Microsoft Cloud Hardening Report

Anonymisierte Kurzfassung

Oktober 2026

Aaron Siller - siller.consulting GmbH

INHALT

01 **Management Summary**

02 **Einführung und Vorwort**

03 **So priorisieren wir**

04 **Entra ID**
7 Prio 1 · 38 Prio 2

05 **Defender XDR**
3 Prio 1 · 20 Prio 2

06 **Exchange Online**
2 Prio 1 · 7 Prio 2

07 **SharePoint & OneDrive**
1 Prio 1 · 7 Prio 2

08 **Teams**
1 Prio 1 · 14 Prio 2

09 **Intune**
15 Prio 2

10 **Purview**
6 Prio 2

11 **Microsoft 365 Admin Center**
5 Prio 2

12 **Schlussfolgerung**

01

Management Summary

Die Analyse des Microsoft 365 Tenants des untersuchten Unternehmens ergibt einen Reifegrad, der als **kritisch** eingestuft wird. Von 340 geprüften Sicherheitskonfigurationen sind 181 konform. Daraus ergeben sich 14 kritische Feststellungen (Prio 1) und 112 Optimierungen (Prio 2). Wie die Prioritäten zustande kommen, erläutert der Abschnitt „So priorisieren wir“.

340
GEPRÜFTE KONFIGURATIONEN

181
DAVON KONFORM

14
KRITISCH (PRIO 1)

112
OPTIMIERUNG (PRIO 2)



181
KONFORM

340
GEPRÜFT

340 PRÜFUNGEN

181 konform · 53 % | **159 nicht konform**

DIE 159 NICHT KONFORMEN PRÜFUNGEN ERGEBEN 126 FESTSTELLUNGEN

14 Prio 1 | **112 Prio 2 · Optimierung**

Mehrere nicht konforme Prüfungen können dieselbe Ursache haben und werden dann zu einer Feststellung zusammengefasst.

Die fünf dringendsten Maßnahmen

1

1. Admin-Konten aus den MFA-Ausnahmen entfernen

(MS365-273) · Kontoübernahme

Die Globalen Administratoren Admin-Konto A und Admin-Konto B (IT-Dienstleister) sind von allen drei MFA-Richtlinien ausgenommen (MFA für alle Benutzer, MFA für Admin-Portale, phishing-resistente MFA für Admins), ohne dass eine andere Richtlinie sie erfasst. **Maßnahme:** Ausnahmen der Admin-Konten aus den MFA-Richtlinien entfernen; nur dokumentierte Notfallkonten bleiben ausgenommen, Dienstkonten erhalten eine eigene Ersatzrichtlinie

2

2. Anzahl der Global Administratoren auf zwei bis vier reduzieren

(MS365-006) · Kontoübernahme

Sechs Konten sind dauerhaft Global Administrator: das Assessment-Konto (nach Abschluss entfernen), Admin-Konto A, Admin-Konto C, Admin-Konto D, Admin-Konto B (IT-Dienstleister) und Configuration AADConnect User. **Maßnahme:** Global Admins auf zwei bis vier begrenzen, Assessment-Konto entfernen, Configuration AADConnect User auf die Rolle Hybrid Identity Administrator zurückstufen

3

3. User Consent für Apps deaktivieren, nur Admin Consent zulassen

(MS365-027) · Kontoübernahme

Wenn Benutzer eigenständig App-Berechtigungen (Consent) erteilen können, ist dies ein häufiger Angriffsvektor (Consent Phishing / Illicit Consent Grant). **Maßnahme:** User Consent auf ‘Do not allow user consent’ setzen

4

4. SMTP AUTH deaktivieren

(MS365-107) · Kontoübernahme

SMTP AUTH ist organisationsweit oder für einzelne Postfächer aktiv. **Maßnahme:** SMTP AUTH organisationsweit abschalten, Ausnahmen nur für dokumentierte Service-Postfächer mit OAuth

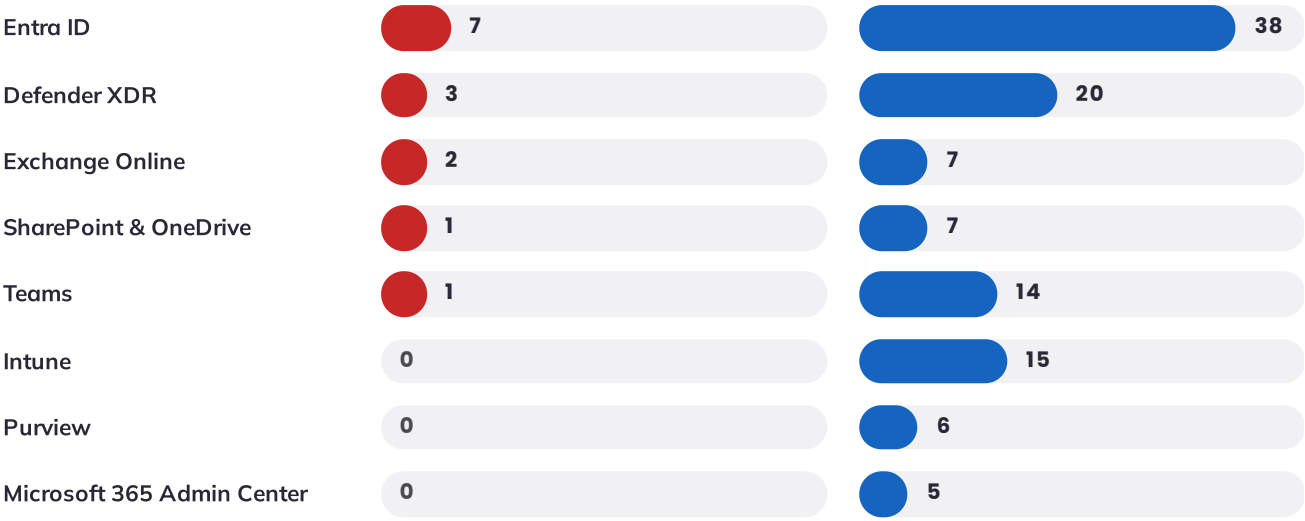
5

5. Device Code Flow per Conditional Access blockieren

(MS365-072) · Kontoübernahme

Der Device Code Flow ermöglicht Authentifizierung über https://microsoft.com/devicelogin und wird aktiv für Device Code Phishing missbraucht. **Maßnahme:** Device Code Flow per Conditional Access blockieren

Bewertung je Bereich



Entra ID

KRITISCHER HANDLUNGSBEDARF

7 kritische Findings erfordern sofortigen Handlungsbedarf. Zusätzlich 38 Optimierungen empfohlen.

Defender XDR

KRITISCHER HANDLUNGSBEDARF

3 kritische Findings erfordern sofortigen Handlungsbedarf. Zusätzlich 20 Optimierungen empfohlen.

Exchange Online

KRITISCHER HANDLUNGSBEDARF

2 kritische Findings erfordern sofortigen Handlungsbedarf. Zusätzlich 7 Optimierungen empfohlen.

SharePoint & OneDrive

KRITISCHER HANDLUNGSBEDARF

1 kritisches Finding erfordert sofortigen Handlungsbedarf. Zusätzlich 7 Optimierungen empfohlen.

Teams

KRITISCHER HANDLUNGSBEDARF

1 kritisches Finding erfordert sofortigen Handlungsbedarf. Zusätzlich 14 Optimierungen empfohlen.

Intune

OPTIMIERUNGSBEDARF

Grundlegende Konfiguration vorhanden, 15 Optimierungen empfohlen.

Purview

OPTIMIERUNGSBEDARF

Grundlegende Konfiguration vorhanden, 6 Optimierungen empfohlen.

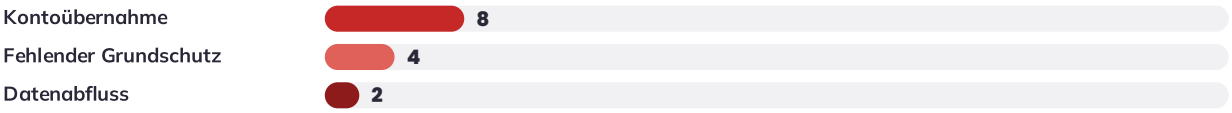
Microsoft 365 Admin Center

OPTIMIERUNGSBEDARF

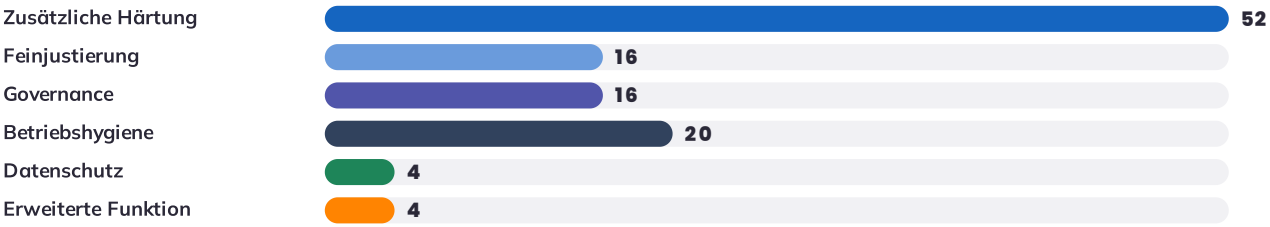
Grundlegende Konfiguration vorhanden, 5 Optimierungen empfohlen.

Feststellungen nach Begründung

PRIO 1 · KRITISCH



PRIO 2 · OPTIMIERUNG



Die Begründungen sind im Abschnitt „So priorisieren wir“ erläutert.

02

Einführung und Vorwort

Das vorliegende Dokument bietet auf Basis der durchgeführten Analyse eine Übersicht, Bewertung und Handlungsempfehlung zur aktuellen Microsoft Cloud Infrastruktur des untersuchten Unternehmens.

Im Kern wurden Microsoft 365 und die dazugehörigen Sicherheitskomponenten auf ihre bestehende Konfiguration hin untersucht. Der Bericht ist nach den Admin Centern gegliedert, in denen die jeweilige Einstellung liegt. So findet die IT jede Maßnahme dort, wo sie umgesetzt wird:

ABSCHNITT	ADMIN CENTER
Entra ID	Microsoft Entra Admin Center
Defender XDR	Microsoft Defender Portal
Exchange Online	Exchange Admin Center
SharePoint & OneDrive	SharePoint Admin Center
Teams	Microsoft Teams Admin Center
Intune	Microsoft Intune Admin Center
Purview	Microsoft Purview Portal
Microsoft 365 Admin Center	Microsoft 365 Admin Center

Die einzelnen Admin Center und die darin enthaltenen Dienste wurden auf ihre aktuelle Konfiguration hin überprüft und, soweit erforderlich, mit Handlungsempfehlungen und Priorisierung versehen. Wie die Prioritäten zustande kommen, beschreibt der folgende Abschnitt.

Aufgrund der starken Verzahnung der einzelnen Microsoft 365- und Cloud-Dienste sind viele konfigurierbare Optionen mehrfach vorhanden. Im Bericht wird der jeweilige Dienst nur einmal aufgeführt und gilt für den gesamten Microsoft Cloud Tenant.

Services, die bereits korrekt konfiguriert sind und keiner weiteren Betrachtung bedürfen, werden nicht gesondert aufgelistet.

Zu dieser Fassung

Dies ist eine anonymisierte Kurzfassung eines realen Kundenberichts. Alle 14 kritischen Feststellungen (Prio 1) sind vollständig enthalten, mit Befund, Begründung, Klickpfad und Rechtsbezug. Die 112 Optimierungen (Prio 2) sind je Bereich als Übersicht zusammengefasst.

Unternehmens-, Personen-, Konto- und Domänennamen sind durch neutrale Bezeichnungen ersetzt (zum Beispiel „Admin-Konto A“), das Messdatum ist entfernt. Umsetzungsskripte und die ausführliche Darstellung der Optimierungen sind der Vollfassung vorbehalten.

03

So priorisieren wir

Jede Feststellung erhält eine von zwei Prioritäten und eine kurze Begründung, warum sie so eingestuft ist. Maßgeblich ist, was die jeweilige Prüfung in Ihrem Tenant konkret festgestellt hat, nicht das Themenfeld. Dieselbe Begründung steht bei jeder Feststellung neben der Priorität.

PRIORITÄT 1 · KRITISCH:

Eine Lücke, die ein Angreifer ohne weitere Fehlkonfiguration ausnutzen kann, oder über die Daten das Unternehmen unkontrolliert verlassen. Diese Punkte sollten zeitnah umgesetzt werden.

BEGRÜNDUNG	BEDEUTUNG
Kontoübernahme	Angreifer können Benutzer- oder Administratorkonten übernehmen oder sich höhere Rechte verschaffen, etwa weil MFA fehlt oder alte Anmeldeverfahren offen sind.
Datenabfluss	Unternehmensdaten können das Unternehmen ohne wirksame Kontrolle verlassen, zum Beispiel über anonyme Freigabelinks oder automatische Weiterleitungen.
Fehlender Grundschutz	Der Schutz gegen die häufigsten Angriffswege (Phishing, Schadsoftware, gefälschte Absender) fehlt oder ist abgeschaltet.
Fehlende Protokollierung	Unified Audit Log oder Postfach-Auditing sind abgeschaltet. Bei einem Sicherheitsvorfall fehlen die Protokolle, um ihn aufzuklären und die Meldepflichten nach DSGVO und NIS2 zu erfüllen.
Besitzerlose Gruppen	Microsoft-365-Gruppen und Teams ohne Besitzer: Niemand pflegt Mitglieder, Gäste und Freigaben, Zugriffe bleiben unkontrolliert bestehen.

PRIORITÄT 2 · OPTIMIERUNG:

Die Grundabsicherung ist vorhanden. Die Maßnahme erhöht das Sicherheitsniveau weiter oder verbessert Betrieb und Nachweisführung. Umsetzung nach den kritischen Punkten, planbar im Regelbetrieb.

BEGRÜNDUNG	BEDEUTUNG
Zusätzliche Härtung	Eine weitere Schutzschicht neben dem vorhandenen Grundschutz, die Angriffe zusätzlich erschwert.

BEGRÜNDUNG	BEDEUTUNG
Feinjustierung	Eine vorhandene Einstellung wird auf den empfohlenen Wert angepasst, etwa Schwellenwert, Dauer oder Aktion.
Governance	Regelmäßige Überprüfung und klare Abläufe für Konten, Gäste und Berechtigungen.
Betriebshygiene	Benachrichtigungen, Aufräumen und Pflege, damit Probleme früh auffallen.
Datenschutz	Einstellungen, die die Datenverarbeitung durch Microsoft-Dienste oder Auswertungen über Mitarbeitende begrenzen.
Erweiterte Funktion	Ein zusätzlicher Schutzbaustein, der eine weitere Lizenz oder ein Einführungsprojekt voraussetzt.

