Kapitel 2
Die Exchange Server-Plattform

Exchange Server ist ein sehr tolerantes Produkt, das sich in zahlreichen Varianten betreiben lässt. Jedoch wird nicht jede Betriebsvariante dem Produkt gerecht. Manche Varianten stören regelrecht den stabilen und sicheren Betrieb von Exchange Server.

Im ersten Teil unserer Reise mit Exchange Server habe ich die Historie von Exchange Server beleuchtet. Für den Aufbau einer Exchange Server-Plattform ist die Kenntnis der Historie dieses Produkts sehr hilfreich, denn Sie werden immer wieder diese Momente erleben, in denen Sie sich fragen, warum eine Exchange Server-Funktion oder ein Exchange Server-Verhalten so ist, wie es ist. In den meisten Fällen sind dies historische Abhängigkeiten, die der Abwärtskompatibilität geschuldet sind.

Die Evolution der Exchange Server-Messaging-Plattform von einem reinen On-Premises-Produkt hin zu einem Hybrid- und Cloud-Produkt hat weitreichende Auswirkungen auf die Planung einer neuen Exchange Server-Plattform. In diesem Kapitel betrachten wir die Möglichkeiten, eine Exchange Server-Plattform zu betreiben. Die detaillierte Planung einer Exchange Server-Plattform wird im nächsten Kapitel gezeigt.

In früheren Jahren waren die Möglichkeiten, eine Exchange Server-Plattform zu betreiben, sehr stringent. Die heutigen Betriebsmöglichkeiten bieten eine fast unübersichtliche Vielfalt und erschweren die Entscheidungsfindung.

Es kommt ganz darauf an

Wenn Sie für die Planung Ihrer Exchange Server-Plattform mit einem externen Berater zusammenarbeiten, werden Sie mit hoher Wahrscheinlichkeit auf Ihre Anforderung »Ich möchte Exchange Server nutzen. Was brauche ich dazu?« eine Antwort erhalten, die Ihnen nicht auf Anhieb gefallen wird:

»Es kommt ganz darauf an.«

Für den Aufbau einer verlässlich funktionierenden Exchange Server-Plattform ist es unerlässlich, genau zu wissen, wie man Exchange Server-Funktionen bereitstellt und wie die Exchange Server-Plattform betrieben werden soll. Dies gilt gleichermaßen für Neuinstallationen von Exchange Server 2019 wie auch für eine Transition einer bestehenden Exchange Server-Plattform zu Exchange Server 2019.

Bevor wir uns nun den unterschiedlichen Betriebsmodellen zuwenden, möchte ich zwei wichtige Begriffe für den weiteren Gebrauch in diesem Buch klären:

- Exchange-Organisation
- Exchange Server-Plattform

Im Kontext der Konfiguration und des Betriebs des Produkts Exchange Server spricht man von einer *Exchange-Organisation*. Eine Exchange-Organisation beschreibt die logische Konfiguration innerhalb der Konfigurationspartition eines *Active Directory Forest*. Alle Exchange-Mitgliedsserver lesen ihre Konfiguration beim Start der Dienste aus dieser Konfigurationspartition. Ebenso werden durch die Exchange Server-Dienste die notwendigen Betriebsparameter und Konfigurationsänderungen in die Konfigurationspartition geschrieben. Dies ist auch der Grund, warum in einer Active Directory-Site mit Exchange Server-Systemen kein *Read-Only Domain Controller* vorhanden sein darf: Exchange Server benötigt immer Schreibzugriff auf Domänencontroller.

In Abbildung 2.1 sehen Sie den Eintrag der Exchange-Organisation mit dem Namen *GRANIKOSLABS* in der Konfigurationspartition des Active Directory.

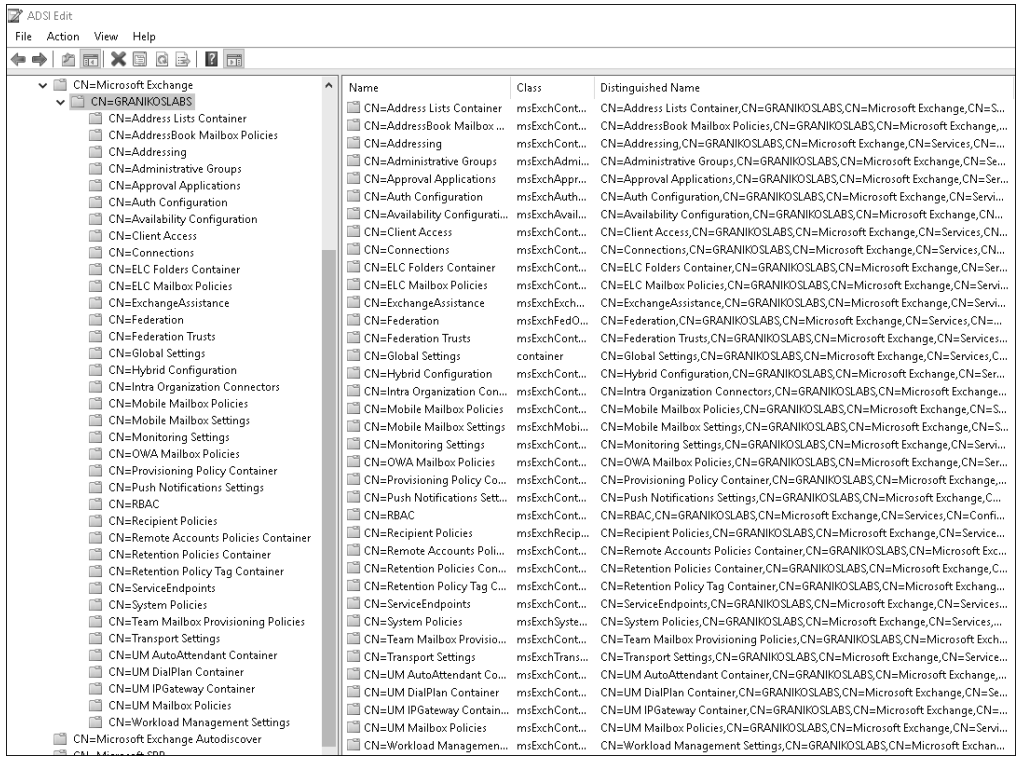

Abbildung 2.1 Beispiel eines Exchange-Organisationseintrages in der Konfigurationspartition des Active Directory

Wie Sie mit dieser Partition des Active Directory arbeiten können, insbesondere wenn es um das Troubleshooting einer Exchange Server-Plattform geht, sehen Sie im Kapitel 7, »Betrieb der Exchange-Plattform«.

Als *Exchange Server-Plattform* bezeichnen wir die Gesamtkonstellation aller technischen Komponenten, um Exchange Server zu betreiben. Zu diesen Komponenten gehören z. B. die Server, der Diskspeicher oder der *Load Balancer* (siehe Abbildung 2.2).

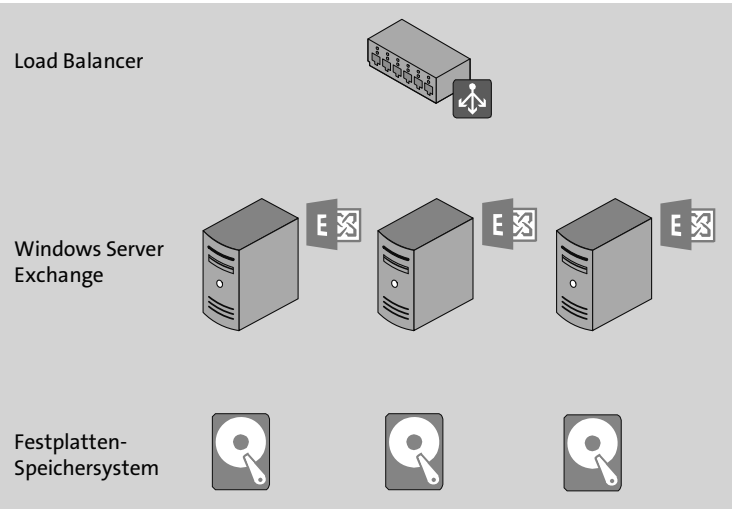

Abbildung 2.2 Beispiel einer Exchange-Plattform mit den dazugehörigen Komponenten

Welche technischen Komponenten direkt zu Ihrer Exchange Server-Plattform gezählt werden, hängt davon ab, wie in Ihrem Unternehmen die Abgrenzungen der einzelnen Fachbereiche erfolgen. Gerade aktive Netzwerkkomponenten, wie Load Balancer, werden oftmals durch ein dediziertes Netzwerk-Team betrieben. Load Balancer sind aber ein existenzieller Teil der Betriebsarchitektur von Exchange Server. Daher müssen Sie, z. B. für eine Exchange Server-Wartung, Zugriff auf die Verwaltungsoberfläche der Load Balancer erhalten. Ähnlich sieht die Situation beim Active Directory selbst aus. Das Active Directory ist direkt Bestandteil der Exchange Server-Plattform, und ohne ein gut funktionierendes Active Directory gibt es auch keine gut funktionierende Exchange Server-Plattform.

Im Zusammenspiel der beiden Begriffe kann man sagen, dass wir eine Exchange-Organisation auf einer Exchange Server-Plattform betreiben.

In diesem Kapitel behandele ich auch das Thema Datensicherung. Aus meiner Sicht gehört es in die Betrachtung der Exchange Server-Plattform, da ich ein Verfechter der in Exchange Server integrierten Möglichkeiten zur Datensicherung bin. Warum dies so ist, lesen Sie in Abschnitt 2.12.

2.1 Muss es Exchange Server sein?

Vor der Frage »*Wie* möchte ich meine Exchange Server-Plattform betreiben?« müssen Sie sich eine andere Frage stellen:

> *Ist Exchange Server das passende Produkt, um in meinem Unternehmen eine E-Mail-Plattform aufzubauen?*

Es gibt zahlreiche E-Mail-Server-Produkte auf dem Markt, die sich selbst als Alternative zu Exchange Server positionieren. Diese Lösungen unterstützen im Regelfall auch Outlook für Desktop als Standard-Client. Ebenso können mobile Endgeräte entweder das ActiveSync-Protokoll oder Exchange Web Services für den Zugriff verwenden.

Die größten Unterschiede zu den alternativen E-Mail-Server-Lösungen liegen in der Betriebsart einer hochverfügbaren Bereitstellung von E-Mail-Diensten, in der Verwaltung der E-Mail-Server-Umgebung und in den Zugriffsmöglichkeiten für Endanwender.

Die Anforderungen an eine E-Mail-Server-Lösung sind in jedem Unternehmen unterschiedlich, wie Sie sicher aus persönlicher Erfahrung wissen. Aus diesem Grund kann ich Ihnen für die Auswahl eines E-Mail-Server-Produkts keinen strukturierten Entscheidungsbaum anbieten.

Jedoch tragen die folgenden Fragestellungen dazu bei, das für Ihr Unternehmen passende Produkt zu finden:

- Wird eine hochverfügbare E-Mail-Server-Lösung benötigt?
- Welche E-Mail-Clients benötigen Zugriff auf Postfächer?
  - Outlook für Desktop (Windows/Mac, ab bzw. bis zu welcher Version?)
  - Welche mobilen Endgeräte kommen zum Einsatz?
  - Gibt es klassische POP3/SMTP-Clients (z. B. Thunderbird)?
  - Welche Browser-Versionen sollen unterstützt werden?
- Werden die Funktionen der Öffentlichen Ordner benötigt?
- Wie erfolgt eine Datensicherung der Postfächer?
- Wird eine klassische Datensicherung wirklich benötigt?
- Ist das Wissen, wie die E-Mail-Server-Lösung administriert wird, im Hause vorhanden?
- Wie und durch wen erfolgt die Betreuung des Betriebs der E-Mail-Server-Lösung?
- Wird ein *Mobile Device Management* benötigt oder erwartet?
- Wird ein SMTP-Gateway für Anti-Spam- oder Anti-Malware-Schutz benötigt?
- Sollen E-Mail-Nachrichten per S/MIME oder PGP zentral ent- und verschlüsselt werden?

- Unterstützten alle internen Applikationen und Geräte, die E-Mail-Nachrichten versenden oder empfangen, moderne Authentifizierung und TLS 1.2 oder höher?
- ...

Ergänzen Sie diese Liste einfach durch die Anforderungen, die Sie in Ihrem Exchange Server-Projektteam erarbeitet haben.

Die Anforderungen der Alternativen zu Exchange Server zu betrachten, ist natürlich nicht Bestandteil dieses Buches. Hier kann ich nur auf die eventuell zur Verfügung stehenden Best Practices-Empfehlungen der jeweiligen Hersteller verweisen. Ich möchte Sie aber einladen, mir zu schreiben, welche Gründe für *Sie* einen Einsatz von Exchange Server gerechtfertigt haben oder eben auch nicht. Ich bin davon überzeugt, dass nur eine stete Kollaboration zu einer guten E-Mail-Server-Implementierung führt. Meine Kontaktdaten finden Sie am Anfang des Buches.

In den folgenden Kapiteln betrachten wir die einzelnen Möglichkeiten, um Exchange Server zu installieren und zu betreiben. Zuerst gebe ich aber einen Überblick über die grundsätzliche Architektur von Exchange, aus der sich einheitliche Anforderungen für die unterschiedlichen Installationsvarianten ableiten (siehe Abschnitt 2.2). Daran anschließend stelle ich Ihnen in Abschnitt 2.3 und 2.4 die beiden noch verbliebenen Funktionsrollen von Exchange Server 2019 vor. Das Verständnis der Exchange Server 2019-Architektur ist für den sicheren Betrieb unerlässlich.

Anschließend zeige ich in Abschnitt 2.5 die klassische Methode, also die Installation auf physischen Systemen, und lege dar, warum dies die vom Produktteam bevorzugte Variante ist. Danach bespreche ich den Betrieb von Exchange Server 2019 in einer Virtualisierungsplattform, und zwar getrennt für den Betrieb in einer lokal betriebenen und in einer cloudbasierten Virtualisierungsplattform (siehe Abschnitt 2.6 und 2.7). Die letzte Variante ist die Nutzung von Exchange im Rahmen eines Software-as-a-Service-Angebotes, wie z. B. Microsoft 365, die wir uns in Abschnitt 2.8 ansehen.

Zur einer Exchange Server-Plattform gehören weitere Komponenten, wie Unified Messaging (siehe Abschnitt 2.9), das Active Directory (siehe Abschnitt 2.10) und die E-Mail-Clients (siehe Abschnitt 2.11).

2.2 Die richtige Exchange-Architektur

Das Exchange Server-Produktteam hat für

- Exchange Server 2013 (*https://techcommunity.microsoft.com/t5/exchange-team-blog/the-preferred-architecture/ba-p/586755*),
- Exchange Server 2016 (*https://techcommunity.microsoft.com/t5/exchange-team-blog/the-exchange-2016-preferred-architecture/ba-p/604024*) und

- Exchange Server 2019 (*https://docs.microsoft.com/exchange/plan-and-deploy/deployment-ref/preferred-architecture-2019*)

jeweils eine Empfehlung unter dem Titel *Preferred Architecture* (PA) herausgegeben. Die Architekturempfehlung (siehe Abbildung 2.3) basiert auf den Betriebserfahrungen im internen Gebrauch bei Microsoft, den Erfahrungen im Cloudbetrieb von Exchange Online und auf den Erfahrungen im Kundenbetrieb – hier insbesondere unter Berücksichtigung der Erfahrungen im Produkt-Support für die unterschiedlichen Exchange Server Versionen.

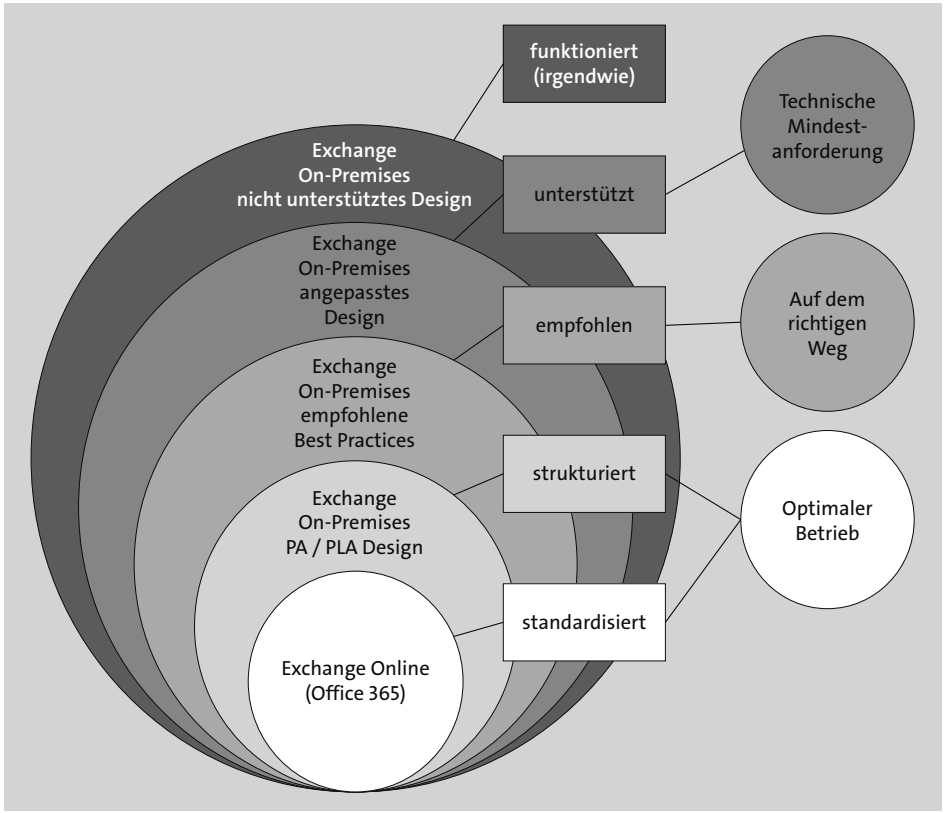

Abbildung 2.3 Übersicht der Exchange Server-Design-Optionen

- **Standardisiert**
  Exchange Online ist eine standardisierte Plattform für Exchange Server-Funktionen und wird als Teil der Software-as-a-Service-Plattform von Office 365 angeboten. Wenn Sie sich für Exchange Online entscheiden, sind Sie reiner Nutzer der angebotenen Dienste und Funktionen. Hierbei haben Sie keinerlei Zugriff auf die Serverhardware oder die verwendeten Betriebssysteme. Die Verwaltung aller

Infrastrukturkomponenten obliegt Microsoft. Sie konzentrieren sich ganz auf die Konfiguration Ihrer Exchange Online-Organisation und eventuell auf die Hybridanbindung Ihrer verbliebenen On-Premises-Exchange Server.

- **Strukturiert**
  Bei einer strukturierten Implementierung einer On-Premises-Exchange-Server-Plattform folgen Sie der Preferred Architecture der Exchange Server-Produktgruppe oder der *Product Line Architecture* (PLA), die auf Erfahrungen von IT-Architekten der Microsoft Consulting Services basiert. Von den Empfehlungen der PA oder PLA wird nicht abgewichen.
- **Empfohlen**
  Eine On-Premises-Exchange-Server-Implementierung, die den Best-Practices-Empfehlungen für Exchange Server folgt, weicht in signifikanten Punkten von der PA ab, stellt aber weiterhin einen sicheren und stabilen Betrieb sicher. Eine solche signifikante Abweichung kann z. B. der Betrieb auf einer Hypervisor-Plattform sein, allerdings unter Berücksichtigung der Best Practices für den Betrieb von Exchange Server auf physischen Systemen (Stichwort: feste Reservierung von Ressourcen). Die Einhaltung der Best Practices können Sie mit dem *Best Practices Analyzer* (BPA) überprüfen. Der Exchange Server BPA steht als Click-to-run-Applikation im Exchange Admin Center zur Verfügung. Alternativ können Sie auch das auf GitHub veröffentlichte *Exchange Analyzer PowerShell Script* (siehe *https://github.com/ExchangeAnalyzer/ExchangeAnalyzer*) von Paul Cunningham verwenden.
- **Unterstützt**
  Eine nur unterstützte Exchange Server-Implementierung weicht in zahlreichen Punkten von der PA für Exchange Server ab. Die Systemanforderungen für eine unterstützte Implementierung werden aber angewandt. Bei der Implementierung werden jedoch die Systemanforderungen der *Server Supportability Matrix* (*https://docs.microsoft.com/exchange/exchange-server-supportability-matrix-exchange-2013-help*) und die *Konfigurationsoptionen für Exchange Server-Speicher* (*https://docs.microsoft.com/Exchange/plan-and-deploy/deployment-ref/storage-configuration*) beachtet. Diese Implementierungsvariante ist als *absolutes Minimum* für den Betrieb von Exchange Server anzusehen.
- **Funktioniert**
  Bei dieser Form der Implementierung von Exchange Server wird das Produkt in einer IT-Infrastruktur betrieben, die teilweise oder vollständig außerhalb einer unterstützten Konfiguration ist. Exchange Server wird *irgendwie* lauffähig gemacht. Diese Form der Implementierung ist die denkbar schlechteste und trägt somit das größte Betriebsrisiko.

Optimaler Betrieb, der richtige Weg und technische Mindestanforderungen

Eine *standardisierte* oder *strukturierte* Implementierung von Exchange Server stellt eine optimale Implementierung von Exchange Server dar und ist die bevorzugte Wahl, wenn es um eine Entscheidungsfindung geht. Ist keine dieser beiden Optionen für Sie möglich, so sollten Sie sich für die *empfohlene* Variante entscheiden und den Best Practices für Exchange Server folgen. Wenn Sie Exchange Server auch in der dritten Variante nicht implementieren können, so bleibt Ihnen die vierte valide Option: Implementieren Sie Exchange Server im Rahmen der *unterstützten* System- und Speicheranforderungen.

Wenn keine dieser vier Optionen für Sie infrage kommt, so sollten Sie sich fragen, warum dies der Fall ist und ob Exchange Server für Sie und Ihr Unternehmen die richtige Wahl ist.

Exchange Server ist eine Lösung für den Aufbau einer Messaging-Plattform mit einer hochverfügbaren Bereitstellung von Postfächern und einer fehlertoleranten Nachrichtenzustellung. Diese Funktionen können aber nur gewährleistet werden, wenn die Exchange-Plattform passend implementiert wurde.

