Versagen oder vorsätzlicher Datenlöschung jederzeit zu gewährleisten. Gleichzeitig soll die Lösung den gesetzlichen und betrieblichen Compliance-Anforderungen entsprechen und die IT-Abteilung durch eine automatisierte, benutzerfreundliche Backup- und Wiederherstellungsfunktion nachhaltig entlasten. Angesichts der zunehmenden Risiken durch Cyberattacken und Datenverluste ist es essenziell, dass die in der Microsoft 365 Cloud gespeicherten Daten der Ashampoo GmbH & Co. KG zuverlässig gesichert und im Bedarfsfall schnell wiederhergestellt werden können.

1.3 Projektbegründung

Im Zuge der zunehmenden Verlagerung von IT-Diensten in die Cloud setzt die Ashampoo GmbH & Co. KG verstärkt auf Microsoft 365. Dienste wie Exchange Online, OneDrive for Business, SharePoint Online und Microsoft Teams bilden dabei zentrale Bestandteile der täglichen Kommunikation und Zusammenarbeit im Unternehmen.

Mit der Nutzung dieser cloudbasierten Dienste entstehen neue Anforderungen an die Datensicherung. Microsoft selbst bietet lediglich grundlegende Wiederherstellungsfunktionen,

die in Bezug auf Aufbewahrungsdauer, Granularität und Kontrolle nicht ausreichen, um die unternehmensinternen sowie datenschutzrechtlichen Anforderungen vollständig zu erfüllen. Insbesondere bei versehentlicher Löschung, Cyberangriffen oder dem Bedarf zur Wiederherstellung von Daten ausgeschiedener Mitarbeitender besteht die Gefahr, dass kritische Daten verloren gehen oder nicht zeitnah wiederhergestellt werden können.

Zur Schließung dieser Lücke wird eine professionelle Backup-Lösung benötigt, die speziell auf Microsoft 365-Dienste ausgelegt ist. Ziel ist es, eine unabhängige, automatisierte und skalierbare Sicherung aller relevanten Daten zu ermöglichen – einschließlich granularer Wiederherstellungen einzelner Objekte wie E-Mails, Dateien oder Kalendereinträge. Außerdem soll der Zugriff auf gesicherte Daten klar geregelt und für autorisierte Personen nachvollziehbar gestaltet werden.

Die neue Lösung soll zudem die bestehende IT-Infrastruktur sinnvoll ergänzen, lokale Speicherressourcen sowie Cloud-basierte Speicherziele unterstützen und sich flexibel an zukünftige Anforderungen anpassen lassen. Durch die Einführung eines entsprechenden Backup-Systems können Risiken minimiert, Wiederherstellungszeiten verkürzt und der Aufwand für den IT-Support reduziert werden.

1.4 Projektschnittstellen

1.4.1 Organisatorische Schnittstellen

Tabelle 1: Organisatorische Schnittstellen

Name	Abteilung	Beschreibung
[REDACTED]	Produktion / Technology	Ausbilderin
[REDACTED]	Administration	Auftraggeber / Projektsprechpartner

1.4.2 Technische Schnittstellen

- Microsoft 365: Die zu sichernden Daten (Exchange Online, OneDrive, SharePoint Microsoft Teams) werden über die Microsoft Graph API und Exchange Web Services angebunden.
- ASHSRVBACKUP02: Die Backup-Daten werden auf einem bestehenden Backup System abgelegt, welches bereits benutzt wird für Veeam Backup & Replication 12.

1.5 Projektabgrenzung

Im Rahmen dieses Projekts liegt der Fokus ausschließlich auf der Sicherung der Microsoft 365-Dienste. Lokale Systeme, wie etwa Windows- oder Linux-Server sowie physische Clients, sind ausdrücklich von diesem Backup-Konzept ausgenommen. Ebenso wird keine revisionssichere Archivierung umgesetzt. Zwar wird eine langfristige Aufbewahrung der Daten konfiguriert, jedoch gehört eine rechtssichere Archivierung – beispielsweise durch den Einsatz von Lösungen wie MailStore – nicht zum Leistungsumfang dieses Projekts. Auch die Anbindung externer Cloud-Dienste, etwa zur Speicherung von Backups in AWS S3, ist nicht vorgesehen. Stattdessen erfolgt die Ablage der Sicherungen lokal auf einem bereitgestellten Backup-Server. Darüber hinaus werden weitere Microsoft-Dienste außerhalb von Microsoft 365, wie Power BI, Microsoft Planner oder Azure DevOps, nicht berücksichtigt.

Der Einsatz eines Tape-Systems zur langfristigen Offline-Archivierung ist zum aktuellen Zeitpunkt nicht Bestandteil des Projekts, da hierfür die notwendige Hardware (z. B. LTO-Bandlaufwerk) aktuell noch nicht zur Verfügung steht. Zwar existiert bereits eine AWS-Infrastruktur, jedoch wird diese in der aktuellen Projektumsetzung nicht für die Speicherung von Backups genutzt. Eine spätere Erweiterung um S3-kompatiblen Cloud-Speicher für

Offsite-Backups wird jedoch aktiv in Betracht gezogen, um die Datensicherheit und Resilienz gegenüber physikalischen Ausfällen oder Cyberbedrohungen weiter zu erhöhen.

2 Projektplanung

2.1 Projektphasen

Das Projekt wird im Zeitraum vom 24.03.2025 bis zum 31.03.2025 durchgeführt.

Die Bearbeitung erfolgt im Rahmen der regulären betrieblichen Ausbildungszeit mit einer täglichen Projektarbeitszeit von 8 Stunden (Mo–Fr), unter Anleitung und Begleitung der betrieblichen Ausbilder.

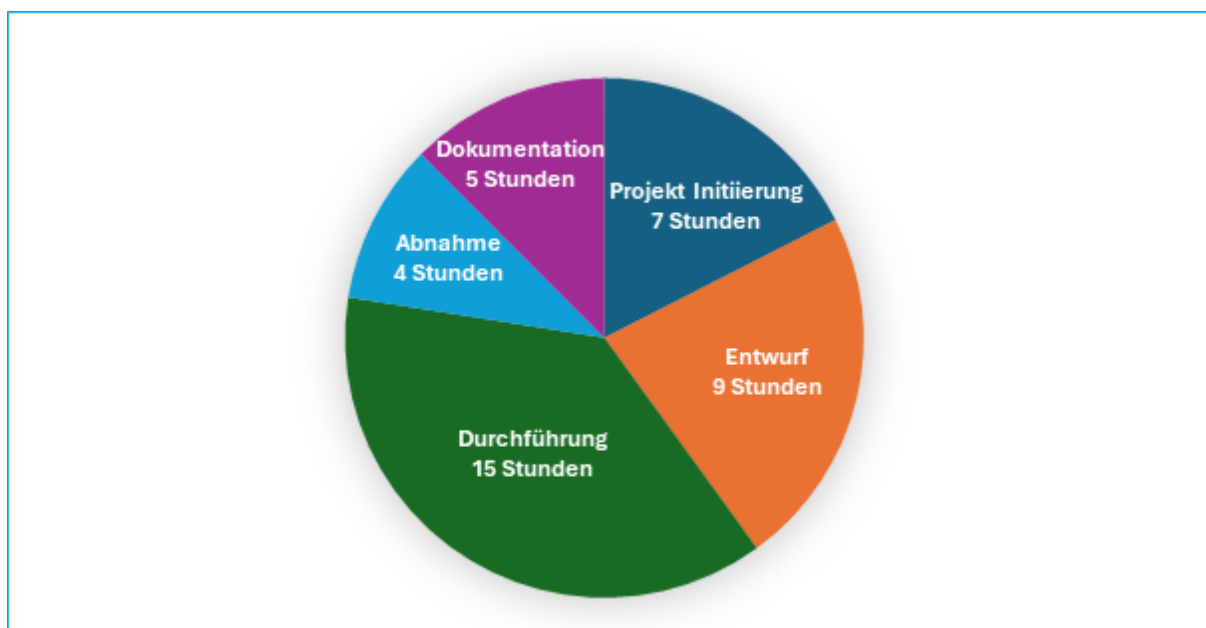


Abbildung 1: Projektphasen im Kuchendiagramm

Tabelle 2: Projektphasen mit Zeiteinteilung

Projektphase	Zeit in Stunden
Projekt Initiierung	7
Entwurf	9
Durchführung	15
Abnahme	4
Dokumentation	5
Gesamt	40

Tabelle 3: Projektphasen mit Arbeitspaketen

Initiierung	7 h
• Projektziel ermitteln	2 h
• Durchführen der Ist-Analyse	2 h
• Stakeholder-Analyse	1 h
• Definition des Soll-Zustands	2 h
Entwurf	9 h
• Evaluierung und Auswahl der Backup-Lösung	4 h
• Erstellung eines detaillierten Migrationsplans	5 h
Durchführung	15 h
• Einrichtung der Backup-Umgebung	3 h
• Durchführung einer Testmigration (Backup & Restore)	2 h
• Evaluierung und Optimierung nach der Testmigration	2 h
• Umsetzen der finalen Migration	8 h
Abnahme	4 h
• Überprüfung der Funktionsfähigkeit	1 h
• Schulung der IT-Mitarbeiter	2 h
• Abschlusspräsentation und Abnahme	1 h
Dokumentation	5 h
• Erstellen der Anwenderdokumentation	2 h
• Erstellen der Systemdokumentation	3 h

2.2 Ressourcenplanung

Für die erfolgreiche Durchführung des Projekts standen mir verschiedene technische und organisatorische Ressourcen zur Verfügung. Die Umsetzung erfolgte eigenständig im Rahmen der betrieblichen Ausbildungszeit mit einer täglichen Projektarbeitszeit von acht Stunden.

Als Hardware-Ressource wurde ein dedizierter Backup-Server mit ausreichend Speicherplatz (RAID6) verwendet, welcher bereits im Unternehmen vorhanden war. Der Server wurde als zentrale Komponente zur Datensicherung eingesetzt und diente als Speicherziel für alle Microsoft 365-Backups. Die benötigte Software „Veeam Backup for Microsoft 365“ wurde durch den Ausbildungsbetrieb lizenziert und zur Verfügung gestellt.

Zur Einrichtung der Sicherung war zudem ein vollwertiger administrativer Zugriff auf die Microsoft 365-Umgebung sowie auf das Microsoft EntraID erforderlich. Dies war notwendig, um App-Registrierungen, API-Zugriffe und die Rechtevergabe für das Restore Portal korrekt umsetzen zu können.

Die Einrichtung und Konfiguration erfolgte über meinen Ausbildungsarbeitsplatz, der mit allen nötigen Werkzeugen wie Remote-Verwaltungssoftware, Office-Anwendungen, Internetzugang und einem zweiten Monitor zur parallelen Arbeit ausgestattet war. Weitere Ressourcen wie Büroräume, Testbenutzerkonten oder DNS-Zugriffe wurden intern bereitgestellt.