04

/Entra ID

Microsoft Entra Admin Center · https://entra.microsoft.com

7

PRIO 1 · KRITISCH

38

PRIO 2 · OPTIMIERUNG

Was ist Entra ID?

Im Microsoft Entra Admin Center liegen Identitäten, Anmeldung und Zugriffssteuerung: Benutzer, Gruppen, Gäste, Administratorrollen, Authentifizierungsmethoden, Conditional Access, Identity Protection und Global Secure Access.

Rolle in der Microsoft 365 Architektur

Jeder Zugriff auf Exchange, SharePoint, Teams oder Defender läuft über eine Anmeldung in Entra ID. Schwächen hier wirken auf alle nachgelagerten Dienste.

Abhängigkeiten zu anderen Diensten

- Conditional Access nutzt Entra ID-Signale für Zugriffsentscheidungen
- Intune prüft Geräte-Compliance über Entra ID-registrierte Devices
- Purview Sensitivity Labels werden über Entra ID-Gruppenmitgliedschaften gesteuert
- Conditional Access basiert auf Entra ID-Signalen (Benutzer, Gruppen, Rollen)

Schlüsselkonzepte

- **Privileged Identity Management (PIM):** PIM stellt sicher, dass Admin-Rollen nicht dauerhaft zugewiesen sind, sondern nur bei Bedarf aktiviert werden (Just-in-Time Access). Das reduziert die Angriffsfläche durch stehende Berechtigungen erheblich.
- **Identity Protection:** Identity Protection erkennt riskante Anmeldeversuche und kompromittierte Identitäten anhand von Microsoft-Threat-Intelligence-Signalen. Risikostufen (niedrig, mittel, hoch) können automatisierte Reaktionen wie MFA-Challenges oder Passwort-Resets auslösen.
- **Multi-Faktor-Authentifizierung (MFA):** MFA erfordert neben dem Passwort einen zweiten Faktor (Authenticator App, FIDO2-Key, Telefon). Ohne MFA-Enforcement sind Passwort-Spray und Credential-Stuffing die häufigsten erfolgreichen Angriffsvektoren auf M365 Tenants.
- **Zero Trust Enforcement:** Conditional Access setzt das Zero-Trust-Prinzip „Never trust, always verify" technisch um. Jeder Zugriff wird anhand von Signalen bewertet - es gibt kein implizites Vertrauen basierend auf Netzwerk oder Gerät.

Einordnung für Entscheider

Dieser Bereich weist 7 kritische Sicherheitslücken auf. Zusätzlich wurden 38 Optimierungspotenziale identifiziert. Bei Nicht-Umsetzung bestehen unmittelbare Risiken für die Vertraulichkeit und Integrität der Unternehmensdaten. Die Geschäftsführung sollte die Umsetzung der Sofortmaßnahmen in diesem Bereich persönlich nachverfolgen.

KRITIKALITÄT:	Hoch
COMPLIANCE-RELEVANZ:	Direkte Auswirkung auf DSGVO Art. 32 (Zugangssteuerung) und § 30 Abs. 2 Nr. 9 und 10 BSIG (Zugriffskontrolle, MFA)
BETRIEBLICHE AUSWIRKUNG:	Kompromittierte Identitäten betreffen alle verbundenen Dienste und können den gesamten Tenant lahmlegen

Handlungsempfehlung zu Entra ID

Im Rahmen der Analyse sind die folgenden kritischen Konfigurationsabweichungen aufgefallen, die zeitnah adressiert werden müssen:

MS365-273 PRIO 1 Kontoübernahme

Admin-Konten aus den MFA-Ausnahmen entfernen

1. Befund:

Die Prüfung „Alle ausgeschlossenen Objekte haben Fallback-Include“ ist nicht erfüllt.

Conditional Access Policies arbeiten mit Include- und Exclude-Logik. Ein Benutzer, der aus einer Richtlinie ausgeschlossen wird, sollte idealerweise durch eine andere Richtlinie abgedeckt sein. Andernfalls entsteht eine Lücke, in der der Benutzer keiner Zugriffskontrolle unterliegt.

Gemessen im Tenant:

OBJEKT	AUSGENOMMEN IN RICHTLINIE
Admin-Konto A	CA Only Managed Devices; Microsoft-managed: Multifactor authentication for admins accessing Microsoft Admin Portals; Microsoft-managed: Require phishing-resistant multifactor authentication for admins; Multi-Faktor-Authentifizierung für alle Benutzer erfordern
Admin-Konto D	CA Only Managed Devices; Microsoft-managed: Multifactor authentication for admins accessing Microsoft Admin Portals; Microsoft-managed: Require phishing-resistant multifactor authentication for admins; Multi-Faktor-Authentifizierung für alle Benutzer erfordern
Admin-Konto C	CA Only Managed Devices; Multi-Faktor-Authentifizierung für alle Benutzer erfordern
Admin-Konto B (IT-Dienstleister)	CA Only Managed Devices; Microsoft-managed: Multifactor authentication for admins accessing Microsoft Admin Portals; Microsoft-managed: Require phishing-resistant multifactor authentication for admins; Multi-Faktor-Authentifizierung für alle Benutzer erfordern
Admin-Konto E (externer Dienstleister)	Microsoft-managed: Multifactor authentication for admins accessing Microsoft Admin Portals; Microsoft-managed: Require phishing-resistant multifactor authentication for admins; Multi-Faktor-Authentifizierung für alle Benutzer erfordern
Dienstkonto Scanner	Microsoft-managed: Block legacy authentication; Multi-Faktor-Authentifizierung für alle Benutzer erfordern
Dienstkonto Automatisierung	Multi-Faktor-Authentifizierung für alle Benutzer erfordern
Funktionskonto Abteilung	Multi-Faktor-Authentifizierung für alle Benutzer erfordern
Raumkonto	Multi-Faktor-Authentifizierung für alle Benutzer erfordern
Dienstkonto Drucker	Multi-Faktor-Authentifizierung für alle Benutzer erfordern
Plattform: windows	CA Only Managed Devices

2. Warum kritisch?

Die Globalen Administratoren Admin-Konto A und Admin-Konto B (IT-Dienstleister) sind von allen drei MFA-Richtlinien ausgenommen (MFA für alle Benutzer, MFA für Admin-Portale, phishing-resistente MFA für Admins), ohne dass eine andere Richtlinie sie erfasst. Conditional Access erzwingt für diese Konten keine MFA. Gleiches gilt für Admin-Konto D

(als Notfallkonto erkannt) und Admin-Konto E (externer Dienstleister); Admin-Konto C ist von der Richtlinie für alle Benutzer ausgenommen. Von der MFA-Richtlinie für alle Benutzer sind außerdem Dienstkonto Scanner, Dienstkonto Automatisierung, Funktionskonto Abteilung, Raumkonto und Dienstkonto Drucker ausgenommen.

CA-Ausschlüsse ohne Fallback-Include schaffen „blinde Flecken" im Sicherheitskonzept. Angreifer, die ein ausgeschlossenes Konto kompromittieren, umgehen sämtliche Conditional-Access-Kontrollen.

> SZENARIO: *Ein Service Account wird aus der MFA-Richtlinie ausgeschlossen, aber in keiner alternativen Richtlinie erfasst. Ein Angreifer erlangt die Zugangsdaten dieses Service Accounts und meldet sich ohne MFA und ohne jegliche CA-Kontrolle an.*

3. Wie zu schließen:

Ausnahmen der Admin-Konten aus den MFA-Richtlinien entfernen; nur dokumentierte Notfallkonten bleiben ausgenommen, Dienstkonten erhalten eine eigene Ersatzrichtlinie

Klickpfad:

1. Microsoft Entra Admin Center (entra.microsoft.com) mit mindestens der Rolle Conditional Access Administrator öffnen
2. Erhebung: Entra ID → Conditional Access → Policies → je aktiver Richtlinie die Ausschlüsse notieren (Users/Groups/Roles, Target resources, Network, Device platforms); die betroffenen Objekte stehen im Prüfergebnis
3. Je Ausschluss klären, warum er besteht und welche Kontrolle stattdessen für dieses Objekt gelten soll
4. Ergänzende Richtlinie anlegen, die das ausgeschlossene Objekt ausdrücklich einschließt (Muster laut Microsoft: Richtlinie A gilt für eine Gruppe, Richtlinie B 'Include All users / Exclude <gruppe>' regelt alle übrigen), z. B. ausgeschlossenes Dienstkonto nur aus festem Netz, ausgeschlossene Plattform blockieren
5. Nicht mehr benötigte Ausschlüsse entfernen statt sie abzusichern
6. Notfallkonten bleiben ohne Fallback-Include und werden in keine einschränkende Richtlinie aufgenommen; sie sind über phishing-resistente Anmeldemethoden (Passkey/FIDO2) und die Überwachung ihrer Anmeldungen abzusichern, die Ausnahme wird dokumentiert
7. Neue ergänzende Richtlinien zuerst im Modus Report-only testen und mit dem What If-Werkzeug (Entra ID → Conditional Access → Policies → What If) gegenprüfen

MICROSOFT-DOKUMENTATION: https://learn.microsoft.com/en-us/entra/identity/conditional-access/plan-conditional-access, https://learn.microsoft.com/en-us/entra/identity/conditional-access/what-if-tool, https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/security-emergency-access

4. Warum relevant für DSGVO, NIS2 und ISO 27001:

Jeder Ausschluss ohne Ersatzregel ist eine Lücke, in der für das betroffene Konto oder Gerät keine Kontrolle greift. Eine lückenlose Abdeckung unterstützt die Zugriffskontrolle nach NIS2 und trägt dazu bei, dass der Zugang zu personenbezogenen Daten angemessen geschützt bleibt.

Art. 32 Abs. 1 lit. b DSGVO:	Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme
§ 30 Abs. 2 Nr. 9 BSIG (Art. 21 Abs. 2 lit. i NIS2):	Personalsicherheit, Zugriffskontrolle und Management von Anlagen
ISO/IEC 27001 A.5.15:	Zugangssteuerung

ISO/IEC 27001 A.8.9:	Konfigurationsmanagement

MS365-006 PRIO 1 Kontoübernahme

Anzahl der Global Administratoren auf zwei bis vier reduzieren

1. Befund:

Die Prüfung „Maximale Anzahl Globaler Administratoren (2-5)“ ist nicht erfüllt.

Der Global Administrator ist die mächtigste Rolle in Microsoft 365 mit uneingeschränktem Zugriff auf alle Dienste und Einstellungen. Microsoft empfiehlt 2-5 Global Admins - genug für Redundanz, aber wenig genug für Kontrolle. Break-Glass-Accounts zählen separat und dienen nur für Notfälle.

2. Warum kritisch?

Sechs Konten sind dauerhaft Global Administrator: das Assessment-Konto (nach Abschluss entfernen), Admin-Konto A, Admin-Konto C, Admin-Konto D, Admin-Konto B (IT-Dienstleister) und Configuration AADConnect User. Auch ohne das Assessment-Konto bleiben fünf, CIS empfiehlt höchstens vier. Jeder Global Admin kann den gesamten Tenant verändern.

Jeder zusätzliche Global Admin vergrößert die Angriffsfläche linear. Bei zu vielen Admins verliert die Organisation den Überblick, wer wann welche Änderungen vornimmt. Gleichzeitig muss mindestens ein zweiter Admin verfügbar sein, falls der primäre Account gesperrt wird.

> SZENARIO: *Ein Angreifer scannt den Tenant auf Global Admin-Accounts und findet 12 Konten mit dieser Rolle. Er startet gezielte Spear-Phishing-Kampagnen gegen alle 12 und kompromittiert eines davon. Mit nur 3 Global Admins hätte er deutlich weniger Angriffsfläche gehabt.*

3. Wie zu schließen:

Global Admins auf zwei bis vier begrenzen, Assessment-Konto entfernen, Configuration AADConnect User auf die Rolle Hybrid Identity Administrator zurückstufen

Klickpfad:

1. Microsoft Entra Admin Center (entra.microsoft.com) mit mindestens der Rolle Privileged Role Administrator öffnen
2. Entra ID → Roles & admins → Global Administrator → Assignments: alle aktiven und berechtigten Zuweisungen erfassen (Grundgesamtheit inkl. Notfallkonten notieren)
3. Zielbild festlegen: zwei cloud-only Notfallkonten mit dauerhafter Global-Administrator-Zuweisung, dazu weniger als fünf persönliche Global Administratoren
4. Für jede überzählige Person die passende Fachrolle zuweisen (z. B. Exchange Administrator, SharePoint Administrator, Security Administrator, User Administrator): Entra ID → Roles & admins → Rolle → Add assignments
5. Danach die Global-Administrator-Zuweisung dieser Person entfernen: Entra ID → Roles & admins → Global Administrator → Assignments → Eintrag markieren → Remove assignments

6. Mit Entra ID P2: ID Governance → Privileged Identity Management → Microsoft Entra roles → Alerts → ‘There are too many Global Administrators’ prüfen und Schwellwert in Setting hinterlegen

MICROSOFT-DOKUMENTATION: https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/best-practices, https://learn.microsoft.com/en-us/graph/api/rbacapplication-list-roleassignments?view=graph-rest-1.0, https://learn.microsoft.com/en-us/graph/api/rbacapplication-post-roleassignments?view=graph-rest-1.0, https://learn.microsoft.com/en-us/graph/api/unifiedroleassignment-delete?view=graph-rest-1.0, https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-how-to-configure-security-alerts

4. Warum relevant für DSGVO, NIS2 und ISO 27001:

Jeder zusätzliche Global Administrator ist ein weiteres Konto, über das der gesamte Tenant übernommen werden kann. Eine kleine, begründete Zahl unterstützt das Prinzip der minimalen Rechte und die Zugriffskontrolle nach § 30 Abs. 2 Nr. 9 BSIG; fachbezogene Rollen begrenzen den Schaden einer Kontoübernahme in der Regel deutlich.

Art. 32 Abs. 1 lit. b DSGVO:	Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme
§ 30 Abs. 2 Nr. 9 BSIG (Art. 21 Abs. 2 lit. i NIS2):	Personalsicherheit, Zugriffskontrolle und Management von Anlagen
ISO/IEC 27001 A.8.2:	Privilegierte Zugangsrechte
ISO/IEC 27001 A.5.15:	Zugangssteuerung

MS365-027 PRIO 1 Kontoübernahme

User Consent für Apps deaktivieren, nur Admin Consent zulassen

1. Befund:

Die Prüfung „User Consent für Apps deaktiviert, nur Admin Consent“ ist nicht erfüllt.

