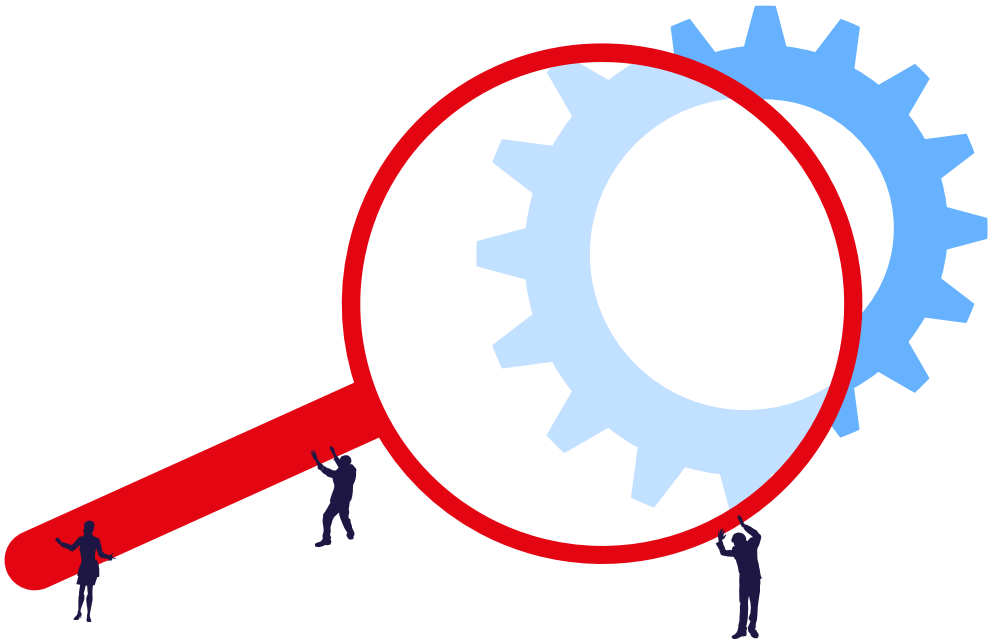
Digitale Verwaltung Schweiz
Administration numérique suisse
Amministrazione digitale Svizzera

Design Exchange in der Cloud

Studie im Auftrag der Arbeitsgruppe Cloud Governance und Workplace der Digitalen Verwaltung Schweiz



Januar 2024

Vorwort

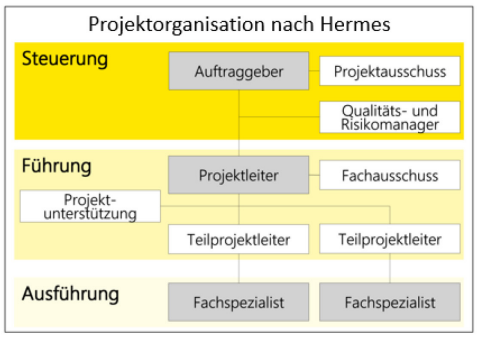
Liebe Leserinnen, liebe Leser

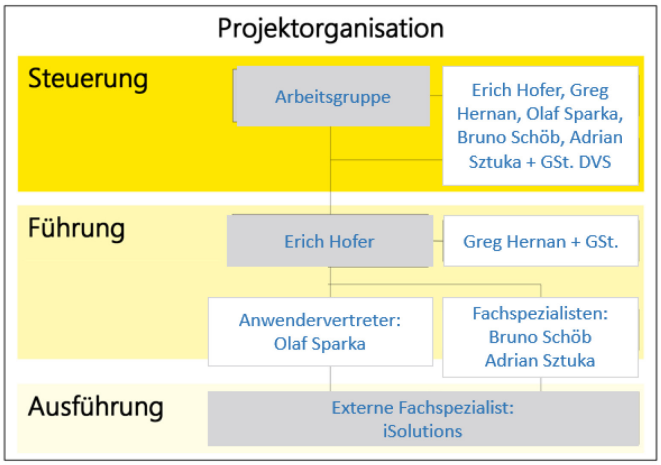
Die Arbeitsgruppen Cloud Governance und Workplace der DVS konnten im Jahr 2023 gemeinsam agieren. Der Grund dafür ist, dass es einige gemeinsame Themen gibt, die beide Arbeitsgruppen beschäftigen. Den Arbeitsgruppen der DVS wird ein minimales Projektbudget zur Verfügung gestellt. Damit können Studien, Konzepte oder andere kleine bis mittelgrosse Projekte initiiert werden. Diese Projekte können je nach Grösse in andere Initiativen des DVS (z.B. Ambition) eingebracht werden.

Die Diskussionen in den Arbeitsgruppen haben sich in den letzten zwei Jahren auf die Produkte von Microsoft in der Cloud (Online Services) konzentriert. Die Problematik der Nutzer, die mit Datenklassifizierungen und neuen Eigenverantwortlichkeiten bezüglich der Daten konfrontiert sind, sind nicht neu, bekommen aber mit Werkzeugen wie Exchange eine hohe Bedeutung, wenn dieses Produkt in der Cloud angeboten und integriert wird. Es handelt sich um eine globale E-Mail-Kommunikation, die alle Arten von Daten enthalten kann und im Zukunft in der Cloud zu finden ist.

Anfang 2023 waren sich die Arbeitsgruppen einig, dass Exchange in der Cloud eine der Hürden für die Implementierung der Online Services Produkte von Microsoft (M365, Teams) ist und starteten das Projekt: «Design Exchange in der Cloud». Nach kurzer Suche nach externen Spezialisten konnte der Auftrag an iSolutions vergeben werden.

Projektorganigramm





Ergebnis

Die Projektgruppe kam zu dem Schluss, dass die Hauptziele zwar grösstenteils genannt wurden, aber nicht durch eine Studie gelöst werden können. Das Dokument listet die Schritte auf, die eine Organisation, die Exchange in die Cloud integrieren will, unbedingt angehen und lösen muss. Die Arbeitsgruppe Cloud Governance und Workplace (Zusammenlegung in 2024) hat aus dieser Erfahrung 3-4 weitere Themen herauskristallisiert, die wir in Form von weiteren Projekten verfolgen und lösen bzw. Lösungen so nahe wie möglich kommen wollen. Für weitere Informationen wenden Sie sich bitte an Erich Hofer oder Greg Hernan.

Design Exchange in der Cloud – Exkurs

Cloud Einführung/Migration in der öffentlichen Verwaltung

Management Summary für Entscheidungsträger

Autor: Erich Hofer, DVS Arbeitsgruppe Cloud Governance und Workplace
Stand 15.02.2023 V1

Grundsätzlich ist die Einführung bzw. Migration in die Cloud wie z.B. Exchange 365 (Microsoft Cloud) ein Organisationsprojekt. Damit dieses Projekt erfolgreich durchgeführt werden kann, sind die nachfolgend aufgeführten Themen in der betroffenen Organisation sorgfältig abzuklären. Ebenso sind die notwendigen Entscheidungen auf Führungsebene zu treffen und die daraus resultierenden Konsequenzen und Maßnahmen in der Organisation im Vorfeld umzusetzen.

Ebenso ist es leider nicht möglich, einen allgemeingültigen Standard zu definieren, der sehr oft von DVS-Mitgliedern gefordert wird. Um diesem Umstand Rechnung tragen zu können (DVS-Standard), müssten zuerst die gesetzlichen Grundlagen und Rahmenbedingungen der öffentlichen Verwaltungen (Bund, Kantone, Städte, Gemeinden etc.) konsolidiert und vereinheitlicht werden. Ein solch massiver Eingriff in die Souveränität der schweizerischen Rechtsstaatslandschaft ist derzeit nicht realisierbar.

Damit diese Überlegungen, Abklärungen und Entscheide möglichst erfolgreich umgesetzt werden können, empfehlen wir ein zweistufiges Vorgehen in jeder übergeordneten Organisationseinheit (z.B. Kanton):

Stufe 1 im Sinne einer grundsätzlichen Einführung bzw. Migration in die Cloud (Grundversorgung)

Stufe 2 für eine Abklärung pro Organisationseinheit (Amt, Abteilung etc.) je nach Rahmenbedingungen bzw. Ergebnis der Klassifikation der vorhandenen Daten und deren Datenschutzrelevanz in der betroffenen Organisationseinheit.

Stufe 1:

Folgende Themen sollten vor einer möglichen Cloud-Einführung/Migration geklärt werden:

1. Rechtliche Rahmenbedingungen

Die rechtlichen Rahmenbedingungen (gesetzliche Grundlagen) sind zu prüfen, ob ein Outsourcing der Datenverarbeitung in der Organisation überhaupt möglich ist. Insbesondere wenn Daten ausserhalb des Staatsgebietes (Schweiz) gespeichert oder verarbeitet werden. Es ist sicherzustellen, dass entsprechende vertragliche Vereinbarungen getroffen werden, um die Einhaltung der gesetzlichen Anforderungen zu gewährleisten.

2. Datenschutz und Datensicherheit

In der öffentlichen Verwaltung werden häufig personenbezogene Daten verarbeitet, die eines besonderen Schutzes bedürfen. Beim Outsourcing in eine Cloud-Lösung besteht die Gefahr, dass sensible Daten ohne angemessene Schutz- und Sicherheitsvorkehrungen übertragen und gespeichert werden. Hier sind die Vorgaben der betroffenen Organisationseinheit zu prüfen und mittels einer Risikobewertung entsprechend abzuwägen, ob und wie eine Auslagerung mit den möglichen Maßnahmen des Cloud-Betreibers überhaupt möglich ist.

3. Vertrauen in den Anbieter (z.B. Microsoft etc.)

Grundsätzlich muss ein Grundvertrauen in den Cloud Betreiber als verlässlichen Lieferanten und Vertragspartner bestehen. (Kunden-Lieferanten-Beziehung). Dies ist eine wichtige Voraussetzung für eine erfolgreiche Cloud Migration im Sinne eines umfangreichen Projektes.

4. Abhängigkeit von Cloud-Anbietern (Dritten)

Beim Outsourcing in die Cloud ist die öffentliche Verwaltung von einem externen Anbieter abhängig. Störungen, Ausfallzeiten oder Vertragsänderungen seitens des Anbieters können sich auf den Betrieb und die Leistungserbringung der öffentlichen Verwaltung auswirken.

5. Vendor Lock-in

Beim Wechsel des Cloud-Anbieters besteht das Risiko eines Vendor-Lock-ins, bei dem die öffentliche Verwaltung Schwierigkeiten hat, ihre Daten und Dienste in eine andere Umgebung oder Plattform zu migrieren. Dies kann die Flexibilität und Wettbewerbsfähigkeit der öffentlichen Verwaltung beeinträchtigen. Im Rahmen des öffentlichen Beschaffungswesens (WTO z.B. Vertragslaufzeiten, keine Übervorteilung von Lieferanten etc.) kann dies zu neuen Herausforderungen führen.

6. Wirtschaftlichkeit und Kostenkontrolle

Obwohl Cloud-Lösungen oft kosteneffizient sind, können unerwartete Kosten entstehen. Überschreitet die Nutzung oder Speicherung von Daten die festgelegten Budgets, kann dies zu finanziellen Herausforderungen führen. Auch Erweiterungen, die der Cloud-Betreiber einführt und die Kosten entsprechend anpasst, können die Wirtschaftlichkeit der Lösung in Frage stellen. Ebenso werden Investitionskosten (CapEx) zu Lasten steigender Betriebskosten (OpEx) im bestehenden IT-Budget eliminiert.

7. Ausbildung der betroffenen Mitarbeiterinnen und Mitarbeiter

Für den richtigen Umgang in der Cloud sind die Mitarbeitenden entsprechend zu schulen (Datenschutz, zeitlich flexible Updates durch den Betreiber, neue Funktionen und deren mögliche Abhängigkeiten zu bestehenden Fachlösungen). Allfällige Prozessanpassungen für eine effiziente Cloud-Nutzung werden für die Mitarbeitenden unumgänglich sein. Auch diese werden vom Cloud-Betreiber in einem bestimmten zeitlichen Rahmen vorgegeben.

8. Verlust von Know-how

Durch die Auslagerung bestimmter IT-Aufgaben kann internes Know-how und Fachwissen verloren gehen. Dies kann dazu führen, dass das Unternehmen in Zukunft vollständig auf externe Unterstützung angewiesen ist.

Stufe 2:

Auf dieser Stufe (z.B. Amt, Abteilung etc.) sind die Details, insbesondere der Datenschutz, eines allfälligen Cloud-Einsatzes zu klären. Dies auf der bestehenden Basis der Datenklassifizierung gemäss den Governance-Vorgaben der Organisation (z.B. kantonaler Datenschutz). Der Verantwortliche der Organisationseinheit entscheidet und übernimmt die Verantwortung für einen allfälligen Cloud-Einsatz (er ist auch für seine Daten und deren korrekte Klassifizierung verantwortlich). Dieses Vorgehen kann durch ein risikobasiertes Verfahren unterstützt werden. Ebenso tendiert dieses Vorgehen und dessen Ergebnis in den übergeordneten Organisationen zu sogenannten Hybridmodellen (OnPremise und Cloud Einsatz). Ob dieses Modell langfristig wirtschaftlich tragbar ist, sollte im Vorfeld geklärt werden.

Hier empfiehlt sich eine neutrale Beratung und Unterstützung zur Klärung der aktuellen Datenklassifizierung.

Mit dieser Vorgehensweise wird zumindest ein Weg aufgezeigt, um die aktuelle Situation und ein mögliches Vorgehen darzustellen. Selbstverständlich sind die einzelnen Schritte umfangreicher, als dies in einem „Management Summary“ möglich ist. Ebenso wurde diese Empfehlung nach bestem Wissen und Stand der Erfahrungen erstellt. Dieses Dokument muss in regelmäßigen Abständen von der Arbeitsgruppe überprüft und gegebenenfalls ergänzt werden. Die aktuelle Marktsituation der Cloud-Anbieter ist einem extrem starken Wandel und damit kurzen Lebenszyklen unterworfen.

Als Referenz und Beispiel für mögliche Vorgehensweisen:
- Kanton Zürich RRB
- Kanton Bern Entscheid M365 RR

isolutions

Blueprint: Design für Exchange in der Cloud

Digitale Verwaltung Schweiz DVS

Angaben zum Dokument

Ihre Ansprechpersonen:

Andres Bohren
Senior Microsoft 365 Architekt

D +41 31 560 89 85
M +41 79 693 71 48
Andres.bohren@isolutions.ch

Lukas Koslowski
Senior Security Consultant

D +41 31 560 89 47
M +41 79 561 80 56
Lukas.koslowski@isolutions.ch

Kunde	**Digitale Verwaltung Schweiz DVS**
Projekt	**Blueprint: Design für Exchange in der Cloud**
Version	**1.0**
Ausgabe vom	**20.12.2023**
Status	**Intern**
Verteiler	**Greg Hernan - Geschäftsstelle Digitale Verwaltung Schweiz (DVS)**

Hinweis: Zur besseren Lesbarkeit wird in diesem Dokument auf geschlechtsspezifische Formulierungen verzichtet. Wo personenbezogene Begriffe nur in der männlichen Form verwendet werden, beziehen sie sich auf Männer und Frauen in gleicher Weise.

isolutions

Inhaltsverzeichnis

Abbildungsverzeichnis

Abkürzungen und Begriffe

Abkürzung	Bedeutung	Erklärung
EXO	Exchange Online	Cloudbasierter Dienst von Microsoft
Azure AD	Azure Active Directory	Active Directory in Azure
PIM	Priviledged Identity Management	Lösung für Vergabe temporärer Adminrechte
IAM	Identity und Access Management	Lösung für die Vergabe von Zugriffsrechten
M365	Microsoft 365	Cloud Service von Microsoft
SaaS	Software as a Service	Bezugsvariante von Cloud Services

Änderungskontrolle

Datum	Person	Änderung	Version

1 Management Summary

Mit der Übersichtsstudie «Blueprint: Design für Exchange in der Cloud» soll den Entscheidungsträgern der öffentlichen Verwaltung aus dem Bereich Informatik die Integrationsperspektiven von Exchange in der Cloud, auf Basis Microsoft 365, aufgezeigt werden. Dabei sollen die wesentlichen Rahmenbedingungen sowie der Handlungsbedarf für eine nachhaltige, interoperable, möglichst konvergente, sichere und datenschutzkonforme Lösung für die öffentliche Verwaltung aufgezeigt werden. Der Fokus liegt dabei weniger auf der Anbindung, sondern eher wie mit den Exchange und Outlook Funktionen im Kontext einer kantonalen Verwaltung umgegangen werden soll.

Unsere Übersichtsstudie bietet einen effektiven Fahrplan mit den relevanten Aspekten für die Vorbereitungen, die Migration und Verwaltung von Microsoft Exchange in die Cloud. Dieses Vorgehen ist entscheidend für Unternehmen, die ihre Kommunikation und Zusammenarbeit optimieren und die Vorteile der Cloud-Technologie voll ausschöpfen möchten.

Das Zielpublikum sind IT-Verantwortliche, IT-Architekten und Sicherheitsverantwortliche.

Die Cloud bietet Organisationen die Möglichkeit, Ressourcen zu optimieren, Kosten zu senken und die Verfügbarkeit zu erhöhen. Unser Blueprint unterstützt Sie dabei, diese Vorteile bestmöglich zu nutzen und Ihre E-Mail- und Zusammenarbeitsplattform in die moderne Ära der Cloud-Technologie zu führen.

Kurz gesagt: Unser Blueprint für "Exchange in der Cloud" ist der Schlüssel zur Optimierung Ihrer Kommunikation und Zusammenarbeit in einer sicheren, effizienten und skalierbaren Cloud-Umgebung. Mit diesem klaren Fahrplan sind Sie bestens gerüstet, um die Chancen der digitalen Zukunft zu nutzen.

Die Services werden seitens Microsofts stetig weiterentwickelt. Daher können Unterschiede in den funktionalen Möglichkeiten oder geänderte Begrifflichkeiten im Zeitverlauf auftreten.

2 Ausgangslage

Die DVS koordiniert Arbeitsgruppen, in denen Fachthemen adressiert werden. Die Arbeitsgruppen «Workplace und Cloud Governance» suchen mit dieser Ausschreibung weitere externe Unterstützung zum Thema Cloud Governance.

2.1 Thematik der Studie

2.1.1 Ausgangslage Exchange on premise

Derzeit wird Exchange noch im eigenen Rechenzentrum betrieben. Das bedeutet, dass alle internen Mails und auch die Mails auf der gleichen Exchange-Infrastruktur in einer lokalen Datenbank gespeichert werden. Sie müssen nur dann zusätzlich geschützt werden, wenn sie an Dritte versendet werden. Das heisst, derzeit werden interne Mails nicht verschlüsselt, beim Versand werden vertrauliche oder geheime Mails mit Verschlüsselungsverfahren (z.B. SEPPMail) an die entsprechenden Empfänger versendet.

2.1.2 Exchange in der Cloud

Wird Exchange zukünftig in der Cloud oder hybrid betrieben, befinden sich einige Postfächer auf einem Exchange Server in der Cloud. Diese Postfächer müssen wie on premise geschützt werden, sowohl gegen Angreifer und Missbrauch, aber unter Umständen auch gegen Zugriffe von Microsoft im Rahmen des US CLOUD Act oder generell eines Lawful Access. (Betreiber ist eine externe Instanz - US-Firma - die amerikanischem Recht unterliegt).

2.1.3 DVS-Gefäss für den Wissensaustausch

Die DVS-Arbeitsgruppen Workplace und Cloud Governance unterstützen die öffentlichen Verwaltungen der Schweiz bei der Integration ihrer Systeme in die Cloud-Infrastruktur. Unter der Leitung der Arbeitsgruppen Workplace und Cloud Governance wird eine Übersichtsstudie durchgeführt, um die Frage zu beantworten: Wie sieht die Cloud Governance beim Einsatz des Produktes Exchange Online (Teil von M365) in der öffentlichen Verwaltung aus? Die beiden Arbeitsgruppen organisieren eine Veranstaltung am 31.08.2023. Dort wird das Thema je nach Fortschritt der Studien den Teilnehmern vorgestellt.

2.1.4 Abgrenzung

Die Studie fokussiert auf den in der Zielsetzung dargelegten Aspekte bezüglich der Nutzung von Microsoft Exchange Online und den definierten Use Cases, welche seitens Auftraggeber definiert wurden. Bei wichtigen Abhängigkeiten wurden punktuell angrenzende Themen angeschnitten, um diese visibel, im Sinne von Hinweisen, zu beleuchten.

Aufgrund unterschiedlicher kantonaler Voraussetzungen (z.B. Datenschutzgesetze, Klassifizierungen) wurden diese generisch betrachtet.

Microsoft entwickelt ihre Services stetig weiter, weshalb Namensgebungen und Funktionsumfänge sich ändern können.

3 Zielsetzungen

Im Rahmen dieser Studie sollen definierte Use Cases, wie auch mögliche Ziellösungen geprüft und detailliert beschrieben werden. Die Adressaten der Studie sind die Verantwortlichen der öffentlichen Verwaltungen für die Integration von Cloud-Produkten, insbesondere M365. Die Studie verfolgt folgenden Ziele:

- Ein Best Practice Vorschlag ist zu entwerfen, der beschreibt, wie der Exchange hybrid oder vollständig möglichst sicher in der MS Cloud betrieben werden kann. Best Practices sollen im Umgang mit unterschiedlich klassifizierten Informationen (öffentlich, intern, vertraulich, geheim) geschildert werden.
- Der Vorschlag soll Lösungen für die typischen Use Cases aufzeigen (Kapitel 6 und 7)
- Dokumente und Informationen sollen datenschutzkonform (gemäss aktuellem Datenschutzgesetz) behandelt werden. Es soll ein gesetzeskonformer Schutz erreicht werden, aber die Benutzerfreundlichkeit (wie wir sie heute von MS-Produkten kennen) soll soweit möglich nicht beeinträchtigt werden (z.B. durch gewisse Verschlüsselungen Kapitel 5.4.1.4).
- Automatisierte Prozesse sind zu bevorzugen, um Schutzlücken durch Vergessen oder Fehlbedienung zu vermeiden
- Wie sehen die obigen Szenarien aus, bei Zugriff per
  - Outlook
  - Outlook on the web
  - Mobilen Geräten (Smartphones / Tablets)

Zusätzlich sollen die folgenden weiteren Resultate bei Abschluss der Studie vorliegen:

- Wir wissen, was mit der Integration von Exchange in der Cloud auf uns zukommt und wie wir eigene und fremde Dienste integrieren können (E-Mail, Kalender, Kontakte, Aufgaben, Ordner, Notizen, Verknüpfungen, Online Status etc. ...).
- Es besteht Klarheit, wie wir auf ein für eigene Organisation standardisiertes Design (Blueprint) der Integration von Exchange in der Cloud hinarbeiten können.
- Wir kennen die Datenschutz-, Sicherheits- und Verfügbarkeits-Aspekte, sowie Restrisiken der Nutzung eines Exchange in der Cloud resp. die zu umsetzenden Massnahmen im Microsoft Umfeld.
- Wir verfügen über Lösungsansätze, was wir im Falle eines längeren Ausfalls des Exchange Servers in der Cloud machen können

4 Kritische Erfolgsfaktoren

Die kritischen Erfolgsfaktoren für eine allfällige Exchange Hybrid oder Exchange Online Migration sind vielfältig und lassen sich in folgende Bereiche bündeln:

Schaffung von Security Grundlagen

Microsoft Exchange Online kann aufgrund der starken Interaktion und Integration mit anderen Produkten der Microsoft 365 Suite, wie auch dem Azure Active Directory nicht als gesondertes Produkt angeschaut werden. Für die Prüfung aller Voraussetzungen und Schaffung der Grundlagen sollte Exchange Online als integraler Bestandteil der M365 Plattform inklusive dem zugrundeliegenden Tenant angeschaut werden. Dies bedeutet Exchange Online ist für gewisse Anwendungsfälle eine Voraussetzung, ein Beispiel hierfür sind gewisse Funktionalitäten in Microsoft Teams. Sprich sollte ein Leistungsbezüger geplant haben gewisse Anwendungsfälle mittels Microsoft Teams zu verbessern ist eine Exchange Online Migration oder eine hybride Nutzung allenfalls eine Voraussetzung.

Die Schaffung von Security Grundlagen sollte ebenfalls gesamtheitlich für Microsoft 365 angegangen werden, beispielsweise soll für alle M365 Services soweit möglich und zweckmässig, einheitlich definiert werden, welche Umstände für einen Zugriff eines Users erfüllt sein müssen.

Sollten gewisse Datensätze aufgrund ihrer Sensitivität nicht nach M365 migriert werden können, müssen die Auswirkungen im Detail geprüft werden. Beispielsweise ob sich entsprechend der geplante Anwendungsfall aufgrund der Einschränkung noch realisieren lässt.

Schaffung der Voraussetzungen für eine Exchange Hybrid / Online-Migration

Exchange Online ist oftmals einer der ersten M365 Workloads welche für eine Cloud Migration in Frage kommen. Im Rahmen dieser Migration müssen gewisse Vorarbeiten für einen gesamtheitlichen Rollout adressiert werden. Dies bedeutet unter anderem die Schaffung der technischen Voraussetzungen für einen erfolgreichen Zugriff auf M365 Ressourcen aus dem Unternehmensnetzwerk, wie aber auch von mobilen Geräten. Zusätzlich gilt es im Rahmen der entsprechenden Phasen zu prüfen ob alle Voraussetzungen im Bereich Identitäten erfüllt sind. Weitere Voraussetzungen sind im Bereich der organisatorischen Prozesse hinsichtlich BCM, oder Leistungserbringung zu klären.

Auswirkungen auf die IT-Architektur eines Leistungsbezügers

Eine M365 Einführung hat typischerweise wesentlichen Einfluss auf die IT-Architektur eines Leistungsbezügers. Eine M365 Einführung hat Einfluss auf die Elemente Netzwerk, IT-Sicherheit, Workplaces und Application Integration. Gilt es doch entsprechende Grundsatzentscheide wie Netzwerkanbindung von M365, Backup, etc zu definieren. Weiter

müssen Geschäftsapplikationen, welche heute mit Exchange on premises interagieren zukünftig in der Lage sein dies ebenfalls mit Exchange Online zu können.

Auswirkungen auf die Betriebsprozesse eines Leistungsbezügers.

Die Einführung von Microsoft 365 hat ebenfalls Auswirkungen auf die IT-Betriebsprozesse einer Organisation. Die grösste Änderung hierbei sind die Auswirkungen des sogenannten Evergreen Prozesses. Hierbei gilt es zu definieren wie mit Änderungen, welche durch Microsoft im Rahmen der Plattformentwicklung angestossen werden, umgegangen wird. Die Kadenz dieser Änderungen ist sehr hoch und es gilt entsprechend circa 50 -100 Changes pro Monat auf entsprechende Auswirkungen zu prüfen. Zusätzlich sind auch Elemente im Bereich Self Service Request Management neu zu definieren. Zusammenfassend kann folgendes Fazit gezogen werden: Um einen stabilen Betrieb von Microsoft 365 gewährleisten zu können sind die relevanten IT-Prozesse detailliert zu analysieren und gegebenenfalls anzupassen. Dies kann im Extremfall auch zu einem erhöhten Ressourcenbedarf im späteren Betrieb führen, falls Testing, Schulung von Helpdesk und Kommunikation an die Endbenutzer berücksichtigt wird. Diese Herausforderungen müssen bereits mit Einsatz von Exchange Online, als geschäftskritische Lösung mit komplexen Abhängigkeiten berücksichtigt werden.

5 Sicherheit

Dieses Kapitel beschreibt die Sicherheitsaspekte, welche bei der Nutzung von Cloud Services bewertet werden müssen. Dabei gehen wird zunächst auf das Shared Responsibility Model ein und zeigen auf, wie sich die Verantwortlichkeiten zwischen Cloud-Provider und Cloud-Kunde je nach Service Model unterscheiden.

Im Anschluss geht diese Studie auf die Risiken der Informationssicherheit und Datenschutz ein, welche mit adäquaten Schutzmassahmen adressiert werden müssen.

Zuletzt werden die Aspekte des Business Continuity Managements im Kontext Cloud beleuchtet und die Notwendigkeit einer Exitstrategie erläutert.

5.1 Informationssicherheit in der Cloud

5.1.1 Shared Responsibility Model

Die Nutzung von Cloud Services führt immer zu einer geteilten Verantwortung in Bezug auf Sicherheit. Die Aufteilung hängt dabei vom gewählten Service Modell ab. Microsoft ist grundsätzlich für den Schutz der Cloud-Infrastruktur verantwortlich. Microsoft Exchange Online wird als Software-as-a-Service (SaaS) bereitgestellt. Das Shared Responsibility Model zeigt die Aufteilung zwischen Kunden und Microsoft in einem SaaS-Szenario auf.

