100 Maßnahmen

Wie sicher ist Ihr Microsoft-365-Tenant?

Security Audit & Hardening Checkliste für Microsoft 365

Aaron Siller

Microsoft MVP &
Cloud Security Architect

Microsoft® Most Valuable Professional

siller.consulting
INTELLIGENCE FOR IT

Microsoft 365 Security Check

100 Maßnahmen

Erstellt von: Aaron Siller, Microsoft MVP & Cloud Security Architect

---

Wie sicher ist Ihr Microsoft-365-Tenant?

80 % aller erfolgreichen Angriffe auf Microsoft-365-Umgebungen nutzen weniger als fünf Schwachstellen: fehlendes MFA-Enforcement, offene Legacy-Protokolle, unkontrollierte App-Berechtigungen, fehlende Geräte-Compliance und deaktiviertes Audit Logging. Die meisten dieser Schwachstellen sind in weniger als einer Stunde behebbar — wenn man weiß, wo man suchen muss. Doch die Realität in DACH-Unternehmen zeigt ein anderes Bild: Selbst Organisationen mit dedizierten IT-Abteilungen betreiben ihre Microsoft-365-Tenants mit Konfigurationen, die Identity-basierte Angriffe, OAuth-Consent-Phishing und laterale Bewegung im Tenant ermöglichen. Fehlkonfigurationen bei Conditional Access, offene Gastzugriffe ohne Access Reviews und fehlende App-Governance sind keine Ausnahme — sie sind der Normalzustand in der Mehrheit der Tenants, die ich in Hardening-Projekten analysiere.

Die Angriffsfläche von Microsoft 365 geht weit über E-Mail und Passwörter hinaus. Angreifer nutzen Token Theft über kompromittierte Sessions, OAuth-Consent-Flows zur dauerhaften Persistenz im Tenant, überprivilegierte Enterprise Apps als Backdoor und unkontrollierte externe Freigaben als Datenabflusskanal. Jede dieser Schwachstellen existiert unabhängig von klassischer Perimeter-Security — sie liegt in der Konfiguration des Tenants selbst. Wer seinen Tenant nicht aktiv härtet, verlässt sich auf Microsofts Standardeinstellungen, die für Benutzerfreundlichkeit optimiert sind, nicht für Sicherheit.

Dieser Security Check richtet sich an IT-Leitungen, CISOs, Entscheider und IT-Administratoren, die den tatsächlichen Sicherheitsstatus ihrer Microsoft-365-Umgebung kennen müssen — nicht auf Basis von Annahmen, sondern anhand konkreter, prüfbarer Maßnahmen. Jeder der 100 Punkte beschreibt eine spezifische Konfiguration mit Begründung, warum sie notwendig ist, und dem exakten Konfigurationsort im Admin Center. Am Ende erhalten Sie einen Score, der zeigt, wo Ihr Tenant steht — und wo die größten Risiken liegen.

Für wen ist dieser Security Check?

- **IT-Leiter und CIOs** — Überblick über den Sicherheitsstatus der M365-Umgebung
- **CISOs und Security-Verantwortliche** — systematische Prüfung aller Angriffsflächen
- **Microsoft-365-Administratoren** — konkrete Handlungsanweisungen mit Navigationspfaden

So funktioniert der Check

1. **Tenant prüfen** — Arbeiten Sie die Checkliste Bereich für Bereich durch und dokumentieren Sie den Status jeder Maßnahme
2. **Maßnahmen priorisieren** — Beginnen Sie mit den Be reichen, in denen die meisten Punkte offen sind
3. **Security Score verbessern** — Setzen Sie offene Maßnahmen um und wiederholen Sie den Check regelmäßig

Wie diese Checkliste zu lesen ist

Jede Maßnahme beschreibt nicht nur eine Konfiguration, sondern einen konkreten Schutzmechanismus gegen typische Angriffspfade in Microsoft 365. Offene Punkte bedeuten daher nicht nur „fehlende Best Practice", sondern potenziell ausnutzbare Sicherheitslücken.