User Consent erlaubt Benutzern, Drittanbieter-Apps eigenständig Zugriffsberechtigungen auf Unternehmensdaten zu erteilen (OAuth Consent). Consent Phishing (Illicit Consent Grant) ist ein Angriff, bei dem Benutzer dazu verleitet werden, bösartigen Apps weitreichende Berechtigungen zu gewähren.

Gemessen im Tenant:

Gemessen: ManagePermissionGrantsForSelf.microsoft-user-default-allow-consent-apps ManagePermissionGrantsForSelf.microsoft-user-default-recommended · **Empfohlen:** ManagePermissionGrantsForSelf.microsoft-user-default-low

2. Warum kritisch?

Wenn Benutzer eigenständig App-Berechtigungen (Consent) erteilen können, ist dies ein häufiger Angriffsvektor (Consent Phishing / Illicit Consent Grant). Angreifer erstellen bösartige Apps und bringen Benutzer dazu, Zugriffsrechte zu gewähren.

Consent Phishing ist einer der gefährlichsten Angriffsvektoren in Microsoft 365. Der Benutzer erteilt der App Berechtigungen, die auch nach einer Passwortänderung

bestehen bleiben. Nur die zentrale Steuerung über Admin Consent verhindert, dass Benutzer unkontrolliert Rechte vergeben.

> SZENARIO: *Ein Mitarbeiter erhält eine E-Mail mit dem Link zu einer vermeintlichen Productivity-App. Er klickt auf 'Zustimmen' und erteilt der App Mail.ReadWrite und Files.Read.All. Die bösartige App exfiltriert ab sofort alle E-Mails und OneDrive-Dateien - auch nach Passwortänderung, da der OAuth-Consent bestehen bleibt.*

3. Wie zu schließen:

User Consent auf 'Do not allow user consent' setzen

Klickpfad:

1. Microsoft Entra Admin Center (entra.microsoft.com) mit der Rolle Global Administrator öffnen (per Graph genügt Privileged Role Administrator)
2. Entra ID → Enterprise apps → Consent and permissions → User consent settings
3. User consent for applications: Do not allow user consent → Save
4. Vorher den Admin Consent Workflow einrichten (MS365-028), damit Benutzer benötigte Apps beantragen können
5. Bestehende Benutzer-Zustimmungen prüfen: Entra ID → Enterprise apps → All applications → App → Permissions → User consent; die Änderung wirkt nur für künftige Zustimmungen

MICROSOFT-DOKUMENTATION: https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/configure-user-consent, https://learn.microsoft.com/en-us/graph/api/authorizationpolicy-update, https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/manage-application-permissions

4. Warum relevant für DSGVO, NIS2 und ISO 27001:

Consent Phishing verschafft Angreifern dauerhaften Zugriff auf Postfächer und Dateien, ohne dass ein Kennwort gestohlen werden muss. Die Freigabe von App-Berechtigungen nur durch Administratoren unterstützt die Kontrolle von Drittanbietern und trägt zum Schutz personenbezogener Daten vor unbefugter Weitergabe bei.

Art. 28 DSGVO:	Auftragsverarbeitung (Kontrolle von Dienstleistern und Drittanbietern)
Art. 32 Abs. 1 lit. b DSGVO:	Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme
§ 30 Abs. 2 Nr. 4 BSIG (Art. 21 Abs. 2 lit. d NIS2):	Sicherheit der Lieferkette
§ 30 Abs. 2 Nr. 9 BSIG (Art. 21 Abs. 2 lit. i NIS2):	Personalsicherheit, Zugriffskontrolle und Management von Anlagen
ISO/IEC 27001 A.5.19:	Informationssicherheit in Lieferantenbeziehungen
ISO/IEC 27001 A.5.15:	Zugangssteuerung

MS365-072 PRIO 1 Kontoübernahme

Device Code Flow per Conditional Access blockieren

1. Befund:

Die Prüfung „Device Code Flow blockiert“ ist nicht erfüllt.

Der Device Code Flow (OAuth 2.0 Device Authorization Grant) wurde für Geräte ohne Browser entwickelt, z.B. Smart-TVs oder IoT-Geräte. Der Benutzer gibt einen Code auf einem separaten Gerät ein und autorisiert damit den Zugriff. Microsoft hat im Conditional Access eine dedizierte Bedingung für Authentication Flows eingeführt, um diesen Vektor gezielt zu kontrollieren.

2. Warum kritisch?

Der Device Code Flow ermöglicht Authentifizierung über https://microsoft.com/devicelogin und wird aktiv für Device Code Phishing missbraucht. Angreifer nutzen Tools wie TokenTactics, um Benutzer zur Eingabe eines Gerätecodes zu verleiten und anschließend Zugangs- und Refresh-Token zu stehlen. Diese Token ermöglichen Zugriff ohne erneute Authentifizierung.

Device Code Phishing ist seit 2022 einer der am schnellsten wachsenden Angriffsvektoren gegen Microsoft 365. Da der Benutzer die Authentifizierung auf einem vertrauenswürdigen Gerät durchführt, wird MFA korrekt abgeschlossen - der Token landet jedoch beim Angreifer.

> SZENARIO: *Der Angreifer sendet eine Teams-Nachricht mit einem Device Code und der Aufforderung, diesen unter microsoft.com/devicelogin einzugeben. Das Opfer authentifiziert sich inkl. MFA. Der Angreifer erhält ein Refresh Token mit voller Sitzungsdauer und greift auf alle M365-Daten des Opfers zu.*

3. Wie zu schließen:

Device Code Flow per Conditional Access blockieren

Klickpfad:

1. Vorbereitung: in den Sign-in logs prüfen, wer den Device Code Flow legitim nutzt (z. B. Raumkontogeräte, Kommandozeilenwerkzeuge); diese Fälle über eine eigene Ausschlussgruppe abbilden
2. Microsoft Entra Admin Center (entra.microsoft.com) mit mindestens der Rolle Conditional Access Administrator öffnen
3. Entra ID → Conditional Access → Policies → New policy, Name z. B. ‘CA010 - Alle Benutzer - Device Code Flow blockieren’
4. Assignments → Users or workload identities → Include: All users; Exclude: Notfallkonten und dokumentierte Ausnahmegruppe
5. Target resources → Resources (formerly cloud apps) → Include: All resources (formerly ‘All cloud apps’)
6. Conditions → Authentication Flows → Configure: Yes → Device code flow → Done
7. Access controls → Grant → Block access → Select
8. Enable policy: Report-only, Treffer auswerten, dann On → Create

MICROSOFT-DOKUMENTATION: https://learn.microsoft.com/en-us/entra/identity/conditional-access/policy-block-authentication-flows, https://learn.microsoft.com/en-us/graph/api/conditionalaccessroot-post-policies, https://learn.microsoft.com/en-us/graph/api/resources/conditionalaccessauthenticationflows?view=graph-rest-1.0

4. Warum relevant für DSGVO, NIS2 und ISO 27001:

Device Code Phishing umgeht die gewohnte Anmeldeseite und erbeutet gültige Tokens, oft trotz MFA. Die Blockierung des Ablaufs reduziert diesen aktiv genutzten Angriffsweg und unterstützt in der Regel die Anforderungen an sichere Authentisierung nach NIS2 und an die Vertraulichkeit nach DSGVO.

Art. 32 Abs. 1 lit. b DSGVO:	Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme
§ 30 Abs. 2 Nr. 10 BSIG (Art. 21 Abs. 2 lit. j NIS2):	Multi-Faktor-Authentifizierung, gesicherte Kommunikation und Notfallkommunikation
ISO/IEC 27001 A.8.5:	Sichere Authentisierung
ISO/IEC 27001 A.5.15:	Zugangssteuerung

MS365-003 PRIO 1 Kontoübernahme

Phishing-resistente MFA für Global Administratoren erzwingen

1. Befund:

Die Prüfung „Global Administratoren verwenden Phishing-resistente MFA“ ist nicht erfüllt.

Phishing-resistente MFA-Methoden (FIDO2 Security Keys, Windows Hello for Business, Certificate-based Authentication) sind gegen Phishing-Angriffe geschützt, da sie kryptographisch an die Zieldomain gebunden sind. Push-basierte MFA (Authenticator-App) und SMS sind dagegen durch MFA-Fatigue und SIM-Swapping angreifbar.

2. Warum kritisch?

Für hochprivilegierte Rollen wie Global Administrator erzwingt keine Richtlinie phishing-resistente Anmeldemethoden, bzw. die FIDO2-Methode ist nicht passend konfiguriert. Admins können sich daher weiter mit SMS oder App-basierter MFA anmelden, die für MFA-Fatigue, SIM-Swapping und Adversary-in-the-Middle-Angriffe anfällig sind. Bei einem kompromittierten Admin-Konto ist der gesamte Tenant gefährdet.

Global Administratoren haben uneingeschränkten Zugriff auf den gesamten Tenant. Die Kompromittierung eines Global Admin-Accounts ist der schlimmste anzunehmende Fall. Phishing-resistente MFA ist die einzige Methode, die auch gegen fortgeschrittene Adversary-in-the-Middle-Angriffe (AiTM) schützt.

> SZENARIO: *Ein Angreifer setzt eine AiTM-Phishing-Seite auf, die den Microsoft-Login imitiert. Ein Global Admin gibt Passwort und Authenticator-Code ein - der Proxy leitet beides an Microsoft weiter und fängt das Session-Token ab. Mit FIDO2 hätte der Key die Phishing-Domain erkannt und die Authentifizierung verweigert.*

3. Wie zu schließen:

FIDO2 Security Keys oder Windows Hello for Business für alle Global Admins einrichten

Klickpfad:

1. Microsoft Entra Admin Center (entra.microsoft.com) mit mindestens der Rolle Authentication Policy Administrator öffnen (für die Conditional-Access-Richtlinie zusätzlich Conditional Access Administrator)
2. Entra ID → Authentication methods → Policies → Passkey (FIDO2): Enable auf On, Target: All users oder eine Admin-Gruppe, Allow self-service set up auf Yes

→ Save

3. Für Administratoren ein eigenes Passkey-Profil anlegen (Configure → + Add passkey profile): Passkey-Typ device-bound, Enforce attestation: Yes, optional zugelassene Schlüsselmodelle per AAGUID (Target specific authenticators) → Save, dann unter Enable and Target der Admin-Gruppe zuweisen
4. Alle Administratoren registrieren mindestens einen Passkey (FIDO2-Sicherheitsschlüssel oder Windows Hello for Business); für die Ersteinrichtung ohne vorhandene starke Methode einen Temporary Access Pass ausgeben
5. Entra ID → Conditional Access → Policies → New policy, Name z. B. 'CA002 - Admin-Rollen - Phishing-resistente MFA'
6. Assignments → Users, agents or workload identities → Include: Directory roles, mindestens Global Administrator, Privileged Role Administrator, Privileged Authentication Administrator, Security Administrator, Conditional Access Administrator, Exchange Administrator, SharePoint Administrator, User Administrator, Application Administrator, Cloud Application Administrator, Authentication Administrator, Helpdesk Administrator, Password Administrator, Billing Administrator; Exclude: Notfallkonten (Break-Glass-Gruppe)
7. Target resources → Resources (formerly cloud apps) → Include: All resources (formerly 'All cloud apps')
8. Access controls → Grant → Grant access → Require authentication strength → Phishing-resistant MFA → Select
9. Enable policy zunächst auf Report-only → Create; nach Prüfung der Anmeldeprotokolle auf On umstellen

MICROSOFT-DOKUMENTATION: https://learn.microsoft.com/en-us/entra/identity/conditional-access/policy-admin-phish-resistant-mfa, https://learn.microsoft.com/en-us/entra/identity/authentication/how-to-authentication-passkeys-fido2, https://learn.microsoft.com/en-us/graph/api/fido2authenticationmethodconfiguration-update?view=graph-rest-1.0, https://learn.microsoft.com/en-us/graph/api/conditionalaccessroot-post-policies, https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference

4. Warum relevant für DSGVO, NIS2 und ISO 27001:

Für Konten mit Administratorrechten genügt einfache MFA in der Regel nicht mehr, weil Adversary-in-the-Middle-Phishing Einmalcodes und Push-Bestätigungen abgreifen kann. Phishing-resistente Verfahren unterstützen die in § 30 Abs. 2 Nr. 10 BSIG geforderte Multi-Faktor-Authentifizierung und tragen zum angemessenen Schutz der Daten des gesamten Tenants bei.

Art. 32 Abs. 1 lit. b DSGVO:	Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme
§ 30 Abs. 2 Nr. 10 BSIG (Art. 21 Abs. 2 lit. j NIS2):	Multi-Faktor-Authentifizierung, gesicherte Kommunikation und Notfallkommunikation
§ 38 BSIG (Art. 20 NIS2):	Umsetzungs-, Überwachungs- und Schulungspflicht der Geschäftsleitung
ISO/IEC 27001 A.8.5:	Sichere Authentisierung
ISO/IEC 27001 A.8.2:	Privilegierte Zugangsrechte
ISO/IEC 27001 A.5.17:	Authentisierungsinformationen

MS365-262 PRIO 1 Kontoübernahme

Postfach und permanente Control-Plane-Rolle trennen

1. Befund:

Die Prüfung „Kein Benutzer mit Postfach und permanenter Control-Plane-Rolle“ ist nicht erfüllt.

Das Trennen von Administrator- und Alltagskonten ist ein grundlegendes Sicherheitsprinzip. Ein Postfach macht ein Konto angreifbar über E-Mail-basierte Angriffe wie Phishing, während permanente Control-Plane-Rollen sofortigen Vollzugriff ohne weitere Genehmigung ermöglichen.

Gemessen im Tenant:

- Admin-Konto A with Global Administrator on scope directory (tenant-wide)
- Admin-Konto A with Azure AD Joined Device Local Administrator on scope directory (tenant-wide)
- Admin-Konto B (IT-Dienstleister) with Security Administrator on scope directory (tenant-wide)
- Admin-Konto B (IT-Dienstleister) with Global Administrator on scope directory (tenant-wide)
- Admin-Konto B (IT-Dienstleister) with Cloud Device Administrator on scope directory (tenant-wide)
- Admin-Konto B (IT-Dienstleister) with Azure AD Joined Device Local Administrator on scope directory (tenant-wide)
- Benutzer F (synchronisiert) with Azure AD Joined Device Local Administrator on scope directory (tenant-wide)

2. Warum kritisch?

Benutzerkonten mit Postfach und permanenter hochprivilegierter Rolle (z.B. Global Admin) sind besonders exponiert. Das Postfach ist ein primärer Angriffsvektor über Phishing, während die permanente Rolle sofortigen Vollzugriff auf den Tenant gewährt.