Die Empfehlung der *Preferred Architecture* (PA) greift genau diese hochverfügbare und ausfallsichere Bereitstellung von Exchange Server auf:

- Hochverfügbarkeit sowohl innerhalb eines Rechenzentrums als auch zwischen mehreren Rechenzentren
- schnelle Aktivierung einer Postfachdatenbank im Fehlerfall durch die Verfügbarkeit mehrerer Datenbankkopien
- Reduzierung der Kosten für die Messaging-Plattform
- Erhöhung der Verfügbarkeit durch eine optimierte Fehlerbehandlung und die Reduzierung der Komplexität

Diese vier Ziele sollten Sie für Ihre Exchange Server-Implementierung im Blick haben, ganz unabhängig davon, für welche Implementierungsvariante Sie sich entscheiden.

Exchange Server-Resilienz

Im Kontext von Exchange Server wird immer wieder von *Mailbox Resiliency* und *Site Resiliency* gesprochen (*https://docs.microsoft.com/exchange/high-availability-and-site-resilience-exchange-2013-help*). In seiner deutschen Übersetzung wird der Begriff *Resilienz* meist im Bereich der Materialwissenschaften oder der Psychologie angewandt. In der klassischen IT bevorzugen wir die Begriffe *Redundanz* und *Hochverfügbarkeit*. Damit wird aber nur die technische Implementierung von Systemen beschrieben, nicht jedoch ihr Verhalten.

Der Programmcode von Exchange Server beinhaltet zahlreiche Funktionen, um genau dieses Verhalten der Resilienz zu gewährleisten. Bei einem Teilausfall der Exchange Server versuchen die verbleibenden Server einer DAG, einen Totalausfall der Exchange Server-Funktionen zu unterbinden. Sobald ausgefallene Systeme wieder verfügbar sind, erfolgt eine automatische Integration in den Betrieb und damit eine Stabilisierung der Exchange Server-Plattform. Die wichtigste Komponente ist der *Active Manager*, der sich um die Fehlerüberwachung kümmert und die notwendigen Korrekturmaßnahmen ergreift. Exchange Server beinhaltet weitere Funktionen, um eine Resilienz zu gewährleisten. Diese Art der Implementierung ist in der Preferred Architecture berücksichtigt.

Aus dem Building-Block-Ansatz der Preferred Architecture leitet sich die *Product Line Architecture* (PLA) ab, die von IT-Architekten der Microsoft Consulting Services entwickelt wurde. Die PLA-Architektur basiert auf folgenden Eckpunkten:

- 4 Datenbankkopien in 2 Rechenzentren (je eine Active Directory-Site), *File Share Witness*-Server in einer dritten Active Directory-Site
- einheitlicher Namensraum (*Unbound Namespace*)
- DAS-Festplattenspeicher (*Direct-Attached Storage*) für Postfachdatenbanken, entweder als NL-SAS oder als SATA-JBOD
- SSD-Festplattenspeicher für Metacache-Datenbanken (Exchange Server 2019)
- *Level 7 Load Balancer* ohne *Session Affinity*
- große Postfächer mit mindestens 50 GB Speichervolumen
- sicherer HTTPS-Zugriff für alle internen und externen Clients
- Exchange Server-Verfügbarkeit über Managed Availability
- *System Center Operations Manager* für das Monitoring
- *Exchange Online Protection* für Anti-Spam und Anti-Malware

Wichtig für die gesamte Planung und den folgenden Betrieb einer Exchange Server-Plattform ist der Hauptgrundsatz moderner Exchange-Versionen:

Hauptgrundsatz moderner Exchange Server-Versionen

Die Bereitstellung von Hochverfügbarkeit von Exchange Server-Funktionen erfolgt auf Applikationsebene.

Moderne Exchange Server-Versionen basieren auf dem Grundsatz *»Jeder Server ist eine Insel«*. Das bedeutet, dass jeder Server für sich autark über alle notwendigen Informationen und Funktionen verfügt, um alle Aufgaben zu erfüllen. Die Funktionen eines Exchange Servers gliedern sich in die drei Schichten *Protokolle und Serveragenten*, *Geschäftslogik* sowie *Speicherfunktionen*, die aufeinander aufbauen. Zwischen

Exchange Servern findet die Kommunikation nur auf der Ebene *Protokolle und Serveragenten* statt. Abbildung 2.4 verdeutlicht die Funktionsebenen und die Server-zu-Server-Kommunikation von Exchange Server 2019.

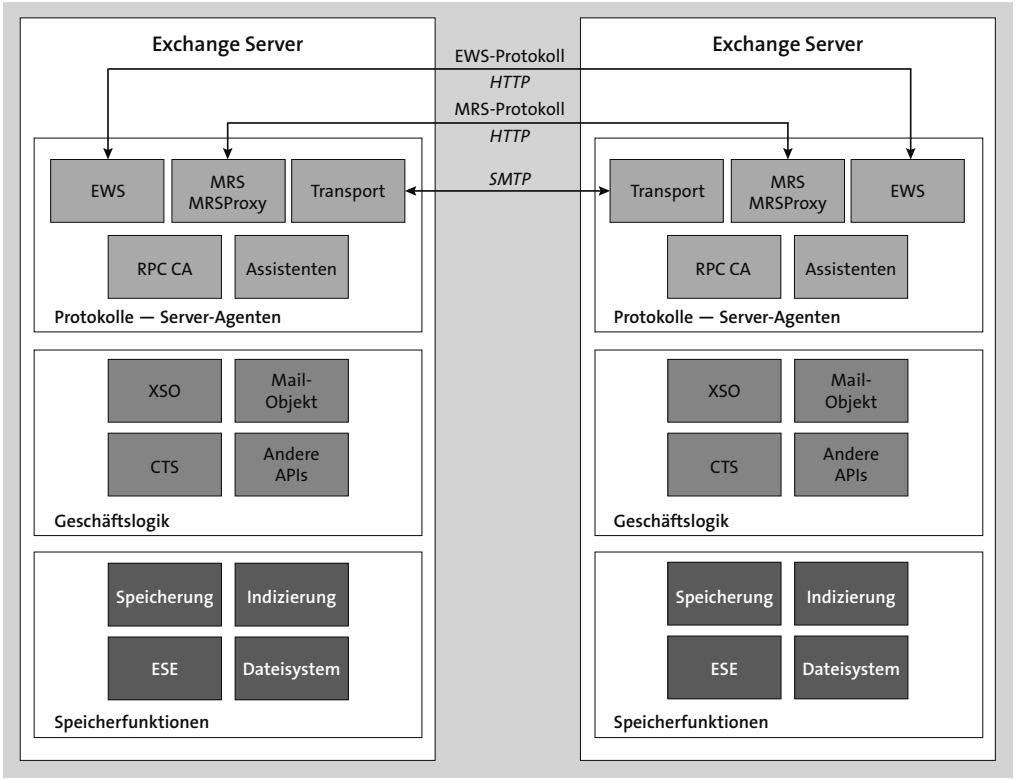

Abbildung 2.4 Exchange-Funktionsebenen und Server-zu-Server-Kommunikation

Seit Exchange Server 2016 steht nur noch eine Serverrolle für die Installation im internen Unternehmensnetzwerk zur Verfügung: die *Postfach-Rolle*.

Dieser Umstand vereinheitlicht die Anforderungen an die Serverhardware und an das Betriebssystem. Diese Vereinheitlichung vereinfacht nicht nur die Beschaffung der Serversysteme, sondern wirkt sich auch kostensparend auf die regelmäßige Wartung und den laufenden Betrieb der Systeme aus.

Viele Unternehmen versuchen einen Vorteil für den IT-Betrieb zu schaffen, indem sie Hypervisor-Plattformen für Server und Festplatten einsetzen. Das Gegenteil ist, gerade in Bezug auf Exchange Server, leider der Fall. Lassen Sie mich dies am Beispiel von Abbildung 2.5 verdeutlichen.

Auf der Ebene der Exchange Server, die in virtualisierten Gast-Systemen auf einer Hypervisor-Plattform betrieben werden, haben wir noch keine Herausforderungen. Uns steht ein Betriebssystem zur Verfügung, das über Prozessor-Ressourcen, zugewiesenen Arbeitsspeicher, Netzwerkverbindungen und Festplattenspeicher verfügt. Um eine Ausfallsicherheit zu erreichen, ist es erforderlich, alle benötigten Hardware-Ressourcen *mindestens* redundant auszulegen. Die Host-Systeme einer Hypervisor-Plattform gehören aber nun nicht zu den günstigen Hardware-Ressourcen. Sie sind teuer in der Anschaffung und kostenintensiv im Unterhalt. Dies gilt insbesondere für Blade-Chassis.

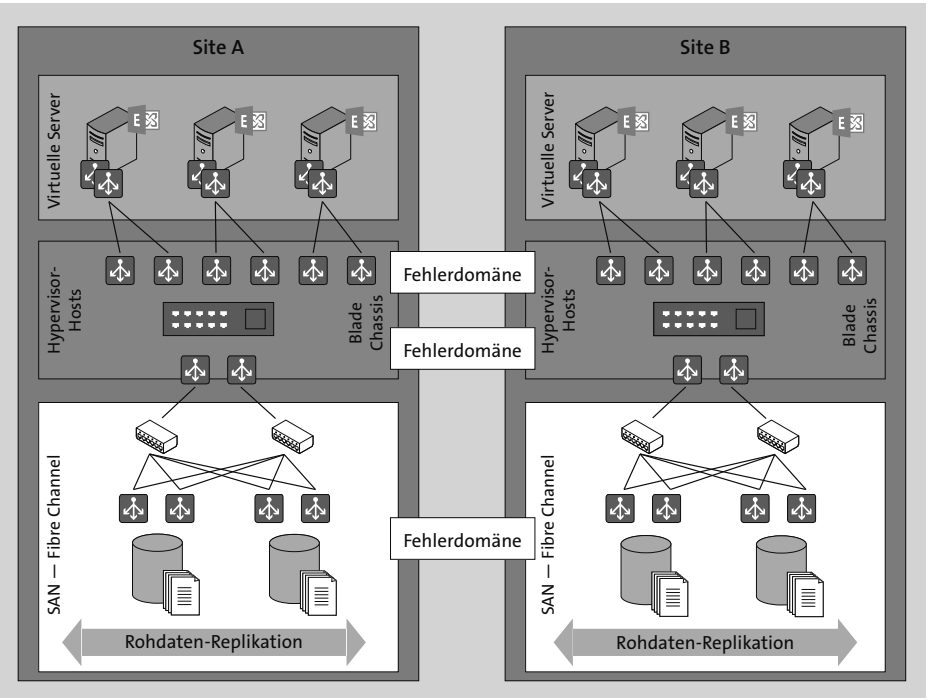

Abbildung 2.5 Komplexität und Fehlerdomäne bei der Virtualisierung

Bei Blade-Chassis kommen noch weitere Herausforderungen auf uns zu. Durch die Natur dieser Chassis werden automatisch weitere Applikationen auf den Serversystemen im gleichen Blade-Chassis betrieben. Diese können durch technisches Fehlverhalten oder bewusste »Hyper-Kommunikation« als laute Nachbarn, sogenannte *Noisy Neighbors*, auffallen und unnötige Last sowohl auf den Netzwerk- als auch auf den Diskspeicherkanälen des Blade-Chassis erzeugen. Hierdurch verlieren unsere Exchange Server-Systeme wertvolle Netzwerkbandbreite und Disk-I/O, auf die wir angewiesen sind und von denen das Betriebssystem und unser Exchange Server annehmen, dass beides zur Verfügung steht.

Auf dieser Ebene haben wir zwei mögliche Fehlerdomänen, die gegen betriebliche Risiken abgesichert werden müssen. Dies sind die Hypervisor-Hosts und das Blade-Chassis. Die möglichen Kompatibilitätsprobleme zwischen den einzelnen Firmware-Komponenten sind nicht zu vernachlässigen.

Die Bereitstellung des redundanten SAN-Festplattenspeichers über ebenso redundante Zugriffskanäle erfordert weitere Hardwarekomponenten, die in der Anschaffung und im laufenden Betrieb mit hohen Kosten verbunden sind. Die SAN-Lösung selbst ist eine einzige große Fehlerdomäne. Zu den möglichen Problemen gehören dynamische Disk-Provisionierung, virtuelles LUN-Management, aufgeteilte Spindel-Zuordnungen oder SSDs aus einer Produktionscharge. Ergänzt wird diese unnötige Komplexität durch eine SAN-interne Datenreplikation.

Wenn wir uns nun im Gegensatz zur Komplexität einer virtualisierten Exchange-Plattform die Einfachheit einer physischen Implementierung anschauen (siehe Abbildung 2.6), wird der Unterschied schnell deutlich.

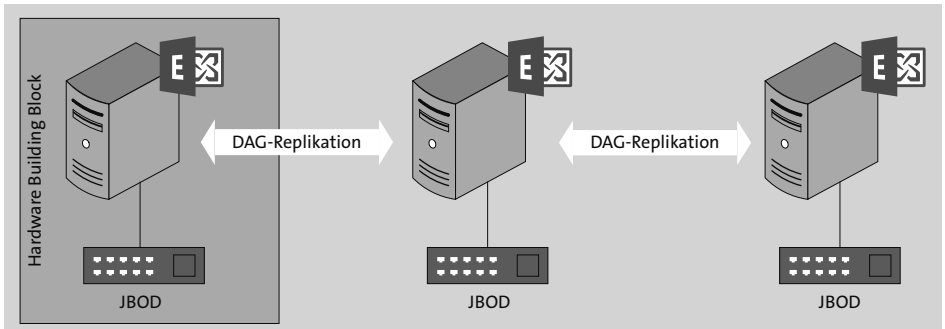

Abbildung 2.6 Exchange Server Building Blocks

Jeder *Hardware Building Block* besteht aus einem physischen Server und lokal verbundenem Festplattenspeicher. Die Hochverfügbarkeit und Ausfallsicherheit wird durch die Replikation innerhalb der *Database Availability Group* (DAG) erreicht. Stellen Sie sich eine DAG einfach als RAID auf Applikationsebene vor.

Möchten Sie SAN? Darf es etwa mehr sein?

Sie haben sicherlich erkannt, dass ich nicht zu den Verfechtern einer SAN-Lösung gehöre. Der Grund ist einfach: Exchange Server benötigt keine überteuerte SAN-Lösung.

Ist ein Systemhaus, das sowohl IT-Beratung als auch Hardware-Vertrieb bietet, in die Planungen zur Exchange-Architektur involviert, gibt es einen Interessenskonflikt. Der Vertrieb von Speicherlösungen bietet Margen, die durch das Beratungsgeschäft nur schwer zu erreichen sind. Gern wird daher auch eine größere Speicherlösung empfohlen, um das Wachstum der nächsten Jahre aufnehmen zu können, angereicht durch unnötige Zusatzfunktionen, die eventuell noch separat zu lizenzieren sind.

Kurz und knapp: Für den stabilen und sicheren Betrieb einer Exchange Server-Plattform benötigen Sie all das nicht.

Für die Bereitstellung von Festplattenspeicher unterstützt Exchange Server die folgenden Speicherarchitekturen:

- Direct-Attached Storage (DAS)
- Serially Attached SCSI (SAS)
- Storage Area Network (SAN) – Internet SCSI (iSCSI)
- Storage Area Network (SAN) – Fibre Channel (FC)

Die Anforderungen an die unterstützten Speicherarchitekturen gelten sowohl für rein physische Exchange-Server-Systeme als auch für die Bereitstellung von Laufwerksmedien in virtualisierten Umgebungen (*https://docs.microsoft.com/exchange/exchange-2013-storage-configuration-options-exchange-2013-help*). Wählen Sie die für Ihre Infrastruktur passende Speicherarchitektur auch immer unter dem Gesichtspunkt des einfachen Betriebs aus. Exchange Server benötigt keinen hochpreisigen Datenspeicher oder Lösungen zur Datenspiegelung zwischen Standorten. Solche Lösungen erhöhen die Komplexität der IT-Infrastruktur nur unnötig und erschweren bei Problemen im Betrieb die Fehleranalyse.

Noch ein Satz zum möglichen Mischbetrieb von physischen und virtualisierten Exchange Servern: Eine Mischung von physischen und virtualisierten Exchange Servern innerhalb einer DAG ist technisch zwar möglich und wird von Microsoft auch unterstützt – er wird jedoch von der Exchange Server-Produktgruppe nicht empfohlen. Was sich zuerst wie ein Widerspruch liest, wird klar, wenn wir uns noch einmal vor Augen führen, dass die Produktgruppe eine möglichst einfache Implementierung anstrebt. Durch eine Mischung der Betriebsplattformen »physisch« und »virtualisiert« erreicht man genau das Gegenteil, da Komponenten mit gleicher Funktion, z. B. Netzwerkkarten, gänzlich unterschiedlich arbeiten.

2.3 Die Exchange Server-Postfach-Rolle

Bevor wir die unterschiedlichen Möglichkeiten zur Implementierung von Exchange Server betrachten, wenden wir uns den beiden Funktionsrollen von Exchange Server zu. Sie müssen die grundlegende Architektur von Exchange Server kennen, um diejenige Betriebsplattform auswählen zu können, die zu Ihrem Unternehmen passt.

Seit Exchange Server 2016 existiert nur noch eine Funktionsrolle für die Installation eines Exchange Servers im internen Netzwerk: die Postfach-Rolle. Sie beinhaltet alle notwendigen Funktionen für den Betrieb des Exchange Servers, die in früheren Versionen in mehrere Rollen untergliedert waren. Diese Funktionen sind:

- **Client-Zugriffsdienste (Client Access Services)**
  Die Client-Zugriffsdienste stellen alle Protokollendpunkte für den Zugriff von Clients bereit. Zu diesen Endpunkten gehören die Protokolle HTTP, POP3, IMAP4 und SMTP. SIP und RTP stehen in Exchange Server 2019 nicht mehr zur Verfügung.

- **Transportdienst (Hub Transport)**
  Der Transportdienst ist die Hauptkomponente für die Verarbeitung von E-Mail-Nachrichten, die über das Protokoll SMTP empfangen und gesendet werden. Über diesen Dienst werden auch die Funktionen zur Hochverfügbarkeit des E-Mail-Transports bereitgestellt.
- **Postfachdienst (Mailbox)**
  Der Postfachdienst ist die Hauptkomponente für die Bereitstellung der Postfächer und für das Rendering von Postfachinhalten für Outlook on the Web. In diesen Bereich fallen auch alle relevanten Funktionen zur hochverfügbaren Bereitstellung von Postfächern mithilfe einer DAG.
- **Unified Messaging**
  Die Unified-Messaging-(UM-)Funktionen bieten mit *Outlook Voice Access* unter anderem die Möglichkeit, auf Postfachinhalte wie E-Mail-Nachrichten oder Termine per Telefon zuzugreifen.

  Die UM-Funktion steht ab Exchange Server 2019 nicht mehr zur Verfügung.

Die einzelnen Dienstkomponenten eines Exchange Servers gliedern sich in einen Frontend- und einen Backend-Teil. Hierbei sind die Frontend-Komponenten der Teil eines Exchange Servers, der direkt sowohl von Clients als auch von Nicht-Exchange-Servern angesprochen wird.

Die Frontend-Komponenten beinhalten keine Logik zur Verarbeitung von Informationen, sondern dienen nur dazu, die Verbindungen des jeweiligen Protokolls zum eigentlichen Endpunkt im Backend zu verwalten. Wir sprechen hier von einer *Proxy-Verbindung*, die immer zu dem Exchange Server aufgebaut wird, der im Moment des Verbindungsaufbaus die aktive Datenbankkopie hält, in der das Zielpostfach liegt. Dieses Ziel kann entweder der gleiche Exchange Server sein oder aber ein anderer Exchange Server in der gleichen Exchange-Organisation.

Abbildung 2.7 verdeutlicht den Aufbau eines Exchange Servers in Bezug auf die Unterteilung der Frontend- und Backend-Komponenten.

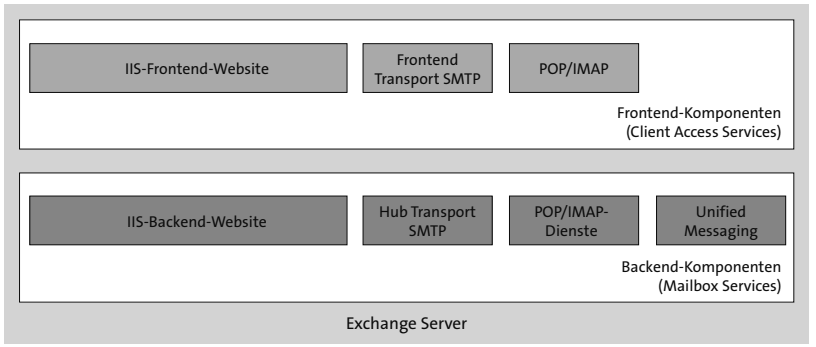

Abbildung 2.7 Allgemeine Funktionsweise der Exchange Server-Frontend- und Backend-Komponenten

Das Verständnis dieser Funktionsweise ist wichtig für den sicheren Betrieb einer Exchange Server-Umgebung und natürlich für die Fehlersuche und Fehlerbehebung. Diesen Themen werden wir uns in Kapitel 7 widmen.

Die Zugriffswege für die Protokolle *HTTP*, *POP3*, *IMAP4*, *SMTP*, *SIP* und *RTP* (Exchange Server 2016) werden in Abbildung 2.8 deutlich. Wichtig ist insbesondere, dass Sie die Abhängigkeit zu den Internet Information Services (IIS) von Windows Server verstehen.

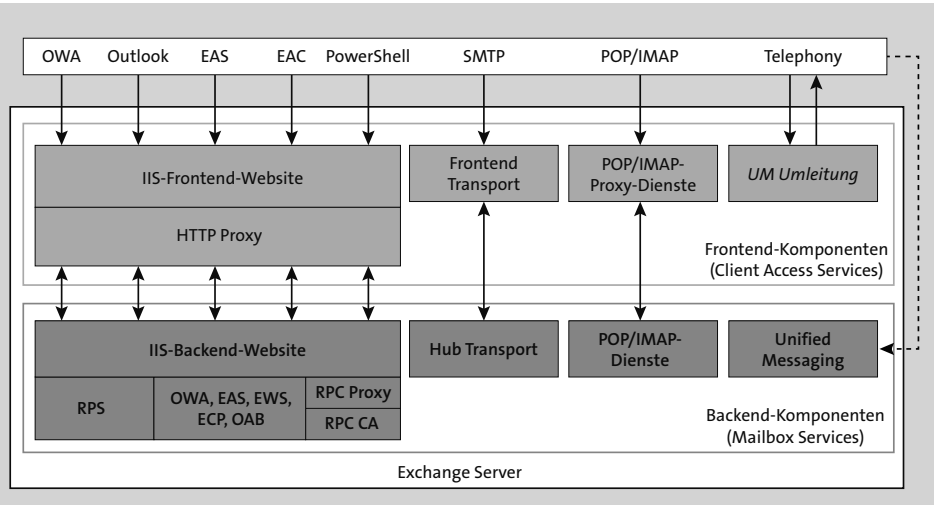

Abbildung 2.8 Übersicht über die Client-Zugriffsarchitektur

Die Mailbox-Rolle von Exchange Server beinhaltet natürlich noch wesentlich mehr. Sie ist das Arbeitstier von Exchange Server und verantwortlich für alle Funktionen, die mit der Verarbeitung, dem Schutz, der Bereitstellung und der Speicherung von Postfachdaten zu tun haben. Eine detaillierte technische Beschreibung aller Funktionen würde den Rahmen dieses Buches sprengen. Um Exchange Server grundsätzlich besser kennenzulernen, empfehle ich Ihnen die technische Dokumentation von Microsoft oder die Teilnahme an einem Exchange Server-Einführungsworkshop bei einem Microsoft-Trainingspartner.

