

Sicherheitsanforderung

M365 Exchange Online

Deutsche Telekom Gruppe

Version	2.2
Datum	01.07.2025
Status	Freigegeben

Impressum

Herausgeber
Deutsche Telekom AG
Vorstandsbereich Technology & Innovation
Chief Security Officer

Reuterstrasse 65, 53315 Bonn
Deutschland

Dateiname	Dokumentennummer 8.07	Dokumententyp Sicherheitsanforderung
Version 2.2	Stand 01.07.2025	Status Freigegeben
Fachlicher Ansprechpartner Telekom Security psa.telekom.de	Gültigkeitsdauer 01.07.2025 - 30.06.2030	Freigegeben von Stefan Pütz, Leiter SEC-T-TST

Zusammenfassung

Microsoft Exchange Online ist eine gehostete Messaginglösung, die E-Mails, Kalender, Kontakte und Aufgaben von PCs, dem Web und mobilen Geräten übermittelt. Es ist vollständig in Azure Active Directory integriert, sodass Administratoren Gruppenrichtlinien sowie andere Verwaltungstools verwenden können, um Exchange Online Features in ihrer gesamten Umgebung zu verwalten.

Copyright © 2025 by Deutsche Telekom AG.

Alle Rechte, auch die des auszugsweisen Nachdrucks, der fotomechanischen Wiedergabe (einschließlich Mikrokopie) sowie der Auswertung durch Datenbanken oder ähnliche Einrichtungen, vorbehalten.

Inhaltsverzeichnis

1.	Einleitung	4
2.	Email Encryption	5
3.	Malware & Spam Protection	6
4.	Mail Transport	7
5.	Logging & Detection	10

1. Einleitung

Dieses Dokument wurde auf Basis der Vorgaben aus der Konzernrichtlinie Sicherheit (Group Security Policy). Die vorliegende Sicherheitsanforderung dient u.a. als Grundlage zur Freigabe im PSA-Prozess. Sie dient darüber hinaus als Umsetzungsempfehlung für Vorgaben der Konzernrichtlinie Sicherheit (Group Security Policy) in Einheiten, die nicht am PSA-Verfahren teilnehmen. Diese Anforderungen müssen bereits während der Planungs- und Entscheidungsprozesse berücksichtigt werden und gelten für alle M365 Umgebungen der jeweiligen Einheit.

Bei der Umsetzung der Sicherheitsanforderung ist das jeweils vorrangige nationale, internationale und supranationale Recht zu beachten. Sollte die Einhaltung der beschriebenen Anforderungen in individuellen Fällen nicht oder nur eingeschränkt umsetzbar sein, ist gemeinsam mit einem Sicherheits- und/oder Datenschutzexperten (entsprechend der betroffenen Anforderung) eine Risikobewertung vorzunehmen und mögliche alternative Schutzmaßnahmen abzustimmen.

2. Email Encryption

Req 1	Um einen sicheren, verschlüsselten Email-Verkehr via S/MIME zu ermöglichen, muss eine sichere PKI Infrastruktur betrieben werden
-------	--

Um einen sicheren, verschlüsselten Email-Verkehr via S/MIME zu ermöglichen, muss eine sichere PKI Infrastruktur betrieben werden.

Gültigkeit: Plattformbetrieb

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unbemerkt durchführbare Angriffe

ID: 8.07-1/2.2

3. Malware & Spam Protection

Req 2 Der Common Attachment Types Filter muss verwendet werden

Um zu verhindern, dass Malware über Attachments in Emails verteilt wird, muss der Common Attachment Filter aktiviert werden.

Gültigkeit: Plattformbetrieb

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit
- Abstreiten von durchgeführten Aktionen
- Unbemerkt durchführbare Angriffe

ID: 8.07-2/2.2

Req 3 Exchange Online Spam Policies müssen verwendet werden

Um (übernommene) Accounts, die Spam Emails versenden, zu identifizieren und zu blockieren, müssen die Exchange Online Spam Policies konfiguriert und aktiviert werden.

Gültigkeit: Plattformbetrieb

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Nutzung von Diensten oder Ressourcen

ID: 8.07-3/2.2

4. Mail Transport

Req 4 Emails dürfen nur zu erlaubten Domains weitergeleitet werden

Um eine Data Exfiltration via Email zu unterbinden, dürfen Weiterleitungen außerhalb der Organisation nur an erlaubte Domains durchgeführt werden.

Gültigkeit: Plattformbetrieb

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unbemerkt durchführbare Angriffe

ID: 8.07-4/2.2

Req 5 Für alle Exchange Online Domains muss DKIM verwendet werden.
Es muss mindestens ein DKIM-Schlüssel mit einer Länge von 2.048-Bit sein.

Um gefälschte Emails, die aussehen, als ob sie von der eigenen Organisation kommen, zu verhindern, muss DKIM verwendet werden.

Gültigkeit: Plattformbetrieb

Motivation: Mit DKIM kann das Risiko von Spoofing gesenkt bzw. fast verhindert werden, dass ausgehenden Nachrichten als Spam markiert werden.

*Spoofing ist eine Art E-Mail-Angriff, bei dem die **Von**-Adresse einer E-Mail-Nachricht gefälscht wird. Derart gefälschte Nachrichten erwecken den Anschein von einer bestimmten Organisation oder Domain zu stammen. Über DKIM lässt sich erkennen, dass eine Nachricht geändert wurde und dass nicht autorisierte Änderungen an der **Von**-Adresse der Nachricht vorgenommen wurden.*

Somit lassen sich proaktiv Spoofing, Phishing und Business Email Compromise (BEC) minimieren.