Die Kombination aus Postfach und permanenter Admin-Rolle schafft einen direkten Pfad vom Phishing-Angriff zum Tenant-Takeover. Wird das Konto per E-Mail-Phishing kompromittiert, hat der Angreifer sofort volle Administrative Kontrolle.

> SZENARIO: *Ein Angreifer sendet eine gezielte Phishing-Mail an einen Global Admin mit Postfach. Der Admin klickt auf den Link und gibt seine Zugangsdaten ein. Da die Rolle permanent aktiv ist, hat der Angreifer sofort Global-Admin-Zugriff ohne PIM-Aktivierung.*

3. Wie zu schließen:

Admin-Konten von Postfächern trennen oder permanente Rollen durch PIM-Berechtigung ersetzen

Klickpfad:

1. Microsoft Entra Admin Center (entra.microsoft.com) mit mindestens der Rolle Privileged Role Administrator öffnen
2. Erhebung: Entra ID → Roles & admins → hochprivilegierte Rollen (z. B. Global Administrator, Privileged Role Administrator) öffnen und Mitglieder mit lizenziertem Postfach notieren
3. Option A (bevorzugt): für jede betroffene Person ein separates, reines Cloud-Administratorkonto ohne Exchange-Lizenz anlegen, die Rolle dort zuweisen und vom Alltagskonto entfernen
4. Option B (Entra ID P2): ID Governance → Privileged Identity Management → Microsoft Entra roles → Roles → Rolle wählen → Add assignments → Assignment

type: Eligible

5. Danach im Tab Active assignments die bisherige permanente Zuweisung des Kontos auswählen → Remove
6. Notfallkonten behalten ihre permanente Global-Administrator-Zuweisung, dürfen aber kein Postfach haben
7. Kontrolle: in der Rollenliste keine permanente aktive Zuweisung mehr für Konten mit Postfach

MICROSOFT-DOKUMENTATION: https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-how-to-add-role-to-user, https://learn.microsoft.com/en-us/graph/api/rbacapplication-post-roleeligibilityscheduleequests, https://learn.microsoft.com/en-us/graph/api/rbacapplication-list-roleassignments, https://learn.microsoft.com/en-us/graph/api/unifiedroleassignment-delete, https://learn.microsoft.com/en-us/graph/api/resources/expirationpattern

4. Warum relevant für DSGVO, NIS2 und ISO 27001:

Konten mit Postfach sind über Phishing direkt erreichbar; mit permanenter hochprivilegierter Rolle führt eine einzige erfolgreiche Phishing-Mail zum Vollzugriff auf den Tenant. Getrennte Administratorkonten bzw. Just-in-time-Zuweisungen unterstützen die Verwaltung privilegierter Zugänge nach § 30 BSIG und den Schutz personenbezogener Daten.

Art. 32 Abs. 1 lit. b DSGVO:	Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme
§ 30 Abs. 2 Nr. 9 BSIG (Art. 21 Abs. 2 lit. i NIS2):	Personalsicherheit, Zugriffskontrolle und Management von Anlagen
ISO/IEC 27001 A.8.2:	Privilegierte Zugangsrechte
ISO/IEC 27001 A.5.18:	Zugangsrechte

MS365-042 PRIO 1 Kontoübernahme

Hybrid-Benutzer aus permanenten Control-Plane-Rollen entfernen

1. Befund:

Die Prüfung „Kein Hybrid-User mit permanenter Control-Plane-Rolle“ ist nicht erfüllt.

Hybrid-Benutzer sind Konten, die aus dem On-Premises Active Directory nach Entra ID synchronisiert werden. Sie unterliegen den Sicherheitsstandards beider Umgebungen. Control-Plane-Rollen (Global Admin, Security Admin, etc.) sind die mächtigsten Rollen im Tenant und sollten ausschließlich Cloud-Only-Konten vorbehalten sein.

Gemessen im Tenant:

- Benutzer F (synchronisiert) with Azure AD Joined Device Local Administrator on scope directory (tenant-wide)

2. Warum kritisch?

Synchronisierte (Hybrid-)Benutzer mit permanenten Control-Plane-Rollen schaffen eine Brücke zwischen On-Premises und Cloud. Bei Kompromittierung des lokalen AD erhält der Angreifer automatisch Cloud-Admin-Rechte.

Das Tiering-Modell trennt On-Premises (Tier 0) strikt von der Cloud (Control Plane). Synchronisierte Konten in Control-Plane-Rollen durchbrechen diese Trennung. Ein Angriff auf das On-Premises AD kompromittiert dann automatisch die gesamte Cloud-Infrastruktur.

> SZENARIO: *Ein Angreifer kompromittiert den On-Premises Domain Controller und ändert das Passwort eines synchronisierten Kontos mit Global Admin-Rolle. Nach der nächsten Synchronisation (alle 30 Minuten) ist das neue Passwort in Entra ID aktiv, und der Angreifer hat vollen Cloud-Zugriff.*

3. Wie zu schließen:

Synchronisierte Benutzer aus permanenten Control-Plane-Rollen entfernen

Klickpfad:

1. Microsoft Entra Admin Center (entra.microsoft.com) mit mindestens der Rolle Privileged Role Administrator öffnen
2. Entra ID → Users → All users → Filter: On-premises sync enabled = Yes; mit den Mitgliedern privilegierter Rollen unter Entra ID → Roles & admins abgleichen
3. Je betroffener Person ein reines Cloud-Admin-Konto anlegen (UPN auf der onmicrosoft.com-Domain bzw. einer nicht föderierten Domain, ohne Postfach, mit phishing-resistenter MFA)
4. Rolle dem Cloud-Konto zuweisen, bevorzugt als Eligible assignment über Privileged Identity Management
5. Anmeldung mit dem Cloud-Konto testen, danach die Rollenzuweisung des synchronisierten Kontos unter Roles & admins → Rolle → Assignments → Remove assignments entfernen
6. Sicherstellen, dass mindestens zwei Notfallkonten (cloud-only) mit Global Administrator bestehen, bevor Zuweisungen entfernt werden

MICROSOFT-DOKUMENTATION: https://learn.microsoft.com/en-us/entra/architecture/protect-m365-from-on-premises-attacks, https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/security-planning, https://learn.microsoft.com/en-us/graph/api/unifiedroleassignment-delete?view=graph-rest-1.0, https://learn.microsoft.com/en-us/graph/api/rbacapplication-list-roleassignments?view=graph-rest-1.0

4. Warum relevant für DSGVO, NIS2 und ISO 27001:

Synchronisierte Admin-Konten verbinden das lokale Active Directory direkt mit den höchsten Cloud-Rechten, sodass eine Kompromittierung on-premises in der Regel auf Microsoft 365 durchschlägt. Getrennte Cloud-Admin-Konten unterstützen die Zugriffskontrolle nach NIS2 und begrenzen die Folgen eines Angriffs auf das lokale Netz.

Art. 32 Abs. 1 lit. b DSGVO:	Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme
§ 30 Abs. 2 Nr. 9 BSIG (Art. 21 Abs. 2 lit. i NIS2):	Personalsicherheit, Zugriffskontrolle und Management von Anlagen
ISO/IEC 27001 A.8.2:	Privilegierte Zugangsrechte
ISO/IEC 27001 A.5.16:	Identitätsmanagement

Weitere Optimierungen (Prio 2)

38 OPTIMIERUNGEN NACH ART



ID	MASSNAHME	ART
MS365-014	Self-Service-Kennwortzurücksetzung für Administratoren deaktivieren	Zusätzliche Härtung
MS365-017	Schwache MFA-Methoden deaktivieren (SMS, Telefon, E-Mail OTP)	Zusätzliche Härtung
MS365-019	Anwendungsname und Standort in Microsoft Authenticator anzeigen	Zusätzliche Härtung
MS365-047	Gastzugriff auf das Verzeichnis maximal einschränken	Zusätzliche Härtung
MS365-073	Authentication Transfer (QR-Code-Flow) per Conditional Access blockieren	Zusätzliche Härtung
MS365-074	Token Protection für Anmeldesitzungen per Conditional Access einrichten	Zusätzliche Härtung
MS365-081	Gerätecompliance per Conditional Access als Zugriffsbedingung erzwingen	Zusätzliche Härtung
MS365-082	Anmeldungen aus Hochrisikoländern per Conditional Access blockieren	Zusätzliche Härtung
MS365-084	Admin-Zugriff auf Privileged Access Workstations (PAW) beschränken	Zusätzliche Härtung
MS365-085	Admin-Anmeldung von mobilen Endgeräten blockieren	Zusätzliche Härtung
MS365-086	Registrierung von Sicherheitsinformationen außerhalb von Trusted Locations an MFA binden	Zusätzliche Härtung
MS365-087	MFA für Geräte-Join und -Registrierung erzwingen	Zusätzliche Härtung
MS365-089	Office 365: App-Einschränkungen per Conditional Access aktivieren (nur Browserzugriff)	Zusätzliche Härtung
MS365-097	Unbekannte und nicht unterstützte Geräteplattformen blockieren	Zusätzliche Härtung
MS365-101	CA-Sicherheitsgruppen durch RMAU schützen	Zusätzliche Härtung
MS365-160	Defender for Cloud Apps: Session Control in Conditional Access integrieren	Zusätzliche Härtung
MS365-263	Geräte-Join auf ausgewählte Benutzer/Gruppen beschränken	Zusätzliche Härtung
MS365-266	Phishing-resistente MFA für alle Benutzer ausrollen	Zusätzliche Härtung
MS365-267	Verwaltete Geräte für die Authentifizierung voraussetzen	Zusätzliche Härtung
MS365-268	MFA-Registrierung nur von verwalteten Geräten erlauben	Zusätzliche Härtung
MS365-373	Hochprivilegierte Microsoft-Apps nur mit expliziter Zuweisung freigeben	Zusätzliche Härtung
MS365-378	Abruf von BitLocker-Schlüsseln durch Benutzer sperren	Zusätzliche Härtung
MS365-039	Geräte-Registrierungslimit pro Benutzer reduzieren	Feinjustierung
MS365-090	Persistente Browsersitzungen auf nicht verwalteten Geräten unterbinden	Feinjustierung
MS365-092	Anmeldehäufigkeit auf nicht verwalteten Geräten begrenzen	Feinjustierung
MS365-270	Temporary Access Pass auf Einmal-Nutzung beschränken	Feinjustierung
MS365-271	Benutzerdefinierte Banned-Password-Liste erzwingen	Feinjustierung

ID	MASSNAHME	ART
MS365-007	Admin-Konten ohne Klarnamen benennen (anonymisierte Namenskonvention)	Governance
MS365-013	Ablaufrichtlinie für Microsoft 365 Gruppen konfigurieren	Governance
MS365-048	Gast-Einladungen auf berechtigte Rollen/Personen beschränken	Governance
MS365-049	Eingehende B2B-Zusammenarbeit auf freigegebene Organisationen beschränken	Governance
MS365-057	Ausgehenden Cross-Tenant-Zugriff einschränken	Governance
MS365-020	Verdächtige Aktivitäten melden (Report Suspicious Activity) aktivieren	Betriebshygiene
MS365-045	Benachrichtigung bei Gruppen-Ablauf an eine Sammeladresse senden	Betriebshygiene
MS365-050	Selbstregistrierung per E-Mail-Verifizierung deaktivieren	Betriebshygiene
MS365-079	Notfallkonten (Break-Glass) korrekt einrichten und von Conditional Access ausnehmen	Betriebshygiene
MS365-206	Microsoft Entra registered Geräte (BYOD) prüfen und bereinigen	Betriebshygiene
MS365-374	Anmeldung über das alte MSOnline-PowerShell-Modul blockieren	Betriebshygiene

05

/Defender XDR

Microsoft Defender Portal · https://security.microsoft.com

3

PRIO 1 · KRITISCH

20

PRIO 2 · OPTIMIERUNG

Was ist Defender XDR?

Im Microsoft Defender Portal liegen der Schutz vor Phishing und Schadsoftware in E-Mail und Zusammenarbeit (Defender for Office 365), die Geräte-Sicherheit (Defender for Endpoint), Warnungen, Untersuchungen und Exposure Management.

Rolle in der Microsoft 365 Architektur

Defender XDR erkennt und blockiert Angriffe über E-Mail, Geräte, Identitäten und Cloud-Apps hinweg und korreliert die Signale zu Vorfällen.

Abhängigkeiten zu anderen Diensten

- Defender for Office 365 schützt Exchange Online mit Safe Links und Safe Attachments
- Defender for Endpoint liefert Endpunkt-Telemetrie über Intune-verwaltete Geräte
- Entra ID Identity Protection speist Risikosignale in die XDR-Korrelation ein

Schlüsselkonzepte

- **Safe Links / Safe Attachments:** Safe Links prüft URLs zum Klickzeitpunkt (Time-of-Click) gegen aktuelle Bedrohungsdaten. Safe Attachments detoniert Anhänge in einer Sandbox, bevor sie zugestellt werden. Beide Funktionen ergänzen den Basis-Schutz von EOP.
- **Anti-Phishing-Policies:** Defender Anti-Phishing erkennt Impersonation-Angriffe durch Mailbox Intelligence und schützt gezielt VIP-Benutzer und Domains vor Identitätsmissbrauch. Ohne dedizierte Policies ist der Schutz auf Standarderkennung begrenzt.
- **Automated Investigation and Response (AIR):** AIR automatisiert die Untersuchung und Behebung von Sicherheitsvorfällen. Nach einem erkannten Phishing-Angriff kann AIR automatisch betroffene E-Mails entfernen und kompromittierte Konten sperren - vorausgesetzt, die Policies sind aktiv.

Einordnung für Entscheider

Dieser Bereich weist 3 kritische Sicherheitslücken auf. Zusätzlich wurden 20 Optimierungspotenziale identifiziert. Bei Nicht-Umsetzung bestehen unmittelbare Risiken für die Vertraulichkeit und Integrität der Unternehmensdaten. Die Geschäftsführung sollte die Umsetzung der Sofortmaßnahmen in diesem Bereich persönlich nachverfolgen.

KRITIKALITÄT:	Hoch
COMPLIANCE-RELEVANZ:	Erfüllung der Meldepflichten nach § 32 BSIG (NIS2) und Art. 33 DSGVO setzt funktionsfähige Erkennung voraus
BETRIEBLICHE AUSWIRKUNG:	Ohne wirksame Erkennung bleiben Angriffe lange unbemerkt und richten Schaden an, bevor reagiert wird

Handlungsempfehlung zu Defender XDR

Im Rahmen der Analyse sind die folgenden kritischen Konfigurationsabweichungen aufgefallen, die zeitnah adressiert werden müssen:

MS365-111 PRIO 1 Datenabfluss

Externe Mail-Weiterleitung blockieren

1. Befund:

Die Prüfung „Externe Mail-Weiterleitung blockiert“ ist nicht erfüllt.

