Osterman Research

BERICHT

Bericht von Osterman Research
Veröffentlicht im **Juli 2023**
Gesponsert von **MailStore**

Die Vorteile von unabhängigen E-Mail-Archivierungslösungen für Nutzer von Microsoft 365

Überblick

E-Mails sind für die meisten Nutzer nach wie vor das wichtigste Mittel der Kommunikation und Zusammenarbeit – trotz der zunehmenden Nutzung neuer Lösungen wie Microsoft Teams und Slack. Sie enthalten eine Fülle wichtiger Informationen, die durch robuste Backup- und Archivierungsfunktionen geschützt werden müssen, damit Unternehmen und Benutzer jederzeit Zugriff auf ihre Daten haben.

Unternehmen, die zu Microsoft 365 wechseln, müssen bewährte Verfahren zur Sicherung und Archivierung von E-Mails anwenden, um ihre Unternehmensdaten zu schützen und verfügbar zu halten. Sicherung und Archivierung erfolgen in Microsoft 365 nicht automatisch. Zudem müssen die Backup- und Archivierungsfunktionen auch Szenarien abdecken, die Microsoft 365 nicht so gut beherrscht wie einige Drittanbieter, darunter hybride Umgebungen und solche mit Daten, die nicht von Microsoft stammen.

Das vorliegende Whitepaper geht der Frage nach, warum kleine und mittelständische Unternehmen (KMU) eine Lösung zur Archivierung ihrer E-Mails einsetzen und warum sie dabei auch Drittanbieter in Betracht ziehen sollten.

KMU benötigen zuverlässige Backup- und Archivierungs-funktionen, um den Schutz, die Aufbewahrung und die Verfügbarkeit ihrer wichtigen Datenbestände zu gewährleisten.

DAS WICHTIGSTE IN KÜRZE

Diese Themen werden im Whitepaper behandelt:

- **Microsoft 365 wird von KMU in großem Umfang genutzt**
  Microsoft 365 bietet eine breite Palette von Kommunikations- und Kollaborationsfunktionen zu einem günstigen Preis. Darüber hinaus erfordert die Wartung nur minimalen IT-Aufwand und wird von einem vertrauenswürdigen, zuverlässigen Anbieter durchgeführt.
- **Entscheidungsträger sind zum Schutz ihrer Daten verpflichtet**
  Ein gemeinsamer Cloud-Anbieter für E-Mail, Zusammenarbeit, Backup, Archivierung und mehr entlastet die IT. Dies entbindet die Entscheidungsträger jedoch nicht von ihrer Pflicht, ihre Daten zu schützen.
- **KMU brauchen robuste Backup- und Archivierungsfunktionen für E-Mails**
  KMU benötigen zuverlässige Backup- und Archivierungsfunktionen für E-Mails, um ihre kritischen Datenbestände zu schützen und aufzubewahren, von denen sich viele auf den E-Mail-Systemen befinden. Das Backup und die Archivierung von E-Mails gehören zusammen und sind gleichermaßen wichtig.
- **Microsoft ist nicht für den Schutz und die Aufbewahrung kundenseitiger Daten verantwortlich**
  Gemäß dem Modell der geteilten Verantwortung („Shared Responsibility Model“) von Microsoft 365 müssen die Kunden aktiv dafür sorgen, dass ihre Daten ausreichend gesichert und archiviert werden.

- **Unzureichender Datenschutz kann gravierende Folgen haben**
  Dazu gehört u. a. das versehentliche oder böswillige Löschen wichtiger Daten, Ransomware, die den Datenzugriff verhindert, und die Unfähigkeit, rechtsverbindliche Anforderungen zu erfüllen.
- **Eine robuste Lösung für die Archivierung von E-Mails**
  Jedes Unternehmen sollte eine robuste E-Mail-Archivierungslösung einsetzen und pflegen, um seine Geschäftsunterlagen zu erhalten und sicherzustellen, dass diese durchsucht und abgerufen werden können. Und die Entscheidungsträger sollten bei der Aufbewahrung und Archivierung ihrer Daten auch Drittanbieter in Betracht ziehen.

ZU DIESEM WHITEPAPER

Das vorliegende Whitepaper wurde von MailStore in Auftrag gegeben. Nähere Informationen zu MailStore finden sich am Ende des Dokuments.

Die wachsende Bedeutung von Microsoft 365 für Unternehmen

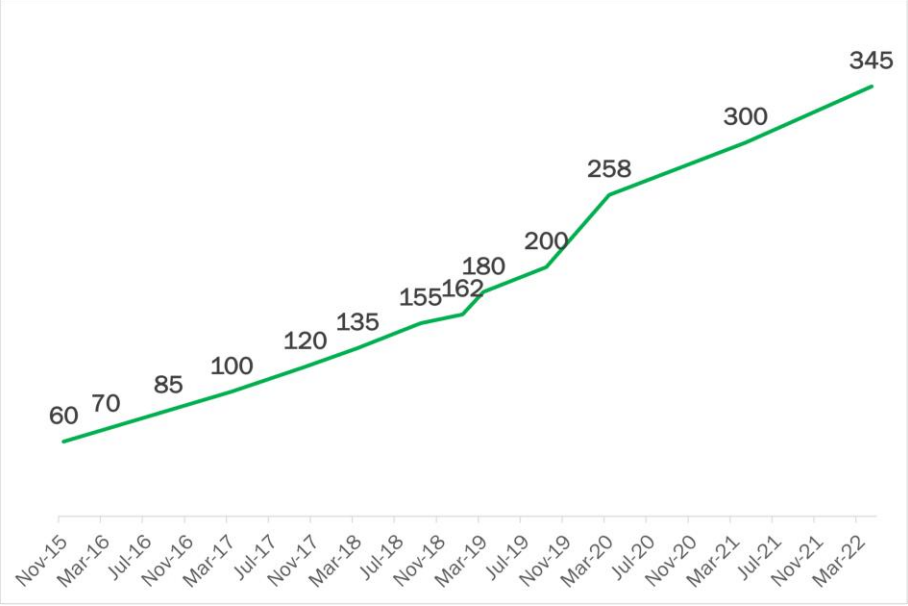
Microsoft 365 ist für Unternehmen in aller Welt von wachsender Bedeutung. In diesem Abschnitt wird deshalb seine zunehmende Marktdurchdringung in den Bereichen geschäftliche E-Mails und Zusammenarbeit analysiert.

IMMER MEHR UNTERNEHMEN SETZEN AUF MICROSOFT 365

Microsoft 365 ist eine zuverlässige und vielseitige Plattform, die eine große Bandbreite an Funktionen bietet. Hierzu zählen E-Mail, Desktop-Produktivitätsanwendungen, Kollaboration, Security, Archivierung, Verschlüsselung, Sprache und andere Dienste. Es gibt verschiedene Tarife für kleine Unternehmen, Konzerne, staatliche Stellen, Bildungseinrichtungen und private Anwender.

Microsoft bietet bereits seit Ende der Neunzigerjahre gehostete Lösungen in unterschiedlichen Varianten an. Microsoft 365 ist dabei die bislang erfolgreichste nicht standortgebundene Lösung des Unternehmens für E-Mail und Kollaboration. Ausgehend von den aktuellsten vorliegenden Microsoft-Daten verzeichnete das Unternehmen zum Ende des ersten Quartals 2022 knapp 345 Mio. Nutzer (siehe Abbildung 1).[1] Das ist fast sechsmal so viel wie noch im November 2015.

Abbildung 1
Microsoft 365 Unternehmenstarife – Nutzer weltweit
In Mio. Nutzern

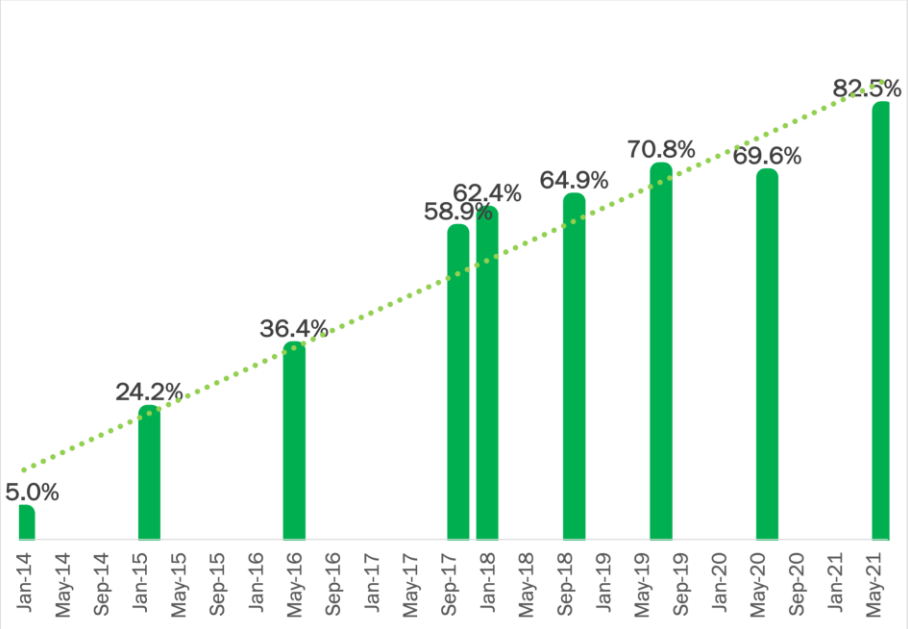


Quelle: Osterman Research, 2023. Datenquelle: Microsoft Corporation.

Microsoft 365 ist eine zuverlässige und leistungsfähige Plattform.

Mit dem Wachstum der Installationsbasis von Microsoft 365 geht die zunehmende Durchdringung von Microsoft 365 in den E-Mail- und Kollaborationsmarkt für Unternehmen einher. Die Marktdaten von Osterman Research basieren auf mehreren Umfragen in den vergangenen Jahren und deuten auf eine kontinuierlich gestiegene Nutzung von Microsoft 365 für E-Mails durch nordamerikanische Unternehmen hin. Die Marktdurchdringung beläuft sich auf 80 % und wurde in weniger als zehn Jahren erreicht (siehe Abbildung 2).

Abbildung 2
Microsoft 365 – Verbreitung
Anteil nordamerikanischer Unternehmenskunden mit Microsoft 365 für E-Mail



Quelle: Osterman Research, 2023.