Warum diese Checkliste besonders relevant ist

Moderne Angriffe zielen nicht mehr nur auf Passwörter. Sie nutzen OAuth-Zustimmungen, Session-Tokens, ungemanagte Geräte, externe Freigaben und überprivilegierte Apps. Klassische „MFA an und fertig"-Sicherheit reicht nicht mehr aus. Dieser Check deckt die tatsächlichen Angriffsflächen ab, die in realen Tenant-Kompromittierungen ausgenutzt werden.

Die 5 häufigsten Microsoft-365-Angriffe

Angriffstyp	Ausgenutzte Schwachstelle	Abgedeckt in
MFA Fatigue / Push Abuse	Fehlende Number Matching, keine phishing-resistente MFA	Bereich 2, 3
Legacy Authentication Abuse	Offene IMAP/POP3/SMTP-Protokolle umgehen MFA	Bereich 3
OAuth Consent Phishing	Unkontrollierte App-Berechtigungen, fehlender Admin Consent Workflow	Bereich 7
Token Theft / Session Hijacking	Fehlende Token Protection, keine Sign-in Frequency	Bereich 3
Guest Account Abuse	Nicht auditierte Gäste, offene Collaboration Settings	Bereich 6

Arbeiten Sie die Punkte systematisch durch und dokumentieren Sie den Status. Punkte mit (P1) erfordern mindestens Entra ID P1, Punkte mit (P2) erfordern Entra ID P2.

Prioritäts-Kategorien

- ■ **Quick Win** — in unter 30 Minuten prüf- oder umsetzbar
- ■ **High Impact** — schließt häufige Angriffspfade
- ■ **Lizenzabhängig** — erfordert Entra ID P1/P2 oder Defender
- ■■ **Betriebsrelevant** — kann User Experience beeinflussen

1. Organisationseinstellungen

#	Maßnahme	Status	Anmerkung
1.1	Security Defaults Status geprüft		

Organisationseinstellungen wirken tenantweit. Eine offene Standardeinstellung erzeugt keinen Einzelfehler, sondern einen systemischen Angriffsraum. Security Defaults sind Microsofts Basisschutz für Tenants ohne Conditional Access. Die Prüfung stellt sicher, dass entweder Security Defaults aktiv sind oder durch eine vollständige CA-Konfiguration ersetzt wurden — ein Tenant ohne beides ist ungeschützt.

 Quick Win | **Konfigurationsort**: `Entra Admin Center → Overview → Properties → Manage Security defaults`

1.2. Organisationseinstellungen im Admin Center geprüft

Das M365 Admin Center enthält Standardeinstellungen, die externen Zugriff, App-Registrierungen und Self-Service-Funktionen regeln. Kritische Settings: User Consent, Gruppenerstellung, Self-Service Sign-up, App-Registrierungen. Ohne Prüfung bleiben Einstellungen aktiv, die Angreifern unnötige Angriffsfläche bieten.

 Quick Win | **Konfigurationsort:** `Microsoft 365 Admin Center → Settings → org settings → Security & privacy`

1.3 Sicherheitsrelevante Org-Settings angepasst

 High Impact | **Konfigurationsort:** `Microsoft 365 Admin Center → Settings → org settings`

Dazu gehören Einstellungen wie das Deaktivieren von User Consent für Apps, die Einschränkung von Gruppen-Erstellung und die Kontrolle externer Kalenderfreigaben. Jede offene Standardeinstellung ist ein potenzieller Angriffsvektor. Typischer Fehlzustand: Settings werden bei Tenant-Erstellung nicht angepasst und bleiben jahrelang auf Default.