Exchange Online bietet mehrere Mechanismen für E-Mail-Weiterleitung: Postfach-Weiterleitungsregeln (Inbox Rules), automatische Weiterleitung (Auto-Forwarding) und Transport-Regeln. Angreifer nutzen nach einer Kontoübernahme bevorzugt Inbox Rules mit Weiterleitung, da diese auch nach Passwortänderung aktiv bleiben. Die Outbound-Spam-Policy und Remote-Domain-Einstellungen kontrollieren externe Weiterleitung.

Gemessen im Tenant:

NAME	DOMAIN	AUTOMATIC FORWARDING	ERGEBNIS
Default	*	Allow automatic forwarding	nicht erfüllt

2. Warum kritisch?

Automatische E-Mail-Weiterleitung an externe Adressen ermöglicht Datenexfiltration durch kompromittierte oder böswillige Benutzer. Angreifer richten nach Kontoübernahme häufig versteckte Weiterleitungsregeln ein, um dauerhaft Kopien aller E-Mails an externe Postfächer zu erhalten - auch nach Passwortänderung.

Externe E-Mail-Weiterleitung ist der häufigste Persistenzmechanismus nach Business Email Compromise. Angreifer erhalten dauerhaft Kopien aller E-Mails, selbst wenn das Passwort geändert und MFA aktiviert wird. Die Blockierung unterbindet diesen kritischen Datenexfiltrationskanal.

> SZENARIO: *Nach erfolgreicher Phishing-Attacke kompromittiert ein Angreifer das Konto eines Mitarbeiters. Er erstellt eine versteckte Inbox Rule, die alle eingehenden E-Mails an ein externes Gmail-Postfach weiterleitet. Das IT-Team bemerkt den Angriff und setzt das Passwort zurück - die Weiterleitungsregel bleibt jedoch aktiv. Über Monate hinweg liest der Angreifer vertrauliche E-Mails mit Kundendaten und Vertragsinformationen.*

3. Wie zu schließen:

Alle Formen der externen E-Mail-Weiterleitung blockieren

Klickpfad:

1. Microsoft Defender Portal (security.microsoft.com) → Email & collaboration → Policies & rules → Threat policies → Anti-spam
2. Anti-spam outbound policy (Default) öffnen → Edit protection settings
3. Forwarding rules → Automatic forwarding rules: Off - Forwarding is disabled → Save
4. Benötigte Ausnahmen (z. B. ein Funktionspostfach) über eine eigene, eng zugewiesene Outbound-Richtlinie mit ‘On - Forwarding is enabled’ abbilden
5. Exchange Admin Center (admin.exchange.microsoft.com) → Mail flow → Remote domains → Default → Email reply types → Automatic replies: automatische Weiterleitung nicht zulassen → Save

6. Bestehende Weiterleitungen prüfen: Postfächer mit gesetzter Weiterleitungsadresse und Posteingangsregeln mit Weiterleitung an externe Adressen entfernen

MICROSOFT-DOKUMENTATION: https://learn.microsoft.com/en-us/defender-office-365/outbound-spam-policies-external-email-forwarding, https://learn.microsoft.com/en-us/powershell/module/exchangepowershell/set-hostedoutboundspamfilterpolicy, https://learn.microsoft.com/en-us/powershell/module/exchangepowershell/set-remotedomain

4. Warum relevant für DSGVO, NIS2 und ISO 27001:

Automatische Weiterleitungen an externe Adressen sind ein klassischer Weg für unbemerkten Datenabfluss nach einer Kontoübernahme. Fließen so E-Mails mit personenbezogenen Daten ab, liegt in der Regel eine Datenschutzverletzung vor, die binnen 72 Stunden zu melden ist.

Art. 5 Abs. 1 lit. f DSGVO:	Integrität und Vertraulichkeit personenbezogener Daten
Art. 32 Abs. 1 lit. b DSGVO:	Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme
Art. 33 und 34 DSGVO:	Meldung und Benachrichtigung bei Datenschutzverletzungen
§ 30 Abs. 2 Nr. 9 BSIG (Art. 21 Abs. 2 lit. i NIS2):	Personalsicherheit, Zugriffskontrolle und Management von Anlagen
ISO/IEC 27001 A.5.14:	Informationsübertragung
ISO/IEC 27001 A.8.12:	Verhinderung von Datenlecks

MS365-128 PRIO 1 Fehlender Grundschutz

Safe Attachments und Dateitypfilter für E-Mail-Anhänge aktivieren

1. Befund:

Die Prüfung „Safe Attachments und Dateitypfilter für E-Mail-Anhänge aktiv“ ist nicht erfüllt.

Zwei Schutzschichten prüfen E-Mail-Anhänge: Der Dateitypfilter (common attachments filter) in den Anti-Malware-Richtlinien weist Dateitypen wie exe, iso, lnk oder vbs ab, ohne sie zu scannen. Safe Attachments aus Defender for Office 365 öffnet Anhänge in einer Sandbox und erkennt so auch unbekannte Schadsoftware. Microsoft empfiehlt für beide Block als Aktion; die Voreinstellung Built-in protection wendet Safe Attachments auf alle nicht anders erfassten Empfänger an.

Gemessen im Tenant:

POLICY NAME	ENABLED	ENABLEFILEFILTER	EXTENSIONS	ERGEBNIS
Default	True	False	ace, ani, apk, app, appx, & 48 others	nicht erfüllt

2. Warum kritisch?

In mindestens einer aktiven Anti-Malware-Richtlinie ist der Dateitypfilter ausgeschaltet oder Safe Attachments greift nicht mit der Aktion Block. Ausführbare Dateien, Skripte und Image-Dateien können damit zugestellt werden, und neue Schadsoftware, die keine Signatur trifft, wird nicht in der Sandbox abgefangen.

Für viele Dateitypen gibt es im normalen Geschäftsverkehr keinen Grund, sie per E-Mail zu empfangen; sie pauschal abzuweisen, ist die einfachste wirksame Maßnahme. Die Sandbox-Prüfung ergänzt die signaturbasierte Erkennung um eine Verhaltensanalyse.

> SZENARIO: *Ein Angreifer verschickt eine Bewerbung mit einer ISO-Datei, die eine getarnte Verknüpfung (lnk) enthält. Weil der Dateitypfilter in der Richtlinie für die Personalabteilung ausgeschaltet ist, wird der Anhang zugestellt. Die Sachbearbeiterin öffnet die Datei, das Skript lädt eine Schadsoftware nach.*

3. Wie zu schließen:

Dateitypfilter in allen aktiven Anti-Malware-Richtlinien einschalten, Safe Attachments mit Aktion Block für alle Empfänger

Klickpfad:

1. Microsoft Defender Portal (security.microsoft.com) mit der Rolle Security Administrator öffnen (Lizenz Defender for Office 365 Plan 1 oder höher)
2. Empfohlen: Email & collaboration → Policies & rules → Threat policies → Preset Security Policies → Standard bzw. Strict protection einschalten und Empfänger zuweisen
3. Für eine eigene Richtlinie: Threat policies → Safe Attachments (security.microsoft.com/safeattachmentv2) → Create
4. Name z. B. ‘Safe Attachments - Alle Empfänger’; Users and domains → Domains: alle akzeptierten Domänen
5. Settings: Safe Attachments unknown malware response: Block; Quarantine policy: AdminOnlyAccessPolicy
6. Block messages containing encrypted attachments that could not be scanned: ‘Block unscanned attachments’ auswählen → Next → Submit
7. Kontrolle: Keine Richtlinie mit Off oder Monitor darf Empfänger abdecken; Ausnahmen nur für nicht lizenzierte Konten
8. Threat policies → Anti-malware (security.microsoft.com/antimalwarev2): Standardrichtlinie und jede eigene Richtlinie öffnen → Schutzeinstellungen bearbeiten → ‘Enable the common attachments filter’ auswählen → Save

MICROSOFT-DOKUMENTATION: https://learn.microsoft.com/en-us/defender-office-365/safe-attachments-policies-configure, https://learn.microsoft.com/en-us/powershell/module/exchangepowershell/new-safeattachmentpolicy, https://learn.microsoft.com/en-us/powershell/module/exchangepowershell/new-safeattachmentrule, https://learn.microsoft.com/en-us/defender-office-365/anti-malware-policies-configure, https://learn.microsoft.com/en-us/powershell/module/exchangepowershell/set-malwarefilterpolicy

4. Warum relevant für DSGVO, NIS2 und ISO 27001:

Unbekannte Schadsoftware in Anhängen umgeht signaturbasierte Filter. Die Sandbox-Prüfung vor der Zustellung ist eine technische Maßnahme, die in der Regel wesentlich zum Schutz vor Ransomware und damit zur Verfügbarkeit und Vertraulichkeit der Daten beiträgt.

Art. 32 Abs. 1 lit. b DSGVO:	Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme

§ 30 Abs. 2 Nr. 1 BSIG (Art. 21 Abs. 2 lit. a NIS2):	Risikoanalyse und Sicherheit der Informationssysteme
ISO/IEC 27001 A.8.7:	Schutz gegen Schadsoftware

MS365-138 PRIO 1 Fehlender Grundschutz

Anti-Malware: Ausführbare Dateien blockieren

1. Befund:

Die Prüfung „Anti-Malware: Ausführbare Dateien blockiert“ ist nicht erfüllt.

Der Common Attachment Types Filter in der Anti-Malware-Richtlinie blockiert E-Mails mit Anhängen bestimmter Dateitypen, unabhängig vom Malware-Scan-Ergebnis. Die Standardliste umfasst über 60 Dateitypen wie .exe, .bat, .cmd, .ps1, .vbs, .js, .wsf, .scr und weitere. Die Liste kann um zusätzliche Dateitypen erweitert werden.

Gemessen im Tenant:

POLICY	ERGEBNIS
Standard	nicht erfüllt

POLICY NAME	ERGEBNIS
Default	nicht erfüllt

2. Warum kritisch?

Ausführbare Dateien (.exe, .bat, .cmd, .ps1 etc.) als E-Mail-Anhänge sind einer der häufigsten Verbreitungswege für Malware. Ohne Blockierung dieser Dateitypen können Benutzer potenziell schädliche Anhänge öffnen und ausführen. Der Common Attachment Filter sollte alle gängigen ausführbaren Dateitypen blockieren.

Ausführbare Dateien per E-Mail zu empfangen ist in den meisten Geschäftsprozessen nicht erforderlich. Die Blockierung eliminiert einen der häufigsten Malware-Verbreitungswege proaktiv, unabhängig davon, ob die Malware bereits bekannt ist oder nicht.

> SZENARIO: *Ein Angreifer verpackt einen Ransomware-Dropper als .exe-Datei in einem ZIP-Archiv und sendet ihn als angebliche Rechnungsanlage. Ohne Blockierung ausführbarer Dateitypen wird der Anhang zugestellt. Der Benutzer entpackt die Datei und führt sie aus, wodurch Ransomware das gesamte Netzwerk verschlüsselt und Lösegeld gefordert wird.*

3. Wie zu schließen:

Blockierung ausführbarer Dateien in der Anti-Malware-Richtlinie aktivieren

Klickpfad:

1. Microsoft Defender Portal (security.microsoft.com) mit der Rolle Security Administrator öffnen
2. Preset Security Policies (Pflicht für die Prüfung): Email & collaboration → Policies & rules → Threat policies → Preset Security Policies (security.microsoft.com/presetSecurityPolicies) → Standard protection und Strict

protection auf On, Manage protection settings → Strict für Führungskräfte und Admins (Gruppe), Standard für alle akzeptierten Domänen zuweisen

3. Email & collaboration → Policies & rules → Threat policies → Anti-Malware (security.microsoft.com/antimalwarev2) → Default und jede eigene Richtlinie öffnen
4. Protection settings → Edit protection settings → 'Enable the common attachments filter' auswählen
5. Select file types: Microsoft-Standardliste beibehalten (enthält u. a. exe, cmd, bat, vbe, vbs, wsf, wsh, msi, scr, iso) und bei Bedarf ergänzen
6. 'When these file types are found': Reject the message with a non-delivery report (NDR) → Save

MICROSOFT-DOKUMENTATION: https://learn.microsoft.com/en-us/defender-office-365/anti-malware-policies-configure, https://learn.microsoft.com/en-us/defender-office-365/anti-malware-protection-about, https://learn.microsoft.com/en-us/powershell/module/exchangepowershell/set-malwarefilterpolicy, https://learn.microsoft.com/en-us/defender-office-365/preset-security-policies

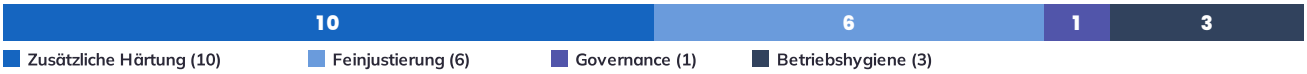
4. Warum relevant für DSGVO, NIS2 und ISO 27001:

Ausführbare Anhänge sind einer der häufigsten Wege, über die Schadsoftware in ein Unternehmen gelangt. Ihr Blockieren am Gateway trägt zum Schutz der Systeme und der darin verarbeiteten personenbezogenen Daten bei und ist eine grundlegende technische Maßnahme im Sinne von Art. 32 DSGVO und § 30 BSIG.