MICROSOFT 365 BIETET VIEL SPEICHERPLATZ, HAT ABER AUCH EINEN NACHTEIL

Einer der größten Vorteile von Exchange Online, der E-Mail-Komponente von Microsoft 365, sind die besonders großen Postfächer. In der Regel ist das Postfach in den Business-Tarifen 50 Gigabyte und in den teureren Enterprise-Paketen von Microsoft 365 und Office 365 100 Gigabyte groß.[2]

Sehr große Postfächer können ein Segen für die Benutzerproduktivität sein, da quasi unbegrenzt viele Daten gespeichert werden können und sich die Unternehmen in dieser Hinsicht keine Gedanken machen müssen. Die enorme Menge an Speicherplatz, die dabei jedem Nutzer zur Verfügung steht, hat jedoch auch gewisse Nachteile. Diese werden hier aufgelistet:

- **Weitreichende Folgen bei Hackerangriffen**
  Werden Anmeldedaten eines Microsoft 365-Benutzerkontos per Phishing abgegriffen, erhalten die Angreifer Zugang zu vielen wertvoller Geschäftsdaten. Liegen die Daten dagegen in einem abgetrennten Archiv, ist das Ausmaß der Datenschutzverletzung deutlich geringer.
- **Zeitaufwändige Wiederherstellung**
  Muss ein 50 oder 100 Gigabyte großes Postfach aus einem Backup wiederhergestellt werden, sind die betroffenen Benutzer viel länger offline, als wenn die Daten fortlaufend in ein Archiv verschoben worden wären.
- **Überlastung von Outlook**
  Die Reaktions- und Leistungsfähigkeit von Outlook kann abnehmen, wenn Ordner zu viele Elemente enthalten.[3] So ist bei Postfächern mit mehr als 10 GB mit häufigen Verzögerungen zu rechnen[4].

Unternehmen mit sehr großen Benutzerpost-fächern haben einige Nachteile – wie häufigere Datenlecks, eine zeitaufwändige Datenwiederher-stellung und eine geringere Leistung der Anwendung.

E-Mail-Archivierung ist unverzichtbar

Unternehmen, die E-Mails für die geschäftliche Kommunikation nutzen, müssen sich auf die Richtigkeit und Vollständigkeit ihrer archivierten E-Mails verlassen können. Deshalb geht es in diesem Abschnitt um die geschäftlichen Hintergründe der E-Mail-Archivierung und ihre Merkmale gegenüber Backups.

GRÜNDE FÜR DIE E-MAIL-ARCHIVIERUNG

In den meisten Unternehmen (einschließlich KMU) sind E-Mails nach wie vor das wichtigste Mittel für Kommunikation und Zusammenarbeit. Dementsprechend enthalten E-Mail-Systeme eine Vielzahl verschiedener Daten wie Verträge, Bestellungen, Marketingpläne, Versanddokumente, Kundenkommunikation, Antworten auf technische Supportanfragen, Personaldaten, Belege für sexuelle Belästigung oder die unfaire Behandlung von Mitarbeitern und viele andere Informationen – allesamt geschäftliche Dokumente. Um genau nachvollziehen zu können, was angeboten, erklärt, vereinbart oder bestritten wurde, ist eine korrekte und vollständige Aufzeichnung der E-Mails für Unternehmen zur Erfüllung ihrer geschäftlichen, administrativen oder behördlichen Anforderungen also unerlässlich. Hier einige Beispiele für alltägliche Situationen, in denen der problemlose Zugriff auf E-Mail-Daten hilfreich ist:

- **Reklamationen**
  Ein Kunde reklamiert einen Auftrag und der Vertrieb muss alle zugehörigen Informationen finden.
- **Fragen zu Vereinbarungen**
  Ein Lieferant fragt nach einer Bestätigung, die ihm gegeben wurde.
- **Versehentliche Löschung von E-Mails**
  Ein Benutzer hat versehentlich E-Mails aus seinem Postfach gelöscht.
- **Nicht verfügbarer E-Mail-Dienst**
  Aufgrund eines Ausfalls des E-Mail-Dienstes ist der Zugriff auf das Postfach nicht möglich und die gesuchte E-Mail kann auch im letzten Backup nicht gefunden werden.
- **Juristische Ermittlungen**
  Konkurrenten, Kunden, Geschäftspartner und verärgerte Mitarbeiter können rechtliche Schritte gegen Unternehmen einleiten, um eine Entschädigung für angebliches Fehlverhalten zu erwirken.
- **Interne Untersuchungen**
  Anschuldigungen wegen sexueller Belästigung, ungerechter Behandlung, rassistischer Diskriminierung und anderen arbeitsrechtlichen Vorwürfen kann nur nachgegangen werden, wenn vollständige und korrekte Nachweise vorliegen.

In den meisten Unternehmen (einschließlich KMU) sind E-Mails nach wie vor das wichtigste Mittel für Kommunikation und Zusammenarbeit.

E-MAIL-ARCHIVIERUNG UND COMPLIANCE

Effiziente organisatorische Abläufe und die Bewältigung alltäglicher Situationen sind nur zwei Gründe dafür, warum eine korrekte und vollständige Aufzeichnung von E-Mails so wichtig ist. Denn die Unternehmen sehen sich auch mit einer wachsenden Zahl von gesetzlichen Auflagen, Branchenanforderungen und Gerichtsurteilen konfrontiert. Dazu zählen:

- **EU-DSGVO**
  Es muss nachgewiesen werden können, ob das Unternehmen die Datenschutz-Grundverordnung der Europäischen Union (DSGVO) einhält – auch mit Blick auf Datenerhebung, -verarbeitung und -speicherung.
- **Weltweite Datenschutzvorschriften**
  Die Datenschutzvorschriften anderer Länder, wie zum Beispiel den USA, enthalten oft ähnliche Anforderungen zu Datenerhebung und -verarbeitung wie die DSGVO.
- **Aufbewahrungspflichten**
  Rechtliche Vorschriften, die nicht nur für regulierte Branchen wie das Gesundheitswesen, die Finanzbranche oder das verarbeitende Gewerbe gelten, verlangen häufig auch die Aufbewahrung von E-Mails. Auch wenn sie je nach Land und Branche unterschiedlich ausgestaltet sind, müssen E-Mails in der Regel mehrere Jahre aufbewahrt werden.

Und da geschäftliche Dokumente aufgrund von rechtlichen Verpflichtungen, juristischem Rat oder sogenannten Best Practices eine bestimmte Zeit lang aufbewahrt werden müssen, benötigt jedes Unternehmen ein Archiv für E-Mails und Anhänge, in dem diese Datensätze entsprechend gespeichert werden.

Verstöße können weitreichende Konsequenzen haben. Dazu zählen auch Geldbußen und Strafen für die unzureichende Aufbewahrung der vorgeschriebenen Datensätze sowie der Verlust von Daten, die im betrieblichen Alltag benötigt werden könnten.

BACKUPS STATT E-MAIL-ARCHIVIERUNG?

Es gibt einige gute Argumente dafür, beide Verfahren einzusetzen. Schließlich handelt es sich um einander ergänzende Verfahren, die auf unterschiedliche strategische Anwendungsfälle abzielen:

- **Backups dienen der Wiederherstellung im Notfall**
  E-Mail-Backups sind für die Aufrechterhaltung der Geschäftstätigkeit und die Wiederherstellung im Notfall gedacht (*Disaster Recovery*) – auch bei Problemen, die zu Datenverlusten führen. Das können missglückte Software-Upgrades sein oder aber Administratoren und Mitarbeiter mit böswilligen Absichten, die Daten löschen. Backups dienen zur kurzfristigen Speicherung. Sie enthalten nicht indizierte Daten, werden in der Regel 30 bis 90 Tage lang aufbewahrt und erfassen die Daten zu einem bestimmten Zeitpunkt.

Entscheidungs-träger, die Microsoft 365 in Betracht ziehen oder bereits nutzen, sollten die Vor- und Nachteile der nativen Archivierungsfun ktionen kennen.

- **Die E-Mail-Archivierung dient dem Schutz, der Verfügbarkeit und der Auffindbarkeit von Daten**
  E-Mail-Archive dienen einem anderen strategischen Zweck: der Aufbewahrung von Geschäftsdaten zur Erfüllung rechtlicher, regulatorischer und branchenspezifischer Anforderungen. Die E-Mail-Archivierung bietet wichtige Vorteile. Denn sie ermöglicht nicht nur die Aufbewahrung der Daten in ihrer ursprünglichen Form und die Indizierung des E-Mail-Inhalts zum Zweck der Durchsuchung und des Wiederauffindens, sondern stellt auch sicher, dass Daten jederzeit verfügbar sind und abgerufen werden können. Und während Backups eher kurzfristig angelegt sind, sind E-Mail-Archive für Daten gedacht, die länger aufbewahrt werden müssen – oft über Jahre oder unbefristet. Hinzu kommt, dass E-Mail-Backups lediglich Momentaufnahmen der Daten erfassen. Bei der E-Mail-Archivierung werden dagegen alle geschäftlichen Datensätze fortlaufend erfasst. Und das ermöglicht ihre Durchsuchung und Wiederherstellung sowie die Erfüllung geltender Aufbewahrungspflichten.

VOR- UND NACHTEILE DER E-MAIL-ARCHIVIERUNG IN MICROSOFT 365

Entscheidungsträger, die ein E-Mail-System mit Archivierungsfunktion wie Microsoft 365 in Erwägung ziehen oder bereits verwenden, sollten wissen, was dieses leistet und was nicht. Auf dieser Grundlage muss dann entschieden werden, ob es die Anforderungen des jeweiligen Unternehmens erfüllt.

Die native Archivierung in Microsoft 365

Mit Microsoft 365 bietet Microsoft eine zuverlässige und vielseitige Kommunikations- und Kollaborationslösung, E-Mails werden jedoch nicht automatisch archiviert. Unternehmen, die Microsoft 365 nutzen, haben zwei Möglichkeiten. Sie können die Zeit und Arbeit investieren, um herauszufinden, wie sie Funktionen rund um *Information Governance* und *Compliance* nutzen können, etwa in Form von Aufbewahrungsvorschriften. Alternativ können sie auf eine benutzerfreundlichere E-Mail-Archivierungslösung eines Drittanbieters zurückgreifen. Letzteres ist besonders relevant für KMU mit knappen oder gar keinen IT-Ressourcen. Im folgenden Abschnitt wird daher der Funktionsumfang von Microsoft 365 vorgestellt.