2.4 Die Exchange Server-Edge-Transport-Rolle

Die Edge-Transport-Rolle wurde mit Exchange Server 2007 eingeführt und fristet seit dieser Zeit ein Nischendasein. Dieses Nischendasein ist völlig unberechtigt.

Eines der Hauptargumente für die Nichtnutzung der Edge-Transport-Rolle ist die größere Komplexität der Exchange Server-Umgebung. Wenn dieses Argument angeführt wird, frage ich gerne nach, welche alternative Lösung als E-Mail-Gateway vom und ins Internet genutzt wird. Schließlich möchte niemand, dass interne Exchange Server als Mitgliedsserver einer Active Directory-Domäne direkt aus dem Internet erreichbar sind. An diesem Punkt werden immer Drittanbieterlösungen genannt, die entweder in der internen IT-Infrastruktur platziert sind oder aber als Cloud-Lösungen eine direkte Kommunikation mit den Exchange Servern erfordern. Diese Lösungen nutzen zusätzliche Schnittstellen, um über einen Zugriff auf das Active Directory die Liste der gültigen E-Mail-Adressen nutzen zu können. Aber war da nicht das Argument »Komplexität«?

Ein Grund für die Nichtnutzung der Edge-Transport-Rolle sind die zusätzlichen Kosten für die Windows Server-Betriebssystemlizenz und die Exchange Server-Standardlizenz. Ob diese zusätzlichen Kosten die Lizenzkosten und die Betriebskosten einer alternativen Mail-Gateway-Lösung übersteigen, vermag ich an dieser Stelle nicht zu beurteilen. Aber bedenken Sie bei Ihren Überlegungen, dass die benötigte Lizenz für Exchange Server völlig unabhängig von der tatsächlichen E-Mail-Nutzeranzahl ist. Und wenn Sie die Edge-Transport-Rolle im Rahmen einer Hybridanbindnung mit Exchange Online betreiben möchten, erfolgt die Lizenzierung unter Verwendung des kostenlos bereitgestellten *Hybrid-Keys*. Diese Form der Lizenzierung ist mit Exchange Server 2019 seit dem kumulativen Update 12 kostenfrei. Vor der Änderung der Lizenzbedingungen war die Nutzung von Exchange Server 2019 für die reine Hybrid-Nutzung lizenzpflichtig (*https://techcommunity.microsoft.com/t5/exchange-team-blog/released-2022-h1-cumulative-updates-for-exchange-server/ba-p/3285026*).

Lizenzierung der Hybrid Server

Im Blogartikel zu Exchange Server 2019 CU12 wird hinsichtlich der kostenfreien Lizenzierung nur von *Hybrid-Servern* gesprochen. Es wird nicht klar definiert, ob dies nun die Edge-Transport-Server inkludiert oder nicht. Auch die Exchange Server-Lizenz-FAQ (*https://www.microsoft.com/microsoft-365/exchange/microsoft-exchange-licensing-faq-email-for-business*) sind keine Hilfe.

Diese Situation ist nicht neu. Auch mit Exchange Server 2013 oder 2016 standen wir vor dem gleichen Dilemma. Es ist und bleibt eine lizenztechnische Grauzone.

Die Edge-Transport-Rolle kommuniziert für den E-Mail-Verkehr bidirektional. Die notwendigen Konfigurationen der Exchange-Organisation und die Informationen über gültige E-Mail-Adressen von Empfängern werden unidirektional zur Edge-Transport-Rolle verschlüsselt übertragen.

In Abbildung 2.9 ist die einfache Implementierung der Edge-Transport-Rolle dargestellt.

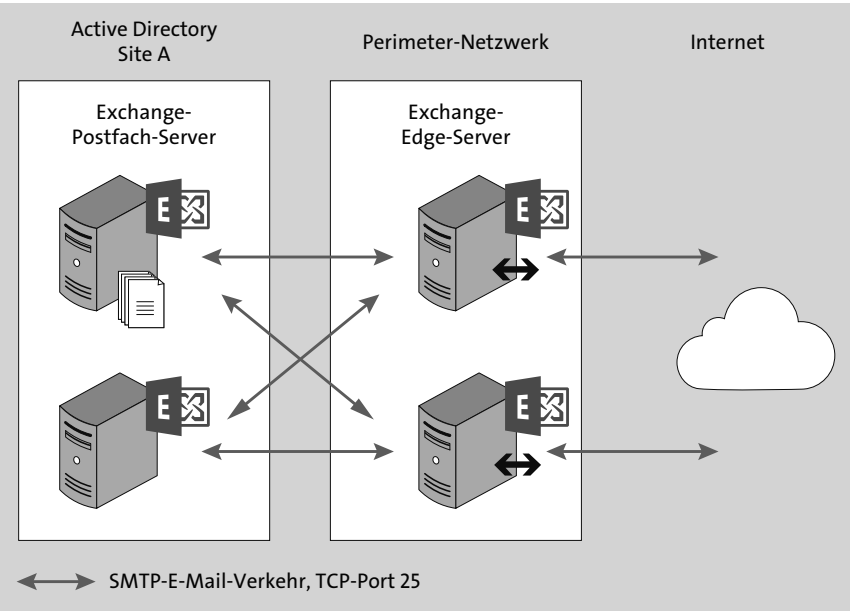

Abbildung 2.9 Übersicht des E-Mail-Verkehrs zwischen internen Exchange-Mailbox-Servern, Exchange-Edge-Transport-Servern und dem Internet

Zwei Exchange Server mit Edge-Transport-Rolle sind im Perimeter-Netzwerk platziert und können aus dem Internet über zwei getrennte MX-Einträge von anderen E-Mail-Servern (MTA, *Message Transfer Agents*) erreicht werden. Beide Edge-Server sind für die Active Directory-Site A registriert. In der Standard-Konfiguration führt eine solche Registrierung der beiden Edge-Server dazu, dass automatisch ein redundanter E-Mail-Verkehr für eingehende und ausgehende Nachrichten gewährleistet ist.

Ähnlich ist es für die Synchronisierung der notwendigen Konfigurationen der Exchange-Organisation und der Liste der gültigen E-Mail-Empfänger im Unternehmen durch *EdgeSync*. Abbildung 2.10 verdeutlicht die EdgeSync-Kommunikation der Exchange Server in der Active Directory-Site A mit den beiden Edge-Servern im Perimeter-Netzwerk. Die Active Directory-Synchronisation (*Secure LDAP*) erfolgt wechselweise von allen Exchange-Servern in der Active Directory-Site zu den Edge-Servern auf TCP-Port 50636. Dieser Port muss ausgehend in Richtung des Perimeter-Netzwerks in der Firewall freigegeben sein.

Die Anbindung von Edge-Servern an die interne Exchange-Organisation erfolgt durch die Einrichtung eines Edge-Abonnements. Die Verschlüsselung der Informationen in der lokalen AD LDS-Instanz auf dem Edge-Server und die Verschlüsselung der EdgeSync-Übertragung erfolgt auf Basis des konfigurierten Standard-SMTP-Zertifikats. Die Schritte zur Erstellung des Edge-Abonnements schauen wir uns später an.

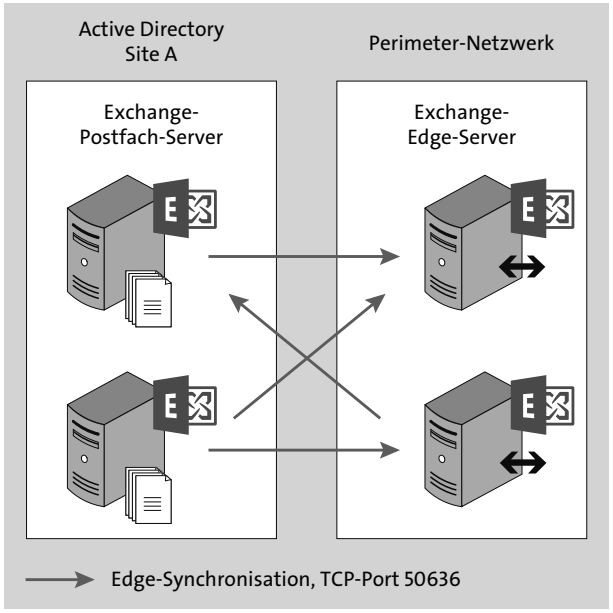

Abbildung 2.10 Übersicht der Edge-Synchronisation (EdgeSync) von internen Exchange-Servern in Site A zu zwei Edge-Servern im Perimeter-Netzwerk

Mit EdgeSync werden folgende Informationen der Exchange-Organisation zu einer Edge-Transport-Rolle übertragen:

- Edge-Sendekonnektoren
- Liste der konfigurierten internen SMTP-Server
- Liste der Exchange Server in der abonnierten Active Directory-Site
- akzeptierte SMTP-Domänen
- Remote SMTP-Domänen
- Liste sicherer E-Mail-Absender
- Liste blockierter E-Mail-Absender
- Adressen gültiger interner E-Mail-Empfänger
- Liste der Partner-Domänen für sicheren Versand und Empfang mit *Domain Secure*

Die Edge-Transport-Rolle verfügt über keine Funktionen zur Bereitstellung von Postfächern. Sie beinhaltet also nur Funktionen für den E-Mail-Transport mit SMTP. Auf einer Edge-Transport-Rolle kann bei Bedarf auch eine Anti-Malware-Lösung eines Drittanbieters installiert werden.

Edge-Transport-Rolle ohne EdgeSync

Die Edge-Transport-Rolle kann auch ohne Edge-Abonnement als SMTP-Gateway im Perimeter-Netzwerk betrieben werden. Dies ist immer dann eine Option, wenn keine direkte Kommunikation über TCP-Port 50636 erwünscht ist oder die Netzwerkstrecke von den internen Exchange Servern in das Perimeter-Netzwerk nur TCP-Port 25 zulässt.

In solch einem Betriebsszenario müssen die notwendigen Konnektoren manuell erstellt werden, da eine automatische Konfiguration per EdgeSync nicht möglich ist. In der Online-Dokumentation sind die notwendigen Schritte für solch eine Implementierung beschrieben (*https://docs.microsoft.com/Exchange/architecture/edge-transport-servers/configure-without-edgesync*).

Wenn Sie den Betrieb einer hybriden Anbindung mit Exchange Online planen, können Sie diese manuelle Variante nicht verwenden. Der *Hybrid Configuration Wizard* unterstützt nur den Betrieb von Edge-Transport-Servern in Verbindung mit EdgeSync.

Wenn Sie Ihre bestehende lokale Exchange Server-Plattform mit Exchange Online im Hybrid-Betrieb konfigurieren möchten, so führt kein Weg an Edge-Servern vorbei. Offiziell erfordert die Konfiguration des hybriden E-Mail-Verkehrs, dass als SMTP-Endpunkt in der lokalen IT-Intrastruktur ein Exchange Server von Exchange Online direkt angesprochen wird (*https://docs.microsoft.com/exchange/edge-transport-servers*). Dies bedeutet nicht automatisch, dass der direkt anzusprechende E-Mail-Server ein Edge-Server sein muss. Es muss aber ein Exchange Server mit Transport-Rolle sein. Hinsichtlich der von Microsoft unterstützten Varianten bleiben Ihnen für den offiziellen Betrieb des hybriden E-Mail-Verkehrs die beiden folgenden Optionen:

1. direkter SMTP-Zugriff aus dem Internet auf einen oder mehrere Exchange Server mit Mailbox-Rolle im internen Unternehmensnetzwerk
2. direkter SMTP-Zugriff aus dem Internet auf einen oder mehrere Exchange Server mit Edge-Transport-Rolle im Perimeter-Netzwerk

In Abbildung 2.11 erkennen Sie den Unterschied zwischen diesen beiden Varianten. Da die meisten Unternehmen eine direkte Verbindung zu Systemen, die sich im internen Unternehmensnetzwerk befinden, nicht zulassen, ist die zweite Option die beste Wahl, wenn eine Hybridanbindung mit Exchange Online gewünscht ist.

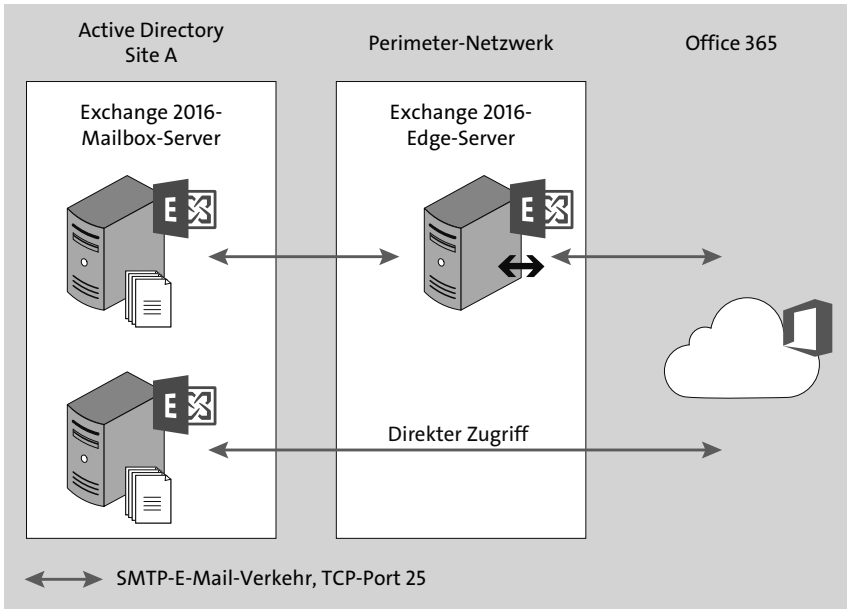

Abbildung 2.11 Vergleich des hybriden E-Mail-Verkehrs mit und ohne Edge-Transport-Server

Aber was ist eine hybride Konfiguration für den E-Mail-Verkehr? Eine hybride Konfiguration zwischen einer lokalen Exchange-Organisation und Exchange Online wird immer dann benötigt, wenn sich E-Mail-aktivierte Objekte sowohl in der lokalen Exchange-Organisation als auch in Exchange Online befinden. Mögliche Konstellationen sind z. B.:

- Exchange-Benutzerpostfächer befinden sich in der lokalen Exchange-Organisation und in Exchange Online.
- In der lokalen Exchange-Organisation befinden sich öffentliche Ordner mit E-Mail-aktivierten Ordnern.
- Alle Exchange-Benutzerpostfächer befinden sich in Exchange Online und es wird eine zentrale E-Mail-Signatur-Lösung verwendet.
- Das *Journaling*-Postfach ist aktiv und wird auf einem lokalen Exchange Server gehostet, während sich alle Exchange-Benutzerpostfächer in Exchange Online befinden.

Es gibt also zahlreiche Gründe, warum ein hybrider E-Mail-Verkehr notwendig ist.

2.5 Exchange Server auf physischen Systemen

Exchange Server wurde schon immer auf physischen Servern installiert, und erst mit dem Aufkommen von Virtualisierungsplattformen ergaben sich neue Möglichkeiten. Nichtsdestotrotz ist und bleibt der Betrieb von Exchange Server auf physischen Systemen die empfohlene Methode.

Wie in Abschnitt 2.2 beschrieben, ist einer der größten Vorteile moderner Exchange-Versionen, dass für den Betrieb Standardserver (sogenannte *Commodity Server*) mit kostengünstigem Datenspeicher eingesetzt werden können. Es gibt keine technisch begründete Notwendigkeit, teuren SAN-Speicher einsetzen zu müssen.

SAN oder nicht SAN?

Ob Sie Ihren Exchange-Systemen SAN-Datenspeicher zur Verfügung stellen oder nicht, müssen Sie selbst entscheiden. Ich weise nur immer wieder darauf hin, dass dies technisch absolut nicht notwendig ist und in den meisten Fällen nur unnötig die Betriebskosten in die Höhe treibt. Das Kostenargument wiegt umso schwerer, wenn Sie den Betrieb Ihrer Serversysteme und Datenspeicher an einen externen Dienstleister ausgelagert haben.

Da der Bedarf an Datenspeicher unter anderem durch die Anzahl der Datenbankkopien bestimmt wird, sehen clevere Vertreter des Managements hier immer die erste Möglichkeit, um den Rotstift anzusetzen. Dies führt aber automatisch zu einer Designanpassung der Exchange Server-Plattform, die nichts mehr mit Hochverfügbarkeit zu tun hat.

Seien Sie standhaft, und verteidigen Sie die Speicheranforderungen für Ihr Exchange Server-Plattformdesign. Exchange Server bevorzugt Festplatten in einer JBOD-Konfiguration. SAN-Speicher ist zu teuer und erhöht nur die Anzahl möglicher Fehlerquellen.

Ein Standardserver für den Betrieb von Exchange Server 2019 verfügt über folgende Hardware-Konfiguration:

- 2U (Höheneinheiten)
- Dual-Sockel-CPU (24 bis 48 Cores), je nach Prozessortyp
- bis zu 256 GB Arbeitsspeicher
- batteriegepufferter Write-Cache-Controller
- 12 oder mehr Festplattenbänke im 2U-Servergehäuse
- 1 Netzwerkadapter *ohne* Teaming
- SSD für MCDB in Exchange Server 2019

Abbildung 2.12 verdeutlicht die erforderlichen Komponenten für ein physisches System mit Exchange Server.

Die lokal im Servergehäuse zur Verfügung stehende Festplattenkapazität kann bei Bedarf durch zusätzliche *DAS-Laufwerke* erweitert werden. Innerhalb jedes Diskpools für Postfachdatenbanken wird eine Festplatte als sogenannter Hot-Spare für *Auto-Reseed* konfiguriert. AutoReseed ermöglicht es einem Exchange Server, die Datenbankredundanz bei Ausfall einer Festplatte automatisch wiederherzustellen, indem eine Reservefestplatte (Hot Spare) automatisch aktiviert und für die vom Ausfall betroffenen Datenbankkopien in Betrieb genommen wird.

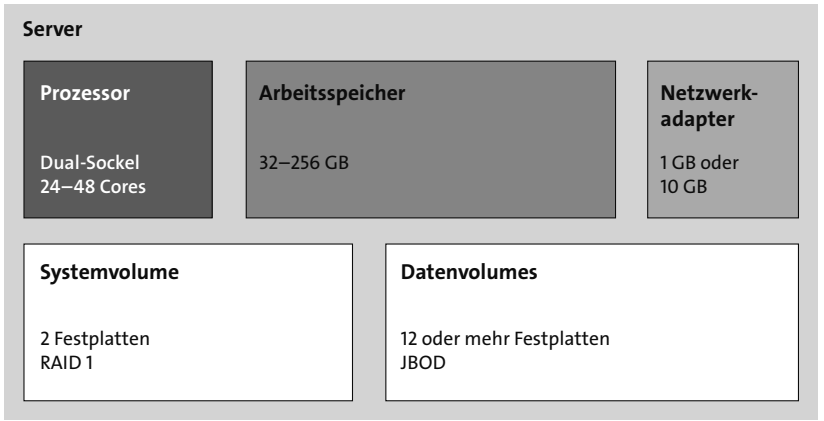

Abbildung 2.12 Exchange Server auf einem physischen System

Die Konfiguration der lokalen Festplatten ist in Tabelle 2.1 dargestellt.

Zweck	Betriebsart	Disktyp
Betriebssystem, Exchange Server, Exchange-Protokolldateien, Transportdatenbank	RAID1 NTFS BitLocker	SAS, 7,2K RPM
Postfachdatenbanken, Transaktionsprotokolle, Inhaltsindizes	JBOD ReFS BitLocker	SAS, 7,2K RPM

Tabelle 2.1 Festplattenkonfigurationen für physische Server

Wie Sie sehen, sind die Hardware-Anforderungen und empfohlenen Hardware-Konfigurationen sehr überschaubar. Gerade im Hinblick auf Erweiterungen oder auf den Austausch im Fehlerfall sind diese Anforderungen hilfreich.

Optional können Sie das Serverdesign um SSD-Festplatten für die Metacache-Datenbanken (eine neue Funktion von Exchange Server 2019) erweitern. Idealerweise planen Sie hierzu allerdings den Einsatz von M.2-SSDs ein, die mithilfe eines *Riser-Boards* direkt im Server platziert werden.

Exchange unterstützt die folgenden physischen Datenträgertypen:

- Serial ATA (SATA)
- Serial Attached SCSI (SAS)
- Fibre Channel
- Solid-State-Disks (SSD)

2.6 Exchange Server auf einer Hypervisor-Plattform

Moderne Exchange Server-Versionen können natürlich auf unterstützten Hypervisor-Plattformen betrieben werden (*https://docs.microsoft.com/Exchange/plan-and-deploy/virtualization*).

Bei der Virtualisierung von Exchange Server werden dem Gastbetriebssystem die benötigten Ressourcen über die Konfiguration des Hypervisor-Hosts zugewiesen. Hierzu gehören:

- Prozessor-Cores
- Arbeitsspeicher
- Netzwerkadapter
- Festplattenspeicher

Was ist ein Hypervisor?

Ein Hypervisor trennt die vorhandene Hardware eines Systems als abstrahierte Schicht von zusätzlich zu installierenden virtuellen Systemen auf bzw. über dem Hypervisor (siehe Abbildung 2.13).