Art. 32 Abs. 1 lit. b DSGVO:	Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme
§ 30 Abs. 2 Nr. 1 BSIG (Art. 21 Abs. 2 lit. a NIS2):	Risikoanalyse und Sicherheit der Informationssysteme
ISO/IEC 27001 A.8.7:	Schutz gegen Schadsoftware

Weitere Optimierungen (Prio 2)

20 OPTIMIERUNGEN NACH ART



ID	MASSNAHME	ART
MS365-125	Safe Links: Klickverfolgung aktivieren und Voreinstellungen Standard/Strict einrichten	Zusätzliche Härtung
MS365-126	Safe Links: Prüfung interner Links aktivieren	Zusätzliche Härtung
MS365-131	Anti-Phishing: Impersonation-Schutz aktivieren	Zusätzliche Härtung
MS365-132	Anti-Phishing: Mailbox Intelligence aktivieren	Zusätzliche Härtung
MS365-134	Anti-Phishing: Sicherheitstipps (Safety Tips) aktivieren	Zusätzliche Härtung
MS365-140	Antispam: Voreinstellungen Standard und Strict einrichten	Zusätzliche Härtung
MS365-146	Attachment Filter: Comprehensive Filtering aktivieren	Zusätzliche Härtung
MS365-149	External Sender Warning aktivieren	Zusätzliche Härtung
MS365-313	Safe-Links-Richtlinie für jede akzeptierte Domäne sicherstellen	Zusätzliche Härtung

ID	MASSNAHME	ART
MS365-321	Safe-Attachments-Richtlinie für jede akzeptierte Domäne sicherstellen	Zusätzliche Härtung
MS365-118	Benutzer bei Nachrichtenlimit-Überschreitung sperren	Feinjustierung
MS365-124	Safe Links: Echtzeit-URL-Prüfung aktivieren	Feinjustierung
MS365-130	Anti-Phishing: Phishing-Schwellenwert auf mindestens 2 setzen	Feinjustierung
MS365-136	Anti-Phishing: Aktionen bei Impersonation auf Quarantäne setzen	Feinjustierung
MS365-141	Antispam: Spam in Junk-E-Mail oder Quarantäne leiten, Voreinstellungen einrichten	Feinjustierung
MS365-281	Outbound-Spamfilter konfigurieren	Feinjustierung
MS365-121	SecOps-Postfach in der Advanced Delivery Policy hinterlegen	Governance
MS365-114	Exchange Online Spam-Richtlinien: Admin-Benachrichtigungen einrichten	Betriebshygiene
MS365-137	Anti-Malware: Admin-Benachrichtigung bei Alarmen aktivieren	Betriebshygiene
MS365-244	Alarm bei Änderungen durch Administratoren einrichten	Betriebshygiene

06

/Exchange Online

Exchange Admin Center · https://admin.exchange.microsoft.com

2

PRIO 1 · KRITISCH

7

PRIO 2 · OPTIMIERUNG

Was ist Exchange Online?

Im Exchange Admin Center und in der Exchange Online PowerShell liegen Postfächer, Mail-Fluss-Regeln, Weiterleitungen, Freigaberichtlinien und die Anmeldeverfahren für E-Mail. Die DNS-Einträge für SPF, DKIM, DMARC und DANE gehören fachlich hierher, gesetzt werden sie beim Domain-Anbieter.

Rolle in der Microsoft 365 Architektur

E-Mail ist die wichtigste externe Schnittstelle des Unternehmens und das häufigste Ziel für Betrug und Phishing.

Abhängigkeiten zu anderen Diensten

- Defender for Office 365 ergänzt Exchange Online um Safe Links und Safe Attachments
- Conditional Access steuert den Zugriff auf Exchange Online Mailboxen
- Purview DLP-Policies greifen auf Exchange Online Transportebene

Schlüsselkonzepte

- **SPF / DKIM / DMARC:** Diese drei DNS-basierten Protokolle authentifizieren E-Mails und verhindern Domain-Spoofing. SPF definiert erlaubte Absender-Server, DKIM signiert Nachrichten kryptographisch und DMARC gibt vor, wie mit fehlgeschlagenen Prüfungen umgegangen wird.
- **Transportregeln:** Transportregeln (Mail Flow Rules) verarbeiten E-Mails auf Serverebene, bevor sie den Empfänger erreichen. Sie ermöglichen Disclaimer, Verschlüsselungspflichten oder das Blockieren bestimmter Anhänge und Muster.
- **Anti-Spam-Policies:** Exchange Online Protection (EOP) filtert eingehende und ausgehende E-Mails auf Spam und Bulk-Mail. Die Standardkonfiguration reicht oft nicht aus - insbesondere Allow-Listen und SCL-Schwellenwerte müssen regelmäßig geprüft werden.

Einordnung für Entscheider

Dieser Bereich weist 2 kritische Sicherheitslücken auf. Zusätzlich wurden 7 Optimierungspotenziale identifiziert. Bei Nicht-Umsetzung bestehen unmittelbare Risiken für die Vertraulichkeit und Integrität der Unternehmensdaten. Die Geschäftsführung sollte die Umsetzung der Sofortmaßnahmen in diesem Bereich persönlich nachverfolgen.

KRITIKALITÄT:	Hoch
COMPLIANCE-RELEVANZ:	E-Mail-Sicherheit betrifft DSGVO (personenbezogene Daten in E-Mails) und GoBD (Aufbewahrungspflichten)
BETRIEBLICHE AUSWIRKUNG:	Kompromittierte Postfächer oder gefälschte Absender treffen die Geschäftskommunikation mit Kunden und Partnern unmittelbar

Handlungsempfehlung zu Exchange Online

Im Rahmen der Analyse sind die folgenden kritischen Konfigurationsabweichungen aufgefallen, die zeitnah adressiert werden müssen:

MS365-107 PRIO 1 Kontoübernahme

SMTP AUTH deaktivieren

1. Befund:

Die Prüfung „SMTP AUTH deaktiviert“ ist nicht erfüllt.

SMTP AUTH (RFC 4954) wird heute vor allem von Multifunktionsgeräten, Scannern und Anwendungen genutzt. Microsoft hat den Zeitplan für Basic Auth bei SMTP AUTH verschoben: Bis Dezember 2026 bleibt das Verhalten unverändert, Ende Dezember 2026 wird es für bestehende Tenants standardmäßig deaktiviert (Administratoren können es wieder einschalten), neue Tenants haben es dann gar nicht mehr. Das endgültige Abschaltdatum kündigt Microsoft im zweiten Halbjahr 2027 an (Message Center MC786329, Stand 27.01.2026). OAuth für SMTP AUTH bleibt unterstützt.

2. Warum kritisch?

SMTP AUTH ist organisationsweit oder für einzelne Postfächer aktiv. Das Protokoll erlaubt den Mailversand mit Benutzername und Kennwort (Basic Auth) ohne zweiten Faktor und wird für Passwort-Spray und den Versand von Spam und Phishing über übernommene Konten genutzt. Betroffen sind in der Praxis meist Service-Postfächer von Geräten und Anwendungen.

Service-Postfächer haben oft einfache, nie geänderte Kennwörter und keinen zweiten Faktor. Genau dort setzt Passwort-Spray über SMTP AUTH an.

> SZENARIO: *Ein Angreifer probiert über SMTP AUTH gängige Kennwörter gegen die Postfächer eines Unternehmens durch. Beim Postfach des Scanners ‘scan@firma.de’ hat er Erfolg und verschickt darüber Rechnungs-Phishing an Kunden, das aus Sicht der Empfänger von einer echten Firmenadresse kommt.*

3. Wie zu schließen:

SMTP AUTH organisationsweit abschalten, Ausnahmen nur für dokumentierte Service-Postfächer mit OAuth

Klickpfad:

1. Bestandsaufnahme: Exchange Admin Center (admin.exchange.microsoft.com) mit mindestens der Rolle Exchange Administrator öffnen und Geräte, Anwendungen und Postfächer ermitteln, die SMTP AUTH noch nutzen (Bericht zu SMTP AUTH-Clients bzw. Anmeldeprotokolle)
2. Diese Geräte und Anwendungen auf OAuth, einen Connector oder einen Relay-Dienst umstellen
3. Exchange Admin Center → Settings → Mail flow → ‘Turn off SMTP AUTH protocol for your organization’ aktivieren → Save
4. Verbleibende, dokumentierte Ausnahmen nur auf Postfachebene: Microsoft 365 Admin Center → Users → Active users → Benutzer → Mail → Manage email apps → Authenticated SMTP aktivieren
5. Alle übrigen Postfächer mit aktivierter Postfach-Ausnahme zurücksetzen, da die Postfacheinstellung die Organisationseinstellung überschreibt
6. Ausnahmen zusätzlich per Conditional Access einschränken (z. B. nur von festen IP-Adressen)

MICROSOFT-DOKUMENTATION: https://learn.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/authenticated-client-smtp-submission, https://learn.microsoft.com/en-us/powershell/module/exchangepowershell/set-transportconfig, https://learn.microsoft.com/en-us/powershell/module/exchangepowershell/set-casmailbox

4. Warum relevant für DSGVO, NIS2 und ISO 27001:

SMTP AUTH mit Benutzername und Kennwort umgeht in der Regel die Multi-Faktor-Authentifizierung und ist ein bevorzugtes Ziel für Password-Spray. Das Abschalten unterstützt die in § 30 Abs. 2 Nr. 10 BSIG geforderte starke Authentisierung und den Schutz der Postfächer nach Art. 32 DSGVO.

Art. 32 Abs. 1 lit. b DSGVO:	Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme
§ 30 Abs. 2 Nr. 10 BSIG (Art. 21 Abs. 2 lit. j NIS2):	Multi-Faktor-Authentifizierung, gesicherte Kommunikation und Notfallkommunikation
ISO/IEC 27001 A.8.5:	Sichere Authentisierung
ISO/IEC 27001 A.5.17:	Authentisierungsinformationen

MS365-106 PRIO 1 Fehlender Grundschutz

DMARC-Policy (p=reject) für alle Domänen konfigurieren

1. Befund:

Die Prüfung „DMARC-Policy (p=reject) für alle Domänen konfiguriert“ ist nicht erfüllt.

DMARC (Domain-based Message Authentication, Reporting and Conformance) ist ein E-Mail-Authentifizierungsprotokoll gemäß RFC 7489, das auf SPF und DKIM aufbaut. DMARC definiert als DNS-Record, wie Empfänger mit E-Mails umgehen sollen, die SPF- oder DKIM-Prüfungen nicht bestehen. Die Policy-Stufen reichen von Monitoring (p=none) über Quarantäne (p=quarantine) bis zur Ablehnung (p=reject).

Gemessen im Tenant:

Nachgeprüft per DNS-Abfrage (1.1.1.1, 8.8.8.8): Keine der beiden E-Mail-Domänen des Unternehmens veröffentlicht einen DMARC-Record (Hauptdomäne: NXDOMAIN, Zweitdomäne: kein TXT-Eintrag).

2. Warum kritisch?

DMARC (Domain-based Message Authentication, Reporting and Conformance) ermöglicht die Absenderauthentifizierung und -berichterstattung, sodass gefälschte E-Mails erkannt und blockiert werden können. Ohne DMARC-Policy mit p=reject werden gefälschte E-Mails zwar erkannt, aber nicht blockiert. Angreifer können weiterhin E-Mails im Namen der Organisation versenden, die bei Empfängern zugestellt werden.

Nur mit DMARC p=reject werden gefälschte E-Mails tatsächlich blockiert und nicht zugestellt. Ohne DMARC oder mit schwacher Policy (p=none) können Angreifer weiterhin E-Mails im Namen der Organisation versenden. DMARC-Reports liefern zusätzlich Transparenz über alle Sendequellen.

> SZENARIO: *Ein Angreifer startet eine groß angelegte Phishing-Kampagne gegen Kunden der Organisation. Er versendet tausende E-Mails mit der gefälschten Absenderdomäne und fordert zur Passwortänderung über einen manipulierten Link auf. Ohne DMARC p=reject werden diese E-Mails zugestellt, hunderte Kunden geben ihre Zugangsdaten preis, und die Organisation erleidet massiven Reputationsschaden.*

3. Wie zu schließen:

DMARC-Policy mit p=reject für alle Domänen konfigurieren

Klickpfad:

1. Voraussetzung prüfen: SPF (MS365-104) und DKIM (MS365-105) sind für jede Domäne korrekt eingerichtet
2. Beim DNS-Hoster je Domäne einen TXT-Record _dmarc.<domain> anlegen, Start mit Überwachung: v=DMARC1; p=none; pct=100; rua=mailto:<berichtspostfach>
3. Aggregate Reports (rua) auswerten und fehlende legitime Absenderquellen in SPF/DKIM nachziehen
4. Richtlinie stufenweise verschärfen: p=quarantine (optional mit pct=10, 25, 50, 75, 100), danach p=reject; pct=100
5. Nicht für E-Mail genutzte Domänen direkt mit v=DMARC1; p=reject; versehen
6. *.onmicrosoft.com-Domäne: Microsoft 365 Admin Center (admin.microsoft.com) mit der Rolle Domain Name Administrator → Settings → Domains → *.onmicrosoft.com-Domäne → DNS records → Add record: TXT, Name _dmarc, Wert v=DMARC1; p=reject
7. Kontrolle je Domäne: nslookup -type=txt _dmarc.<domain> liefert p=reject ohne pct-Wert unter 100

MICROSOFT-DOKUMENTATION: https://learn.microsoft.com/en-us/defender-office-365/email-authentication-dmarc-configure

4. Warum relevant für DSGVO, NIS2 und ISO 27001:

Erst DMARC mit p=reject sorgt dafür, dass Empfänger gefälschte E-Mails im Namen des Unternehmens tatsächlich abweisen. Das schützt Kunden und Partner vor Phishing unter der eigenen Domäne und trägt zur gesicherten Kommunikation nach § 30 BSIG sowie zur Integrität nach Art. 32 DSGVO bei.

Art. 32 Abs. 1 lit. b DSGVO:	Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme
§ 30 Abs. 2 Nr. 1 BSIG (Art. 21 Abs. 2 lit. a NIS2):	Risikoanalyse und Sicherheit der Informationssysteme
§ 30 Abs. 2 Nr. 10 BSIG (Art. 21 Abs. 2 lit. j NIS2):	Multi-Faktor-Authentifizierung, gesicherte Kommunikation und Notfallkommunikation
ISO/IEC 27001 A.5.14:	Informationsübertragung
ISO/IEC 27001 A.8.20:	Netzwerksicherheit

Weitere Optimierungen (Prio 2)

7 OPTIMIERUNGEN NACH ART



Zusätzliche Härtung (6) Governance (1)

ID	MASSNAHME	ART
MS365-108	IMAP und POP3 deaktivieren	Zusätzliche Härtung

ID	MASSNAHME	ART
MS365-109	TLS für ausgehende E-Mails per Mail-Fluss-Regel erzwingen	Zusätzliche Härtung
MS365-110	DNSSEC und SMTP DANE konfigurieren	Zusätzliche Härtung
MS365-122	Anmeldung an Shared Mailboxes blockieren	Zusätzliche Härtung
MS365-242	MailTips für Endbenutzer aktivieren	Zusätzliche Härtung
MS365-372	Direct Send für den Tenant abweisen	Zusätzliche Härtung
MS365-241	Zusätzliche Speicheranbieter in Outlook im Web einschränken	Governance

07

/SharePoint & OneDrive

SharePoint Admin Center · https://admin.microsoft.com/sharepoint

1

PRIO 1 · KRITISCH

7

PRIO 2 · OPTIMIERUNG

Was ist SharePoint & OneDrive?

