

LEITFADEN · TOMORIS TOOLBOX

Exchange Online: Schutz vor Spam, Phishing und Schadsoftware

Integrierter Schutz, voreingestellte Richtlinien, Defender for Office 365 Plan 1 und 2, Quarantäne und Absenderauthentifizierung, nach Microsoft Learn und RFC

STAND

25.10.2026

UMFANG

PDF, 11 Seiten

ONLINE

tomoris.com/downloads/exchange-online-schutz-leitfaden

AUF EINEN BLICK

3 Stufen

Schutzleiter: integriert, Plan 1, Plan 2

48 h

rückwirkend prüft ZAP zugestellte E-Mails

30 Tage

Aufbewahrung in der Quarantäne bei Standard und Streng

350

Personen je Richtlinie im Identitätswechselschutz

FÜR WEN

- Administration von Microsoft 365 und Exchange Online in kleinen und mittleren Unternehmen
- IT-Dienstleister, die Mandanten ihrer Kunden einrichten und betreuen
- IT-Leitung, die Lizenzen und Schutzniveau für E-Mail festlegt

WORUM ES GEHT

Jedes Postfach in Exchange Online wird auf Spam, Schadsoftware und Phishing geprüft, doch erst die richtigen Einstellungen machen daraus wirksamen Schutz. Dieser Leitfaden ordnet die Schutzschichten ein, trennt die integrierten Funktionen von denen, die Microsoft Defender for Office 365 Plan 1 oder Plan 2 voraussetzen, und zeigt die von Microsoft empfohlenen Werte: voreingestellte Richtlinien Standard und Streng, Anti-phishing mit Spoofing- und Identitätswechselschutz, Sichere Links, Sichere Anlagen, ZAP, Quarantäne, Meldungen und die Absenderauthentifizierung der eigenen Domäne. Eine Checkliste und die häufigsten Fehler schließen ab.

Leitfaden und Checkliste sind eine Empfehlung von TOMORIS und an die eigene Umgebung anzupassen; sie ersetzen keine Rechtsberatung. Microsoft ändert Funktionen, Bezeichnungen, Menüs, Standardwerte und Lizenzumfänge laufend: Maßgeblich sind die verlinkten Seiten von Microsoft Learn in der aktuellen Fassung, für NIS2-Pflichten der Gesetzestext des NISG 2026 in der geltenden Fassung. Die DNS-Einträge sind Beispiele mit reservierten Beispieldomänen.

INHALT

01	Schutzschichten auf einen Blick	2
02	Was der integrierte Schutz immer tut	3
03	Voreingestellte Richtlinien als Startpunkt	4
04	Einstellungen im Einzelnen	5
05	Absenderauthentifizierung der eigenen Domäne	6
06	Quarantäne und Meldungen	7
07	Zulassen, Sperren und häufige Fehler	8
08	Checkliste zum Abhaken	9
09	Quellen	10

01 —

Schutzschichten auf einen Blick

Was jedes Postfach in Exchange Online mitbringt und was Defender for Office 365 Plan 1 und Plan 2 ergänzen.

Jede Organisation mit Postfächern in Exchange Online erhält ohne Zusatzlizenz Schutz vor Spam, Schadsoftware und Phishing. Was viele als Exchange Online Protection (EOP) kennen, heißt auf Microsoft Learn inzwischen „integrierte Sicherheitsfeatures für alle Cloudpostfächer“; der Assistent für voreingestellte Richtlinien und die PowerShell-Cmdlets verwenden weiter den Namen EOP. Eingehende Nachrichten durchlaufen den Verbindungsfilter (Ruf des Absenders, hier endet der meiste Spam), die Antischadsoftware, die Nachrichtenflussregeln und schließlich Antispam und Antiphishing. Defender for Office 365 ergänzt diese Schicht, ersetzt sie aber nicht.

