|  |  |
| --- | --- |
| Version: | 1.0 |
| Status: | Freigegeben |
| Dokumentenklassifizierung: | intern |

Sicherheitsrichtlinie "Microsoft Exchange und Outlook"

1. Januar 2020

Allgemeine Informationen zum vorliegenden Dokument

|  |  |  |
| --- | --- | --- |
| Bezeichnung | Inhalt | Bearbeitungshinweis |
| Eigentümer |  | [verantwortlich für die Erstellung und Pflege des Dokuments = Abteilungsleitung] |
| Autor |  | [operative Verantwortung für das Dokument] |
| Status | Freigegeben | [Einstufung des aktuellen Dokumentenstatus <Entwurf, Finaler Entwurf, Final/Freigegeben>] |
| Klassifizierung | intern | [Einstufung der Dokumentenvertraulichkeitoffen, intern, vertraulich, streng vertraulich] |
| Dokumen­tenkennung | ISMS300056 | [Die Dokumenten-Kennung wird von der Dokumentenlenkung vergeben] |
| Name des Dokuments | Sicherheitsrichtlinie "Microsoft Exchange und Outlook" | [Bezeichnung des Dokuments wie auf dem Titelblatt beschrieben.] |
| Version  | 1.0 | [zweistellige Versionsnummer] |
| Veröffentlichungsform | digital | [Veröffentlichungsform Papier, digital] |
| Speicherort |  | [Ablageort des Dokumentes] |
| Freigabe am | <TT.MM.YYYY> | [Datum der Freigabe durch den Eigentümer] |
| Freigabe bis | <TT.MM.YYYY> | [Datum der Freigabe bis durch den Eigentümer] |
| Revisionszyklus | Alle zwei Jahre | [Revisionszyklus alle 1, 2 Jahre] |
| Archivierungszeitraum | 10 Jahre | [Archivierungszeitraum nach Ablauf 5, 10 Jahre] |

# Dokumentenhistorie

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Beschreibung | Autor | Datum |
| 0.1 | initiale Erstellung |  |  |
| 0.2 – 0.8 | draft |  |  |
| 0.9 | final draft |  |  |
| 1.0 | final/freigegeben |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Inhaltsverzeichnis

[Allgemeine Informationen zum vorliegenden Dokument 2](#_Toc82712562)

[Dokumentenhistorie 3](#_Toc82712563)

[Inhaltsverzeichnis 4](#_Toc82712564)

[Allgemeine Festlegungen 5](#_Toc82712565)

[Ziel / Zweck 5](#_Toc82712566)

[Geltungsbereich 5](#_Toc82712567)

[Zuständigkeiten 5](#_Toc82712568)

[Genehmigungs- und Änderungsverfahren 6](#_Toc82712569)

[Aufbau des Dokuments 6](#_Toc82712570)

[Sicherheitsrichtlinie „Microsoft Exchange und Outlook" 7](#_Toc82712571)

[Basismaßnahmen 7](#_Toc82712572)

[Auswahl einer geeigneten Microsoft Exchange-Infrastruktur (APP.5.2.A2) 7](#_Toc82712573)

[Berechtigungsmanagement und Zugriffsrechte (APP.5.2.A3) 7](#_Toc82712574)

[Zugriffsrechte auf Microsoft Exchange-Objekte (APP.5.2.bd.A1) 7](#_Toc82712575)

[Datensicherung von Microsoft Exchange (APP.5.2.A5) 8](#_Toc82712576)

[Standardmaßnahmen 8](#_Toc82712577)

[Sichere Installation eines Microsoft Exchange-Systems (APP.5.2.bd.A2) 8](#_Toc82712578)

[Migration von Microsoft Exchange-Systemen (APP.5.2.A7) 8](#_Toc82712579)

[Sicherer Betrieb von Microsoft Exchange (APP.5.2.bd.A3) 8](#_Toc82712580)

[Sichere Konfiguration von Microsoft Exchange-Servern (APP.5.2.A9) 9](#_Toc82712581)

[Sichere Konfiguration von Outlook (APP.5.2.A10) 9](#_Toc82712582)