KONZEPTIONELLE ECKPFEILER DER E-MAIL-ARCHIVIERUNG IN MICROSOFT 365

Der konzeptionelle Ansatz und die Architektur der E-Mail-Archivierung in Microsoft 365 beruhen auf vier Eckpfeilern:

1. **Nachrichten werden dort „archiviert", wo sie sich in Exchange Online befinden – und nirgendwo sonst**
   E-Mails können vor dem Löschen geschützt werden – unabhängig davon, wo sie sich in Exchange Online befinden. So entsteht sozusagen ein Archiv mit geschützten Inhalten. Archivkopien werden in Microsoft 365 aber nicht erstellt. Denn nach Auffassung von Microsoft sind diese nicht erforderlich, solange für E-Mails und Anhänge ein geeigneter Löschschutz eingerichtet wird. Dieser Ansatz birgt ein klares Risiko. Denn wenn die Schutzmaßnahmen umgangen werden oder versagen, gehen die Daten leicht verloren.
2. **Aufbewahrungsrichtlinien entscheiden, was aufbewahrt wird und was nicht – und für wie lange**
   Mit Aufbewahrungsrichtlinien kann man festlegen, wie lange Nachrichten nicht gelöscht werden können und ab wann dies möglich ist – und zwar sowohl aus dem Posteingang als auch dem Archiv des jeweiligen Benutzers. Die Aufbewahrungsrichtlinien gelten für das Postfach und das Archiv des jeweiligen Benutzers. Und die Nachrichten werden ungeachtet ihres Aufbewahrungsorts geschützt. Die Größe des Postfachs richtet sich dabei nach dem gewählten Tarif und kann das festgelegte Volumen nicht überschreiten.
3. **Archivierungsrichtlinien legen fest, wann Nachrichten in das Archiv verschoben werden**
   Archivierungsrichtlinien legen fest, welche Nachrichten in das Archiv des jeweiligen Benutzers verschoben werden, sofern die E-Mail-Archivierung aktiviert ist oder die Archivierung in Exchange Online verwendet wird. Auf dieser Grundlage werden Nachrichten dann aus dem Postfach ins Archiv verschoben, meist auf Basis von bereits vergangener Zeit.
4. **Archiv-, Rechts- und eDiscovery-Funktionen hängen vom Tarif ab**
   Die für Archivierung, Aufbewahrung und eDiscovery verfügbaren Funktionen werden je nach Benutzer festgelegt – und nicht für die Organisation als Ganzes. Während Microsoft 365 die Kombination und Anpassung von Tarifen innerhalb von Organisationen ermöglicht, müssen für den vollen Funktionsumfang höherpreisige Tarife abgeschlossen werden.

Microsoft 365 ist eine zuverlässige und vielseitige Lösung für Kommunikation und Zusammenarbeit – E-Mails werden aber nicht automatisch archiviert.

Diese konzeptionelle Architektur bedeutet, dass die „Archivierungs“-Optionen von Microsoft 365 festlegen, wo Nachrichten gespeichert werden. Doch keine dieser nativen Archivierungsoptionen beinhaltet einen besonderen Schutz vor Änderungen und Löschung; dazu ist der ergänzende Einsatz von Aufbewahrungsrichtlinien notwendig. Bei Exchange Online Archiving (EOA) reduziert das Archivpostfach das Speichervolumen des eigentlichen Postfachs, das maximal 50 oder 100 GB erreichen kann (je nach gewähltem Tarif).

Dabei ist zu beachten, dass die Vor-Ort-Archivierung (also das Anwenden von Aufbewahrungsrichtlinien an dem Ort wo sich die Nachricht befindet) bedeutet, dass alle Daten, die in Microsoft 365 empfangen, erstellt oder gespeichert werden, als Teil des jeweiligen Datensatzes angesehen werden – und zwar unabhängig von ihrem Speicherort. Neu empfangene E-Mails in Exchange Online befinden sich also bereits im Speicherspektrum von Microsoft 365. Und ob sie im Posteingang verbleiben oder ins Archiv verschoben werden, ist irrelevant. Und sind Compliance- und Information-Governance-Funktionen im jeweiligen Tarif enthalten, sind diese sowohl im Posteingang als auch im Archiv verfügbar.

Es gibt vier Möglichkeiten zur Archivierung von E-Mails und anderen Dateien in Microsoft 365: die PST-Archivierung, die Archivierung in einen separaten Ordner über die Schaltfläche „Archivieren“ in Outlook, die Archivierung in ein anderes Postfach und die Archivierung in ein anderes Postfach per Exchange Online Archiving. Im Folgenden werden diese vier Optionen näher erläutert.

OPTION 1: PST-ARCHIVIERUNG

Benutzer können ihre E-Mails in PST-Dateien „archivieren“, die dann lokal oder in der Cloud gespeichert werden. Die Inhalte werden dabei nicht indiziert, sodass es schwierig werden kann, sie im Rahmen interner Ermittlungen, Fallprüfungen oder juristischer Zusammenhänge aufzufinden. Die Archivierung in PST-Dateien ist somit nicht zu empfehlen, um die Anforderungen an Compliance und Information Governance zu erfüllen. Zudem dienen PST-Dateien lediglich der Archivierung von Outlook-Inhalten, da die ursprüngliche Outlook-Archivierungsfunktion („AutoArchive“) auf PST-Dateien basiert. Microsoft nennt diese Funktion zwar „Archivierung“, es handelt sich aber nicht um ein Archiv im eigentlichen Sinne. Die Funktion ist lediglich dazu gedacht, Postfächer von kaum genutzten und älteren E-Mails zu entlasten.

Und so funktioniert es: Benutzer können Ordner oder einzelne E-Mails zur Archivierung auswählen, und diese können manuell oder automatisch aus dem primären Postfach verschoben werden. Die Inhalte werden dann in einer PST-Datei an einem individuell ausgewählten Ort gespeichert.

PST-Dateien können von jedem, der Zugriff auf sie hat, nach Belieben gelöscht werden und gehen unwiederbringlich verloren, wenn der jeweilige Computer beschädigt wird, abhandenkommt oder gestohlen wird. Werden PST-Dateien in OneDrive gespeichert, gehen sie verloren, sobald der jeweilige Benutzer das Unternehmen verlässt und sein Office 365-Konto deaktiviert wird (sofern der Inhalt von OneDrive zuvor nicht eigens davon ausgenommen wird).

OPTION 2: NACHRICHTEN PER „ARCHIVIEREN“-SCHALTFLÄCHE IN DEN OUTLOOK-ARCHIVORDNER VERSCHIEBEN

Der Outlook-Client enthält die Schaltfläche „Archivieren“, die sich jedoch lediglich auf einen Ordner namens „Archiv“ im Postfach des Benutzers bezieht (und über

Beim „Archivieren“ werden Nachrichten in Outlook lediglich in einen Ordner namens „Archiv“ im Postfach des Benutzers verschoben. Laut Microsoft ist dieser als normaler Ordner anzusehen.

Outlook zugänglich ist). Somit wird nur der Speicherort der Nachricht im Postfach geändert. Mit Blick auf Rechtssicherheit und Information Governance hat dies nichts mit einer tatsächlichen Archivierung zu tun – sofern für das Exchange Online-Postfach zuvor keine gesonderten Aufbewahrungsrichtlinien aufgestellt wurden. Ohne Aufbewahrungsrichtlinien kann der Benutzer Nachrichten aus diesem „Archiv“ also weiterhin löschen und ändern.

Das zeigt auch die Empfehlung von Microsoft zur Verwendung der „Archivieren“-Schaltfläche in Outlook: *„Wir empfehlen, die Archivfunktion zu verwenden, um Ihren Posteingang von Nachrichten freizuhalten, die Sie bereits beantwortet oder bearbeitet haben. Das Archiv kann man sich wie einen Aktenordner vorstellen. Sie können Elemente im Archivordner speichern und trotzdem problemlos auf sie zugreifen. Sie können die Nachrichten auch löschen oder in beliebige andere Ordner verschieben*.“[5]

Die Archivierungsschaltfläche in Outlook ist vor allem für Organisationen gedacht, die die 50 GB ihres Exchange Online-Postfachs in den günstigeren Tarifen von Microsoft 365 und Office 365 ohnehin nicht überschreiten. Damit ist laut Microsoft auch eine Archivierung in einem separaten Postfach überflüssig. Da das Postfach in diesen Tarifen maximal 50 GB groß sein kann, ist das Archivpostfach Microsofts Lösung falls mehr Speicherplatz benötigt wird (Option 3).

OPTION 3: ARCHIVPOSTFACH OHNE EXCHANGE ONLINE ARCHIVIERUNG

Der Spartarif Office 365 Enterprise E1 und zwei der Business-Tarife von Microsoft 365 enthalten ein optionales Archivpostfach mit maximal 50 GB als Ergänzung des eigentlichen Postfachs mit ebenfalls 50 GB. Dieses Archivpostfach muss allerdings von einem Administrator über das Exchange Admin Center oder PowerShell eingerichtet werden. Die erwähnten Tarife für Office 365 und Microsoft 365 enthalten allerdings keine Funktionen für eDiscovery oder Legal Hold. Und auch Aufbewahrungsrichtlinien werden darin nicht unterstützt.

Die Funktion war in Office 365 früher als „In-Situ-Archivierung“ bekannt.

OPTION 4: ARCHIVPOSTFACH MIT EXCHANGE ONLINE ARCHIVIERUNG

Exchange Online Archivierung (Exchange Online Archiving, EOA) ist die Microsoft-Unternehmenslösung für die E-Mail-Archivierung. Mit EOA können Benutzer E-Mails zwischen Postfach und Archivpostfach verschieben. Und Administratoren können Archivierungs- und Aufbewahrungsrichtlinien aufstellen, die das Verschieben, Verwalten, Aufbewahren und Löschen der E-Mails regeln. EOA enthält dieselben grundlegenden Archivierungsfunktionen wie Option 3 (s. o.), vergrößert das Archivpostfach allerdings auf 100 GB mit der Möglichkeit, den Archivspeicher automatisch auf bis zu 1,5 TB je Benutzer zu vergrößern. [6] EOA muss von einem Administrator eingerichtet werden. Und um das versehentliche Löschen von E-Mails durch die Benutzer zu verhindern, sind zudem Aufbewahrungsrichtlinien erforderlich. Die Archivpostfächer können vom Administrator über das Exchange Admin Center oder PowerShell aktiviert und deaktiviert werden.

EOA muss von einem Administrator eingerichtet werden. Und um das versehentliche Löschen von E-Mails durch die Benutzer zu verhindern, sind Aufbewahrungs-richtlinien erforderlich.