Die Schutzleiter laut Microsoft Learn (Stand 25.10.2026)

STUFE	ENTHALTEN IN	WAS DAZUKOMMT
Integriert (EOP)	allen Abonnements mit Cloud-postfächern	Antischadsoftware, Antispam, Antiphishing mit Spoofingschutz, ZAP für E-Mail, Quarantäne, Meldungen, Mandanten-Zulassungs-/Sperrliste, voreingestellte Richtlinien, Konfigurationsanalyse
Defender for Office 365 Plan 1	z. B. Microsoft 365 Business Premium, seit Juli 2026 auch Microsoft 365 E3; sonst als Add-on	Identitätswechselschutz, Phishing-Schwellenwerte, Sichere Anlagen, Sichere Links, integrierter Schutz, Echtzeiterkennungen, ZAP für Teams
Defender for Office 365 Plan 2	z. B. Microsoft 365 E5, A5 und G5	alles aus Plan 1, dazu Angriffssimulationstraining, Threat Explorer, automatisierte Untersuchung und Reaktion (AIR), erweiterte Suche

Ihre Lizenzen zeigt das Microsoft 365 Admin Center unter „Ihre Produkte“; im Defender-Portal steht unter E-Mail & Zusammenarbeit bei Plan 1 der Menüpunkt Echtzeiterkennungen, bei Plan 2 Explorer.

Änderungen 2025 und 2026



März 2025

Zulassen direkt in der Liste

Zulassungen für Domänen, Adressen und URLs lassen sich direkt in der Zulassungs-/Sperrliste anlegen.



Jänner 2026

ZAP für Teams in Plan 1

ZAP für Teams und die Verwaltung von Teams-Nachrichten in der Quarantäne gibt es auch in Plan 1.



Mai 2026

RFC 9989 für DMARC

Ersetzt mit RFC 9990 und RFC 9991 (Berichte) den bisherigen RFC 7489. Das Tag **pct** entfällt, eine Testphase kennzeichnet **t=y**.



Juli 2026

E3 mit Plan 1, Prompt-Injection

Microsoft 365 E3 enthält jetzt Plan 1. Plan 2 erkennt versteckte Anweisungen an KI-Assistenten in eingehenden E-Mails als Phishing mit hoher Zuverlässigkeit.

02

Was der integrierte Schutz immer tut

Standardrichtlinien für alle Empfänger und „Secure by Default“ für Schadsoftware und Phishing mit hoher Zuverlässigkeit.

Für Antischadsoftware, Antispam und Antiphishing gibt es Standardrichtlinien. Sie gelten für alle Empfänger, lassen sich nicht abschalten und greifen immer zuletzt; voreingestellte und eigene Richtlinien gehen ihnen vor.

Schadsoftware

Ein Fund in einer Anlage führt zur Quarantäne. Ansehen dürfen standardmäßig nur Administratoren; Benutzer können nie selbst freigeben, höchstens die Freigabe anfordern. Der Filter für allgemeine Anlagen weist die Dateitypen seiner Liste mit Unzustellbarkeitsbericht ab; in der Standardrichtlinie ist er ab Werk eingeschaltet in Mandanten, die nach dem 1. Dezember 2023 angelegt wurden; in älteren Mandanten den Schalter prüfen.

Secure by Default

Schadsoftware und Phishing mit hoher Zuverlässigkeit kommen in die Quarantäne, auch wenn zugelassene Absender oder Domänen, sichere Absender in Outlook, die IP-Zulassungsliste oder Nachrichtenflussregeln sie zulassen würden; bei Phishing mit hoher Zuverlässigkeit bleibt nur die Aktion „Nachricht an E-Mail-Adresse umleiten“ unberührt. Das ist kein Schalter und gilt nur, solange der MX-Eintrag auf Microsoft 365 zeigt. Vorgesehene Ausnahmen: erweiterte Übermittlung für SecOps-Postfächer und Phishing-Simulationen, Einreichungen bei Fehlalarmen.

Spoofingschutz

Spoofintelligenz ist eingeschaltet und erkennt Absender, deren Adresse im Feld „Von“ nicht zur Quelle passt. Microsoft fasst SPF, DKIM und DMARC zur zusammengesetzten Authentifizierung (**compauth**) zusammen; ein Fehlschlag allein blockiert nicht, bewertet wird die Nachricht als Ganzes.

