Muster-Prüfprogramm

# E-Mail-Sicherheit

## 12 Prüfschritte · BSI, ISO 27001, RFC

12 Prüfschritte mit Kriterium, Fundstelle, Prüfhandlung und erwarteten Nachweisen. 8 Unterlagen zur Anforderung und die typischen Feststellungen.

BSI APP.5.3 · ISO/IEC 27001:2022 Anhang A 5.14 · RFC 7208 · RFC 6376 · RFC 9989 · RFC 9990 · BSI TR-03108 · ISO/IEC 27001:2022 Anhang A 8.7 · ISO/IEC 27001:2022 Anhang A 8.7 und 8.23 · § 30 Abs. 2 Nr. 10 BSIG · ISO/IEC 27001:2022 Anhang A 8.5 · ISO/IEC 27001:2022 Anhang A 8.15 · ISO/IEC 27001:2022 Anhang A 6.8 · § 147 Abs. 1 Nr. 2 und 3 AO

## Prüfungsziel und Geltungsbereich

Die Prüfung beurteilt, ob die Organisation ihre E-Mail-Kommunikation technisch und organisatorisch absichert: Absenderauthentifizierung der eigenen Domänen, verschlüsselter Transport, Filterung von Schadprogrammen und Phishing, sichere Konfiguration der Mailplattform wie Exchange Online und ein funktionierender Meldeweg für verdächtige Nachrichten. Sie beurteilt außerdem, ob die Aufbewahrung geschäftlicher E-Mails geregelt ist.

### GELTUNGSBEREICH

- Alle E-Mail-Domänen der Organisation, auch solche, die nicht zum Versand genutzt werden
- Mailplattform (zum Beispiel Exchange Online oder Exchange Server) und vorgelagerte Filterdienste
- Externe Dienste, die im Namen der Organisation E-Mails versenden, etwa Newsletter oder Ticketsysteme
- Nicht Gegenstand: Ende-zu-Ende-Verschlüsselung einzelner Fachverfahren, sofern nicht gesondert vereinbart

## Prüfschritte 1 bis 3

Schritt 01 — BSI APP.5.3; ISO/IEC 27001:2022 Anhang A 5.14

### Eine Richtlinie regelt die dienstliche Nutzung von E-Mail, den Versand vertraulicher Informationen und die Weiterleitung nach extern.

**Prüfhandlung** Richtlinie lesen, Freigabe prüfen und mit den technischen Einstellungen zur Weiterleitung abgleichen.

**Nachweise** E-Mail-Richtlinie, Regelungen zum Informationsaustausch

Schritt 02 — RFC 7208

### Für jede Domäne ist ein SPF-Eintrag veröffentlicht, der nur berechtigte Versender zulässt; nicht versendende Domänen schließen Versand aus.

**Prüfhandlung** DNS-Einträge aller Domänen abfragen und die genannten Versender mit der Liste der tatsächlichen Versanddienste vergleichen.

**Nachweise** Domänenliste, DNS-Abfrage, Liste der Versanddienste

Schritt 03 — RFC 6376

### Ausgehende Nachrichten werden mit DKIM signiert; Schlüssel haben eine angemessene Länge und werden gewechselt.

**Prüfhandlung** Kopfzeilen von Testnachrichten aller Versandwege auswerten und Schlüssellänge sowie letzten Schlüsselwechsel erfragen.

**Nachweise** Kopfzeilen der Testnachrichten, DKIM-Konfiguration

## Prüfschritte 4 bis 6

Schritt 04 — RFC 9989; RFC 9990

### Eine DMARC-Richtlinie ist veröffentlicht und auf Ablehnung oder Quarantäne gestellt; die Berichte werden ausgewertet.

**Prüfhandlung** DMARC-Eintrag abfragen, Richtlinienstufe feststellen und die Auswertung der Berichte der letzten drei Monate ansehen.

**Nachweise** DNS-Abfrage, Auswertung der DMARC-Berichte, Maßnahmen zu Fehlkonfigurationen

Schritt 05 — BSI TR-03108

### Der Transport zwischen Mailservern ist verschlüsselt und gegen Herabstufung abgesichert, etwa über DANE oder MTA-STS mit TLS-Berichten.

**Prüfhandlung** Konfiguration des Transports prüfen und mit einem externen Prüfwerkzeug die Verschlüsselung der eigenen Mailserver testen.

**Nachweise** Testergebnis des Prüfwerkzeugs, Konfiguration der Konnektoren, TLS-Berichte

Schritt 06 — ISO/IEC 27001:2022 Anhang A 8.7; BSI APP.5.3

### Eingehende Nachrichten werden auf Schadprogramme geprüft; gefährliche Anhänge werden blockiert oder isoliert geöffnet.

**Prüfhandlung** Filterregeln und gesperrte Dateitypen ansehen und die Statistik der Funde der letzten drei Monate auswerten.

