Security requirement

M365 Exchange Online

Deutsche Telekom Group

Version	2.0
Date	Jul 1, 2024
Status	Released

Publication Details

Published by
Deutsche Telekom AG
Vorstandsbereich Technology & Innovation
Chief Security Officer

Reuterstrasse 65, 53315 Bonn
Germany

File name	Document number	Document type
	8.07	Security requirement
Version	**State**	**Status**
2.0	Jul 1, 2024	Released
Contact	**Validity**	**Released by**
Telekom Security psa.telekom.de	Jul 1, 2024 - Jun 30, 2029	Stefan Pütz, Leiter SEC-T-TST

Summary
Microsoft Exchange Online is a hosted messaging solution that delivers email, calendars, contacts, and tasks from PCs, the web, and mobile devices. It is fully integrated with Azure Active Directory, allowing administrators to use Group Policy and other management tools to manage Exchange Online features throughout their environment.

Copyright © 2024 by Deutsche Telekom AG.
All rights reserved.

Table of Contents

1. Introduction 4
2. Email Encryption 5
3. Malware & Spam Protection 6
4. Mail Transport 7
5. Logging & Detection 9

1. Introduction

This document was prepared on the basis of the requirements of the Group Security Policy. The present safety requirement serves, among other things, as a basis for approval in the PSA process. It also serves as an implementation recommendation for the requirements of the Group Security Policy in units that do not participate in the PSA procedure. These requirements must be taken into account during the planning and decision-making processes and apply to all M365 environments of the respective unit.

When implementing the security requirement, the priority national, international and supranational law must be observed. If compliance with the described requirements cannot be implemented or can only be implemented to a limited extent in individual cases, a risk assessment must be carried out together with a security and/or data protection expert (in accordance with the relevant requirement) and possible alternative protective measures must be coordinated.

2. Email Encryption

Req 1	In order to enable secure, encrypted email traffic via S/MIME, a secure and approved PKI infrastructure must be operated

In order to enable secure, encrypted email traffic via S/MIME, a secure and approved PKI infrastructure must be operated.

Validity: Platform operation

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unnoticeable feasible attacks

ID: 8.07-1/2.0

3. Malware & Spam Protection

Req 2	The Common Attachment Types Filter must be used

To prevent malware from being distributed via attachments in emails, the Common Attachment Filter must be activated.

Validity: Platform operation

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Disruption of availability
- Denial of executed activities
- Unnoticeable feasible attacks

ID: 8.07-2/2.0

Req 3	Exchange Online Spam Policies Must Be Used

In order to identify and block (acquired) accounts that send spam emails, the Exchange Online Spam Policies must be configured and activated.

Validity: Platform operation

For this requirement the following threats are relevant:
- Unauthorized use of services or resources

ID: 8.07-3/2.0

4. Mail Transport

Req 4	Emails may only be forwarded to allowed domains

In order to prevent data exfiltration via email, redirects outside the organization may only be carried out to permitted domains.

Validity: Platform operation

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unnoticeable feasible attacks

ID: 8.07-4/2.0

Req 5	DKIM must be used for all Exchange Online domains. It must be at least a DKIM key with a length of 2,048 bits.

To prevent fake emails that look like they come from your own organization, DKIM must be used.

Validity: Platform operation

Motivation: DKIM can reduce the risk of spoofing or almost prevent outgoing messages from being marked as spam. Spoofing is a type of email attack that spoofs the **From-***address of an email message. Such fake messages appear to come from a specific organization or domain. DKIM indicates that a message has been modified and that unauthorized changes have been made to the message's From address. This allows you to proactively minimize spoofing, phishing and business email compromise (BEC).*

Implementation example: In the implementation example, the selector is called "dkim". The domain used is "example.com".
To indicate to the receiving server which DNS record affects DKIM, the selector "._domainkey" must be added.
The name of the TXT record in the DNS is: "dkim._domainkey.example.com". The "Entry" part starts with assigning the version of the DKIM protocol as "v=DKIM1", followed by a "k" for the key type such as RSA. "p" indicates the public key.

TXT record = "v DKIM1; k=rsa;
p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA5vyh9icvuvA1DBqiRlHlaKYGhP6NqmToFzLv2cV2SAf
QHVcHXS4DZue6Xi2BDUZ84CsauRYMGlsKTL/ComPdv/
TKAT1AIQ6glwqLvsUUYfwNQTTe2PsA6fzgp1KQGPr1PCHFuYcr3AQk2Cu9gPwKZLkPvVoCTYpqqbpo4VVFXFfYGc
BttM+inzd0wC4DjPhz5nh7A7PD/SLNnsvvRZG6H4ao/FWIPn2RLrWzZTgIDvMqVpzbgLu+qUbgWnHJJ/
LuqxGicvUJBuH8Kp9VxNfiQlu6gJkGTnTcJxpEXvOLhvWKO3XolWVTf9Cz3DMsfDE0Rt3Qlzj9S5xTvjymluy7lQlDAQAB
"

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Disruption of availability
- Unnoticeable feasible attacks

ID: 8.07-5/2.0

Req 6	SPF must be used for all Exchange Online domains

To prevent fake emails that look like they come from your own organization, SPF must be used.

Validity: Platform operation

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Disruption of availability
- Unnoticeable feasible attacks

ID: 8.07-6/2.0

Req 7	For all Exchange Online domains, DMARC must be set with the parameters "v=DMARC1; p=reject".

To prevent fake emails that look like they come from your own organization, DMARC must be used.

Before enabling DMARC, Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM) must be configured and activated at least 48 hours in advance to authenticate email messages correctly.

Validity: Platform operation

Motivation: The DMARC parameters "v=DMARC1; p=reject" cause email messages from email servers that are not authenticated correctly to be rejected. This successfully prevents spoofing and phishing attacks via email.

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Disruption of availability
- Unnoticeable feasible attacks

ID: 8.07-7/2.0

5. Logging & Detection

Req 8	Mailbox auditing for all users must be enabled

To monitor the behavior of the users of a mailbox, mailbox auditing must be enabled for all users.

Validity: Platform operation

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Denial of executed activities
- Unnoticeable feasible attacks

ID: 8.07-8/2.0