Umsetzungsbeispiel: In dem Umsetzungsbeispiel wird der Selektor "dkim" genannt. Die verwendete Domäne ist "example.com".

Um dem empfangenden Server anzuzeigen, welcher DNS-Eintrag DKIM betrifft, muss der Selektor "._domainkey" hinzugefügt werden.

Der Name des TXT-Eintrags im DNS lautet: "dkim._domainkey.example.com".

Der "Eintrag"-Teil beginnt mit der Zuweisung der Version des DKIM-Protokolls als "v=DKIM1", gefolgt von einem "k" für den Schlüsseltyp wie z.B. RSA. "p" gibt den öffentlichen Schlüssel an.

```
T X T - E i n t r a g                      =                      " v                      D K I M 1 ;                      k = r s a ;  
p=MII BjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQE A5vyh9icvuvA1DBqiRIHlaKY GhP6NmToFzLv2cV2SAf  
Q H V c H X S 4 D Z u e 6 X i 2 B D U Z 8 4 C s a u R Y M G l s K T L / C o m P d v /  
TKAT1AIQ6glwqLvsUUyfwNQTTe2PsA6fzgp1KQGPr1PCHFuYcr3AQk2Cu9gPwKZLkPvVoCTYpqqbpo4VVFXYFYGc  
BttM+inzdOwC4DjPhz5nh7A7PD/SLNnsvvRZG6H4ao/FWIPn2RLrWzZTgIDvMqVpzbgLu+qUbgWnHJJ/  
LuqxGicvUJBuH8Kp9VxNfiQlu6gJkGTnTcJxpEXvOLhvWKO3XoIWVTf9Cz3DMsfDE0Rt3QlZj9S5xTvjymluy7IQIDAQAB  
"
```

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit
- Unbemerkt durchführbare Angriffe

ID: 8.07-5/2.2

Req 6 Für alle Exchange Online Domains muss SPF mit den Parametern "v=spf1 include:_spf.domain.tld ~all" verwendet werden.

Um gefälschte Emails, die aussehen, als ob sie von der eigenen Organisation kommen, zu verhindern, muss SPF mit den oben angeführten Parametern verwendet werden. Der kursiv geschriebene Parameter *_spf.domain.tld* muss entsprechend der eigenen Infrastruktur angepasst werden.

Der Parameter "~all" wurde aufgrund der Maximalvorgabe seitens Betreiber und Security des Telekom Emailbackbones gesetzt. Idealerweise wird hier der Parameter "-all" gesetzt.

Gültigkeit: Plattformbetrieb

Umsetzungsbeispiel: **Beispiel Konfiguration Telekom Emailbackbone:**

Include:_spf.telekom.com

v=spf1 ip4:194.25.225.128/26 ip4:194.25.225.192/26 ip4:194.25.225.35 ip4:194.25.225.36 ip4:3.78.33.34 ip4:3.67.17.164
include:spf.protection.outlook.com ~all

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System
- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit
- Unbemerkt durchführbare Angriffe

ID: 8.07-6/2.2

Req 7 Für alle Exchange Online Domains muss DMARC mit den Parametern "v=DMARC1; p=quarantine" verwendet werden.

Um gefälschte Emails, die aussehen, als ob sie von der eigenen Organisation kommen, zu verhindern, muss DMARC verwendet werden.

Vor der Aktivierung von DMARC müssen Sender Policy Framework (SPF) und DomainKeys Identified Mail (DKIM) konfiguriert und mindestens 48 Stunden vorher aktiviert werden, um Emailnachrichten korrekt zu authentifizieren.

Der Parameter "p=quarantine" wurde aufgrund der Maximalvorgabe seitens Betreiber und Security des Telekom Emailbackbones gesetzt. Idealerweise wird hier der Parameter "p=reject" gesetzt.

Gültigkeit: Plattformbetrieb

Motivation: Die DMARC-Parameter "v=DMARC1; p=reject" bewirken, dass Email-Nachrichten von nicht korrekt authentifizierten Emailservern abgelehnt werden. Damit werden erfolgreich Spoofing und Phishing Angriffe per Email verhindert.

Wird statt dessen der Parameter "v=DMARC1; p=quarantine" gesetzt, werden Emails von nicht korrekt authentifizierten Emailservern in das Quarantäneverzeichnis verschoben und der Empfänger hat dann die Möglichkeit zu entscheiden, ob diese Email ins Emailpostfach zugestellt werden soll oder nicht.

Umsetzungsbeispiel: **Beispielkonfiguration Telekom Emailbackbone:**

v=DMARC1;p=quarantine;rua=mailto:dmarc@telekom.com;ruf=mailto:dmarc@telekom.com

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigter Zugang zum System

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Unberechtigte Nutzung von Diensten oder Ressourcen
- Störung der Verfügbarkeit
- Unbemerkt durchführbare Angriffe

ID: 8.07-7/2.2

5. Logging & Detection

Req 8 Mailbox Auditing für alle Benutzer muss aktiviert werden

Um das Verhalten der Benutzer einer Mailbox überwachen zu können, muss Mailbox Auditing für alle Benutzer aktiviert werden.

Gültigkeit: Plattformbetrieb

Für diese Anforderung sind folgende Bedrohungen relevant:

- Unberechtigte Einsichtnahme oder Abgriff von Daten
- Unberechtigte Modifikation von Daten
- Abstreiten von durchgeführten Aktionen
- Unbemerkt durchführbare Angriffe

ID: 8.07-8/2.2