Zero-Hour Auto Purge (ZAP)

Verschiebt bereits zugestellte Nachrichten, die sich nachträglich als Schadsoftware, Phishing oder, solange ungelesen, Spam erweisen, je nach Urteil und Aktion der Richtlinie in die Quarantäne oder den Junk-E-Mail-Ordner; durchsucht werden die letzten 48 Stunden. Benutzer werden nicht benachrichtigt. Für E-Mail ohne Zusatzlizenz, für Teams ab Plan 1.

03

Voreingestellte Richtlinien als Startpunkt

Standard für alle, Streng für besonders gefährdete Personen, integrierter Schutz als Netz für Sichere Links und Sichere Anlagen.

Voreingestellte Sicherheitsrichtlinien setzen die von Microsoft empfohlenen, kaum änderbaren Werte. Microsoft rät, Standard und/oder Streng allen Empfängern zuzuweisen; bis dahin gelten sie für niemanden. Streng ist für besonders gefährdete Personen gedacht („high value targets or priority users“). Den integrierten Schutz erhalten automatisch alle Empfänger ohne andere Richtlinie für Sichere Links und Sichere Anlagen, sobald der Mandant mindestens eine Lizenz für Defender for Office 365 hat; Microsoft empfiehlt Lizenzen für alle Benutzer.

1

Seite öffnen

Microsoft Defender-Portal > E-Mail & Zusammenarbeit > Richtlinien & Regeln > Bedrohungsrichtlinien > Voreingestellte Sicherheitsrichtlinien (security.microsoft.com/presetSecurityPolicies).

2

Standardschutz zuweisen

Schalter auf „Ein“, dann „Schutzeinstellungen verwalten“ und bei „Exchange Online Protection anwenden“ „Alle Empfänger“ wählen. Haben nicht alle Benutzer eine Lizenz, den Schutz durch Defender for Office 365 nur den lizenzierten zuweisen.

3

Identitätswechselschutz befüllen (Plan 1)

Bis zu 350 Personen, die Angreifer imitieren könnten, etwa Geschäftsführung und Finanzleitung, und bis zu 50 fremde Domänen, mit denen Sie oft korrespondieren. Eigene Domänen und die Postfachintelligenz sind automatisch geschützt.

4

Streng ergänzen und prüfen

Gefährdete Personen zusätzlich Streng zuweisen. Test: Spam landet bei Standard im Junk-E-Mail-Ordner, bei Streng in der Quarantäne. Die Richtlinien der Profile nicht per PowerShell ändern; das unterstützt Microsoft nicht.

Steht ein Empfänger in mehreren Richtlinien, wirkt nur die erste in dieser Reihenfolge: Streng, Standard, Evaluierungsrichtlinien von Defender for Office 365, eigene Richtlinien nach Priorität, zuletzt integrierter Schutz und Standardrichtlinien. Ausgehender Spam und der Teams-Schutz gehören nicht zu den Profilen.

04

Einstellungen im Einzelnen

Die Werte der Standardrichtlinie und der Profile Standard und Streng, dazu die Funktionen, die Defender for Office 365 voraussetzen.

Antispam und Antiphishing (Vorgabe = Standardrichtlinie ohne Profil, Junk = Junk-E-Mail-Ordner)

EINSTELLUNG	VORGABE	STANDARD	STRENG
Massen-E-Mail: Schwelle (BCL), Aktion	7, Junk	6, Junk	5, Quarantäne
Spam	Junk	Junk	Quarantäne
Spam mit hoher Zuverlässigkeit	Junk	Quarantäne	Quarantäne
Phishing	Junk	Quarantäne	Quarantäne
Aufbewahrung in der Quarantäne	15 Tage	30 Tage	30 Tage
Spoof laut Spoofintelligenz	Junk	Junk	Quarantäne
DMARC des Absenders: p=quarantine / p=reject	Quarantäne / ablehnen	Quarantäne / ablehnen	Quarantäne / ablehnen
Sicherheitstipp beim ersten Kontakt	aus	ein	ein
Phishing-Schwellenwert (Plan 1)	1	3	4
Identitätswechsel von Benutzern und Domänen (Plan 1)	keine Aktion	Quarantäne	Quarantäne
Identitätswechsel laut Postfachintelligenz (Plan 1)	keine Aktion	Junk	Quarantäne

Bei Phishing gilt Junk für die Standardrichtlinie und per PowerShell angelegte Richtlinien; im Portal neu angelegte Richtlinien stellen Phishing in die Quarantäne. Antischadsoftware, Sichere Anlagen und Sichere Links sind in Standard und Streng gleich eingestellt.