Videos: M365 Hardening Teil 1: Organisationseinstellungen

2. Identity & MFA

#	Maßnahme	Status	Anmerkung
2.1	MFA-Status aller User geprüft (PowerShell)		

Nicht nur Policy-Zuweisung prüfen, sondern unterscheiden zwischen registrierten Methoden, tatsächlicher Nutzung und Ausschlüssen. In vielen Tenants ist MFA formal eingeführt, aber Break-Glass-, Service- oder Alt-Accounts sind ausgenommen. Ohne Überblick über den MFA-Status existieren Accounts ohne zweiten Faktor — das häufigste Einfallstor bei Identity-basierten Angriffen

 Quick Win | **Konfigurationsort:** `PowerShell (Get-MgUser + Get-MgUserAuthenticationMethod)`

2.2 Authentication Methods Policy konfiguriert

Die Policy steuert tenantweit oder gruppenbasiert, welche MFA-Methoden erlaubt sind. Dadurch können alte oder schwache Verfahren sauber abgekündigt werden. Ohne explizite Konfiguration können unsichere Methoden wie Telefonanrufe oder App-Passwörter aktiv bleiben.

 High Impact | **Konfigurationsort:** `Entra Admin Center → Protection → Authentication methods → Policies`

2.3 SMS als MFA-Methode deaktiviert

SMS ist kein phishing-resistenter Faktor. Der Schutz basiert auf Besitz des Mobilfunkkanals, nicht auf kryptografischer Bindung an den Anmeldevorgang. SIM-Swapping und SS7-Angriffe umgehen diesen Schutz. Die Authenticator App oder FIDO2-Keys bieten nachweislich höheren Schutz.

 Quick Win | **Konfigurationsort:** `Entra Admin Center → Protection → Authentication methods → Policies → SMS`

2.4 Number Matching für Authenticator bestätigt

Number Matching schützt konkret gegen MFA Prompt Bombing. Die Bestätigung wird an einen sichtbaren Login-Kontext gekoppelt, nicht nur als Approve/Deny durchgeführt. Ohne Number Matching können Angreifer MFA-Fatigue-Angriffe durchführen — massenhaftes Senden von Push-Anfragen, bis der User versehentlich bestätigt.

 Quick Win | **Konfigurationsort:** `Entra Admin Center → Protection → Authentication methods → Microsoft Authenticator → Settings`

2.5 MFA Registration Campaign aktiviert

Die Registration Campaign fordert User proaktiv auf, sich für die Authenticator App zu registrieren. Ohne aktive Kampagne bleiben User bei schwächeren Methoden oder registrieren sich gar nicht.

 Quick Win | **Konfigurationsort:** Entra Admin Center → Protection → Authentication methods → Registration campaign

2.6 Self-Service Password Reset (SSPR) aktiviert

SSPR reduziert Helpdesk-Tickets und sorgt dafür, dass Passwort-Resets sicher über MFA-verifizierte Kanäle laufen. Ohne SSPR rufen User den Support an — ein Prozess, der anfällig für Social Engineering ist.

 High Impact ·· Betriebsrelevant | **Konfigurationsort:** Entra Admin Center → Protection → Password reset

2.7 Entra ID Protection konfiguriert (P2)

Risiko wird nicht nur anhand des Passworts bewertet, sondern anhand von Signalen wie IP-Reputation, Leaked Credentials, atypischen Standorten und Verhaltensmustern. Das macht Identitätsschutz adaptiv statt statisch. Ohne diese Erkennung bleiben kompromittierte Accounts unentdeckt, bis der Schaden sichtbar wird.

 High Impact · Lizenzabhängig | **Konfigurationsort:** Entra Admin Center → Protection → Identity Protection

2.8 User Risk Policy: Remediation bei Medium/High

Bei erkanntem User-Risiko (z.B. geleakte Credentials) erzwingt die Policy eine Passwortänderung. Ohne automatische Remediation bleibt der kompromittierte Account aktiv, bis ein Admin manuell eingreift.