Da ich über die nötigen Berechtigungen und das technische Know-how verfügte, konnte das gesamte Projekt ohne personelle Unterstützung durchgeführt werden. Die Abstimmung mit der IT-Leitung erfolgte lediglich zur Zieldefinition und zur abschließenden Abnahme.

3 Analysephase

3.1 Ist-Analyse

Die Ashampoo GmbH & Co. KG ist ein Unternehmen, das in der Softwareentwicklung und der Bereitstellung eines Marktplatzes für Software tätig ist. Die Ashampoo GmbH & Co. KG hat vor kurzem begonnen, seine lokalen Serverstrukturen in die Cloud zu migrieren. Die Nutzung von Microsoft 365 als zentrale Plattform für Dokumente und Kommunikation hat stark zugenommen. Derzeit existiert jedoch kein eigenständiges Backup-System für Microsoft 365 Daten (SharePoint, Exchange Online, OneDrive und Microsoft Teams). Microsoft bietet zwar eine gewisse Redundanz, jedoch keine granulare Backup- und Wiederherstellungslösung für gelöschte oder beschädigte Daten über längere Zeiträume hinaus. Die IT-Abteilung ist für die Datensicherung verantwortlich und benötigt eine zuverlässige, DSGVO-Konforme und einfach zu verwaltende Backup-Lösung.

3.2 Stakeholder Analyse

Im Rahmen des Projekts „Einführung von Veeam Backup for Microsoft 365 (Self Hosted)“ wurden verschiedene Stakeholder identifiziert, die in unterschiedlichem Maße von der Planung, Umsetzung und dem späteren Betrieb der Lösung betroffen sind. Ziel der Stakeholder-Analyse ist es, die jeweiligen Interessen, Einflussmöglichkeiten und Kommunikationsbedarfe transparent darzustellen, um potenzielle Konflikte zu vermeiden und die Akzeptanz der Lösung sicherzustellen.

Zu den zentralen Stakeholdern gehört insbesondere die IT-Abteilung, da sie sowohl für die technische Umsetzung als auch für den langfristigen Betrieb des Systems verantwortlich ist. Auch die Geschäftsführung ist indirekt beteiligt, da sie das Projekt im Hinblick auf Wirtschaftlichkeit, Sicherheit und strategische Entscheidungen unterstützt.

Ein weiterer relevanter Stakeholder sind die regulären Anwenderinnen und Anwender, da sie durch das Restore Portal direkt mit der Lösung interagieren. Deshalb ist es wichtig, diese Zielgruppe durch eine benutzerfreundliche Oberfläche sowie eine verständliche Anwenderdokumentation zu unterstützen und in den Change-Prozess einzubinden.

Die konkrete Zuordnung der Stakeholder sowie ihre Interessen und Einflussgrade sind in **Tabelle 5: Stakeholder Analyse** im Anhang zusammengefasst. Auf Basis dieser Analyse wurde eine Kommunikationsstrategie entwickelt, die sicherstellt, dass alle Beteiligten bedarfsgerecht informiert und einbezogen werden. Dies erfolgt beispielsweise durch technische Abstimmungen, Schulungsmaßnahmen oder Ergebnispräsentationen.

3.3 Wirtschaftlichkeitsanalyse

Microsoft 365 stellt Dienste wie Exchange Online, OneDrive und SharePoint bereit – mit hoher Verfügbarkeit und Replikation. Diese Redundanz ersetzt jedoch kein Backup. Microsoft übernimmt im Rahmen des Shared Responsibility Models keine Verantwortung für den Schutz der Inhalte – insbesondere nicht gegen:

- Versehentliches oder böswilliges Löschen
- Interne / Externe Angriffe (z.B. Ransomware, Phishing)
- Compliance- oder rechtliche Anforderungen an Datenaufbewahrung

Das Ziel ist es also:

- Alle Microsoft 365 Dienste zuverlässig und nachvollziehbar zu sichern
- Granulare Wiederherstellungen zu ermöglichen
- Betriebsausfälle und Produktivitätsverluste bei Datenverlust zu minimieren

3.3.1 Potenzielle Schadenskosten ohne Backup

Laut einer Verizon Studie, können selbst „kleine“ Datenpannen bis zu einer halben Million Dollar kosten, „große“ sogar 200 Millionen. (Reed & Watson, 2021)

Die Einführung eines Backup-Systems für Microsoft 365 stellt sowohl aus wirtschaftlicher als auch aus sicherheitstechnischer Sicht eine strategisch sinnvolle Entscheidung dar. Schon die Vermeidung eines einzigen kritischen Datenverlusts kompensiert die gesamten Projektkosten mehrfach.

Die Einführung reduziert nicht nur das Risiko von Datenverlust, sondern erhöht auch die Reaktionsfähigkeit und Rechtssicherheit im Krisenfall.

3.4 Nutzwertanalyse

Im Rahmen der Entscheidungsfindung zur Auswahl einer geeigneten Backup-Lösung für Microsoft 365 wurde eine Nutzwertanalyse durchgeführt. Dabei wurden fünf verschiedene Lösungen miteinander verglichen: Veeam Self-Hosted, Synology Active Backup, CloudAlly, Afi.ai sowie Veeam Backup Flex die Online-Lösung von Veeam. Berücksichtigt wurden sowohl wirtschaftliche als auch technische und organisatorische Kriterien. Die Bewertung erfolgte auf Basis gewichteter Faktoren, unter anderem Kosten, Aufbewahrungsmöglichkeiten, Wiederherstellungszeit, Benutzerfreundlichkeit sowie Datenschutzaspekte.

Die höchste Gesamtpunktzahl erzielte die Lösung Veeam Self-Hosted mit 37 Punkten. Sie überzeugte besonders in den Bereichen Wiederherstellungszeit, Datenschutz, Flexibilität und granularer Wiederherstellung. Zwar entstehen hierbei einmalige Investitionskosten für Festplatten, diese relativieren sich jedoch über die geplante Nutzungsdauer von drei Jahren. Ebenfalls gut bewertet wurden Synology Active Backup (36 Punkte) sowie CloudAlly (35 Punkte). Afi.ai schnitt mit 32 Punkten etwas schlechter ab, insbesondere aufgrund höherer Betriebskosten und Einschränkungen bei der Benutzerfreundlichkeit und Administration.


Die vollständige Bewertungsmatrix mit allen Kriterien, Gewichtungen und Ergebnissen ist im **Anhang A.2. Nutzwertanalyse** dieser Dokumentation einsehbar.

3.4.1 Make or Buy Entscheidung

Im Rahmen der Projektplanung wurde geprüft, ob die Backup-Lösung für Microsoft 365 selbst betrieben („Make“) oder als externe Dienstleistung bezogen („Buy“) werden soll. Beide Ansätze bieten funktional ähnliche Möglichkeiten zur Sicherung von Exchange Online, OneDrive, SharePoint und Microsoft Teams, unterscheiden sich jedoch deutlich hinsichtlich Kostenstruktur, Datenhoheit, Flexibilität und Abhängigkeit vom Anbieter.

Beim „Make“-Ansatz wird die Backup-Lösung mit Veeam Backup for Microsoft 365 auf einem eigenen bereits vorhandenen Server betrieben. Die Datensicherung erfolgt lokal, und es entstehen lediglich Lizenzkosten für die Software sowie einmalige Kosten für zusätzliche Festplatten. Der große Vorteil dieses Ansatzes liegt in der vollständigen Datenkontrolle. Die Daten verlassen zu keinem Zeitpunkt das Unternehmen. Nachteilig ist, dass der Betrieb und die Wartung durch die IT-Abteilung erfolgen muss, was jedoch im vorliegenden Fall problemlos möglich ist, da die generelle Benutzeroberfläche von Veeam bereits bekannt ist und Veeam Backup & Replication 12 ebenfalls auf dem schon vorhandenen ASHSRVBACKUP02 Server läuft.

Beim „Buy“-Ansatz handelt es sich um vollständig cloudbasierte Backup-Lösungen, die als Software-as-a-Service (SaaS) angeboten werden. Anbieter wie CloudAlly, Afi.ai oder Veeam Flex bieten einfache Benutzeroberflächen, automatische Updates und geringen Administrationsaufwand. Die Kostenstruktur ist jedoch deutlich anders: Statt einmaliger Lizenzkosten fallen monatlich oder jährlich wiederkehrende Kosten pro Benutzer an. Bei 112



Benutzern entstehen so – je nach Anbieter – zwischen 3.100 € und über 4.000 € pro Jahr. Langfristig gesehen ist dies deutlich teurer als die lokale Lösung. Zusätzlich liegt die Datenspeicherung bei SaaS-Anbietern außerhalb der eigenen Infrastruktur. Dadurch ergeben sich Abhängigkeiten in Bezug auf Datenschutz, Verfügbarkeit und Vertragslaufzeiten.

Im direkten Vergleich zeigt sich, dass die intern betriebene Lösung wirtschaftlich langfristig günstiger, technisch flexibler und datenschutzrechtlich sicherer ist. Die vorhandene Infrastruktur ermöglicht eine reibungslose Umsetzung, und auch die laufenden Betriebskosten sind überschaubar. Die Self-Service-Funktion über das Restore-Portal bietet einen ähnlichen Komfort wie bei SaaS-Lösungen, ohne dass Daten das Unternehmen verlassen.

Aus diesen Gründen fiel die Entscheidung bewusst zugunsten des „Make“-Ansatzes. Die Backup-Lösung wird vollständig im Unternehmen betrieben, bietet volle Kontrolle über die Daten und ist gleichzeitig kosteneffizient – sowohl kurzfristig als auch auf Dauer.

3.4.2 Projektkosten

Tabelle 4: Projektkosten

Position	Menge/Dauer	Einzelpreis	Gesamtkosten
Veeam Backup for Microsoft 365	114 Benutzer/3 Jahre	23,20€	2.645,37€
Arbeitskosten	40 Stunden	80€/Std	3.200,00€
Backupserver	-	-	0,00€
Backupserver Festplatten	12 Festplatten	186€	2.232,00€
Betriebskosten	Strom, Wartung	Pauschal	600€
Gesamtkosten	-	-	8.677,37

4 Entwurfsphase


4.1 Erstellung eines detaillierten Implementierungsplans

Für die Implementierung von Veeam Backup for Microsoft 365 ist geplant, die Software auf dem bereits vorhandenen Server ASHSRVBACKUP02 zu installieren. Dieser dient sowohl als Plattform für die Anwendung als auch als Speicherort für die gesicherten Daten. Vor der Installation werden alle erforderlichen Systemvoraussetzungen geprüft und das Betriebssystem aktualisiert, um eine stabile Grundlage für den Betrieb zu gewährleisten.