Sichere Links (Plan 1)

Prüft URLs vor der Zustellung, schreibt sie um und prüft beim Klick erneut, auch in Teams und Office-Apps. Standard und Streng: interne Nachrichten eingeschlossen, Zustellung erst nach der Prüfung, kein Durchklicken zur ursprünglichen URL. Der integrierte Schutz erlaubt das Durchklicken, schreibt nicht um und lässt interne Nachrichten aus; ebenso wenig schreiben im Portal neu angelegte eigene Richtlinien standardmäßig um (Abschnitt 07).

Sichere Anlagen (Plan 1)

Öffnet Anlagen vor der Zustellung in einer virtuellen Umgebung, meist binnen 15 Minuten. Empfohlen ist „Blockieren“, Funde kommen in die Quarantäne. Den Schutz für SharePoint, OneDrive und Teams schaltet der integrierte Schutz global ein. Optional lassen sich Nachrichten mit kennwortgeschützten Anlagen, die nicht geprüft werden können, in die Quarantäne stellen; in allen Profilen ist das aus.

Automatische Weiterleitung nach außen

`AutoForwardingMode Off`

Richtlinie für ausgehenden Spam, für alle Lizenzen. Die Vorgabe „Automatisch – systemgesteuert“ verhält sich je Organisation unterschiedlich; Microsoft empfiehlt „Aus – Weiterleitung ist deaktiviert“.

Junk-E-Mail-Filter in Outlook

Microsoft empfiehlt „Keine automatische Filterung“, damit Outlook nicht gegen die Urteile von Microsoft 365 arbeitet.

05

Absenderauthentifizierung der eigenen Domäne

SPF, DKIM und DMARC für jede sendende Domäne, Sperreinträge für jede, die nicht sendet; DKIM für eigene Domänen schalten Sie selbst ein.

Laut Microsoft wirken die Bedrohungsrichtlinien am besten, wenn Ihre Domänen korrekt authentifiziert sind. SPF prüft den Absender im Umschlag (MAIL FROM, RFC 7208), DKIM die Signatur der Domäne im Feld d= (RFC 6376), DMARC, ob eine dieser Domänen zur sichtbaren Absenderdomäne passt (RFC 9989).

DNS: Beispiel mit reservierten Beispieldomänen

```
; Zone example.com: nur Microsoft 365 sendet
@           TXT      "v=spf1 include:spf.protection.outlook.com -all"
selector1._domainkey CNAME <Ziel 1 laut Defender-Portal>
selector2._domainkey CNAME <Ziel 2 laut Defender-Portal>
_dmarc      TXT      "v=DMARC1; p=none; rua=mailto:dmarc@example.com"

; Zone example.net: sendet keine E-Mails
@           TXT      "v=spf1 -all"
_dmarc      TXT      "v=DMARC1; p=reject;"
```