**Nachweise** Filterkonfiguration, Liste gesperrter Dateitypen, Fundstatistik

## Prüfschritte 7 bis 9

Schritt 07 — ISO/IEC 27001:2022 Anhang A 8.7 und 8.23

### Links in Nachrichten werden beim Aufruf geprüft, externe Absender sind gekennzeichnet und Absenderfälschungen werden erkannt.

**Prüfhandlung** Einstellungen zu Linkprüfung, Kennzeichnung externer Nachrichten und Schutz vor Identitätsfälschung ansehen und an einer Testnachricht nachvollziehen.

**Nachweise** Konfiguration des Phishing-Schutzes, Testnachricht mit Kennzeichnung

Schritt 08 — BSI APP.5.3

### Die Mailplattform ist gehärtet: automatische Weiterleitung nach extern ist eingeschränkt, veraltete Anmeldeverfahren sind abgeschaltet.

**Prüfhandlung** Einstellungen zu Weiterleitungen, Postfachregeln und Anmeldeverfahren auslesen und Postfächer mit externer Weiterleitung auflisten.

**Nachweise** Auszug der Mandantenkonfiguration, Liste der Postfächer mit Weiterleitung

Schritt 09 — § 30 Abs. 2 Nr. 10 BSIG; ISO/IEC 27001:2022 Anhang A 8.5

### Anmeldungen an Postfächern und an der Verwaltung der Plattform sind mit mehreren Faktoren geschützt.

**Prüfhandlung** Regeln für Mehrfaktor-Authentifizierung ansehen und Konten ohne zweiten Faktor mit Begründung auflisten lassen.

**Nachweise** Richtlinien für bedingten Zugriff, Bericht zur Registrierung der Faktoren, Ausnahmeliste

## Prüfschritte 10 bis 12

**Schritt 10** — ISO/IEC 27001:2022 Anhang A 8.15

### Zugriffe auf Postfächer und administrative Änderungen werden protokolliert und die Protokolle ausreichend lange aufbewahrt.

**Prüfhandlung** Aktivierung der Postfachprotokollierung und Aufbewahrungsdauer prüfen und einen Protokollabruf vorführen lassen.

**Nachweise** Protokolleinstellungen, Beispiel eines Protokollabrufs

**Schritt 11** — ISO/IEC 27001:2022 Anhang A 6.8

### Mitarbeitende können verdächtige Nachrichten einfach melden; Meldungen werden ausgewertet und beantwortet.

**Prüfhandlung** Meldeweg vorführen lassen und für fünf Meldungen Bearbeitung, Bewertung und Rückmeldung nachvollziehen.

**Nachweise** Beschreibung des Meldewegs, bearbeitete Meldungen

**Schritt 12** — § 147 Abs. 1 Nr. 2 und 3 AO

### Die Aufbewahrung geschäftlicher E-Mails, die als Handels- oder Geschäftsbriefe gelten, ist geregelt und technisch umgesetzt.

**Prüfhandlung** Aufbewahrungsregeln und Archivierungslösung ansehen und prüfen, ob Postfachlöschungen die Aufbewahrung unterlaufen können.

**Nachweise** Aufbewahrungsrichtlinie, Konfiguration der Archivierung

Unterlagenanforderung

# Diese 8 Unterlagen vor Prüfungsbeginn anfordern

1. E-Mail-Richtlinie
2. Liste aller Domänen und der Dienste, die im Namen der Organisation versenden
3. DNS-Einträge zu SPF, DKIM und DMARC sowie Auswertung der DMARC-Berichte
4. Konfiguration von Transportverschlüsselung, Filter und Phishing-Schutz
5. Auszug der Mandanten- oder Serverkonfiguration der Mailplattform
6. Bericht zur Mehrfaktor-Authentifizierung mit Ausnahmen
7. Beschreibung des Meldewegs für verdächtige Nachrichten
8. Aufbewahrungsrichtlinie für E-Mails

## TYPISCHE FESTSTELLUNGEN

- Die DMARC-Richtlinie steht dauerhaft auf Beobachtung, Berichte werden nicht gelesen.
- Nicht genutzte Domänen haben keinen Eintrag und können zur Fälschung missbraucht werden.
- Externe Versanddienste sind nicht in SPF oder DKIM eingebunden.
- Automatische Weiterleitung an private Adressen ist erlaubt.
- Einzelne Postfächer und Dienstkonten sind ohne zweiten Faktor erreichbar.
- Gemeldete Phishing-Nachrichten bleiben ohne Auswertung und Rückmeldung.

Bibliothek Muster-Prüfprogramme

# 29 Muster-Prüfprogramme online

**proauditmap.com/pruefprogramme/**

## Vollständiges Prüfpaket in ProAuditMap

**proauditmap.com**

**ProAuditMap**

Muster ohne Gewähr und keine Rechtsberatung. Gesetze, Verordnungen und Standards erscheinen nur als Fundstelle, Normtexte sind nicht abgedruckt. Passen Sie Umfang und Tiefe vor der Verwendung an Ihre Organisation, Ihre Risiken und die aktuelle Fassung der für Sie geltenden Vorschriften an. Stand: 13. Oktober 2026