Nach der Installation wird die Verbindung zu Microsoft 365 über die sogenannte moderne Authentifizierung hergestellt. Dafür werden zwei Applikationen in Azure Enterprise Application registriert: eine Hauptanwendung für den Zugriff auf die Microsoft Graph API und eine zusätzliche Anwendung für den Zugriff auf Exchange Online. Die Authentifizierung erfolgt über ein selbst erzeugtes Zertifikat, das sowohl in Azure als auch in der Veeam-Konfiguration eingebunden wird.

Im nächsten Schritt wird ein lokales Backup-Repository auf dem Server erstellt. Es wird mit einer Item-Level Retention von 3 Jahren konfiguriert, um einzelne Elemente wie E-Mails, Dateien oder Kalendertermine gezielt wiederherstellen zu können. Anschließend werden automatisierte Backup-Jobs eingerichtet, die täglich alle relevanten Microsoft 365-Dienste sichern.

Zur Unterstützung der IT-Abteilung und zur Entlastung im Support wird zusätzlich das Restore Portal eingerichtet. Dieses ist über eine verschlüsselte Verbindung erreichbar und erlaubt



berechtigten Nutzern, selbstständig Daten wiederherzustellen. Für das Portal wird ein DNS-Eintrag angelegt sowie ein separates Zertifikat eingebunden.

Zum Abschluss der Implementierung sind Wiederherstellungstests vorgesehen, um die Funktionsfähigkeit der Backup-Jobs sowie der Restore-Funktionen zu überprüfen. Zusätzlich wird eine E-Mail-Benachrichtigung bei Fehlern eingerichtet. Die gesamte Konfiguration wird in einer technischen Dokumentation festgehalten, die anschließend an die IT-Abteilung übergeben wird.

5 Durchführungsphase

5.1 Installation der Software

Die Software Veeam Backup for Microsoft 365 (VBO365) wurde über die offizielle Veeam-Website heruntergeladen. Die heruntergeladene ISO-Datei wurde als virtuelles Laufwerk eingebunden. Anschließend wurde die Installation über das virtuelle Laufwerk gestartet. Im Verlauf der Installation wurde der Lizenzschlüssel eingebunden und ein dedizierter Administrator-Benutzer für VBO365 eingerichtet. Nach erfolgreicher Installation kann die Software gestartet werden.

5.2 Hinzufügen der Microsoft 365-Organisation

Nach dem Start der Anwendung wird über die Multifunktionsleiste der Punkt „Add Org“ (Organisation hinzufügen) ausgewählt. Im folgenden Schritt wird die Art der Bereitstellung abgefragt. Zur Auswahl stehen:

- Microsoft 365
- Hybrid
- On-Premise

Microsoft 365 ist für Organisationen vorgesehen, deren IT-Infrastruktur vollständig auf Cloud-Dienste von Microsoft basiert. Dies umfasst unter anderem Dienste wie Exchange Online, SharePoint Online, OneDrive for Business sowie Microsoft Teams.

Diese Variante stellt die einfachste Konfiguration dar, da sämtliche zu sichernden Daten über Microsofts Cloud-Infrastruktur bereitgestellt und ausschließlich über die Microsoft Graph API zugänglich gemacht werden.

Bei der Ashampoo GmbH & Co. KG trifft dieses Modell zu, da ein Großteil der unternehmensweiten IT-Dienste cloudbasiert betrieben wird.

Die hybride Konfiguration wird verwendet, wenn es noch einen lokalen Exchange Server oder einen SharePoint Server gibt. Veeam ermöglicht in diesem Fall eine einheitliche Sicherung beider Umgebungen, wobei sowohl lokale Server als auch die MS365 Cloud über APIs angesprochen werden.

On-Premise betrifft Organisationen, deren IT-Infrastruktur vollständig lokal betrieben wird, ohne Anbindung an Microsoft 365. Zum Einsatz kommen hierbei unter anderem lokale Exchange Server oder SharePoint Server.

Veeam kommuniziert in diesem Fall direkt mit den On-Premise-Systemen, um die Datensicherung durchzuführen. Eine Integration mit Microsoft Graph API oder anderen Cloud-spezifischen Schnittstellen ist in diesem Szenario nicht erforderlich.

5.3 Auswahl der zu sichernde Dienste

Im nächsten Schritt wird ausgewählt, welche Dienste gesichert werden sollen, da die Ashampoo GmbH & Co. KG alle Dienste sichern will wird folgendes ausgewählt:

- Exchange Online
- SharePoint Online
- OneDrive for Business
- Microsoft Teams

Bei Microsoft Teams werden je nach Wahl, die Gruppen gesichert oder auch gleich die ganzen privaten Chats. Für das zweitere wird man zur Zahlung für die Nutzung der Microsoft API gefordert.

5.4 Verbindungs- und Authentifizierungseinstellungen

Unter den Verbindungsoptionen wird die Region „Default“ ausgewählt. Weitere Optionen wären „US-Government“ oder „China“.

Als Authentifizierungsmethode wird Modern Authentication verwendet, da Basic Authentication von Microsoft nicht mehr unterstützt wird.

5.5 Registrierung einer Microsoft Azure-Anwendung

Damit VBO365 Zugriff auf Microsoft 365 erhält, wird eine neue Enterprise Application in Azure registriert. Die App erhält den Namen „VBO365 ENApp“.

Außerdem wird für die Enterprise App ein Zertifikat für die Authentifizierung bei Azure erstellt. Das Zertifikat nennen wir „VBO365 EnApp Certificate“.

Anschließend erfolgt die Anmeldung über Device Login mit einem Microsoft-Administratorkonto. Nach erfolgreicher Authentifizierung erscheint die Bestätigung: „You are authenticated to Microsoft 365 as [REDACTED]@ashampoo.com“

Daraufhin prüft VBO365 die Verbindung zu:

- Entra ID
- Microsoft Graph API
- Exchange Web Services (EWS)
- SharePoint Online
- PowerShell
- Exchange Online Plan
- SharePoint Plan

Sollten Berechtigungen fehlen, wird dies bei den jeweiligen Verbindungstests angezeigt.

5.6 Einrichtung eines Auxiliary Backup Accounts

Um API-Limits von Microsoft 365 zu umgehen und parallele Backup-Prozesse zu ermöglichen, wird ein sogenannter Auxiliary Backup Account eingerichtet. Hierzu muss man einen Rechtsklick auf die Organisation machen und dann „Manage Backup Applications“ auswählen. Dort erstellen wir nun eine neue App mit dem Namen „VBO365 EnApp AuxBackup“. Für die App muss ebenfalls ein Zertifikat zur Authentifizierung mit Azure erstellt werden. Dieses nennen wir „VBO EnApp AuxBackup Certificate“. Nach der Erstellung des Zertifikats, wird man wieder gebeten, sich über den Microsoft Device Login zu authentifizieren. Nach Abschluss wird bestätigt, dass 5 Auxiliary Applications erfolgreich erstellt wurden. Diese dienen der Lastverteilung und Performancesteigerung bei Backup- und Restore-Prozessen.

5.7 Repository und Backup-Jobs

Nach erfolgreicher Einrichtung der Organisation muss ein Backup Repository definiert werden. In Veeam Backup for Microsoft 365 erfolgt dies über den Menüpunkt „Backup Infrastructure“, unter welchem sich die Option „Backup Repositories“ befindet. Hierüber wird ein neues Repository hinzugefügt, das als Speicherziel für alle Sicherungen dient.

Während der Einrichtung des Repositories wird neben dem Speicherpfad auch das Retention-Verhalten (Aufbewahrungsrichtlinie) festgelegt. Veeam bietet hierbei zwei unterschiedliche Methoden.

5.7.1 Item-Level Speicherung

Bei der Item-Level Retention handelt es sich um eine objektbasierte Aufbewahrungsmethode. Jedes einzelne Objekt – beispielsweise eine E-Mail, ein OneDrive-Dokument oder ein Kalendereintrag – wird individuell betrachtet. Die definierte Aufbewahrungsfrist beginnt mit dem Zeitpunkt der Erfassung oder Änderung des jeweiligen Objekts im Backup. Sobald die Retention-Zeit eines Objekts abläuft, wird es automatisch aus dem Backup entfernt. Dieses Modell bietet eine hohe Granularität und Flexibilität bei der Verwaltung einzelner Datenobjekte und ist insbesondere im Kontext moderner Microsoft 365-Nutzung von Vorteil. Ein wesentlicher Vorteil besteht in der Speicherersparnis, da nicht mehr benötigte oder gelöschte Daten gezielt entfernt werden können. Darüber hinaus ermöglicht dieses Modell eine gezielte Umsetzung datenschutzrechtlicher Vorgaben, wie sie etwa durch die DSGVO (Datenschutz-Grundverordnung) gefordert werden – beispielsweise das selektive Löschen von Benutzerdaten nach deren Ausscheiden aus dem Unternehmen.

5.7.2 Snapshot-Basierte Speicherung

Die Snapshot-Based Retention, bei der der Zustand der gesicherten Daten zu einem bestimmten Zeitpunkt als Snapshot gespeichert und für die Dauer der Aufbewahrungsfrist vollständig vorgehalten wird. Das bedeutet, dass alle Daten – unabhängig davon, ob sie zwischenzeitlich gelöscht oder verändert wurden – für die festgelegte Zeitspanne verfügbar bleiben. Dieses Modell eignet sich insbesondere für Organisationen, die großen Wert auf die Möglichkeit legen, einen vollständigen Datenzustand zu einem bestimmten Zeitpunkt wiederherzustellen. Die Konfiguration ist in der Regel einfacher und eignet sich gut für Szenarien, in denen Compliance-Anforderungen eine lückenlose Archivierung erfordern. Allerdings geht diese Methode mit einem deutlich höheren Speicherbedarf einher und bietet keine Möglichkeit zur gezielten Entfernung einzelner Datenobjekte.

5.7.3 Auswahl und Begründung der Aufbewahrungs-Methode

Für die Ashampoo GmbH & Co. KG fiel die Wahl auf die Item-Level Retention, da diese Methode besonders gut zu den Anforderungen an Speicherverbrauch, Flexibilität und einfache Verwaltung passt. Im Gegensatz zur Snapshot-basierten Speicherung werden hier einzelne Objekte – etwa E-Mails oder Dokumente – separat betrachtet und nur so lange aufbewahrt, wie es für jedes Objekt individuell vorgesehen ist. Sobald ein Objekt gelöscht wurde und die definierte Frist abläuft, wird es automatisch aus dem Backup entfernt.

Ein wesentlicher Vorteil dieser Methode ist die effizientere Nutzung des Speicherplatzes. Da nicht ganze Datenbestände über lange Zeiträume gehalten werden, lässt sich der Ressourcenverbrauch besser kontrollieren. Gleichzeitig ermöglicht die Item-Level-Methode eine gezielte Wiederherstellung einzelner Objekte, was im Arbeitsalltag Zeit spart und Prozesse vereinfacht.