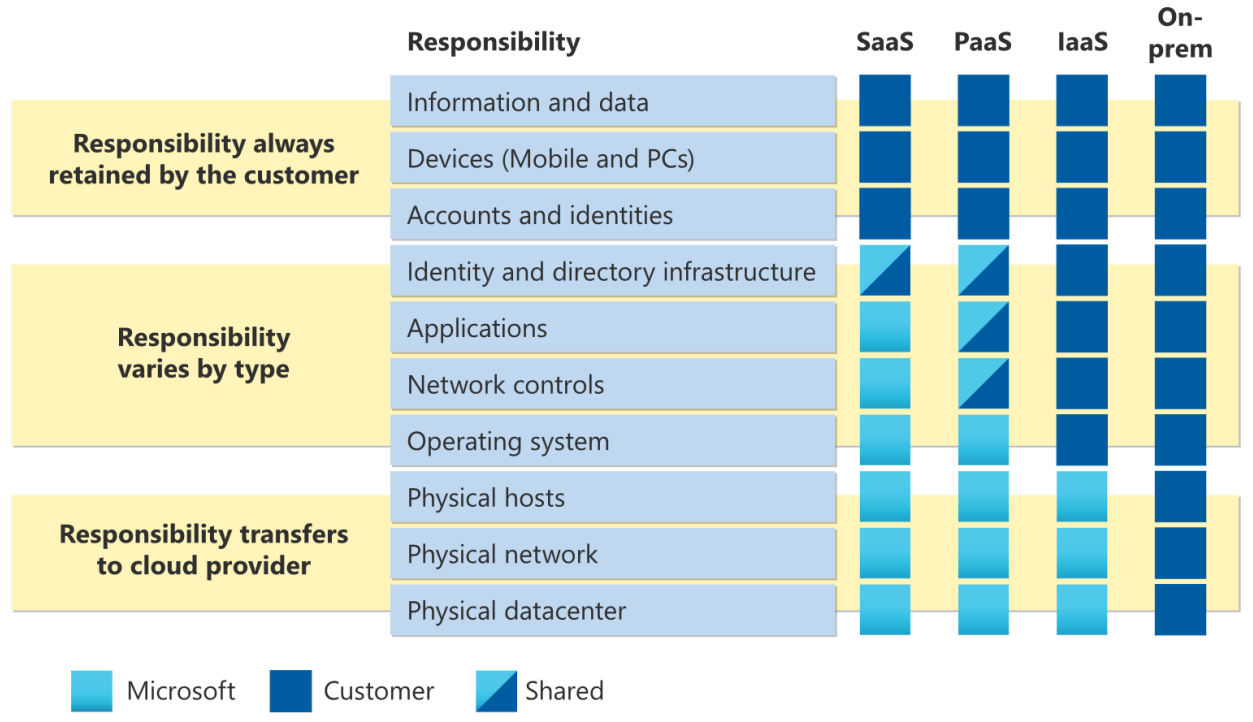


Abbildung 1 - Shared Responsiblity Model

Quelle: Shared responsibility in the cloud - Microsoft Azure | Microsoft Learn

Es zeigt sich, dass im SaaS-Modell der Grossteil der Verantwortung für Sicherheitsmassnahmen bei Microsoft liegt. Gleichwohl hat der Cloud-Kunde die

Verantwortung die Sicherheit der Identities, Devices und Daten sicher zu stellen[1]. Die Gesamtverantwortung für die Daten obliegt aber jederzeit beim Cloud-Kunden. Darüber hinaus muss der Cloud-Kunde ebenfalls überprüfen, ob die vertraglich festgelegten Sicherheitsmassnahmen (Controls) seitens Microsofts eingehalten werden. Um die ergriffenen Massnahmen und deren Einhaltung transparent offen zu legen, ist die Microsoft Cloudumgebung mehrfach zertifiziert. Dabei werden global anerkannte Zertifizierung (ISO 27001, SOC, CIS etc.) und auch regionalspezifische Standards (BSI C5, GDPR, IT-Grundschutz, ENISA etc.) erfüllt. Die Reports müssen kundenseitig geprüft und etwaige Abweichungen bewertet und Massnahmen daraus abgeleitet werden.

Die Zertifizierungen inkl. Auditberichte können kundenseitig im Microsoft Trust Center jederzeit eingesehen werden (servicetrust.microsoft.com).

5.1.2 Sicherheit in der Cloud

Bislang wurden Netzwerke und die darin enthaltenen Informationen durch Perimeter-basierte Schutzmassnahmen geschützt. Vereinfacht gesagt, galt alles innerhalb des internen Netzwerkes einer Organisation als vertrauenswürdig. Umgekehrt wurde alles ausserhalb des eigenen Netzwerkes als nicht vertrauenswürdig eingestuft.

Aus diesem Grund wurden Sicherheitsmassnahmen (Firewalls, IDS, IPS und andere Sicherheitskontrollen) entwickelt, um die Verbindungen zum internen Netzwerk zu überwachen und zu schützen. Der Zugang zum internen Netz basiert in der Regel auf einer vertrauenswürdigen Verbindung und einem legitimen Benutzer. Gelingt es einem Angreifer, die Sicherheitsmassnahmen am Perimeter zu überwinden, kann er sich innerhalb des internen Netzwerks frei bewegen.[2]

Mit der Entwicklung neuer Technologien und Cloud Service Modelle ändert sich die Sicht auf die Sicherheit. Die Nutzung vieler verschiedener Cloud-Dienste macht es immer schwieriger, eine Verteidigungslinie zwischen internen und externen Netzwerken durchzusetzen und somit das interne Netzwerk am Perimeter zu schützen. Darüber hinaus erhöhen Trends wie „Bring Your Own Device", firmeneigene und persönlich genutzte Geräte die Komplexität bei der Definition effektiver Sicherheitsmassnahmen. Deshalb verschwimmt der Perimeter als eindeutige Sicherheitslinie und muss auf die verschiedenen Endpunkte ausgeweitet werden sowie zusätzliche automatisierte Kontrollen umfassen.[3]

Um diesen Trends Rechnung zu tragen, wird die datenfokussierte Sicherheit immer stärker verfolgt. Einfach ausgedrückt bedeutet dies, dass Schutzmassnahmen direkt auf die Daten angewendet werden sollten, unabhängig davon, wo die Daten gespeichert, abgerufen oder verarbeitet werden. Diese neue Denkweise ist Teil des Zero Trust (ZT)-Ansatzes und wird durch diesen formalisiert:[4]

- Zero Trust geht davon aus, dass Vermögenswerten oder Benutzerkonten kein implizites Vertrauen allein aufgrund ihres physischen Standorts oder Netzwerks (d. h.

[1] Die gewählte Lizenzierung hat einen Einfluss auf die verfügbaren Microsoft Sicherheitslösungen.
[2] (Songpon Teerakanok, 2021).
[3] ebd.
[4] (Scott Rose, 2020)

lokale Netzwerke im Gegensatz zum Internet) oder aufgrund des Eigentums an Vermögenswerten (Unternehmen oder Privatpersonen) entgegengebracht wird.
- Die legitime Authentifizierung und Autorisierung (sowohl des Subjekts als auch des Geräts) werden überprüft, bevor eine Sitzung mit einer Unternehmensressource stattfindet.
- Zero Trust konzentriert sich auf den Schutz von Ressourcen (Vermögenswerte, Dienste, Arbeitsabläufe, Netzwerkkonten usw.) und nicht auf Netzwerksegmente, da der Standort des Netzwerks nicht mehr als wichtigste Komponente für die Sicherheit der Ressource angesehen wird. Dies bedeutet, dass unabhängig vom Standort (vor Ort oder in der Cloud) die zugrunde liegende Infrastruktur, aber auch alle Anwendungen, Middleware und Datenbanken dem Zero-Trust-Prinzip folgen müssen.
- Bei Zero Trust handelt es sich nicht um eine einzelne Architektur, sondern um eine Reihe von Leitprinzipien für Arbeitsabläufe, Systemdesign und Betrieb, die zur Verbesserung der Sicherheitslage für jede Klassifizierungs- oder Sensibilitätsstufe verwendet werden können [FIPS199].
- Die Zero-Trust-Architektur ist ein End-to-End-Ansatz für die Sicherheit von Unternehmensressourcen und -daten, der Identität (Personen und Nicht-Personen), Anmeldeinformationen, Zugriffsmanagement, Betrieb, Endpunkte, Hosting-Umgebungen und die verbindende Infrastruktur umfasst.

Es wird deutlich, dass Zero Trust ein übergreifendes Prinzip ist, das durch die Umsetzung von Massnahmen auf allen Informationssystemen (für alle IT-Lösungen inkl. M365, Betriebsmodelle On-Prem, SaaS, Cloud Computing) erreicht und angewendet wird. Da Organisationen in der Regel nicht von Grund auf neu anfangen, sondern über bestehende Netzwerke und Systeme verfügen, ist der Paradigmenwechsel ein Prozess, welcher Schritt für Schritt vollzogen wird. Daher empfiehlt sich die Durchführung einer Analyse der Ist-Situation und die Entwicklung eines Vorgehensplans.

5.2 Schutzziele

Die Risiken durch die Nutzung von Cloud Services sind nicht per se höher als bei on-premises Lösungen, sondern haben zum Teil andere Ausprägungen (z.B. interne Verfügbarkeit und externe Verfügbarkeit bei Ausfall). Die Verfügbarkeit der Services wird oftmals höher bewertet als bei eigenen Hostings. Der Lawful Access zum Beispiel hingegen wird im Zusammenhang mit der Nutzung von Microsoft 365 als neues Risiko angeführt. Nachfolgend wird eine Übersicht der Risiken dargelegt, welche mit der Nutzung von Cloud Services einhergehen.

5.2.1 Datenschutz

Die Verantwortlichkeit in Bezug auf Datenschutz ist gesetzlich klar geregelt. Auch bei der Auslagerung von Dienstleistungen, bleibt das auslagernde Organ vollumfänglich für für Daten verantwortlich. Dies gilt insbesondere, wenn personenbezogene Daten durch Dritte im Auftrag bearbeitet werden.

Daraus resultiert, dass bei der Nutzung von Cloud-Services sichergestellt werden muss, dass die gesetzlichen Bestimmungen zum Datenschutz jederzeit gewährleistet werden können.

Um die konkreten Datenschutzrisiken zu bewerten, muss ein Risk-Assessment durchgeführt werden. Je nach individueller Vorgabe kann das Cloud-Compliance und Risk-Assessment für den öffentlichen Sektor in der Schweiz (CCRA-PS)[5] oder ein anderes Framework dafür verwendet werden.

5.2.2 Informationssicherheit

Dass Ziel der Informationssicherheit ist es, risikobasiert, die Vertraulichkeit, Integrität und Verfügbarkeit der Informationen der Organisation sicherzustellen:

a) **Vertraulichkeit**: Werden Informationen nicht autorisierten Personen, Systemen oder Prozessen zugänglich gemacht ist die Vertraulichkeit verletzt. Durch die Verletzung der Vertraulichkeit von Informationen können beispielsweise Datenschutzverletzungen entstehen oder die Reputation des Kantons geschädigt werden.

   Die Vertraulichkeit kann beispielsweise durch einen erfolgreichen Cyberangriff, durch einen behördlichen Zugriff (Lawful Access) oder Fehlverhalten durch BenutzerInnen verletzt werden.

b) **Integrität**: Werden Informationen unerlaubterweise verändert, ist die Integrität der Information verletzt.

   Bei der Bearbeitung von Informationen, deren Integrität verletzt wurde, können falsche Ergebnisse oder Schlussfolgerungen gezogen werden. Die Integrität kann z.B. im Rahmen eines Cyberangriffes oder durch Fehlbedienung/-Fehlmanipulation verletzt werden.

c) **Verfügbarkeit**: Steht die Information autorisierten Personen, Systemen, Prozesse nicht am gewünschten Ort und zum gewünschten Zeitpunkt zur Verfügung, ist die erforderliche Verfügbarkeit verletzt.

   Stehen Informationen nicht in dem Masse zur Verfügung in welchem sie benötigt werden, können Prozesse zum Stillstand gezwungen sein. Die Verletzung der Verfügbarkeit kann durch den Ausfall von Datenzentren, Applikationen, Internet etc. ohne böswillige Absichten oder Fremdeinwirkungen eintreten oder durch gezielte Cyberangriffe ausgelöst werden.

Die konkreten Informationssicherheitsrisiken werden mit Hilfe einer Schutzbedarfsanalyse (Schuban) ermittelt und bewertet. Die Schutzmassnahmen orientieren sich am BSI C5[6]. Die Erstellung eines ISDS-Konzeptes ist gemäss der Projektmethode HERMES verpflichtend.

[5] https://www.rosenthal.ch/downloads/Rosenthal_CCRA-PS_Slides-DVS.pdf
[6] Cloud Computing Compliance Criteria Catalogue – C5:2020 – Kriterienkatalog Cloud Computing (bund.de)

5.3 Microsoft Schutzmassnahmen[7]

Microsoft Exchange Online ist Teil der Microsoft 365 Subscription und wird als Software-as-a-Services auf der Cloud-Infrastruktur von Microsoft betrieben. In diesem Kontext verantwortet Microsoft die Sicherheit der im Service enthaltenen Infrastruktur und Komponenten. Die nachfolgende Aufstellung bildet einen groben Überblick ohne Anspruch auf Vollständigkeit. Die Details können in der Microsoft Dokumentation jederzeit nachvollzogen werden.

5.3.1 Rechenzentren

Die Rechenzentren werden mit mehrstufigen zeitgemässen Sicherheitssystemen gesichert. Die Konzeption des Sicherheitskonzeptes ist dokumentiert und kann bei Bedarf im Detail nachvollzogen werden.[8]

Die hohe Verfügbarkeit der Services wird durch Azure Availability Zones sichergestellt. Diese Architektur stellt sicher, dass mehrere physisch getrennte Rechenzentrumsstandorte innerhalb jeder Azure-Region, bei lokalen Ausfällen die Verfügbarkeit der Services sicherstellten. Dafür werden die Daten jeweils zeigleich in mehreren Datencentern einer Region gespeichert (Active-Active). Die Ausfälle können aufgrund von Software- und Hardwarefehlern bis hin zu umweltbedingten Störungen durch z.B. Erdbeben, Überschwemmungen und Bränden reichen.

Die Schutzmassnahmen werden im Rahmen der ISO 27001 und SOC 1 und SOC 2 Auditierungen regelmässig überprüft und bescheinigt. Die Ergebnisse sind für Kunden im Microsoft Service Trust Portal jederzeit einsehbar.[9]

5.3.2 Netzwerksicherheit

Um die Sicherheit der Netzwerkinfrastruktur sicherzustellen, werden automatisierte Mechanismen zur Erkennung und Verhinderung netzwerkbasierte Angriffe eingesetzt. Zudem sind die Netzwerke auf logischer Ebene segmentiert und an den Übergangspunkten mit Firewalls überwacht. Dabei werden nur explizit erlaubte Verbindungen zugelassen. Darüber hinaus verfügt die Infrastruktur insbesondere über Schutzmassnahmen zur Erkennung und Abwehr von Distrubuted Denial of Service Angriffen (DDoS-Attacks).

5.3.3 Schwachstellenmanagement

Grundsätzlich können in allen Komponenten eines Services Schwachstellen entstehen bzw. vorhanden sein. Aus diesem Grund wird die Basisinfrastruktur (Server + Netzwerk) regelmässig auf Schwachstellen hin gescannt. Der Scan prüft auf fehlende Security Patches, Konfigurations- sowie Applikationsschwachstellen.[10]

---

[7] Securing the Microsoft Online Services infrastructure - Microsoft Service Assurance | Microsoft Learn

[8] Sicherheit von Rechenzentren (Übersicht) - Microsoft Service Assurance | Microsoft Learn

[9] Service Trust Portal Home Page (microsoft.com)

[10] Bedrohungs- und Sicherheitsrisikoverwaltung - Microsoft Service Assurance | Microsoft Learn

Identifizierte Schwachstellen werden mit Security Patches priorisiert und im Rahmen des Change-Managements geschlossen.

5.3.4 Identity und Access Management

Der Zugriff auf Service-Komponenten, die Kundeninformationen beinhalten ist streng reglementiert und überwacht. Für den Betrieb der Services wird grundsätzlich kein Zugriff auf Kundendaten benötigt. Im Grundsatz gilt, dass kein Microsoft Mitarbeiter Zugang zu Kundendaten hat. Erst durch die Beauftragung durch den Kunden (Ticket) kann ein Microsoft Engineer bei Bedarf einen zeitlich limitierten Zugang beantragen. Dieser Zugriff wird über einen internen Prozess gesteuert (Lockbox Prozess). Nach einer Überprüfung durch einen Manager erhält der Engineer temporäre (just in time) die benötigten Zugriffsrechte (least privileges). Diese Zugriffe sind auditiert und können vom Kunden direkt jederzeit nachvollzogen werden.

5.3.5 Personalsicherheit

Das eingesetzte Personal wird vor Einstellung sowie regelmässig wiederkehrend systematisch einem Screening unterzogen. Personen, die im Rahmen der Microsoft Serviceerbringung eine Aufgabe wahrnehmen und Zugang zu Kundendaten haben könnten, werden mit zusätzlichen Background-Checks geprüft.

5.3.6 Lieferantensicherheit

Microsoft arbeitet mit Partner zusammen, um die Services erbringen zu können. Da die Zusammenarbeit mit Partnern von zentraler Bedeutung ist, werden diese im Rahmen des Supplier Security and Privacy Assurance (SSPA) Programm aktiv gesteuert. Damit wird sichergestellt, dass die Datenschutz- und Sicherheitsanforderungen durchgängig eingehalten werden.

5.3.7 Business Continuity Management

In erster Linie wird die Sicherstellung der Verfügbarkeit der Services und Daten durch die redundante Architektur sichergestellt.

Zusätzlich stellt ein dediziertes Team sicher, dass im Rahmen des BCM-Prozesses kritische Prozesse und Ressourcen identifiziert, bewertet und mittels Massnahmen zur Stärkung der Resilienz geschützt werden. Die definierten Business Continuity Pläne werden regemässig getestet.

5.3.8 Zertifizierungen

Microsoft verfügt über eine Vielzahl von Zertifizierungen, welche die Umsetzung der Sicherheitsmassnahmen regelmässig bescheinigen. Die Zertifizierungen bzw. aktuellen Auditberichte können kundenseitig im Microsoft Service Trust Portal eingesehen werden.[11]

5.4 Kundenseitige Schutzmassnahmen

Im SaaS-Model ist der Kunde für den Schutz der Informationen bzw. Daten selbst, die eingesetzten Endgeräte und der eigenen Identities verantwortlich. Mögliche technische

[11] Service Trust Portal Home Page (microsoft.com)

Umsetzungen werden nachfolgend beschrieben. Trotz technischer und organisatorischer Massnahmen verbleibt aber ein Restrisiko der Verletzung der Schutzziele der Informationssicherheit (vgl. Kap. 5.2).

5.4.1 Verschlüsselung

Eine Service-Verschlüsselung ist per se aktiv. Somit ist ein Schutz vor einem unbefugten Zugriff (Ausnahme durch Microsoft selbst) auf die Daten gewährleistet. Um einen Schutz vor einem möglichen Zugriff durch Microsoft selbst zu ermöglichen ist die Übernahme des Schlüsselmanagements durch den Kunden (CMK Customer Managed Key) bzw. DKE (Double Key Encryption) eine Option.[12] E-Mails können zusätzlich mit Microsoft-eigenen Verschlüsselungsmöglichkeiten oder eingebundenen Drittlösungen verschlüsselt werden. Je nach eingesetzter Verschlüsselung bzw. Schlüsselmanagement-Option sind Einschränkungen in der Funktionalität zu vergegenwärtigen.

Eine Gegenüberstellung der jeweiligen Verschlüsselungsmethoden ist nachfolgend ersichtlich:

5.4.1.1 Basisverschlüsselung Microsoft

Data at Rest: Neben der Verschlüsselung auf Ebene Festplatte (Volume) verwenden Exchange Online, Microsoft Teams, SharePoint Online und OneDrive for Business auch die Dienstverschlüsselung (Service Encryption), um Kundendaten zu verschlüsseln.

Microsoft verwaltet alle kryptografischen Schlüssel (Microsoft Managed Keys), einschliesslich der Stammschlüssel für die Dienstverschlüsselung. Diese Option ist derzeit standardmässig für Exchange Online, SharePoint Online OneDrive for Business und Teams aktiviert.

Data in Motion: Die Datenübertragung zu Microsoft erfolgt immer über HTTPS oder einer TLS-Transportschicht. Somit sind alle Datenübertragungen Client zu Server oder Server zu Server mit mindestens TLS 1.2 abgesichert. Bei SMTP werden die Daten mit STARTTLS über Port 25 abgesichert und die Datenübertragungen somit mit TLS zu M365 geschützt.

5.4.1.2 Kundenschlüssel-Verschlüsselung (Customer Key Encryption)

Mittels Customer Key können Kunden ihre Daten im Ruhezustand in Microsoft-Rechenzentren zusätzlich zum durch den von Microsoft verwalteten-Schlüssel (Microsoft Managed Keys) mit einem Kundenschlüssel verschlüsseln. Dies setzt eine entsprechende Lizenz voraus voraus.

Diese Massnahme kann im laufenden Betrieb als «Service Encryption with Customer Key» in der Grundkonfiguration umgesetzt werden und umfasst dann auch die bis dahin angefallenen Bestandsdaten. Die Benutzer merken von der Einführung des Customer Key nichts. Eine Encryption kann pro Workload welche dies unterstützen (Exchange Online,

[12] Siehe Kapitel 5.4.1.1, 5.4.1.4

SharePoint Online, OneDrive for Business und Teams) einzeln aktiviert werden. Die nachfolgende Tabelle zeigt die Schlüsselhierarchie innerhalb der Verschlüsselung.

Es gibt noch weitere Möglichkeiten den Customer Key abzulegen, welche von Microsoft unter untenstehendem Link dokumentiert sind.
https://learn.microsoft.com/en-us/azure/security/fundamentals/key-management-choose

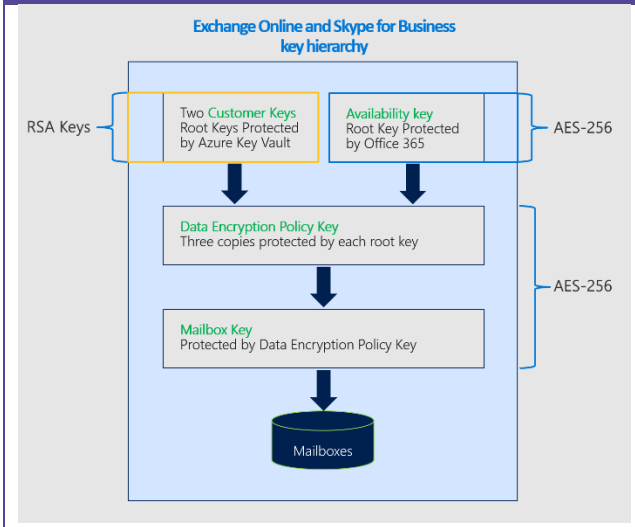
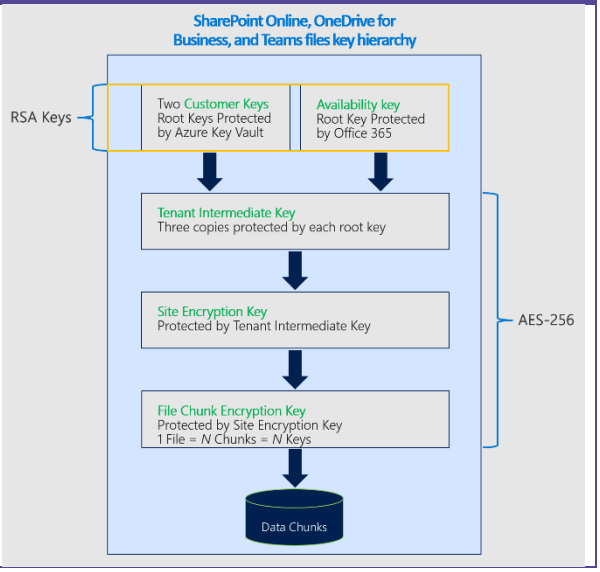
Exchange / Skype	SharePoint Online / Onedrive for Business und Teams Files
	

Tabelle 1 - Customer Key

5.4.1.3 Verfügbarkeitsschlüssel (Availability Key)

Der Verfügbarkeitsschlüssel bietet eine Hochverfügbarkeitsfunktion, wenn Microsoft 365-Dienste, aufgrund vorübergehender Fehler, keine in Azure Key Vault gehosteten Schlüssel erreichen können. Diese Regel gilt nur für die Verschlüsselung von Exchange Online-. SharePoint Online-, OneDrive for Business- und Teams-Dateien verwenden niemals den Verfügbarkeitsschlüssel, es sei denn, Sie weisen Microsoft explizit an, den Wiederherstellungsprozess zu initiieren.

Basierend auf der Architektur von M365 hat Microsoft via dem Availability Key bei der Verwendung des Customer Key trotzdem Zugriff auf die Daten innerhalb von Exchange Online. Basierend auf der „prefered Architecture" von Microsoft werden die Schlüssel „Customer Keys" zudem in einem sogenannten Key Vault innerhalb Microsoft Azure gespeichert. Im Rahmen dieses Szenarios werden die Schlüssel und der entsprechende Tresor beim gleichen Anbieter gehostet. Eine Gewaltentrennung wird somit im Rahmen der Prozesse auf Seiten Microsoft vorgenommen.

Stärke	Schwäche
Customer Key anstatt Microsoft-Schlüssel.	Bringt zusätzliche Komplexität und erfordert neue Skills. Zusätzliche Kosten Kann nur für einige Dienste genutzt werden (Exchange Online, SharePoint Online, Onedrive und Teams) Mit Availability Key hat Microsoft trotzdem Zugriff auf die Mailbox Daten.
Gelegenheit	**Bedrohung**
Ermöglicht den Einsatz von Exchange Online bei erhöhten Anforderungen bezüglich dem Schutz von gewissen Daten.	Verantwortung für den Key. Falsche Handhabung von Schlüsseln.

Tabelle 2 - SWOT Customer Key

5.4.1.4 Doppelte Schlüsselverschlüsselung (DKE)

Die Doppelte Schlüsselverschlüsselung bietet erweiterte Schutzmechanismen für Ihre sensibelsten Daten, die den strengsten Schutzanforderungen unterliegen. Die doppelte Verschlüsselung schützt die Daten vor Zugriff von Seite Microsoft. Dabei gehen für den Anwender aber sämtliche Kollaborationsfunktionen verloren. Diese sind wie folgt unten aufgelistet: Transportregeln, einschliesslich Antimalware und Spam, die einen Einblick in die Anlage erfordern

- Microsoft Delve
- eDiscovery
- Inhaltssuche und -indizierung
- Office Web-Apps einschliesslich Funktionen für die gemeinsame Dokumenterstellung

DKE bringt die folgenden Voraussetzungen mit sich:

- Lizenz: Microsoft 365 E5 oder Add-on Subscriptions.
- Software: Azure Information Protection Unified Labeling Client Version 2.7.93.0 oder höher.

Stärke	Schwäche
Maximale Verschlüsselungsstufe.	Verlust von M365-Sicherheitstools (AntiVirus / AntiSpam / AntiPhishing / Identity Protection / Exchange Transportregeln / Compliance Search) Supportfähigkeit von Microsoft eingeschränkt Outlook Stellvertretung funktioniert nicht mehr.
Gelegenheit	**Bedrohung**
Ermöglicht die Speicherung von höchst schützenswerten Daten in der Cloud.	Compliance Search kann nicht durchgeführt werden Komplexität und korrekte Handhabung beim Key Management. Das Hosting, respektive der Betrieb des Key muss vom Kunden selbständig erbracht werden.

Tabelle 3 - SWOT DKE

5.4.1.5 Datenverschlüsselung im Ruhezustand

Alle EXO (Exchange Online)-Daten werden im Ruhezustand verschlüsselt in M365 gespeichert, wobei die von Microsoft bereitgestellte M365-Technologie verwendet wird. Dies bedeutet, sämtliche Daten sind auf den Servern physisch verschlüsselt.
Microsoft verschlüsselt alle EXO-Daten im Ruhezustand in den Microsoft-Rechenzentren mit BitLocker Drive Encryption. Dies schützt die E-Mail-Daten vor dem direkten, unbefugten Zugriff auf einem Datenträger, sog. “offline encryption”.

5.4.1.6 Datenverschlüsselung bei der Übermittlung

Die Verschlüsselung bei der Übertragung innerhalb von EXO wird vollständig von Microsoft verwaltet. Integrationen von lokalen Systemen (oder anderen Cloud-Anwendungen) zu und von Microsofts Cloud-Dienst dürfen nur über sichere Protokolle erfolgen. Microsoft bietet mit einigen Ausnahmen (z. B. POP, IMAP) keine unsicheren Endpunkte an. Für die entsprechenden Ausnahmen ist von einer Verwendung abzuraten.

5.4.1.7 E-Mail-Verschlüsselung mit S/MIME

Die E-Mail-Verschlüsselung mittels S/MIME dient dem Zweck des Schutzes vor Vertraulichkeitsverlust.

Um eine E-Mail mit S/MIME zu verschlüsseln setzt eine gültige S/MIME Signatur des Empfängers voraus. Es wird ein public-key des Empfängers vorausgesetzt, der vorgängig

ausgetauscht werden muss - und der Umgang mit key-pairs in public-key-Verfahren ist für Laienbenutzer typischerweise überfordernd.

Stärke	Schwäche
End-to-End Verschlüsselung	Outlook Delegate funktioniert nicht (kann verschlüsselte Mails nicht lesen oder versenden) S/MIME Szenarien mit Mobile und OWA sind komplex und aufwändig Zertifikatsverwaltung auf den Geräten und Aufbewahrung abgelaufener Zertifikate S/MIME Zertifikatshandling bei Benutzern führt zu höherem Supportaufkommen S/MIME Verschlüsselte Anlagen können vom der Compliance Search nicht gefunden werden (fehlender Schlüssel)
Gelegenheit	**Bedrohung**
Für einige wenige Benutzer kann S/MIME eine kostengünstige Variante darstellen	End-to-End Verschlüsselte Inhalte können von Mailfiltern nicht analysiert werden (Antivirus / Antispam / Antiphishing)

5.4.1.8 Microsoft Purview Message Encryption OME)

Die E-Mail-Verschlüsselung mittels 5.4.1.8 Microsoft Purview Message Encryption , früher bekannt als Office 365 Message Encryption (OME), dient dem Zweck des Schutzes vor Datenverlust, sowie der Kontrolle über Weiterleitung und Druck.