Ob ein Benutzer Zugriff auf Exchange Online Archivierung hat oder nicht, hängt von seinem Tarif ab. EOA ist in Office 365 und Microsoft 365 inbegriffen, sofern der Exchange Online Plan 2 enthalten ist. Ist dagegen nur Exchange Online Plan 1 enthalten, kann es separat lizenziert werden. In Office 365 Enterprise und Microsoft 365 Enterprise mit Exchange Online Plan 2 sind zudem Funktionen für

eDiscovery, Legal Hold und Retention enthalten. Im Tarif Microsoft 365 Business Premium sind diese dagegen nicht vorhanden.

Die eDiscovery-Tools von Microsoft fügen sich nahtlos in den Posteingang und ins Archiv ein. Zudem können Sperrfristen, sogenannte *Legal Holds*, aufgestellt werden, die die Bearbeitung von E-Mails verhindern. Aufgrund der Architektur der Vor-Ort-Archivierung und der Aufbewahrungsrichtlinien kann eDiscovery allerdings nur die Inhalte finden, die für die Aufbewahrung vorausgewählt wurden. Solange nicht alle E-Mails richtlinienbasiert aufbewahrt werden und die Benutzer überhaupt nichts löschen können, sind also nicht alle Daten für die eDiscovery zugänglich.

Für EOA gelten gewisse Einschränkungen:

- **Nicht möglich: Transportregeln, Journaling und automatisches Weiterleiten**
  EOA ist für die Archivierung von E-Mails durch die jeweiligen Benutzer ausgelegt. Transportregeln, Journaling und automatische Weiterleitung zur Verschiebung von Inhalten in andere Archivpostfächer sind mit EOA daher nicht gestattet.[7] Diese Methoden können auch nicht in anderen E-Mail-Anwendungen zur Erstellung unveränderlicher Archive eingesetzt werden.
- **Nur für Microsoft**
  EOA ist ausschließlich für Microsoft 365 und die neuesten Versionen von Microsoft Exchange Server vorgesehen. Plattformunabhängigkeit oder die parallele Nutzung mehrerer E-Mail-Plattformen sind somit nicht möglich. Das bedeutet, dass Unternehmen, die auch andere cloudbasierte E-Mail-Dienste (z. B. Google Workspace) oder lokale E-Mail-Server (z. B. MDaemon, IceWarp oder IMAP- und POP3-E-Mail-Server) verwenden, EOA nicht als E-Mail-Archiv nutzen können.
- **Archivpostfächer können deaktiviert und unwiederbringlich gelöscht werden**
  Wenn ein Administrator das Archivpostfach eines Benutzers im Exchange Admin Center oder per PowerShell deaktiviert, wird es nach 30 Tagen endgültig gelöscht. Wird es allerdings innerhalb der 30 Tage wieder durch einen Administrator aktiviert, wird die Verbindung mit dem vorher deaktivierten Archivpostfach wiederhergestellt. Geschieht dies nach Ablauf der 30 Tage, erhält der Benutzer ein neues, leeres Archivpostfach.[8] Wenn allerdings eine einfache Konfigurationsänderung ausreicht, um Inhalte zu löschen, die eigentlich archiviert werden sollten, ergeben sich daraus erhebliche Geschäfts- und Rechtssicherheitsrisiken.

Exchange Online Archivierung ist ausschließlich für Microsoft 365 vorgesehen. Plattform-unabhängigkeit und die Unterstützung mehrerer E-Mail-Plattformen sind somit ausgeschlossen.

MICROSOFT-ARCHIVIERUNGSVERFAHREN IM VERGLEICH

Abbildung 3 werden die verschiedenen Archivierungsverfahren in Microsoft 365 zusammengefasst.

Abbildung 3
Gegenüberstellung der Archivierungsverfahren für E-Mails in Microsoft 365

Archivierung-verfahren	**PST-Archivierung (Option 1)**	**Archiv-ordner (Option 2)**	**Archivpostfach (Option 3)**			**Exchange Online Archivierung (Option 4)**		
Microsoft Plan	**Alle Pläne**	**Alle Pläne**	**Microsoft 365 Business Basic/ Standard**	**Office 365 Enterprise E1**	**Office 365 Enterprise F3**	**Microsoft 365 Business Premium**	**Microsoft 365 Enterprise E3/E5**	**Office 365 Enterprise E3/E5**
Postfach-begrenzung	Nicht zutreffend	Nicht zutreffend	50 GB	50 GB	2 GB	50 GB	100 GB	100 GB
Archiv-postfach	Nicht zutreffend	Nicht zutreffend	50 GB	50 GB	N. z.	100 GB	100 GB	100 GB
Automatisch erweiterte Archivierung	Nicht zutreffend	Nicht zutreffend	Nein	Nein	Nein	Bis 1,5 TB	Bis 1,5 TB	Bis 1,5 TB
Inhaltsindizier-ung und -suche	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Ja
eDiscovery mit Aufbewahrung und Export	Nein	Tarif-abhängig	Nein	Nein	Nein	Nein	Ja	Ja
Aufbewahrung für juristische Zwecke zur Erfüllung rechtlicher Anforderungen	Nein	Tarif-abhängig	Nein	Nein	Nein	Ja	Ja	Ja
Aufbewahrungs-bezeichnungen	Nein	Tarif-abhängig	Nein	Nur manuell	Nur manuell	Nur manuell	E3 (nur manuell); E5 (manuell und regel-basiert)	E3 (nur manuell); E5 (manuell und regel-basiert)
Archivierung von E-Mails Microsoft-fremder Quellen	Nein	Nein	Nein	Nein	Nein	Nein	Nein[9]	Nein[10]
Plattform-unabhängigkeit	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein

Quelle: Osterman Research, 2023.

Grenzen der nativen Archivierung in Microsoft 365

Das E-Mail-„Archiv“ in Microsoft 365 hat verwirrenderweise genau dieselbe Bezeichnung wie es bei professionellen E-Mail-Archivierungslösungen von Drittanbietern der Fall ist. Doch es existieren beträchtliche Unterschiede zwischen beiden, die sich durch die Einschränkungen bei der nativen Archivierung in Microsoft 365 bemerkbar machen. Diese müssen den Unternehmen bewusst sein.

KEIN EIGENSTÄNDIGES ARCHIV

Die Archivierung erfolgt anhand von Aufbewahrungsrichtlinien. Die Daten befinden sich also zusammen mit allen anderen Microsoft 365-Daten im Microsoft-Mandanten. Probleme wie Ransomware, Kontoübernahmen, fehlerhafte Aufbewahrungsrichtlinien und Dienstausfälle betreffen somit also auch die E-Mail-Archive in Microsoft 365. Und auch der Wechsel zu einer anderen Lösung (wie Google Workspace) oder einem anderen Mandanten, wie er bei Firmenübernahmen und -fusionen immer wieder erforderlich ist, birgt enorme technische Herausforderungen. Denn es muss sichergestellt werden, dass alle aktuellen und archivierten Daten sowie die gesetzlichen Aufbewahrungsfristen übertragen werden, ohne die „Beweismittelkette“ zu verletzen.

Im Gegensatz dazu sind Archivierungslösungen von Drittanbietern nicht an Microsoft 365 gebunden und daher völlig unabhängig von Microsoft. Sie bieten Unternehmen damit die Flexibilität, jederzeit und ohne Folgen für das eigene Archiv auf eine andere E-Mail-Lösung umzusteigen. Ebenso können sie ohne großen technischen Aufwand, langwierige Geschäftsunterbrechungen oder Compliance- und Rechtsrisiken zu einem anderen Microsoft 365-Mandanten wechseln.

Externe Archivierungs-lösungen sind nicht an Microsoft 365 gebunden und daher völlig unabhängig.

KOMPLEXITÄT ERHÖHT DAS DATENRISIKO

Unabhängige E-Mail-Archivierungslösungen erfassen den kompletten Verlauf aller vom Unternehmen gesendeten und empfangenen E-Mails. Dies erfolgt normalerweise per Journaling, dem Mitschneiden des E-Mail-Verkehrs. Das Verfahren ist schon lange etabliert und erfordert nur eine einmalige Konfiguration. Das Archiv ist ein separater Aufbewahrungsort für E-Mails und erfüllt damit die geschäftlichen, juristischen und aufsichtsrechtlichen Anforderungen. Das Archiv ist von dem übrigen System, das die Mitarbeiter für den Versand und Empfang von E-Mails verwenden, komplett unabhängig.

Bei der nativen Archivierung in Microsoft 365 erfolgt kein Journaling. Da alles „an Ort und Stelle“ archiviert wird, ist ein koordinierter Ansatz notwendig, der ein oder mehrere Postfächer pro Benutzer, Aufbewahrungsrichtlinien und häufig auch die Verwaltung von Messaging-Datensätzen („Messaging Records Management“) umfasst. Um in Microsoft 365 das gleiche Ergebnis wie mit einem Journaling-basierten E-Mail-Archiv zu erzielen, müssen alle diese Methoden einheitlich und fehlerfrei angewendet werden. Und damit immer sämtliche E-Mails erfasst werden, wie dies beim Journaling der Fall ist, muss die Aufbewahrung für juristische Zwecke (= „full legal hold“) auf alle Benutzer dauerhaft angewendet werden. Damit ist das Verfahren jedoch äußerst schwerfällig.

AUFBEWAHRUNGSRICHTLINIEN SCHÜTZEN NICHT VOR ADMINISTRATORFEHLERN

Aufbewahrungsrichtlinien in Microsoft 365 sind der Schlüsselmechanismus, um sicherzustellen, dass E-Mails aufbewahrt und nicht gelöscht werden. Allerdings können sie auch versagen, da sie nicht vor Fehlern der IT-Administratoren gefeit sind. So empfiehlt Microsoft bei Mitarbeiterabgängen eine Änderung der Aufbewahrungsrichtlinien, damit deren Exchange-Postfach gelöscht und nicht nur deaktiviert werden kann. Doch auch dabei kann einiges schiefgehen. Einem Administrator bei KPMG ist beispielsweise bei der Aktualisierung einer Aufbewahrungsrichtlinie zu persönlichen Chats in Microsoft Teams (die im Exchange-Postfach des Benutzers gespeichert werden) ein Fehler unterlaufen. Dieser führte zur dauerhaften Löschung der Chatverläufe von 145.000 Benutzern. Da schon ein einfacher Fehler dazu führen kann, dass Daten, die eigentlich aufbewahrt werden sollen, dauerhaft gelöscht werden, besteht bei Microsoft 365 ein erhebliches Risiko versehentlich gegen Aufbewahrungspflichten zu verstoßen, da Microsoft darauf beharrt, dass kein separates Archiv erforderlich ist.