Gerade in einer modernen, cloudbasierten IT-Umgebung wie bei Ashampoo, in der sich Inhalte schnell ändern und große Datenmengen entstehen, bietet diese Methode eine sinnvolle Kombination aus Kontrolle, Übersichtlichkeit und Skalierbarkeit.

5.8 Konfiguration des Backup-Jobs

Nach der Erstellung des Backup-Repositories kann im nächsten Schritt ein Backup-Job angelegt werden. Dieser definiert, welche Inhalte gesichert werden sollen und nutzt das vorherig erstellte Backup Repository als Speicherziel.

Zunächst wird dem Backup-Job ein Name zugewiesen. In diesem Fall nennen wir es „*Primary Organization Backup*“. Darauf wird dem Backup-Job noch eine kurze Beschreibung über Zweck und Umfang der Sicherung hinzugefügt. Anschließend wird die Option „*Back up entire organization*“ ausgewählt, wodurch standardmäßig alle verfügbaren Microsoft 365 Komponenten der Organisation gesichert werden.

Daraufhin bietet Veeam die Möglichkeit, gezielt bestimmte Objekte von der Sicherung auszuschließen. Dies können beispielsweise einzelne Benutzerkonten, Gruppen, SharePoint-Seiten oder Teams-Kanäle sein. In der initialen Einrichtung wurde aufgrund von zeitgleichen Arbeiten an der SharePoint Migration des Design Teams, dieses Team aus dem initialen Backup rausgenommen. Das Design Team wurde nach der durchgeführten Migration in das Backup mit aufgenommen.

Im nächsten Schritt wird das zuvor erstellte Repository als Ziel für die Sicherungsdaten ausgewählt. Abschließend wird der Sicherungsplan definiert. In diesem Fall wurde ein tägliches Backup um 23:00 Uhr gewählt. Zusätzlich wurde die Option aktiviert, fehlgeschlagene Sicherungsversuche automatisch bis zu drei Mal zu wiederholen, mit einem Intervall von jeweils zehn Minuten zwischen den Versuchen.

Das Initial Backup nahm eine Laufzeit von etwa 29 Stunden in Anspruch. Die folgenden inkrementellen Backups, die nur noch Änderungen seit dem letzten Durchlauf erfassen, benötigen im Durchschnitt nur noch drei bis zehn Minuten, da nur noch neue oder veränderte Dateien und E-Mails gesichert werden.


Anders als bei klassischen inkrementellen Backup-Strategien handelt es sich bei Veeam um das sogenannte „Forever Incremental“-Verfahren. Dabei wird lediglich einmalig ein vollständiges Backup durchgeführt. Alle nachfolgenden Sicherungen speichern ausschließlich die Änderungen seit dem letzten Backup. Im Gegensatz zu traditionellen inkrementellen Methoden, bei denen zur Wiederherstellung oft die gesamte Kette aller Backups benötigt wird, verwaltet Veeam die Daten intern so, dass auch bei Verlust einzelner Inkremente eine Wiederherstellung weiterhin möglich ist. Dies erhöht die Ausfallsicherheit, reduziert den Speicherbedarf deutlich und ermöglicht dennoch eine vollständige Wiederherstellung zu jedem Zeitpunkt innerhalb der definierten Aufbewahrungsfrist.

5.9 Einrichtung des Self-Service Restore Portals

Nach der Konfiguration der Backup-Jobs folgt die optionale Einrichtung des Self-Service-Portals. Dies ermöglicht es den Nutzern, eigenständig Daten wiederherzustellen, wie etwa gelöschte E-Mails, OneDrive Dateien oder Persönliche SharePoint Seiten, ohne dass ein Administrator direkt eingreifen muss. Die Einrichtung basiert auf dem in Veeam integrierten Restore Portal und erfordert mehrere Konfigurationsschritte sowie die Anbindung an Microsoft Entra ID (ehemals Azure Active Directory).

Zunächst muss unter „*General Options*“ im Bereich „*Authentication*“ die Anmeldung über Microsoft-Anmeldeinformationen aktiviert werden. Damit sich Nutzer per Microsoft-365 Konto anmelden können, muss ein entsprechendes Zertifikat erstellt und eingebunden werden. Dieses nennen wir „*VMB365 Auth Certificate*“.

Anschließend wird im Reiter „*Restore Portal*“ das eigentliche Portal aktiviert. Dafür ist die Registrierung einer neuen Azure-Anwendung erforderlich. Auch hier wird die Region „*Default*“



ausgewählt, da keine spezielle Umgebung wie US-Regierung oder China verwendet wird. Die Anwendung wird unter dem Namen „VBO365 Portal“ registriert und ebenfalls mit einem eigenen Zertifikat versehen, das den Namen „VBO365 Portal Certificate“ bekommt.

Im Anschluss wird die Zugriffsadresse des Portals festgelegt. In diesem Fall erfolgt der Zugriff intern über die IP-Adresse des Backup Servers ASHSRVBACKUP02. Die Adresse, worüber das Veeam Wiederherstellungsportal intern erreicht werden kann, ist: <https://10.21.0.37:4443>. Der Port 4443 wird von Veeam empfohlen und ist eine Alternative zu dem HTTPS/SSL Port 443.

Zur Authentifizierung der Anwendung gegenüber Microsoft 365 ist ein letzter Anmeldevorgang über den Device Login erforderlich.

Im letzten Schritt wird die Veeam REST API aktiviert. Hierfür wird auch ein Zertifikat benötigt. Wir können uns hier entscheiden, ob wir ein neues Zertifikat erstellen oder ein vorhandenes benutzen. Durch die Verwendung des Zertifikats von „ashampoo.com“, zeigt der Browser beim Aufruf des Restore Portals an, dass es eine Sichere Seite ist. Um das Zertifikat von Ashampoo dort hinzuzufügen, müssen wir uns die pfx (Personal Information Exchange) Datei von unserem Passwortmanager herunterladen und dieses dann hinzufügen.

Nach Abschluss der technischen Einrichtung folgt die Konfiguration der Wiederherstellungsberechtigungen. Hierzu wird im Menüpunkt „*Manage Users & Roles*“ unter „*Restore Operators*“ eine Benutzergruppe definiert, die Zugriff auf das Portal und die dort verfügbaren Restore-Funktionen erhält. In diesem Fall wurde die Gruppe Microsoft 365 Gruppe „*Admins*“ ausgewählt. Daraufhin muss der Gruppe „*Admins*“ die Organisation zugeordnet werden, damit diese jederzeit eine Wiederherstellung von bestimmten Objekten starten können.

Damit Benutzer sich die IP nicht merken müssen, wird auf dem lokalen Domain Controller ein neuer A-Name Record erstellt. Der A-Name Record verweist ein dann bei Eingabe der Adresse <https://recovery.ashampoo.com> auf die IP „10.21.0.37:4443“.

Da der Domain Controller nur lokal auf die IP-Adresse verweisen kann und nicht wenn man im Home-Office arbeitet, wird dazu noch ein Eintrag in AWS Route53 hinzugefügt. Dort muss man auf die gehosteten Zonen gehen und dann den Eintrag „*ashampoo.com*“ suchen und öffnen. Hier erstellen wir dann einen neuen CNAME Eintrag und nennen ihn „*recovery*“ mit dem Wert „*recovery.ashampoo.local.*“, dies wird nun gespeichert und die Adresse <https://recovery.ashampoo.com:4443> ist nun auch über VPN erreichbar. Wenn man versucht diese Adresse ohne VPN zu öffnen, bekommt man lediglich den Fehler „*ERR_NAME_NOT_RESOLVED*“.

Damit Azure auch über die Adresse <https://recovery.ashampoo.com:4443> und <https://recovery.ashampoo.local:4443> Bescheid weiß, muss dieses dort in der vorher erstellten App „*VPM365 Restore Portal*“ als URI (Uniform Ressource Identifier) als mögliche Adresse hinzugefügt werden. Die App findet man in „*Azure App Registrations*“.

Für die benutzerfreundliche Wiederherstellung einzelner Objekte wurde das Restore Portal eingerichtet. Dieses ermöglicht autorisierten Mitarbeitenden über eine Weboberfläche Zugriff auf gesicherte Inhalte. Das Portal wurde mit einem eigenen SSL-Zertifikat abgesichert und über die Adresse <https://recovery.ashampoo.com:4443> erreichbar gemacht. Dazu wurden sowohl ein interner DNS-Eintrag (*recovery.ashampoo.local*) als auch ein externer CNAME-Eintrag für die öffentliche Domain konfiguriert. In Azure wurde eine zusätzliche App-Registrierung vorgenommen, um das Portal mit Microsoft 365 zu verbinden. Darüber hinaus wurden sogenannte Restore Scopes definiert, um granular festzulegen, welcher Benutzer auf welche Daten zugreifen darf.

5.10 Wiederherstellungstests

Nach Abschluss der Backup-Konfiguration wurden verschiedene Wiederherstellungsszenarien erfolgreich getestet, Hierzu zählten unter anderem die Wiederherstellung einer einzelnen E-Mail an dem ursprünglichen Ort, das Wiederherstellen einer Datei aus OneDrive for Business in das alternative Verzeichnis „Restore“, das Wiederherstellen einer SharePoint Site und von SharePoint Dokumenten sowie das Wiederherstellen eines Kalendertermins in Outlook. Die Tests wurden sowohl über das Restore Portal als auch direkt in der Veeam-Konsole durchgeführt.

Sämtliche Wiederherstellungsvorgänge sowie Zugriffe, sowohl über das Restore Portal als auch über die Veeam Konsole wurden ordnungsgemäß protokolliert. Diese enthalten unter anderem Informationen zu Zeitpunkt, Benutzerkonto, wiederhergestelltem Objekt, Kommentar und Zielort der Wiederherstellung.

5.11 E-Mail-Benachrichtigungen

Nach der vollständigen Konfiguration und Wiederherstellungstests, werden die E-Mail-Benachrichtigungen eingestellt. Hierzu wird unter dem Punkt „General Options“ der Reiter „Notifications“ ausgewählt. Dort wird der Haken bei „Enable E-Mail notifications“ gesetzt und verifizieren uns über den Microsoft 365 (modern authentication) Mail Server. Hier benutzen wir das Konto [REDACTED]@ashampoo.com. Danach müssen wir den Absender und den Empfänger für die Benachrichtigungen auswählen. Der Sender ist [REDACTED]@ashampoo.com, der Empfänger ist [REDACTED]@ashampoo.com, welche die E-Mail-Adresse unseres Ticket Systems ist. Auf diese Weise ist sichergestellt, dass mögliche Probleme unmittelbar an die IT-Abteilung weitergeleitet werden.