[Absicherung der Kommunikation zwischen Microsoft Exchange-Systemen (APP.5.2.A11) 9](#_Toc82712583)

[Einsatz von Outlook Anywhere, MAPI over HTTP und Outlook Web App (APP.5.2.A12) 10](#_Toc82712584)

[Schulung zu Sicherheitsmechanismen von Outlook für Anwender (APP.5.2.A14) 10](#_Toc82712585)

[Betriebsdokumentation für Microsoft Exchange (APP.5.2.A15) 10](#_Toc82712586)

[Erstellung eines Notfallplans für den Ausfall von Microsoft Exchange und Outlook (APP.5.2.bd.A4) 10](#_Toc82712587)

[Maßnahmen bei erhöhtem Schutzbedarf 10](#_Toc82712588)

[Verschlüsselung von Microsoft Exchange-Datenbankdateien (APP.5.2.A17 - CI) 11](#_Toc82712589)

[• eigene Verschlüsselungsfunktionen, 11](#_Toc82712590)

[• Verschlüsselungsgrade und 11](#_Toc82712591)

[• Mechanismen zur Absicherung der Daten in einer PST-Datei. 11](#_Toc82712592)

[Regelmäßige Sicherheitsprüfungen für Microsoft Exchange-Systeme (APP.5.2.bd.A5- CIA) 11](#_Toc82712593)

# Allgemeine Festlegungen

## Ziel / Zweck

Microsoft Exchange ist eine Groupware-Lösung, welche für den geschäftlichen Einsatz in KMUs und großen Institutionen konzipiert wurde. Nachrichten, wie E-Mails, können mit Microsoft Exchange zentral verwaltet, zugestellt, gefiltert und versendet werden. Ebenso können typische Groupware-Anwendungen, wie Notizen, Kontaktlisten, Kalender und Aufgabenlisten angeboten und verwaltet werden. Um die Funktionen von Microsoft Exchange nutzen zu können, ist neben dem Server-Dienst eine zusätzliche Client-Software, mobile App oder ein Web-Browser nötig. Die Kombination aus Microsoft Exchange-Servern und Outlook-Clients wird in dieser Sicherheitsrichtlinie als Microsoft Exchange-System bezeichnet.

Microsoft Outlook ist ein Client, der durch die Installation des Office-Pakets von Microsoft oder durch Integration in die Betriebssysteme von mobilen Geräten direkt zur Verfügung gestellt wird. Darüber hinaus ermöglicht die Webanwendung „Outlook Web App“ (OWA) über den Browser z. B. auf E-Mails, Kontakte und den Kalender zugreifen.

Ziel dieser Sicherheitsrichtlinie ist es, über typische Gefährdungen für Microsoft Exchange und Outlook zu informieren sowie aufzuzeigen, wie Microsoft Exchange und Outlook sicher in der <Institution> eingesetzt werden kann. Für die Erstellung dieser Sicherheitsrichtlinie wurde auf die Vorgaben des BSI Bausteines APP.5.2 „Microsoft Exchange und Outlook" zurückgegriffen.

## Geltungsbereich

Die Vorgaben des Dokumentes sind für alle Prozessverantwortlichen der <Institution> verbindlich und entsprechend durch die zuständigen Rollenträger umzusetzen.

Anzuwenden sind die Vorgaben für alle durch die <Institution> verantworteten Geschäftsprozesse, Hard- und Softwarekomponenten sowie ihren Konfigurationen. Die Umsetzung dieser Arbeitsanweisung ist durch die entsprechenden Führungskräfte sicherzustellen.

Die im Folgenden beschriebenen Vorgaben sind hingegen nicht bindend für Prozessverantwortliche von Geschäftsprozessen, die nicht durch die <Institution> wahrgenommen werden. In diesen Fällen besitzen die beschriebenen Vorgaben einen empfehlenden Charakter, auf eine Einhaltung muss durch die <Institution> hingewirkt werden.

Interne Regelungen sind geschlechterneutral zu formulieren. Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung männlicher und weiblicher Sprachformen verzichtet. Sämtliche personenbezogenen Bezeichnungen in männlicher Form werden verallgemeinernd verwendet und beziehen sich stets auf alle Geschlechter.