- SPF: höchstens ein Eintrag `v=spf1` je Domäne, mehrere ergeben `permerror` (RFC 7208, Abschnitt 4.5), und höchstens 10 Terme, die DNS-Abfragen auslösen (`include`, `a`, `mx`, `ptr`, `exists`, `redirect`), verschachtelte eingerechnet (Abschnitt 4.6.4). Microsoft empfiehlt `-all` und rät, den `include` von Microsoft nicht durch IP-Adressen zu ersetzen.
- DKIM: Automatisch signiert Microsoft nur E-Mails von Adressen der *.onmicrosoft.com-Domäne; E-Mails eigener Domänen bleiben ohne Einrichtung unsigniert. Dafür unter Bedrohungsrichtlinien > E-Mail-Authentifizierungseinstellungen > DKIM die zwei angezeigten CNAME-Einträge anlegen und „Nachrichten für diese Domäne mit DKIM-Signaturen signieren“ einschalten.
- DKIM-Schlüssel, die per PowerShell angelegt werden, haben 1024 Bit; `Rotate-DkimSigningConfig -KeySize 2048` wechselt bei der Rotation auf 2048 Bit.
- DMARC: beim DNS-Anbieter anlegen und von `p=none` über `p=quarantine` zu `p=reject` verschärfen, Subdomänen mit wenig Verkehr zuerst, die Hauptdomäne zuletzt. Microsofts Beispiele nennen noch `pct`, das RFC 9989 gestrichen hat.
- Ungenutzte Domänen erhalten `v=spf1 -all` und `v=DMARC1; p=reject;`, aber keinen DKIM-Eintrag. Ein ungenutztes *.onmicrosoft.com braucht ebenfalls `p=reject`; den Eintrag legen Sie im Microsoft 365 Admin Center an (Einstellungen > Domänen > DNS-Einträge).
- Für fremde Versanddienste wie Newsletter-Plattformen empfiehlt Microsoft eine Subdomäne wie `marketing.example.com`, mit eigenem SPF und DKIM.

Eingehend berücksichtigt Microsoft 365 die DMARC-Richtlinie fremder Absender („DMARC-Eintragsrichtlinie berücksichtigen“, Vorgabe ein): `p=reject` wird abgelehnt, `p=quarantine` kommt in die Quarantäne. Den Einführungsplan enthält der Download „SPF, DKIM und DMARC in fünf Schritten“.

06

Quarantäne und Meldungen

Quarantänerichtlinien steuern, was Benutzer dürfen und ob sie benachrichtigt werden; gemeldete Nachrichten gehören in ein eigenes Postfach.

Eine Quarantänerichtlinie bündelt Berechtigungen (Kein Zugriff, Eingeschränkter Zugriff, Vollzugriff) und legt fest, ob Benutzer benachrichtigt werden (alle vier Stunden, täglich oder wöchentlich). Standardrichtlinien sind schreibgeschützt; eigene legen Sie unter Bedrohungsrichtlinien > Quarantänerichtlinien an. Eine geänderte Zuweisung wirkt nur für künftig isolierte Nachrichten.

Standard-Quarantänerichtlinien (Microsoft Learn)

RICHTLINIE	BENUTZER DÜRFEN	HINWEIS
<code>AdminOnlyAccessPolicy</code>	nichts, nur Administratoren verwalten (Schadsoftware, Phishing mit hoher Zuverlässigkeit)	nein
<code>DefaultFullAccessPolicy</code>	freigeben, löschen, Vorschau, Absender zulassen	nein
<code>DefaultFullAccessWithNotificationPolicy</code>	wie oben; in Standard und Streng statt der vorigen	ja
<code>NotificationEnabledPolicy</code>	wie oben; nur in manchen älteren Organisationen	ja

- Schadsoftware und Phishing mit hoher Zuverlässigkeit können Benutzer nie selbst freigeben; erlaubt die Quarantänerichtlinie die Freigabe, können sie sie nur anfordern. Die Warnungsrichtlinie „User requested to release a quarantined message“ meldet das der Administration.
- Die Aufbewahrung von 1 bis 30 Tagen regelt die Antispamrichtlinie („Spam so viele Tage in Quarantäne aufbewahren“); sie gilt auch für Antiphishing. Danach ist die Nachricht gelöscht und nicht wiederherstellbar.
- Meldungen: unter Einstellungen > E-Mail & Zusammenarbeit > Vom Benutzer gemeldete Einstellungen „Gemeldete Nachrichten in Outlook überwachen“ mit der integrierten Schaltfläche „Melden“ wählen und ein eigenes Exchange-Online-Postfach eintragen; vorgegeben ist das Postfach des globalen Administrators.
- Das Berichtspostfach als SecOps-Postfach in der erweiterten Übermittlung eintragen und von DLP ausnehmen, sonst werden gemeldete Nachrichten gefiltert. Den Meldenden antworten Sie auf der Seite Einreichungen mit „Als markieren und benachrichtigen“.