Überblick der Lösung: Die E-Mail wird an Externe gesendet und der Empfänger erhält nur einen Link. Er muss sich auf der OME-Website unter M365 anmelden und sich mit einem Gmail-, Yahoo- oder Microsoft-Konto authentifizieren. Es besteht auch die Möglichkeit, sich zum ersten Mal mit einem OTP-Code zu authentifizieren. Dieser OTP-Code wird per Mail an den Empfänger der Email geliefert. Sollte der Anwender bereits an einem M365 Tenant angemeldet sein, entfällt die entsprechende Anmeldung. Diese Lösung bietet Vor- wie aber auch Nachteile, welche in der untenstehenden Tabelle ersichtlich sind:

Stärke	Schwäche
Sicher und einfach zu installieren DLP - Daten verlassen nie das Unternehmen	Daten können trotzdem als Screenshot gespeichert werden

Es gibt keine Kopien beim Empfänger oder einer Gruppe von Empfängern. Zeitliche Beschränkung des Datenzugriffs möglich.	Nur ein Link im Postfach des Empfängers - Inhalt kann nicht gesucht und gefunden werden Passwort nicht über einen separaten Kanal übermittelt (ebenfalls Email)
Gelegenheit	**Bedrohung**
Einfache Möglichkeit um mit externen gelegentlich zu kommunizieren.	Zusätzliche Unterstützung beim Versuch, sich auf der OMA-Website einzuloggen

5.4.1.9 SEPPMail Gateway Verschlüsslung

SEPPMail ist ein Schweizer Anbieter von Email Security Lösungen. Entsprechende Appliances können im Rechenzentrum, oder in Azure installiert und in den Emailfluss integriert werden.

Die Stärke des Produkts liegt darin, dass es sehr gut auf den Schweizer Markt und dessen Bedürfnisse ausgerichtet ist. Spezifische Schweizer Dienste wie das HIN Netzwerk oder Incamail werden unterstützt. Ein automatisiertes Ausstellen von S/MIME Zertifikaten von der SwissSign Certification Authority (CA) ist möglich.

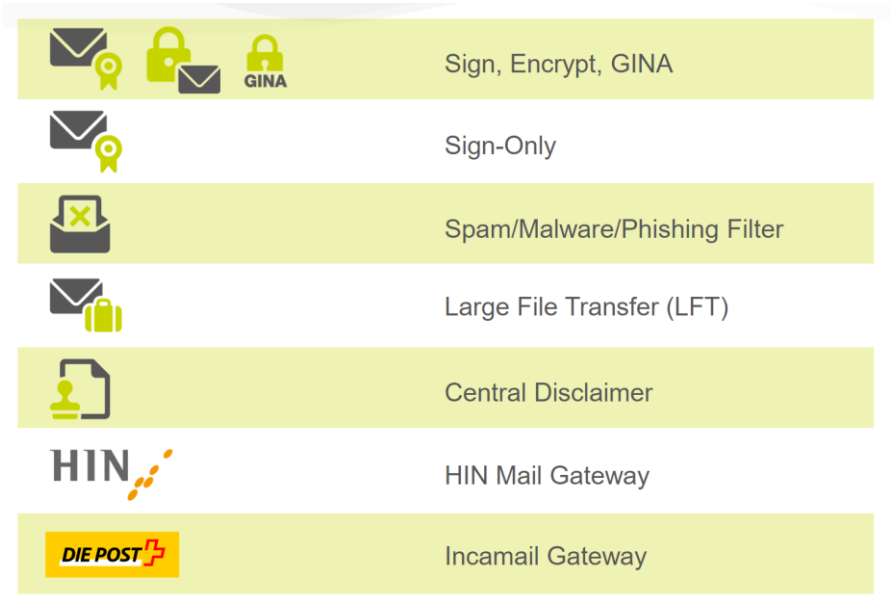


Abbildung 2 SEPPMail Produkte

Das Produkt Sepp Mail umfasst mehrere Stufen, um eine Nachricht zu schützen, diese sind in der folgenden Tabelle ersichtlich:

Produkt	Beschreibung
Sign/ Encrypt / GINA	Ausgehende Mails können mit S/MIME oder PGP-Signiert oder Verschlüsselt werden.

	Dies kann über Regeln oder über ein Plugin im Outlook gesteuert werden. Bei GINA wird dem Empfänger nur ein Link zugesellt. Er muss sich auf der SeppMail HTTPS Weboberfläche anmelden, um den Inhalt lesen zu können oder zu antworten.
Sign-Only	Ausgehende Mails werden mit S/MIME oder PGP signiert werden
Spam/Malware/Phishing Filter	SEPPMail bietet auch Antispam / Antimalware und AntiPhishing Filter an.
Large File Transfer	Möglichkeit um grosse Files zu übermitteln. Steht in Konkurrenz zu Sicherem FileTransfer oder Links in OneDrive/SharePoint Online.
Central Disclaimer	Möglichkeit Disclaimer an Nachrichten anzuhängen
HIN Mail Gateway	Unterstützt das Health Info Net (HIN)
Incamail Gateway	Unterstützt die Anforderungen um Nachrichten an den IncaMail Service der schweizerischen Post zu übermitteln.

Stärke	Schwäche
Unterstützt alle gängigen Verschlüsselungen (S/Mime / PGP) und spezifisce Service (Incamail / HIN) Kann auch für S/Mime Signierung benutzt werden (Sign-only) Zentrale Verwaltung Verschlüsselung am Gateway ins Internet Schweizer Anbieter Separater Kanal um das Passwort für GINA Mails zu übermitteln.	Keine End-to-End Verschlüsselung Erhöhte Komplexität in der Architektur sowie im Betrieb.
Gelegenheit	**Bedrohung**
Bietet die Möglichkeit Daten sicher mit Partnern auszutauschen.	

5.4.2 Klassifizierung

Um einen effektiven Schutz sicherzustellen, gilt es die eigenen Daten und ihren «Wert» für die Organisation und die gesetzlichen Anforderungen zu kennen, gezielte Schutzmassnahmen zu definieren, absichtlichen oder unabsichtlichen Datenverlust bzw. Offenlegung zu verhindern und den gesamten Lebenszyklus dabei zu berücksichtigen.

Die Klassifizierung von Informationen bildet die Basis für die Festlegung von Schutzmassnahmen und unterstützt die Mitarbeitenden im adäquaten Umgang mit geschäftlichen Informationen.

Microsoft Purview Information Protection bietet die Möglichkeit verschiedene Sensitivity Labels und Sublabels pro Klassifizierungsstufe zu definieren. Dies erlaubt z.B. eine Unterscheidung verschiedener Vertraulichkeitslabels. Auf der einen Seite ermöglicht dies eine granulare Steuerung des Schutzlevels innerhalb einer Klassifizierungsstufe.[13] Auf der anderen Seite erhöht dies jedoch auch Komplexität für die Benutzer*Innen und erfordert daher mehr Schulungsaufwand. Um die Komplexität gering zu halten, empfehlen wir mit einer 1:1 Übernahme der bestehenden Klassifizierungsstufen in Microsoft Sensitivity Labels.[14]

Die in diesem Dokument verwendeten Klassifizierungsstufen sind ein Good Practice Vorschlag und beinhaltet keine Definition der jeweiligen Stufen. Diese muss jede Behörde definieren und schulen.

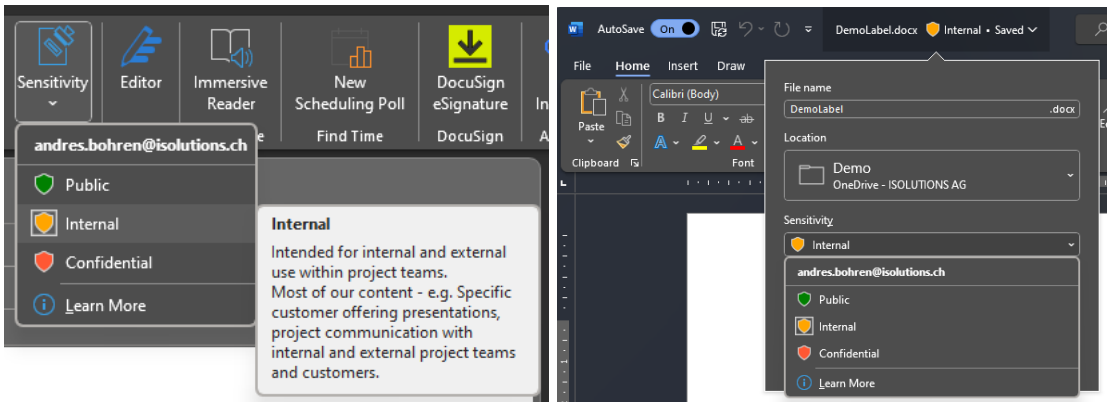


Abbildung 3 Labeling von Outlook Nachrichten und Office Dokumenten

Unabhängig davon, wie der Versand von klassifizierten E-Mails geregelt wird, kann nicht ausgeschlossen werden, dass vertrauliche oder geheime Information per E-Mail empfangen werden. Somit kann nicht ausgeschlossen werden, dass Informationen der

[13] Die Funktionalitäten der Lösung werden stetig seitens Microsofts weiterentwickelt, weshalb eine diese regelmässig neu bewertet werden müssen.
[14] Die Unterstützung diverser Dokumentenarten wird kontinuierlich ausgebaut. Aktuelle Übersicht: File types supported by the Azure Information Protection (AIP) unified labeling client | Microsoft Learn

Klassifizierungsstufe vertraulich oder geheim in der Cloud bearbeitet werden. Gleichwohl ist dieser Use Case nicht durch die Behörde steuerbar und kann somit nicht geregelt werden.[15]

5.4.3 Data Loss Preventions (DLP)

Auf Basis der Klassifizierung bzw. Auf Basis der Inhalte, Verhaltensmuster der Benutzer, Sender- bzw. Empfänger-Konstellationen etc. können gezielte Schutzmassnahmen (Data Loss Prevention) definiert und durchgesetzt werden. Das Ziel ist es, die (klassifizierten) Information, unabhängig von ihrem Speicherort, zu schützen. Mit Microsoft Purview Information Protection oder DLP können (gelabelte) E-Mails bzw. E-Mail-Anhänge mit Schutzmassnahmen versehen und geschützt werden.

5.4.4 Backup

Exchange Online verfügt nicht über klassische Backup-Funktionalitäten. So können beispielsweise einzelne E-Mails während 30 Tagen von den Benutzer*Innen selbst wiederhergestellt werden. Die Wiederherstellung gelöschter Postfächer ist für Admins ebenfalls während 30 Tagen möglich.

Sofern eine Sicherung der Postfächer darüber hinaus notwendig ist, muss eine Drittlösung zusätzlich verwendet werden.

5.4.5 Customer Lockbox

Damit ein Zugriff durch Microsoft (z.B. zur Behebung von technischen Problemen) nicht unkontrolliert stattfindet, besteht die Möglichkeit die «Customer Lockbox» einzurichten. Diese stellt einen Genehmigungsprozess sicher, welcher durchlaufen werden muss, bevor ein Zugriff durch Microsoft erfolgt. Erst mit der kundenseitigen Genehmigung wird der Zugriff zeitlich begrenzt und geloggt gewährt. Ohne "Customer Lockbox" kommt bei einem Zugriff auf Kundendaten durch Microsoft in jedem Fall der Microsoft "Lockbox" Prozess zum Tragen, d.h. die vorgesetzte Stelle eines Microsoft-Mitarbeitenden muss den Zugriff freigeben, der wiederum zeitlich begrenzt (just-in-time) und protokolliert stattfindet. Solche Zugriffsprotokolle sind durch den Kunden jederzeit einsehbar.

5.4.6 Device Management inkl. Malwareschutz

Für die Geräteverwaltung können unterschiedliche Ansätze verwendet werden:

1. Mobile Device Management (MDM)

Über ein Mobile Device Management kann die Organisation die ganzen Geräte steuern (z.B. Conditional Access) und hat somit die volle Kontrolle. Dieser Ansatz wird insbesondere dann favorisiert, wenn die Organisation die Besitzerin der Geräte ist und der private Gebrauch eingeschränkt erlaubt oder verboten ist.

2. Mobile Applikation Management

Gehört das Gerät dem Mitarbeitenden, ist die Verwendung eines Mobile Device Managements für die Steuerung des gesamten Gerätes nicht praktikabel, weil die

[15] Der Empfang von E-Mails mit vertraulichen oder geheimen Informationen kann seitens Absender ebenfalls durch Exchange Online erfolgen.

Organisation damit zu sehr in den privaten Bereich der Mitarbeitenden eingreift.[16] In diesem Fall bietet sich der Einsatz eines Mobile Applikation Managements an, bei dem nur einzelne Applikationen und die darin enthaltenden Daten von der Organisation gesteuert werden können. Auch eine Löschung bei einem Austritt oder Verlust beschränkt sich in diesem Fall auf die geschäftlichen Daten.

Das Management der Endgeräte (Clients & Smartphones) kann über Microsoft Lösung Intune erfolgen:[17]

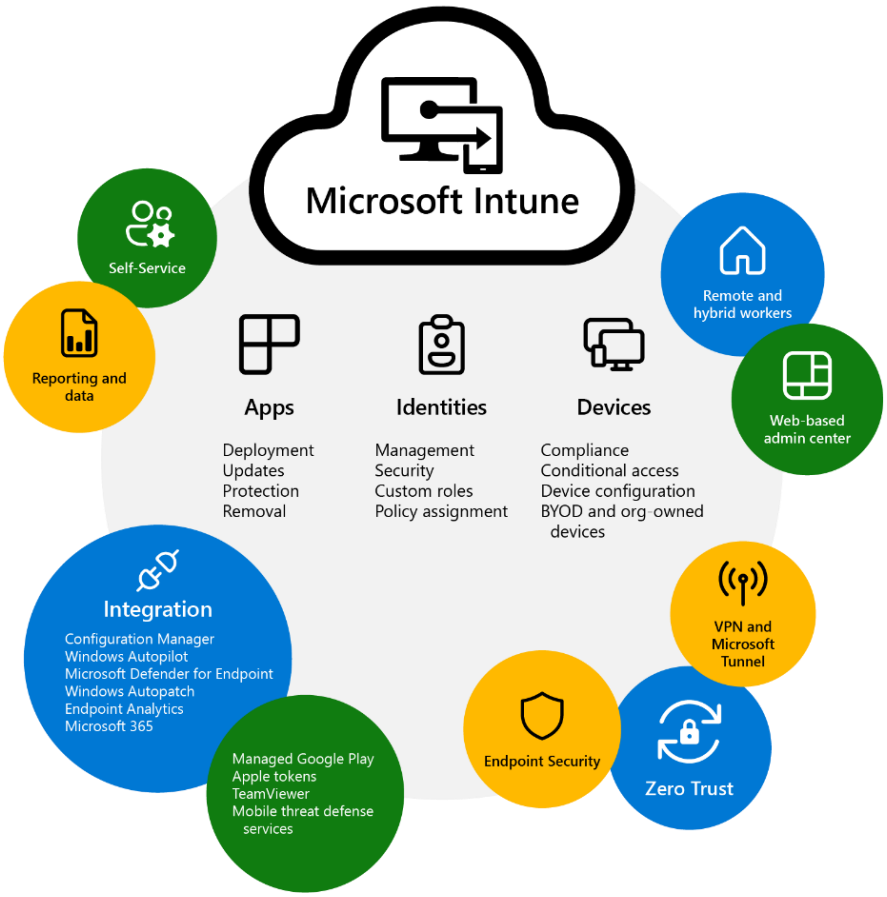


Abbildung 4 - Übersicht Microsoft Intune

Quelle: Microsoft Intune | Microsoft Learn

5.4.7 Organisatorische Regelungen

Neben den technischen Schutzmassnahmen müssen organisatorische Massnahmen (Governance & Weisungen) definiert werden, um dien adäquaten Umgang zu gewährleisten.

[16] Würde die Organisation bei einem Verlust das Geräte remote Wipen, würden ebenfalls die privaten Daten des Mitarbeitenden gelöscht werden.
[17] Details Kapitel 9.2

5.5 Lawfull Access

Im behördlichen Kontext ist insbesondere der Umgang mit einem Lawful Access aus den USA eine wichtige Frage.[18] Um dieses Risiko besser einordnen zu können, zeigt die nachfolgende Tabelle die Zugriffsanfragen sowie die herausgegebenen Daten über die letzten 10 Jahre in der Schweiz:

	2013H1	2013H2	2014H1	2014H2	2015H1	2015H2	2016H1	2016H2	2017H1	2017H2	2018H1	2018H2	2019H1	2019H2	2020H1	2020H2	2021H1	2021H2	2022H1
CH Requests	43	72	46	64	117	105	98	119	1	88	101	139	185	240	255	263	444	522	776
CH Users	80	162	103	93	232	174	132	212	1	182	131	210	244	319	344	411	581	1188	1266
CH Discosure Content	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
CH Discosure NonContent	27	44	34	47	81	68	68	76	0	56	60	90	92	103	100	123	184	300	275
CH No Data Found	11	9	6	4	10	12	14	16	1	13	16	24	61	91	119	77	63	76	110
CH Request Rejected	5	19	6	13	26	25	16	27	0	19	25	25	32	46	36	63	197	101	185

Es wird deutlich, dass in den vergangen 10 Jahren, trotz kontinuierlicher Anfragen keine personenbezogenen Daten seitens Microsofts herausgegeben wurden. Es ist jedoch zu beachten, dass es sich um eine retroperspektive Betrachtung handelt und diese keine 100-prozentige Sicherheit für die Zukunft voraussagt.

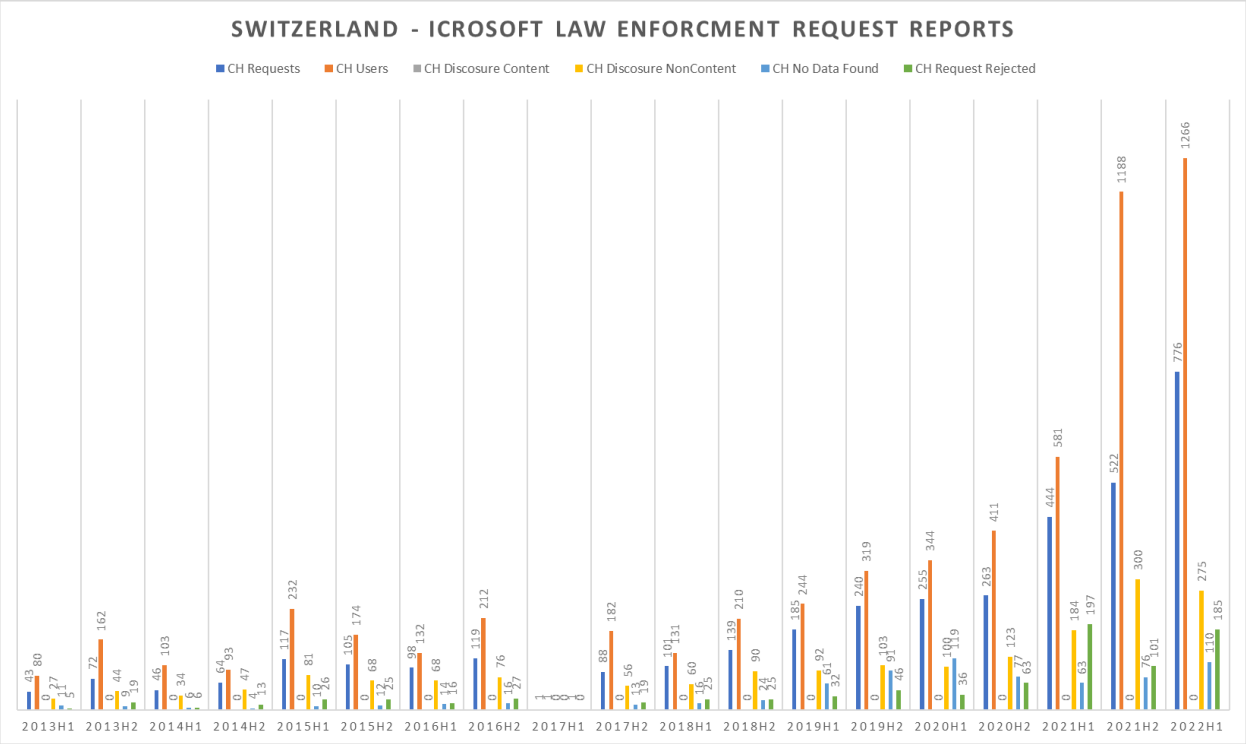
Law Enforcement Requests Report 2022

Requests received for all Microsoft Services from January to June 2022

	Total Requests		Some Customer Data Disclosed				No Customer Data Disclosed			
	Total Number of Law Enforcement Requests	Accounts / Users Specified in Requests	Law Enforcement Requests Resulting in Disclosure of Content		Law Enforcement Requests Resulting in Disclosure of Only Subscriber/Transactional (Non-Content) Data		Law Enforcement Requests Resulting in Disclosure of No Customer Data (No Data Found)		Law Enforcement Requests Resulting in Disclosure of No Customer Data (Request Rejected for Not Meeting Legal Requirements)	
	#	#	%	#	%	#	%	#	%	#
TOTAL	26'365	58'665	3.76%	992	53.26%	14'043	17.94%	4'730	25.03%	6'600
Austria	219	236	0.00%	0	57.99%	127	9.13%	20	32.88%	72
France	1'643	3'273	0.00%	0	50.03%	822	16.98%	279	32.99%	542
Germany	6'455	12'522	0.00%	0	52.04%	3'359	12.27%	792	35.69%	2'304
Luxembourg	5	7	0.00%	0	100.00%	5	0.00%	0	0.00%	0
Netherlands	267	280	2.25%	6	58.80%	157	14.61%	39	24.34%	65
Portugal	340	390	0.00%	0	52.06%	177	14.41%	49	33.53%	114
Spain	1'138	1'297	0.00%	0	62.92%	716	14.32%	163	22.76%	259
Sweden	369	773	0.00%	0	74.53%	275	19.51%	72	5.96%	22
Switzerland	776	1'266	0.00%	0	61.98%	481	14.18%	110	23.84%	185
United States	5'560	17'337	9.89%	550	43.78%	2'434	33.67%	1'872	12.66%	704

Abbildung 5 - Law Enforcement Requests

[18] Tabelle Lawful Access Reports



5.6 Business Continuity

Microsoft setzt für den sicheren Betrieb ihrer Microsoft 365 Cloud einerseits auf die Redundanz ihrer Datacenter, wie auch für gewisse Services auf integrierte Backup Massnahmen.

Für die Exchange Online Umgebung eines Kunden in der Schweiz sieht dies beispielsweise wie folgt aus:

Sämtliche Microsoft Exchange Daten (Mailboxdatenbanken) sind vierfach vorhanden und in den Microsoft Regionen Zürich und Genf verteilt. Dies bedeutet eine Mailboxdatenbank ist mehrfach redundant, hinsichtlich äusserer Einflüsse (Unwetter, Erdbeben etc.), wie auch im Falle eines Hardware- oder Softwareausfalles, vorhanden.

Ob und welche Workloads im Rahmen von Microsoft 365 zusätzlich mittels einer dedizierten Backuplösung gesichert werden müssen, gilt es gesondert zu prüfen.

5.7 Exit Strategie

Mit der Transformation der Services in die Cloud kommt es zu einer erhöhten Abhängigkeit zu Anbieter. Daraus entsteht das Bedürfnis eines Exit Strategie, um dieses erhöhte Risiko zu beschreiben und zu begrenzen.
Dabei gilt es jedoch folgende Punkte zu beachten:

- Eine Cloud Exit Strategie ist kein Business Continuity Plan für den Fall eines Desasters in der Cloud. Um ein solches Szenario abzudecken, wäre eine sehr komplexe und teure technische Lösung zu implementieren. Damit sind aber die nicht technischen Aspekte wie Change-Management und Betrieb diese Lösung noch nicht definiert.
- Ein Anbieter «Lock-In» gibt es auch mit on-premise Systemen. Je nach Lizenzierung und technischer Umsetzung, ist dieses Lock-In vergleichbar mit der Konstellation in der Cloud.

Ein Exit Plan beschreibt die Vorgehensweise für die Umsetzung einer Exit Strategie. Er sollte folgende Punkte beinhalten.

1. Planung und Analyse
2. Risiko Bewertung
3. Entscheiden über die Exit Strategie (Szenarienbasiert)
4. Beschreiben der neuen Plattform
5. Grober Migrationsplan
6. Exit Plan Testen
7. Exit Plan regelmässig aktualisieren
8. Und

Die Schwierigkeit eines Cloud Exit Szenarios hinsichtlich einer M365 Migration liegt vor allem auf dem Service Microsoft Teams. Dieser Service ist als on-premise Produkt seitens Microsofts nicht verfügbar. Somit wäre für die Kollaboration und Kommunikation ein alternatives Produkt im Falle einer M365 Exit Strategie zu evaluieren.

Basierend auf einem erweiterten M365 Rollout wären folgende on-premise Services die Zielplattformen im Falle einer Rückmigration:

M365 Service	onpremise Produkt
Azure AD	Active Directory
Yammer	
Teams for Conferencing and Collaboration	• Skype for Business 2019 • Klassische Filer • SharePoint 2019
Exchange Online	**Microsoft Exchange 2019**
SharePoint Online	Microsoft SharePoint 2019
OneDrive	Microsoft SharePoint 2019 Klassisches Homedrive
ToDo	
Planner	
Microsoft 365 Apps for Enterprise	Microsoft Office 2021
M365 Endpoint Manager (für mobile Devices)	Alternative MDM Lösung wie beispielsweise Ivanti MobileIron

Tabelle 4 - Cloud Exit Strategie

Eine Migration für Exchange wäre beispielsweise relativ einfach zu realisieren, aufgrund der Anforderungen der Unternnehmen wird selbst bei einem M365 Rollout eine entsprechende on-premises Infrastruktur vorhanden bleiben. Dies ist oftmals auf entsprechende Kernapplikationen zurückzuführen. Basierend auf den Erfahrungen der isolutions gibt es in grösseren Unternehmen, respektive Behörden Applikationen welche nicht hybrid, respektive Cloud fähi sind. Dadurch müssen nur entsprechende Storage & Compute Ressourcen hinzugefügt werden, bevor anschliessend eine Rückmigration der Postfächer durchgeführt werden kann.
Die Kollaboration hingegen muss auf mehrere Services aufgeteilt werden, die Dateien beispielsweise zurück nach SharePoint On-Premise oder auf klassische Laufwerke, und die Kommunikation auf einen weiteren Service. Hierzu gilt es vor allem die User Adoption vertieft zu berücksichtigen.
Basierend auf diesen Fakten lässt sich folgendes Fazit ziehen:

Eine Cloud Exit Migration ist grossmehrheitlich möglich jedoch mit extremem Aufwand verbunden, dies vor allem im Bereich der Enduser Adoption. Für Exchange Online wiederum ist die Durchführung der Exit Strategie mit angemessenen Aufwand verbunden.

6 Use Cases

Die verwendeten Klassifizierungsstufen «öffentlich», «intern», «vertraulich» und «geheim» sind ein Best Practice Vorschlag. Wenn innerhalb einer Klassifikationsstufe weitere Unterscheidungen erforderlich sind, können diese durch Sub-Labels ergänzt werden. Die Definition der Klassifizierungsstufen und damit verbundenen Schutzniveau liegt in der Verantwortung jedes Kantons und muss individuell vorgenommen werden.

Das Wichtigste in Kürze:

- Eine Klassifizierung muss von jeder Organisationseinheit vorgenommen werden.
- Um eine Klassifikation eines Dokuments sichtbar zu machen, werden diese mit einem Microsoft Sensitivity Label gekennzeichnet.
- Dokumente müssen vor der Speicherung in der Cloud gelabelt (Kennzeichnung der Klassifizierung) werden.
- Die Sensitivity Labeling-Funktionalität ist erst mit Einsatz von M365 möglich. Sofern im Vorfeld Daten in der Cloud gespeichert werden sollen, muss dies organisatorisch geregelt (Weisung) werden.

Zur Nachvollziehbarkeit der Use Cases werden die Klassifizierungsstufen beispielhaft wie folgt definiert:

Öffentlich

Als «öffentlich» gelten Informationen, die von der zuständigen Behörde zur Veröffentlichung freigegeben werden.

Eine unbeabsichtigte Offenlegung hat kein Schadenspotential.

Intern

Als «Intern» gelten Informationen, die nur von Mitarbeitenden des Kantons bzw. vertraglich gebundenen Dritten eingesehen werden dürfen. Diese beinhalten schützenswerte Inhalte, die nicht für die Öffentlichkeit vorgesehen sind.

Eine unbeabsichtigte Offenlegung hat ein niedriges Schadenspotential.

Vertraulich

Als «vertraulich» gelten Informationen, die nur von einem eingeschränkten Personenkreis eingesehen werden dürfen.

Eine unbeabsichtigte Offenlegung hat ein mittleres Schadenspotential.

Geheim

Als «geheim» gelten Informationen, die nur von einem eingeschränkten und namentlich definierten Personenkreis eingesehen werden dürfen.

Eine unbeabsichtigte Offenlegung hat ein hohes bis sehr hohes Schadenspotential.