AUFBEWAHRUNGSRICHTLINIEN SCHÜTZEN NICHT VOR VORSÄTZLICH BÖSWILLIGEM VERHALTEN

Aufbewahrungsrichtlinien können zwar das unbeabsichtigte Löschen von Daten verhindern, schützen aber nicht vor Administratoren, die Daten absichtlich löschen oder Aufbewahrungsrichtlinien ändern – und erst recht nicht vor Hackern, die diese Richtlinien außer Kraft setzen wollen. Microsoft 365 unterstützt zwar Erhaltungssperren (Preservation Lock capability), die böswillige Akteure und Hacker daran hindern, Aufbewahrungsrichtlinien zu ändern oder zu deaktivieren. Diese können aber nicht rückgängig gemacht werden. Deshalb sollten zwei Dinge beachtet werden[10]:

- Ist der Speicher eines Benutzerkontos voll, muss zusätzlicher Speicherplatz erworben werden, da Daten, die einer Sperre unterliegen, nicht gelöscht werden können.
- Laut Datenschutzrichtlinien wie der DSGVO können betroffene Personen die Löschung ihrer Daten beantragen. Der Datenverantwortliche oder der Datenverarbeiter ist dann nicht mehr verpflichtet, diese Daten aufzubewahren, bzw. es gibt keine rechtliche Grundlage mehr für die Aufbewahrung der Daten. Die von der Datensperre betroffenen Daten können jedoch nicht gemäß der Datenschutzrichtlinie gelöscht werden. Dies führt unter Umständen zu einem Compliance-Verstoß.

Unternehmen erhöhen mit Microsoft 365 das Risiko von Verstößen. Denn Microsoft beharrt darauf, dass kein separates Archiv erforderlich ist.

AUFBEWAHRUNGSRICHTLINIEN KOSTEN SPEICHERPLATZ

Aufbewahrungsrichtlinien erhöhen den Speicherplatzverbrauch von Haupt- und Archivpostfach in Exchange Online. Dies führt zu einem erheblichen Anstieg des Speichervolumens im Vergleich zu den E-Mail-Archivierungslösungen anderer Anbieter.

Bei Microsofts Ansatz wird das Speichervolumen nicht benutzerübergreifend per „Single-Instance-Storage“ optimiert, wie dies bei vielen E-Mail-Archivierungslösungen anderer Anbieter der Fall ist. Unternehmen, die E-Mail-Archivierungslösungen von Drittanbietern verwenden, können den Gesamtspeicherbedarf auf dem E-Mail-Server reduzieren, indem sie Inhalte sicher in einem sekundären Archiv ablegen, Single-Instance-Storage verwenden und das Original vom E-Mail-Server löschen.

ÜBERWACHUNGSPROTOKOLLE WERDEN NUR VORÜBERGEHEND AUFBEWAHRT

In Microsoft 365 werden standardmäßig Überwachungsdatensätze (Audit Logs) zu Mailbox-Aktivitäten erstellt. Diese erfassen Ereignisse, z. B., wenn ein Benutzer eine Nachricht in seinem Postfach liest oder darauf zugreift, eine Nachricht löscht oder eine E-Mail aus seinem Postfach entfernt („endgültiges Löschen“, bei dem eine Nachricht dauerhaft gelöscht wird). Der Zugang zu den Überwachungsprotokollen ist in Microsoft 365 von entscheidender Bedeutung. Denn ohne Auditing könnten Benutzer Nachrichten löschen, um ihre Spuren zu verwischen.

Die Daten im Audit-Protokoll werden ohne E5-Lizenz (Office 365 oder Microsoft 365) jedoch nur maximal 90 Tage lang gespeichert und bei Benutzern, denen eine E5-Lizenz zugewiesen wurde, standardmäßig für ein Jahr.[11] Die Speicherdauer der Audit-Daten hängt von der Lizenz ab, die dem jeweiligen Benutzer zugewiesen wurde, ist also nicht im gesamten Unternehmen einheitlich. Mit anderen Worten: Um Audit-Daten ein Jahr oder länger aufzubewahren, müssen alle Benutzer eine teure E5-Lizenz oder Zusatzlizenz besitzen (oder eine gleichwertige für Bildungseinrichtungen bzw. Behörden). Doch selbst wenn die Audit-Daten ein Jahr lang gespeichert werden, sind sie längst weg, wenn erst drei Jahre später eine interne Untersuchung eingeleitet wird.

GRÖßERES SICHERHEITSRISIKO UND MEHR ANGRIFFSFLÄCHE

Microsoft bietet lizenzierten Benutzern von Microsoft 365 Postfächer mit 50 oder 100 GB sowie bis zu 1,5 TB zusätzlichen E-Mail-Speicher, wenn das primäre Postfach voll ist oder sich der Obergrenze nähert. Das sind riesige Datenmengen, die in den Postfächern problemlos zugänglich sind und mit den Anmeldedaten geöffnet werden können. Da so viele Unternehmen Microsoft 365 verwenden und derart viele Daten zugänglich sind, ist Microsoft 365 auch ein äußerst attraktives Ziel für Hacker. Es genügt, dass die Zugangsdaten per Phishing, Credential Stuffing oder auf anderem Wege kompromittiert werden. Und schon haben Hacker Zugang zu umfangreichen Daten im Postfach und den zugehörigen Archiven. Die Angriffsfläche ist also erheblich.

Da so viele Unternehmen Microsoft 365 verwenden und darin derart viele Daten zugänglich sind, ist Microsoft 365 ein äußerst attraktives Ziel für Hacker.

Mit E-Mail-Archivierungslösungen von Drittanbietern, die das komplette E-Mail-Archiv in einem sekundären System ablegen, kann die Größe des Postfachs dagegen verkleinert werden, was die negativen Folgen möglicher Datenlecks entschärft.

SCHUTZ VOR VERSEHENTLICHER UND ABSICHTLICHER LÖSCHUNG

Microsoft 365 bietet die Möglichkeit, versehentlich oder absichtlich gelöschte Inhalte in den Haupt- und Archivpostfächern wiederherzustellen, wobei es dafür nur ein bestimmtes Zeitfenster gibt. Inhalte, die vom Benutzer gelöscht werden, werden in den Papierkorb („Gelöscht“-Ordner) verschoben und sind dort standardmäßig 30 Tage lang verfügbar. Wird dieser nicht geleert, lässt sich sein Inhalt ganz einfach wiederherstellen, indem man ihn auf den Desktop oder in einen anderen Ordner verschiebt. Und auch gelöschte Inhalte, die älter als 30 Tage sind, können noch 14 weitere Tage aus dem „Gelöscht“-Ordner wiederhergestellt werden. Unbeabsichtigt gelöschte Inhalte sind also standardmäßig noch 44 Tage lange erreichbar.[12] Da das „Archiv“ in Microsoft 365 nur als Speicherplatz dient (sofern keine Aufbewahrungsrichtlinien aufgestellt werden), können E-Mails daraus nach Belieben gelöscht werden.

Es gibt einige wichtige Einschränkungen, was den Schutz vor unbeabsichtigtem Löschen betrifft:

- Sobald ein Benutzer seinen Papierkorb oder den Ordner „Gelöschte Elemente“ leert, können die Inhalte nicht wiederhergestellt werden.
- Inhalte können nur für den ursprünglichen Benutzer wiederhergestellt werden. Für andere Benutzer sind sie nicht zugänglich, es sei denn, sie werden wiederhergestellt und anschließend an einen anderen Benutzer übertragen.
- Der Papierkorb ist Teil des Speicherkontingents jedes Benutzers.

Wenn Unternehmen die E-Mail-Archivierung von Microsoft nutzen und einen richtlinienbasierten Schutz vor versehentlichem und absichtlichem Löschen wollen, müssen sie Aufbewahrungsrichtlinien oder das Beweissicherungsverfahren (auch Aufbewahrung für juristische Zwecke oder Litigation Hold) verwenden. Die Konfiguration von Aufbewahrungsrichtlinien und Aufbewahrungsbezeichnungen ist aufwändig und kompliziert und muss frühzeitig durchgeführt werden, damit wirklich alle E-Mails erfasst und aufbewahrt werden.[13]Zusätzlich kann die Aufbewahrung für juristische Zwecke aktiviert werden. Diese hat Vorrang vor den Aufbewahrungsrichtlinien.[14] Damit können Daten jedoch nicht rückwirkend erfasst werden, und es werden keine Daten geschützt, die vor Aktivierung geändert oder gelöscht wurden.

LAUT CLOUD ACT HAT DIE US-REGIERUNG ZUGRIFF AUF SÄMTLICHE BENUTZERDATEN – AUCH IN EUROPA

Der U.S. CLOUD Act von 2018 ermöglicht es den Vereinigten Staaten, auf alle Daten zuzugreifen, die weltweit auf Servern von US-Unternehmen gespeichert sind. Dazu gehören auch Microsoft 365-Daten von Unternehmen, die überhaupt nicht in den Vereinigten Staaten tätig sind – und sogar Daten über Benutzer, die keine amerikanische Staatsbürgerschaft haben.

Die europäischen Behörden sind davon natürlich nicht begeistert. Denn der CLOUD Act steht im Widerspruch zu den Bestimmungen der DSGVO. Bei Unternehmen, die Microsoft 365 weiterhin für Kommunikation und Zusammenarbeit nutzen möchten, führt die Vor-Ort-Archivierung zu einem ständig wachsenden Bestand an E-Mail-Daten, die dem CLOUD Act unterliegen. Wenn sich die Daten in Microsoft 365 befinden, so verfügen die US-Regierung und ihre Behörden über Mechanismen, um Zugang darauf zu erhalten.

Der U.S. CLOUD Act sieht allerdings keinen Zugang zu Datensystemen vor, die von außeramerikanischen Unternehmen erstellt wurden. Die Daten in den E-Mail-Archivierungslösungen europäischer Unternehmen beispielsweise sind also vor dem Zugriff der USA sicher.

Die deutschen Datenschutz-behörden sehen in Microsoft 365 nach wie vor mehrere erhebliche Verstöße gegen die DSGVO.