07

Zulassen, Sperren und häufige Fehler

Die Mandanten-Zulassungs-/Sperrliste zuerst, Zulassungen nur befristet, und die typischen Fehler, die den Schutz aushebeln.

Microsoft reiht die Wege, Absender zuzulassen, vom meistempfohlenen an: Mandanten-Zulassungs-/Sperrliste, Nachrichtenflussregeln, sichere Absender in Outlook, IP-Zulassungsliste, Zulassungslisten in Antispamrichtlinien. In der Liste gehen Sperren vor; gesperrte Domänen, Adressen und URLs gelten als Phishing mit hoher Zuverlässigkeit. Direkte Zulassungen wirken nur gegen die Urteile Massen-E-Mail, Spam, Spam mit hoher Zuverlässigkeit und Phishing, gegen Schadsoftware und Phishing mit hoher Zuverlässigkeit nur über die Seite Einreichungen; unnötige Zulassungen entfernt Microsoft selbst.

Häufige Fehler laut Microsoft Learn

Transportregel nur mit Absenderdomäne

Eine Nachrichtenflussregel, die die Spamfilterung (SCL -1) allein anhand der Absenderdomäne umgeht, erhöht laut Microsoft deutlich das Risiko, dass gefälschte Absender ungefiltert ankommen. Microsoft sieht zusätzlich `dmarc=pass` oder `dmarc=bestguesspass` in der Kopfzeile `Authentication-Results` oder eine eng gefasste IP-Zulassung vor und rät von eigenen und verbreiteten Domänen als Bedingung ab.

Zugelassene Domänen in Antispam

Laut Microsoft „a bad idea“: Absender umgehen fast alle Filter samt SPF, DKIM und DMARC. Höchstens befristet zum Testen, nie für verbreitete Domänen wie microsoft.com.

Simulationen per Regel freigeschaltet

Für Phishing-Simulationen von Drittanbietern und SecOps-Postfächer ist die Richtlinie für erweiterte Übermittlung vorgesehen, keine Nachrichtenflussregel und keine URL-Zulassung.

Fremdfilter vor Microsoft 365

Zeigt der MX-Eintrag auf einen anderen Dienst, gilt Secure by Default nicht, und die DMARC-Richtlinie des Absenders wirkt nur mit erweiterter Filterung für Connectors. Diese aktivieren, statt den Spoofingschutz abzuschalten.

Sichere Links aufgeweicht

Im Portal neu angelegte eigene Richtlinien schreiben standardmäßig nicht um und erlauben das Durchklicken; beide Häkchen bewusst setzen bzw. entfernen. Nur Prüfung per API heißt: später scharf geschaltete Links in Clients ohne diese Schnittstelle unerkant bleiben; zu breite Einträge in „Folgende URLs nicht umschreiben“: `*contoso.com*` erfasst auch Betrugsdomänen wie `falsecontoso.com`, `*.contoso.com/*` nicht.

08

Checkliste zum Abhaken

Die Punkte in der Reihenfolge, die TOMORIS empfiehlt, mit der Konfigurationsanalyse als Kontrolle.

Die Konfigurationsanalyse (Bedrohungsrichtlinien > Konfigurationsanalyse) vergleicht eigene Richtlinien mit Standard und Streng, prüft SPF- und DKIM-Einträge im DNS und zeigt Änderungen der letzten 90 Tage.