Grundschutz von Microsoft: Data at Rest und Data in Motion sind per se schon verschlüsselt (Siehe Kapitel 5.4.1.1)

Data at Rest: Neben der Verschlüsselung auf Ebene Festplatte (Volume) verwenden Exchange Online, Microsoft Teams, SharePoint Online und OneDrive for Business auch die Dienstverschlüsselung (Service Encryption), um Kundendaten zu verschlüsseln.

Microsoft verwaltet alle kryptografischen Schlüssel (Microsoft Managed Keys), einschliesslich der Stammschlüssel für die Dienstverschlüsselung. Diese Option ist derzeit standardmässig für Exchange Online, SharePoint Online OneDrive for Business aktiviert. Alternativ kann ein Customer Key verwendet werden.

Data in Motion: Die Datenübertragung zu Microsoft erfolgt immer über HTTPS oder einer TLS-Transportschicht. Somit sind alle Datenübertragungen Client zu Server oder Server zu Server mit TLS 1.2 abgesichert. Bei SMTP werden die Daten mit STARTTLS über Port 25 abgesichert und die Datenübertragungen somit mit TLS zu M365 geschützt

Die nachfolgende Aufstellung beschreibt die durch die DVS vorgegebenen verschiedenen Use Cases, welche im Rahmen der Studie hinsichtlich ihrer unterschiedlichen Ausprägungen von Schutzmassnahmen in Abhängigkeit der Klassifizierung, geprüft werden sollen.[19]

6.1 Versand von E-Mails Intern nach Intern

Der manuelle Versand von E-Mails innerhalb der Organisation durch Mitarbeitende des Kantons.

öffentlich	Keine Schutzmassnahmen erforderlich. Als «öffentlich» klassifizierte Informationen unterliegen keinem Schutzbedarf.
intern	Standard-Schutzmassnahmen des Microsoft-Services (gem. Kapitel 5.3), sowie die kundenseitige Standard-Schutzmassnahmen (gem. Kapitel 5.4).
vertraulich	Microsoft sowie kundenseitige Standard-Schutzmassnahmen (gem. Kapitel 5.3 und 5.4) insbesondere zusätzlicher Transportverschlüsselung. Die konkreten Schutzmassnahmen müssen von jeder Organisationseinheit bzw. Dienststelle individuell geprüft werden. Bei besonders schützenswerten Personendaten[20] u.ä. ist eine zusätzliche Transport Verschlüsselung wie HIN Netzwerk oder INCA Mail zu prüfen. Die Organisationseinheit prüft Alternativen wie z.B.: • Versand per Link innerhalb einer Fachanwendung • Versand per einer Webtransferlösung

[19] Eine Klassifizierungsstufe "nicht klassifiziert" wird nicht berücksichtigt, da E-Mails und Dokumente, die versendet werden sollen, grundsätzlich mit den Stufen öffentlich, intern, vertraulich oder geheim gelabelt sein müssen.

[20] "besonders schützenswerte Personen" nach dem Schweizer Datenschutzgesetz

	• Mail-Anlage mit zusätzlicher Verschlüsselung per S/Mime (s. Vor- und Nachteile)
geheim	Microsoft sowie kundenseitige Standard-Schutzmassnahmen (gem. Kapitel 5.3 und 5.4) insbesondere zusätzlicher Transportverschlüsselung. Die konkreten Schutzmassnahmen müssen von jeder Organisationseinheit bzw. Dienststelle individuell geprüft werden. Geheime Daten sollten nicht ohne zusätzlichen Schutz in der Cloud bearbeitet werden und somit auch nicht ohne zusätzlichen Schutz per Mail verschickt. Bei besonders schützenswerten Personendaten u.ä. ist eine zusätzliche Transport Verschlüsselung wie HIN Netzwerk oder INCA Mail zu prüfen. Die Organisationseinheit prüft Alternativen wie z.B.: • Versand per Link innerhalb einer Fachanwendung • Versand per einer Webtransferlösung • Mail-Anlage mit zusätzlicher Verschlüsselung per S/Mime (s. Vor- und Nachteile)

Empfehlung:
Mittels der Technologie der «Mailtips» ist der Benutzer in der Lage zu erkennen, dass eine Mailbox in Exchange Online ist. Und darf somit Emails der Klassifizierung öffentlich und intern den entsprechenden Empfängern zukommen lassen. Für die Klassifizierung vertraulich und geheim ist dies zu prüfen. Für diesen Use Case braucht es daher andere Lösungen. Die Herausforderung bei diesem Use Case ist die entsprechende Sensibilisierung und Implementierung der organisatorischen Massnahmen.

6.2 Versand Intern nach Extern

Der manuelle Versand von E-Mails durch Mitarbeitende des Kantons an externe Empfänger.

öffentlich	Keine Schutzmassnahmen erforderlich. Als «öffentlich» klassifizierte Informationen unterliegen keinem Schutzbedarf.
intern	Standard-Schutzmassnahmen des Microsoft-Services (gem. Kapitel 5.3), sowie die kundenseitige Standard-Schutzmassnahmen (gem. Kapitel 5.4).
vertraulich	Microsoft sowie kundenseitige Standard-Schutzmassnahmen (gem. Kapitel 5.3 und 5.4) insbesondere zusätzlicher Transportverschlüsselung. Die konkreten Schutzmassnahmen müssen von jeder Organisationsheinheit bzw. Dienststelle individuell geprüft werden. Bei besonders schützenswerten Personendaten u.ä. ist eine zusätzliche Transport Verschlüsselung wie HIN Netzwerk oder INCA Mail zu prüfen.

	Die Organisationseinheit prüft Alternativen wie z.B.: • Versand per Link innerhalb einer Fachanwendung • Versand per einer Webtransferlösung • Mail-Anlage mit zusätzlicher Verschlüsselung per S/Mime (s. Vor- und Nachteile)
geheim	Microsoft sowie kundenseitige Standard-Schutzmassnahmen (gem. Kapitel 5.3 und 5.4) insbesondere zusätzlicher Transportverschlüsselung. Die konkreten Schutzmassnahmen müssen von jeder Organisationsheinheit bzw. Dienststelle individuell geprüft werden. Geheime Daten sollten nicht ohne zusätzlichen Schutz in der Cloud bearbeitet werden und somit auch nicht ohne zusätzlichen Schutz per Mail verschickt. Bei besonders schützenswerten Personendaten u.ä. ist eine zusätzliche Transport Verschlüsselung wie HIN Netzwerk oder INCA Mail zu prüfen. Die Organisationseinheit prüft Alternativen wie z.B.: • Versand per Link innerhalb einer Fachanwendung • Versand per einer Webtransferlösung • Mail-Anlage mit zusätzlicher Verschlüsselung per S/Mime (s. Vor- und Nachteile)

Empfehlung:

An diesem Use Case ändert sich grundsätzlich nichts. Emails der Klassifizierung vertraulich und geheim dürfen schon heute nicht per E-Mail versendet werden.

Generell gilt:

Eingehende E-Mail-Nachrichten können nicht kontrolliert werden. Das heisst, dass potenziell Nachrichten in Exchange Online Mailboxen der Klassifizierung vertraulich oder geheim landen könnten.

Viele der Massnahmen beruhen darauf, dass die Benutzer sich an die Vorgaben halten, welche technisch nicht durchgesetzt werden können. Dies bedeutet schlussendlich eine gewisse Risikoakzeptanz.

6.3 Manueller Versand durch Stellvertretungen

Der manuelle E-Mail-Versand durch Stellvertretungen kantonaler Mitarbeitenden.

öffentlich	Keine Schutzmassnahmen erforderlich. Als «öffentlich» klassifizierte Informationen unterliegen keinem Schutzbedarf.

intern	Standard-Schutzmassnahmen des Microsoft-Services (gem. Kapitel 5.3), sowie die kundenseitige Standard-Schutzmassnahmen (gem. Kapitel 5.4).
vertraulich	Microsoft sowie kundenseitige Standard-Schutzmassnahmen (gem. Kapitel 5.3 und 5.4) insbesondere zusätzlicher Transportverschlüsselung. Die konkreten Schutzmassnahmen müssen von jeder Organisationseinheit bzw. Dienststelle individuell geprüft werden. Bei besonders schützenswerten Personendaten u.ä. ist eine zusätzliche Transport Verschlüsselung wie HIN Netzwerk oder INCA Mail zu prüfen. Die Organisationseinheit prüft Alternativen wie z.B.: • Versand per Link innerhalb einer Fachanwendung • Versand per einer Webtransferlösung • Mail-Anlage mit zusätzlicher Verschlüsselung per S/Mime (s. Vor- und Nachteile)
geheim	Microsoft sowie kundenseitige Standard-Schutzmassnahmen (gem. Kapitel 5.3 und 5.4) insbesondere zusätzlicher Transportverschlüsselung. Die konkreten Schutzmassnahmen müssen von jeder Organisationseinheit bzw. Dienststelle individuell geprüft werden. Geheime Daten sollten nicht ohne zusätzlichen Schutz in der Cloud bearbeitet werden und somit auch nicht ohne zusätzlichen Schutz per Mail verschickt. Bei besonders schützenswerten Personendaten u.ä. ist eine zusätzliche Transport Verschlüsselung wie HIN Netzwerk oder INCA Mail zu prüfen. Die Organisationseinheit prüft Alternativen wie z.B.: • Versand per Link innerhalb einer Fachanwendung • Versand per einer Webtransferlösung • Mail-Anlage mit zusätzlicher Verschlüsselung per S/Mime (s. Vor- und Nachteile)

Empfehlung:

Dieser Use Case kann mit Technologien wie S/MIME oder Double Key Encryption nicht umgesetzt werden, da hier die Funktionalität nicht zur Verfügung steht.

Wie bei den Vorangegangenen Use Cases dürfen keine Emails mit den Klassifizierungen vertraulich und geheim versendet werden.

6.4 Versand durch Fachapplikationen

Der Versand von E-Mails durch Fachapplikationen.

öffentlich	Keine Schutzmassnahmen erforderlich. Als «öffentlich» klassifizierte Informationen unterliegen keinem Schutzbedarf.
intern	Standard-Schutzmassnahmen des Microsoft-Services (gem. Kapitel 5.3), sowie die kundenseitige Standard-Schutzmassnahmen (gem. Kapitel 5.4).
vertraulich	Microsoft sowie kundenseitige Standard-Schutzmassnahmen (gem. Kapitel 5.3 und 5.4) insbesondere zusätzlicher Transportverschlüsselung. Die konkreten Schutzmassnahmen müssen von jeder Organisationseinheit bzw. Dienststelle individuell geprüft werden. Bei besonders schützenswerten Personendaten u.ä. ist eine zusätzliche Transport Verschlüsselung wie HIN Netzwerk oder INCA Mail zu prüfen. Die Organisationseinheit prüft Alternativen wie z.B.: • Versand per Link innerhalb einer Fachanwendung • Versand per einer Webtransferlösung • Mail-Anlage mit zusätzlicher Verschlüsselung per S/Mime (s. Vor- und Nachteile)
geheim	Microsoft sowie kundenseitige Standard-Schutzmassnahmen (gem. Kapitel 5.3 und 5.4) insbesondere zusätzlicher Transportverschlüsselung. Die konkreten Schutzmassnahmen müssen von jeder Organisationseinheit bzw. Dienststelle individuell geprüft werden. Geheime Daten sollten nicht ohne zusätzlichen Schutz in der Cloud bearbeitet werden und somit auch nicht ohne zusätzlichen Schutz per Mail verschickt. Bei besonders schützenswerten Personendaten u.ä. ist eine zusätzliche Transport Verschlüsselung wie HIN Netzwerk oder INCA Mail zu prüfen. Die Organisationseinheit prüft Alternativen wie z.B.: • Versand per Link innerhalb einer Fachanwendung • Versand per einer Webtransferlösung • Mail-Anlage mit zusätzlicher Verschlüsselung per S/Mime (s. Vor- und Nachteile)

Empfehlung:

Bei der Analyse der Applikation muss geklärt werden, ob E-Mails der Klassifizierungen vertraulich oder geheim versendet werden. Ausserdem muss der Empfängerkreis analysiert werden. In diesem Falle dürfen weder die Mailbox der Fachapplikation noch die Mailboxen der Empfänger nach Exchange Online migriert werden.

6.5 Scan-to-Mail

Der Versand von gescannten Dokumenten an angegebene E-Mailadressen durch das Gerät.

öffentlich	Keine Schutzmassnahmen erforderlich. Als «öffentlich» klassifizierte Informationen unterliegen keinem Schutzbedarf.
intern	Standard-Schutzmassnahmen des Microsoft-Services (gem. Kapitel 5.3), sowie die kundenseitige Standard-Schutzmassnahmen (gem. Kapitel 5.4).
vertraulich	Microsoft sowie kundenseitige Standard-Schutzmassnahmen (gem. Kapitel 5.3 und 5.4) insbesondere zusätzlicher Transportverschlüsselung.
geheim	Microsoft sowie kundenseitige Standard-Schutzmassnahmen (gem. Kapitel 5.3 und 5.4) insbesondere zusätzlicher Transportverschlüsselung. Alternative: Scan-To-Private-Folder

Empfehlung:

Basierend auf der Klassifizierung kann entweder „Scan to Mail" oder „Scan-To-Private-Folder" benutzt werden. Die Herausforderung bei diesem Use Case ist die entsprechende Sensibilisierung und Implementierung der organisatorischen Massnahmen.

6.6 Kalendereinträge

Kalender können bei Verwendung von Microsoft Exchange Online für Personen innerhalb und ausserhalb der Organisation freigegeben werden. Aus diesem Grund ist besonders wichtig die Freigaben über die Kalenderdetails genau zu prüfen bzw. restriktiv zu halten.

öffentlich	Keine Schutzmassnahmen erforderlich. Als «öffentlich» klassifizierte Informationen unterliegen keinem Schutzbedarf.
intern	Standard-Schutzmassnahmen des Microsoft-Services (gem. Kapitel 5.3), sowie die kundenseitige Standard-Schutzmassnahmen (gem. Kapitel 5.4).
vertraulich	Vertrauliche Informationen sollen nicht als Anhang in Kalendereinträgen hinzugefügt werden. Stattdessen sollten Links zu den entsprechenden Dokumenten verwendet werden. Dadurch ist eine unbeabsichtigte Offenlegung ausgeschlossen. Zusätzlich sollte der Kalendereintrag als «privat» markiert und Kalenderberechtigungen angepasst werden, sodass Ditte keine Details des Kalendereintrags sehen können.
geheim	Geheime Informationen sollen nicht als Anhang in Kalendereinträgen hinzugefügt werden. Stattdessen sollten Links zu den entsprechenden Dokumenten verwendet werden. Dadurch ist eine unbeabsichtigte Offenlegung ausgeschlossen. Zusätzlich sollte der Kalendereintrag als «privat» markiert werden, sodass Ditte keine Details des Kalendereintrags sehen können.

Empfehlung:

Vertrauliche Informationen sollen nicht als Anhang in Kalendereinträgen hinzugefügt werden. Stattdessen sollten Links zu den entsprechenden Dokumenten verwendet werden. Dadurch ist eine unbeabsichtigte Offenlegung ausgeschlossen. Zusätzlich sollte der Kalendereintrag als «privat» markiert werden, sodass Ditte keine Details des Kalendereintrags sehen können.

6.7 Zugriff & Schutzmassnahmen

Es wurde herausgestellt, dass sowohl seitens Service Provider (Microsoft) umfassende Schutzmassnahmen vorhanden sind, als auch kundenseitig (Verwaltungsbehörde) zusätzliche Schutzmassnahmen notwendig sind, um die Informationen angemessen schützen zu können. Mit der Verwendung von Microsoft Exchange Online wird ein standardisierter Microsoft-Service verwendet, welcher mehrere Use Cases umfasst. Eine isolierte Betrachtung pro Use Case (Kapitel 6) ist aufgrund des Service-Designs, ineinandergreifender Funktionalitäten sowie gegenseitiger Abhängigkeiten mit hoher Komplexität verbunden.

Aus diesem Grund empfehlen wir eine ganzheitliche Betrachtung und Bewertung des Microsoft Exchange Online Services. Dafür ist eine erlaubte Nutzung des Exchange Online Services notwendig. Ausgangspunkt sollte die klassifizierte Information sein, welche das notwendige Schutzniveau vorgibt. Zusätzlich ist die Zugriffsart auf die Information entscheidend.

Wir unterscheiden zwischen einem Zugriff auf Informationen von einem managed Device (1) und einem und einem unmanaged Device (2).

Managed Device

Ein managed Device gehört der Behörde und steht damit vollständig unter ihrer Kontrolle. D.h. sie kann über die erlaubte Verwendung bestimmen und unerwünschtes Verhalten unterbinden. Zudem sind alle Komponenten unter ihrer Kontrolle, sodass bekannt ist, welche Applikationen installiert sind und welcher Netzwerkverkehr ermöglicht wird.

Erfolgt der Zugriff auf Exchange Online Services von einem managed Device aus, empfehlen wir für die Klassifizierungsstufen «öffentlich», «intern» die built-in Schutzmassnahmen zu verwenden, um einen angemessenen Schutz sicherzustellen.

Das bedeutet konkret:

Standard Schutzmassnahmen
Umsetzung einer technischen Klassifizierung (Labeling) der Daten Dies umfasst z.B.: • Manuelles Labeln durch Mitarbeitende • Aktivierung von Autolabeling • Ändern von Labeln unter Angabe einer Begründung
Implementierung von Data Loss Prevention Policys Dies umfasst z.B.: • Versand geheimer Informationen wird blockiert • Versand vertraulicher Informationen löst einen Freigabeworkflow aus oder verlangt eine Begründung
Backup • Sicherung der Mailboxen mit einer zusätzlichen Lösung

Device Management & Malwareschutz auf den Clients • Mobile Applikation Management • Multi-Faktor Authentisierung • Conditional Access • Monitoring des Patchings • Vulnerability Scanning • Malwareschutz
Customer Lockbox • Aktivierung der Customer Lockbox für den Microsoft Tenant
Organisatorische Regelungen: Umgang mit klassifizierten Informationen • Anwenden von Labeln • Nutzen der Scan-to-Mail Funktionalität • Informationen in Kalendereinträgen

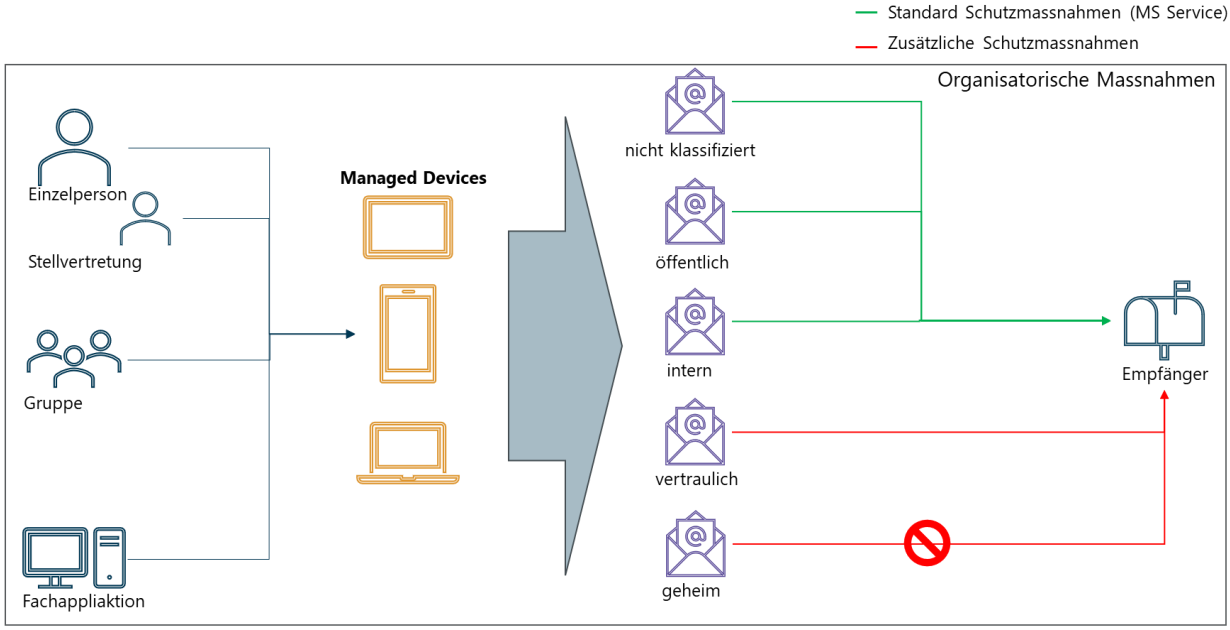
Für die Verarbeitung von «vertraulich» klassifizierter Informationen empfehlen wir zusätzlich:

Zusätzliche Schutzmassnahmen «vertraulich»
Implementierung einer zusätzlichen Verschlüsselung (Siehe 5.4.1)
Organisatorische Regelungen: Umgang mit klassifizierten Informationen

Es ist möglich, mit SeppMail Daten der Klassifizierung Vertraulich am Gateway zu verschlüsseln. Dies bedeutet jedoch, dass Emails mit dieser Klassifizierung bei einer Exchange Online Mailbox im Ordner „Gesendete Objekte“ liegen. Hier muss eine Risikoabschätzung vorgenommen werden, ob das so erlaubt ist oder nicht.

Die Verarbeitung «geheim» klassifizierte Informationen ist nicht erlaubt.

Die Grafik zeigt, welche Klassifikationsstufen bei Verwendung eines managed Device weitergehende Schutzmassnahmen zusätzlich zu den Standardmassnahmen erfordern:



*Der Empfang vertraulicher oder geheimer Informationen via Mail kann nicht ausgeschlossen werden.
*Die Freigaben über die Kalenderdetails sollten restriktiv gehalten werden. Sensitive Informationen sollten nicht als Anhang eingefügt, sondern verlinkt werden.

Vertrauliche Informationen sollen nicht in einen frei lesbaren Kalender hineingeschrieben werden oder als Dokument angehängt werden. Stattdessen sollten Links zu abgelegten Dokumenten verwendet werden, sodass die Berechtigungen zum Dokument erhalten bleiben. Sollte z.B. der Betreff bereits vertrauliche Informationen erhalten sollte zudem der Termin als «Privat» gekennzeichnet werden, sodass eine Offenlegung vertraulicher Inforationen über den Terminnamen verhindert wird.

Für die Nutzung der Scan-to-Mail Funktionalität sollten die gleichen Schutzmassnahmen implementiert werden, die für den E-Mail-Versand verwendet werden. Zusätzlich muss organisatorisch geregelt werden, dass «geheim» klassifizierte Dokumente nicht mit der Scan-to-Mail Funktion verarbeitet werden.

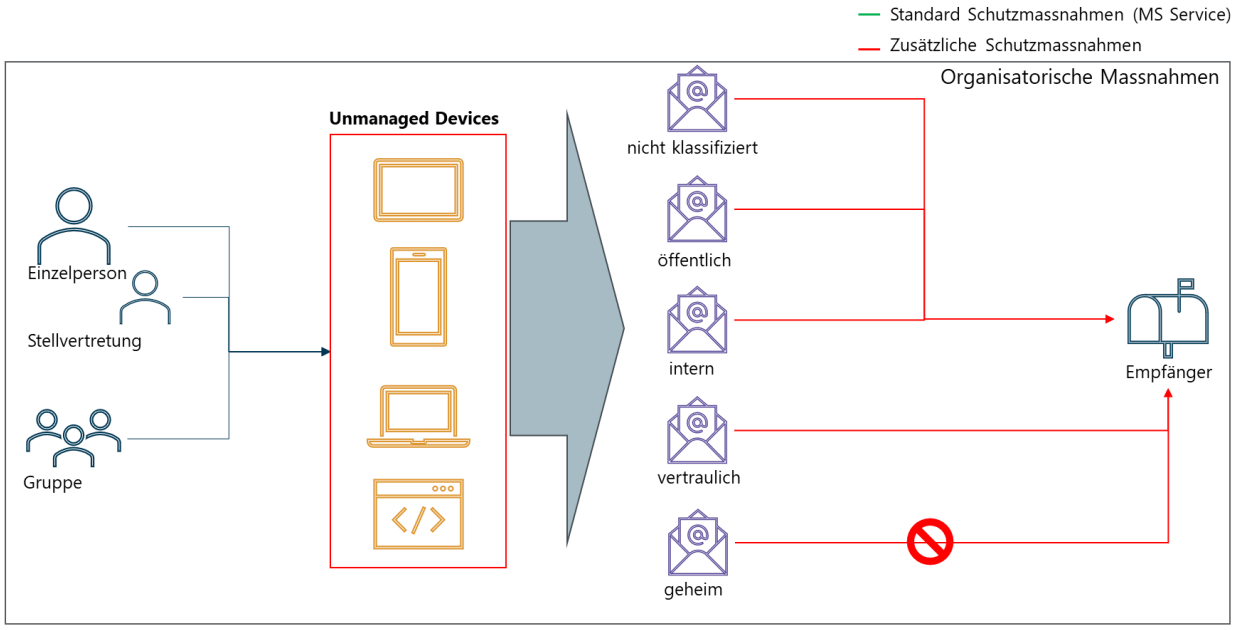
Unmanaged Device

Die Nutzung von Exchange Online ermöglicht ebenfalls den Zugriff auf E-Mails von einem, nicht durch die Behörde verwaltetem Gerät (z.B. Tablet, Smartphone). Da es sich bei unmanaged Devices in der Regel um private Geräte der Mitarbeitenden handelt, können diese nicht mit einem Device Management verwaltet werden.[21] Aus diesem Grund sollte der Zugang über ein unmanged Device mit einem Mobile Applikation Management geschützt werden. Hiermit kann dediziert die Applikation Outlook auf dem privaten Gerät verwalten. Dadurch kann ein wirksamer Zugriffsschutz gewährleistet werden und, sofern notwendig, entzogen werden, ohne dass auf das Gerät des Mitarbeitenden als Ganzes eingegriffen werden muss.

[21] Mit der Zustimmung des Mitarbeitenden kann auch ein Device Management auf privaten Geräten verwendet werden.

Ausserdem kann über ein beliebiges Gerät über den Web-Access auf die Mailbox zugegriffen werden. Um auch diesen Zugriffsweg vor unerlaubten Handlungen zu schützen, sollte eine Multi-Faktor-Authentication und Conditional Access verwendet werden.

Die Grafik zeigt, dass der Zugriff auf klassifizierte Informationen mittels unmanaged Devices mittels einem Mobile Applikation Management bzw. Multi-Faktor-Authentifikation zusätzlich geschützt wird:



*Der Empfang vertraulicher oder geheimer Informationen via Mail kann nicht ausgeschlossen werden.
*Die Freigaben über die Kalenderdetails sollten restriktiv gehalten werden. Sensitive Informationen sollten nicht als Anhang eingefügt, sondern verlinkt werden.

7 Systemübersicht

7.1 Übersicht

Microsoft 365 und damit auch Exchange Online kann als Software as a Service Dienstleistung von Microsoft bezogen werden. Um die verschiedenen Anforderungen ihrer Kunden gerecht werden zu können bietet Microsoft die Services in verschiedenen Regionen der Welt an. Für Europa beispielsweise können Kunden wählen in welchem Land ihre ruhenden Daten gespeichert werden sollen. [22]

Country	Datacenter Location
European Union	Austria (Vienna), Finland (Helsinki), France (Paris, Marseille), Ireland (Dublin), Netherlands (Amsterdam), Poland (Warsaw), (Sweden (Gävle, Sandviken, Staffanstorp)
France	Paris, Marseille
Germany	Frankfurt, Berlin
Norway	Oslo, Stavanger
Poland	Warsaw
Sweden	Gävle, Sandviken, Staffanstorp
Switzerland	Geneva, Zurich

Tabelle 5 - Datenstandorte Microsoft

Microsoft 365 wiederum umfasst zahlreiche Subservices welche wiederum die Umsetzung von definierten Use Cases vereinfachen sollen.