Im SharePoint Admin Center liegen die Freigabe- und Zugriffseinstellungen für SharePoint-Sites und OneDrive: externe Freigabe, Freigabelinks, Synchronisierung, Zugriff von nicht verwalteten Geräten.

Rolle in der Microsoft 365 Architektur

SharePoint und OneDrive sind die zentralen Dokumentenspeicher; Teams legt seine Dateien ebenfalls dort ab.

Abhängigkeiten zu anderen Diensten

- Teams nutzt SharePoint als Backend für Dateispeicherung in Kanälen
- Purview Sensitivity Labels schützen Dokumente in SharePoint und OneDrive
- Conditional Access kann den Zugriff auf SharePoint standort- oder gerätebasiert einschränken

Schlüsselkonzepte

- **Externe Freigabe (Sharing):** SharePoint bietet mehrere Freigabestufen: Keine externe Freigabe, authentifizierte Gäste, Anyone-Links. Anyone-Links sind der häufigste Konfigurationsfehler - sie ermöglichen anonymen Zugriff auf Unternehmensdaten ohne jede Nachverfolgung.
- **Site-Level Permissions:** Jede SharePoint Site hat eigene Berechtigungsstufen (Owner, Member, Visitor). Zu breite Berechtigungen oder vererbte Zugriffsrechte führen regelmäßig dazu, dass Benutzer auf Daten zugreifen können, die nicht für sie bestimmt sind.
- **Versionierung und Papierkorb:** Die Dokumentversionierung und der zweistufige Papierkorb schützen vor versehentlichem oder bösartigem Datenverlust. Ohne aktivierte Versionierung gibt es bei Ransomware-Angriffen auf OneDrive keine einfache Wiederherstellungsmöglichkeit.

Einordnung für Entscheider

Dieser Bereich weist 1 kritische Sicherheitslücken auf. Zusätzlich wurden 7 Optimierungspotenziale identifiziert. Bei Nicht-Umsetzung bestehen unmittelbare Risiken für die Vertraulichkeit und Integrität der Unternehmensdaten. Die Geschäftsführung sollte die Umsetzung der Sofortmaßnahmen in diesem Bereich persönlich nachverfolgen.

KRITIKALITÄT:	Hoch
COMPLIANCE-RELEVANZ:	Dateifreigabe betrifft DSGVO Art. 32 (Vertraulichkeit) und das Geschäftsgeheimnisgesetz
BETRIEBLICHE AUSWIRKUNG:	Unkontrollierte Freigaben führen zu Datenabfluss, der oft erst spät bemerkt wird

Handlungsempfehlung zu SharePoint & OneDrive

Im Rahmen der Analyse sind die folgenden kritischen Konfigurationsabweichungen aufgefallen, die zeitnah adressiert werden müssen:

MS365-161 PRIO 1 Datenabfluss

Externe Freigabe für SharePoint und OneDrive auf bestehende Gäste beschränken

1. Befund:

Die Prüfung „Externe Freigabe für SharePoint und OneDrive auf bestehende Gäste beschränkt“ ist nicht erfüllt.

SharePoint und OneDrive kennen vier Stufen der externen Freigabe: Anyone, New and existing guests, Existing guests und Only people in your organization. Die Einstellung auf Organisationsebene ist die Obergrenze für alle Sites; die OneDrive-Stufe darf gleich oder restriktiver sein als die SharePoint-Stufe, nie offener. Mit „Existing guests“ ist Teilen nur mit Gästen möglich, die bereits im Verzeichnis stehen.

Gemessen im Tenant:

Gemessen: externalUserSharingOnly · **Empfohlen:** ExistingExternalUserSharingOnly, Disabled

2. Warum kritisch?

Für SharePoint oder OneDrive ist die externe Freigabe auf „New and existing guests“ oder „Anyone“ eingestellt. Benutzer können damit Dateien und Sites eigenständig mit beliebigen neuen externen Personen teilen, ohne dass jemand prüft, wer neu eingeladen wird. Bei „Anyone“ kommen Links ohne Anmeldung hinzu.

Mit „Existing guests“ wird die Aufnahme neuer externer Personen zu einem bewussten Schritt über die Gasteinladung in Microsoft Entra ID. Danach kann mit diesen Gästen wie gewohnt geteilt werden, aber Freigaben an spontan eingetippte Adressen sind nicht mehr möglich.

> SZENARIO: *Ein Mitarbeiter teilt einen Ordner mit Angebotskalkulationen an eine private Adresse, um am Wochenende daran zu arbeiten, und vertippt sich bei der Domäne. Der Inhaber der falschen Adresse bestätigt den Code und erhält Zugriff auf die Kalkulationen. Mit „Existing guests“ wäre die Freigabe an die unbekannte Adresse nicht möglich gewesen.*

3. Wie zu schließen:

Externe Freigabe für SharePoint und OneDrive auf „Existing guests“ oder „Only people in your organization“ setzen

Klickpfad:

1. SharePoint Admin Center (<tenant>-admin.sharepoint.com) mit mindestens der Rolle SharePoint Administrator öffnen
2. Erhebung: Policies → Sharing; aktuelle Stufen für SharePoint und OneDrive notieren und klären, welche Sites heute mit neuen Externen geteilt werden
3. Unter External sharing den Regler für SharePoint auf ‘Existing guests’ setzen (nur Gäste, die bereits im Verzeichnis sind) oder auf ‘Only people in your organization’
4. Den Regler für OneDrive auf dieselbe oder eine restriktivere Stufe setzen (‘Existing guests’ bzw. ‘Only people in your organization’) → Save
5. Neue Gäste künftig gezielt über die Gasteinladung in Microsoft Entra ID aufnehmen; danach können sie mit ‘Existing guests’ berechtigt werden

6. Sites, die eine weitergehende Freigabe brauchen, nicht über die Organisationsebene öffnen; die Organisationsebene ist die Obergrenze für alle Sites
7. Bestehende externe Freigaben prüfen und nicht mehr benötigte entfernen; laut Microsoft verlieren Gäste nach einer Einschränkung in der Regel binnen einer Stunde den Zugriff

MICROSOFT-DOKUMENTATION: https://learn.microsoft.com/en-us/sharepoint/turn-external-sharing-on-or-off, https://learn.microsoft.com/en-us/powershell/module/microsoft.online.sharepoint.powershell/set-spotenant

4. Warum relevant für DSGVO, NIS2 und ISO 27001:

Die Beschränkung auf bekannte Gäste sorgt dafür, dass Unternehmensdaten nur mit Personen geteilt werden, die bewusst ins Verzeichnis aufgenommen wurden. Das unterstützt die Vertraulichkeit personenbezogener Daten und eine nachvollziehbare Steuerung der Informationsweitergabe an Dritte.

Art. 5 Abs. 1 lit. f DSGVO:	Integrität und Vertraulichkeit personenbezogener Daten
Art. 32 Abs. 1 lit. b DSGVO:	Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme
§ 30 Abs. 2 Nr. 9 BSIG (Art. 21 Abs. 2 lit. i NIS2):	Personalsicherheit, Zugriffskontrolle und Management von Anlagen
ISO/IEC 27001 A.5.14:	Informationsübertragung
ISO/IEC 27001 A.8.12:	Verhinderung von Datenlecks

Weitere Optimierungen (Prio 2)

7 OPTIMIERUNGEN NACH ART



ID	MASSNAHME	ART
MS365-163	Freigabelinks Standard auf ‘Bestimmte Personen’ setzen	Zusätzliche Härtung
MS365-165	Zugriff von nicht verwalteten Geräten auf reinen Webzugriff beschränken	Zusätzliche Härtung
MS365-166	OneDrive-Synchronisierung zentral steuern / einschränken	Zusätzliche Härtung
MS365-174	Externe Freigabe auf genehmigte Domänen beschränken	Zusätzliche Härtung
MS365-164	Standard-Berechtigung bei Freigabe auf ‘Lesen’ setzen	Feinjustierung
MS365-167	Anlage von SharePoint-Sites durch Endbenutzer deaktivieren	Governance
MS365-171	Versionsverlauf auf sinnvolles Maß reduzieren	Betriebshygiene

08

/Teams

Microsoft Teams Admin Center · https://admin.teams.microsoft.com

1

PRIO 1 · KRITISCH

14

PRIO 2 · OPTIMIERUNG

Was ist Teams?

Im Microsoft Teams Admin Center liegen externe Kommunikation, Besprechungsrichtlinien, Apps und Gastzugriff in Teams.

Rolle in der Microsoft 365 Architektur

Teams ist die zentrale Kommunikationsplattform und Zugang zu Chats, Besprechungen und Dateien.

Abhängigkeiten zu anderen Diensten

- Teams speichert Dateien in SharePoint Online (Kanäle) und OneDrive (Chats)
- Teams-Meetings nutzen Exchange Online Kalender für Terminplanung
- Conditional Access steuert den Zugriff auf Teams nach Gerät, Standort und Risiko

Schlüsselkonzepte

- **Externer Zugriff und Gastzugang:** Teams unterscheidet zwischen externem Zugriff (Federation mit anderen Tenants) und Gastzugang (Entra ID B2B-Gäste in Teams). Beide Kanäle müssen separat konfiguriert werden - eine offene Standardkonfiguration erlaubt unkontrollierte Kommunikation.
- **Meeting-Sicherheit:** Meeting-Policies steuern, wer Meetings beitreten kann, ob Lobby-Wartebereiche aktiv sind und welche Funktionen (Bildschirmfreigabe, Aufzeichnung) erlaubt sind. Ohne restriktive Policies können externe Teilnehmer unbemerkt Meetings beitreten.
- **App-Berechtigungen:** Teams erlaubt die Integration von Drittanbieter-Apps, die potenziell auf Unternehmensdaten zugreifen. Ohne eine restriktive App-Policy können Benutzer beliebige Apps installieren und damit unkontrollierte Datenflüsse erzeugen.

Einordnung für Entscheider

Dieser Bereich weist 1 kritische Sicherheitslücken auf. Zusätzlich wurden 14 Optimierungspotenziale identifiziert. Bei Nicht-Umsetzung bestehen unmittelbare Risiken für die Vertraulichkeit und Integrität der Unternehmensdaten. Die Geschäftsführung sollte die Umsetzung der Sofortmaßnahmen in diesem Bereich persönlich nachverfolgen.

KRITIKALITÄT:	Hoch
COMPLIANCE-RELEVANZ:	Kollaborationssicherheit relevant für DSGVO (Datenweitergabe) und Betriebsvereinbarungen
BETRIEBLICHE AUSWIRKUNG:	Unkontrollierte externe Kommunikation kann vertrauliche Informationen preisgeben

Handlungsempfehlung zu Teams

Im Rahmen der Analyse sind die folgenden kritischen Konfigurationsabweichungen aufgefallen, die zeitnah adressiert werden müssen:

MS365-177 PRIO 1 Fehlender Grundschutz

Kommunikation mit nicht verwalteten Teams-Benutzern deaktivieren

1. Befund:

Die Prüfung „Kommunikation mit nicht verwalteten Teams-Benutzern deaktivieren“ ist nicht erfüllt.

Microsoft Teams unterscheidet zwischen verwalteten (organisationsgebundenen) und nicht verwalteten (Consumer) Teams-Accounts. Consumer-Accounts sind private Microsoft-Konten, die keiner Organisation zugeordnet sind und keiner Unternehmens-Governance unterliegen. Die Kommunikation mit Consumer-Accounts ist standardmäßig aktiviert.

2. Warum kritisch?

Wenn die Kommunikation mit nicht verwalteten Teams-Benutzern (Consumer-Accounts) aktiviert ist, können Mitarbeiter mit privaten Teams- und Skype-Konten chatten. Private Accounts unterliegen keiner Unternehmens-Governance und stellen ein erhebliches Risiko für Datenabfluss und Social Engineering dar, da die Identität des Gegenübers nicht durch eine Organisation verifiziert wird.

Consumer-Accounts unterliegen keinen Sicherheitsrichtlinien und die Identität des Gegenübers kann nicht durch eine Organisation verifiziert werden. Die Deaktivierung schließt einen unkontrollierten Kommunikationskanal, der für Social Engineering missbraucht werden kann.

> SZENARIO: *Ein Angreifer erstellt einen privaten Teams-Consumer-Account mit dem Namen eines bekannten Geschäftspartners und kontaktiert einen Mitarbeiter. Im Chat fordert er vertrauliche Dokumente an, die der Mitarbeiter im Vertrauen auf die vermeintliche Identität bereitstellt.*

3. Wie zu schließen:

Teams Consumer Access (nicht verwaltete Benutzer) deaktivieren

Klickpfad:

1. Microsoft Teams Admin Center (admin.teams.microsoft.com) mit mindestens der Rolle Teams Administrator öffnen
2. Users → External access
3. ‘People in my organization can communicate with unmanaged Teams accounts’ auf Off → Save
4. Falls eine geschäftliche Notwendigkeit besteht und die Einstellung an bleiben muss: mindestens ‘External users with Teams accounts not managed by an organization can contact users in my organization’ deaktivieren und den Zugriff per External access policy auf einzelne Benutzer beschränken

MICROSOFT-DOKUMENTATION: https://learn.microsoft.com/en-us/microsoftteams/trusted-organizations-external-meetings-chat, https://learn.microsoft.com/en-us/powershell/module/microsoftteams/set-cstenantfederationconfiguration

4. Warum relevant für DSGVO, NIS2 und ISO 27001:

Private Teams-Konten unterliegen keiner Unternehmensverwaltung, die Identität des Gegenübers ist nicht durch eine Organisation bestätigt. Das Abschalten verringert das Risiko von Social Engineering und unkontrolliertem Abfluss personenbezogener Daten.