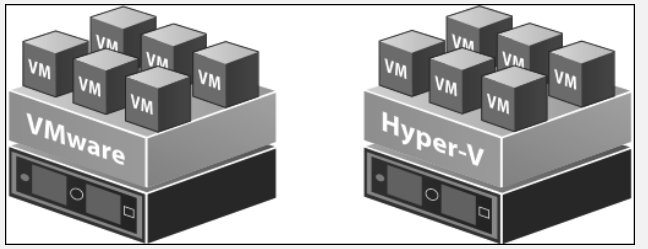

Abbildung 2.13 VMware und Hyper-V als Hypervisor-Plattformen für die Ausführung mehrerer virtueller Systeme auf einer Hardware

Im Rahmen einer Virtualisierung können heutzutage sowohl vollständige Serverbetriebssysteme als auch nur Serverapplikationen (z. B. mit Docker) virtualisiert betrieben werden. Exchange Server unterstützt die Virtualisierung als (Container-) Applikation nicht. Exchange Server muss immer in einem vollständig virtualisierten Gastbetriebssystem betrieben werden.

Die Anforderungen an ein virtualisiertes Exchange Server-System entsprechen genau den Anforderungen für physische Exchange Server (siehe Abbildung 2.14). Hierzu gehört, dass die zugewiesenen Ressourcen für Prozessor und Arbeitsspeicher als fest reservierte Ressourcen konfiguriert sind. Diese Abhängigkeit wird für den Betrieb von virtualisierten Exchange Servern häufig ignoriert.

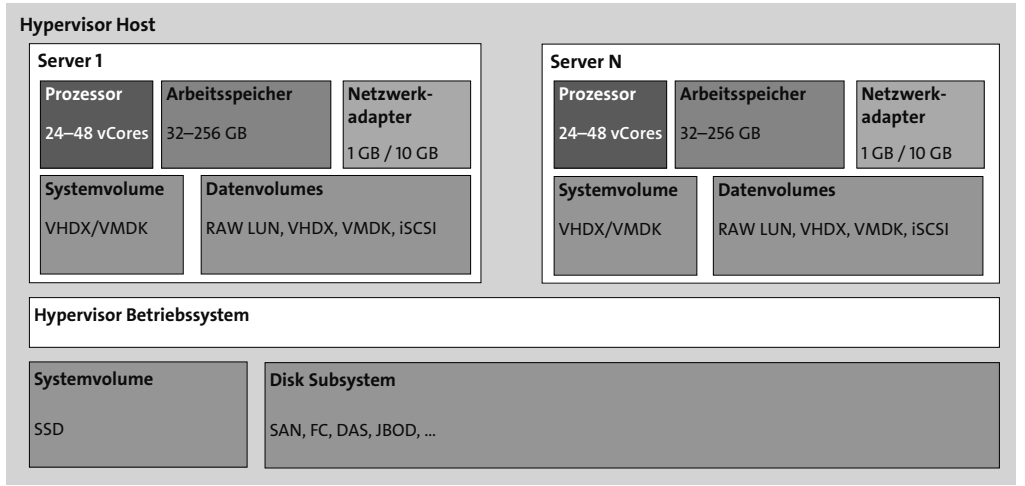

Abbildung 2.14 Exchange Server in einer Hypervisor-Plattform

Hypervisor-Funktionen zur Hochverfügbarkeit

Die Marketingabteilungen von Hypervisor-Herstellern preisen eifrig ihre neuesten Funktionen rund um Hochverfügbarkeit an. Diese Funktionen werden auch gern in sogenannten *Best Practices Guides für Exchange* platziert.

All die angepriesenen HA-Funktionen der Hypervisor-Hersteller sind für einen sicheren und stabilen HA-Betrieb von Exchange Server unnötig. Die HA-Komponente von Exchange Server ist die Database Availability Group (DAG).

In den meisten Fällen werden Applikationen auf einer Hypervisor-Plattform betrieben, weil es in der Vergangenheit eine Managemententscheidung für 100 % Virtualisierung gab. Diese Entscheidung wurde aber später nie überprüft, geschweige denn infrage gestellt.

Auch im Betrieb virtualisierter Systeme gibt die Applikation die Anforderungen vor und nicht die Hypervisor-Plattform. Sie kennen sicher die Situation, dass Ihr Hypervisor-Team Ihnen vorschreibt, wie ein mögliches System konfiguriert ist.

Ein Beispiel:

Sie benötigen für Ihre Exchange Server je ein System mit 16 Cores, 48 GB Arbeitsspeicher, 1 Systemvolume à 128 GB und 6 Datenvolumes à 2 TB.

Sie können aber maximal je Server 8 Cores, 32 GB Arbeitsspeicher, 1 Systemvolume à 80 GB und 4 Datenvolumes à 1 TB bekommen.

Was machen Sie?

In den meisten Fällen geht es hauptsächlich um den Betrieb und die genaue Abgrenzung der Zuständigkeiten zwischen den Abteilungen. Im oben genannten Beispiel werden Ihnen die Einschränkungen aus reiner Faulheit präsentiert, da das Hypervisor-Team Ihnen die Systeme nur auf Basis einer Vorlage bereitstellen möchte. Seien Sie standhaft, und fordern Sie die Systemkonfiguration, die Sie festgelegt haben. Um unnötige Diskussionen zu vermeiden, die meist sehr schnell emotional geführt werden, erfragen Sie vor der Planung Ihrer virtualisierten Exchange-Umgebung, welche Maximalkonfiguration technisch möglich ist. Passen Ihre Anforderungen nun gar nicht zur Hypervisor-Plattform, so kann in den meisten Fällen horizontal skaliert werden; Sie benötigen z. B. acht anstelle von sechs Servern. Diese horizontale Skalierung geht natürlich mit anderen Abhängigkeiten einher:

- zusätzliche Windows Server-Lizenzen
- zusätzliche Exchange Server-Lizenzen
- zusätzliche Lizenzen für Drittanbieter-Software auf Exchange Server-Systemen
- zusätzlicher Speicherbedarf für System- und Datenvolumes

Meine Empfehlungen für die Konfiguration eines virtualisierten Exchange Server-Systems finden Sie in Tabelle 2.2.

Komponente	Empfehlung
CPU	Maximal 24 Cores Kein Hyperthreading
Arbeitsspeicher	Maximal 256 GB RAM Fest reserviert, ohne dynamische Verwaltung wie *Ballooning* oder ähnliche Technologien
Netzwerkadapter	1 Netzwerkadapter mit mindestens 1 GB
Systemvolume	128 GB Dateiformat NTFS
Datenvolumes	Größe ja nach Bedarf Dateiformat ReFS LUNs auf dedizierten Spindeln

Tabelle 2.2 Empfehlung für ein virtualisiertes Exchange Server-System

Diese Empfehlung stellt keinen Ersatz für die Ergebnisse aus dem *Exchange Sizing Calculator* dar. Sie ist eher die Essenz aus meinen Erfahrungen im Betrieb virtualisierter Exchange Server bei Kunden.

In einer Hypervisor-Plattform wird der Festplattenspeicher für Hypervisor-Hosts aus einer ebenfalls virtualisierten Festplattenumgebung bereitgestellt. Innerhalb dieser Speicherumgebung werden eine oder mehrere physikalische Festplatten zu einer logischen Speichereinheit (*Logical Unit Number*, *LUN*) konfiguriert. Diese Speichereinheit kann nun dem Hypervisor-Host als Speichermedium für virtualisierte Festplatten zur Verfügung gestellt oder aber direkt mit einem Hypervisor-Gast verbunden werden. Welches die bessere Variante ist, hängt ganz vom Softwarestand der bei Ihnen eingesetzten Hypervisor-Plattform und von der eingesetzten Lösung zur Virtualisierung von Festplatten ab.

Sinn und Unsinn von Virtualisierung

Sie haben sicherlich den Eindruck gewonnen, dass ich nicht der größte Freund einer Virtualisierung von Exchange Server bin. Hypervisor-Plattformen wurden in der Vergangenheit eingeführt, weil man dem Versprechen (der Hypervisor-Anbieter) von Kostenreduktion und Kapazitätsverdichtung gefolgt ist. Leider wurden viele Hypervisor-Plattformen zwar technisch implementiert, das technische Personal wurde aber nie umfassend für die Hypervisor-Plattform geschult.

Das Thema Virtualisierung endet nun einmal nicht bei der Hypervisor-Plattform, auf der *nur* das Gastsystem betrieben wird. Die wirklich großen Probleme betreten die Bühne, wenn ein schlecht konfiguriertes System zur Virtualisierung von Festplattenspeicher mitspielt oder aktive Netzwerkkomponenten in der Hypervisor-Plattform ihr Eigenleben entwickeln.

Wenn Sie von Ihrem Hypervisor-Team nicht die Systemkonfiguration erhalten, die Sie für Ihre Exchange-Systeme festgelegt haben, können Sie *keine* Aussage über die Exchange-Performance machen und *keinerlei* SLA zusichern. Lassen Sie sich hier nie auf einen Handel ein!

System-Volumes werden in Hypervisor-Plattformen meist als virtualisierte Festplattendatei (z. B. *VHD*, *VHDX* oder *VMDK*) bereitgestellt. Daten-Volumes wiederum können sowohl als virtualisierte Festplattendatei oder als sogenanntes *RAW Device* bereitgestellt werden. Wird ein Daten-Volume als virtualisierte Festplatte bereitgestellt, so muss die virtualisierte Festplatte in der Hypervisor-Plattform für den gesamten Speicher reserviert sein (VMware-Terminologie: *Thick Provisioning Eager Zeroed*). Nur so wird die gewünschte vollständige Leistung beim Schreiben von Daten erreicht. Diese Art der Bereitstellung bietet sich auch für Systemvolumes an.

2.7 Exchange Server in einer Cloud-Plattform

Der Betrieb eines oder mehrerer Exchange Server in einer Cloud-Plattform ist technisch identisch mit dem Betrieb auf einer Hypervisor-Plattform. Der größte Unterschied ist, dass Sie die Hypervisor-Plattform nicht selbst betreiben, sondern diese als *Infrastructure-as-a-Service* (IaaS) mieten.

In einer Cloud-Plattform können Sie unterschiedliche Nutzungsszenarien aufbauen:

- Betrieb einer vollständigen Exchange-Organisation, mit einer Netzwerkanbindung als Erweiterung des internen Unternehmensnetzwerks
- Betrieb von Exchange Servern mit Edge-Transport-Rolle, sozusagen im ausgelagerten Perimeter-Netzwerk
- Betrieb von Exchange Servern im Rahmen einer Koexistenz mit Office 365 (aka *Hybrid-Server*)

  Es gibt technisch keine Exchange Server-Rolle mit dem Namen »Hybrid-Server«. In einer hybriden Konfiguration mit Office 365 wird der eingesetzte Exchange Server umgangssprachlich gerne so benannt. Die korrekte technische Bezeichnung ist *Koexistenz-Rolle*. Diese Bezeichnung wird auch nach der Lizenzierung über das Cmdlet `Get-ExchangeServer` angezeigt.
- Betrieb des *File-Share-Witness-Servers*, der technisch betrachtet zwar kein dedizierter Exchange Server ist, aber trotzdem dazugehört

Abbildung 2.15 zeigt Ihnen die Platzierung von Exchange Server in *Microsoft Azure*. Die Anbindung zwischen der lokalen Netzwerkinfrastruktur des Unternehmens und der virtualisierten Netzwerkinfrastruktur von Microsoft Azure erfolgt über eine VPN-Verbindung. Interne Clients greifen hierbei immer über die VPN-Verbindung auf Exchange zu. Für Exchange wird in diesem Beispiel auch ein separater Domänen-Controller in Azure benötigt, da ein sicherer Exchange-Betrieb sonst nicht gewährleistet werden kann.

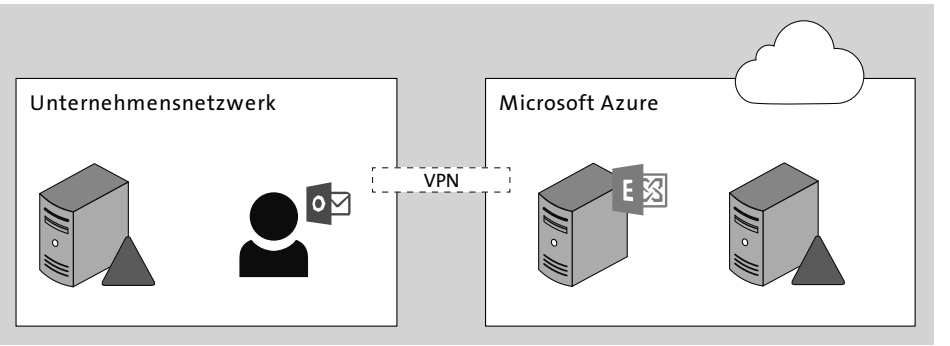

Abbildung 2.15 Exchange Server in einer Infrastructure-as-a-Service-Implementierung

Ob eines dieser Szenarien für Sie passend erscheint, müssen Sie entscheiden. Der Umzug zu einem Clouddienst mit virtualisierten Exchange Servern wird gerne dann durchgeführt, wenn die lokale Hypervisor-Plattform nicht mehr über ausreichende Kapazitäten verfügt oder nur für den Zeitraum einer Migration der lokalen Exchange-Umgebung zu Office 365 benötigt wird.

Ob Sie sich nun für Microsoft Azure als IaaS-Anbieter entscheiden oder aber für einen alternativen Anbieter, müssen Sie selbst entscheiden. Im Rahmen eines unterstützten Betriebs steht Ihnen nur der Weg zu Microsoft Azure offen. Der Betrieb von Exchange Server auf einer anderen Cloud-Plattform wird nicht unterstützt. Ebenso gibt es genaue Vorgaben für den zu verwendenden Diskspeicher, damit ein unterstützter Betrieb von Exchange Server in Microsoft Azure gewährleistet ist.

2.8 Exchange als Software-as-a-Service (SaaS)

Eine weitere Option für die Nutzung von Exchange Server ist *Software-as-a-Service*. Das bekannteste SaaS-Angebot ist *Exchange Online* als Bestandteil des Office 365-Angebotes von Microsoft. Obwohl es neben Office 365 noch weitere Anbieter am Markt gibt, die auf der Basis von Exchange Server E-Mail-Funktionen anbieten, werde ich mich hier auf Office 365 und Exchange Online beschränken.

Office 365 und Microsoft 365

Microsoft ist gut darin, Produkt- und Dienstbezeichnungen regelmäßig anzupassen. Im Rahmen der SaaS-Angebote von Microsoft begegnen Ihnen die Begriffe Office 365 und Microsoft 365 regelmäßig. Wo ist der Unterschied?

Der Name »Office 365« steht als allumfassende Klammer für alle SaaS-Produkte und -Dienste, die Endanwender nutzen können. Ergänzend wird der Name für die aus der Cloud installierbare Office Desktop-Version verwendet. Dieses installierbare Produkt hat den Namen *Microsoft 365 Apps*, die früher unter dem Namen *Office 365 ProPlus* bekannt waren. Dieses Applikationspaket steht, je nach Lizenzplan, in den Varianten *Microsoft 365 Apps for Enterprise* oder *Microsoft 365 Apps for Business* zur Verfügung.

Microsoft 365 wiederum ist der Name für ein Produktpaket, das auch Office 365 umfasst. Zusätzlich umfasst es die Lizenzierung von Windows Enterprise und die erweiterten Enterprise Mobility- und Security-Schutzfunktionen von Office 365.

Die Lizenzierung von Office 365 und Microsoft 365 ist ein komplexes Thema. Wenn Sie sich einen guten und leicht zu lesenden Überblick verschaffen möchten, empfehle ich Ihnen die Webseite *Microsoft 365 Licensing* von Aaron Dinnage (*https://m365maps.com*). Er hat das Kunststück vollbracht, die Komplexität der Lizenzierung übersichtlich darzustellen. Jede dargestellte Komponente ist mit den Detailinformation der Microsoft Online-Dokumentation verlinkt.

Das SaaS-Angebot bietet Ihnen als Kunden grundsätzlich zwei Möglichkeiten für die Nutzung von Exchange Server-Funktionen:

- Nutzung von Exchange Server-Funktionen nur in Office 365 (auch als *Cloud-Only* bezeichnet)
- Nutzung von Exchange Server-Funktionen in Office 365 und in der lokalen Exchange-Organisation durch einen Hybrid-Betrieb

Bei der reinen Nutzung von Office 365 betreiben Sie keinen Exchange Server in Ihrer lokalen IT-Infrastruktur. Alle Postfächer werden bei Exchange Online gehostet. Die Verwaltung der Benutzerkonten für diese Postfächer erfolgt entweder in Office 365 oder in Ihrer lokalen Active Directory-Infrastruktur. In letzterem Fall spricht man noch nicht von einer Hybrid-Umgebung.

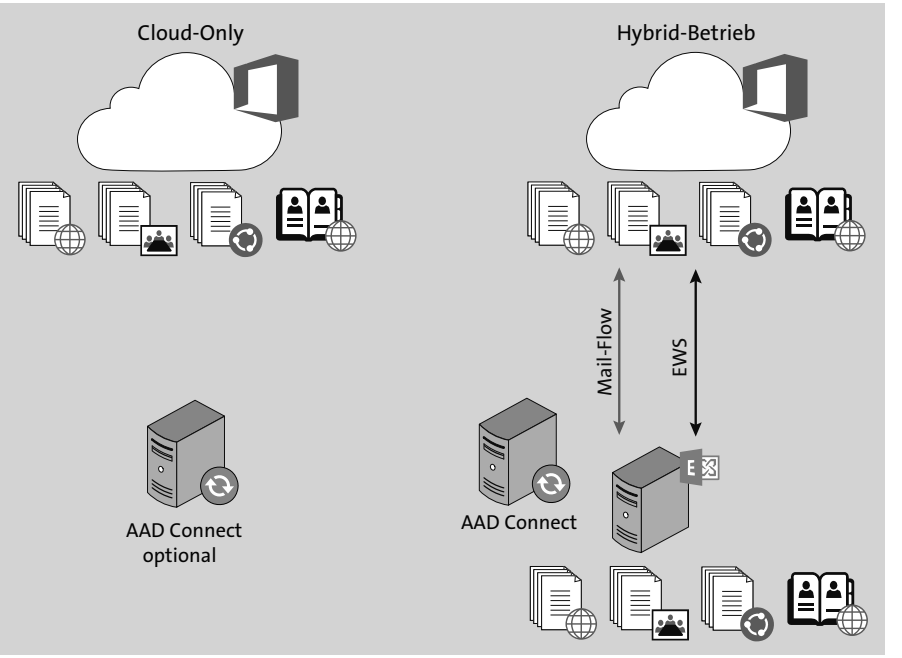

Abbildung 2.16 Der Unterschied zwischen Cloud-Only- und Hybrid-Betrieb

Eine Hybrid-Umgebung beschreibt die Anbindung einer lokalen Exchange-Organisation an Exchange Online. Es existieren sowohl Postfächer auf Exchange Servern in der lokalen IT-Infrastruktur als auch in Exchange Online. In solch einem Fall spricht man von einer *Rich-Hybrid*-Implementierung (siehe Abbildung 2.17). Wird eine hybride Anbindung nur für das Verschieben von lokalen Postfächern hin zu Exchange Online implementiert, spricht man von einer *Simple-Hybrid*-Implementierung. Das Ziel einer Simple-Hybrid-Implementierung ist immer das Verschieben aller Postfächer zu Office 365.

Eine Rich-Hybrid-Implementierung ist immer dann erforderlich, wenn Anwender beider Umgebungen in die Lage versetzt werden sollen, auf Verfügbarkeitszeiten für Terminplanungen mit Teilnehmern aus der jeweils anderen Umgebung zuzugreifen oder wenn z. B. bestimmte Postfächer aus rechtlichen Gründen nicht zu Office 365 verschoben werden dürfen. Ein anderes Anwendungsbeispiel ist die Platzierung der Öffentlichen Ordner auf Servern in der lokalen Infrastruktur, während die Benutzer-Postfächer in Exchange Online gehostet werden.

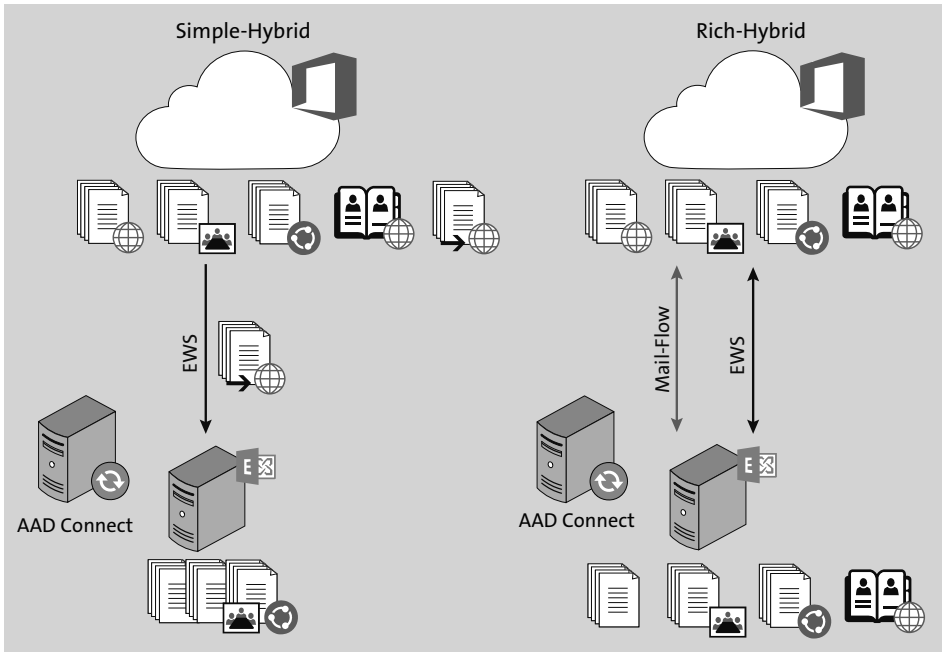

Abbildung 2.17 Der Unterschied zwischen der Simple-Hybrid- und der Rich-Hybrid-Implementierung

Bei der Bestimmung der Betriebsart einer hybriden Implementierung wird nicht nur die Lokation von Postfächern und der Zugriff darauf betrachtet. Die andere wichtige Funktion von Exchange Server ist die Art und Weise der E-Mail-Zustellung. Die E-Mail-Zustellung von und zu Exchange-Postfächern erfolgt in den seltensten Fällen direkt an die Exchange Server, die Benutzer-Postfächer hosten. Im SaaS-Angebot von Office 365 erfolgen die Zustellung und der Versand über *Exchange Online Protection*. Eine lokale Exchange Server-Infrastruktur verwendet für den Versand und Empfang von Nachrichten entweder Server mit der Exchange-Edge-Transport-Rolle oder E-Mail-Gateway-Systeme von Drittanbietern.