Abbildung 6 - Microsoft 365 Services

[22] Overview and Definitions - Microsoft 365 Enterprise | Microsoft Learn

Dabei ist die Nutzungsmöglichkeit der Services für den Kunden basierend auf der gewählten Lizenz möglich. In der untenstehenden Abbildung sind beispielsweise die Services, welche in der M365 E3 Lizenz enthalten sind, ersichtlich:

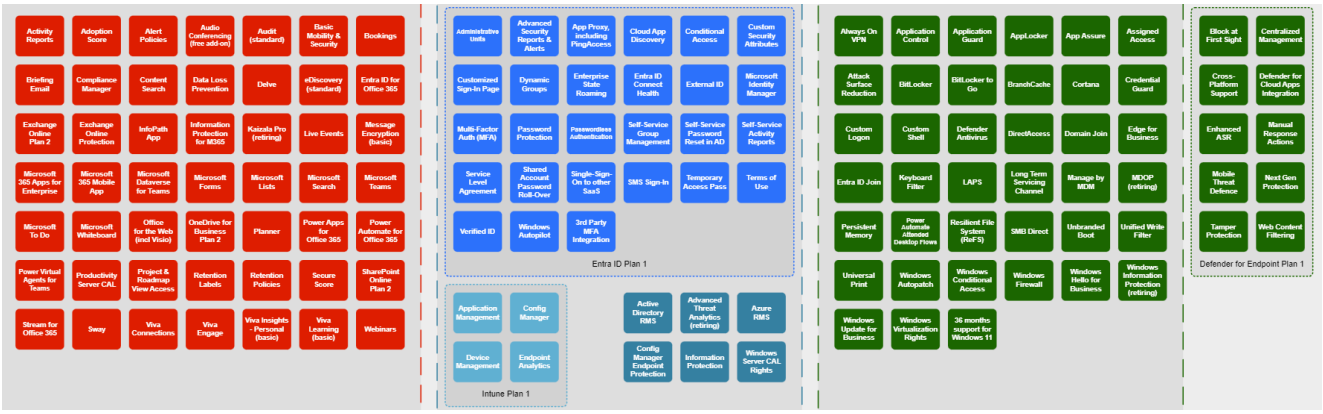


Abbildung 7 Quelle: Home | M365 Maps – Microsoft Services pro Lizenz;

Basierend auf den verfügbaren Services in M365, sowie den entsprechenden Anwendungsfällen kann Microsoft 365 entsprechend als weiteres Datacenter eines Leistungsbezügers angeschaut werden. Dies ist in der untenstehenden Grafik ebenfalls nochmals erläutert. Mit M365 werden gewisse Services aus dem on premise Datacenter durch die Cloud ergänzt, respektive ersetzt:

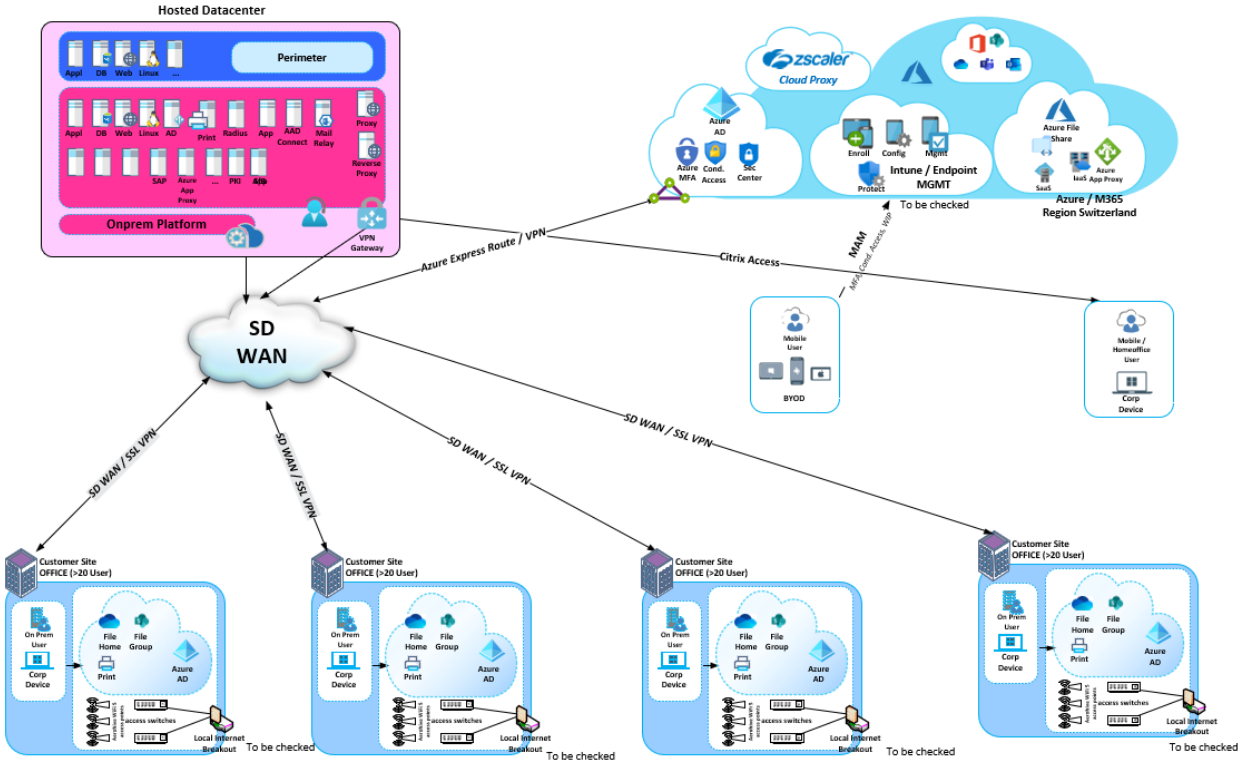


Abbildung 8 - Netzwerkdiagramm M365

7.2 Service Sicht M365 Cloud

Microsoft 365 ist eine Plattform und muss daher auch gesamtheitlich betrachtet werden. Eine Teilung der Services in Silos, welche on premise durchaus möglich ist, kann in der Cloud nur schwer umgesetzt werden. Sprich Exchange Online hat diverse Berührungspunkte mit anderen Services und entsprechende Abhängigkeiten. Im Rahmen dieser Studie liegt Exchange Online, respektive der Service E-Mail eines Leistungsbezügers im Fokus. Mit einer Einführung der Exchange hybrid / Onlineumgebung wird dieser Service entsprechend „breiter", das heisst er inkludiert nicht nur die OnPrem Komponenten, sondern auch Exchange Online Protection, Exchange Online, Defender für Office und weitere.

Wie bereits einleitend erläutert sind daher Einführungen von Microsoft 365 immer gesamtheitlich basierend auf den Anwendungsfällen, respektive dem zu erzielenden Mehrwert, zu prüfen. Nach einer erfolgten Migration hat Microsoft 365 ebenfalls starke Auswirkungen auf den IT-Betrieb eines Leistungsbezügers. Microsoft führt diverse Änderungen an der Plattform periodisch durch, welche jeweils mehrere Produkte betreffen.

Aufgrund der Komplexität des Services-E-Mail muss von einem längerfristigen Hybridbetrieb ausgegangen werden. Dies hat sowohl Vor- wie auch Nachteile zur Folge.

Domain	Vorteile	Nachteile
Projekt	Die Migration kann gestaffelt und basierend auf den Möglichkeiten erfolgen	
Betriebsorganisation	Die Migration kann in Wellen erfolgen, um die vorhandenen Ressourcen nicht zu überlasten	Der Betrieb einer Hybridinfrastruktur erhöht die Komplexität eines Betriebes.
Applikationen		Geschäftsapplikationen welche mit Exchange interagieren müssen in der Lage sein eine hybride Umgebung bedienen zu können.
Limitationen		Eine Exchange Hybridumgebung bringt gewisse Einschränkungen mit sich. (Cross Premise Berechtigungen)

Tabelle 6 - Komplexität Hybridbetrieb

7.3 Exchange Online

Da Exchange Online ein SaaS Service ist unterliegen die Einschränkungen einer stetigen Änderung und die Limitationen von Exchange Online sind hier dokumentiert: Exchange Online-Begrenzungen - Service Descriptions | Microsoft Learn

Zur Übersicht sind aber die wichtigsten Abgrenzungen untenstehend ersichtlich.

7.3.1 Mailbox-Speicherbegrenzungen

- Die Speichergrenze liegt bei 100 GB pro Postfach (User Mailbox). Zusätzlich verfügt jede Mailbox noch über ein Archiv mit 1.5TB.
- Ein gemeinsam genutztes Postfach (Shared Mailbox) mit einem Kontingent von mehr als 50 GB benötigt eine Lizenz, unter diesen 50 GB ist keine Lizenz erforderlich.

7.3.2 Empfangsgrenzen

Empfangsgrenzen gelten für die Anzahl der Nachrichten, die ein Benutzer, eine Gruppe oder ein öffentlicher Ordner pro Stunde aus allen Quellen empfangen kann. Dazu gehören Nachrichten von internen Absendern, Nachrichten aus dem Internet und Nachrichten von Servern vor Ort. Wenn das Empfangslimit für ein Postfach überschritten wurde, werden die an das Postfach gesendeten Nachrichten in einem Nichtzustellungsbericht (auch als NDR- oder Bounce-Nachricht bezeichnet) an den Absender zurückgesendet, der angibt, dass das Postfach die maximale Zustellungsgrenze überschritten hat. Nach einer Stunde wird der Grenzwert aktualisiert, und das Postfach kann wieder Nachrichten empfangen.

Empfangene Nachrichten: 3600 Nachrichten pro Stunde

7.3.3 Grenzwerte für die Übermittlung

Sendebeschränkungen gelten für die Anzahl der Empfänger, die Anzahl der Nachrichten und die Anzahl der Empfänger pro Nachricht, die ein Benutzer von seinem Exchange Online Konto senden kann.

Bei Verteilergruppen, die im Adressbuch einer Organisation gespeichert sind, wird die Gruppe als ein Empfänger gezählt. Bei Verteilergruppen, die in der Kontaktmappe eines Postfachs gespeichert sind, werden die Mitglieder der Gruppe einzeln gezählt.

Merkmal	Office 365 Unternehmen E5
Höchstsatz für Empfänger	10.000 Empfänger pro Tag
Obergrenze des Empfängers	Anpassbar an bis zu 1000 Empfänger
Begrenzung der Proxy-Adressen des Empfängers	400
Begrenzung der Nachrichtenrate	30 Nachrichten pro Minute

Tabelle 7 - Limitationen Exchange Online

7.4 Exchange Migration

7.4.1 Migrationsplan (Vorschlag):

Migrationsstrategie

Die erste Entscheidung, die bei der Planung einer Migration getroffen werden muss, ist die, wie Ihre lokalen Postfächer zu EXO migriert werden sollen. Typischerweise wird der hybride Migrationsansatz verwendet:

Andere Migrationsszenarien wie beispielsweise der Start mit einer leeren Mailbox in Exchange Online sind aus Erfahrung der isolutions aufgrund fehlender Benutzerakzeptanz keine Option.

Hybrid:

Die Best-Practice-Migrationsmethode für EXO ist hybrid. Diese Methodik erfordert Exchange Server 2016 oder 2019 als Ausgangspunkt und unterstützt die Migration von Postfächern im Laufe der Zeit. Auch wenn das Ziel einer Organisation darin besteht, alle Postfächer auf EXO zu migrieren, ist es in vielen Fällen aus verschiedenen Gründen erforderlich, die hybride Implementierung dauerhaft beizubehalten.

Durch den Einsatz der hybriden Migrationstechnologie kann ein Postfach bis zu einem Fertigstellungsgrad von 95% vorsynchronisiert werden, ohne dass dies Auswirkungen auf die Endanwenderseite hat. Daher werden alle Postfächer, die von diesem Cloud-Umzug betroffen sind, vorsynchronisiert, und der Cutover findet dann in der Nacht statt. Die genaue Anzahl der Migrationen pro Nacht, respektive der Zeitpunkt muss unter Berücksichtigung der folgenden Kriterien geplant werden:

- Kapazität des Internet-Breakouts in den entsprechenden Rechenzentren
- Kapazität der Exchange-Server vor Ort im Hinblick auf die CPU- und RAM-Auslastung
- Kapazität der Supportorganisation und anderer operativer Teams, um neu migrierte Benutzer bei Fragen zu unterstützen.
- Kapazität von Microsoft 365 - die standardmässige Drosselung könnte Auswirkungen auf den Migrationszeitplan haben.

7.4.2 Migrationsprozess pro Mailbox (highlevel)

Der Migrationsprozess auf hoher Ebene wird im folgenden Abschnitt erläutert. Die vier Hauptschritte sind die folgenden:

Vorbereitung:

In dieser Phase werden alle Abhängigkeiten für die anstehende Migrationsplanung analysiert und die entsprechende Stapelplanung durchgeführt. Ein weiterer Schritt in diesem Teil ist die Überprüfung der Grösse des gemeinsamen Postfachs, um sicherzustellen, dass eine Migration stattfinden kann oder eine Lizenzzuweisung vor der Migration erfolgt.

Ebenfalls muss festgelegt werden, welche Mailboxen nicht nach Exchange Online migriert werden sollen oder dürfen.

Vor-Migrations-Schritte:

In den Schritten vor der Migration werden die geplanten Batches für die Migration aktiviert. Die Daten der Mailbox werden nach Exchange Online synchronisiert. Zu diesem Zeitpunkt ist der Endbenutzer noch nicht betroffen.

Migration / Cutover:

In dieser Phase wird der Benutzer finalisiert und das Postfach in ein Exchange-Online-Postfach umgewandelt.

Post-Migrationsschritt:

In diesem Schritt wird der Benutzer über seine erfolgreiche Migration zu EXO informiert und die benötigten Lizenzen werden über eine IAM-Rolle zugewiesen.

Des Weiteren werden alle notwendigen Stakeholder über die Liste der migrierten Postfächer informiert.

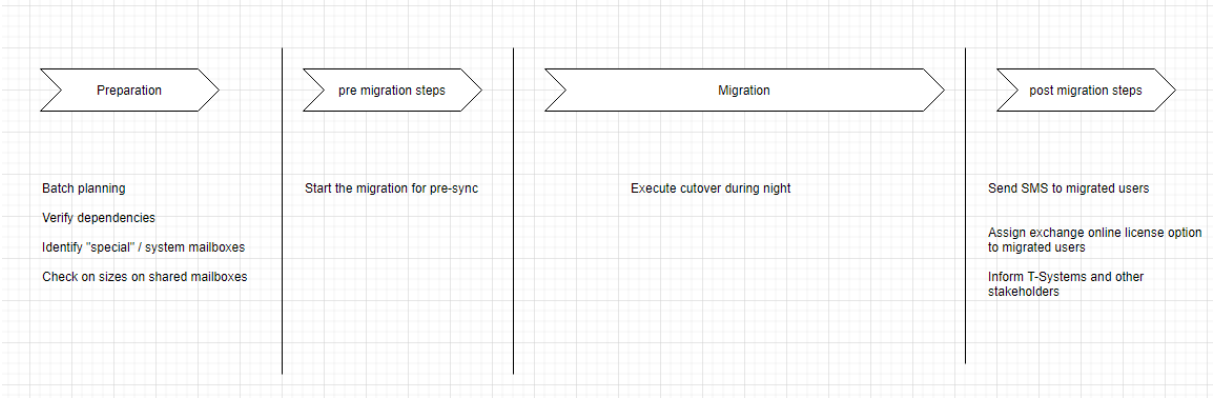


Figure 1 - Migrationsprozess

Bei der Migration wird ein Mail Tip auf der Mailbox hinterlegt, so dass die Benutzer erkennen können, dass die Mailbox in Exchange Online liegt.

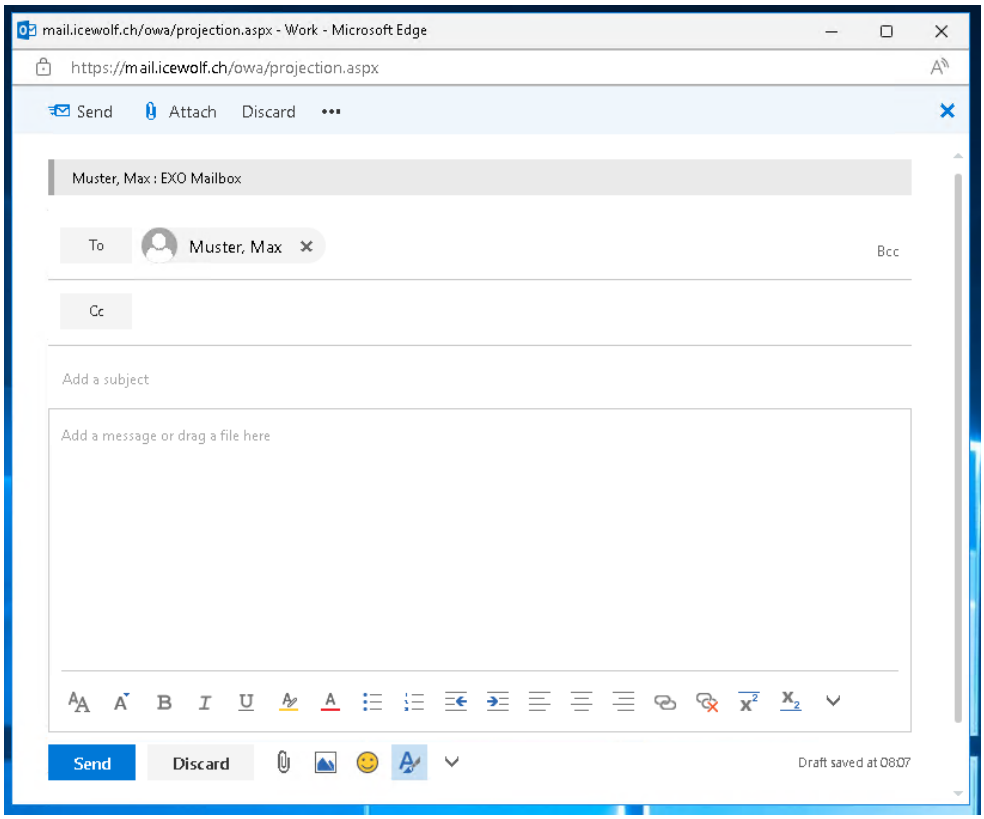


Figure 2 - Mail Tip

7.4.3 Migration process per mailbox in detail

Die folgende Abbildung zeigt den Prozess der Postfachmigration im Detail, insbesondere die in den einzelnen Phasen der Migration erforderlichen Massnahmen.

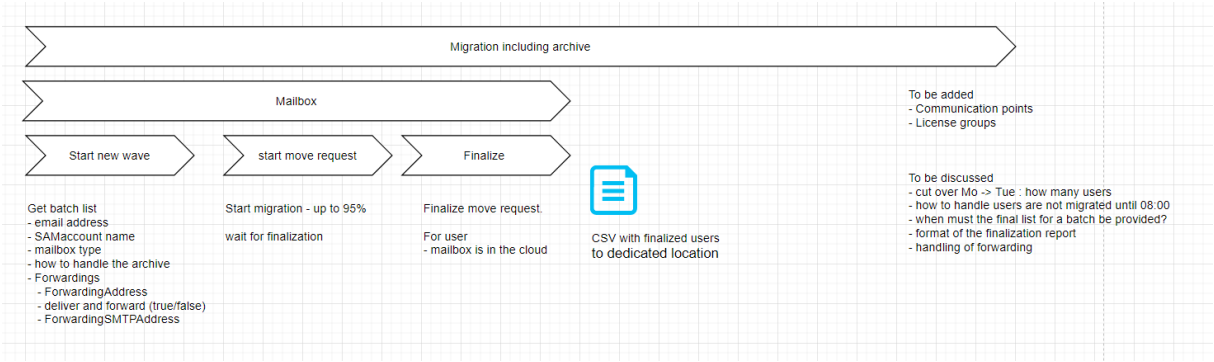


Figure 3 - Migrationsprozess im Detail

7.4.4 Migrationsabhängigkeiten sammeln

Um eine reibungslose Migrationsplanung zu gewährleisten, muss eine Reihe von Abhängigkeiten gesammelt werden, um sicherzustellen, dass alle entsprechenden Benutzer gemeinsam migriert werden, um die Auswirkungen während der Migration zu minimieren. Die folgenden Abhängigkeiten werden dabei in Erfahrung gebracht:

- Outlook Delegates (Stellvertretungen)
- Senden im Namen Berechtigungen für Postfächer
- Senden als Berechtigungen für Postfächer
- Remote-Routing-Adresse für das Postfach vorhanden

7.4.5 Sammeln von Migrationsabhängigkeiten (Schnittstellen)

Um Migrationsabhängigkeiten zu erkennen, die durch Anwendungsschnittstellen entstehen, müssen die entsprechenden Verantwortlichen vor der Batch-Planung ihre Eingaben machen.

7.4.6 Start des Migrationsbatches (Pre-Sync)

Nach der Freigabe des Migrationsbatches wird die Vorsynchronisation des Batches initialisiert. In diesem Schritt werden alle Mailboxdaten bis zu 95% der Daten mit EXO synchronisiert, um einen reibungslosen und schnellen Übergang während der Migration zu gewährleisten. Der Endbenutzer ist von diesem Vorgang nicht betroffen, daher ist die Pre-Sync-Kapazität auf die Internet-Break-Out-Kapazität und die verfügbaren HW-Ressourcen der Exchange-Server beschränkt. Um Leistungsprobleme zu vermeiden, wird der erste Pre-Sync ausserhalb der Geschäftszeiten mit maximal 200 Benutzern gestartet.

7.4.7 Mailbox-Migrations-Fallback-Szenario

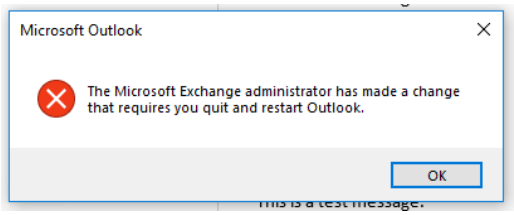
Aufgrund der verwendeten Migrationstechnologie wird die gesamte Mailbox verschoben, anstatt eine Kopie in EXO zu erstellen. Daher kann eine Fallback-Migration für einen Benutzer bis zu mehreren Stunden dauern, abhängig von der Grösse des betroffenen Postfachs. Aus diesem Grund wird eine Forward-Fixing-Strategie verwendet, was bedeutet, dass eine Fallback-Migration nach der Vervollständigung des Cutover für einen einzelnen Benutzer nicht möglich ist. Aus technischer Sicht wäre dies zwar möglich, aber aufgrund der betrieblichen Abläufe ist dieses Szenario nicht umsetzbar.

Das häufigste Problem bei der Migration ist eine fehlgeschlagene Migration einzelner Elemente, wie z. B. Kalenderberechtigungen usw. In diesem Fall kann ein detailliertes Protokoll erstellt werden, so dass die betroffenen Berechtigungen durch den Benutzer oder einen Exchange-Administrator wieder erteilt werden können.

7.4.8 Batch-Cutover der Exchange-Online-Migration

Sobald das Migrationsdatum erreicht ist und der Batch vollständig synchronisiert ist, wird der Cutover nach den Geschäftszeiten gestartet. In diesem Schritt werden die letzten 5% der Daten repliziert und der Benutzer wird in einen EXO-Postfachbenutzer umgewandelt.

Sollte ein Benutzer während dieses Prozesses Outlook geöffnet haben, wird die folgende Aufforderung angezeigt:



Wenn der Benutzer Outlook geschlossen hat, ist keine Aktivität des Benutzers erforderlich. Der Autodiscover-Dienst wird den Umzug des Postfachs erkennen und Outlook wird sich automatisch mit EXO verbinden.

Aufgrund der aktuellen Nutzung von Outlook Mobile ist kein manuelles Eingreifen erforderlich.

Sobald die Umstellung abgeschlossen ist, wird der Benutzer in Exchange on-premise als Microsoft 365-Benutzer angezeigt.

7.5 Exchange Hybrid

Die nachfolgende Abbildung zeigt eine Übersicht der Komponenten im Rahmen eines Exchange Hybrid Szenarios

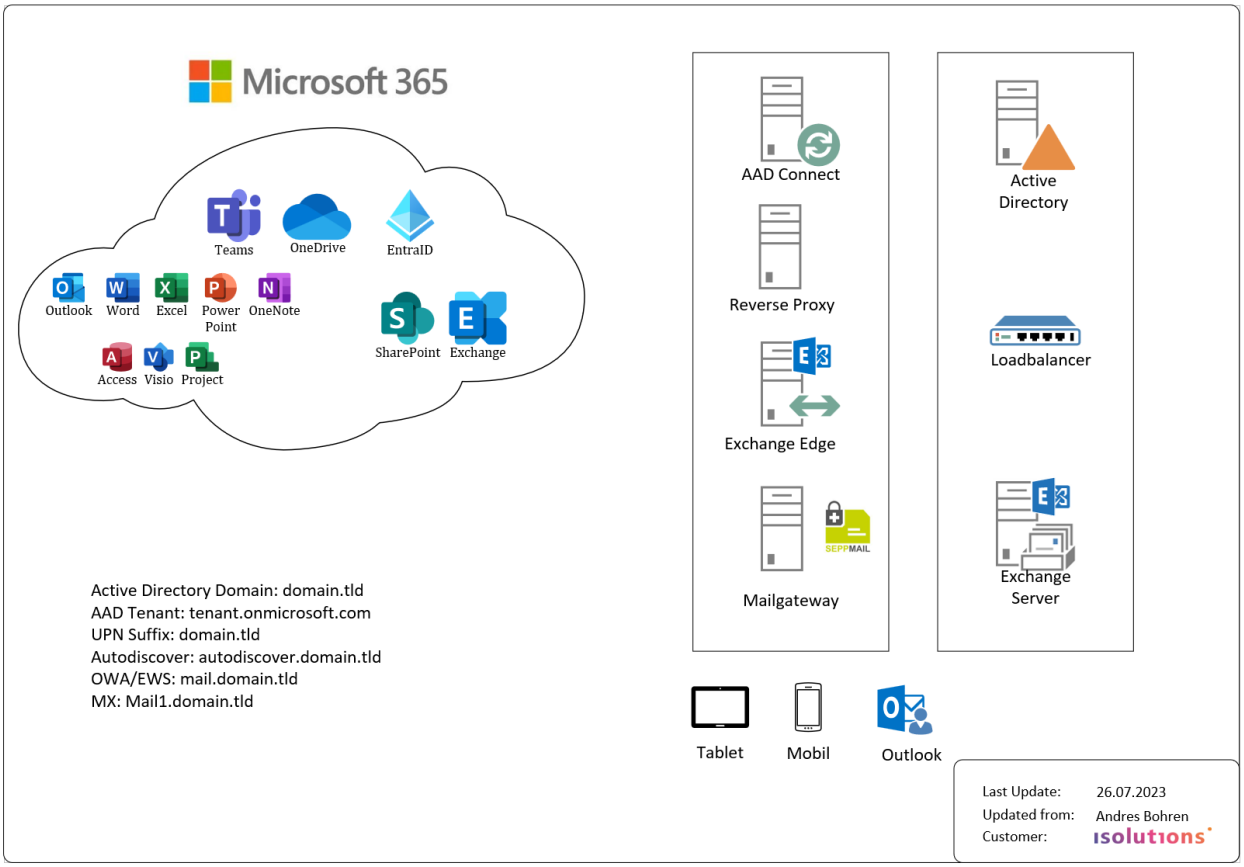


Abbildung 9 - Übersicht Exchange Hybrid

Bei Exchange Hybrid werden zwei unabhängige Exchange Organisationen (Exchange on-premise und Exchange Online) so miteinander verknüpft, dass die Benutzer kaum bemerken, dass sie zwei Exchange Organisationen angehören.

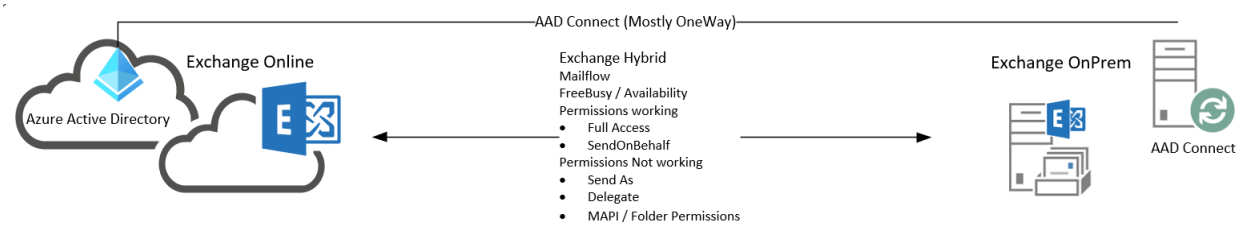


Abbildung 10 - Funktionsübersicht Hybrid

Unter Exchange Hybrid werden folgende Funktionen zusammengefasst:

- Sicheres Mailrouting mit einem gemeinsamem Addressspace *.domain.tld
- Globale Addressliste (mit gewissen Einschränkungen – da nicht alle Objekte synchronisiert werden können oder allenfalls nur in der Cloud existieren)

- FreeBusy / Availability (Verfügbarkeit für die Kalenderbuchung)
- Mailbox Berechtigungen (FullAccess / Send-As / Send On Behalf / Ordner Berechtigungen)
- Mailbox Replication Service (MRS) zum Verschieben von Postfächern zwischen den Organisationen
- Nachrichtenverfolgung (Message Trace)
- Exchange Online Archiv – Archivpostfächer können nach Exchange Online ausgelagert werden
- Exchange Hybrid ist die Grundlage für weitere Dienste, welche auf Mail oder Kalender zugreifen (Beispielsweise Microsoft Teams mit Kalenderfunktionalität)

7.5.1 Einschränkungen im Hybridbetrieb

Ein Hybridbetrieb von Exchange bringt zahlreiche Einschränkungen mit sich, welche in der Planung detailliert berücksichtigt werden müssen:

Gebiet	Einschränkung	Mitigation
Berechtigungen	Send As Berechtigungen werden cross-premise“ – also zwischen den zwei Exchange Organisationen – nicht unterstützt	Umstellung auf Send on Behalf Berechtigungen oder entsprechende Gruppierung der Mailboxen bei der Migration
Berechtigungen	Outlook Delegate Berechtigungen cross-premise“ – also zwischen den zwei Exchange Organisationen – werden nicht unterstützt	Personen mit gegenseitiger Delegation müssen gemeinsam migriert werden.
Berechtigungen	MAPI Ordnerberechtigungen cross-premise“ – also zwischen den zwei Exchange Organisationen – werden nicht unterstützt	Personen mit gegenseitiger Delegation müssen gemeinsam migriert werden
Berechtigungen	Berechtigungen in Exchange Online funktionieren nur mit MailEnabled Security Groups	Prüfen der Berechtigten Gruppen bei der Vorbereitung und Konvertierung oder ersetzen der Gruppen durch den richtigen Typ.

Authentifizierung	Basic Authentication durch Applikationen an Exchange werden nicht unterstützt	Rekonfiguration der Applikation
Umsysteme	Umsysteme welche auf Exchange Online müssen angepasst werden.	Frühzeitige Planung der Applikationen, sowie ausführliche Kommunikation.
Prozesse	Joiner- / Leaverprozesse können gegebenfalls nicht einheitlich gehandhabt werden	Frühzeitige Prozessanpassungen initialisieren.