 High Impact · Lizenzabhängig | **Konfigurationsort:** Entra Admin Center → Protection → Identity Protection → User risk policy

2.9 Self-Service Password Reset (SSPR) korrekt konfiguriert

SSPR muss mit MFA-Registrierung kombiniert werden. Ohne SSPR-Policy müssen Admins Passwörter manuell zurücksetzen — das erzeugt Helpdesk-Last und Social-Engineering-Risiko. SSPR ohne MFA-Pflicht erlaubt Angreifern, Passwörter über kompromittierte E-Mail-Adressen zurückzusetzen.

 Quick Win | **Konfigurationsort:** `Entra Admin Center → Protection → Password reset`

2.10	Passwort-Schutz (Banned Passwords) aktiviert

Entra ID Password Protection sperrt häufig verwendete und organisationsspezifische Passwörter. Ohne Custom Banned Password List nutzen Mitarbeiter vorhersagbare Passwörter wie Firmenname+Jahr.
Die globale Liste deckt nur bekannte schwache Passwörter ab — Custom Lists schützen gegen organisationsspezifische Muster.

 High Impact | **Konfigurationsort:** `Entra Admin Center → Protection → Authentication methods → Password protection`

2.11.	Sign-in Risk Policy: MFA bei Medium, Block bei High

Die Sign-in Risk Policy reagiert auf verdächtige Anmeldungen in Echtzeit. Bei mittlerem Risiko wird zusätzlich MFA verlangt, bei hohem Risiko wird der Zugriff komplett blockiert — das verhindert aktive Account-Übernahmen.

 High Impact · Lizenzabhängig | **Konfigurationsort:** `Entra Admin Center → Protection → Identity Protection → Sign-in risk policy`

Videos: MFA-Fehler vermeiden | MFA-Bypass verhindern | Entra ID Protection

Zwischenauswertung: Wenn in diesem Bereich mehr als 3 Punkte offen sind, besteht ein erhöhtes Risiko für Identity-basierte Angriffe. → **Tenant Security Check empfohlen**

3. Conditional Access

#	Maßnahme	Status	Anmerkung
3.1	CA-001: MFA für alle User (P1)		

Die Basis-Policy: Jeder Zugriff auf M365-Ressourcen erfordert MFA. Ohne diese Policy können Angreifer mit gestohlenen Passwörtern direkt auf den Tenant zugreifen. Conditional Access ist granularer als Security Defaults.

 High Impact · Lizenzabhängig | **Konfigurationsort:** `Entra Admin Center → Protection → Conditional Access → Policies → New policy`

3.2 CA-002: Legacy Authentication blockieren (P1)

Legacy-Protokolle wie IMAP, POP3 und SMTP Basic Auth authentifizieren sich außerhalb moderner tokenbasierter Richtlinien. MFA- und Session-Kontrollen greifen nicht. Das Blockieren ist ein direkter Bypass-Blocker.

 High Impact · Lizenzabhängig | **Konfigurationsort:** `Entra Admin Center → Protection → Conditional Access → Policies`

3.3 CA-003: Admin-Zugriff auf Named Locations beschränken (P1)

Admin-Zugriffe nur aus bekannten Netzwerken zuzulassen schränkt die Angriffsfläche für privilegierte Accounts massiv ein. Ein kompromittierter Admin-Account kann aus einem unbekannten Netzwerk dann nicht genutzt werden.

 High Impact · Lizenzabhängig | **Konfigurationsort:** `Entra Admin Center → Protection → Conditional Access → Policies`

3.4 CA-004: Compliant Device für M365-Zugriff erforderlich (P1)

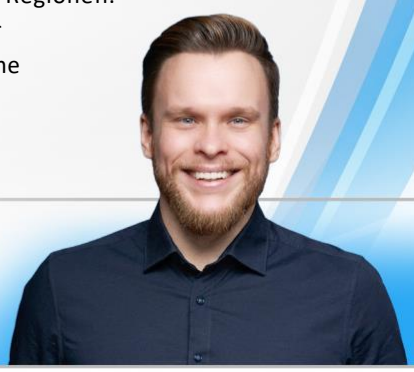
Diese Einstellung verbindet Identität und Gerätezustand. Der Zugriff wird nicht allein aufgrund des Benutzerkontos erlaubt, sondern anhand des von Intune gemeldeten Compliance-Status.
Nicht-compliant Geräte werden automatisch blockiert — die Brücke zwischen Identity und Endpoint Security.