Anschließend wird festgelegt, in welchen Fällen Benachrichtigungen versendet werden sollen. Es wurde konfiguriert, dass Benachrichtigungen bei Warnungen und Fehlermeldungen erfolgen. Dabei werden die E-Mails jedoch erst verschickt, wenn alle drei Wiederholungsversuche eines fehlgeschlagenen Backup-Jobs erfolglos geblieben sind.

Die Option, auch bei erfolgreich durchgeführten Backups eine Bestätigung per E-Mail zu erhalten, wurde deaktiviert, um unnötige Systemmeldungen zu vermeiden.

6 Abnahmephase

Nach Abschluss der Implementierung wurde die Lösung einer strukturierten Abnahme unterzogen, um die Funktionsfähigkeit sicherzustellen und die Übergabe an den produktiven Betrieb vorzubereiten.

Zunächst erfolgte eine vollständige Überprüfung der Funktionsfähigkeit. Dabei wurden alle konfigurierten Backup-Jobs auf ihren erfolgreichen Abschluss hin überprüft. Die tägliche Sicherung aller relevanten Microsoft 365-Dienste – darunter Exchange Online, OneDrive, SharePoint und Teams – konnte zuverlässig nachgewiesen werden. Auch das Backup-Repository zeigte eine erwartungskonforme Datenbelegung entsprechend den Retention-Einstellungen. Zusätzlich wurden mehrere Wiederherstellungen in unterschiedlichen Varianten getestet, um die Integrität der Sicherungen sicherzustellen. Dazu zählten u. a. das Wiederherstellen einzelner E-Mails, OneDrive-Dateien sowie Kalendereinträge – sowohl an den ursprünglichen Speicherort als auch in alternative Ziele.

Im Anschluss daran wurde eine kurze Einweisung für die IT-Mitarbeitenden durchgeführt. In dieser wurden die wichtigsten Funktionen und Bedienelemente der Veeam-Konsole sowie des Restore Portals erläutert. Besonders hervorgehoben wurden dabei die Wiederherstellungsfunktionen, die Überwachung laufender Jobs sowie der Umgang mit



Benachrichtigungen bei Backup-Fehlern. Die Dokumentation wurde der IT übergeben und zusätzlich zentral abgelegt, um eine langfristige Nachvollziehbarkeit zu gewährleisten.

Abschließend wurde das Projekt im Rahmen einer Abschlusspräsentation der IT-Leitung vorgestellt. Dabei wurden die Ziele, das Vorgehen sowie die erarbeiteten Ergebnisse erläutert. Auch die getroffenen Entscheidungen zur Repository-Struktur, zur Auswahl der Retention-Strategie und zur Nutzerberechtigung im Restore Portal wurden begründet dargelegt. Nach Prüfung aller Ergebnisse wurde das Projekt offiziell freigegeben und abgenommen. Die Backup-Lösung befindet sich seitdem im operativen Einsatz.

7 Fazit

Mit der Umsetzung dieses Projekts wurde eine zentrale und zuverlässige Backup-Lösung für Microsoft 365 eingeführt, die den modernen Anforderungen an Datensicherheit, Wiederherstellbarkeit und Transparenz entspricht. Durch die Sicherung von Exchange Online, OneDrive for Business, SharePoint Online und Microsoft Teams wurde eine umfassende Datensicherungslösung etabliert, die unabhängig von den Standardfunktionen von Microsoft arbeitet und eine echte Absicherung vor Datenverlust bietet.

Die gewählte Item-Level Retention ermöglicht eine effiziente und flexible Datenhaltung mit geringerem Speicherbedarf, während gleichzeitig eine granulare Wiederherstellung einzelner Objekte jederzeit möglich ist. Der Einsatz des Restore Portals bietet zudem die Möglichkeit, Zugriffsrechte für Wiederherstellungen gezielt zu delegieren und so den IT-Support zu entlasten.

Die Umsetzung konnte vollständig, eigenständig und innerhalb des geplanten Zeitrahmens durchgeführt werden. Alle gesetzten Ziele wurden erreicht, die Backup-Jobs laufen automatisiert, die Wiederherstellung wurde erfolgreich getestet und die Lösung ist dokumentiert und abgenommen. Darüber hinaus wurde eine solide Grundlage für eine spätere Erweiterung – beispielsweise durch Offsite-Backup oder revisionssichere Archivierung – geschaffen.

Insgesamt war das Projekt technisch wie organisatorisch ein voller Erfolg und stellt einen wichtigen Beitrag zur Betriebssicherheit und Datenverfügbarkeit im Unternehmen dar.



8 Literaturverzeichnis

Reed, & Watson. (2021). *Microsoft 365 Backup für Dummies – Gekürzte Veeam-Sonderausgabe*. John Wiley & Sons, Inc.

Veeam Software Group. (24. 03 2025). *Veeam Backup for Microsoft 365 User Guide*. Von https://helpcenter.veeam.com/docs/vbo365/guide/vbo_used_ports.html?ver=80 abgerufen

A. Anhänge

A.1. Stakeholder Analyse

Stakeholder	Interesse	Einfluss	Beteiligung	Maßnahmen / Kommunikation
IT-Abteilung	Sicherstellung des Betriebs, Wiederherstellung, Backup-Kontrolle	Hoch	Direkt beteiligt	Aktualisierung des Systems, Benutzerrechte verwalten
Geschäfts-führung	Kosteneffizienz, Datensicherheit, DSGVO-Konformität	Mittel	Indirekt	Projektpräsentation, Statusberichte, Nutzenargumentation
Endanwender	Zugriff auf Wiederherstellungen, einfache Nutzung	Gering – Mittel	Betroffen	Schulung / Anwenderdokumentation, Self-Service Portal
Auszubildender (Projekt-leitung)	Umsetzung des Projekts, technische Konfiguration	Mittel (intern)	Operativ verantwortlich	Eigenständige Durchführung, Dokumentation
Veeam	Softwarebereitstellung, Support bei Problemen	Gering	Technisch eingebunden	Bei Bedarf Kontaktaufnahme über Support oder Partner

Tabelle 5: Stakeholder Analyse

Backup-Lösung	Unterstützte Dienste	Gewichtung (5)	Kosten im Jahr (114 Benutzer)	Gewichtung (5)	Granulare Wiederherstellung	Gewichtung (3)	Aufbewahrung	Gewichtung (4)
Veeam Self Host	Exchange, SharePoint, OneDrive, Teams	5	881,79 €	4	Ja	3	Unbegrenzt	4
Synology Active Backup (NAS)	Exchange, SharePoint, OneDrive, Teams	5	0 €	5	Ja	3	Unbegrenzt	4
CloudAlly	Exchange, SharePoint, OneDrive, Teams	5	3.192 €	3	Ja	3	Unbegrenzt	4
Afi.ai	Exchange, SharePoint, OneDrive, Teams	5	4.104 €	2	Ja	3	Unbegrenzt	4
Veeam Backup Flex	Exchange, SharePoint, OneDrive, Teams	5	3.597,84 €	3	Ja	3	Unbegrenzt	4

Tabelle 7: Nutzwertanalyse Teil 1

Backup-Lösung	Ver-schlüsselung	Gewichtung (5)	Autom. Backups	Gewichtung (5)	Wiederherstellungszeit	Gewichtung (2)	Bereitstellung	Gewichtung (3)
Veeam Self Host	Ja	5	Ja	5	Minuten	2	On-Premise	3
Synology	Ja	5	Ja	5	Minuten	2	On-Premise (Synology NAS)	1
CloudAlly	Ja	5	Ja	5	Minuten	2	Cloud	2
Afi.ai	Ja	5	Ja	5	Echzeit	2	Cloud	2
Veeam Backup Flex	Ja	5	Ja	5	Minuten	2	Cloud	2

Tabelle 6: Nutzwertanalyse Teil 2

A.2. Nutzwertanalyse

Backup-Lösung	Benutzerfreundlichkeit (Admin)	Gewichtung (3)	Benutzerfreundlichkeit End-User	Gewichtung (3)	Gesamtbewertung (38)
Veeam Self Host	Bekannt aus Backup&Repl.	3	Sehr Benutzerfreundlich	3	37
Synology	Sehr Benutzerfreundlich	3	Sehr Benutzerfreundlich	3	36
CloudAlly	Sehr benutzerfreundlich	3	Sehr Benutzerfreundlich	3	35
Afi.ai	Durch <u>SLA</u> Einstellungen etwas umständlich	2	Nicht so gut wie CloudAlly oder Veeam	2	32
Veeam Backup Flex	Benutzerfreundlich	3	Sehr Benutzerfreundlich	3	35

Tabelle 8: Nutzwertanalyse Teil 3

A.3. Gantt-Diagramm

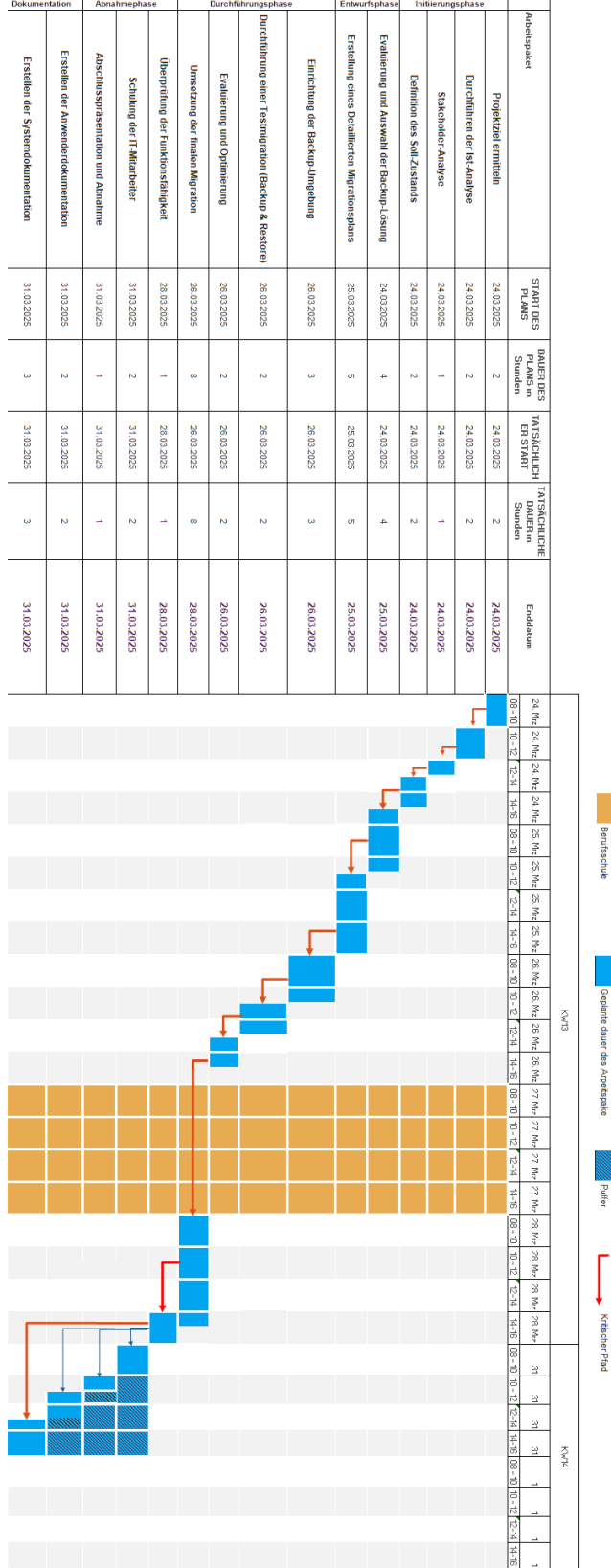


Abbildung 2: Gantt-Diagramm

A.4. Systemdokumentation

Ziel des Systems:

Sicherung und Wiederherstellung von Microsoft 365 Daten (Exchange Online, SharePoint Online, OneDrive for Business, Microsoft Teams) zur Erhöhung der Ausfallsicherheit, Wiederherstellbarkeit und Datenhoheit.