Im Rahmen einer Nutzung von Exchange Online spricht man bei der Konfiguration der E-Mail-Zustellung von zwei Varianten (siehe Abbildung 2.18):

- normaler Mail-Flow
- zentralisierter Mail-Flow

Die Variante *normaler Mail-Flow* bedeutet, dass eingehende Nachrichten von externen Absendern und ausgehende Nachrichten an externe Empfänger durch *Exchange Online Protection* verarbeitet werden. Im Gegensatz dazu werden bei der Variante *zentralisierter Mail-Flow* die Nachrichten von Postfächern in Exchange Online zu einem Exchange Server in Ihrer lokalen Infrastruktur geleitet, um dann über ein Gateway eines Drittanbieters ihren Weg ins Internet zu finden. Eingehende Nachrichten werden hierbei direkt vom Gateway eines Drittanbieters empfangen und entweder an ein lokales Postfach oder an ein Postfach in Exchange Online geleitet.

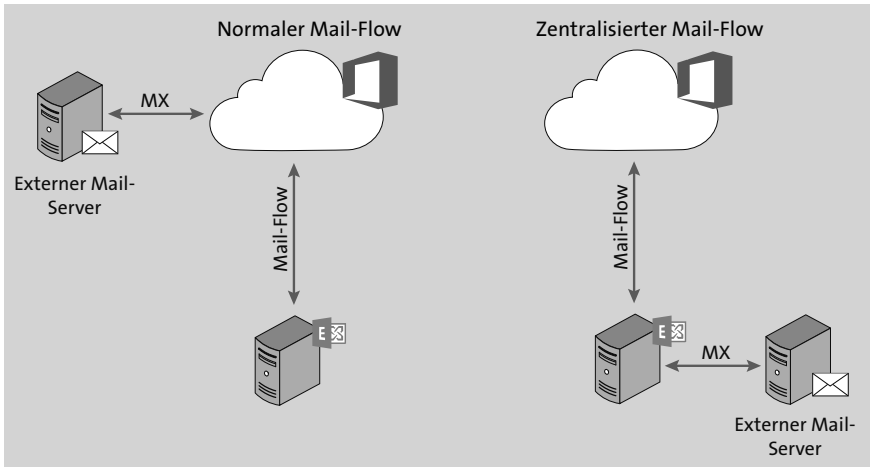

Abbildung 2.18 Der Unterschied zwischen dem normalen und dem zentralisierten Mail-Flow

Die einfachen Übersetzungen dieser beiden Varianten für den E-Mail-Transport sind:

- **Normaler Mail-Flow:** Der MX-DNS-Eintrag verweist auf Exchange Online Protection.
- **Zentralisierter Mail-Flow:** Der MX-DNS-Eintrag verweist auf Ihre lokale IT-Infrastruktur.

Die Anbindung von Exchange Online an die lokale IT-Intrastruktur erfordert für E-Mail-Nachrichten eine direkte SMTP-Verbindung zu einem lokalen Exchange Server. Der Grund für diese Anforderung ist, dass es sich technisch um zwei getrennte Exchange-Organisationen handelt, die im Rahmen ihrer gemeinsamen Hybrid-Konfiguration als eine »einheitliche« Exchange-Organisation agieren. Nachrichten zwischen diesen beiden Organisationen werden als »intern« angesehen und besonders behandelt.

Grundsätzlich ist es zwar möglich, hierzu auch einen SMTP-Server eines Drittanbieters zu implementieren, jedoch ist eine solche Anbindung immer fehlerbehaftet, da Informationen aus den Kopfinformationen der Nachrichten herausgefiltert werden. Aber gerade diese Informationen sind für einen stabilen und sicheren Betrieb einer hybriden Exchange-Implementierung notwendig.

Meine Empfehlung lautet: Damit der Nachrichtenfluss über eine Exchange-Hybrid-Anbindung funktioniert, sollten Sie Edge-Transport-Server verwenden. Die Details dazu finden Sie in Abschnitt 2.4.

In Kapitel 8 befassen wir uns ausführlich mit Exchange Online.

2.9 Unified Messaging (UM)

Exchange Server 2019 beinhaltet keine *Unified Messaging*-Rolle mehr. Daher ist eine Anbindung von *Skype for Business* (SfB) an Exchange Server 2019 nicht mehr möglich. Die Nutzung von Voice-Mail-Funktionen erfordert den Betrieb einer lokalen Skype for Business-Plattform und/oder die Nutzung von *Cloud Voice Mail* als Bestandteil von Office 365.

Tabelle 2.3 gibt Ihnen einen Überblick über die Möglichkeiten zur Implementierung von Voice-Mail-Funktionen.

Enterprise Voice	Postfach-Server-Version	Exchange UM	Exchange Online UM	Cloud VoiceMail
SfB 2015	Exchange 2016	Ja	Nein	Nein
SfB 2015	Exchange 2019	Nein	Nein	Nein
SfB 2015	Exchange Online	Nein	Ja	Nein
SfB 2019	Exchange 2016	Ja	Nein	Nein
SfB 2019	Exchange 2019	Nein	Nein	Ja
SfB 2019	Exchange Online	Nein	Nein	Ja
SfB Online	Exchange 2016	Nein	Nein	Ja
SfB Online	Exchange 2019	Nein	Nein	Ja
SfB Online	Exchange Online	Nein	Nein	Ja
SfB Online (ohne EV[1])	Exchange 2016	Nein	Nein	Ja

Tabelle 2.3 Möglichkeiten zur Voice-Mail-Nutzung je nach Exchange-Version

Kapitel 9
Exchange und Compliance

Oft wird sehr viel Aufwand betrieben, um sich gegen Malware-Angriffe von externen Quellen zu schützen. Der Schutz vor dem Abfluss sensibler Unternehmensinformationen wird dagegen sträflich vernachlässigt. Mit Data Loss Prevention (DLP) können Sie Ihr Unternehmen vor unberechtigtem Datenabfluss schützen.

Wenn man über den Betrieb einer Exchange Server-Plattform spricht, kommt man früher oder später zu den Themen *Compliance* und *Archivierung*. Beides sind Begriffe, die unterschiedlich interpretiert werden und die in ihrer Bedeutung für ein Unternehmen ebenso unterschiedlich gewichtet werden. Seit der Veröffentlichung von Exchange Server 2019 hat sich das Produkt im Themenfeld Compliance nicht sonderlich weiterentwickelt. In Exchange Online sieht dies anders aus.

Im Clouddienst Microsoft 365 existiert ein dediziertes *Compliance Center* unter *https://compliance.microsoft.com/*, das Compliance-Funktionen für Microsoft 365-Workloads bereitstellt und seit dem Sommer 2022 den Namen *Purview Compliance-Portal* trägt. DLP-Regeln gegen den Verlust von Daten lassen sich, einheitlich konfiguriert, auf mehrere Ziele anwenden. So besteht keine Notwendigkeit mehr, getrennte Regeln für Exchange Online, SharePoint Online oder Teams zu erstellen. Zum Compliance Center gehört auch eine RBAC-basierte Zugriffssteuerung, um sicherzustellen, dass nur berechtigte Personen auf möglicherweise sensible Daten zugreifen können. Die Funktionen des Microsoft 365 Compliance Centers sind um ein Vielfaches umfangreicher als die in Exchange Server 2019 integrierten Funktionen. Allein aus diesem Grunde kann eine Migration zu Microsoft 365 und Exchange Online sinnvoll sein. Die Betrachtung des Compliance Centers ist nicht Bestandteil dieses Buches.

Bevor wir uns den Funktionen und Möglichkeiten zuwenden, die uns Exchange Server 2019 für die beiden Themenkomplexe bietet, müssen wir uns zu Beginn auf eine gemeinsame Definition der Begriffe einigen. Diese Einigung müssen Sie auch in Ihrem Unternehmen erreichen, bevor Sie diese Themen im Detail weiterverfolgen. Ohne solch eine Einigung auf die Bedeutung der Begriffe wird es unweigerlich zu Missverständnissen kommen.

9.1 Begriffsklärung

Der Begriff *Archivierung* wird gerne und schnell verwendet, wenn es um die Aufbewahrung von E-Mail-Nachrichten und verwandten Objekten geht. »Verwandte Objekte« sind in diesem Kontext alle weiteren Objekttypen, die Exchange Server speichert, z. B. Kalendereinträge, Notizen, Sprachnachrichten oder auch Skype for Business-Unterhaltungen.

Im Bereich der Archivierung müssen wir die folgenden Varianten thematisch unterscheiden und klar gegeneinander abgrenzen:

- Archivierung zur Verkleinerung der Postfachgröße; hierzu gehören auch Postfächer für Öffentliche Ordner.
- Archivierung zur Zusammenführung von Objekten aus unterschiedlichen Systemen, z. B. ERP- oder CRM-Systemen
- rechtssichere Archivierung; unter Umständen auch als Compliance-Archiv bezeichnet

Technisch unterscheiden wir zwei Möglichkeiten zur Archivierung von Objekten:

- serverbasierte Archivierung von Objekten, ganz ohne Interaktion durch den Anwender
- clientbasierte oder manuelle Archivierung von Objekten; erfolgt durch Auswahl und Verschlagwortung durch den Anwender.

Archivierung beschreibt also die Ablage und die Aufbewahrung von Objektdaten für einen definierten Zeitraum. Den Zustand dieser archivierten Daten bezeichnet man mit dem englischen Begriff *at rest*.

In den folgenden Abschnitten werde ich Empfehlungen für die Archivierungsvarianten aussprechen, jedoch ist jede dieser Empfehlungen durch meine subjektive Erfahrung in Kundenprojekten geprägt. Sie müssen für Ihr Unternehmen immer die passende Lösung finden und – was noch wichtiger ist – auch rechtlich prüfen lassen. Ohne eine rechtliche Prüfung wähnen Sie sich in einer trügerischen Sicherheit.

Im Gegensatz zur Archivierung beschreibt der Begriff *Compliance* den Umgang mit Daten, an denen Anwender arbeiten oder die in dem Moment, in dem sie versendet werden, geschützt werden müssen. Zusätzlich zu den gesetzlichen Anforderungen müssen Regelungen berücksichtigt werden, die durch die Compliance-Abteilung definiert wurden. Compliance-Regeln sind eine Kombination aus Regeln, die extern verpflichtend und intern freiwillig definiert wurden.

Eine kombinierte Zwischenstufe aus Archivierung und Compliance bilden die beiden Möglichkeiten zur Aufbewahrung von Nachrichten in Postfächern, die Exchange Server 2019 bietet. Aus Sicht von Exchange Server sind die Grenzen zwischen klassischer Archivierung und einer Compliance-basierten Aufbewahrung von Nachrichten unscharf. Daher erläutere ich das Thema in zwei getrennten Abschnitten.

Im Rahmen der Compliance definieren Sie unter anderem:

- Welche Arten von Dokumententypen gibt es (z. B. intern, vertraulich, geheim)?
- Wie ist jeder einzelne Dokumententyp zu schützen?
- Wo und wie darf oder muss jeder einzelne Dokumententyp gespeichert werden?
- Welchem Personenkreis ist es erlaubt, einen bestimmen Dokumententyp an externe Empfänger zu senden?
- Über welche Kommunikationswege darf oder muss auf einen bestimmten Dokumententyp zugegriffen werden?
- Welcher Personenkreis unterliegt einer vollständigen Aufbewahrungspflicht der gesendeten, empfangenen und bearbeiteten Dokumente?

Die genannten Punkte erheben keinen Anspruch auf Vollständigkeit. Jedes Unternehmen hat ganz eigene Anforderungen an den Umgang mit Dokumenten. Die Anforderungen ergeben sich aus dem Schutzbedarf der Informationen und aus dem Tätigkeitsfeld des Unternehmens.

9.2 Archivierung

Die Aufbewahrung von Postfachinhalten kann entweder mit dem zum Exchange Server 2019-Funktionsumfang gehörenden Online Archiv-Postfach oder mithilfe einer Drittanbieter-Lösung erfolgen. Beide Optionen haben ganz unterschiedliche Vor- und Nachteile.

9.2.1 Exchange Server-Archiv-Postfach

Mit Exchange Server 2010 wurde das *Online Archiv-Postfach* eingeführt. In der damaligen Zeit waren die hohen Kosten für Festplattenspeicher der Grund für diese neue Funktion. Online Archiv-Postfächer konnten in separaten Postfachdatenbanken bereitgestellt werden, die auf kostengünstigeren Festplatten gespeichert waren. So wurden die primären Benutzerpostfächer auf *Tier-1-Speicher*, also schnellen und teuren Festplatten, und Online Archiv-Postfächer auf *Tier-2-Speicher*, also langsameren und günstigeren Festplatten, bereitgestellt (siehe Abbildung 9.1). Anstelle von Tier-1- und Tier-2-Speicher wurden unterschiedliche Speicherqualitäten auch als *Platin*-, *Gold*- und *Silber*-Speicher bezeichnet.

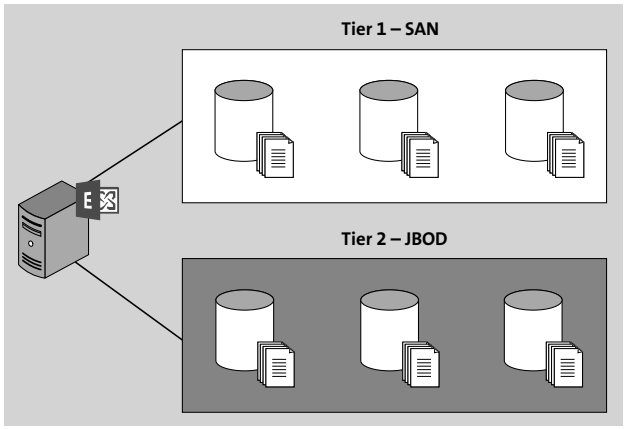

Abbildung 9.1 Bereitstellung von Postfachdatenbanken in Tier-1- und Tier-2-Festplattenspeicher

Diese Option wurde nur in wenigen Exchange Server-Umgebungen realisiert, da die Kunden meist nicht bereit waren, in unterschiedliche Speichertechnologien zu investieren, oder weil das benötigte Fachwissen für den Betrieb unterschiedlicher Technologien nicht vorhanden war.

Technisch handelt es sich bei den Online Archiv-Postfächern um, wie der Name schon sagt, *Online-Postfächer*. Diese Art von Postfächern ist nicht Bestandteil der Outlook-Cached-Mode-Konfiguration, und diese Postfächer werden daher nicht in die lokale OST-Cache-Datei des Windows-Clients synchronisiert. Das erklärte Ziel bei der Einführung der Online Archiv-Postfächer war die Verkleinerung des primären Postfachs von Anwendern, um so die Leistungsfähigkeit des persönlichen Hauptpostfachs sicherzustellen. Dies ist mit modernen Outlook für Desktop-Versionen nicht mehr notwendig.

Die Bereitstellung eines Online Archiv-Postfachs führt aber zu keiner automatischen Archivierung von Objekten aus dem primären Postfach. Erst mithilfe von Aufbewahrungstags und Aufbewahrungsrichtlinien zur Archivierung von Postfachobjekten entfaltet das Online Archiv-Postfach seinen vollen Nutzen. Ich spreche hier bewusst von »Objekten« und nicht nur von »E-Mail-Nachrichten«, da nicht nur E-Mail-Nachrichten, sondern z. B. auch Kalendereinträge archiviert werden können. Die Aufbewahrungsrichtlinien und Aufbewahrungstags finden Sie im Exchange Admin Center im Abschnitt VERWALTUNG DER COMPLIANCE (siehe Abbildung 9.2).

Jedem Postfach wird genau eine Aufbewahrungsrichtlinie zugewiesen. Sie können in einer Exchange-Organisation unterschiedliche Aufbewahrungsrichtlinien definieren. Jede Aufbewahrungsrichtlinie besteht wiederum aus einer Sammlung von zugeordneten Aufbewahrungstags (siehe Abbildung 9.3).

Abbildung 9.2 Aufbewahrungsrichtlinien im Exchange Admin Center

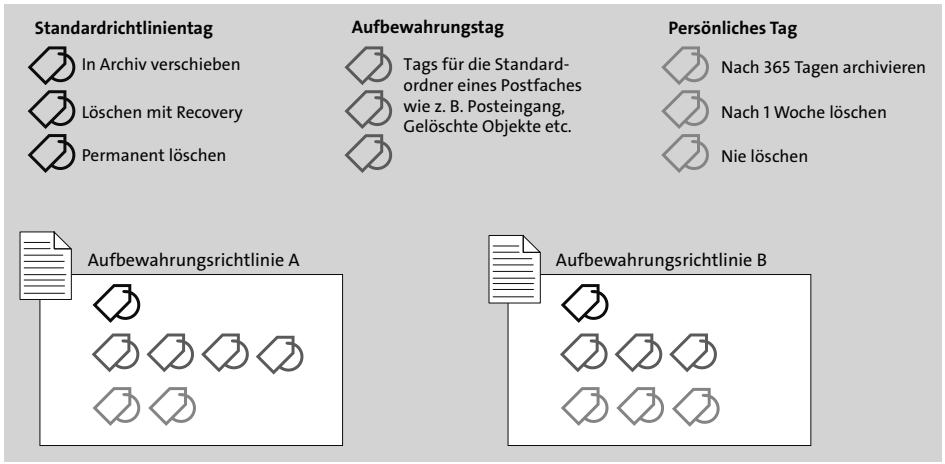

Abbildung 9.3 Zusammenspiel von Richtlinientags und Aufbewahrungsrichtlinien

Es gibt drei unterschiedliche Tag-Arten, über die die Archivierungsfunktionen definiert und gesteuert werden:

- **Standardrichtlinientag** (*Default Policy Tag*, DPT)
  Ein Standardrichtlinientag gilt für das gesamte Postfach und definiert die Aufbewahrungsaktion(en) für die Elemente, für die kein anderes Tag – entweder durch direkte Zuordnung oder durch Vererbung – aktiv ist.

- **Aufbewahrungstag für Standardordner** (*Retention Policy Tag*, RPT)
  Ein RPT wird immer für einen bekannten Standardordner (*Well Known Folder*) eines Postfachs konfiguriert. Sie können für folgende Standardordner Aufbewahrungstags definieren:
  - Archiv
  - Clutter
  - Entwürfe
  - Gelöschte Elemente
  - Gesendete Elemente
  - Journal
  - Junk-E-Mail
  - Kalender
  - Notizen
  - Posteingang
  - RSS-Feeds
  - Verlauf der Unterhaltung
- **Persönliches Tag**
  Ein persönliches Tag steht Anwendern zur individuellen Zuordnung an Postfachobjekte zur Verfügung. Solch ein Tag kann sowohl eigenen Postfachordnern als auch Objekten zugeordnet werden.

Es empfiehlt sich, unterschiedliche Aufbewahrungsrichtlinien für unterschiedliche Anwendergruppen zu definieren und diese Richtlinien automatisiert zuzuordnen (siehe Abbildung 9.4). Weisen Sie die Aufbewahrungsrichtlinien schon bei der Erstellung des Postfachs zu und nicht erst bei der Aktivierung des persönlichen Online Archiv-Postfachs.

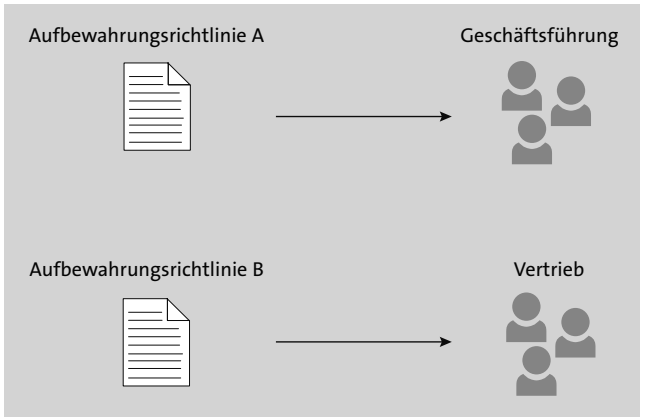

Abbildung 9.4 Zuordnung unterschiedlicher Aufbewahrungsrichtlinien

Eine zugeordnete Aufbewahrungsrichtlinie wirkt sich mit all ihren konfigurierten Tags auf das Postfach, auf Standardordner und auf individuelle Ordner aus. Der Anwender kann persönliche Tags sowohl in *Outlook für Desktop* als auch in *Outlook on the Web* den Ordnern und individuellen Objekten im Postfach zuordnen (siehe Abbildung 9.5).

Bei der Zuordnung persönlicher Tags werden die Tag-Informationen im Element gespeichert. Eine nachträgliche Änderung der Tag-Konfiguration wirkt sich nicht auf bereits durchgeführte Zuordnungen aus. Daher sollten Sie von zu häufigen Änderungen der Tag-Konfigurationen absehen. Investieren Sie lieber Zeit in eine gute Planung der Anforderungen an die Aufbewahrung von Postfachinhalten.

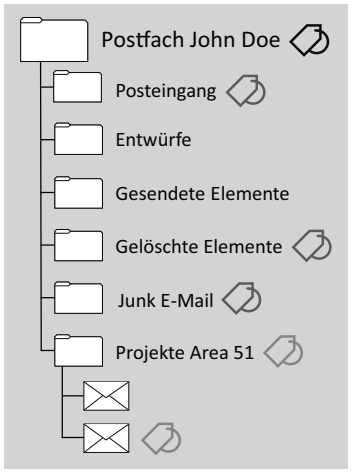

Abbildung 9.5 Beispiel für Aufbewahrungstags im Postfach

Bedenken Sie, dass durch die Installation von Exchange Server bereits eine Richtlinie (*Default MRM Policy*) existiert, die vielleicht nicht den Anforderungen Ihres Unternehmens entspricht. Überprüfen Sie die Standardrichtlinie im Exchange Admin Center. Wenn Sie mehr als eine Aufbewahrungsrichtlinie konfiguriert haben, ist eine dieser Richtlinien als Standardrichtlinie gekennzeichnet. Diese Standardrichtlinien werden einem Postfach mit aktiviertem Online Archiv-Postfach immer dann zugeordnet, wenn keine andere Aufbewahrungsrichtlinie explizit zugeordnet wird.

Es ist eventuell einfacher, größere Postfächer bereitzustellen, anstatt Anwender mit zwei Arten von Postfächern zu verwirren, die in ihrem Zugriffsverhalten unterschiedlich sind. Daher lautet meine Empfehlung, Anwendern lieber große Postfächer mit mindestens 50 GB zur Verfügung zu stellen. Outlook für Desktop kümmert sich mit der entsprechenden Konfiguration (siehe Abbildung 9.6) darum, dass nur ein Teil des Postfachinhalts auf den lokalen Client synchronisiert wird. Diese Einstellung sollten Sie auf jeden Fall mithilfe einer Gruppenrichtlinie einheitlich konfigurieren (*https://docs.microsoft.com/exchange/outlook/cached-exchange-mode*).