GROßE ZWEIFEL AN DER DSGVO-KONFORMITÄT VON MICROSOFT 365

Stand Anfang 2023 sehen die deutschen Datenschutzbehörden bei Microsoft 365 weiterhin erhebliche Mängel im Hinblick auf die DSGVO. Dabei stützen sie sich auf eine zwei Jahre dauernde Untersuchung zu mehreren Datenschutzproblemen.[15] Ein Ergebnis war das Verbot von Microsoft 365 für Bildungseinrichtungen in Deutschland[16]. Außerdem wurden Bedenken hinsichtlich seiner Verwendung im öffentlichen Sektor generell laut. Die deutschen Datenschutzbehörden kamen zu dem Schluss, dass die mangelnde Transparenz hinsichtlich der Verarbeitung personenbezogener Daten durch Microsoft für dessen eigene Zwecke bedeutet, dass Microsoft 365 nicht der DSGVO entspricht – selbst nach Veröffentlichung des Datenschutzzusatzes von Microsoft im September 2022.[17] Microsoft ist mit dieser

Darstellung natürlich nicht einverstanden, und die Differenzen zwischen den beiden Parteien bleiben ungelöst.[18]

Unternehmen, die der DSGVO unterliegen und Microsoft 365 für die langfristige Speicherung von E-Mail-Archiven nutzen, müssen sich also darüber im Klaren sein, dass Stand Anfang 2023 noch erhebliche Streitpunkte zwischen den europäischen Datenschutzbehörden und Microsoft bezüglich der Einhaltung der DSGVO gibt. Wenn Microsoft 365 weiterhin gegen die Vorschriften verstößt, könnten Organisationen in Europa, die der DSGVO unterliegen, daher gezwungen sein, andere E-Mail-, Kollaborations- und Produktivitätstools zu nutzen. Dieses mögliche Szenario verdeutlicht das Risiko der Nutzung von E-Mail-Archivierungsfunktionen und Aufbewahrungsrichtlinien in Microsoft 365 im Vergleich zur Verwendung einer Drittanbieterlösung. Letztere ermöglichen eine langfristige Speicherung und Verarbeitung der E-Mail-Daten, die von vornherein DSGVO-konform ist, sowie die Migration zu anderen E-Mail-Lösungen, falls diese zur Einhaltung der DSGVO erforderlich sein sollte.

UNGEWISSHEIT BEIM DATENAUFBEWAHRUNGSORT

Unternehmen, die Archivierungslösungen von Drittanbietern verwenden, haben absolute Gewissheit darüber, wo ihre Daten gespeichert werden. Da sie die volle Kontrolle über die Standorte von Servern und Rechenzentren, die Auswahl der Dienstleister mit Garantien zur Datenaufbewahrung und den Standort der Backup-Dateien haben, können sie sich darauf verlassen, dass ihre internen Richtlinien und die externen Vorschriften zur Datenaufbewahrung eingehalten werden.

Bei Microsoft 365 ist das nicht so einfach. Unternehmen, die Microsoft 365 verwenden, erhalten lediglich Zusicherungen, wo ihre Daten gespeichert werden – doch die bedeuten keineswegs absolute Gewissheit. Die Frage, wie sich Microsoft 365 hinsichtlich der Datenaufbewahrung verhält, ist vielschichtig und berührt die folgenden Gesichtspunkte:

- **Nur ein Mandant**
  Seit den Anfängen von Microsoft 365 war die Mandanten-Architektur so konzipiert, dass jedes Unternehmen nur einen regional festgelegten Mandanten verwendet, zu dem der gesamte Datenverkehr von außerhalb der Region geleitet wird. Dieses Design eignet sich optimal für Unternehmen, die nur in einer bestimmten Region, der Region des Mandanten, aktiv sind. Für multinationale, überregionale Organisationen kann es jedoch erhebliche Herausforderungen bezüglich Datenhoheit und Datenresidenz mit sich bringen. Der Mandanten-Standort des Unternehmens wird bei der Erstregistrierung für Microsoft 365 festgelegt. Dennoch werden einige Inhaltstypen in Microsoft 365 bisher ausschließlich aus der Region Nordamerika heraus bedient – ungeachtet des Unternehmensstandorts. Dies ändert sich jedoch allmählich für die meisten (aber nicht alle) Datentypen.

Microsoft ergänzt Microsoft 365 laufend um weitere Optionen, um das Problem des Datenauf-bewahrungsorts zu lösen, obwohl immer wiederbehauptet wird, dass alle Probleme zuvor gelöst worden seien.

- **Multi-Geo erlaubt Mandanten-Splitting in logische Regionen**
  Mit dem Add-on Multi-Geo können Organisationen mit Benutzern in mehreren geografischen Regionen ihren Mandanten auf mehrere logische Regionen aufteilen – eine Hauptregion und eine oder mehrere Nebenregionen. Benutzer können einer solchen Nebenregion zugewiesen werden, in der sich dann auch ihr Haupt- und Archivpostfach befindet[19] – neben Daten für andere Microsoft 365-Workloads, die aber nicht Thema des vorliegenden Whitepapers sind. Multi-Geo ist vor allem für größere und komplexere Organisationen gedacht und mit einer zusätzlichen benutzerabhängigen Gebühr verbunden. Multi-Geo wurde erst durch den Aufbau lokaler Microsoft-Rechenzentren in Ländern wie Deutschland ermöglicht.[20]
- **Erweiterte Datenresidenz für den Betrieb von Workloads und die Speicherung von Daten an speziell definierten Orten**
  Das Add-on „Erweiterte Datenresidenz (Advanced Data Residency) für Unternehmenskunden von Microsoft 365 wurde entwickelt, um die Anforderungen an die Datenresidenz zu erfüllen.[21] Es stellt sicher, dass Workloads in Microsoft 365 an ganz bestimmten Standorten ausgeführt werden und dort auch die Kundendaten gespeichert werden. Für das Add-on fällt eine zusätzliche Gebühr je Benutzer für alle lizenzierten Benutzer an (also alle lizenzierten Benutzer des Mandanten). Advanced Data Residency wurde erstmals im November 2022 veröffentlicht[22] und ist damit noch relativ neu. Es bleibt also abzuwarten, wie sich die kommenden Versionen entwickeln.
- **EU-Datengrenze für die Microsoft-Cloud**
  Microsofts jüngste Verpflichtung zur Datenaufbewahrung in Europa wird als EU-Datengrenze (*EU Data Boundary*) bezeichnet und gilt für Azure, Microsoft 365 und Dynamics 365.[23] Dabei handelt es sich um eine Verpflichtung, mehr personenbezogene Daten in Europa zu speichern und zu verarbeiten und die Datenübermittlung in die Vereinigten Staaten zu begrenzen.

Es ist noch nicht abzusehen, inwieweit diese neuen Ansätze das Problem der Datenresidenz lösen können. Denn mit jedem neuen Add-on wiederholt Microsoft seine Behauptung, das Thema damit gelöst zu haben, und stellt damit den Wahrheitsgehalt seiner früheren Behauptungen in Frage.

MANGELNDE RECHTSSICHERHEIT BEI DER DATENÜBERTRAGUNG ZWISCHEN DER EU UND DEN USA

Zwei frühere Rahmenübereinkommen zur Übermittlung von Daten zwischen der Europäischen Union und den Vereinigten Staaten sind vom Gerichtshof der Europäischen Union (EuGH) kassiert worden:

- **Im Oktober 2015 wird Safe Harbor für ungültig erklärt**
  Das Safe-Harbor-Rahmenwerk ermöglichte den Austausch personenbezogener Daten zwischen der Europäischen Union und den Vereinigten Staaten zu kommerziellen Zwecken. Doch nach den Enthüllungen über das heimliche Abgreifen dieser Daten durch die amerikanische National Security Agency (NSA) und andere Stellen wurde es im Oktober 2015 vom EuGH für ungültig erklärt.
- **Im Juli 2020 wird Privacy Shield gekippt**
  Nachdem die US-Datenschutzgesetze von europäischen Datenschützern bemängelt worden waren, weil sie nicht dasselbe Schutzniveau wie die in der EU bieten und die Anforderungen der DSGVO nicht erfüllen, kippte der EuGH im Juli 2020 auch das überarbeitete Privacy Shield. Die Aufhebung hatte weitreichende Folgen, da rund 5.000 US-Unternehmen und 250 Unternehmen

2023 soll das neue Datenschutz-abkommen zwischen der EU und den USA ratifiziert werden. Noch bleibt abzuwarten, ob und wie es von europäischen Datenschützern angefochten wird.

aus Europa an das Abkommen gebunden waren.[24] Kunden, die personenbezogene Daten von EU-Bürgern in die USA übermitteln möchten, können dies gemäß Privacy Shield nicht mehr tun und müssen sich stattdessen Alternativen suchen. Eine Datenübertragung in die USA ist zwar weiterhin möglich, allerdings potenziell aufwändiger, langsamer und teurer.

Eine Alternative zum Privacy Shield sind die Standardvertragsklauseln (*Standard Contractual Clauses*, SCC), die allerdings auch kein Allheilmittel sind. Sie sind problematisch, da der EuGH die Datenschutzbehörden in der Europäischen Union dazu verpflichtet hat, entsprechende Datentransfers genauer zu prüfen und gegebenenfalls zu verhindern. Eine weitere Alternative sind die *Binding Corporate Rules*, die allerdings schwer umzusetzen sind und daher für kleinere Unternehmen eine unzumutbare Belastung darstellen. Ohne Privacy Shield müssen Unternehmen also mit den riskanten Standardvertragsklauseln vorliebnehmen oder andere Wege der Datenübertragung finden.

Dass 2023 eine juristische Lösung gefunden wird, ist immer wahrscheinlicher.[25] Das neue Datenschutzabkommen zwischen der EU und den USA (mit der ursprünglichen Bezeichnung *Trans-Atlantic Data Privacy Framework*) wurde im März 2022 angekündigt.[26] Nach einem Erlass von US-Präsident Joe Biden im Oktober 2022, in dem er sich zu etlichen wichtigen Schutzmaßnahmen verpflichtete, um der Nichtigerklärung des Privacy Shield zu begegnen,[27] entschied die Europäische Kommission im Dezember 2022, dass das neue Rahmenübereinkommen die europäischen Anforderungen erfüllt.[28] Es handelt sich jedoch lediglich um einen Beschlussentwurf, da mehrere EU-Gremien den Rahmen erst noch ratifizieren müssen, damit er endgültig angenommen werden kann. Noch bleibt also abzuwarten, ob und wie er von den europäischen Datenschützern angefochten wird.