Systemart:

Selbst-gehostetes Backup-System mit täglicher Datensicherung auf lokalem Server.

Primäre Komponenten:

- Veeam Backup for Microsoft 365
- Veeam Restore Portal (Weboberfläche)
- Microsoft 365 Tenant
- Azure Enterprise Applications
- Backup-Speicher auf RAID 6

Systemkomponenten:

Komponente	Bezeichnung	Funktion
Backup Server	ASHSRVBACKUP02	Plattform für Veeam Backup und lokaler Speicherort für Backups
Backup-Software	Veeam Backup for Microsoft 365	Backup Verwaltung für M365-Daten
Azure Enterprise Applications	Modern Auth App & Auxiliary App	Zugriff auf M365 über Graph API und Exchange Online
Restore Portal	Web-GUI unter: https://recovery.ashampoo.com:4443	Web-Portal zur eigenständigen Wiederherstellung von Objekten
Repository	Lokaler Speicher (B:\Backup\VBO365)	Speicherort für alle gesicherten MS365-Daten

Tabelle 9: Systemkomponenten

Datenfluss & Schnittstellen:

Datenerfassung: Tägliche automatische Sicherung aller Microsoft 365 Daten über Veeam Backup for Microsoft 365

Verbindung zu Microsoft 365: Authentifizierung erfolgt über Azure Enterprise Applications mittels Zertifikats (OAuth 2.0). Der Zugriff erfolgt über Microsoft Graph API und EWS

Speicherung: Die Daten werden direkt auf dem Backup Server ASHSRVBACKUP02 im Repository gespeichert. Verwendet wird die Item-Level Retention mit einer Aufbewahrungsfrist von 3 Jahren

Zugriff & Restore: Admins und berechtigte Benutzer können über das Restore Portal (<https://recovery.ashampoo.com>) auf Objekte zugreifen und Wiederherstellungen anstoßen

Der Zugriff erfolgt per Microsoft Anmeldung (Modern Authentication)

Benutzte Ports:

Verbindung	Port	Protokoll	Richtung	Beschreibung
Veeam-Server → Microsoft Exchange Online	443	HTTPS	Ausgehend	Verbindung zu Exchange Online über EWS.
Veeam-Server → Microsoft SharePoint Online	443	HTTPS	Ausgehend	Verbindung zu SharePoint Online und OneDrive for Business.
Veeam-Server → Microsoft Teams	443	HTTPS	Ausgehend	Verbindung zu Microsoft Teams über Graph API.
Veeam-Server → Microsoft 365 (Graph API)	443	HTTPS	Ausgehend	Authentifizierung und Datenzugriff über Microsoft Graph API.
Veeam-Server → Entra ID	443	HTTPS	Ausgehend	Authentifizierung gegenüber Entra ID.
Veeam-Server → SMTP- Server	25 / 465 / 587	SMTP / SMTPS	Ausgehend	Versand von E-Mail-Benachrichtigungen.
Veeam-Server → Lizenz- und Update-Server	443	HTTPS	Ausgehend	Zugriff auf Veeam Auto-Update- und Lizenzserver.
Benutzer-PC → Restore Portal	4443 (Standard)	HTTPS	Eingehend auf Veeam- Server	Webzugriff auf das Restore-Portal für autorisierte Benutzer.
Veeam Explorer (Exchange, SharePoint, Teams)	9194	TCP	Eingehend auf Veeam- Server	Kommunikation mit Veeam Explorers für Wiederherstellungen.
Veeam Backup components → Veeam-Server	9191	TCP	Eingehend auf Veeam- Server	Kommunikation zwischen REST-API, PowerShell, Veeam.Archiver.Shell und Veeam-Server.
Veeam-Server → PostgreSQL- Datenbank	5432	TCP	Ausgehend	Verbindung zur Konfigurationsdatenbank (PostgreSQL).

Tabelle 10: Veeam Ports

(Veeam Software Group, 2025)

Netzwerktopologie:

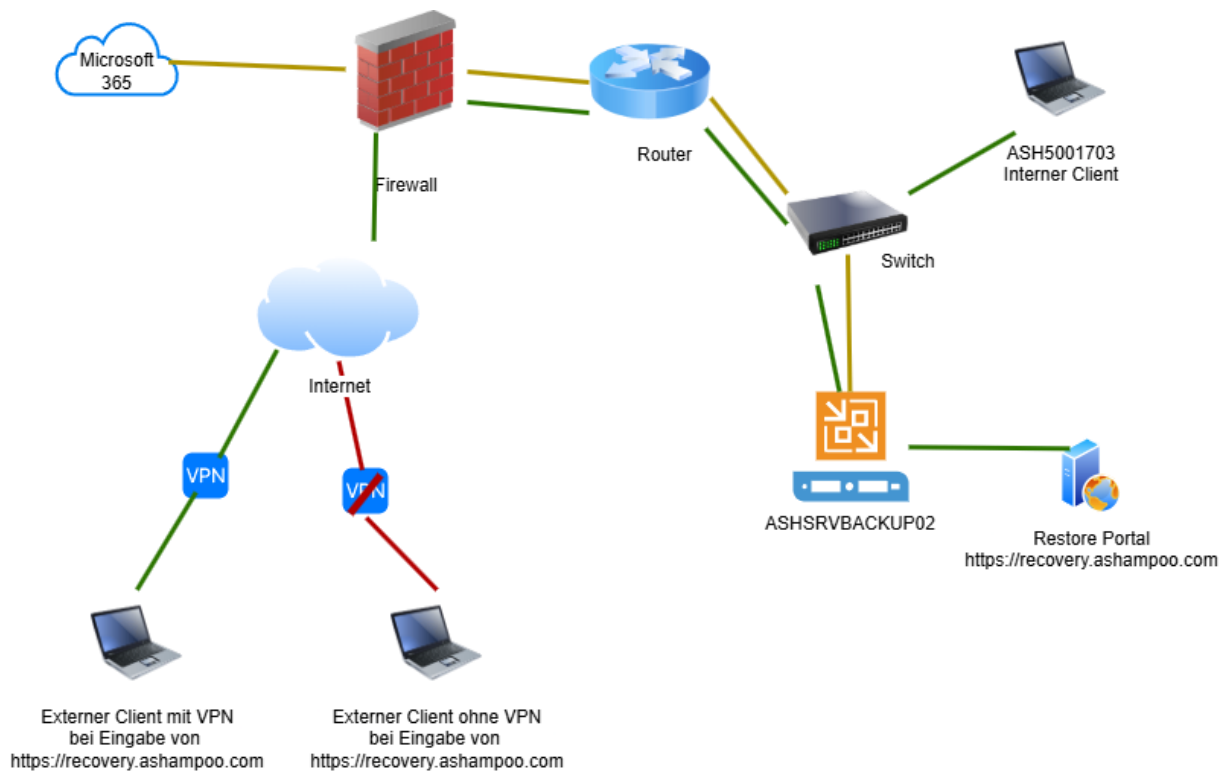


Abbildung 3: Netzwerktopologie

Im vorherigen Schaubild wird die grundlegende Netzwerk-Topologie dargestellt. Zu sehen ist die Verbindung des Backup-Servers zur Microsoft 365-Cloud (gelbe Linie) sowie der Zugriff auf das Restore-Portal durch verschiedene Clients.

Ein interner Client sowie ein externer Client mit aktiver VPN-Verbindung können über eine gesicherte Verbindung (grüne Linie) erfolgreich auf das Restore-Portal zugreifen. Ein weiterer externer Client ohne VPN-Verbindung versucht ebenfalls auf das Portal zuzugreifen, wird jedoch – wie durch die rote Linie dargestellt – nicht vom DNS weitergeleitet.

Rechte & Rollen:

Benutzerrolle	Berechtigungen
Administrator (IT)	Vollzugriff auf Backup-Jobs, Repository, Restore-Funktionen, Portal-Administration
Berechtigter Benutzer	Zugriff auf zugewiesene Restore-Scopes im Web-Portal

Tabelle 11: Rechte und Rollen

Backup Konfiguration:

Einstellung	Wert
Backup-Zeitplan	Täglich, 23 Uhr
Aufbewahrungsdauer	3 Jahre (Item-Level-Retention)
Repositories	B:\Backup\VBO365
Gesicherte Dienste	Exchange, OneDrive, SharePoint, Teams
Wiederherstellung	Granular, über Portal oder Konsole
Restore-Scopes	Benutzerbasiert definiert in Veeam. Wenn einzelne Nutzer in einer SharePoint Gruppe was wiederherstellen müssen, brauchen diese die Berechtigung für diese Gruppe.

Tabelle 12: Backup Konfiguration

Sicherheit & Datenschutz:

- Zertifikatbasierte Authentifizierung bei Azure
- SSL-Verschlüsselung des Restore-Portals
- Keine Datenübertragung in eine externe Cloud
- Zugriffsberechtigungen gesteuert nach Microsoft 365 Benutzern
- Manuelle Kontrolle über Restore Zugriffe und Restore-Scopes

Wartung & Monitoring:

- Überwachung: Bei Fehlern wird eine E-Mail-Benachrichtigung verschickt und bei Server Fehlern ist das Monitoring System Icinga2 zuständig
- Updates: Software- und Windows Updates manuell durch die IT
- Restore-Tests: Geplant in regelmäßigen Abständen und durchgeführt von der IT

Dokumentierte Wiederherstellungstests:

Testfall	Ergebnis
Wiederherstellung einer gelöschten Kunden-E-Mail	Erfolgreich – E-Mail wurde korrekt ins Postfach des Benutzers wiederhergestellt
Wiederherstellung einer versehentlich gelöschten OneDrive-Datei	Erfolgreich – Datei konnte im Originalordner wiederhergestellt werden
Wiederherstellung einer älteren Version eines SharePoint-Dokuments	Erfolgreich – Gewünschte ältere Version wurde aus dem Versionsverlauf wiederhergestellt
Restore einer gesamten Teams-Gruppe (nur Metadaten)	Erfolgreich – Metadaten der Teams-Gruppe konnten wiederhergestellt werden

Tabelle 13: Wiederherstellungstests

A.5. Anwenderdokumentation

Das Veeam Restore Portal ermöglicht es Daten aus Microsoft 365 eigenständig wiederherzustellen. Unterstützt werden Exchange Online, welches für eure E-Mails, Kalender und Kontakte zuständig ist, OneDrive, SharePoint und Microsoft Teams Gruppen.