- ☐ Lizenzen geklärt; Schutz durch Defender for Office 365 nur lizenzierten Benutzern zugewiesen.
- ☐ Jede sendende Domäne mit SPF (`-all`), DKIM mit eigener Domäne und DMARC mit Berichtsadresse; Ziel `p=reject`.
- ☐ Domänen ohne Versand mit `v=spf1 -all` und `p=reject` gesperrt, auch ein ungenutztes `*.onmicrosoft.com` per DMARC.
- ☐ Profil Standard für alle Empfänger, Streng für besonders gefährdete Personen.
- ☐ Identitätswechselschutz mit Führungskräften und wichtigen Partnerdomänen befüllt (Plan 1).
- ☐ Integrierter Schutz ohne Ausnahmen für lizenzierte Benutzer (Plan 1); Filter für allgemeine Anlagen eingeschaltet.
- ☐ Automatische Weiterleitung nach außen aus; begründete Ausnahmen in eigener Richtlinie.
- ☐ Junk-E-Mail-Filter in Outlook auf „Keine automatische Filterung“.
- ☐ Quarantäne mit Benachrichtigung, Freigabebeanforderungen werden bearbeitet; „Melden“ aktiv, Berichtspostfach als SecOps-Postfach.
- ☐ Zulassungen nur befristet in der Mandanten-Zulassungs-/Sperrliste; Zulassungslisten in Antispam leer.
- ☐ Keine Nachrichtenflussregel umgeht die Spamfilterung nur anhand der Absenderdomäne.
- ☐ Konfigurationsanalyse ohne offene Empfehlungen.

Die Checkliste ist eine Empfehlung von TOMORIS nach den Empfehlungen von Microsoft. Wesentliche und wichtige Einrichtungen müssen seit 1. Oktober 2026 geeignete und verhältnismäßige Risikomanagementmaßnahmen umsetzen, die unter Berücksichtigung des Stands der Technik ein dem Risiko angemessenes Cybersicherheitsniveau gewährleisten (§ 32 Abs. 1 und 2 NISG 2026). Nach § 2 NISV 2026 gilt dafür der Anhang der DVO (EU) 2024/2690, darunter ein Durchführungsplan für moderne E-Mail-Kommunikationsnormen (Nr. 6.7.2 lit. k) und Schutz vor Schadsoftware (Nr. 6.9); welche Einstellungen das konkret erfordert, ergibt die eigene Risikoanalyse.

NÄCHSTER SCHRITT

Selbst prüfen oder gemeinsam umsetzen

KOSTENLOS PRÜFEN

E-Mail-Sicherheits-Check

tomoris.com/tools/email-security-check

Microsoft-365-Domain-Check

tomoris.com/tools/microsoft-365-check

UMSETZUNG BESPRECHEN

Kontakt aufnehmen

tomoris.com/contact

contact@tomoris.com

09

Quellen

Alle Aussagen sind belegt. Gesetzestexte gelten in der jeweils geltenden Fassung.