## Zuständigkeiten

Zuständig für die Einhaltung der in diesem Dokument aufgeführten Pflichten und Anforderungen sind:

* Eigene Mitarbeitende und beauftragte Dienstleister, welche administrative Arbeiten an IT- Systemen und Anwendungen von der <Institution> durchführen,
* Eigene Mitarbeitende und beauftragte Dienstleister, welche Applikationsbetreuung mit administrativem Charakter (z. B. Versionspflege, Benutzerverwaltung) betreiben. Die Kontrolle der korrekten Umsetzung der Vorgaben erfolgt durch den <Bereich ???> bei der <Institution>.

## Genehmigungs- und Änderungsverfahren

Die Sicherheitsrichtlinie „Microsoft Exchange und Outlook“ wird durch den <Informationssicherheitsbeauftragter> verantwortet. Die Pflege dieses Dokuments unterliegt dem <Bereich ???> vertreten durch den <Informationssicherheitsbeauftragter>. Änderungen werden ausschließlich von dieser Person oder seinem Stellvertreter vorgenommen. Eine Genehmigung und Freigabe erfolgt durch den <Informationssicherheitsbeauftragter>.

## Aufbau des Dokuments

Das vorliegende Dokument ist wie folgt aufgebaut:

* Kapitel Basismaßnahmen: Beschreibung der Kernmaßnahmen, die für das Anforderungsmanagement zwingend erforderlich sind.
* Kapitel Standardmaßnahmen: Definition von Maßnahmen zur Erreichung eines vollumfänglichen Standardabsicherungsschutzniveaus für einen Schutzbedarf von „Normal“ in den Informationssicherheitsschutzzielen Vertraulichkeit, Integrität und Verfügbarkeit.
* Kapitel Maßnahmen bei erhöhtem Schutzbedarf: Erläuterung von Maßnahmen die einen erhöhten Schutzbedarf (Schutzbedarfe „Hoch“, „Sehr hoch“) gewährleisten. Der Einsatz ist je Anwendungsfall im Rahmen einer Verhältnismäßigkeitsprüfung abzuwägen.

# Sicherheitsrichtlinie „Microsoft Exchange und Outlook"

## Basismaßnahmen

Die nachfolgenden Basismaßnahmen sind vorrangig zur Gewährleistung der sicherheitstechnischen Anforderungen aus der Leitlinie umzusetzen.

**Planung des Einsatzes von Microsoft Exchange und Outlook (APP.5.2.A1)**

Der Einsatz von Microsoft Exchange und Outlook wurde sorgfältig geplant. Im Rahmen der Planungsphase wurden unter anderem folgende Punkte beachtet:

* Aufbau der E-Mail-Infrastruktur,
* anzubindende Clients beziehungsweise Server-Systeme,
* zu verwendende Betriebssystem- und Versionen von Microsoft Exchange und Outlook,
* Nutzung von funktionalen Erweiterungen,
* Absicherung der Zugangsports der Server-/Client-Komponenten,
* Vereinbarte SLAs und OLAs,
* Zu realisierende Schützbedarfe (Vertraulichkeit, Integrität und Verfügbarkeit),
* Vereinbarte SLAs und OLAs,
* zu verwendende Protokolle sowie
* Integration der Server- und Client-Systeme in die hierfür vorgesehenen Netzsegmente.

### Auswahl einer geeigneten Microsoft Exchange-Infrastruktur (APP.5.2.A2)

Unter Berücksichtigung der Cloud-Strategie der<Institution> muss von den Verantwortlichen für den Betrieb zusammen mit den Architekturverantwortlichen der Einsatz von Microsoft Exchange entscheiden. Im Rahmen der Planung und Entscheidungsfindung muss definiert werden, mit welchen Systemen und Anwendungskomponenten sowie in welcher hierarchischen Abstufung die Microsoft Exchange-Infrastruktur realisiert wird. Im Rahmen der Auswahl der Komponenten und Plattformen muss auch entschieden werden, ob die Systeme als SaaS-, Cloud- oder lokalen Dienst betrieben werden sollen.