Tabelle 8 - Einschränkungen Exchange Hybrid

7.5.2 Umsysteme

Gerade bei Umsystemen braucht es eine detaillierte Analyse mit welchen Protokollen und was für Funktionen auf Exchange zugegriffen wird.

Applikationen, welche POP3 oder IMAP4 Protokolle einsetzen, sind nicht kompatibel mit Exchange Online, da die Basic Authentication in Exchange Online für diese Protokolle nicht mehr zur Verfügung steht. Wenn bei der Applikation die Authentication auf Modern Authentication angepasst werden kann, ist es möglich die Applikation weiter zu verwenden. Meist ist dann der Aufwand, um die Abfragen auf Microsoft Graph zu portieren nicht mehr sehr hoch.

7.5.2.1 SMTP Versand

Bei einer Applikation mit SMTP-Versand, wird die Funktionalität weiterhin möglich sein. Allerdings muss geprüft werden, ob über die Applikation Daten mit Klassifizierungen versendet wird, welche nicht in der Cloud landen dürfen.

7.5.2.2 Scan to Mail

Alternativen wie Scan to Personal Folder sind zu prüfen.

7.5.2.3 Exchange Web Services

Bei Applikationen welche Exchange Web Services benutzten benötigt es eine vertiefte Analyse. Insbesondere bei Applikationen mit Impersonation muss geprüft werden, ob diese Hybridfähig gemacht werden können und Modern Authentication (Authentisierung mit Registrierter Azure AD App) unterstützen. Es ist damit zu rechnen, dass die Applikationen angepasst werden müssen – insbesondere, wenn eine längerfristige Exchange Hybrid Koexistenz vorhanden bleibt (Falls nicht alle Mailboxen in die Cloud migriert werden können). Zu prüfen ist, ob die Applikation auf Microsoft Graph Zugriffe für Exchange Online umgestellt werden kann.

Achtung: Microsoft hat kürzlich angekündigt, dass die Exchange Web Services (EWS) per 1. Oktober 2026 abgekündigt sind. Das bedeutet, dass nicht bloss die

Authentifizierung auf Modern Authentication umgestellt werden muss, sondern auch die Abfragen auf Microsoft Graph migriert werden müssen

8 Empfehlung und Ausblick

Generell gilt es zu prüfen welche Konsequenzen die Einführung von EXO hinsichtlich Mehrwerts, Risiko Akzeptanz, sowie möglicher Mitigationsmassnahmen hat.

Es wurde herausgestellt, dass sowohl seitens Service Provider (Microsoft) umfassende Schutzmassnahmen vorhanden sind, als auch kundenseitig (Verwaltungsbehörde) zusätzliche Schutzmassnahmen sichergestellt werden müssen, um die Informationen angemessen schützen zu können. Mit der Verwendung von Microsoft Exchange Online wird ein standardisierter Microsoft-Service verwendet, welcher mehrere Use Cases umfasst. Eine isolierte Betrachtung pro Use Case (Kapitel 6) ist aufgrund des Service-Designs, ineinandergreifender Funktionalitäten sowie gegenseitiger Abhängigkeiten mit hoher Komplexität verbunden.

Aus diesem Grund empfehlen wir eine ganzheitliche Betrachtung und Bewertung des Microsoft Exchange Online Services. Dafür ist eine erlaubte Nutzung des Exchange Online Services notwendig. Ausgangspunkt sollte die klassifizierte Information sein, welche das notwendige Schutzniveau vorgibt. Zusätzlich ist die Zugriffsart auf die Information entscheidend.

Dabei wird typischerweise basierend auf den spezifischen Use Cases und Anforderungen für die Verwendung der M365 Cloud Plattform eine genaue Detailspezifikation mit der jeweiligen nutzenden Organisation vorgenommen. Im Rahmen dieser Spezifikation gilt es eine gesamtheitliche Betrachtung der Office 365 Plattform mit deren Nutzen und Risiken vorzunehmen. Basierend auf den Erfahrungen von isolutions gehört Exchange Online zu den sogenannten Basisdiensten, welche weiterführenden Produkte unterstützen. Für gewisse Anwendungsfälle, respektive den Einsatz gewisser M365 Technologie, sogar eine Voraussetzung. Aus diesem Grund kann Exchange Online deshalb nicht isoliert betrachtet werden. Aus Sicht Anwendernutzen sind in erster Linie die grössere Postfächer und ein einfacherer jedoch sicherer Zugriff (mit MFA oder Managed Device) von überall her bemerkbar. Gewisse Szenarien wie Zugriffe auf Shared Mailbox und Delegate Szenarien werden mittels Exchange Online in Verbindung mit der Outlook Mobile App ermöglicht.

Aus Sicht der IT Security gibt es mehrere Aspekte beim Einsatz von Exchange Online, welche positiv zu bewerten sind. Unter anderem bietet Exchange Online moderne Authentication und unterstützt mit Ausnahme von SMTP Authentication keine legacy Authentication (Basic Authentication) mehr. Sprich eine Einführung von Exchange Online kann als Momentum genutzt werden, um die Application Security innerhalb der Applikationslandschaft erhöhen zu können.

9 Appendix A

In den nachfolgenden Kapiteln finden Sie detaillierte Informationen zu den technischen Vorbedingungen für eine Exchange Online Implementation:

9.1 Identity

Die digitale Identität ist der Schlüssel und somit ein Erfolgsfaktor bei einer Microsoft 365 Einführung. Im Rahmen von Microsoft 365 erfolgt jegliche Assoziation einer Workloads zu einem Anwender immer über dessen Identität. Im Rahmen einer M365 Einführung gilt es daher zu prüfen wie die heutigen Authentifizierungslösungen für Azure AD und die zukünftig angebundenen SaaS Services wie M365 und weitere Apps kann für die Verwendung beibehalten werden kann. Dabei gilt es die zentrale Frage nach dem Master Directory zu beantworten, sprich sollen Authentifizierungen zukünftig mehrheitlich via Azure Active Directory erfolgen?

In der folgenden Grafik ist die zentrale Rolle des Azure Active Directory für die Authentifizierung dargestellt:

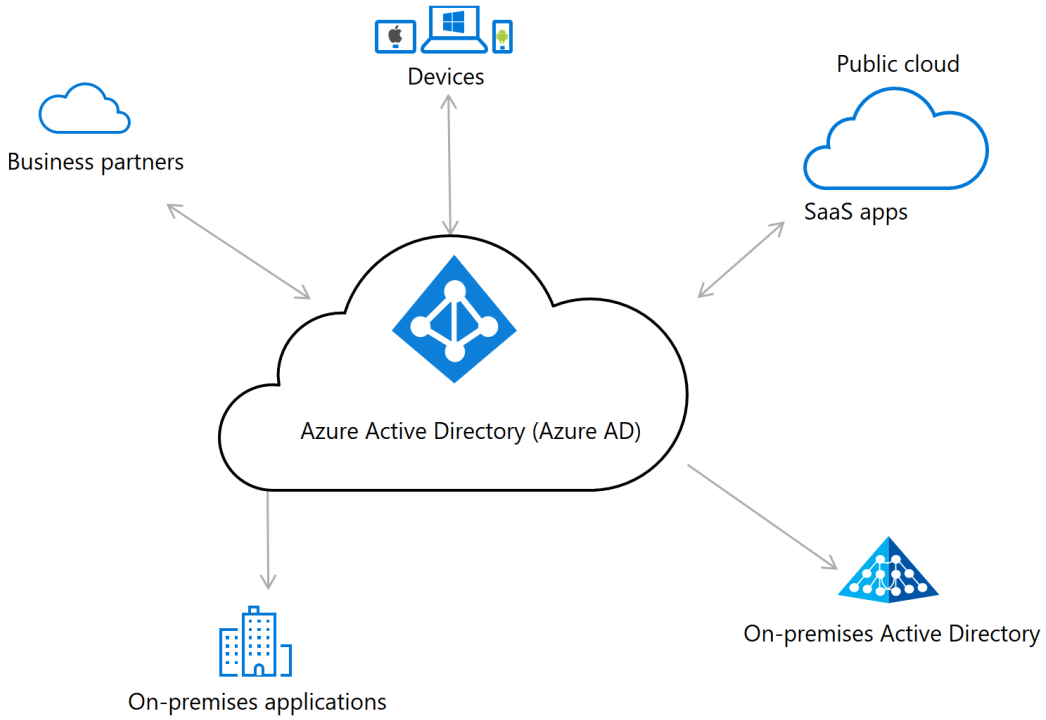


Abbildung 11 - Funktionsprinzip Azure AD

Basierend auf den Erfahrungen der isolutions aus zahlreichen Cloud Transformationen kommt den IAM Systemen ebenfalls eine enorme Bedeutung zu. Gewisse Prozesse funktionieren in der Cloud anders, respektive für gewisse Anwendungsfälle im Bereich IAM sind die Möglichkeiten von Microsoft 365, respektive Azure AD eingeschränkt.

Beispiele:

- Erstellen von Cloud Only Admin Accounts mit einer Verknüpfung zur Persona (Persona hat mehrere Accounts und wird bei Austritt in allen Systemen gelöscht)
- Privileged Identity Management (PIM): Hinzufügen und entfernen von Admi- oder CloudOnly Accounts zu PIM Rollen.

Zusätzlich kommt mit dem Einsatz von Azure Active Directory noch ein weiterer Typ Benutzerkonto hinzu. Der Einsatz von Gast Accounts (Guests) ist ein wesentlicher Vorteil um die Kollaboration zwischen verschiedenen Organisationen erhöhen zu können.

Die B2B-Zusammenarbeit ist eine Funktion von Azure AD External Identities, mit der Sie mit Benutzern und Partnern ausserhalb Ihres Unternehmens zusammenarbeiten können. Bei der B2B-Zusammenarbeit wird ein externer Benutzer eingeladen, sich mit seinen eigenen Anmeldedaten bei Ihrer Azure AD-Organisation anzumelden. Dieser Benutzer für B2B-Zusammenarbeit kann dann auf die Anwendungen und Ressourcen zugreifen, die Sie für ihn freigeben möchten. Für den Benutzer der B2B-Zusammenarbeit wird ein Benutzerobjekt im gleichen Verzeichnis wie Ihre Mitarbeiter erstellt. B2B-Collaboration-Benutzerobjekte verfügen in Ihrem Verzeichnis standardmässig über eingeschränkte Berechtigungen und können, wie Mitarbeiter verwaltet, zu Gruppen hinzugefügt werden usw. In diesem Artikel werden die Eigenschaften dieses Benutzerobjekts und die Möglichkeiten zu seiner Verwaltung beschrieben.

In der folgenden Tabelle werden Benutzer für B2B-Zusammenarbeit auf der Grundlage ihrer Authentifizierung (intern oder extern) und ihrer Beziehung zu Ihrem Unternehmen (Gast oder Mitglied) beschrieben.

		UserType property	
		Guest	**Member**
How the user authenticates	**External**	**External guest** Uses an external Azure AD account, social identity, or other external identity provider to sign in. Most external users fall into this category.	**External member** Uses an external account to authenticate but has member-level access in your organization. Common scenario in multi-tenant organizations.
	Internal	**Internal guest** Has an account in your Azure AD directory but only guest-level access in your organization. This is often a legacy guest user created before the availability of Azure AD B2B.	**Internal member** Has an account in your Azure AD directory and member-level access in your organization. Generally considered employees of your organization.

Abbildung 12 - Übersicht Benutzertypen

Bevor aber die Daten des bestehenden onpremises Active Directory nach Azure repliziert werden, gilt es die notwendigen Voraussetzungen in der Datenqualität zu schaffen. Hierbei gilt es vor allem sicherzustellen, dass der sogenannte User Principal Name (UPN) eines Benutzers seiner Mailadresse entspricht. Dies ist eine klare best practise im Rahmen einer Microsoft 365 Einführung. Die Auswirkungen einer solchen Umstellung müssen vorgängig im Rahmen eines Teilprojektes analysiert und bewertet werden.

9.1.1 Hybride Identität

Sobald die erforderliche Datenqualität vorhanden ist, kann die Datenreplizierung in Richtung Azure AD erfolgen. Dabei empfiehlt isolutions die Verwendung des sogenannten Azure AD Connect Servers. Eine grafische Abbildung der Authentifizierung und der Replikation ist nachfolgend eingefügt.

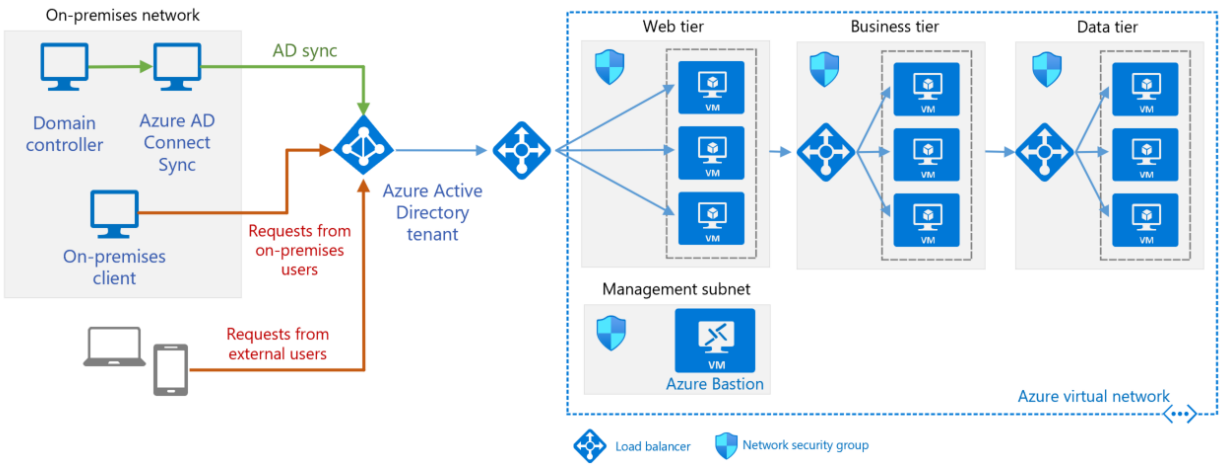


Abbildung 13 - Übersicht Hybride Identität

Für die Einführung von Microsoft 365 werden nicht alle AD Objekte in der Cloud benötigt werden. Daher empfiehlt es sich die zu Synchronisierenden Objekte zu limitieren. Dies kann über verschiedene Filter, wie Active Directory OU oder mittels zusätzliche Attribute (beispielsweise ExtensionAttribute1-15), erfolgen. Für Exchange Online ist es jedoch wichtig ist, dass alle Objekte mit einer Emailadressse synchronisiert werden. Dies ermöglicht die Bereitstellung eines vollständigen Globalen Adressbuch auch in Exchange Online.

9.1.1.1 Azure AD Connect Konfiguration

Für die einwandfreie Synchronisation der Identitäten sowie den Betrieb von Exchange Online müssen gewisse Einstellungen in der Azure AD Connect Konfiguration vorgenommen werden. Diese sind entsprechend in der nachfolgenden Abbildung dokumentiert:

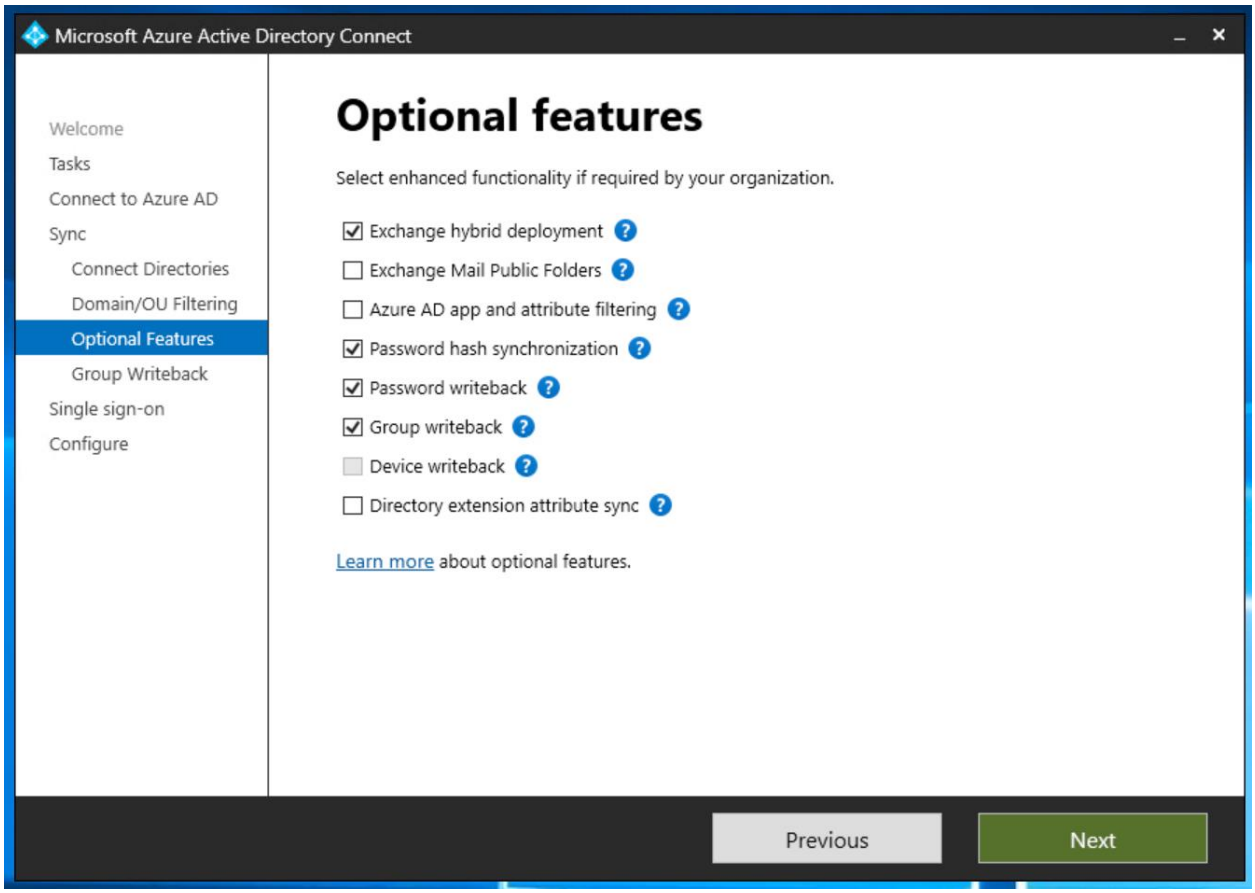


Abbildung 14 - Konfiguration Azure AD Connect

Eine detaillierte Erläuterung der entsprechenden Funktionen ist in der untenstehenden Tabelle verfügbar[23].

[23] https://learn.microsoft.com/de-de/azure/active-directory/hybrid/connect/how-to-connect-install-custom

Optionale Features	Beschreibung
Exchange-Hybridbereitstellung **(Exchange Hybrid)**	Das Feature „Exchange-Hybridbereitstellung“ unterstützt die Koexistenz lokaler und Microsoft 365-basierter Exchange-Postfächer. Azure AD Connect synchronisiert eine bestimmte Gruppe von Attributen aus Azure AD mit Ihrem lokalen Verzeichnis.
Öffentliche Exchange-E-Mail-Ordner (Mail Enabled Public Folder)	Mit dem Feature „Öffentliche Exchange-E-Mail-Ordner“ können Sie Objekte für E-Mail-aktivierte öffentliche Ordner von Ihrer lokalen Active Directory-Instanz nach Azure AD synchronisieren. Beachten Sie, dass die Synchronisierung von Gruppen, die öffentliche Ordner als Mitglieder enthalten, nicht unterstützt wird. Ein entsprechender Versuch verursacht einen Synchronisierungsfehler.
Azure AD-App- und Attributfilterung **(Azure AD app and attribute filtering)**	Mithilfe der App- und Attributfilterung von Azure AD kann die Gruppe synchronisierter Attribute individuell angepasst werden. Durch diese Option wird der Assistent um zwei weitere Konfigurationsseiten erweitert. Weitere Informationen finden Sie unter Azure AD-App- und Attributfilterung.
Kennworthashsynchronisierung **(Password hash sync)**	Wenn Sie als Anmeldelösung die Verbundoption ausgewählt haben, können Sie die Kennworthashsynchronisierung aktivieren. Anschliessend können Sie diese als Sicherungsoption verwenden. Wenn Sie die Passthrough-Authentifizierung ausgewählt haben, kann diese Option aktiviert werden, um sicherzustellen, dass Legacyclients unterstützt werden, und um eine Sicherungslösung bereitzustellen.
Kennwortrückschreiben **(Password writeback)**	Verwenden Sie diese Option, um sicherzustellen, dass Kennwortänderungen aus Azure AD in Ihr lokales Verzeichnis zurückgeschrieben werden. Weitere Informationen finden Sie unter Erste Schritte mit der Kennwortverwaltung.
Gruppenrückschreiben **(Group writeback)**	Wenn Sie Microsoft 365-Gruppen verwenden, können Sie Gruppen in der lokalen Active Directory-Instanz darstellen. Diese Option ist nur verfügbar,

	wenn Exchange in Ihrer lokalen Active Directory-Instanz enthalten ist. Weitere Informationen finden Sie unter Gruppenrückschreiben in Azure AD Connect.
Geräterückschreiben **(Device writeback)**	Verwenden Sie diese Option für Szenarien mit bedingtem Zugriff zum Rückschreiben von Geräteobjekten in Azure AD auf Ihre lokale Active Directory-Instanz. Weitere Informationen finden Sie unter Aktivieren des Geräterückschreibens in Azure AD Connect.
Verzeichniserweiterungen-Attributsynchronisierung **(Directory extension attribute sync)**	Wählen Sie diese Option aus, um bestimmte Attribute mit Azure AD zu synchronisieren. Weitere Informationen finden Sie unter Verzeichniserweiterungen.

Tabelle 9 - Funktionsbeschrieb Azure AD Features

9.1.1.2 EntraID (Azure Active Directory)

Das Produkt Microsoft Entra ID bringt gewisse Einschränkungen [24]mit sich, diese sind oftmals nur für grössere Organisationen von Bedeutung. Die entsprechenden Einschränkungen sind in der untenstehenden Tabelle dokumentiert:

Kategorie	Einschränkung
Tenants	Ein User kann maximal zu 500 Tenants als Member oder Gast angehören Maximal 300 Lizenzbasierte Abbonements pro Tenant
Domänen	5000 managed Domains 2500 Domains federated Domains
Resourcen	50'000 Azure AD Objekte bzw 300’000 Azure AD Objkete mit einer verifizierten Domäne

[24] https://learn.microsoft.com/de-de/azure/active-directory/enterprise-users/directory-service-limits-restrictions

Gruppen	Maximal 5'000 dynamische Gruppen und dynamische Verwaltungseinheiten Maximal 100 Owner einer Gruppe Bei SharePoint darf ein Benutzer maximal 2'049 Gruppen angehören
Conditional Access	Maximal 195 Richtlinien pro Tenant
Nutzungsbedingungen	Pro Tenant können maximal 40 Nutzungsbedingungen erstellt werden.

Tabelle 10 - Einschränkungen Azure Active Directory

9.1.1.3 Lizenzverwaltung (Group Based Licensing)

Bei der Verwendung von Microsoft 365 sind sämtliche Applikationen mittels Lizenz an einen User gebunden. Sprich die Verwaltung der Lizenzen ist ein Schlüsselfaktor für einen sicheren Betrieb. Die Zuweisung der Lizenzen erfolgt gemäss Best-Practice mittels Gruppenbasierte Lizenzierung (Group Based Licensing). Hierzu werden oft Azure AD Gruppen verwendet, um die Synchronisierung zwischen lokalem Active Directory und Azure Active Directory nicht abwarten zu müssen. Die genauen Prozesse müssen basierend auf den vorhanden Prozessen und Lösungen definiert werden.

9.1.1.4 Admin Accounts / Tiering

Den Konten welche über erhöhte Berechtigungen wie Adminberechtigungen verfügen kommt eine besondere Bedeutung hinzu.
Hierbei gilt es zu prüfen inwiefern bestehende Tiering Modelle einer Organisation auf die Cloud übertragen werden können. Basierend auf den Erfahrungen von isolutions gibt es best practices, jedoch sind diese oftmals nicht mit den bestehenden Konzepten einer Organisation vereinbar. Generell können aber die folgenden Empfehlungen ausgesprochen werden:

Nummer	Empfehlung
1	Benutzer mit erhöhten Rechten erhalten einen Cloud only Account. Sprich der Account wird nicht aus dem onpremises Active Directory sychronisiert.
2	Benutzer erhalten lediglich eingeschränkte Rechte auf permanenter Basis
3	Erhöhte Rechte, welche nicht dauernd benötigt werden, sind temporär zu beantragen. Dabei kann PIM verwendet werden.
4	Sämtliche Adminaccounts (ausser Notfall Accounts) sind mit MFA zu schützen.

5	Notfall Accounts sind von aller Sicherheitsvorkehrungen (wie MFA) ausgenommen.
6	Der Zugriff, sowie die Passwörter der Notfall Accounts müssen besonders geschützt und die entsprechenden Prozesse definiert sein.

Tabelle 11 - Empfehlungen Admin Rechte

Die nachfolgende Abbildung [25]zeigt ein Beispiel eines entsprechenden Tiering Modells:

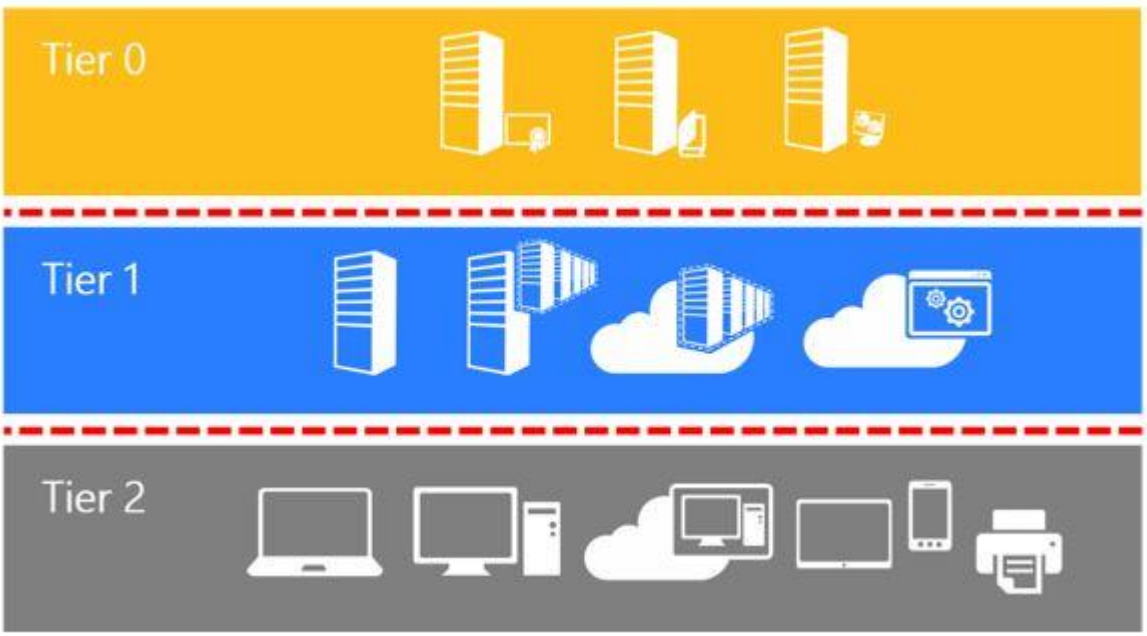


Abbildung 15 - Tiering Modell

[25] https://learn.microsoft.com/en-us/security/privileged-access-workstations/privileged-access-access-model

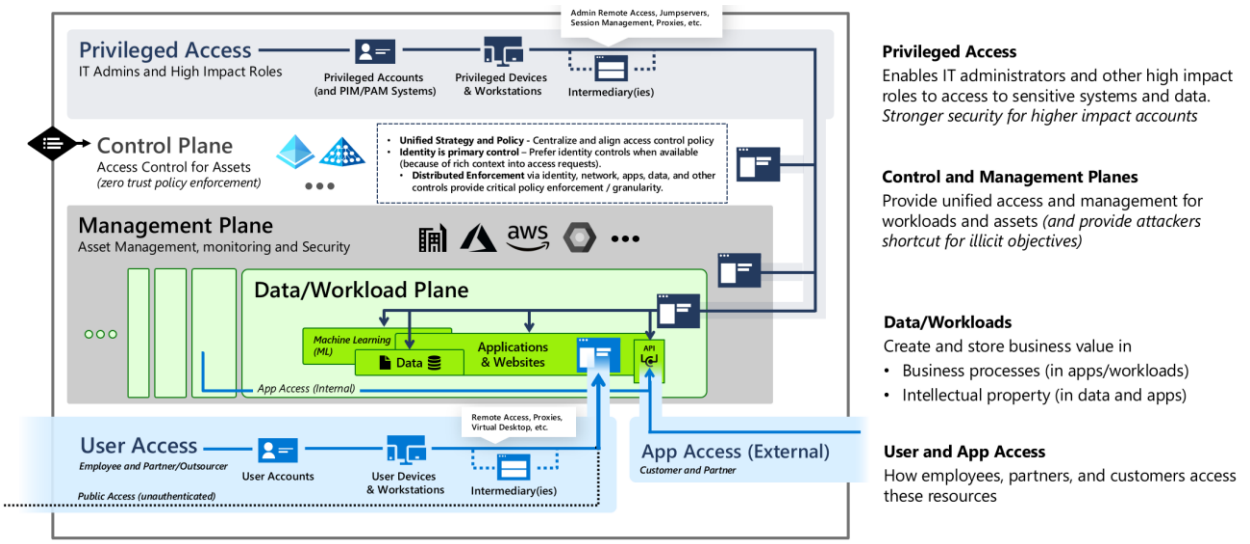


Abbildung 16 - Tiering Modell detailliert

9.1.1.5 Privileged Identity Management (PIM)

Basierend auf den Empfehlungen gemäss der obenstehenden Tabelle sind erhöhte Rechte temporär zu beantragen. Sollte die Organisation hierfür noch keinen Prozess definiert, respective eine entsprechende Toollösung betreiben, ist der Einsatz von PIM empfohlen.