Art. 5 Abs. 1 lit. f DSGVO:	Integrität und Vertraulichkeit personenbezogener Daten
Art. 32 Abs. 1 lit. b DSGVO:	Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme
§ 30 Abs. 2 Nr. 10 BSIG (Art. 21 Abs. 2 lit. j NIS2):	Multi-Faktor-Authentifizierung, gesicherte Kommunikation und Notfallkommunikation
ISO/IEC 27001 A.5.14:	Informationsübertragung
ISO/IEC 27001 A.8.12:	Verhinderung von Datenlecks

Weitere Optimierungen (Prio 2)

14 OPTIMIERUNGEN NACH ART



ID	MASSNAHME	ART
MS365-184	Meeting: Anonyme Benutzer einschränken	Zusätzliche Härtung
MS365-194	Drittanbieter- und Custom Apps blockieren/einschränken	Zusätzliche Härtung
MS365-195	Externe Cloud-Speicher in Teams deaktivieren	Zusätzliche Härtung
MS365-191	Teams: Mindestens 2 Besitzer pro Team sicherstellen	Governance
MS365-196	Meldung von Sicherheitsbedenken in Teams aktivieren	Governance
MS365-176	Externen Zugriff einschränken (Domain-Whitelisting)	Betriebshygiene
MS365-179	Giphy-Dienst in Teams deaktivieren	Betriebshygiene
MS365-183	Meeting: Lobby-Bypass einschränken (nur eingeladene Benutzer)	Betriebshygiene
MS365-186	Meeting: Steuerungsübergabe an externe Teilnehmer deaktivieren	Betriebshygiene
MS365-187	Meeting: Präsentationsrecht und Bildschirmsteuerung einschränken	Betriebshygiene
MS365-189	Live Events: Standard-Aufzeichnung deaktivieren	Betriebshygiene
MS365-197	E-Mail-Einladungen für Teams-Meetings anpassen (Sicherheitshinweise)	Betriebshygiene
MS365-180	URL-Vorschau in Teams-Chats deaktivieren	Datenschutz
MS365-182	Meeting: Teilnahme-Report/Anwesenheitsbericht deaktivieren	Datenschutz

09

/Intune

Microsoft Intune Admin Center · https://intune.microsoft.com

15

PRIO 2 · OPTIMIERUNG

Was ist Intune?

Im Microsoft Intune Admin Center liegen Geräteverwaltung, Konformitätsrichtlinien, Verschlüsselung, Defender-Antivirus- und ASR-Richtlinien, LAPS und App-Schutz.

Rolle in der Microsoft 365 Architektur

Intune macht Geräte messbar: Erst konforme Geräte erlauben Conditional Access, Zugriffe an den Gerätezustand zu binden.

Abhängigkeiten zu anderen Diensten

- Conditional Access nutzt Intune Compliance-Status als Grant-Bedingung
- Defender for Endpoint liefert Risikosignale an Intune Compliance Policies
- Entra ID Hybrid Join verbindet On-Premises-Geräte mit der Cloud-Verwaltung

Schlüsselkonzepte

- **Compliance Policies:** Compliance Policies definieren Mindestanforderungen an Geräte: Betriebssystem-Version, Verschlüsselung, PIN-Komplexität, Jailbreak-Erkennung. Nicht-konforme Geräte können über Conditional Access automatisch vom Zugriff auf Unternehmensdaten ausgeschlossen werden.
- **BYOD vs. Corporate Devices:** Intune unterscheidet zwischen firmeneigenen und privaten Geräten (BYOD). Bei BYOD schützt App Protection (MAM) Unternehmensdaten innerhalb von Apps, ohne das gesamte Gerät zu verwalten - ein wichtiger Datenschutz-Kompromiss.
- **Configuration Profiles:** Configuration Profiles setzen Sicherheitseinstellungen auf Geräteebene durch: BitLocker-Verschlüsselung, Firewall-Regeln, Passwort-Policies. Sie ergänzen Compliance Policies, die nur den Zustand prüfen, um aktive Konfigurationsdurchsetzung.

Einordnung für Entscheider

Die Grundkonfiguration in diesem Bereich ist vorhanden. 15 Optimierungspotenziale wurden identifiziert, die den Sicherheitsreifegrad weiter erhöhen. Keine sofortige Eskalation erforderlich, aber die Umsetzung wird empfohlen.

KRITIKALITÄT:	Mittel
COMPLIANCE-RELEVANZ:	Gerätesicherheit zentral für DSGVO Art. 32 (technische Maßnahmen) und BSI-Grundschutz
BETRIEBLICHE AUSWIRKUNG:	Nicht verwaltete oder ungeschützte Geräte sind ein häufiges Einfallstor für Ransomware und Datenabfluss

Handlungsempfehlung zu Intune

Im Rahmen der Analyse wurden die folgenden Optimierungspotenziale identifiziert:



ID	MASSNAHME	ART
MS365-088	App-Schutzrichtlinien (MAM) für mobile Geräte erzwingen	Zusätzliche Härtung

ID	MASSNAHME	ART
MS365-201	Geräte ohne Konformitätsrichtlinie als ‘Nicht konform’ markieren	Zusätzliche Härtung
MS365-380	BitLocker-Vollverschlüsselung per Intune-Datenträgerrichtlinie vorgeben	Zusätzliche Härtung
MS365-381	Windows LAPS: lokale Administratorkennwörter per Intune verwalten	Zusätzliche Härtung
MS365-382	ASR-Standardschutzregeln per Intune konfigurieren	Zusätzliche Härtung
MS365-404	Defender Antivirus: Netzwerkschutz und Schutz vor unerwünschten Apps (PUA) einschalten	Zusätzliche Härtung
MS365-405	Defender Antivirus: Übernahme lokaler Ausschlüsse (Local Admin Merge) deaktivieren	Zusätzliche Härtung
MS365-204	Geräteanzahl pro Benutzer in Intune und Entra ID begrenzen	Feinjustierung
MS365-402	Defender Antivirus: Archive, Skripte, E-Mail, Wechseldatenträger, Netzwerkdateien scannen	Feinjustierung
MS365-403	Defender Antivirus: Cloud-Schutzniveau, Signaturen und Probenübermittlung schärfen	Feinjustierung
MS365-407	Defender Antivirus: Scanparameter auf Leistung abstimmen	Feinjustierung
MS365-277	Windows Feature Update Policies auf unterstützte Versionen umstellen	Betriebshygiene
MS365-406	Defender Antivirus: Scan planen, bereinigte Schadsoftware mindestens 30 Tage aufbewahren	Betriebshygiene
MS365-409	App Control: über Intune verteilten Apps vertrauen (Managed Installer)	Betriebshygiene
MS365-408	App Control for Business per Intune einrichten	Erweiterte Funktion

10

/Purview

Microsoft Purview Portal · https://purview.microsoft.com

6

PRIO 2 · OPTIMIERUNG

Was ist Purview?

Im Microsoft Purview Portal liegen Audit, Vertraulichkeitsbezeichnungen, Data Loss Prevention, Aufbewahrung und Insider-Risiko.

Rolle in der Microsoft 365 Architektur

Purview klassifiziert und schützt Daten unabhängig vom Speicherort und liefert die Protokolle für Nachweise und Aufklärung.

Abhängigkeiten zu anderen Diensten

- DLP-Policies greifen auf Exchange Online Transportebene und in SharePoint/OneDrive
- Sensitivity Labels nutzen Entra ID-Gruppen für automatische Zuweisungen
- Audit Logging erfasst Aktivitäten aus allen M365-Diensten zentral

Schlüsselkonzepte

- **Sensitivity Labels:** Sensitivity Labels klassifizieren und schützen Dokumente und E-Mails nach Vertraulichkeitsstufe. Sie können Verschlüsselung, Wasserzeichen und Zugriffseinschränkungen automatisch durchsetzen - unabhängig vom Speicherort.
- **Data Loss Prevention (DLP):** DLP-Policies erkennen und blockieren die unbeabsichtigte Weitergabe sensibler Daten wie Kreditkartennummern, Personalausweisnummern oder Gesundheitsdaten. Ohne DLP gibt es keine technische Kontrolle gegen Datenabfluss per E-Mail oder Freigabe.
- **Audit Logging:** Das Unified Audit Log erfasst Benutzer- und Admin-Aktivitäten über alle M365-Dienste. Es ist die Grundlage für Incident Response und forensische Analysen. Standardmäßig werden Logs nur 180 Tage aufbewahrt - für Compliance-Anforderungen ist oft eine längere Aufbewahrung erforderlich.

Einordnung für Entscheider

Die Grundkonfiguration in diesem Bereich ist vorhanden. 6 Optimierungspotenziale wurden identifiziert, die den Sicherheitsreifegrad weiter erhöhen. Keine sofortige Eskalation erforderlich, aber die Umsetzung wird empfohlen.

KRITIKALITÄT:	Mittel
COMPLIANCE-RELEVANZ:	Direkte Umsetzung von DSGVO-Anforderungen (Klassifizierung, DLP, Protokollierung)
BETRIEBLICHE AUSWIRKUNG:	Fehlende Protokolle machen Sicherheitsvorfälle nicht nachvollziehbar und erschweren die Aufklärung

Handlungsempfehlung zu Purview

Im Rahmen der Analyse wurden die folgenden Optimierungspotenziale identifiziert:

6 OPTIMIERUNGEN NACH ART



ID	MASSNAHME	ART
MS365-212	Default Sensitivity Label für interne Dokumente setzen	Governance

ID	MASSNAHME	ART
MS365-216	Vertraulichkeitsbezeichnungen für Dateien veröffentlichen (Basis für Copilot-Schutz)	Governance
MS365-256	Aufbewahrungsrichtlinien (Retention Policies) konfigurieren	Governance
MS365-211	Sensitivity Labels mit technischer Reglementierung konfigurieren	Erweiterte Funktion
MS365-213	Data Loss Prevention (DLP) Richtlinien einrichten	Erweiterte Funktion
MS365-214	DLP-Schutz für Kreditkarten, ITIN, SSN und personenbezogene Daten einrichten	Erweiterte Funktion

11

/Microsoft 365 Admin Center

Microsoft 365 Admin Center · https://admin.microsoft.com

5

PRIO 2 · OPTIMIERUNG

Was ist Microsoft 365 Admin Center?

Im Microsoft 365 Admin Center liegen die Organisationseinstellungen: Dienste und Add-ins, Domänen, Kennwortablauf, Self-Service-Käufe, Gruppen und Datenschutzoptionen der Microsoft-365-Apps.

Rolle in der Microsoft 365 Architektur

Hier wird festgelegt, welche Dienste und Funktionen im Unternehmen überhaupt zur Verfügung stehen.

Abhängigkeiten zu anderen Diensten

- Connected Experiences senden Office-Nutzungsdaten an Microsoft Cloud-Dienste
- Office-Store und Self-Service ermöglichen Benutzern unkontrollierte App-Installationen
- Viva und Delve aggregieren Benutzeraktivitäten über Exchange, SharePoint und Teams

Schlüsselkonzepte

- **Privacy by Default:** Gemäß DSGVO Art. 25 müssen Systeme datenschutzfreundlich vorkonfiguriert sein. In Microsoft 365 bedeutet das: Dienste die Nutzungsdaten sammeln oder an Dritte weitergeben sollten standardmäßig deaktiviert sein.
- **Self-Service-Kontrolle:** Self-Service-Funktionen wie Self-Service-Purchases, Office-Store und Trial-Lizenzen ermöglichen Benutzern eigenmächtiges Handeln ohne IT-Freigabe. Dies erzeugt Schatten-IT und erschwert Lizenz-Management.
- **Telemetrie und Diagnosedaten:** Microsoft 365 Dienste senden Telemetrie- und Diagnosedaten an Microsoft. Das Niveau lässt sich pro Dienst konfigurieren. Für datenschutzsensible Umgebungen sollte das Minimum eingestellt werden.

Einordnung für Entscheider

Die Grundkonfiguration in diesem Bereich ist vorhanden. 5 Optimierungspotenziale wurden identifiziert, die den Sicherheitsreifegrad weiter erhöhen. Keine sofortige Eskalation erforderlich, aber die Umsetzung wird empfohlen.

KRITIKALITÄT:	Mittel
COMPLIANCE-RELEVANZ:	DSGVO Art. 25 (Datenschutz durch Technikgestaltung): Dienste und Funktionen bewusst freigeben statt Standard übernehmen
BETRIEBLICHE AUSWIRKUNG:	Unkontrollierte Dienste erzeugen Schatten-IT und Datenverarbeitung ohne Sichtbarkeit für die IT

Handlungsempfehlung zu Microsoft 365 Admin Center

Im Rahmen der Analyse wurden die folgenden Optimierungspotenziale identifiziert:

5 OPTIMIERUNGEN NACH ART



ID	MASSNAHME	ART
MS365-222	Office-Store und Testversionen für Benutzer einschränken	Governance
MS365-234	Drittanbieter-Speicher in Office Online deaktivieren	Governance

ID	MASSNAHME	ART
MS365-265	Erstellung öffentlicher Gruppen einschränken und bestehende prüfen	Governance
MS365-226	Externe Kalenderfreigabe einschränken	Datenschutz
MS365-237	Benutzernamen in Microsoft 365 Reports anonymisieren	Datenschutz

12

Schlussfolgerung

Die durchgeführte Analyse zeigt, dass der Microsoft 365 Tenant des untersuchten Unternehmens über grundlegende Sicherheitskonfigurationen verfügt, jedoch in mehreren Bereichen gezielter Anpassungen bedarf.

Insgesamt wurden 14 kritische Konfigurationslücken identifiziert, die ein unmittelbares Risiko für die Vertraulichkeit, Integrität und Verfügbarkeit der Microsoft 365 Umgebung darstellen. Ohne Umsetzung der priorisierten Maßnahmen bestehen konkrete Angriffsvektoren, die von Angreifern aktiv ausgenutzt werden.

Darüber hinaus wurden 112 Optimierungspotenziale identifiziert. Diese stellen kein unmittelbares Risiko dar, erhöhen jedoch den Reifegrad der Sicherheitsarchitektur und verbessern die Compliance-Position des Unternehmens.

Es ist hervorzuheben, dass bereits zahlreiche Konfigurationen den empfohlenen Best Practices entsprechen - 181 von 340 geprüften Einstellungen sind konform. Dies zeigt, dass eine solide Basis vorhanden ist, auf der gezielt aufgebaut werden kann.

Die identifizierten Maßnahmen sind nach Priorität und Fachbereich geordnet und können schrittweise umgesetzt werden. Es wird empfohlen, mit den kritischen Findings in den Bereichen Identitätsmanagement und Conditional Access zu beginnen, da diese das Fundament der gesamten Microsoft 365 Sicherheitsarchitektur bilden.

Umsetzungsfahrplan

01 · ERSTE 30 TAGE	02 · FOLGEQUARTAL	03 · REGELBETRIEB	04 · ALS PROJEKT
14	**68**	**40**	**4**
PRIO 1	PRIO 2	PRIO 2	PRIO 2
Sofort	**Härten**	**Verstetigen**	**Ausbauen**
Kritische Lücken schließen, beginnend mit Identitäten und Conditional Access	Zusätzliche Härtung und Feinjustierung vorhandener Einstellungen	Governance, Betriebshygiene und Datenschutz als laufende Aufgaben	Erweiterte Funktionen mit Lizenz- oder Einführungsbedarf

Empfohlene Reihenfolge; die Zuordnung der Optimierungen folgt ihrer Begründung (Art). Zeiträume sind Richtwerte.

Für eine begleitete Umsetzung der Handlungsempfehlungen steht siller.consulting zur Verfügung.