### Berechtigungsmanagement und Zugriffsrechte (APP.5.2.A3)

Zusätzlich zum allgemeinen Berechtigungskonzept der<Institution> ist ein Berichtigungskonzept speziell für die Systeme der Microsoft Exchange-Infrastruktur zu erstellen, geeignet zu dokumentieren sowie zu etablieren und kontinuierlich an den Bedürfnissen der <Institution> anzupassen.

Der IT-Betrieb muss serverseitige Benutzerprofile für einen rechnerunabhängigen Zugriff der Benutzer auf Micro- soft Exchange-Daten verwenden. Er muss die Standard-NTFS-Berechtigungen für das Microsoft Exchange-Verzeichnis so anpassen, dass nur autorisierte Administratoren und Systemkonten auf die Daten in diesem Verzeichnis zugreifen können.

### Zugriffsrechte auf Microsoft Exchange-Objekte (APP.5.2.bd.A1)

Die Zugriffsberechtigungen auf Microsoft Exchange-Objekte sind nach dem Need-to-know-Prinzip festzulegen. Für einen rechnerunabhängigen Zugriff auf die Microsoft Exchange-Daten sind serverseitige Profile zu verwenden. Die Standard-NTFS-Berechtigungen auf das Microsoft Exchange-Verzeichnis sind so anzupassen, dass nur autorisierte Administratoren der<Institution> und Systemkonten auf die Daten in diesem Verzeichnis zugreifen können.

### Datensicherung von Microsoft Exchange (APP.5.2.A5)

Das bestehende Microsoft Exchange-System ist unter Berücksichtigung der definierten Verfügbarkeits- und maximal tolerierbaren Datenverlustparametern vor Installationen und Konfigurationsänderungen sowie in zyklischen Abständen zu sichern.

Zusätzlich ist eine dokumentierte Vorgehensweise zu definieren, wie die Datensicherung unter Berücksichtigung der maximal tolerierbaren Wiederherstellungszeit erfolgen soll.

## Standardmaßnahmen

Gemeinsam mit den Basismaßnahmen sind die folgenden Standardmaßnahmen zum Erzielen eines normalen Schutzbedarfs zu betrachten und sollten grundsätzlich umgesetzt werden.

### Sichere Installation eines Microsoft Exchange-Systems (APP.5.2.bd.A2)

Die Installation erfolgt auf Basis der Einsatzplanung und der festgelegten Standards der<Institution>. Hierbei werden alle spezifischen Härtungsempfehlungen der Firma Microsoft berücksichtigt. Alle Systeme, auf denen Microsoft Exchange und Outlook installiert werden soll, sind somit entsprechend dem mit dem <Informationssicherheitsbeauftragter> abgestimmten Schutzbedarf (Verfügbarkeit, Vertraulichkeit, Integrität) abgesichert.

### Migration von Microsoft Exchange-Systemen (APP.5.2.A7)

Alle Migrationsschritte werden gründlich durch die Verantwortlichen geplant, dokumentiert und idealerweise vorab erprobt. Hierbei werden folgende Aspekte pro zu migrierender und Zielversion berücksichtigt:

* Postfächer,
* Objekte,
* Sicherheitsrichtlinien,
* Active Directory-Konzepte,
* E-Mail-Systeme sowie
* Funktionsunterschiede.

Die Betriebsverantwortlichen werden an der Planung der Migration beteiligt. Vor der Installation wird die neue Exchange-Infrastruktur in einem separaten Testumfeld auf die korrekte Umsetzung der Use-Cases und Anforderungen aus der<Institution> geprüft. Des Weiteren wird geprüft, ob die bisherigen Mail-gestützten Verfahren der<Institution> vollumfänglich intergiert werden können.

### Sicherer Betrieb von Microsoft Exchange (APP.5.2.bd.A3)

Alle Systeme und Anwendungen sind dem Schutzbedarf (Verfügbarkeit, Vertraulichkeit, Integrität) entsprechend zu konfigurieren. Hierzu ist eine Basiskonfiguration zusammenzustellen und zu dokumentieren. Die Einstellungen der einzelnen Konnektoren sind ebenfalls anzupassen.