Privileged Identity Management (PIM) ist ein Dienst in Azure Active Directory (Azure AD), mit dem Sie den Zugriff auf wichtige Ressourcen in Ihrem Unternehmen verwalten, steuern und überwachen können. Zu diesen Ressourcen gehören Ressourcen in Azure AD, Azure und anderen Microsoft Online Services wie Microsoft 365 oder Microsoft Intune.

Die Herausforderung bei der Implementierung dieses Prozesses, respektive der Lösung ist nicht die technische Umsetzung, sondern die Definition der entsprechenden Prozesse. Beispielsweise gilt es entsprechende Rollen zu definieren, welche Person darf welche Rechte beantragen. Weiter gilt es zu definieren ob und in welcher Ausprägung ein Approval Prozess für eine solche Anfrage nötig ist. Die folgenden Abbildungen geben einen Einblick über das Look and Feel des Produktes.

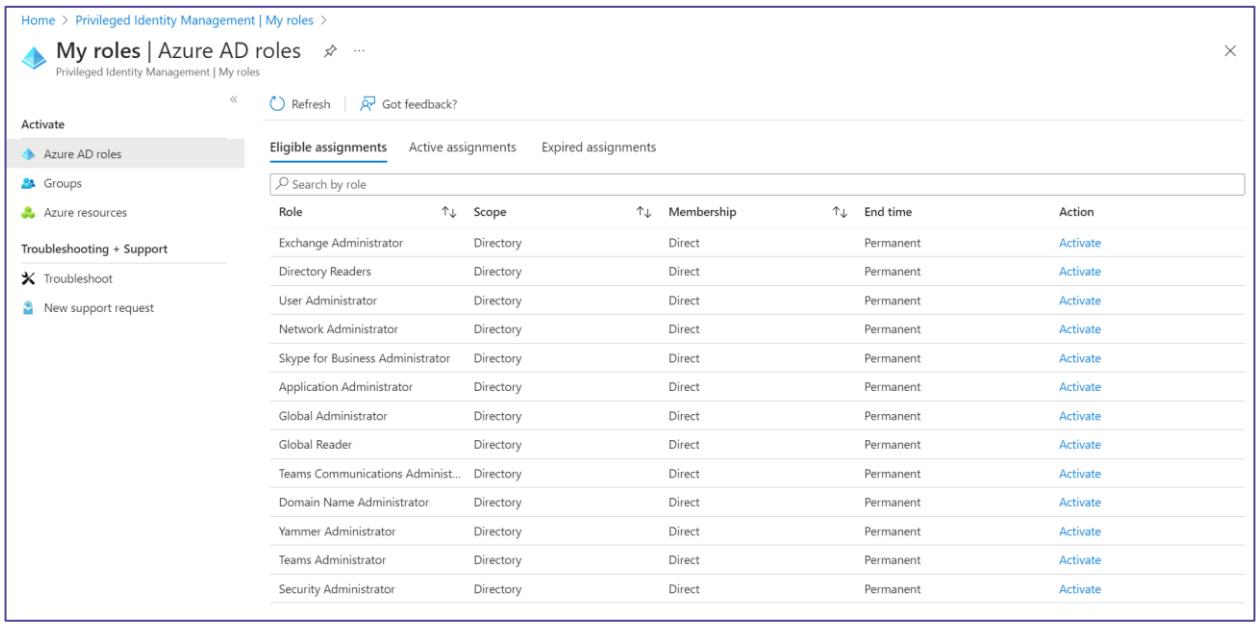


Abbildung 17 - Look and Feel PIM

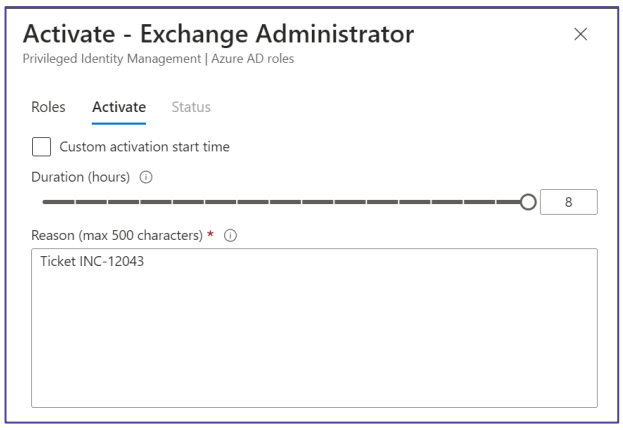


Abbildung 18 - Genehmigungsprozess PIM

9.1.2 Guest Accounts

Wie einleitend in Kapitel 7 beschrieben bieten Guest Accounts grosse Vorteile in der Kollaboration mit anderen Organisationen. Jedoch gilt es die heute für normale Benutzerkonten definierten Joiner- / Mover- / Leaver- und Auditierungsprozesse auf den neuen Benutzertyp Guest Accounts zu erweitern. Dies kann entweder mittels der vorhandenen IAM Lösungen, oder mittels Azure AD Access Review umgesetzt werden.

9.1.3 Microsoft 365 Groups

Mit der Einführung von Microsoft 365 wird ein neuer Gruppentyp eingeführt. Dies sind die sogenannten Microsoft 365 Groups.

Eine Microsoft 365 Gruppe ist eine AD Gruppe, welche mit den Microsoft 365-Tools zusammenarbeitet, die Sie bereits verwenden. Sie können mit Ihren Teamkollegen zusammenarbeiten, wenn Sie Dokumente schreiben, Tabellenkalkulationen erstellen, an Projektplänen arbeiten, Besprechungen planen oder E-Mails senden. Eine Gruppe in Microsoft 365 ermöglicht es Ihnen, eine Gruppe von Personen auszuwählen, mit denen Sie zusammenarbeiten möchten und einfach eine Sammlung von Ressourcen für diese Personen einzurichten. Ressourcen wie ein gemeinsames Outlook-Postfach, ein gemeinsamer Kalender oder eine Dokumentbibliothek zum Zusammenarbeiten an Dateien. Sie müssen sich keine Gedanken darüber machen, manuell Berechtigungen für all diese Ressourcen zuzuweisen, da das Hinzufügen von Mitgliedern zur Gruppe ihnen automatisch die Berechtigungen gibt, die sie für die von Ihrer Gruppe bereitgestellten Tools benötigen. Eine Microsoft 365 Gruppe kann aus einer Vielzahl von Tools erstellt werden, einschliesslich Outlook, Outlook im Web, Outlook Mobile, SharePoint, Planner und Teams und mehr. Welches Tool Sie zum Starten auswählen sollten, hängt davon ab, mit welcher Art von Gruppe Sie arbeiten.

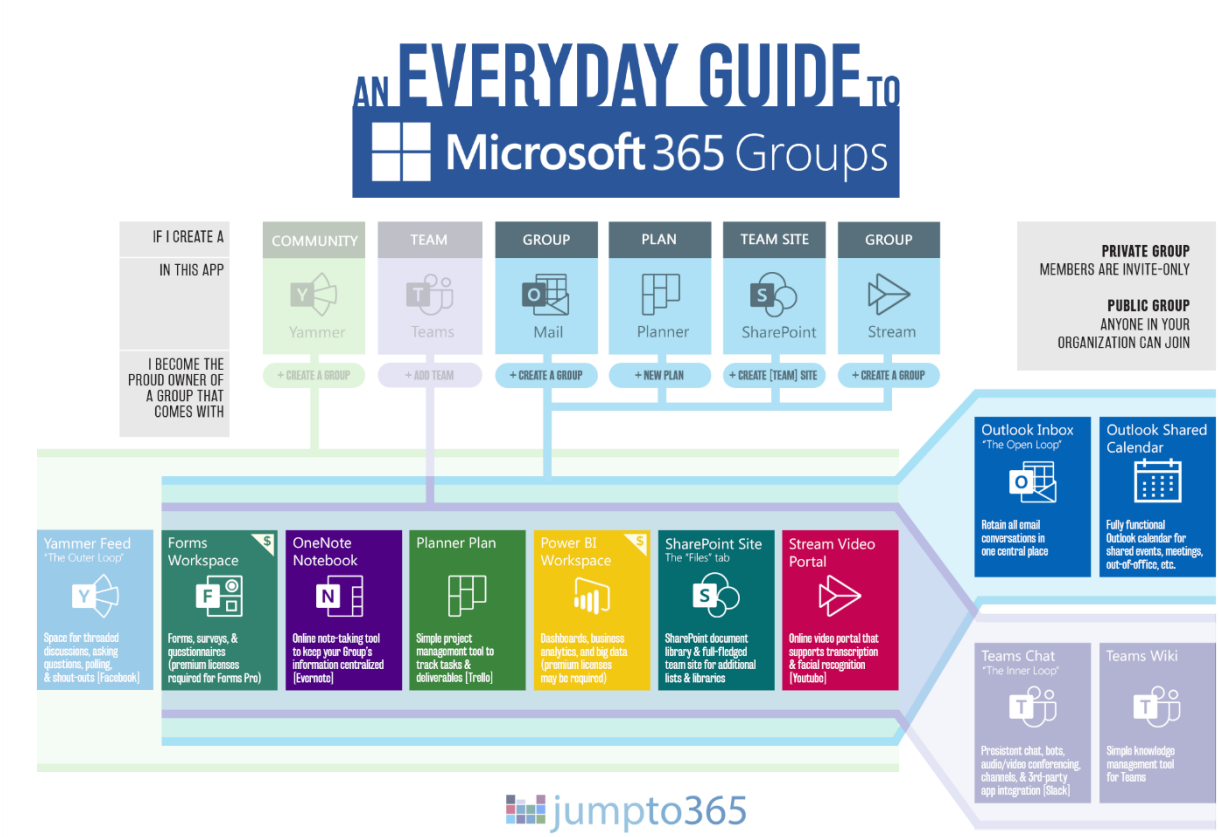


Abbildung 19 - Übersicht M365 Groups

Die Einführung dieser Gruppen bringt gewisse technische, wie organisatorische Voraussetzungen mit sich. Beispielsweise gilt es die Erstellung-, Auditierung- sowie Löschungsprozesse zu definieren. Zusätzlich gibt es auch diverse technische Voraussetzungen wie die Definition der zu verwendenden Namen und Mailadressen.

9.1.4 Multifaktor Authentifizierung (MFA)

Der Zugriff auf Microsoft 365 Ressourcen sollte grundsätzlich immer unter MFA erfolgen. Dabei können aber mehrere Eigenschaften als zusätzlicher Faktor verwendet werden, beispielsweise das Gerät eines Anwenders. Grundsätzlich empfiehlt isolutions die Umsetzung der MFA-Anforderung mittels Azure AD Conditional Access. Als Authentifizierungslösung für MFA sollte nur noch der Microsoft Authenticator verwendet werden. SMS und Telefon zwecks Bestätigung der Identität erfüllen die heutigen Anforderungen hinsichtlich Sicherheit nicht mehr. Die Implementierung von MFA ist mit einer Reise zu vergleichen und erfordert eine gewisse Maturität der Benutzer wie auch der Organisation. Daher kann die Aktivierung in verschiedenen Phasen erfolgen. Eine mögliche Reihenfolge ist in der Abbildung unten ersichtlich.

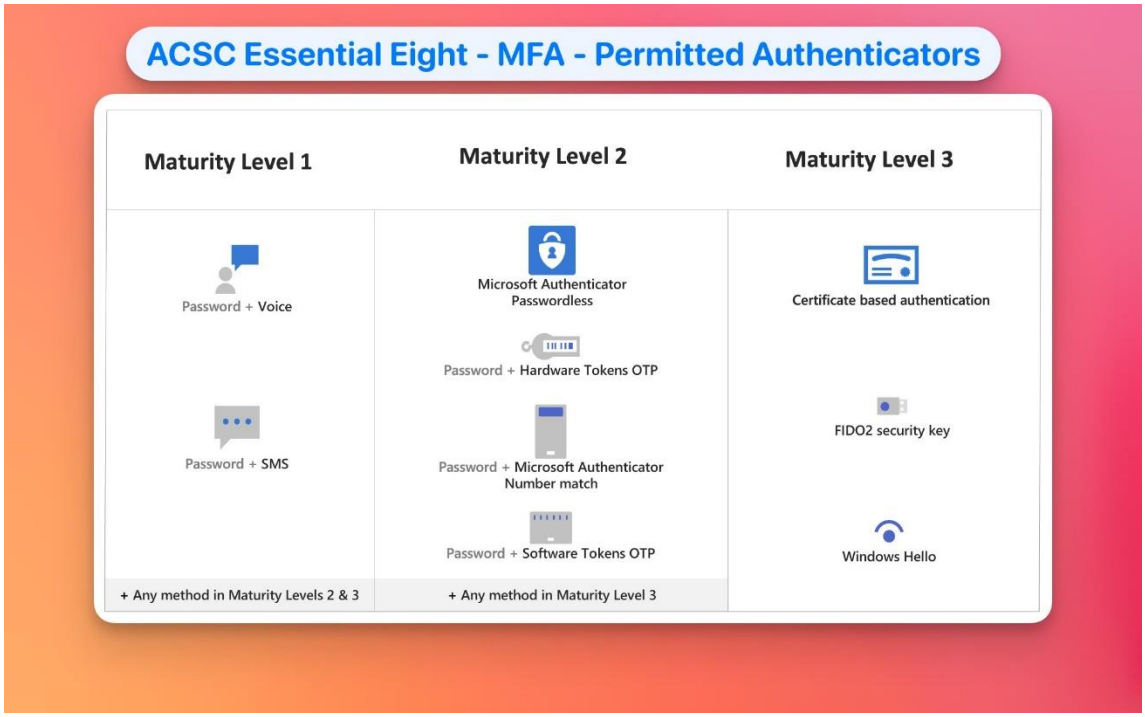


Abbildung 20 - MFA Übersicht

9.1.4.1 Conditional Access

Aufgrund der MFA Anforderung empfiehlt isolutions grundsätzlich die Implementierung von Conditional Access Regeln welche den Zugang zu M365 einschränken. Conditional Access ermöglicht basierend auf verschiedenen Faktoren den Zugriff zu erlauben, blockieren oder einzuschränken.

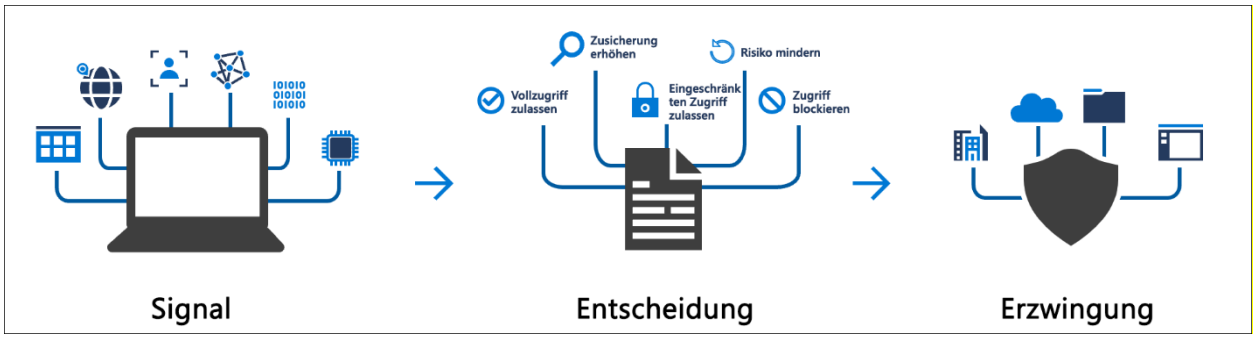


Abbildung 21 - Übersicht Conditional Access

Dabei sind folgende Szenarien denkbar:

Nummer	Zugriff	Verwendetes Gerät	Auswirkung auf Anwender
1	Outlook Zugriff auf Mailbox	Firmengerät	Anwender muss keine MFA bestätigen
2	OWA Zugriff auf Mailbox	Firmengerät	Anwender muss keine MFA bestätigen
3	Active Sync Zugriff auf Mailbox	Corporate Device	Anwender muss keine MFA bestätigen Gerät muss unter Verwaltung stehen.
4	Active Sync Zugriff auf Mailbox	Private Device	Anwender muss keine MFA bestätigen App muss unter Verwaltung stehen
5	Outlook Zugriff auf Mailbox	Privates Gerät	Zugriff ist nicht möglich
	OWA Zugriff auf Mailbox	Privates Gerät	Anwender muss MFA Request auf dem Mobile Device bestätigen.

Tabelle 12 - MFA Szenarien

Grundsätzlich werden aber die Conditional Access Regeln basierend auf der Schutzbedarfsanalyse erarbeitet und umgesetzt. Basierend auf den Erfahrungen von isolutions müssen aber BYOD Szenarien grundsätzlich definiert werden. Dabei sollte generell das Szenario des Zero Trust Prinzips gemäss untenstehender Abbildung verfolgt werden:

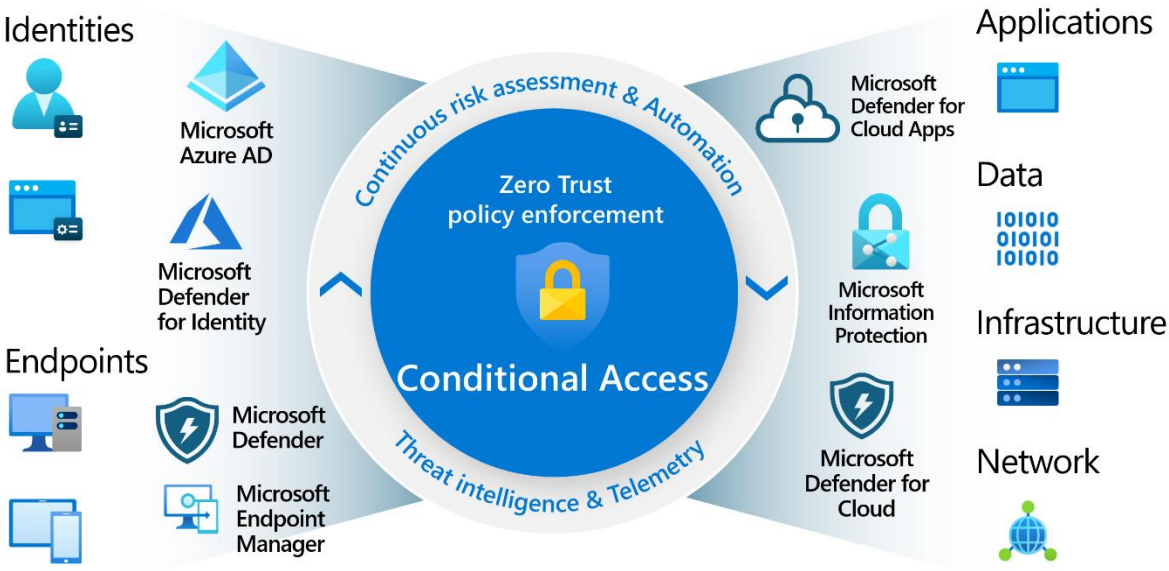


Abbildung 22 - Übersicht Zero Trust

9.2 Client

Im Rahmen einer Microsoft 365 Einführung gilt es die Arten der unterstützten Client Plattformen zu definieren. Basierend auf den Erfahrungen von isolutions können die Plattformen in die nachfolgenden Kategorien gruppiert werden.

9.2.1 Managed Client

Der managed Client ist häufig das Arbeitsgerät eines Benutzer, dies kann sowohl ein Laptop, Desktop aber auch eine VDI Arbeitsumgebung sein. Diese Clients sind heute häufig noch am Active Directory angebunden, und werden mittels einer Software Verteilung und Gruppenrichtlinien verwaltet. Für eine Einführung von Microsoft 365 müssen diese Geräte mittels Hybrid Azure AD Join dem Azure Active Directory hinzugefügt werden. Dies ermöglicht die spätere Verwendung des Gerätes als zweiten Faktor bei der Authentifizierung. Im Rahmen einer M365 Einführung werden diese Geräte zukünftig eventuell via Intune verwaltet und sind gegebenfalls nicht mehr in das lokale Active Directory eingebunden. Applikationsserver, welche mit Exchange interagieren, werden auch als Managed Clients betrachtet, und sind daher ebenfalls nach Azure AD zu synchronisieren.

9.2.2 Unmanaged Client / BYOD

Aufgrund der Funktionalität von Microsoft 365 – Zugriff von überall, zu jeder Zeit, von jedem Gerät muss eine Strategie für den Umgang von BYOD Devices (Laptops, Desktops) im Zusammenhang mit M365 erarbeitet werden. Hierbei gilt es vor allem sicherzustellen, dass Anhänge und Dateien nicht auf die entsprechenden Geräte heruntergeladen werden können. Sprich ein Zugriff von einem solchen Gerät nur auf die entsprechenden Onlinedienste durch einen Browser möglich ist. Mac Devices werden grundsätzlich als BYOD devices klassifiziert, ausser die Geräte sind im entsprechenden MDM des Unternehmens eingebunden.

9.2.3 Mobile

Für die Verwaltung der Geräte gibt es drei Szenarien (unmanaged, MDM, oder MAM). Basierend auf den Anforderungen wie auch anderer Entscheidungskriterien gibt es entsprechende Vorteile in den drei Varianten.

9.2.3.1 Unmanaged

Die Variante «unmanaged» würde bedeuten, dass die Geräte entsprechend nicht verwaltet werden und somit keine Kontrolle über Unternehmensdaten möglich wäre. Dies entspricht sicher nicht den Anforderungen.

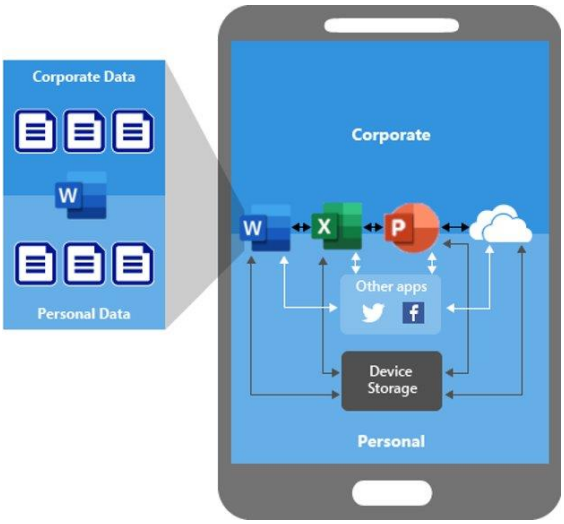


Abbildung 23 - unmanaged Mobile Device

9.2.3.2 Mobile Application Management (MAM)

Der Ansatz des Mobile Application Management wird meistens für private Geräte eingesetzt, bei welchen lediglich die entsprechenden Applikationen mit Unternehmensdaten geschützt werden. Hierfür wird beispielsweise die Authentifizierung via FaceID oder TouchID beim Öffnen der App verlangt. Weiter können Einschränkungen konfiguriert werden, welche das Kopieren von Daten aus den jeweiligen Apps verbieten. Sollte ein Mitarbeiter austreten oder das Gerät verloren gehen, können entsprechend die relevanten Daten für das Unternehmen aus der Ferne gelöscht werden.

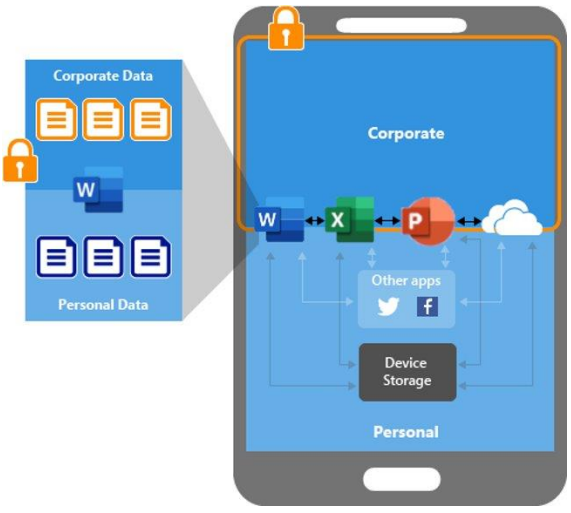


Abbildung 24 - MAM Managed Mobile Device

Bei MAM macht es meist Sinn, die Outlook Kontakte auch in die Kontakte App des Betriebssystems zu kopieren, damit nicht verwaltete Applikationen wie Telefon oder Messanger auf die Daten zugreifen können.

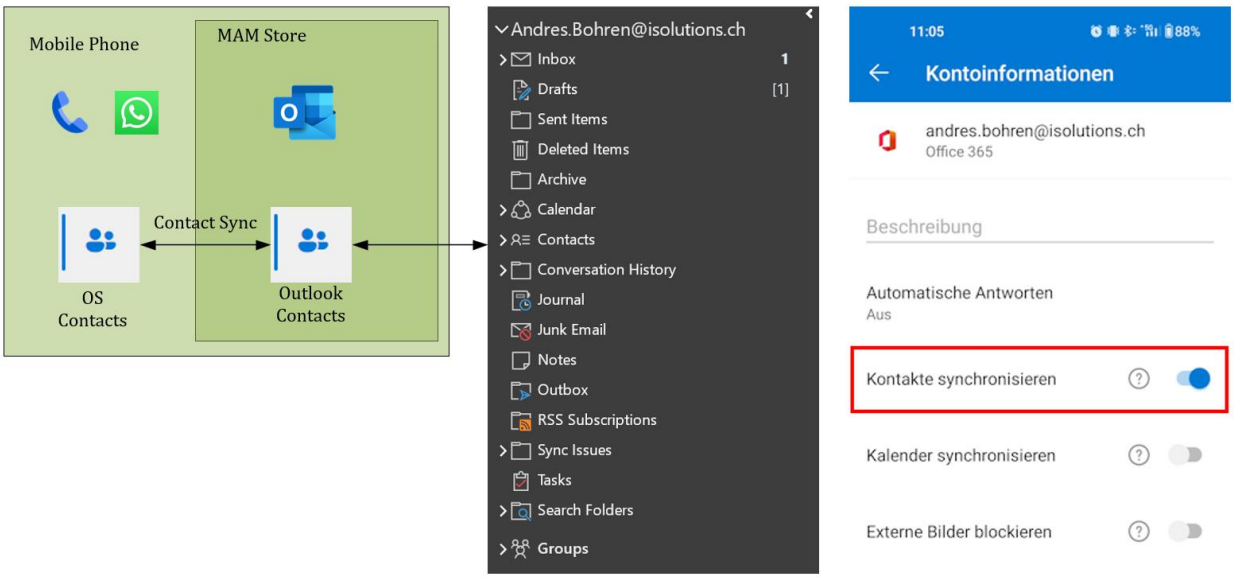


Abbildung 25 - Zusammenspiel MAM - Outlook

9.2.3.3 Mobile Device Management

Das Szenario Mobile Device Management wird im Rahmen der Erfahrung von isolutions mehrheitlich für firmeneigene Geräte verwendet, sprich das Gerät ist im Besitz der Firma und die Mitarbeiter müssen die Geräte bei Austritt retournieren. Hierbei ist die Verwaltung des gesamten Gerätes ein Szenario, welches oft gesehen wird. Beispielsweise kann es durchaus sein, dass der Zugriff auf sensitive Applikationen und Daten lediglich von solchen Geräten zulässig ist. Diese Szenarien können in Microsoft Endpoint Manager abgebildet werden oder durch Drittsysteme, welche den Hybrid Connector zu Intune unterstützen.