Abhängigkeit: Erfordert konfigurierte Intune Compliance Policies (Bereich 8).

 High Impact · Lizenzabhängig ·· Betriebsrelevant | **Konfigurationsort:** `Entra Admin Center → Protection → Conditional Access → Policies`

3.5 CA-005: Sign-ins aus Hochrisiko-Ländern blockieren (P1)

Ein Großteil automatisierter Credential-Stuffing-Angriffe stammt aus wenigen Regionen. Das Blockieren von Ländern, in denen die Organisation keine Mitarbeiter oder Geschäftspartner hat, reduziert das Angriffsvolumen erheblich — ohne legitime User zu beeinträchtigen.



 High Impact · Lizenzabhängig | **Konfigurationsort:** `Entra Admin Center → Protection → Conditional Access → Policies`

3.6 CA-006: MFA für Azure Management erzwingen (P1)

Viele Tenants sichern nur M365-Apps mit MFA, aber nicht das Azure Portal, Azure PowerShell und Azure CLI. Angreifer nutzen diese Lücke gezielt: Ein kompromittierter Account ohne Azure-MFA kann Subscriptions, Ressourcen und IAM-Rollen manipulieren.

 High Impact · Lizenzabhängig | **Konfigurationsort:** `Entra Admin Center → Protection → Conditional Access → Policies`

3.7 CA-007: Phishing-resistente MFA für Admins (P1)

Microsoft empfiehlt FIDO2, Passkeys oder Certificate-Based Authentication. Diese Methoden sind immun gegen Phishing, Token Theft und Adversary-in-the-Middle-Angriffe.

Abhängigkeit: Wirkt am stärksten, wenn gleichzeitig Legacy Authentication blockiert ist (CA-002).

 High Impact · Lizenzabhängig | **Konfigurationsort:** `Entra Admin Center → Protection → Conditional Access → Policies → Grant → Require authentication strength`

3.8 CA-008: Sign-in Frequency und Persistent Browser steuern (P1)

Reduziert die Lebensdauer verwertbarer Sitzungen. Besonders relevant bei Token Theft, Session Hijacking oder gemeinsam genutzten Geräten. Die Policy erzwingt regelmäßige Re-Authentifizierung (z.B. alle 4 Stunden für sensible Apps) und deaktiviert persistente Browser-Sessions auf nicht-verwalteten Geräten.

 High Impact · Lizenzabhängig | **Konfigurationsort:** `Entra Admin Center → Protection → Conditional Access → Policies → Session`

3.9 CA-009: Ungemanagte Geräte auf Web-Only beschränken (P1)

Zugriff auf Inhalte bleibt möglich, ohne lokale Datenhaltung zu erlauben. Collaboration wird nicht blockiert, aber Datenabfluss über Downloads, Synchronisierung oder Offline-Kopien reduziert. Auf nicht-verwalteten Geräten (BYOD ohne Intune) sollte der Zugriff auf Browser-Only eingeschränkt werden, ohne Download-Möglichkeit.

 High Impact · Lizenzabhängig ·· Betriebsrelevant | **Konfigurationsort:** `Entra Admin Center → Protection → Conditional Access → Policies → Session`

3.10 CA-010: Terms of Use für externen Zugriff (P1)

Eine Terms-of-Use-Policy erzwingt, dass Gäste und externe Partner Nutzungsbedingungen akzeptieren, bevor sie auf Tenant-Ressourcen zugreifen. Das schafft eine dokumentierte Rechtsgrundlage und macht externe Zugriffe nachvollziehbar — relevant für DSGVO und Compliance-Audits.