Das Online Archiv-Postfach bietet den Hauptvorteil, dass alle relevanten E-Mail-Daten in einem geschlossenen System gespeichert sind und nicht in Drittsystemen oder womöglich lokalen *PST*-Dateien, die weitere Abhängigkeiten mit sich bringen. Bedenken Sie auch, dass die Bereitstellung eines Online Archiv-Postfachs eine Enterprise-Funktion von Exchange Server 2019 ist und somit für jeden Anwender mit einem aktivierten Online Archiv-Postfach ein *Exchange Enterprise-CAL Add-On* (*https://products.office.com/exchange/microsoft-exchange-server-licensing-licensing-overview*) erfordert.

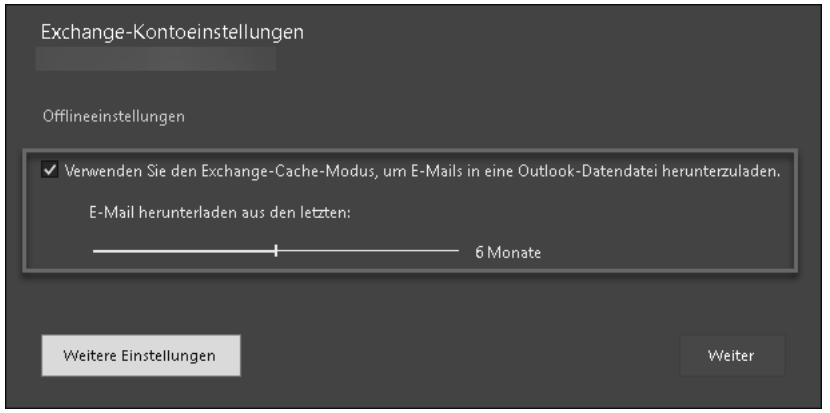

Abbildung 9.6 Outlook-Einstellung zur Bereitstellung von E-Mail-Nachrichten im Offlinemodus

9.2.2 Alternative Archivierungslösungen

Wie verhält es sich mit Archivierungslösungen von Drittanbietern? Lösungen von Drittanbietern verfolgen ein ähnliches Ziel wie Exchange Server selbst: die Verkleinerung der primären Postfächer von Anwendern. Bei dieser Art der Archivierung können wir zwei technische Varianten unterscheiden:

- clientbasierte Archivierung
- serverbasierte Archivierung

Bei der clientbasierten Variante (siehe Abbildung 9.7) müssen Sie eine Softwarekomponente auf jedem Client installieren. Im Idealfall kann eine solche Variante mithilfe von Gruppenrichtlinienobjekten zentral konfiguriert werden. Sobald Outlook für Desktop gestartet ist und eine Verbindung zum Unternehmensnetzwerk besteht, werden Daten aus dem persönlichen Postfach des Anwenders in die Offline-Cache-Datei (*OST*-Datei) heruntergeladen. Dann erfolgt eine regelbasierte Übertragung von E-Mail-Nachrichten aus der lokalen *OST*-Datei auf dem Client zu den Systemen der Archivierungslösung. In den meisten Fällen werden die archivierten Nachrichten in der *OST*-Datei durch Platzhalter (sogenannte *Stubs*) ersetzt. Es ist die Aufgabe von

Outlook, diese Änderungen durch die Cachemodus-Synchronisierung zum Exchange Server zu übertragen.

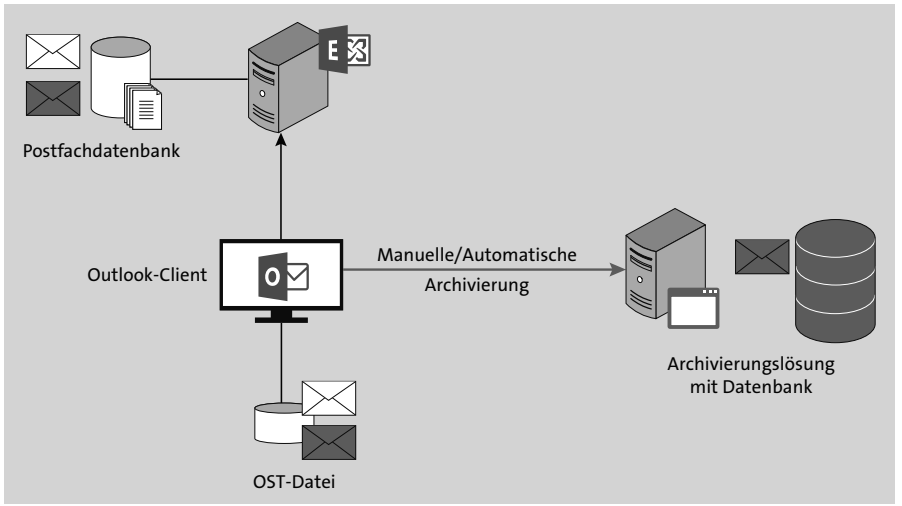

Abbildung 9.7 Clientbasierte Archivierung

Bei einer serverbasierten Variante (siehe Abbildung 9.8) erfolgt der Zugriff auf die zu archivierenden Anwender-Postfächer mithilfe der *Exchange Web Services*. Die Archivierungslösung arbeitet hierbei mit einem speziellen Dienstkonto, das über die notwendigen Berechtigungen verfügt. Hierbei erfolgt die Konfiguration der Archivierungsrichtlinien zentral auf dem Server der Archivierungslösung. Wie bei der clientbasierten Variante werden zentral archivierte E-Mail-Nachrichten oft durch Platzhalter ersetzt.

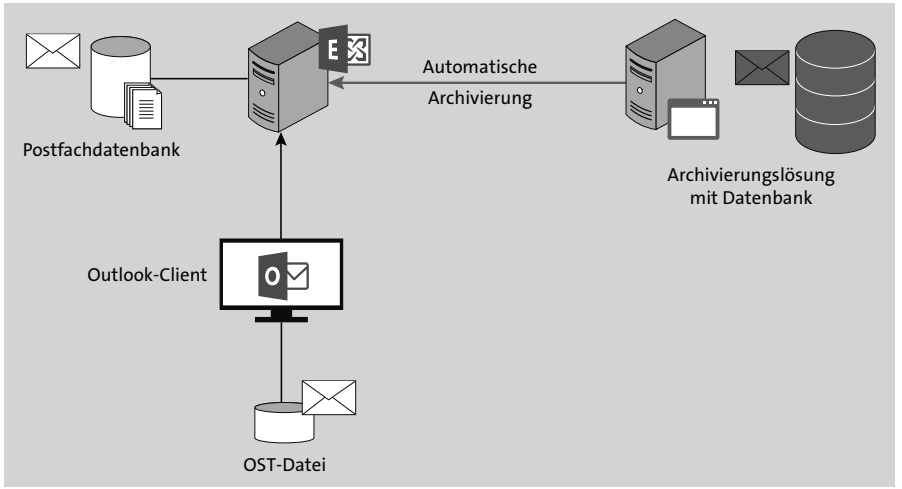

Abbildung 9.8 Serverbasierte Archivierung

E-Mail Platzhalter – gut oder böse?

Das Ersetzen von E-Mail-Nachrichten durch E-Mail-Platzhalter hat, historisch betrachtet, seinen Ursprung in den Zeiten, als Festplattenspeicher teuer und Cluster-Konfigurationen von Exchange Server komplex und kostspielig waren. Leider verfolgen auch heute die Anbieter von Archivierungslösungen den alten Ansatz, Nachrichten durch Platzhalter zu ersetzen.

Zum einen führt das Ersetzen von Nachrichten durch Platzhalter immer zu einem Medienbruch für den Anwender. Das Suchen im Archiv erfolgt immer über die Suchfunktionen der Drittanbieterlösung, während das Suchen im primären Postfach durch die Standardsuche in Outlook für Desktop erfolgt.

Zum anderen führt die Nutzung einer Archivierungslösung mit Platzhalter-Funktion zu einer Abhängigkeit von einem Softwareanbieter. Diese Abhängigkeit wird sich bei einem Wechsel der Lösung, der aus welchem Grund auch immer erfolgt, rächen. Denn die meisten Archivierungslösungen sind nicht darauf ausgerichtet, Daten zu exportieren und in andere Systeme zu übertragen.

Mit Exchange Server 2010 wurde die Portabilität von Postfachdatenbanken eingeführt. Im Falle eines absoluten Desasters benötigen Sie für die Wiederherstellung Ihrer Exchange Server-Umgebung und den Zugriff auf Ihre Postfachdaten genau zwei Komponenten:

- ein funktionierendes Active Directory
- genau eine Kopie jeder konfigurierten Postfachdatenbank

Damit sind Sie in der Lage, Ihre gesamte Exchange Server-Plattform wiederaufzubauen. Sind jedoch E-Mail-Nachrichten durch Platzhalter ersetzt worden, muss auch die gesamte Archivierungslösung wiederhergestellt werden.

Ja, Platzhalter sind böse.

Wenn Sie eine Archivierungslösung einsetzen, sollte die Lösung die Nachrichten kopieren und nicht durch Platzhalter ersetzen. Dies gilt nicht nur für die Postfächer von Anwendern, sondern ebenso für Funktionspostfächer und Öffentliche Ordner in Öffentliche-Ordner-Postfächern.

Eine clientbasierte Archivierung erfordert oftmals die Installation von Outlook-Add-Ins, um den Inhalt von archivierten Nachrichten anzuzeigen, sobald ein Platzhalter ausgewählt wurde. Bietet die Archivierungslösung kein Outlook-Add-In, wird meistens eine Weboberfläche für den Zugriff verwendet, was für den Anwender, wie schon erwähnt, automatisch einen Medienbruch beim E-Mail-Zugriff bedeutet.

Durch das Verschieben der E-Mail-Inhalte in andere Systeme entsteht automatisch die Anforderung, diese Archivierungssysteme redundant zu planen und entsprechend zu sichern. Dadurch erhöht sich die Komplexität Ihrer IT-Infrastruktur, was zusätzliche Prozesse bei der Wartung der zugehörigen Betriebssysteme und Softwarekomponenten erfordert.

PST-Dateien als lokaler Zwischenspeicher

Es gibt Lösungen auf dem Markt, die sowohl eine leistungsstarke Archivierung von E-Mail-Nachrichten und damit eine Reduzierung der Postfachgrößen auf Exchange Servern versprechen als auch eine professionelle Lösung zur Offline-Verfügbarkeit archivierter Nachrichten.

Die Offline-Bereitstellung von archivierten Nachrichten erfolgt hier mithilfe einer lokalen *PST*-Datei. Der Einsatz von *PST*-Dateien ist jedoch keine professionelle Lösung: Die Nutzung von *PST*-Dateien führt zu Leistungseinbußen bei der Nutzung von Outlook für Desktop und sorgt für ein großes Betriebsrisiko hinsichtlich korrupter *PST*-Datendateien im täglichen Betrieb. Anwender kennen den Unterschied zwischen einem Online-Postfach, einer *OST*- oder einer *PST*-Datei nicht und passen daher ihr Arbeitsverhalten mit Outlook für Desktop nicht an.

Von Lösungen, die lokale *PST*-Dateien als Speicher nutzen, kann ich aus persönlicher Erfahrung nur abraten.

Nicht alle Archivlösungen bieten eine Integration mit Outlook on the Web, um Anwendern einen einheitlichen Webzugriff auf das Postfach und das Archiv zu ermöglichen. Ähnlich sieht es bei der Integration von Clients auf mobilen Betriebssystemen wie iOS oder Android aus. Bei der Auswahl einer Archivierungslösung sollten Sie daher nicht nur die technische Seite, sondern immer auch die Anwenderseite betrachten.

9.3 Compliance

Exchange Server stellt für die Umsetzung und Einhaltung von Compliance-Anforderungen mehrere Möglichkeiten zur Verfügung. Die Funktionen der Compliance dienen zur Aufbewahrung von Postfachinhalten, zum Verhindern von unberechtigtem Abfluss von Daten und zur Suche im Rahmen einer eDiscovery Search.

Ob die Bordmittel von Exchange Server in der entsprechenden Konfiguration für Ihr Unternehmen ausreichend sind, um als rechtssichere Archivierung zu gelten, vermag ich nicht zu beurteilen. Diese Bewertung müssen Sie durch die Rechtsabteilung oder eine externe Rechtsberatung prüfen und bestätigen lassen. An dieser Stelle möchte ich auf den öffentlichen Bericht *Compliancemanagement und E-Mail-Archivierung mit Exchange Server 2013 – Eine Analyse der wichtigsten Funktionen nach deutschem Handels- und Steuerrecht* von KPMG hinweisen, den Sie unter *http://www.kpmg.de/bescheinigungen/requestreport.aspx?35886* finden. Einen Bericht zu einer aktuelleren Version von Exchange Server konnte ich nicht recherchieren.

9.3.1 In-Situ-eDiscovery

Unter dem Begriff *eDiscovery* versteht man die Möglichkeit zur einheitlichen Suche in Postfach-Inhalten und anderen Quellen aufgrund einer rechtlichen Anforderung zur Offenlegung von Informationen. In den meisten Fällen erfolgt solch eine Suchanfrage im Rahmen eines Rechtsverfahrens. Um die Anforderungen einer eDiscovery-Suche zu unterstützen, müssen die Inhalte von Postfächern natürlich aufbewahrt werden. Exchange Server 2019 unterstützt zwei unterschiedliche Varianten zur Aufbewahrung von Postfachinhalten.

1. **Beweissicherungsverfahren für ein Postfach**
   Diese Methode der Aufbewahrung wird auch als *Litigation Hold* bezeichnet. Sie wird auf das gesamte Postfach angewendet, für das das Beweissicherungsverfahren aktiviert wurde (*https://docs.microsoft.com/Exchange/policy-and-compliance/holds/litigation-holds*). Die Aktivierung und die Konfiguration erfolgen immer in den Postfach-Einstellungen des jeweiligen Postfachs. Exchange Server erlaubt die Aufbewahrung ohne zeitliche Begrenzung.

```
# Aktivierung von Litigation Hold für ein Postfach ohne Zeitbegrenzung
Set-Mailbox -Identity JohnDoe -LitigationHoldEnabled $true

# Aktivierung von Litigation Hold für ein Postfach, Laufzeit 2 Jahre
Set-Mailbox -Identity JohnDoe -LitigationHoldEnabled $true `
  -LitigationHoldDuration 730
```

Alternativ können Sie das Beweissicherungsverfahren auch in den Postfacheinstellungen im Exchange Admin Center aktivieren (siehe Abbildung 9.9).

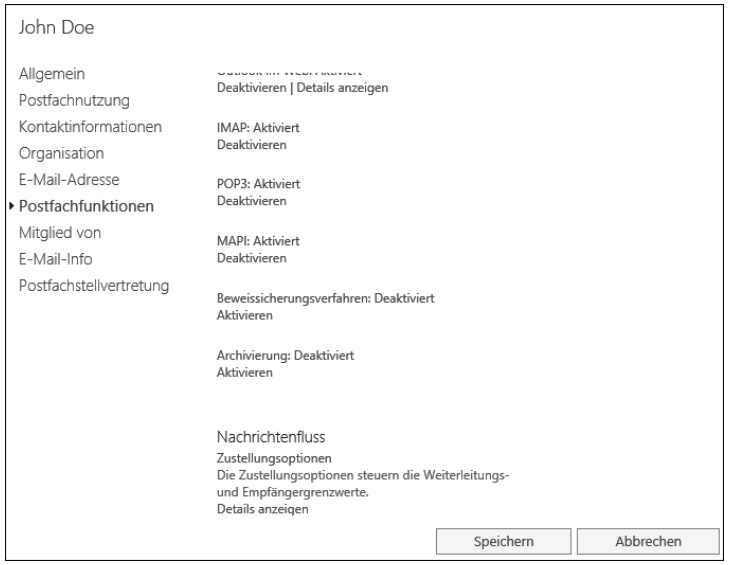

Abbildung 9.9 Aktivierung des Beweissicherungsverfahrens im Exchange Admin Center

2. **In-Situ-Speicher**
   Diese Methode der Aufbewahrung wird auch als *In-Place Hold* bezeichnet. Die Speicherung von Postfachinhalten bezeichnet Microsoft in diesem Kontext als *In-Situ-Speicher* (*https://docs.microsoft.com/Exchange/policy-and-compliance/ediscovery/ediscovery*). Hier können Sie unterschiedliche Aufbewahrungsregeln definieren und diese auf alle oder nur auf ausgewählte Postfächer anwenden. Diese Methode unterstützt auch die Aufbewahrung von Inhalten, die in Öffentlichen Ordnern gespeichert sind. Die Konfiguration erfolgt nicht direkt auf dem Postfach, sondern in den Compliance-Einstellungen des Exchange Admin Centers oder per Exchange Management Shell. Die Konfiguration granularer Aufbewahrungsregeln erfordert die Mitgliedschaft in der RBAC-Rolle *Discovery Management*.

Unabhängig davon, ob Sie das Beweissicherungsverfahren für ein Postfach aktiviert oder eine regelbasierte Aufbewahrung konfiguriert haben, erfolgt die Speicherung von Inhalten immer im betroffenen Postfach. Ist für ein Postfach auch die Funktion eines persönlichen Online Archiv-Postfachs aktiviert, so wirkt sich die Aufbewahrung auch auf das Online Archiv-Postfach aus.

Ein Postfach, für das eine Form der Aufbewahrung aktiviert ist, erlaubt dem Anwender weiterhin, wie gewohnt mit dem Postfach zu arbeiten: Nachrichten können verschoben, bearbeitet und auch gelöscht werden. Jedoch werden veränderte und gelöschte Nachrichten in Systemordnern des Postfachs gespeichert. Diese Ordner sind für den Anwender nicht sichtbar. Die aufbewahrten Elemente werden entweder nach Ablauf der Aufbewahrungsfrist automatisch gelöscht oder aber für immer aufbewahrt.

Aber wie funktioniert die Aufbewahrungsfunktion für ein Postfach genau?

Verfolgen wir eine Nachricht im Postfach eines Anwenders einmal Schritt für Schritt aus Sicht von Exchange Server (siehe Abbildung 9.10 und *https://docs.microsoft.com/exchange/policy-and-compliance/recoverable-items-folder/recoverable-items-folder*):

❶ Die Nachricht wird in das Postfach zugestellt.

❷ Die Nachricht wird in den Ordner *Gelöschte Elemente* verschoben.

❸ Die Nachricht wird gelöscht.

Exchange Server sieht erst das Leeren des Ordners *Gelöschte Elemente* oder eine Löschung mit ⇧+Entf als Löschung an. In beiden Fällen sprechen wir von einem *Soft Delete*.

❹ Nach dem Ablauf der Vorhaltezeit für *Gelöschte Elemente* und bei aktiviertem *Litigation Hold* oder *Single Item Recovery* werden die betroffenen Elemente in den Ordner *Purges* verschoben.

❺ Nach Ablauf der Vorhaltezeit für *Gelöschte Elemente* und bei aktiviertem *In-Place Hold* werden die betroffenen Elemente in den Ordner *DiscoveryHold* verschoben.

❻ Wenn für ein Postfach *In-Place Hold* oder *Litigation Hold* aktiviert ist, werden bei einer Bearbeitung der Nachricht sowohl die Originalnachricht als auch die veränderte Nachricht in den Ordner *Versions* kopiert.

❼ Abgelaufene Elemente werden durch den *Managed Folder Assistenten* (MFA) entweder final gelöscht oder verbleiben im Ordner, sollte *Litigation Hold* aktiv sein.

❽ Sind *Single Item Recovery* und *In-Place-Hold* aktiv, werden die abgelaufenen Nachrichten in den Ordner *DiscoveryHold* verschoben.

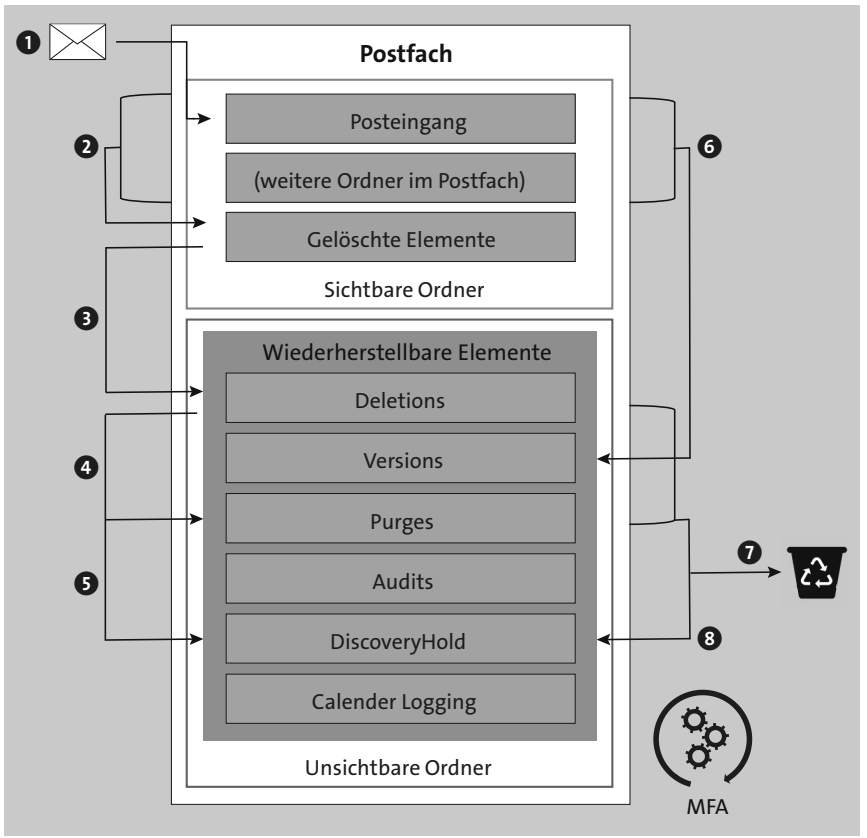

Abbildung 9.10 Arbeitsweise der Aufbewahrungsfunktion in Exchange Server

Der *Managed Folder Assistant* ist ein automatischer Prozess, der zeitgesteuert alle Postfächer untersucht und sie auf Basis der Einstellungen für *Litigation Hold* oder *In-Place Hold* aufräumt.