Der Zugriff auf das Restore Portal erfolgt über eine verschlüsselte Weboberfläche und erfordert eine Authentifizierung via Microsoft 365. Um euch dort einzuloggen, benötigt Ihr also lediglich eure Ashampoo E-Mail-Adresse und euer Passwort.

Voraussetzungen:

- Ein aktives Microsoft 365 Benutzerkonto
- VPN-Zugang bei externem Zugriff
- Aktueller Webbrowser wie Chrome, Edge oder Firefox

Wenn du eine SharePoint-Seite oder Inhalte aus einer Teams-Gruppe wiederherstellen möchtest, muss dir die IT vorab die Berechtigung freigeben.

Bitte stelle dafür ein Ticket unter: [REDACTED]

Aufruf des Restore Portals

Intern (im Büro oder per LAN):

- Öffne die Adresse <https://recovery.ashampoo.com:4443>

Extern (z.B. Homeoffice):

- Verbindet euch mit dem VPN über Sophos Connect
- Öffne die Adresse <https://recovery.ashampoo.com:4443>

Ohne aktive VPN-Verbindung ist der Zugriff von außerhalb nicht möglich.

Anmeldung

1. Trage deine **Ashampoo E-Mail-Adresse** ein und klicke auf **Login**

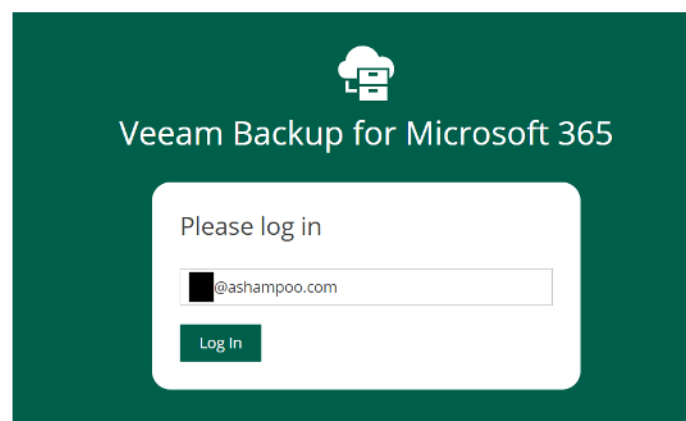


Abbildung 4: Restore Portal Login

2. Du wirst auf die Microsoft-Anmeldemaske weitergeleitet – gib dein Passwort ein

Abbildung 5: Login Microsoft

3. Nach erfolgreicher Anmeldung siehst du die Oberfläche des Restore Portals

Objekte wiederherstellen

1. **Restore Point auswählen** (also das Sicherungsdatum) z. B. 29.03., wenn die Datei an diesem Tag noch vorhanden war.

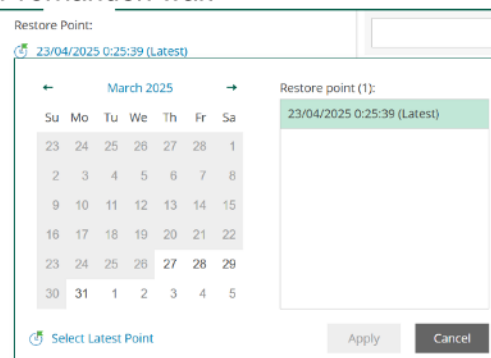


Abbildung 6: Auswahl des Restore Points

2. Auf „**Apply**“ klicken – jetzt werden die verschiedenen Ordner für E-Mail, E-Mail Archiv, OneDrive und SharePoint (Persönliche Site) angezeigt



Abbildung 7: Restore Ordner

- Um ein **Objekt wiederherzustellen**, wähle einfach **den gewünschten Ordner** aus und suche das fehlende Objekt

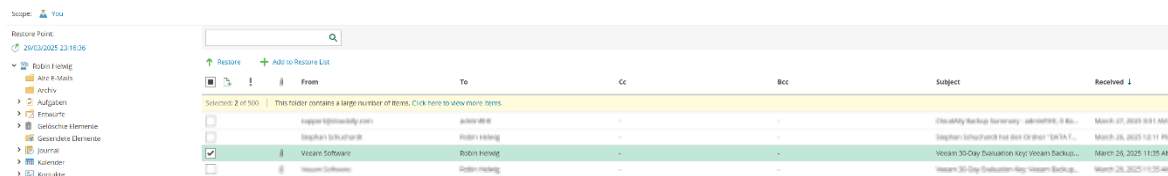


Abbildung 8: Objektauswahl Restore Portal

- Nachdem das Objekt ausgewählt wurde, kannst du es über „**Restore**“ wiederherstellen.
Falls Ihr **mehrere Objekte** direkt wiederherstellen möchtet, drückt auf die **Checkboxen** von den **verschiedenen Objekten** und startet dann die Wiederherstellung.
Falls du noch Objekte von OneDrive oder SharePoint wiederherstellen willst, drücke auf „**Add to restore List**“

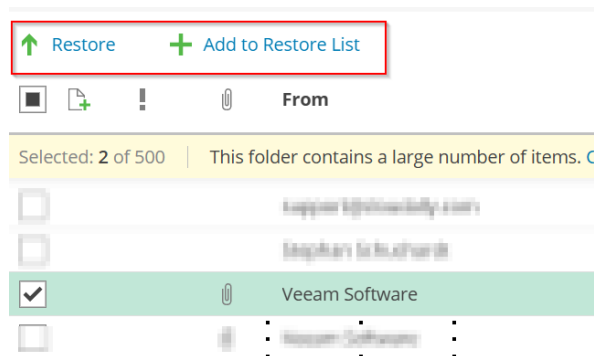


Abbildung 9: Restore und Restore List

- Wenn du auf „**Restore**“ gedrückt hast, wirst du auf die Restore Seite weitergeleitet. Dort werden dir die ausgewählten Objekte noch einmal angezeigt. Falsche Objekte können hier über den „**Remove**“ Knopf aus der Wiederherstellung entfernt werden. Wenn alles richtig ist, drückt Ihr einfach auf „**Next**“

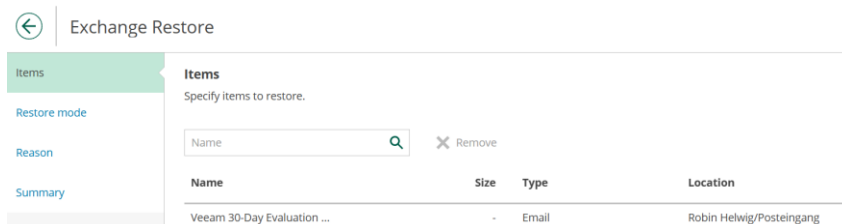


Abbildung 10: Exchange Restore Items

- Auf der **Restore mode Seite**, werdet Ihr gefragt, ob Ihr das Objekt im **Ursprünglichen Ort** wiederherstellen wollt, oder an einem **neuen Ort**. Wenn Ihr das Objekt in einen **neuen Ordner Wiederherstellen** wollt, müsst Ihr den

Ordnernamen dort angeben.

Restore mode
Specify whether you want to restore items to the original location or to another location

☐ Restore to the original location
Quickly initiate the restore of the selected items to their original location.

☒ Restore to a new location
Restore to the following folder:

Restore

[Advanced options...](#)

Abbildung 11: Restore mode

7. Unter „**Advanced Options**“ findest du noch weitere Optionen wie:
- Wiederherstellung von veränderten Objekten
 - Wiederherstellung von fehlenden Objekten
 - Markiere das Wiederhergestellte Objekt als ungelesen

Restore options
Specify restore options.

☒ Restore changed items

☒ Restore missing items

Flag restored items:

☒ Mark restored items as unread

Apply Cancel

Abbildung 12:
Wiederherstellungsoptionen

8. Auf der nächsten Seite gibst du einen **Grund** für deine Wiederherstellung ein, wie z.B. „Aus Versehen gelöschte E-Mail“

Exchange Restore

Reason
Specify the reason to perform the restore operation.

Restore reason:

Aus versehen gelöschte E-Mail

Abbildung 13: Wiederherstellungsgrund

9. Am **Ende** kommt noch eine **Zusammenfassung** und kann dann die Wiederherstellung starten

Items	
Items to restore:	Email: Veeam 30-Day Evaluation Key: Veeam Backup for Microsoft 365 (From: Veeam Software, To: Robin Helwig)
Restore summary	
Restore mode:	Restore to the original location
Restore changed items:	Yes
Restore missing items:	Yes
Mark restored items as unread:	Yes
Reason	
Reason	Aus versehen gelöschte E-Mail

Abbildung 14: Wiederherstellung Zusammenfassung

10. Anschließend wirst du zu „Restore Sessions“ weitergeleitet. Dieser Prozess dauert bei E-Mails meist nur ein paar Sekunden. Bei größeren Dateien wie bei Bildern, kann dies etwas länger dauern.

Explore

Restore Sessions

Restore List (2)

Period:

Last week

Stop

Session	Type	Status
Restore Exchange	Exchange	Success

Session Log:

Status:

Message

Restore session started

Item Veeam 30-Day Evaluation Key: Veeam Backup for Microsoft 365

Restore session completed

Abbildung 15: Restore Sessions

11. Danach ist das Wiederhergestellte Objekt entweder im originalen Ordner zu finden sein oder in dem festgelegten Ordner.

12. Die Wiederherstellung über die Restore List, läuft fast genau gleich ab. Hierzu wählst du einmal alle Objekte aus, die in der Restore List drin sind und drückst auf „**Restore**“.

Wenn Objekte von z.B. OneDrive und Exchange Online (E-Mail) vorhanden sind, fragt euch das System noch einmal was du zuerst wiederherstellen willst

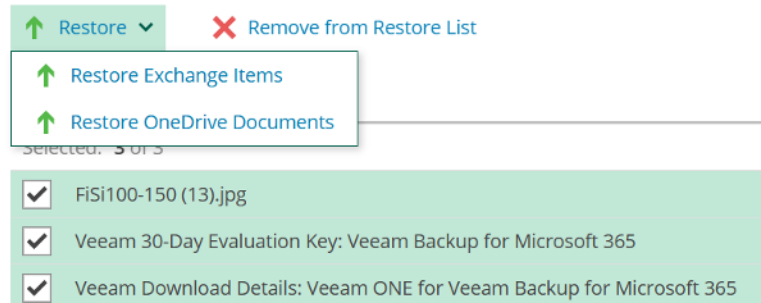


Abbildung 16: Wiederherstellung über Restore List

13. Falls du eine SharePoint Seite oder Dokumente von einer SharePoint Seite Wiederherstellen willst und du die benötigten Berechtigungen hast, wähle oben unter Explore „**Scope**“ aus.