 Lizenzabhängig ·· Betriebsrelevant | **Konfigurationsort:** `Entra Admin Center → Protection → Conditional Access → Policies → Grant → Require terms of use`

3.11 Emergency Access Accounts erstellt (mind. 2)

Technisch sind diese Konten bewusst aus bestimmten Zugriffskontrollen ausgenommen, damit auch bei Fehlkonfigurationen oder MFA-Ausfällen administrativer Zugriff möglich bleibt. Schutz entsteht durch Isolation, starke Passwörter und sichere Verwahrung. Ohne diese Accounts kann ein Lockout den gesamten Tenant unzugänglich machen.

 High Impact | **Konfigurationsort:** `Entra Admin Center → Users → New user (dedizierte Break-Glass-Accounts)`

3.12 Emergency Access Accounts dokumentiert und sicher verwahrt

Die Credentials der Break-Glass-Accounts müssen in einem physischen Safe oder gleichwertig gesicherten Speicher liegen. Undokumentierte Emergency Accounts sind im Ernstfall wertlos, wenn niemand die Zugangsdaten findet.

 Quick Win | **Konfigurationsort:** `Physischer Safe / Passwort-Manager (offline)`

3.13 Named Locations mit Office-IPs eingerichtet

Named Locations definieren vertrauenswürdige Netzwerke (Büro-IPs, VPN-Ranges). Damit können CA-Policies zwischen internen und externen Zugriffen unterscheiden — Grundlage für standortbasierte Zugriffskontrolle.

 Quick Win · Lizenzabhängig | **Konfigurationsort:** `Entra Admin Center → Protection → Conditional Access → Named locations`

3.14 GPS/Named Locations für Conditional Access konfiguriert

Named Locations ermöglichen standortbasierte Zugriffsteuerung. Ohne definierte Standorte können Conditional-Access-Policies nicht zwischen internen und externen Zugriffen unterscheiden. Typischer Fehlzustand: Alle Zugriffe werden gleich behandelt, unabhängig ob sie aus dem Firmennetz oder einem fremden Land kommen.

 Lizenzabhängig | **Konfigurationsort:** `Entra Admin Center → Protection → Conditional Access → Named locations`

3.15 Conditional Access Baseline Policies dokumentiert

Ohne dokumentierte Baseline-Policies fehlt die Grundlage für konsistente Zugriffssteuerung. Mindestens die 10 oben genannten CA-Policies als Baseline definieren und dokumentieren. Fehlende Baselines führen zu Lücken, die erst bei einem Incident sichtbar werden.

 High Impact | **Konfigurationsort:** `Entra Admin Center → Protection → Conditional Access → Policies`

3.16 Alle Policies in Report-only getestet (7 Tage)

Report-only-Modus zeigt, welche Anmeldungen von einer Policy betroffen wären, ohne sie tatsächlich zu blockieren. Ohne diesen Test riskiert man, legitime User auszusperren oder geschäftskritische Workflows zu unterbrechen.

 Quick Win · Lizenzabhängig | **Konfigurationsort:** `Entra Admin Center → Protection → Conditional Access → Policies → Enable policy → Report-only`

3.17 Security Defaults deaktiviert (erst nach CA-Aktivierung)

Security Defaults und Conditional Access können nicht gleichzeitig aktiv sein. Security Defaults müssen deaktiviert werden — aber erst, nachdem die CA-Policies produktiv sind.
Die Reihenfolge ist kritisch: erst CA aktivieren, dann Defaults deaktivieren.