Mit einer eDiscovery-Suche haben Sie die Möglichkeit, eine Suchabfrage zu erstellen, die alle Postfachinhalte durchsucht. Hierbei werden sowohl die für Anwender sichtbaren Inhalte durchsucht als auch die für den Anwender unsichtbar aufbewahrten Nachrichten. Nach der Konfiguration und dem Start der Suchanfrage wird die Suche

im Hintergrund ausgeführt. Je nach Umfang der Suche kann diese einige Zeit in Anspruch nehmen. Das Suchergebnis wird anschließend an ein Zielpostfach zugestellt. Als Standard-Zielpostfach hat das Exchange Server-Installationsprogramm das Postfach *Discovery Search Mailbox* erstellt.

Die Zustellung der Suchergebnisse an ein explizit definiertes Postfach soll sicherstellen, dass nur berechtigte Personen Zugriff auf die Suchergebnisse haben. Naturgemäß enthalten die Suchergebnisse sensible Daten, auf die Sie, in Ihrer Rolle als Exchange-Administrator, keinen Zugriff haben dürfen.

Persönliche Nachrichten in Suchergebnissen

Anwender-Postfächer enthalten immer auch persönliche Nachrichten, auf die nicht jede Person im Rahmen der Suchergebnisse Zugriff haben darf. Zu diesen Informationen gehören z. B. die Kommunikation mit der Personalabteilung oder empfangene private E-Mail-Nachrichten. Aber auch persönliche und private Kalendereinträge sind davon betroffen.

Jeder Zugriff auf solche persönlichen Informationen stellt eine Verletzung des Postgeheimnisses dar. Daher ist es wichtig, dass der Personenkreis, der Zugriff auf das Postfach zur Bereitstellung der Suchergebnisse hat, klar definiert ist . Das Gleiche gilt übrigens auch für den direkten Zugriff auf ein Postfach durch Gewährung einer Vollzugriffsberechtigung: Solch ein Zugriff kann nur im Beisein des Datenschutzbeauftragten und eines Mitglieds des Betriebsrats erfolgen.

Unter Umständen werden Sie weniger Suchergebnisse erhalten, als Sie erwartet haben. Eine Nachricht oder ein Dateianhang sind nicht Bestandteil des Suchergebnisses, wenn einer oder mehrere der folgenden Punkte zutreffen:

- Der Dateityp des Anhangs unterstützt keine Standardindizierung und es ist kein dedizierter *IFilter* für den Dateityp installiert.
- Der Dateityp ist für die Indizierung deaktiviert.
- Es ist ein Indizierungsfehler aufgetreten.
- Der Dateianhang ist mit einer Nicht-Microsoft-Technologie verschlüsselt.
- Der Dateianhang ist kennwortgeschützt.
- Die Nachricht ist mit einem persönlichen Zertifikat verschlüsselt.

Wenn Ihr Unternehmen rechtlich dazu verpflichtet ist, eine eDiscovery-Suche zu ermöglichen, müssen Sie sich Gedanken über das Thema Ende-zu-Ende-Verschlüsselung machen. Eine mögliche Lösung ist der Einsatz von Master-Zertifikaten für persönliche Verschlüsselungszertifikate, über die eine alternative Archivierungslösung in die Lage versetzt wird, Nachrichten unverschlüsselt zu speichern und so durchsuchbar zu machen.

Eine aktuelle Beschreibung zur Erstellung einer In-Situ-eDiscovery-Suche finden Sie in der Online-Dokumentation von Exchange Server: *https://docs.microsoft.com/Exchange/policy-and-compliance/ediscovery/create-searches*

9.3.2 Journaling

Exchange Server bietet die Möglichkeit, sogenannte Journalberichte an ein definiertes Ziel-Postfach zu senden. Die Journaling-Funktion ist nicht neu, sondern steht in abgewandelten Formen seit Exchange Server 5.5 zur Verfügung (*https://docs.microsoft.com/exchange/policy-and-compliance/journaling/journaling*). Die in Exchange Server 2019 verwendeten Journaling-Funktionalitäten sind seit Exchange Server 2010 weitgehend unverändert. Beim Journaling wird durch Exchange Server eine Journalbericht-E-Mail erstellt, die immer die Originalnachricht im Dateianhang und weitere Informationen über die Originalnachricht im Fließtext der Nachricht enthält.

Diese Form der Archivierung ermöglicht eine Form der rechtssicheren Archivierung der E-Mail-Kommunikation, indem die Journalberichte durch eine Drittanbieterlösung aus dem Journal-Postfach ausgelesen und in eine proprietäre Datenbankstruktur überführt werden. Das Ziel dieser Form der Archivierung ist nicht der regelmäßige Recherche-Zugriff durch Clients, sondern der unregelmäßige Zugriff im Rahmen einer eDiscovery-Suche.

Das Zielpostfach für einen Journalbericht ist ein sogenanntes *Journal-Postfach*. Hierbei handelt es sich nicht um einen bestimmten Postfachtyp, sondern um ein normales Benutzerpostfach. Dass es sich um ein Journal-Postfach handelt, geht vielmehr aus dem Namen und der E-Mail-Adresse des Postfachs hervor. Damit unterliegt das Journal-Postfach auch den normalen Regeln hinsichtlich der Größenbeschränkungen von Postfächern. Wenn Sie keine Archivierungslösung eines Drittanbieters verwenden, sondern nur auf das interne Journaling von Exchange Server 2019 setzen, müssen Sie für die Journal-Postfächer explizite Aufbewahrungsrichtlinien definieren. Ohne solche Richtlinien laufen die Postfachgrößen dieser Postfächer aus dem Ruder. Im Zweifel müssen Sie in regelmäßigen Zeitabständen neue Journal-Postfächer erstellen.

Beim Standard-Journaling erfolgt die Konfiguration direkt über die Einstellungen einer Postfachdatenbank. Wenn Sie das Journaling für alle Postfächer aktivieren möchten, müssen Sie für alle Postfachdatenbanken einen Journaling-Empfänger konfigurieren. Das folgende Beispiel konfiguriert das Journaling für eine Postfachdatenbank:

```
# Aktivierung des Journalings für eine Postfachdatenbank
Set-MailboxDatabase -Identity DEMBXDB01 -JournalRecipient `
  journal01@varunagroup.de
```


Eine granulare Konfiguration des Journalings ist nur mithilfe von Premium-Journalregeln möglich. Diese Funktion erfordert Enterprise-CALs für alle Benutzer, die von dieser Form des Journalings betroffen sind. Die Verwaltung der Premium-Journalregeln erfolgt im Exchange Admin Center im Bereich Verwaltung der Compliance (siehe Abbildung 9.11). Definieren Sie zuerst ein Zielpostfach, an das Journalberichte gesendet werden, falls das eigentliche Journaling-Zielpostfach nicht erreichbar oder voll ist. Sowohl das Journaling-Postfach selbst als auch das Postfach für nicht zustellbare Journalberichte unterliegen *nicht* dem Journaling und anderen Transportregeln. Nutzen Sie auch für unzustellbare Journalberichte ein dediziertes Postfach, das keine weiteren Funktionen wahrnimmt. So stellen Sie sicher, dass keine Journalberichte verloren gehen.

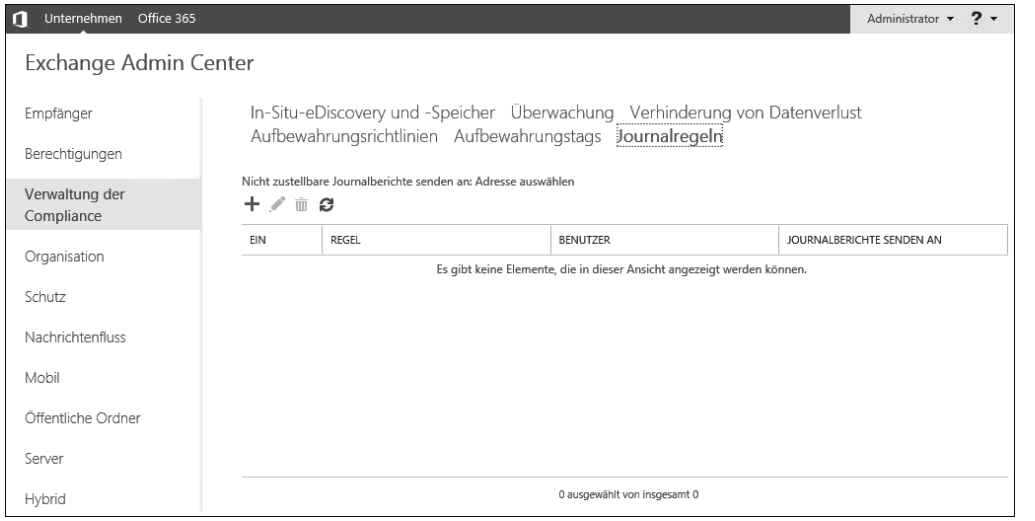

Abbildung 9.11 Konfiguration von Premium-Journalregeln im Exchange Admin Center

Bei der Konfiguration einer Journalregel können Sie auswählen, ob die Regel nur für einen Empfänger, eine Gruppe von Empfängern oder für alle Nachrichten gelten soll. Als zweites Auswahlkriterium müssen Sie auswählen, ob das Journaling nur für Nachrichten an externe Empfänger, nur für Nachrichten an interne Empfänger oder für alle Nachrichten aktiviert werden soll.

Journaling in Exchange Online

Ein Journaling von E-Mail-Nachrichten ist auch mit Exchange Online möglich. Da Sie dort aber keine datenbankspezifischen Konfigurationen vornehmen können, stehen Ihnen nur die Journalregeln zur Verfügung. Das Journal-Postfach darf allerdings kein Exchange Online-Postfach sein, es muss immer in der On-Premises-Exchange-Organisation beheimatet sein.

Wenn Sie Journalregeln in Exchange Online konfigurieren, werden die Journalberichte zur E-Mail-Kommunikation der Exchange Online-Postfächer an ein Journal-Postfach auf Ihrer lokalen Exchange Server-Plattform gesendet. Wenn Sie auf Ihrer Exchange Server-Plattform mit Hybrid-Stellung noch lokale Benutzerpostfächer bereitstellen, müssen Sie für diese Postfächer eine separate Journalregel erstellen. Ob Sie für beide Benutzergruppen das gleiche Journal-Postfach nutzen oder ob Sie unterschiedliche Postfächer für die Journalberichte von der On-Premises-Plattform und Exchange Online nutzen, hängt von der Planung ab.

Die Nutzung der Exchange-Journalfunktionen erfordert eine genaue Planung und eine aktive Überwachung der Postfächer, um Probleme bei der Zustellung der Journalberichte zu vermeiden.

9.3.3 Datenverlust verhindern

Das Thema »Verhinderung von Datenverlust«, die sogenannte *Data Leakage Prevention* (DLP) (*https://docs.microsoft.com/exchange/policy-and-compliance/data-loss-prevention/data-loss-prevention*), wird in Unternehmen häufig diskutiert, aber nur selten technisch umgesetzt. Als Gründe, warum man DLP nicht einsetzt, wird häufig darauf verwiesen, dass die technische Implementierung zu komplex sei oder dass man die Anwender in ihrer Kommunikation nicht einschränken möchte. Das zu erwartende Support-Aufkommen für den Helpdesk sei einfach zu hoch.

Sie werden mir sicherlich zustimmen, dass dies keine gültigen Gründe dafür sind, DLP nicht einzuführen.

Die DLP-Richtlinien von Exchange Server basieren auf speziellen E-Mail-Transportregeln, in denen Bedingungen zur Erkennung von schützenswerten Daten, entsprechende Aktionen und eventuell benötigte Ausnahmen definiert sind. Als integraler Bestandteil der Transport-Pipeline haben die Transportregeln vollen Zugriff auf E-Mails und deren Dateianhänge. Nur so kann eine detaillierte Inhaltsanalyse realisiert werden.

Enterprise-Feature DLP

DLP ist ein Enterprise-Feature und erfordert daher eine Exchange-Enterprise-Client-Access-Lizenz. Die Nutzung der DLP-Funktionen ohne das Enterprise-CAL-Add-On stellt einen Lizenzverstoß dar.

DLP-Richtlinien erlauben auch eine Benachrichtigung des Anwenders in Outlook oder Outlook on the Web. Hierzu stehen Ihnen die Richtlinientipps zur Verfügung. Je nach konfigurierter Aktion der DLP-Richtlinie wird ein anderer Text im Client angezeigt. Sollten die Standardtexte nicht Ihren Vorstellungen entsprechen, können Sie sie auch anpassen. Die folgenden vier Textinformationen können angepasst werden:

- **Absender benachrichtigen** – Dieser Text wird angezeigt, wenn der Anwender nur darüber informiert werden soll, dass eine DLP-Richtlinie Compliance-relevanten Inhalt gefunden hat, die Nachricht aber trotzdem gesendet werden kann.
- **Außerkraftsetzen durch den Absender erlauben** – Dieser Text wird im Client angezeigt, wenn ein Anwender über einen möglichen Compliance-Verstoß informiert werden soll, aber die Möglichkeit hat, die Blockierung außer Kraft zu setzen. Das Außerkraftsetzen wird im DLP-Bericht der Richtlinie festgehalten.
- **Nachricht blockieren** – Dies ist der Text, der einem Anwender im Client angezeigt wird, wenn der Versand einer Nachricht aktiv blockiert wird.
- **URL-Link zur Richtlinientreue** – Bei dieser Einstellung geben Sie einen Link zu einer Webseite an, die über die Unternehmens-Compliance aufklärt und weitere Informationen enthält. Wenn diese URL konfiguriert ist, erscheint im Richtlinientipp ein entsprechender Link, den der Anwender anklicken kann.

Bevor Sie eine DLP-Richtlinie aktivieren, sollten Sie die konfigurierte Richtlinie zuerst im Testmodus nutzen. Im Testmodus wird die Richtlinie noch nicht aktiv durchgesetzt, Sie als Administrator erhalten aber Rückmeldungen, welche Nachrichten erkannt wurden. Alle Informationen hierzu werden im DLP-Bericht zur Richtlinie festgehalten (*https://docs.microsoft.com/exchange/create-incident-reports-for-dlp-policy-detections-exchange-2013-help*). Auf diese Weise können Sie überprüfen, ob die jeweilige Richtlinie korrekt konfiguriert ist.

DLP und Ende-zu-Ende-Verschlüsselung

In manchen Unternehmen ist das Thema E-Mail-Verschlüsselung aktuell hoch im Kurs. Im Zusammenhang mit DLP ergeben sich aber Probleme. Bei Nutzung von S/MIME-Verschlüsselung auf Basis von Soft-Zertifikaten oder Smartcards stehen die DLP-Funktionen von Exchange Server nicht zur Verfügung. Exchange Server hat keine Möglichkeit, den Inhalt zu analysieren und DLP-Richtlinien anzuwenden.

Das sieht anders aus, wenn Sie eine S/MIME-Verschlüsselung ausgehender E-Mail-Nachrichten an einem SMTP-Gateway vornehmen. In diesem Fall können DLP-Richtlinien angewendet werden und die Nachrichten sind für eine eDiscovery-Suche durchsuchbar.

Die Konfiguration der DLP-Richtlinien erfolgt im Exchange Admin Center (EAC) im Abschnitt Verwaltung der Compliance (siehe Abbildung 9.12). In Exchange Server 2019 bietet die DLP-Verwaltung im EAC eine Möglichkeit, um Dokumenten-Fingerprints hochzuladen.

Abbildung 9.12 Konfiguration von DLP im Exchange Admin Center

Exchange Server 2019 unterstützt drei unterschiedliche Methoden zur Einrichtung von DLP-Richtlinien:

- **Nutzung einer mitgelieferten Exchange Server-DLP-Vorlage** – Hierbei greifen Sie bei der Erstellung der DLP-Richtlinie auf die internen Exchange Server-Vorlagen zurück. Für Deutschland werden genau zwei Vorlagen mitgeliefert, um Finanzdaten (*Germany Financial Data*) oder persönliche Informationen (*Germany Personally Identifiable Information (PII) Data*) zu identifizieren.

  Ob diese Vorlagen für Ihre Bedürfnisse ausreichen, müssen Sie selbst entscheiden. Eine vollständige Auflistung der Vorlagen für DLP-Richtlinien finden Sie in der Dokumentation unter *https://docs.microsoft.com/exchange/security-and-compliance/data-loss-prevention/dlp-policy-templates*.

- **Import einer individuellen DLP-Richtlinienvorlage** – Die Entwicklung einer DLP-Richtlinienvorlage ist keine triviale Aufgabe und würde den Rahmen dieses Buches sprengen. Wenn Sie Bedarf an einer individuellen Vorlage haben, empfehle ich Ihnen, diese in enger Zusammenarbeit mit einem Microsoft-Partner zu entwickeln.

  Eine DLP-Vorlage ist zwar grundsätzlich nichts anderes als eine XML-Datei, jedoch ist die Definition der Begriffssuche, der Trefferwahrscheinlichkeit und der Treffergenauigkeit nicht einfach. Microsoft bietet hierzu einen sehr ausführlichen Artikel, der auch das benötigte XML-Schema enthält: *https://docs.microsoft.com/office365/securitycompliance/eop/exchange-online-protection-overview*

- **Erstellung einer individuellen Richtlinie** – Bei dieser Möglichkeit erstellen Sie eine DLP-Richtlinie auf Basis der vorhandenen Aktionen direkt im EAC.

Der Import der XML-Datei einer DLP-Richtlinienvorlage kann sowohl im EAC als auch per PowerShell erfolgen. Die Speicherung erfolgt in der Konfigurationspartition des Active Directory unterhalb des *Transport Settings*-Containers:

```
# Import einer DLP-Richtlinienvorlage aus einem lokalen Verzeichnis
Import-DlpPolicyTemplate -FileData ([Byte[]]$(Get-Content `
  -Path "C:\Policies\Custom-DLP-Policy.xml" -Encoding Byte -ReadCount 0))
```

Sollte das Thema »Data Leakage Prevention mit Exchange Server 2019« in Ihrem Unternehmen noch keine Rolle spielen, so möchte ich Sie auffordern, dies zu ändern. Die DLP-Bordmittel von Exchange Server sind vielleicht nicht selbsterklärend, aber sie sind wirksam.

9.3.4 Das Admin-Audit-Protokoll

Exchange Server 2019 ermöglicht die Protokollierung aller PowerShell-basierten Konfigurationsänderungen in Ihrer Exchange-Organisation. Änderungen, die über das *Exchange Admin Center* (EAC) ausgeführt werden, werden ebenfalls protokolliert, da im Hintergrund PowerShell-Cmdlets ausgeführt werden. Mit den im Admin-Audit-Protokoll gespeicherten Informationen können Sie jede an einem Objekt durchgeführte Änderung nachvollziehen, um regulatorischen Anforderungen gerecht zu werden.

Das Admin-Audit-Protokoll (*https://docs.microsoft.com/exchange/policy-and-compliance/admin-audit-logging/admin-audit-logging*) ist keine Arbeitsüberwachung im negativen Sinne, sondern dient schlicht zur Protokollierung von Änderungen an Objekten in einer Exchange-Organisation. Wenn Ihr Unternehmen über einen Betriebsrat verfügt, sollten Sie die Existenz des Admin-Audit-Protokolls und die Hintergründe hierzu im IT-Ausschuss des Betriebsrats vorstellen. Idealerweise werden der Zugriff auf das Admin-Audit-Protokoll und der Umgang mit ihm in einer generellen IT-Betriebsvereinbarung geregelt.

Die Standardeinstellungen der Admin-Audit-Protokollierung sind:

- aktiviertes Audit-Protokoll
- Aufbewahrungszeitraum 90 Tage
- Protokollierung aller Cmdlets, die Änderungen an Objekten vornehmen können
- Die Protokollierung von Test-Cmdlets ist deaktiviert.
- Protokolleinstellung `None`, was bedeutet, dass das ausgeführte Cmdlet mit Detailinformationen (Wer hat welches Objekt verändert?) protokolliert wird. Mit der

alternativen Einstellung `Verbose` werden die Objektparameter vor und nach der Änderung ebenfalls festgehalten.

- Im Folgenden sehen Sie einen Auszug aus einer Standardkonfiguration:

```
AdminAuditLogEnabled         : True
LogLevel                     : None
TestCmdletLoggingEnabled     : False
AdminAuditLogCmdlets         : {*}
AdminAuditLogParameters      : {*}
AdminAuditLogExcludedCmdlets : {}
AdminAuditLogAgeLimit        : 90.00:00:00
```

Die Einstellungen für die Admin-Audit-Protokollierung können standardmäßig von Mitgliedern der RBAC-Gruppen *Organization Management* und *Records Management* geändert werden. Da die Audit-Protokollierung eine wichtige Rolle für die Compliance eines Unternehmens spielt, sollten Sie darauf achten, dass nur wenige Mitarbeiter die Berechtigung zur Konfigurationsänderung besitzen. Hier hilft Ihnen das PowerShell-Skript *Get-RBACGroupMemberReport.ps1* von Paul Cunningham weiter, das Sie hier finden: *https://practical365.com/powershell-script-to-report-rbac-role-group-membership/*

Die Speicherung des Admin-Audit-Protokolls erfolgt nicht im Dateisystem der Exchange Server, sondern im Systempostfach *SystemMailbox{e0dc1c29-89b3-4034-c678-e6c29d823ed9}*. In einer Multi-Domänen-Umgebung ist dieses Postfach (neben anderen allgemeinen Systempostfächern) in der Root-Domäne der Active Directory-Gesamtstruktur beheimatet.

Zugriff auf Systempostfächer in der Root-Domäne

Die Root-Domäne einer Active Directory-Gesamtstruktur ist aus Sicht der Exchange-Organisation ein integraler Bestandteil der Exchange Server-Konfiguration, ganz unabhängig davon, ob in der Root-Domäne Exchange Server installiert sind. Im Rahmen der Vorbereitung des Active Directory werden dort wichtige Exchange Server-Systemobjekte, wie die organisationsweiten Systempostfächer, erstellt und die erforderlichen Berechtigungen vergeben. Zum einen benötigt die Sicherheitsgruppe *Exchange Trusted Subsystem* die konfigurierten Berechtigungen in der Root-Domäne; zum anderen muss sichergestellt werden, dass die Exchange Server die Domänencontroller der Root-Domäne auch erreichen können.