Zusammenfassend lässt sich sagen, dass die Fragen hinsichtlich Datenresidenz und Datentransfer bei Microsoft 365 komplex und ständigen Veränderungen unterworfen sind und diverse gewinnorientierte, staatliche und regulatorische Akteure um ihre Position ringen. Es bleibt abzuwarten, wie lange es noch dauert, bis ein Konzept zu Datenaufbewahrung und Datenübermittlung gefunden wird, das für alle Beteiligten funktioniert – falls dies überhaupt jemals der Fall sein wird. Unternehmen, die kurzfristig Sicherheit brauchen, sollten bei der Einführung von Microsoft 365 daher äußerst vorsichtig sein.

Empfehlungen und Ausblick

Osterman Research empfiehlt Entscheidern in kleinen und mittelständischen Unternehmen einige Schritte, mit denen sie ihren E-Mail-Archivierungsbedarf ermitteln und eine geeignete Lösung finden können.

SCHRITT 1: ANLASS UND ZWECK DER E-MAIL-ARCHIVIERUNG KLÄREN

Ermitteln Sie, warum die E-Mail-Archivierung für Ihr Unternehmen wichtig ist. IT-Manager und andere Personen, die über die E-Mail-Archivierung und Microsoft 365 zu entscheiden haben, sollten sich mit ihrer Rechts-, Compliance- und/oder Datenschutzabteilung beraten, um die Rechts-, Compliance- und Geschäftsanforderungen zu klären, die es jenseits der IT-Belange zu beachten gilt. Dabei dürften die folgenden Aspekte eine Rolle spielen:

- **Archivierungsbedarf ermitteln**
  Viele Unternehmen sind sich nicht bewusst, wie wichtig die Archivierung von E-Mails und Anhängen tatsächlich ist. Und das gilt keineswegs nur für KMU. Denn auch in vielen großen Unternehmen werden E-Mails und Anhänge nicht archiviert. Doch wie in diesem Whitepaper erläutert wurde, können Unternehmen so ihre gesetzlichen, regulatorischen und sonstigen Pflichten in Bezug auf die Auffindbarkeit und Bereitstellung von Daten nicht ausreichend erfüllen. Die Folge können Geldbußen, weitere Strafmaßnahmen, Rufschädigungen und eine Reihe weiterer gravierender Konsequenzen sein, die fast immer kostspieliger sind als eine Archivierung.
- **DSGVO-Risikotoleranz bestimmen**
  Die deutschen Datenschutzbehörden stellen die Einhaltung der DSGVO durch Microsoft 365 weiterhin in Frage. Daher sind weitere Verhandlungen zwischen den deutschen und europäischen Datenschutzbehörden und Microsoft zu erwarten. Sie sollten sich also fragen, ob Sie diese Ungewissheit ertragen können oder lieber schnelle Gewissheit wollen. Erhebliche Probleme bestehen noch bei den Themen undeklarierte Datenverarbeitung, Datenaufbewahrungsort und Datentransfers in Drittstaaten.

Wozu dient die E-Mail-Archivierung in Ihrem Unternehmen?

SCHRITT 2: ANFORDERUNGEN AN DIE E-MAIL-ARCHIVIERUNG AUFSTELLEN

E-Mail-Archivierungslösungen müssen etliche Kriterien erfüllen. Dazu gehören:

- **Echtheit und Unveränderbarkeit der E-Mails**
  Eine geeignete E-Mail-Archivierungslösung ermöglicht es, authentische, vor Veränderungen geschützte Kopien aller E-Mails aufzubewahren und so die rechtlichen und behördlichen Auflagen und die Branchenanforderungen zu erfüllen. Das bedeutet zum Beispiel, dass es keine Lücken im Datensatz gibt, damit man sich ein vollständiges Bild von der Geschäftstätigkeit machen kann. Mitarbeiter, die Zugriff auf ihre alten E-Mails im Archiv haben, müssen keine Zeit damit verschwenden, Inhalte nachzubilden – was die Produktivität beeinträchtigen würde.
- **Eigenständige Kopien an einem separaten Speicherort**
  Die „3-2-1-Regel“ besagt, dass Unternehmen drei Kopien ihrer Daten aufbewahren sollten: zwei davon lokal und eine von dem System getrennt, auf dem die Daten erstellt und gespeichert werden. So kann beispielsweise eine Kopie der E-Mails und Anhänge auf dem E-Mail-Server liegen und eine zweite in Backup- und Archivierungslösungen gespeichert werden. Die Backups und

archivierten Inhalte werden wiederum gesondert (vor Ort oder in der Cloud) abgelegt. Lösungen wie Microsoft 365, die die Plattform selbst für die Datenspeicherung nutzen, erfüllen diese Regel also nicht.

- **Self-Service-Archivzugriff**
  Endbenutzern die Möglichkeit zu geben, ihre E-Mails selbst mit minimalem Aufwand im Archiv zu suchen, entlastet die IT-Mitarbeiter. Das macht die Mitarbeiter effizienter, weil sie schneller auf ihre E-Mails und Dateien zugreifen können. Davon profitieren sowohl die IT als auch die Mitarbeiter, denn es wird sichergestellt, dass Informationen mit minimalem Aufwand möglichst leicht zugänglich sind.
- **Zukunftssicherheit und Übertragbarkeit**
  Eine E-Mail-Archivierung sollte so gewählt werden, dass das Unternehmen nicht an eine bestimmte E-Mail-Plattform gebunden ist. Archivierungslösungen, die von der E-Mail-Plattform unabhängig sind, ermöglichen es einem Unternehmen, bei Marktveränderungen – und nach Fusionen und Übernahmen – komplikationslos auf andere Plattformen umzusteigen und bei Bedarf ihre Archivierungslösung zu wechseln. Und das ist wichtig, um die Flexibilität zu gewährleisten.
- **Ein Archiv, viele Plattformen**
  Unternehmen, die mehrere E-Mail-Plattformen wie Microsoft 365, Google Workspace und lokale E-Mail-Server (wie MDaemon oder IceWarp) nutzen, müssen E-Mails aus sämtlichen Plattformen archivieren. Nutzt man dafür die nativen Funktionen dieser Plattformen, entstehen Datensilos, die im Laufe der Zeit immer schwieriger zu verwalten, zu pflegen und zu durchsuchen sind. Mit einer einheitlichen E-Mail-Archivierungslösung, die alle Plattformen unterstützt, werden separate, unzusammenhängende Lösungen überflüssig. Noch wichtiger ist, dass ein einheitlicher Ansatz den IT-Verwaltungsaufwand erheblich reduziert und die juristischen, behördlichen und eDiscovery-Prozesse für die Suche und Erstellung von Informationen vereinfacht.
- **Berücksichtigung der Datenschutzbestimmungen**
  Unabhängige E-Mail-Archivierungslösungen berücksichtigen die geltenden Datenschutzbestimmungen und deren Anforderungen. E-Mail-Archivierungslösungen, die in der EU von europäischen Anbietern entwickelt werden, sind dabei von Haus aus besser auf die DSGVO abgestimmt, da es keinen Konflikt zwischen Datenschutzbestimmungen gibt, wie dies bei Anbietern aus den Vereinigten Staaten oft der Fall ist. Da Anbieter aus anderen Ländern gerade erst damit beginnen, die DSGVO und die Datenschutzbestimmungen in ihren Heimatländern zu berücksichtigen, sind die europäischen Anbieter klar im Vorteil.

E-Mail-Archivierungs-lösungen, die in der EU von europäischen Anbietern entwickelt werden, sind von Haus aus besser auf die DSGVO abgestimmt, da sie nur diese berücksichtigen müssen.

SCHRITT 3: VORTEILE VON DRITTANBIETERN PRÜFEN

E-Mail-Archivierungslösungen von Drittanbietern haben gegenüber den nativen Angeboten von Microsoft 365 mehrere Vorteile. Dazu gehören:

- **Unabhängiges Archiv**
  E-Mail-Archivierungslösungen von Drittanbietern haben den Vorteil, dass das Archiv unabhängig von der genutzten E-Mail-Plattform ist und die 3-2-1-Regel erfüllt. Das ist besonders bei der Nutzung eines Cloudservice wie Microsoft 365 wichtig, da sich der E-Mail-Dienst und die E-Mail-Archive sowie Backups keine Infrastruktur teilen sollten.

- **Mehrere Plattformen, ein Archiv**
  Archivierungslösungen von Drittanbietern haben den Vorteil, dass auch die Inhalte von Microsoft-fremden E-Mail-Plattformen in einem gemeinsamen Archiv abgelegt werden können. Wenn mehrere Archivierungslösungen verwaltet werden müssen, erhöht das die Kosten und die Komplexität für die Aufbewahrung von Geschäftsaufzeichnungen. Die Verwendung eines zentralen Archivs reduziert die Anzahl an Lösungen, die von der IT verwaltet und von Benutzern durchsucht werden müssen.
- **Gemeinsames E-Mail-Archiv und Gruppenzugriff auf Archivinhalte**
  E-Mail-Archivierungslösungen von Drittanbietern unterstützen auch neue Anwendungsfälle für den Zugriff auf E-Mail-Inhalte, wie z. B. den gemeinsamen und gruppenweisen Zugriff auf die E-Mail-Archive – vorbehaltlich der Anforderungen an Datenschutz und Datensicherheit. Microsoft 365 kann da nicht mithalten, da Exchange Online Archivierung (EOA) nur für einzelne Benutzer konzipiert ist.[29]
- **Bessere Indizierung**
  E-Mail-Archivierungslösungen von Drittanbietern bieten häufig die Möglichkeit, mehr Dateitypen zu indizieren, was Suche und Abruf erleichtert.
- **Löschschutz**
  E-Mail-Archivierungslösungen von Drittanbietern verhindern, dass Benutzer Inhalte aus ihrem eigenen Archiv löschen können. Und da es sich um eine Standardeinstellung handelt, ist kein zusätzlicher Konfigurationsaufwand erforderlich.
- **Deduplizierung zur Speicher- und Suchoptimierung**
  Viele Archivierungslösungen von Drittanbietern ermöglichen eine Deduplizierung, die den Speicherbedarf erheblich reduziert und die Inhaltssuche beschleunigt.