- 1 **Microsoft Learn: Integrierte Sicherheitsfeatures**
Funktionsweise, Funktionen; 25.10.2026
learn.microsoft.com/de-de/defender-office-365/eop-about
- 2 **Microsoft Learn: Microsoft Defender für Office 365**
Schutzleiter, Plan 1 und Plan 2; 25.10.2026
learn.microsoft.com/de-de/defender-office-365/mdo-about
- 3 **Microsoft Learn: Neuerungen in Defender für Office 365**
März 2025 bis Oktober 2026; 25.10.2026
learn.microsoft.com/de-de/defender-office-365/defender-for-offi...
- 4 **Microsoft Learn: Voreingestellte Sicherheitsrichtlinien**
Zuweisung, Profile, Rangfolge; 25.10.2026
learn.microsoft.com/de-de/defender-office-365/preset-security-p...
- 5 **Microsoft Learn: Empfohlene Sicherheitseinstellungen**
Vorgabe, Standard, Streng, integrierter Schutz; 25.10.2026
learn.microsoft.com/de-de/defender-office-365/recommended-setti...
- 6 **Microsoft Learn: Standardmäßig sicher**
Überschreibungen, Ausnahmen; 25.10.2026
learn.microsoft.com/de-de/defender-office-365/secure-by-default
- 7 **Microsoft Learn: Antispamschutz**
Urteile, Aktionen, Aufbewahrung; 25.10.2026
learn.microsoft.com/de-de/defender-office-365/anti-spam-protect...
- 8 **Microsoft Learn: Antiphishingrichtlinien**
Spoofing, DMARC, Identitätswechsel; 25.10.2026
learn.microsoft.com/de-de/defender-office-365/anti-phishing-pol...
- 9 **Microsoft Learn: Sichere Links**
E-Mail, Teams, Office-Apps, Ausnahmen; 25.10.2026
learn.microsoft.com/de-de/defender-office-365/safe-links-about
- 10 **Microsoft Learn: Sichere Anlagen**
Aktionen, kennwortgeschützte Anlagen; 25.10.2026
learn.microsoft.com/de-de/defender-office-365/safe-attachments-...
- 11 **Microsoft Learn: Zero-Hour Auto Purge**
E-Mail, Teams, Lizenzen; 25.10.2026
learn.microsoft.com/de-de/defender-office-365/zero-hour-auto-pu...
- 12 **Microsoft Learn: Quarantänerichtlinien**
Standardrichtlinien, Berechtigungen; 25.10.2026
learn.microsoft.com/de-de/defender-office-365/quarantine-polic...
- 13 **Microsoft Learn: Vom Benutzer gemeldete Einstellungen**
Berichtspostfach, Ziele; 25.10.2026
learn.microsoft.com/de-de/defender-office-365/submissions-user-...
- 14 **Microsoft Learn: Mandanten-Zulassungs-/Sperrliste**
Sperr- und Zulassungseinträge; 25.10.2026
learn.microsoft.com/de-de/defender-office-365/tenant-allow-bloc...
- 15 **Microsoft Learn: Zulassungslisten erstellen**
Methoden, Nachrichtenflussregeln; 25.10.2026
learn.microsoft.com/de-de/defender-office-365/create-safe-sende...
- 16 **Microsoft Learn: Konfigurationsanalyse**
Empfehlungen, Driftanalyse; 25.10.2026
learn.microsoft.com/de-de/defender-office-365/configuration-ana...

- 17 Microsoft Learn: Prompt-Injection-Schutz**
Plan 2, Urteil, Erkennung; 25.10.2026
learn.microsoft.com/de-de/defender-office-365/step-by-step-guid...
- 19 Microsoft Learn: DKIM einrichten**
CNAME, Einschalten, Schlüssellänge; 25.10.2026
learn.microsoft.com/de-de/defender-office-365/email-authenticat...
- 21 RFC 7208: Sender Policy Framework (SPF)**
Abschnitte 4.5 und 4.6.4
www.rfc-editor.org/rfc/rfc7208
- 23 RFC 9989: DMARC (Mai 2026, Standards Track)**
Abschnitte 4.1 und 4.7 (Tag t), Anhang A.6
www.rfc-editor.org/rfc/rfc9989
- 25 NISG 2026, BGBl. I Nr. 94/2025 (RIS)**
§ 32 Abs. 1 und 2, § 51 Abs. 2; Fassung vom 25.10.2026
www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gese...
- 27 Durchführungsverordnung (EU) 2024/2690, Anhang**
Nr. 6.7.2 lit. k und 6.9; nach § 2 NISV 2026 anwendbar
eur-lex.europa.eu/eli/reg_impl/2024/2690/oj/deu
- 18 Microsoft Learn: SPF einrichten**
Syntax, geparkte Domänen, Flattening; 25.10.2026
learn.microsoft.com/de-de/defender-office-365/email-authenticat...
- 20 Microsoft Learn: DMARC einrichten**
Stufen, *.onmicrosoft.com, Parken; 25.10.2026
learn.microsoft.com/de-de/defender-office-365/email-authenticat...
- 22 RFC 6376: DKIM Signatures**
Abschnitt 3.6.2.1
www.rfc-editor.org/rfc/rfc6376
- 24 RFC 7489: DMARC (2015, Informational)**
laut RFC Editor obsolet, ersetzt durch RFC 9989, 9990 und 9991
www.rfc-editor.org/rfc/rfc7489
- 26 NISV 2026, BGBl. II Nr. 290/2026 (RIS)**
§ 2; kundgemacht am 1.10.2026
www.ris.bka.gv.at/eli/bgbl/II/2026/290