Wenn die Admin-Audit-Protokollierung aktiviert ist und ein Exchange Server die Protokollinformationen nicht im Systempostfach speichern kann, finden Sie im Ereignisprotokoll des Exchange Servers Einträge für die Event-ID 5000 `Failed to save admin audit log for this cmdlet invocation`. In den Detailinformationen finden Sie den

Grund für den Fehler. Neben der Nichterreichbarkeit ist es auch möglich, dass das Systempostfach das Quota erreicht hat.

```
# Anpassung der Quota-Einstellungen für das Systempostfach, in dem
# das Admin-Audit-Protokoll gespeichert ist
Set-ADServerSettings -ViewEntireForest:$true
Set-Mailbox -Arbitration -Identity 'SystemMailbox{e0dc1c29-89c3-4034-
  b678-e6c29d823ed9}' -RecoverableItemsQuota Unlimited `
  -RecoverableItemsWarningQuota Unlimited -CalendarLoggingQuota Unlimited
```

Sie haben zwei Möglichkeiten, das Admin-Audit-Protokoll zu durchsuchen. Mithilfe des Cmdlets `Search-AdminAuditLog` (*https://docs.microsoft.com/powershell/module/exchange/policy-and-compliance-audit/search-adminauditlog*) erhalten Sie Suchergebnisse zur Anzeige oder weiteren Verarbeitung per PowerShell unmittelbar (synchron) in Ihrer aktiven EMS-Session. Das Cmdlet `New-AdminAuditLogSearch` (*https://docs.microsoft.com/powershell/module/exchange/policy-and-compliance-audit/new-adminauditlogsearch*) hilft Ihnen, wenn Sie eine dokumentierte Suchanfrage ausführen und das Ergebnis Dritten zur Verfügung stellen müssen. Bei solch einer asynchronen Suche erstellt Exchange Server einen XML-Ergebnisbericht, der als E-Mail-Anhang an ein angegebenes Zielpostfach zugestellt wird. Die maximale Größe des Berichts beträgt 10 MB.

```
# Beispiel einer direkten Suche in einer PowerShell-Session, um Aktivitäten
# für das Cmdlet New-Mailbox der letzten 90 Tage zu finden

Search-AdminAuditLog -Cmdlets New-Mailbox

RunspaceId         : f259a844-5d84-4b75-a045-6d3f56b16439
ObjectModified     : varunagroup.de/Locations/BER/Shared/MBX-Marketing
CmdletName         : New-Mailbox
CmdletParameters   : {Name, Shared, DisplayName, Alias, OrganizationalUnit,
                     PrimarySmtpAddress}
ModifiedProperties : {}
Caller             : varunagroup.de/Admins/Users/adm_Luke
ExternalAccess     : False
Succeeded          : True
Error              :
RunDate            : 15.07.2022 15:09:55
OriginatingServer  : EX01 (15.00.1395.000)
```

In der Ausgabe können Sie sehen, dass unter der administrativen Anmeldung `adm_Luke` (`Caller`) das Cmdlet `New-Mailbox` (`CmdletName`) zur Erstellung des neuen freigege-

benen Postfachs `MBX-Marketing` ausgeführt wurde und im Rahmen der Neuerstellung die Cmdlet-Parameter `Name`, `Shared`, `DisplayName`, `Alias`, `OrganizationalUnit` und `PrimarySmtpAddress` verwendet wurden. Zusätzlich sehen Sie, dass das Cmdlet am `15. Juli 2022 um 15:09:55` auf dem Server `EX01` (`OriginatingServer`) erfolgreich (`Succeeded`) ausgeführt wurde.

Im Gegensatz dazu erstellen Sie mit dem Cmdlet `New-AdminAuditLogSearch` eine Suchanfrage an Exchange Server 2019, die im Hintergrund asynchron ausgeführt wird:

```
# Beispiel einer Admin-Audit-Protokoll-Suche, um alle Quota-Anpassungen
# für freigegebene Postfächer im Zeitraum 1.-15. Juli 2022 zu finden.
# Gesucht werden die Verwendungen von Set-Mailbox, bei denen auch die
# genannten Parameter verwendet wurden

New-AdminAuditLogSearch -Name "SharedMailbox Quota" -Cmdlets Set-Mailbox `
  -Parameters Shared, UseDatabaseQuotaDefaults, ProhibitSendReceiveQuota, `
  ProhibitSendQuota -StartDate 07/01/2018 -EndDate 07/15/2022 `
  -StatusMailRecipients adm_Luke@varunagroup.de
```

Die Ergebnisse werden nach Abschluss der Suche an den Administrator `adm_Luke` per E-Mail zugestellt.

Eine Anpassung der Einstellungen für die Admin-Audit-Log-Protokollierung ist mithilfe des Cmdlets `Set-AdminAuditLogConfig` möglich:

```
# Einschränkung der Admin-Audit-Protokollierung auf Cmdlets *Mailbox*
# und eine Aufbewahrung von 120 Tagen

Set-AdminAuditLogConfig -AdminAuditLogCmdlets *Mailbox* `
  -AdminAuditLogAgeLimit 120.00:00:00

# Deaktivierung der Admin-Audit-Protokollierung

Set-AdminAuditLogConfig -AdminAuditLogEnabled $false
```

Die Admin-Audit-Protokollierung ist somit ein Hilfsmittel, um Änderungen an Exchange-relevanten Objekten im Active Directory nachzuverfolgen. Der standardmäßige Aufbewahrungszeitraum von 90 Tagen wird in den meisten Exchange-Organisationen unverändert genutzt und ist sicherlich auch ausreichend. Wenn in Ihrem Unternehmen individuelle Anforderungen zur Admin-Audit-Protokollierung existieren, so können Sie die Einstellungen der Protokollierung anpassen. Zusätzlich sollte der Personenkreis, der Änderungen an den Einstellungen für die Admin-Audit-Protokollierung vornehmen kann, sehr klein gehalten werden.

9.3.5 Das Postfach-Audit-Protokoll

Neben der Protokollierung von PowerShell-Befehlen kann in Exchange Server der Zugriff auf Postfächer protokolliert werden. Mit dem Postfach-Audit-Protokoll können Sie die Zugriffe von Postfacheigentümern, Stellvertretern und Administratoren protokollieren.

Die Einstellungen für das Postfach-Audit-Protokoll werden pro Postfach konfiguriert. Hierdurch haben Sie die Möglichkeit, unterschiedliche Audit-Einstellungen pro Postfach bzw. pro Postfachgruppe vorzunehmen. Mögliche Postfachgruppen sind z. B.:

- Mitglieder der Geschäftsführung
- Vertriebsmitarbeiter
- Mitarbeiter der Personalabteilung
- geteilte Postfächer für Projekte und Abteilungen
- Ressourcen-Postfächer
- allgemeine Postfächer

Standardmäßig ist das Postfach-Audit-Protokoll in einer lokalen Exchange-Organisation für alle Postfächer ausgeschaltet. Sie müssen das Audit-Protokoll individuell für ausgewählte Postfächer aktivieren. Die protokollierten Informationen werden im jeweiligen Postfach abgelegt und im Regelfall für 90 Tage gespeichert. Das Postfach-Audit-Protokoll beachtet die Einstellungen für die dauerhafte Aufbewahrung von Postfachinformationen (*In-Place Hold* bzw. *Litigation Hold*) nicht. Wenn in Ihrer Exchange-Organisation eine längere Aufbewahrungsfrist notwendig ist, müssen Sie den Zeitraum mit dem Parameter `AuditLogAgeLimit` konfigurieren.

Das Postfach-Audit-Protokoll kann innerhalb eines Postfachs eine beträchtliche Größe erreichen. Wenn Sie das Audit-Protokoll aktivieren, müssen Sie auch die Größe des *Audits*-Ordners im Blick haben. Mit dem folgenden PowerShell-Beispiel können Sie die Größen der Unterordner von *RecoverableItems* abfragen:

```
# Abfrage der RecoverableItems-Ordnergrößen in einem Postfach
Get-Mailbox JohnDoe | Get-mailboxFolderStatistics `
  -FolderScope RecoverableItems | FT Name,FolderSize -AutoSize
```

Um eine Auswertung über alle Postfächer zu erhalten, empfehle ich Ihnen das Skript *Get-AuditLogOverHead.ps1*, das Sie auf GitHub finden: *https://github.com/cunninghamp/Get-AuditLogOverHead.ps1*

Die zu protokollierenden Aktionen sind je nach zugreifendem Personenkreis vordefiniert, können aber individuell angepasst werden. Die vordefinierten Aktionen sind:

- **Für Eigentümer** – keine
- **Für Stellvertreter** – `Update`, `SoftDelete`, `HardDelete`, `SendAs`, `Create`

- **Für Administratoren** – `Update`, `Move`, `MoveToDeletedItems`, `SoftDelete`, `HardDelete`, `FolderBind`, `SendAs`, `SendOnBehalf`, `Create`

Aktivieren Sie die Protokollierung für Postfacheigentümer nur in besonderen Fällen, z. B. zur Fehlersuche bei Zugriffsproblemen. Die Zugriffe eines Eigentümers führen zu einem exorbitanten Wachstum des Protokolls.

Im Postfach-Audit-Protokoll können die folgenden Postfach-Aktionen protokolliert werden:

Aktion	Beschreibung
Copy	Kopieren eines Objekts in einen anderen Postfachordner
Create	Erstellung eines neuen Objekts im Ordner *Kalender*, *Kontakte* oder *Notizen*; die Erstellung eines neuen Ordners oder einer neuen E-Mail wird nicht protokolliert.
FolderBind	Zugriff auf einen Postfachordner; ein konsolidierter Audit-Eintrag je 24 Stunden
HardDelete	Endgültige Löschung eines Objekts aus den wiederherstellbaren Objekten
MailboxLogin	Anmeldung des Postfacheigentümers an das Postfach; nur verfügbar für POP3-, IMAP4- und OAuth-Zugriffe.
MessageBind	Ein Objekt wurde geöffnet oder in der Leseansicht dargestellt.
Move	Ein Objekt wurde in einen anderen Postfachordner verschoben.
MoveToDeleted-Items	Ein Objekt wurde in den Ordner *Gelöschte Elemente* verschoben.
SendAs	Eine Nachricht wurde mit *Senden als*-Berechtigung gesendet.
SendOnBehalf	Eine Nachricht wurde mit *Senden im Auftrag von*-Berechtigung gesendet.
SoftDelete	Ein Objekt wurde aus dem Ordner *Gelöschte Elemente* entfernt.
Update	Eine Objekteigenschaft wurde aktualisiert.

Tabelle 9.1 Postfach-Audit-Protokoll-Aktionen

Diese Aktionen können nicht gleichermaßen für alle drei Personengruppen verwendet werden. Die Protokollierung von `SendAs` und `SendOnBehalf` ist z. B. für Postfacheigentümer nicht verfügbar.

Die Konfiguration des Postfach-Audit-Protokolls erfolgt mithilfe des Cmdlets `Set-Mailbox`. Hier sind einige Beispiele:

```
# Aktivieren des Postfach-Audit-Protokolls für einen einzelnen Anwender
Set-Mailbox -Identity JohnDoe -AuditEnabled $true

# Aktivieren des Postfach-Audit-Protokolls für alle geteilten Postfächer
Get-Mailbox -ResultSize Unlimited -Filter `
  {RecipientTypeDetails -eq "SharedMailbox"} | Select PrimarySmtpAddress | `
  ForEach {Set-Mailbox -Identity $_.PrimarySmtpAddress -AuditEnabled $true}

# Aktivieren des Postfach-Audit-Protokolls für einen einzelnen Anwender
Set-Mailbox -Identity JohnDoe -AuditEnabled $false

# Aktivieren des Postfach-Audit-Protokolls für Administratorzugriffe
# auf das Postfach eines einzelnen Anwenders
Set-Mailbox -Identity John.Doe@varunagroup.de -AuditAdmin `
  MessageBind,FolderBind -AuditEnabled $true

# Aktivieren des Postfach-Audit-Protokolls für Administratorzugriffe
# für die C-Level-Postfächer in einer dedizierten OU
Get-Mailbox -OrganizationalUnit varunagroup.de/DE/CLevel | Select `
  PrimarySmtpAddress | ForEach {Set-Mailbox -Identity $_.PrimarySmtpAddress `
  -AuditAdmin MessageBind,FolderBind -AuditEnabled $true}
```

Eine Audit-Protokollierung ist nur dann sinnvoll, wenn Sie die Daten auch durchsuchen oder exportieren können. Ebenso wie beim Admin-Audit-Protokoll stehen Ihnen eine synchrone und eine asynchrone Suche zur Verfügung (*https://docs.microsoft.com/powershell/module/exchange/policy-and-compliance-audit/Search-MailboxAuditLog* und *https://docs.microsoft.com/powershell/module/exchange/policy-and-compliance-audit/New-MailboxAuditLogSearch*). Die Ausgabe der synchronen Suchergebnisse erfolgt direkt in der Exchange Management Shell, während die asynchronen Suchergebnisse als XML-Dateianhang per E-Mail zugestellt werden:

```
# Synchrone Suche im Postfach-Audit-Protokoll für Admin- und
# Stellvertreterzugriffe zwischen dem 01.01. und dem 30.06.2022
Search-MailboxAuditLog -Identity JohnDoe -LogonTypes Admin,Delegate `
  -StartDate 1/1/2022 -EndDate 6/30/2022 -ResultSize 2000

# Asynchrone Suche im Postfach-Audit-Protokoll für Admin- und
# Stellvertreterzugriffe zwischen dem 01.01. und dem 30.06.2022
# mit Zustellung der Suchergebnisse an admin@varunagroup.de
```

```
New-MailboxAuditLogSearch "Admin-Stellvertreterzugriff" -Mailboxes `
  "John Doe","Jane Doe" -LogonTypes Admin,Delegate -StartDate 1/1/2022 `
  -EndDate 6/30/2022 -StatusMailRecipients admin@varunagoup.de
```

Die Suchergebnisse werden als XML-Dateianhang an den angegebenen Audit-Empfänger versendet. Erfolgt der Zugriff auf das Postfach des Audit-Empfängers mit Outlook, ist das Dateiformat des Anhangs kein Problem. Wird beim Zugriff auf das Auditor-Postfach aber *Outlook on the Web* verwendet, so muss die OWA-Postfachrichtlinie für den Empfänger angepasst werden. Standardmäßig werden Dateianhänge im XML-Format in Outlook on the Web blockiert. Um den Zugriff auf diese Anhänge zu erlauben, müssen Sie die OWA-Postfachrichtlinie für das Auditor-Postfach anpassen. Im Microsoft-Beispiel zu diesem Thema erfolgt eine Anpassung der Standard-OWA-Richtlinie. Von einer allgemeinen Anpassung der Standardrichtlinie kann ich Ihnen nur abraten, da Sie damit den Zugriff auf XML-Dateianhänge für alle Anwender freigeben. Erstellen Sie für das Auditor-Postfach immer eine separate OWA-Richtlinie, und weisen Sie diese dem Auditor-Postfach zu:

```
# Erstellung einer neuen OWA-Richtlinie
New-OwaMailboxPolicy -Name Audit-OWA-Pol

# Prüfen, ob XML-Dateien in der OWA-Richtlinie blockiert werden
Get-OwaMailboxPolicy -Identity Audit-OWA-Pol | Select-Object `
  -ExpandProperty AllowedFileTypes

# Hinzufügen von XML als erlaubtem Dateityp
Set-OwaMailboxPolicy -Identity Audit-OWA-Pol -AllowedFileTypes @{add='.xml'}
```

Einen Export des Postfach-Audit-Protokolls können Sie über das Exchange Admin Center durchführen. Im Abschnitt Überwachung finden Sie neben anderen vordefinierten Berichten die Funktion Postfachüberwachungsprotokolle exportieren (siehe Abbildung 9.13).

Aber keine Regel ohne Ausnahme: Wenn PowerShell-Skripte oder andere Applikationen regelmäßig unter Verwendung von Dienstkonten auf Postfächer zugreifen, führen diese Zugriffe zu übermäßig vielen Protokolleinträgen. Dadurch verschwinden die interessanten Einträge in der Masse. Damit die Zugriffe der verwendeten Dienstkonten nicht protokolliert werden, können Sie für diese Konten Ausnahmen konfigurieren, den sogenannten *Audit-Protokoll-Bypass*. Die beiden folgenden Beispiele zeigen die Aktivierung und Deaktivierung des Postfach-Audit-Protokoll-Bypasses:

```
# Aktivierung des Audit-Protokoll-Bypasses für das Dienstkonto zz-Monitoring
Set-MailboxAuditBypassAssociation -Identity "zz-Monitoring" `
  -AuditBypassEnabled $true
```



```
# Deaktivierung des Audit-Protokoll-Bypasses für das Dienstkonto
# zz-Monitoring
Set-MailboxAuditBypassAssociation -Identity "zz-Monitoring" `
  -AuditBypassEnabled $false
```

Abbildung 9.13 Überwachungsberichte im Exchange Admin Center

Die Aktivierung des Bypasses stellt durchaus ein Sicherheitsrisiko dar. Daher müssen Sie die Konten, für die ein Protokoll-Bypass konfiguriert ist, regelmäßig auditieren. Das folgende Cmdlet listet alle Bypass-Zuordnungen auf:

```
# Ausgabe aller Postfach-Audit-Protokoll-Zuordnungen
Get-MailboxAuditBypassAssociation -ResultSize unlimited
```

Ich empfehle Ihnen, das Postfach-Audit-Protokoll für alle Postfächer zu aktivieren, in denen wichtige und sensible Unternehmensdaten liegen oder persönliche Daten von Personengruppen, für die die DSGVO gilt.

Wenn Sie Postfächer in Exchange Online verwenden, ist die Aktivierung der Postfach-Audit-Protokollierung ein Kriterium für einen besseren *Secure Score* (*https://docs.microsoft.com/microsoft-365/security/defender/microsoft-secure-score*).

9.4 Dokumenten-Management-Systeme

Beim Betrieb einer Exchange Server-Plattform wird sehr häufig immer nur das Thema E-Mail-Archivierung betrachtet. Dabei stellen E-Mail-Nachrichten genau *einen*

der zu archivierenden Dokumententypen dar. In der rechtlichen Betrachtung der zu archivierenden Dokumente ist es aber notwendig, dass Sie den Fokus erweitern und auch andere Systeme, z. B. ERP oder CRM, mitbetrachten.

Durch den Einsatz einer (Compliance-)Archivierungslösung, die auf einem professionellen Dokumenten-Management-System (DMS) basiert, führen Sie nicht nur die rechtlich relevanten Dokumente in einer zentralen Ablage zusammen. Vielmehr erschaffen Sie so auch eine fachübergreifende Wissenslösung, in der Informationen um Meta-Daten angereicht sind und auf diese Weise kontextbezogen durchsucht werden können.

Ein gutes DMS verfügt über eine zentrale Datenspeicherung unterschiedlicher Dokumententypen und erkennt – gerade im Hinblick auf die Speicherung von E-Mails – Duplikate. Erfolgt eine zentrale Speicherung aller eingehenden E-Mails im DMS, so führt eine zusätzliche manuelle Speicherung der gleichen E-Mail-Nachricht durch einen Anwender nicht zu einer doppelten Ablage der Nachricht. Vielmehr wird die bereits gespeicherte Nachricht um weitere Meta-Daten angereichert. Das DMS kann dadurch diese Nachricht sowohl in einer unternehmensweiten Suche als auch in einer persönlichen Suche des Anwenders anzeigen.

Die Nutzung eines DMS führt natürlich zu neuen Abhängigkeiten und Aufwänden. Gerade im Hinblick auf die zu erwartenden Aufbewahrungs- und damit Betriebszeiten der DMS-Lösung wird eine Entscheidung für oder gegen ein DMS nicht leichter. Eine detaillierte Bewertung zur Auswahl und Einführung eines DMS ist allerdings nicht Bestandteil dieses Buches.

9.5 Zusammenfassung

Die Themen *Archivierung* und *Compliance* nehmen eine immer bedeutendere Stellung für den Betrieb einer Exchange Server-Plattform ein. Gerade im Bereich der Archivierung ist eine genaue Definition des Begriffs *Archiv* notwendig. In diesem Kapitel habe ich versucht, Ihre Aufmerksamkeit für dieses Thema im täglichen Umgang mit der Archivierung zu schärfen. Sie dürfen bei Diskussionen zu diesem Thema nicht davon ausgehen, dass die anderen Beteiligten das Gleiche meinen und das Gleiche verstehen.

Exchange Server bietet uns schon seit geraumer Zeit die Möglichkeit, Anwendern ein persönliches *Online Archiv-Postfach* zur Verfügung zu stellen. Den größtmöglichen Vorteil aus dem Archiv-Postfach können Sie aber nur ziehen, wenn Sie das Postfach in Verbindung mit praktikablen *Aufbewahrungsrichtlinien* betreiben. Ohne diese Richtlinien ist es nur ein zweites Postfach, das Anwender nach Gutdünken nutzen. Ebenso muss seine Einführung mit Informationen im Intranet und IT-Serviceportal begleitet werden. Ansonsten wird die Einführung kein Erfolg.

Wenn Sie sich für eine E-Mail-Archivierungslösung eines Drittanbieters entscheiden, müssen Sie sehr genau prüfen, welche Vor- und Nachteile das Produkt hat. Technisch sind die meisten Produkte sehr ausgereift, und viele sind auch schon seit Jahren auf dem Markt. Jedoch stellen sich immer wichtige Fragen hinsichtlich der Nutzung durch Anwender: Soll die Archivierungslösung auch als Recherchewerkzeug für Anwender genutzt werden können? Wenn ja, ist eine Nutzung ohne Medienbruch für die Anwender möglich?

Naturgemäß versteht man unter einer Archivierung eine unveränderliche Speicherung von Informationen. Sie werden aber immer irgendwann vor der Situation stehen, archivierte Daten in eine andere Archivierungslösung überführen zu müssen. Hier müssen Sie schon vor der Einführung wissen, ob die Software einen späteren Export unterstützt. Bedenken Sie, dass es auch in Ihrem Unternehmen eine Anforderung geben kann, Daten für 26 Jahre oder länger aufzubewahren. Solche Aufbewahrungsfristen sind für Exchange Server jenseits von Gut und Böse und erfordern den Einsatz eines *Dokumenten-Management-Systems*.

Exchange Server kann Ihnen helfen, E-Mail-Nachrichten innerhalb der Postfächer dauerhaft zu speichern. Jedoch bietet das Produkt keine sehr elegante Methode, um regelmäßig auf diese Daten zugreifen zu können. Sein Ziel ist vielmehr die Unterstützung im Falle von eDiscovery-Anfragen.

Um Datenverlust durch das Versenden von ungeschützten Dokumenten zu vermeiden, können Sie auf *DLP* zurückgreifen. Diese Funktion kann den Versand von sensiblen Informationen durch unberechtigte Personen unterbinden und so Schaden vom Ihrem Unternehmen abwenden.

Nachdem Sie nun so viel über Archivierung und Compliance erfahren haben und Exchange Server in Ihrer IT-Infrastruktur nach Best Practices implementiert wurde, schauen wir uns im nächsten Kapitel einmal an, wie man Exchange Server *nicht* implementieren sollte.