SCHRITT 4: DETAILLIERTE KOSTENANALYSE

Führen Sie eine gründliche Kostenanalyse durch, um die Differenz zwischen Microsoft 365 und den Archivierungslösungen anderer Anbieter zu ermitteln. Das sollten Sie dabei berücksichtigen:

- **Verwaltungs- und Konfigurationsaufwand**
  Wenn eine E-Mail-Archivierungslösung eines Drittanbieters gewählt wird, sind Konfiguration und Verwaltung erforderlich. Wird dagegen Microsoft 365 verwendet, kommt es auf die richtige Mischung aus Aufbewahrungsrichtlinien und/oder *Litigation Holds* zur Aufbewahrung der Daten für rechtliche Zwecke an. Es ist wahrscheinlich, dass der jährliche Zeit- und Kostenaufwand für die Verwaltung der E-Mail-Archivierungslösung geringer ist als bei der Microsoft 365-Alternative.
- **Der richtige Tarifmix**
  Exchange Online Archivierung ist nur in den teuersten Tarifen für Office 365 und Microsoft 365 Enterprise enthalten, die zudem für sämtliche Benutzer abgeschlossen werden müssen. Bei Archivierungslösungen von Drittanbietern können Unternehmen dagegen für einige Benutzer günstigere Tarife abschließen und so die Gesamtbetriebskosten sowohl für Microsoft 365 als auch für Kommunikation und Kollaboration insgesamt senken.

Mit Archivierungslösungen von Drittanbietern können Unternehmen günstigere Microsoft 365-Abos abschließen und so ihre Gesamtbetriebskosten senken.

- **Zusatzkosten für Add-ons zur Datenresidenz**
  Für Microsoft 365 gibt es mehrere Add-ons, die den Datenspeicherort sicherstellen. Wenn Ihr Unternehmen strenge Anforderungen an die Datenaufbewahrung erfüllen muss, sollten Sie also die zusätzlichen Kosten für diese Add-ons berücksichtigen.

Die parallele Nutzung von E-Mail-Archivierungslösungen von Drittanbietern und Office 365 erschwert unter Umständen das Lösungs- und Lizenzmanagement in der IT. Die Kostenvorteile wiegen die zusätzliche Komplexität jedoch fast immer auf.

Zusammenfassung

Microsoft 365 ist eine zuverlässige und vielseitige Plattform für E-Mail, Produktivität und Zusammenarbeit. Sie birgt jedoch zahlreiche Einschränkungen in Bezug auf die E-Mail-Archivierung, die Entscheidungsträger in KMU berücksichtigen müssen. Entscheidungsträger, die sich dessen nicht bewusst sind, setzen sich unnötigen Risiken aus. Die Nutzung von E-Mail-Archivierungslösungen von Drittanbietern beseitigt diese Risiken und sollte daher ernsthaft in Betracht gezogen werden.

MailStore

MailStore ist ein Unternehmen von OpenText und hat sich auf die Entwicklung innovativer E-Mail-Archivierungslösungen für kleine und mittelständische Unternehmen spezialisiert. Mit zehntausenden Unternehmenskunden in über 100 Ländern ist MailStore einer der weltweit führenden Anbieter auf diesem Gebiet. Die Produkte und Lösungen des Unternehmens werden von kleinen und mittelständischen Unternehmen aus allen Branchen sowie von staatlichen Stellen und Bildungseinrichtungen genutzt. Zudem nutzen Millionen von privaten Benutzern die kostenlose Software MailStore Home.

MailStore hat sich zum Ziel gesetzt, seine Kunden mit führenden Technologien dabei zu unterstützen, E-Mails – eine der wichtigsten Informationsressourcen unserer Zeit – effizient und nachhaltig zu nutzen und die zunehmenden Compliance-Anforderungen zu erfüllen.

www.mailstore.com

sales@mailstore.com

+49 (0) 2162 502990

+1 800 747 2915 (USA)

[1] Microsoft: *Microsoft FY22 Third Quarter Earnings Conference Call*, April 2022. Online verfügbar unter: https://view.officeapps.live.com/op/view.aspx?src=https://c.s-microsoft.com/en-us/CMSFiles/TranscriptFY22Q3.docx?version=52d815b6-1a9f-0c49-d0ab-5cd077ae469d

[2] Microsoft Learn: *Exchange Online limits,* Dezember 2022. Online verfügbar unter: https://learn.microsoft.com/en-us/office365/servicedescriptions/exchange-online-service-description/exchange-online-limits#mailbox-storage-limits

[3] Microsoft Learn: *Outlook performance issues in a Cached Exchange Mode .ost or .pst file,* September 2022. Online verfügbar unter: https://learn.microsoft.com/en-US/outlook/troubleshoot/performance/performance-issues-if-too-many-items-or-folders

[4] Microsoft Learn: *You may experience application pauses if you have a large Outlook data file,* März 2022. Online verfügbar unter: https://learn.microsoft.com/en-US/outlook/troubleshoot/performance/application-pauses-if-you-have-large-data-file

[5] Microsoft Support: *Archive in Outlook for Windows,* Dezember 2022. Online verfügbar unter: https://support.microsoft.com/en-us/office/archive-in-outlook-for-windows-25f75777-3cdc-4c77-9783-5929c7b47028

[6] Microsoft Learn: *Learn about archive mailboxes,* Oktober 2022. Online verfügbar unter: https://learn.microsoft.com/en-us/microsoft-365/compliance/archive-mailboxes?view=o365-worldwide

[7] Microsoft Learn: *Learn about auto-expanding archiving,* Dezember 2022. Online verfügbar unter: https://learn.microsoft.com/en-us/microsoft-365/compliance/autoexpanding-archiving?view=o365-worldwide

[8] Microsoft Learn: *Enable archive mailboxes for Microsoft 365,* November 2022. Online verfügbar unter: https://learn.microsoft.com/en-us/microsoft-365/compliance/enable-archive-mailboxes?view=o365-worldwide

[9] Mithilfe externer Datenkonnektoren können Inhalte E-Mail-fremder Quellen archiviert werden

[10] Microsoft Learn: *Data immutability in Microsoft 365,* September 2022. Online verfügbar unter: https://learn.microsoft.com/en-us/compliance/assurance/assurance-data-immutability?view=o365-worldwide

[11] Microsoft Learn: *Search the audit log in the compliance portal,* September 2022. Online verfügbar unter: https://learn.microsoft.com/en-au/microsoft-365/compliance/audit-log-search?view=o365-worldwide

[12] Microsoft Learn: *Recoverable Items Folder in Exchange Online,* Juni 2022. Online verfügbar unter: https://learn.microsoft.com/en-us/exchange/security-and-compliance/recoverable-items-folder/recoverable-items-folder

[13] Microsoft Learn: *Learn about retention policies and retention labels,* Dezember 2022. Online verfügbar unter: https://learn.microsoft.com/en-us/microsoft-365/compliance/retention?view=o365-worldwide

[14] Microsoft Learn: *Create a Litigation Hold,* Dezember 2022. Online verfügbar unter: https://learn.microsoft.com/en-us/microsoft-365/compliance/ediscovery-create-a-litigation-hold?view=o365-worldwide

[15] Natasha Loma: *Microsoft 365 faces darkening GDPR compliance clouds after German report,* November 2022. Online verfügbar unter: https://techcrunch.com/2022/11/28/microsoft-365-faces-darkening-gdpr-compliance-clouds-after-german-report/

[16] Vuk Mujovic: *Germany Forces a Microsoft 365 Ban Due to Privacy Concerns,* September 2022. Online verfügbar unter: https://techgenix.com/microsoft-365-ban-in-germany/

[17] DSK: *Festlegung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder,* November 2022. Online verfügbar unter: https://datenschutzkonferenz-online.de/media/dskb/2022_24_11_festlegung_MS365.pdf

[18] Microsoft: *Our Continued Commitment to Meet and Exceed EU Data Privacy Laws*, November 2022. Online verfügbar unter: https://news.microsoft.com/wp-content/uploads/prod/sites/40/2022/11/DSK-Blog-Post_25NOV2022_ENG_FINAL.pdf

[19] Microsoft Learn: *Data Residency for Exchange Online*, November 2022. Online verfügbar unter: https://learn.microsoft.com/en-us/microsoft-365/enterprise/m365-dr-workload-exo?source=recommendations&view=o365-worldwide

[20] Paul Lorimer: *Microsoft Office 365 and Dynamics 365 now available from new German datacenter regions*, Februar 2020. Online verfügbar unter: https://www.microsoft.com/en-us/microsoft-365/blog/2020/02/20/microsoft-office-365-dynamics-365-now-available-from-new-german-datacenter-regions/

[21] Microsoft Learn: *Advanced Data Residency in Microsoft 365*, November 2022. Online verfügbar unter: https://learn.microsoft.com/en-us/microsoft-365/enterprise/advanced-data-residency?view=o365-worldwide

[22] Paul Lorimer: *Microsoft 365 expands data residency commitments and capabilities*, Oktober 2022. Online verfügbar unter: https://www.microsoft.com/en-us/microsoft-365/blog/2022/10/20/microsoft-365-expands-data-residency-commitments-and-capabilities/

[23] Microsoft: *The EU Data Boundary for the Microsoft Cloud*, Dezember 2022. Online verfügbar unter: https://www.microsoft.com/en-us/trust-center/privacy/european-data-boundary-eudb

[24] Dan Swinhoe: *EU court invalidates Privacy Shield data transfer agreement*, Juli 2020. Online verfügbar unter: https://www.csoonline.com/article/3567061/eu-court-invalidates-privacy-shield-data-transfer-agreement.html

[25] Natasha Lomas: *EU confirms draft decision on replacement US data transfer pact*, Dezember 2022. Online verfügbar unter: https://techcrunch.com/2022/12/13/eu-us-data-privacy-framework-draft-decision/

[26] The White House: *United States and European Commission Announce Trans-Atlantic Data Privacy Framework*, März 2022. Online verfügbar unter: https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework/

[27] The White House: *President Biden Signs Executive Order to Implement the European Union-U.S.* Data Privacy Framework, Oktober 2022. Online verfügbar unter: https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/fact-sheet-president-biden-signs-executive-order-to-implement-the-european-union-u-s-data-privacy-framework/

[28] Europäische Kommission: *COMMISSION IMPLEMENTING DECISION of XXX pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework*, Dezember 2022. Online verfügbar unter: https://commission.europa.eu/system/files/2022-12/Draft%20adequacy%20decision%20on%20EU-US%20Data%20Privacy%20Framework_0.pdf

[29] Microsoft Learn: *Exchange Online Archiving service description*, Dezember 2022. Online verfügbar unter: https://learn.microsoft.com/en-us/office365/servicedescriptions/exchange-online-archiving-service-description/exchange-online-archiving-service-description