 Quick Win | **Konfigurationsort:** `Entra Admin Center → Overview → Properties → Manage Security defaults → Disabled`

Videos: CA Must Haves | Erweiterte CA

Zwischenauswertung: Conditional Access ist das Fundament jeder Zero-Trust-Architektur. Wenn mehr als 5 Punkte in diesem Bereich offen sind, fehlt eine wirksame Zugriffskontrolle. → **Tenant Security Check empfohlen**

4. Admin-Rollen & PIM

#	Maßnahme	Status	Anmerkung
4.1	Admin-Rollen-Audit durchgeführt (PowerShell)		

Ein Audit deckt auf, welche Accounts privilegierte Rollen besitzen — häufig finden sich verwaiste Service-Accounts oder User mit unnötigen Berechtigungen. Jeder überflüssige Admin-Account ist ein zusätzlicher Angriffsvektor.

 Quick Win | **Konfigurationsort:** `PowerShell (Get-MgDirectoryRoleMember) oder Entra Admin Center → Roles and administrators`

4.2	Global Admin auf max. 2 permanente Accounts reduziert		

Permanente Global-Admin-Zuweisungen vergrößern die Blast Radius erheblich. Wichtig ist nicht nur die Anzahl, sondern auch die Trennung zwischen Alltagskonto und Admin-Konto. Global Admin hat uneingeschränkten Zugriff auf alle Daten und Einstellungen im Tenant.

 High Impact | **Konfigurationsort:** `Entra Admin Center → Roles and administrators → Global administrator`

4.3	Spezialisierte Rollen statt Global Admin zugewiesen		

Least Privilege bedeutet: Ein Exchange-Admin braucht keinen Global Admin. Spezialisierte Rollen wie Exchange Administrator, Security Administrator oder User Administrator begrenzen den Schaden bei Account-Kompromittierung.

 High Impact | **Konfigurationsort:** `Entra Admin Center → Roles and administrators`

4.4 PIM für Global Admin aktiviert (P2)

PIM reduziert Standing Privilege. Hohe Rechte existieren nicht dauerhaft aktiv, sondern werden nur zeitweise, nachvollziehbar und mit zusätzlicher Bestätigung freigeschaltet. Standing Access wird eliminiert.

 High Impact · Lizenzabhängig | **Konfigurationsort:** `Entra Admin Center → Identity Governance → Privileged Identity Management`

4.5 PIM für weitere privilegierte Rollen aktiviert (P2)

Neben Global Admin sollten auch Exchange Admin, SharePoint Admin, Security Admin und weitere privilegierte Rollen über PIM verwaltet werden. Jede dauerhaft zugewiesene privilegierte Rolle ist ein Risiko.

 High Impact · Lizenzabhängig | **Konfigurationsort:** `Entra Admin Center → Identity Governance → Privileged Identity Management → Entra ID roles`

4.6 Activation-Dauer, MFA und Genehmigung konfiguriert

Die PIM-Konfiguration definiert, wie lange eine Rolle aktiv bleibt (z.B. 4 Stunden), ob MFA bei Aktivierung erforderlich ist und ob ein Genehmigungsworkflow greift. Zu lange Aktivierungsdauern untergraben den Zweck von PIM.

 Lizenzabhängig | **Konfigurationsort:** `PIM → Settings → Role settings`

4.7 Access Reviews für privilegierte Rollen eingerichtet (P2)

Access Reviews verhindern Berechtigungsdrift — Rollen, die über Projekte, Jobwechsel oder historische Sonderfälle unkontrolliert bestehen bleiben (Permission Creep). Ohne Reviews sammeln sich über Monate und Jahre Berechtigungen an, die längst nicht mehr benötigt werden.

 Lizenzabhängig | **Konfigurationsort:** `Entra Admin Center → Identity Governance → Access reviews`

4.8	Emergency Access Accounts (Break Glass) konfiguriert			

Ohne Break-Glass-Accounts kann ein Lockout durch fehlerhafte CA-Policies oder MFA-Ausfälle den gesamten Tenant unzugänglich machen. Mindestens 2 Emergency-Accounts, cloud-only, ohne MFA, mit Global Admin Rolle, sicher verwahrt und monatlich getestet. Fehlende Break-Glass-Accounts sind eines der häufigsten Versäumnisse.