Schwachstellen werden zeitnah in Abhängigkeit vom Schutzbedarf und der Kritikalität durch die Verantwortlichen behoben. Patches und Updates werden nur aus vertrauenswürdigen Quellen bezogen.

### Sichere Konfiguration von Microsoft Exchange-Servern (APP.5.2.A9)

Microsoft Exchange-Server werden nach den Vorgaben aus dem Sicherheitskonzept konfiguriert. Für eingehende sowie ausgehende Nachrichten wurde eine maximal zulässige Größe eingestellt. Vorhandene Konnektoren werden geeignet konfiguriert. Ebenso ist die Protokollierung des Microsoft Exchange-Systems aktiviert. Für vorhandenes Customizing wurde ein entsprechendes Konzept erstellt. Bei der Verwendung von funktionalen Erweiterungen wird sichergestellt, dass die definierten Anforderungen an die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit weiterhin erfüllt sind.

### Sichere Konfiguration von Outlook (APP.5.2.A10)

Nur die betriebsverantwortlichen Administratoren sind dazu berechtigt die Outlook-Umgebung zu ändern. Hierfür wird für jeden Nutzer ein eigenes Outlook-Profil mit den benutzerspezifischen Einstellungen angelegt. Die Mitarbeitenden (Anwender) können nur ausgewählte Einstellungen benutzerdefiniert verändern. Datei-Anhänge können nicht automatisch aus E-Mails heraus geöffnet werden. Vorschaufenster und die Autovorschau sind deaktiviert. Ebenfalls werden E-Mails nicht automatisiert weitergeleitet.

### Absicherung der Kommunikation zwischen Microsoft Exchange-Systemen (APP.5.2.A11)

Die Kommunikation von und zu Microsoft Exchange-Systemen ist abgesichert. Hierzu wurde entschieden welche Schutzmechanismen eingesetzt werden sollen.

Es wurde entschieden und dokumentiert, welches Verfahren der Internet Protocol Security (IPSec) oder Transport Layer Security (TLS) eingesetzt werden soll. Der Einsatz von StartTLS darf auf Grund des nachfolgend aufgezeigten Protokollsequenzverlaufes nicht erfolgen. Für StartTLS ist definiert, dass zunächst eine unverschlüsselte Verbindung aufgebaut wird und erst wenn Microsoft Exchange-StartTLS-Server und Microsoft Exchange-StartTLS-Client feststellen, dass beide TLS unterstützen wird eine verschlüsselte Verbindung aufgebaut. Hierdurch besteht das Risiko, dass trotz Einsatz von StartTLS innerhalb der<Institution> keine verschlüsselte Kommunikation zu anderen Systemen etabliert wird.

Insbesondere sind folgenden Kommunikationsschnittstellen kryptographisch abzusichern:

* Administrationsschnittstellen,
* Client-Server-Kommunikation,
* vorhandene Web-based-Distributed-Authoring-and-Versioning-(WebDAV)-Schnittstellen,
* die Server-Server-Kommunikation, die Nachrichten-Kommunikation sowie
* die Public-Key-Infrastruktur, die auf der E-Mail-Verschlüsselung von Microsoft Outlook (S/MIME) basieren.

### Einsatz von Outlook Anywhere, MAPI over HTTP und Outlook Web App (APP.5.2.A12)

Outlook Anywhere, MAPI over HTTP und die Outlook Web App sind entsprechend den internen Sicherheitsanforderungen der<Institution> zu konfigurieren. Der Zugriff auf Microsoft Exchange über öffentliche Netze insbesondere dem Internet sollte unter Berücksichtigung des Need-to-know-Prinzips auf die notwendigen Benutzer beschränkt werden.

### Schulung zu Sicherheitsmechanismen von Outlook für Anwender (APP.5.2.A14)

Die Mitarbeitenden (Anwender) sollten regelmäßig über bestehende und neue Gefahren beim Arbeiten mit Microsoft Outlook sensibilisiert und geschult werden. Hierbei sind auch relevante Sicherheitsmechanismen und die entsprechenden Vorgehensweisen innerhalb von Outlook zu vermitteln. Hierzu gehören unter anderem auch Regelungen, z. B. für Zugriffsmechanismen, Authentisierungsformen, kryptografische Vorgaben für die E-Mail-Verschlüsselung und die Mechanismen zur Kategorisierung der Vertraulichkeit von E-Mail-Informationen.