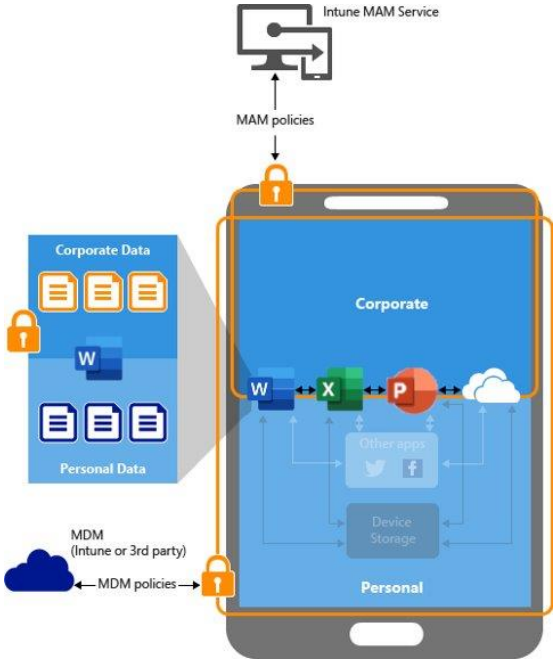
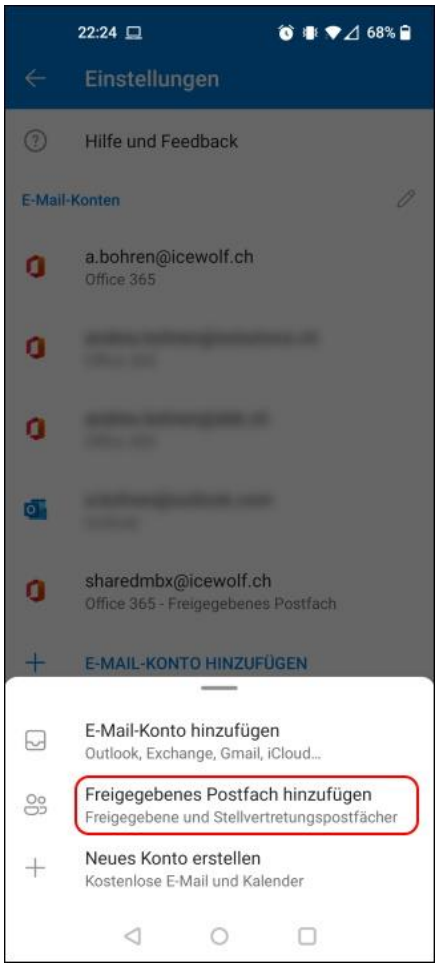


Abbildung 26 - MDM managed Mobile Device

9.2.4 Mobile Zugriff

Mit der Outlook App werden einige Szenarien unterstützt welche unter Active Sync nur mit Workarounds möglich waren. Insbesondere sind hier der Zugriff auf „Shared Mailbox“ und „Delegate“ Postfächer möglich. Diese Szenarien sind OnPrem via ActiveSync nur mit aktiviertem Account einer SharedMailbox und geteilten Passwörtern für die Shared Mailbox realisierbar. Oft wird hier bei Austritten aus dem Team das Passwort nicht gewechselt, was einen möglichen Sicherheitsverstoss nicht auschliesst.

Ausserdem werden mit der Outlook App auch Azure Information Protection (AIP) Labels unterstützt und ein modernes Synchronisatonsprotokoll auf REST Basis mit Modern Auth wird bentutzt.



9.2.5 Office Version

Ein weiteres Kernelement für den Zugriff auf die Microsoft 365 Services sind die entsprechenden Client Komponenten. Hierbei gilt es zu beachten, dass ältere Office-

Versionen für das Herstellen einer Verbindung mit Microsoft 365-Diensten nicht unterstützt werden. Beispielsweise ist ein Zugriff mit Office 2016 ab Oktober 2023 nicht mehr unterstützt. Betroffene Office-Versionen können möglicherweise weiterhin eine Verbindung mit Microsoft 365-Diensten herstellen, aber diese Konnektivität wird nicht unterstützt[26].

In der Praxis bedeutet dies, dass diese älteren Office-Versionen möglicherweise nicht alle neuesten Funktionen und Features von Microsoft 365-Diensten verwenden können. Darüber hinaus können diese älteren Versionen im Laufe der Zeit andere unerwartete Leistungs- oder Zuverlässigkeitsprobleme bei der Verwendung von Microsoft 365-Diensten auftreten. Das liegt daran, dass wir bei der Verbesserung der Microsoft 365-Dienste diese älteren Office-Versionen nicht berücksichtigen oder testen.

[26] https://learn.microsoft.com/de-de/deployoffice/endofsupport/microsoft-365-services-connectivity

9.2.6 Sensitivity Labels

Seit ein paar Monaten werden Sensitivity Labels auch für Meetings und Kalendereinträge unterstützt.

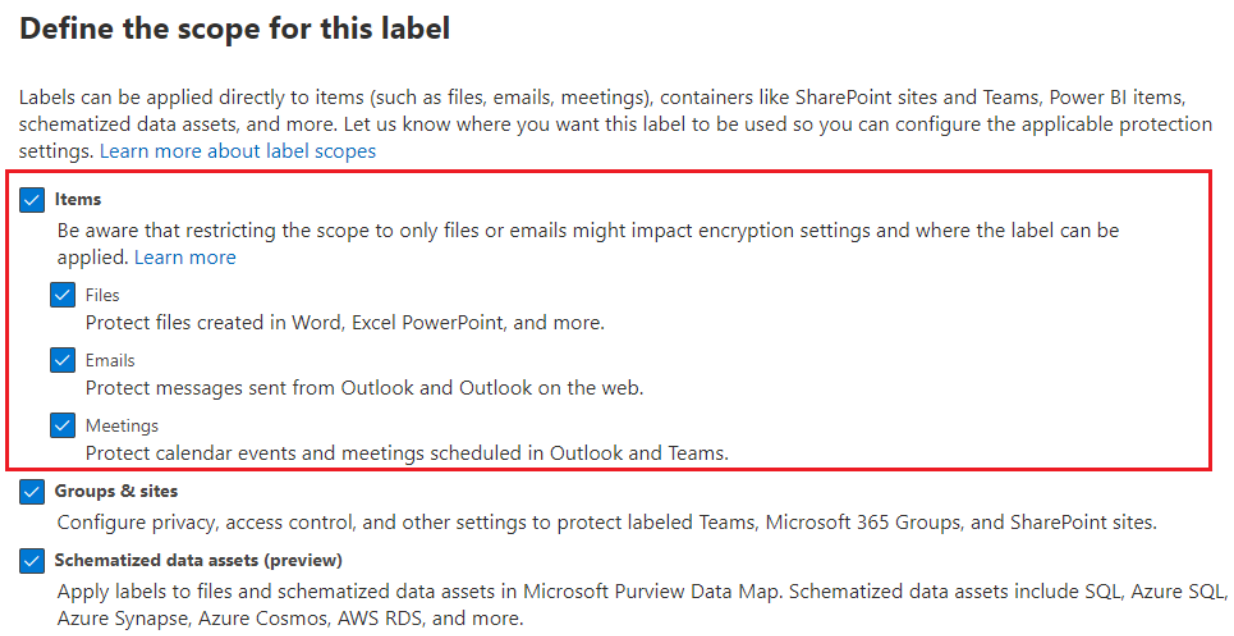


Abbildung 27 Sensitivity Labels unterstützen neu auch Meetings und Kalendereinträge

Allgemeine Limitationen:

- Das Verhindern des Kopierens des Chats weist einige Einschränkungen auf, die im Abschnitt Verhindern des Kopierens des Chats in die Beschriftungseinstellung der Zwischenablage auf dieser Seite aufgeführt sind.
- Kalenderelemente unterstützen keine Bezeichnungsverschlüsselung mit S/MIME- oder Doppelschlüsselverschlüsselung. Sie müssen die Standardverschlüsselung verwenden, die den Azure Rights Management-Dienst von Azure Information Protection verwendet, entweder mit vom Administrator definierten Berechtigungen (die Option Berechtigungen jetzt zuweisen) oder mit benutzerdefinierten Berechtigungen (die Option Benutzern das Zuweisen von Berechtigungen gestatten).
- Die automatische und empfohlene Beschriftung wird nicht unterstützt.
- iOS- und Android-Mobilgeräte unterstützen das Labeling von Kalenderelementen und Teams-Besprechungen nicht.

Outlook Limitationen

- Keine Unterstützung für lokale Postfächer; Benutzerpostfächer müssen sich in Exchange Online befinden.
- Keine Unterstützung für Einladungen zu Gruppenkalenderbesprechungen. Bei den Teilnehmern muss es sich um bestimmte Benutzer handeln.
- Wie bei gekennzeichneten und verschlüsselten E-Mails gilt: Wenn jemand eine Besprechungseinladung von einem anderen E-Mail-Client als Outlook weiterleitet, bleibt die angewendete Verschlüsselung erhalten, aber die Informationen über die Vertraulichkeitsbezeichnung werden aus den E-Mail-Kopfzeilen entfernt.
- Wenn ein mobiler E-Mail-Client eine gekennzeichnete und verschlüsselte Besprechungseinladung empfängt, wird die Einladungsnachricht inline entschlüsselt, wenn der Client verschlüsselte E-Mails unterstützt. Im Kalender kann die Einladung jedoch nicht inline entschlüsselt werden, und es wird ein Link angezeigt, über den Sie sie im Verschlüsselungsportal anzeigen können.

Freigegebene Kalender

- Wenn ein Benutzer seinen Kalender für andere Benutzer freigibt, kann nur der Kalenderbesitzer Vertraulichkeitsbezeichnungen für Besprechungen in diesem Kalender erstellen und ändern.
- Ein freigegebener Postfachkalender unterstützt das Anwenden und Ändern von Vertraulichkeitsbezeichnungen für Besprechungen nicht.

Für einen Serientermin

- Der Organisator kann eine Vertraulichkeitsbezeichnung für die Besprechungsserie anwenden, jedoch nicht auf einzelne Ereignisse.
- Ausnahmen für eine Besprechungsserie werden nur dann beschriftet (und ggf. verschlüsselt), wenn sie erstellt werden, nachdem die Bezeichnung auf die Besprechungsserie angewendet wurde. Vorhandene Ausnahmen, auch solche, die in Zukunft liegen, werden nicht gekennzeichnet.
- Wenn der Organisator den Besprechungstext oder die Anlagen für eine Besprechungsserie ändert, nachdem sie mit einer Vertraulichkeitsbezeichnung verschlüsselt wurde, werden vorhandene Ausnahmen nicht mit diesen Änderungen aktualisiert.
- Wenn der Organisator Besprechungsattribute (z. B. Startdatum, Enddatum, Ort, Besprechungstext oder Anlagen) für ein bestimmtes Vorkommen in einer Serie ändert, nachdem es mit einer Vertraulichkeitsbezeichnung verschlüsselt wurde, erstellt diese Aktion automatisch eine Ausnahme für die Serie mit derselben Bezeichnung für die Besprechungsserie.

9.2.7 Exchange Hybrid Konfiguration

Eine erfolgreiche Exchange Hybrid Konfiguration setzt folgende Anforderungen voraus:

9.2.7.1 Anforderungen

- Identitäten sind mit Azure AD Connect synchronisiert
    - Dies betrifft alle Objekte mit einer Emailadresse – damit das Globale Adressbuch die gleichen Ergebnisse liefert
- Grundsätzlich wird eine Exchange Hybridkonfiguration ab Exchange 2010 unterstützt – beachtet man jedoch den Support Lifecycle von Exchange so ist nur Exchange 2016/2019 unterstützt
- Exchange hat das letzte Cumulative Update und Update Rollup installiert
- Exchange Web Services (EWS) und Mail Replication Service (MRS) Endpunkte dürfen kein SSL Offloading haben.
- Exchange Webservices sind von Exchange Online aus mit Basic Auth Erreichbar
    - HTTPS mit öffentlichem SSL-Zertifikat (Beispiel: hybrid.domain.tld)
- Je nach Netzwerkzonen Anforderungen Exchange Edge Rolle für den SMTP Mailflow
- Separater DNS-Name für den Mailfluss zwischen Exchange OnPrem und Exchange Online (Beispiel: smtp365.domain.tld)
- Öffentliches SSL Zertifikat für den Mailfluss auf Exchange Tansport oder Edge Server (Beispiel: smtp365.domain.tld)

Limitationen

- UM Enabled Mailboxen können nicht migriert werden bzw. müssen für die Migration UM Disabled werden.

Die nachfolgende Abbildung zeigt die verschiedenen Zugriffsarten im Hybridsetup.

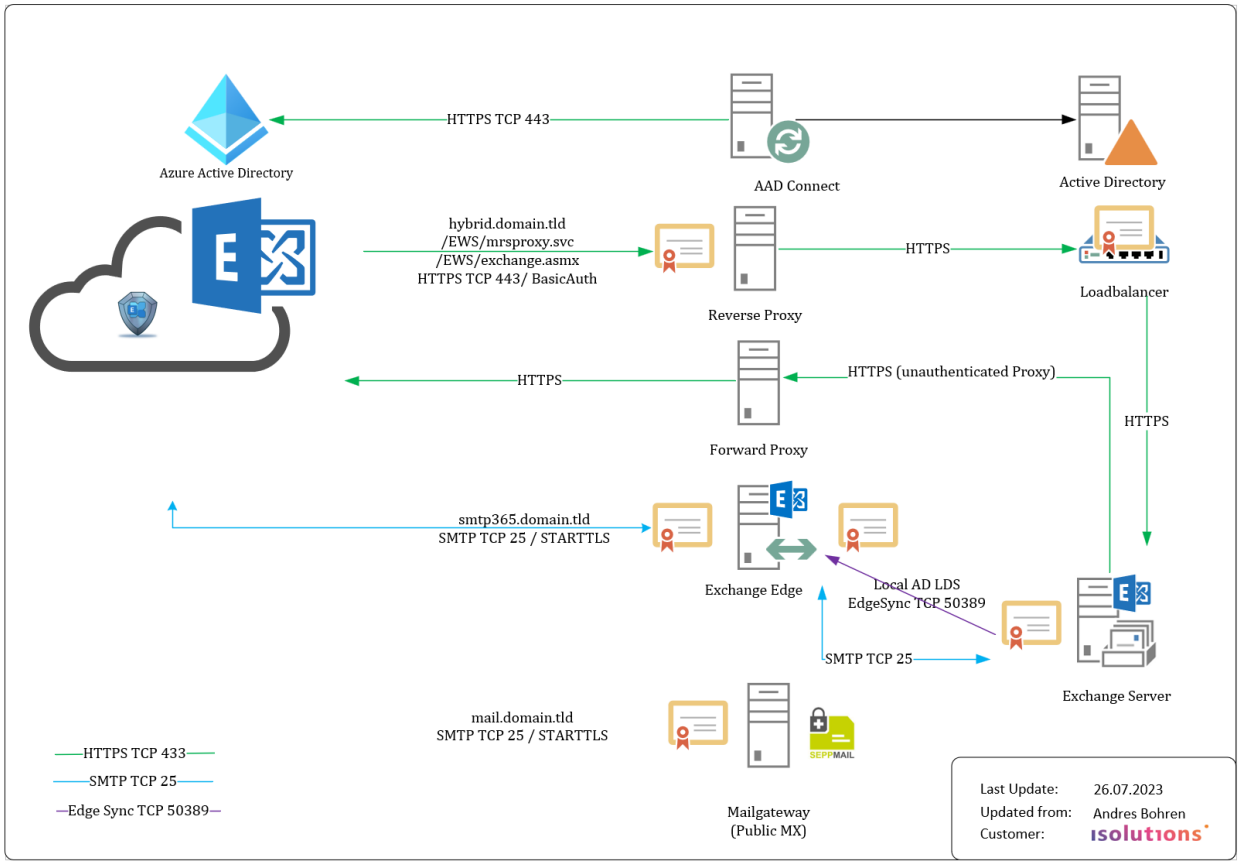


Abbildung 28 - Client Zugriffe im Hybridsetup

9.2.7.2 Classic Hybrid

Die Anforderungen für die Ausführung des Exchange Hybrid Wizards sind wie folgt:

- Autodiscover DNS Record ist im Public DNS eingetragen und zeigt auf den OnPrem Exchange (via Reverse Proxy veröffentlicht)
- Exchange Web Service (EWS) und Mail Replication Service (MRS) ist von Exchange Online aus erreichbar
- Exchange Web Service (EWS) muss über Basic Auth von Exchange Online erreichbar sein.

9.2.8 MailFlow / Centralized Mail Flow

Der Mailflow in Exchange Online kann unterschiedlich gehandhabt werden. Jedoch hat sich basierend auf den Erfahrungen der isolutions gezeigt, dass der centralized Mailflow die präferierte Lösung ist. Hierbei werden ein- und ausgehende Mails von und zum Internet über die bestehenden onpremises Komponenten geleitet. Lediglich ein weiterer Schritt, nämlich die Weiterleitung der Mail vom onpremises Exchange Server hin zur Cloud kommt hinzu. Die folgende Abbildung zeigt dies schematisch:

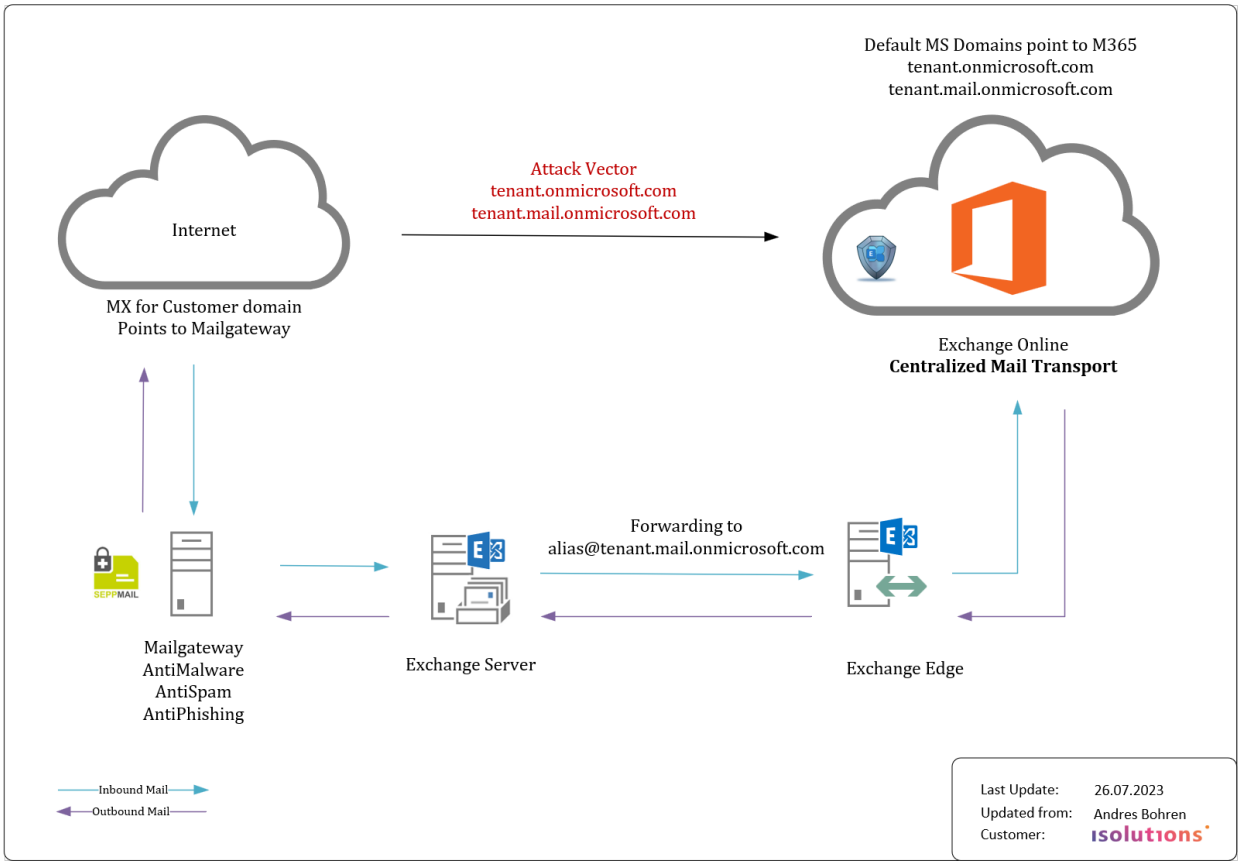


Abbildung 29 - Centralized Mailflow

Dabei gilt es aber zu berücksichtigen, dass Exchange Online standardmässig auch Mails von extern akzeptiert. Dies aus dem folgenden Grund:

Sämtliche MX Records im externen DNS für die Domains customer.mail.onmicrosoft.com und customer.onmicrosoft.com zeigen auf die Exchange Online Services. Daher akzeptiert Exchange Online auch Mails aus dem Internet für diese Adressen. Erschwerend kommt hinzu, dass jeder User aus technischen Gründen über jeweils eine sogenannte Proxyadresse (alias) der beiden Domains verfügt. Sprich sollte ein Absender die verwendeten Adressen kennen, könnten Mails vorbei an den definierten Schutzmassnahmen an die Empfänger gesendet werden. Dazu empfiehlt es sich Exchange Online so zu konfigurieren, dass Mails lediglich von den bestehenden Exchange onpremises Server angenommen werden. Hierbei gilt es aber detailliert zu prüfen ob andere M365 Dienste genau diese Adressen als Empfängeradressen verwenden (beispielsweise M365 Groups / Admin Accounts etc).

Bei Centralized Mail Transport (CMT) werden die ausgehenden Mails auch wieder über die OnPrem Infrastruktur versenden. Es gibt ein paar Ausnahmen bei Centralized Mail Transport welche hier Dokumentiert sind.

Von Centralized Mail Transport nicht unterstützte Szenarien:

- Nachrichten, welche von Exchange on-premises stammen
- Nachrichten zwischen zwei Exchange Online mailboxen
- Weiterleitungen in Exchange Online
- Nachrichten welche über eine Exchange Transport Regel (ETR) an einen spezifischen Outbound Connector weitergeleitet werden. Criteria Based Routing (CBR) hat eine höheren Wert und übersteuert deshal Centralized Mail Transport (CMT).

Aus diesen Gründen muss der SPF Eintrag um „include:spf.protection.outlook.com" erweitert werden.

9.2.9 Exchange Objekte

Im Rahmen einer Exchange Hybrid Umgebung gibt es grundsätzlich verschiedene Objekttypen welchen berücksichtig werden müssen.

Die folgende Abbildung zeigt hierbei eine Übersicht dieser Objekttypen:

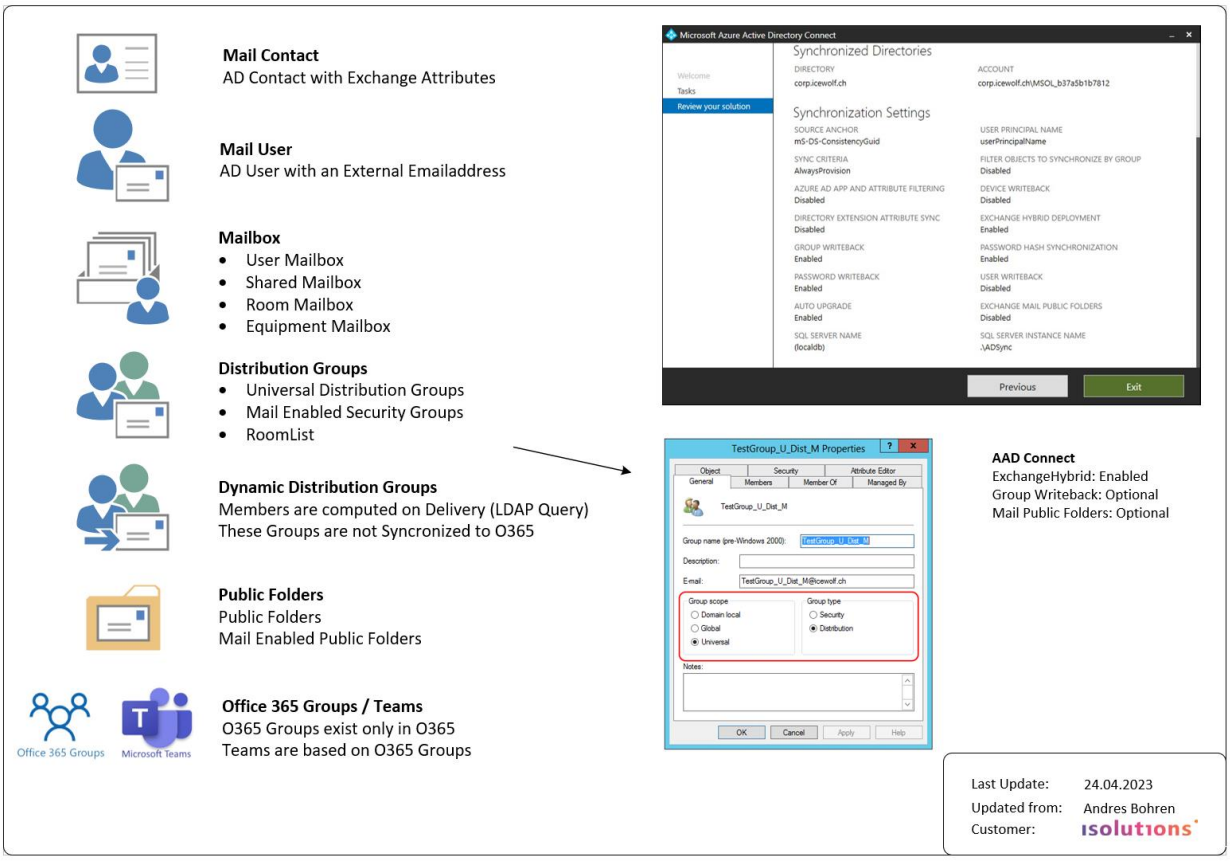


Abbildung 30 - Exchange Objekte

9.2.9.1 Mail Kontakte

Mail Kontakte (Mail Contacts) sind AD Objekte, welche im Globalen Adressbuch erscheinen, mit denen man sich jedoch nicht anmelden kann.

9.2.9.2 Mail User

Mail User sind AD User Objekte, mit denen man sich anmelden kann, haben jedoch keine Mailbox sondern eine externe Emailadresse.

9.2.9.3 Benutzer Mailboxen (User Mailbox)

Benutzer Mailboxen sind Mailboxen welche einem AD Account zugeordnet sind. Typischerweise sind dies Mitarbeiter des Unternehmens.

9.2.9.4 Geteilte Postfächer (Shared Mailbox)

Geteilte Postfächer sind Mailboxen welche durch mehrere Personen des Unternehmens gleichzeitig verwendet werden. Beispielsweise info@company.ch

9.2.9.5 Resourcenpostfächer (Room Mailbox / Equipment Mailbox)

Resourcenpostfächer sind typischerweise Mailboxen von Sitzungszimmern welche entsprechend durch die Anwender reserviert werden können. Hierzu lädt ein Anwender

einfach den gewünschten Raum zur Besprechung ein und dieser wird anschliessend als gebucht angezeigt.

9.2.9.6 Verteilerlisten / RoomLists

Verteilerlisten sind Gruppen welche wiederum verschiedene Empfänger beinhalten. Oftmals sind die alle Mitarbeiter einer Abteilung. Sprich wenn ein Vorgesetzter eine Information an alle Mitarbeiter der Abteilung versenden möchte, kann er die Verteilerliste verwenden und muss nicht alle Empfänger einzeln definieren.

9.2.9.7 Dynamische Verteilerlisten / Moderne Dynamische Verteilerlisten

Dynamische Verteilergruppen (DDGs) sind E-Mail-aktivierte Active Directory-Gruppenobjekte, die erstellt werden, um das massenhafte Senden von E-Mail-Nachrichten und anderen Informationen innerhalb einer Microsoft Exchange-Organisation zu beschleunigen. Dabei wird die Mitgliedschaft basierend auf diversen Kriterien – sogenannten Filtern – festgelegt. Im Rahmen eines hybriden Setups gilt es zu beachten ,dass dynamische Verteilerlisten nicht von Azure AD Connect nach Azure AD synchronisiert und im Globalen Addressbuch angezeigt werden.

Daher müssen im Falle einer Exchange Online Migration die dynamischen Verteilerlisten angepasst werden, damit die Cloud Mailboxen ebenfalls berücksichtigt werden.

Es gibt hier zwei Lösungsansätze:

- Ein Kontaktobjekt in Exchange Online anlegen, welches auf die Dynamische Verteilerliste in Exchange OnPrem verweist
- Ein Kontaktobjekt in Exchange OnPrem, welches auf die Dynamische Verteilerliste in Exchange Online verweist.

Welche der beiden Varianten Sinn macht, kommt darauf an, wo sich die meisten Empfänger Mailboxen der dynamischen Verteilerlisten befinden.

9.2.9.8 Public Folder

Basierend auf den Erfahrungen von isolutions sollte eine moderne Exchange Architektur keine Public Folder mehr beinhalten. Die Anwendungsfälle aus der Vergangenheit können heute mittels neuer Technologien, wie Shared Mailboxes, M365 Groups etc. umgesetzt werden.

Daher empfiehlt es sich allfällige Public Folder vor einer Migration zu bereinigen.

10 Appendix B - Input Microsoft

Kapitel	Input
2.1.1Ausgangslage Exchange on premise	Aus Zero Trust perspektive ist, das Netzwerk ist keine allumfassende Security Boundary.
2.1.2 Exchange in der Cloud	Sensitive Daten müssen geschützt werden, egal wo sie onprem oder in der Cloud oder auf einem USB-Stick sind. Cloud Act ist die US-Variante des "Lawful Access", wir empfehlen nur diesen Begriff zu nehmen
4 Kritische Erfolgsfaktoren	Die Zahl ist zu hoch, zu dem sind die verschiedenen Arten von Changes zu Berücksichtigen, nicht alle betreffen z.b. die Enduser und auch nicht alle müssen/können getestet werden.
5.3.6 Lieferantensicherheit	Bei M365 spezifisch sind es sehr wenige Partner. Weiter ist mit EU Boundary eine Reduktion der Subcontractor geplant.
5.4.6 Device Management inkl. Malwareschutz	Themen Device Managmenet und Applikcation Management werden vermischt.
6 Use Cases	Die Klassifizierung hat keinen direkten Zusammenhang mit der Nutzung von Cloud Services
6.5 Scan-to-Mail	Scan-to-"irgendwas" darf für geheime Dokumente nicht verwendet werden, weil sie immer, auch on prem verschlüsselt sein müssen und daher auch der scan to private folder nicht sicher genug wäre.
Error! **Reference source not found.** Error! **Reference source not found.**	Autolabeling nutzt den sog. "DCS data classification service", ein cloud-basierter Dienst der Teile des Dokuments analysiert, um die Klassifikation vorzuschlagen bzw. durchzuführen. Zudem könnte es herausfordern ein, öffentlich&intern automatisiert zu erkennen... ein Default Labeling wäre vorteilhafter