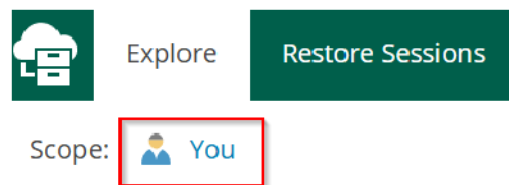


Abbildung 17: User Scope

14. Dort werden dir dann die zugewiesenen Objekte wie SharePoint Seiten, geteilte Postfächer oder Teams Gruppen angezeigt

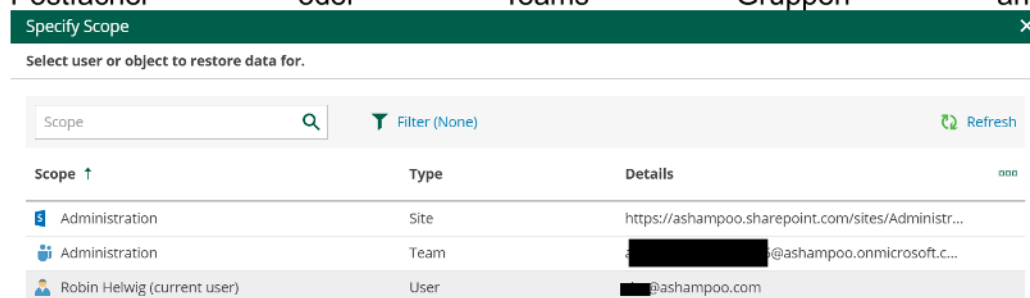


Abbildung 18: Zugewiesene restore scopes

15. Wenn du dann den gewünschten „**Scope**“ ausgewählt hast, läuft das Wiederherstellen genauso ab wie bei einer Persönlichen Wiederherstellung.

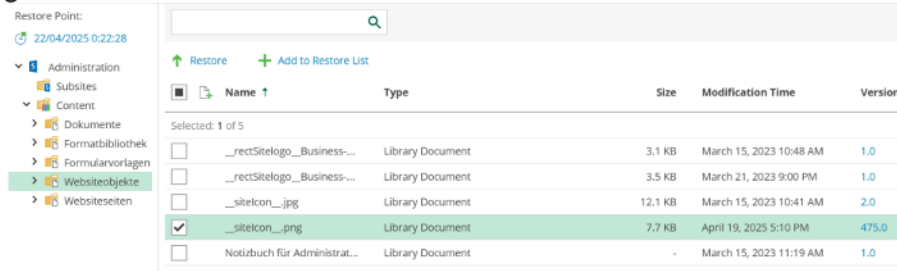


Abbildung 19: Wiederherstellung über Restore Scope

16. Was bei einer SharePoint Wiederherstellung noch wichtig sein kann, ist die Mitsicherung von **verschiedenen Versionen**. Drückt Ihr auf die **Version**, könnt Ihr den ganzen **Versionsverlauf** sehen und einzelne Versionen wiederherstellen.

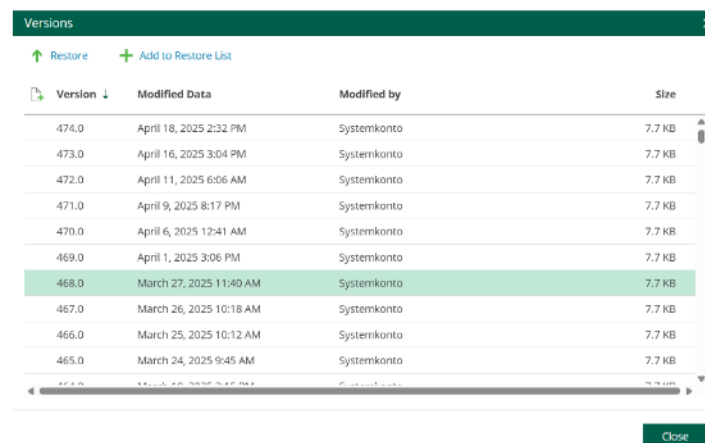


Abbildung 20: Wiederherstellung des Versionsverlaufs

Bei Fragen oder Problemen erstellt ein Support Ticket unter:



A.6. Größere Wiederherstellungen durch Administratoren

Administratoren können genauso wie die User über das „**Restore Portal**“ einzelne Objekte wiederherstellen. Wenn jedoch mehr wiederhergestellt werden muss, gibt es die Option ganze Postfächer, OneDrive Benutzer Ordner, SharePoint Seiten und Teams Gruppen wiederherzustellen.

Dazu muss man auf dem ASHSRVBACKUP02 die Software Veeam Backup for Microsoft 365 öffnen. Dort wählt man dann im Reiter „Explore“ aus und kann von dort dann Exchange Online, SharePoint, OneDrive oder Teams durchsuchen.

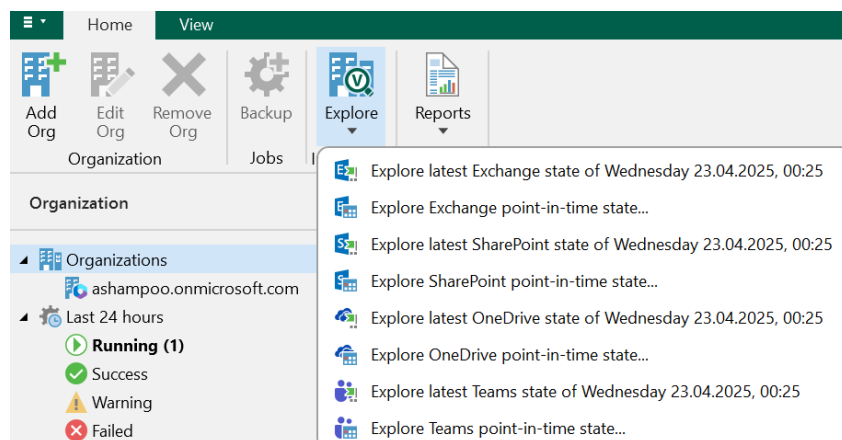


Abbildung 21: Admin Wiederherstellungsauswahl

Daraufhin öffnet sich der Veeam Explorer und man entweder das ganze Postfach für den Benutzer wiederherstellen oder an einem anderen Ort Wiederherstellen.

Man kann auch die Mailbox Exportieren oder mit dem aktuellen Stand vergleichen.

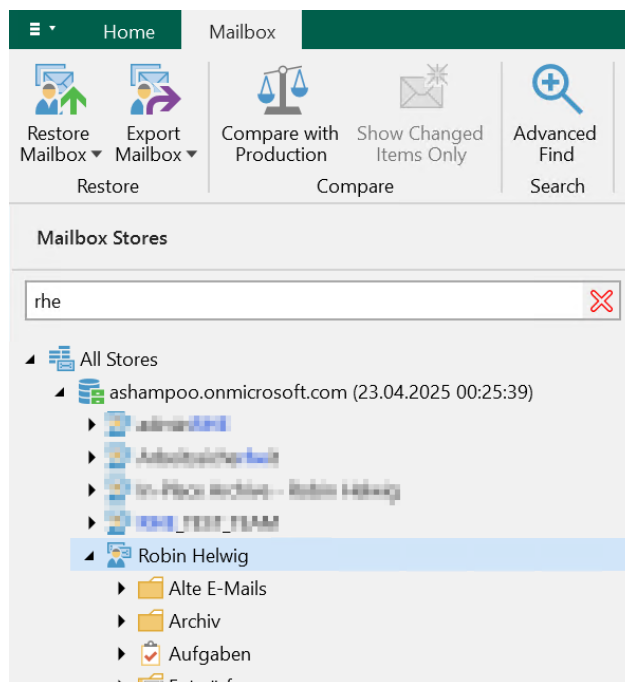


Abbildung 22: Admin Mailbox Wiederherstellung

In OneDrive kann man ebenfalls das gesamte OneDrive wiederherstellen, es an einen anderen Ort kopieren oder versenden.

Wenn man sich dazu entscheiden sollte, einen OneDrive Account wiederherzustellen, kriegt man die Option, die vorhandenen Dateien zu überschreiben oder zu behalten.

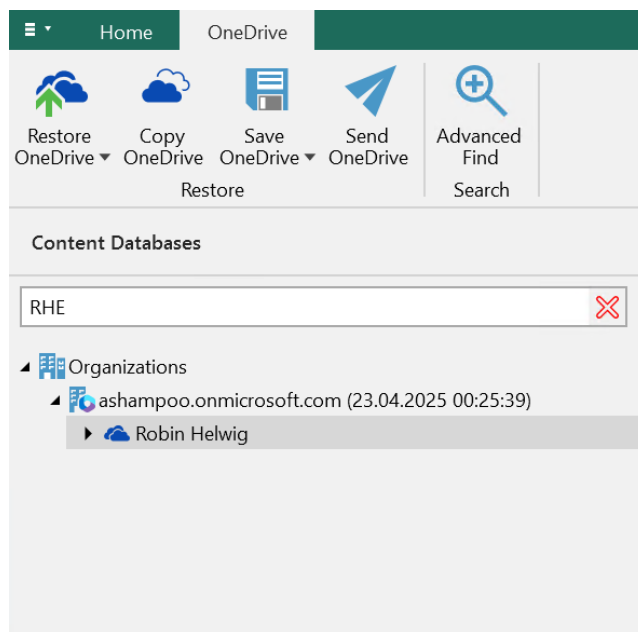


Abbildung 24: Admin OneDrive Wiederherstellung

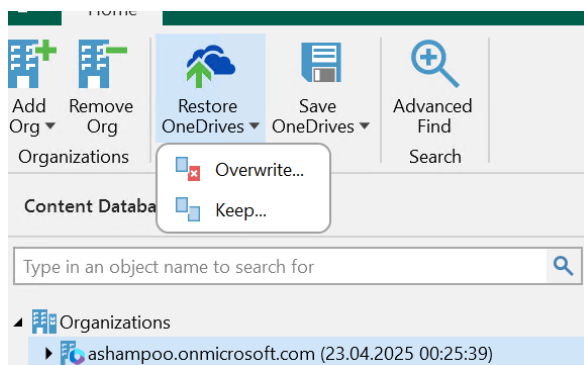


Abbildung 23: Admin OneDrive Wiederherstellungsoptionen