### Betriebsdokumentation für Microsoft Exchange (APP.5.2.A15)

Es muss ein Betriebshandbuch für Microsoft Exchange erstellt werden. Dieses sollte angelehnt an den Lebenszyklus sein und sollte die Phasen der Inbetriebnahme, des Betriebs, der Aussonderung und des Wiederanlaufs beschreiben. Der Zugriff auf die Dokumentation muss vor Unbefugten geschützt werden. Alle Änderungen sind für geschulte Dritte nachvollziehbar zu dokumentieren bzw. zu referenzieren.

### Erstellung eines Notfallplans für den Ausfall von Microsoft Exchange und Outlook (APP.5.2.bd.A4)

Innerhalb der<Institution> wird unter Berücksichtigung der geschäftlichen Kritikalität des Services (BIA) ein Wiederanlaufplan, ein Wiederherstellungsplan (dieser müsste in vielen Passagen identisch zu den Inhalten der Inbetriebnahme aus dem Betriebshandbuch sein) sowie einen Wiederanlaufkoordinationsplan für den Ausfall von Microsoft Exchange und Outlook erstellt. Der zuvor benannten Pläne definieren, mit welchen Schritte bei einem Ausfall eine zeitnahe Wiederherstellung des Normalbetriebs zu gewährleisten ist.

## Maßnahmen bei erhöhtem Schutzbedarf

Gemeinsam mit den Basismaßnahmen und den Standardmaßnahmen sind zum Erzielen eines erhöhten Schutzbedarfs die hier aufgeführten Maßnahmen zu betrachten und sollten grundsätzlich umgesetzt werden. Ist dies aus wirtschaftlichen bzw. organisatorischen Gründen nicht möglich, so ist dies mit dem Sicherheitsmanagement zur weiteren Begegnung von Risiken für die Infrastruktur der <Institution> zu begründen und abzustimmen. Im Folgenden werden die Maßnahmen bei erhöhtem Schutzbedarf aufgeführt. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

### Verschlüsselung von Microsoft Exchange-Datenbankdateien (APP.5.2.A17 - CI)

Es sollte ein Verschlüsselungskonzept für PST-Dateien und Informationsspeicher-Dateien erstellt werden. Alle Mitarbeitenden wurden über die Funktionsweise und die Schutzmechanismen bei der Verschlüsselung von PST-Dateien informiert. Zusätzlich werden folgende Aspekte für lokale PST-Dateien bei der Verschlüsselung von Microsoft Exchange-Datenbanken berücksichtigt:

### eigene Verschlüsselungsfunktionen,

### Verschlüsselungsgrade und

### Mechanismen zur Absicherung der Daten in einer PST-Datei.

Mechanismen wie z. B. Encrypting File System, Microsoft Azure Information Protection (AIP) oder Windows BitLocker Laufwerkverschlüsselung werden zur Absicherung der Daten in einer PST-Datei genutzt.

### Regelmäßige Sicherheitsprüfungen für Microsoft Exchange-Systeme (APP.5.2.bd.A5- CIA)

Es sollten regelmäßige Sicherheitsprüfungen des Microsoft Exchange-Systems stattfinden. Im Rahmen der Sicherheitsprüfung sollte das System auf mögliche Fehlkonfigurationen und Schwachstellen geprüft werden. Die Prüfungen sollten durch unterschiedliche Personen durchgeführt werden. Um einen definierten Prüfumfang zu gewährleisten, muss eine Prüfliste etabliert werden. Diese beinhaltet mindestens die folgenden Aspekte:

* regelmäßige Recherchen sicherheitsrelevanter Informationen,
* Berechtigungen für Revisionsbenutzer,
* regelmäßige Prüfung der Berechtigungen,
* Prüfung der Aktualität der Updates und
* Prüfung der Sicherheit der Kommunikationsschnittstellen.

Die Microsoft Exchange-Berechtigungen sind regelmäßig (mindestens einmal im Jahr) stichprobenartig zu prüfen.