 High Impact | **Konfigurationsort:** `Entra Admin Center → Identity → Users → Create emergency access accounts`

Videos: Admins & Rollen (Teil 8) | PIM (Teil 12)

5. E-Mail-Security

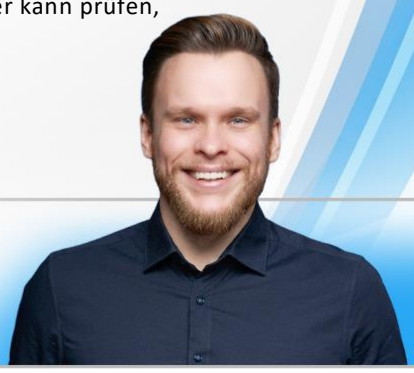
#	Maßnahme	Status	Anmerkung
5.1	SPF-Record geprüft und auf `-all` gesetzt		

SPF prüft den sendenden Server gegen veröffentlichte DNS-Einträge. Technisch schützt es vor Envelope-Spoofing, reicht allein aber nicht für vollständigen Domänenschutz. -all weist empfangende Server an, alle nicht autorisierten Absender abzulehnen.

 Quick Win | **Konfigurationsort:** `DNS-Management (TXT-Record) + Prüfung via mxtoolbox.com`

5.2	DKIM aktiviert und DNS-Records eingetragen			

DKIM versieht Nachrichten mit einer kryptografischen Signatur. Der Empfänger kann prüfen, ob der Mailinhalt auf dem Transportweg verändert wurde. Ohne DKIM fehlt die Integritätsprüfung.



 Quick Win | **Konfigurationsort:** `Microsoft 365 Defender Portal → Email & collaboration → Policies → DKIM`

5.3 DMARC eingerichtet (Ziel: `p=reject`)

DMARC setzt SPF und DKIM in eine Richtlinie um und liefert Reporting. Technisch entscheidend ist das Alignment: Die Übereinstimmung von sichtbarer Absenderdomain und Authentifizierungsdomäne. p=reject weist Empfänger-Server an, gefälschte E-Mails abzulehnen — der stärkste Schutz gegen Domain-Spoofing.

 High Impact | **Konfigurationsort:** `DNS-Management (TXT-Record: _dmarc.domain.tld)`

5.4 Anti-Phishing Policy: Impersonation Protection aktiv

Impersonation Protection erkennt E-Mails, die vortäuschen, von Führungskräften oder bekannten Partnern zu stammen. CEO-Fraud und Business Email Compromise (BEC) nutzen genau diese Technik der Schaden liegt häufig im sechsstelligen Bereich.

 High Impact · Lizenzabhängig | **Konfigurationsort:** `security.microsoft.com → Policies → Anti-phishing`

5.5 Anti-Spam Policy: BCL angepasst

Der Bulk Complaint Level (BCL) steuert, wie aggressiv Massen-E-Mails gefiltert werden. Die Standardeinstellung ist zu permissiv — eine Anpassung reduziert unerwünschte Mails, ohne legitime Kommunikation zu blockieren.

 Quick Win | **Konfigurationsort:** `security.microsoft.com → Policies → Anti-spam`

5.6 Anti-Malware Policy: Attachment Types Filter aktiv

Der Attachment Types Filter blockiert gefährliche Dateitypen (.exe, .js, .vbs, .scr) bereits am Gateway. Ohne diesen Filter können User Malware-Anhänge empfangen und öffnen — ein klassischer Angriffsvektor.

 Quick Win | **Konfigurationsort:** `security.microsoft.com → Policies → Anti-malware`

5.7 Safe Links konfiguriert (Defender P1/P2)

Safe Links ist vor allem gegen verzögert aktivierte Phishing-Ziele wirksam. Die Prüfung erfolgt zum Klickzeitpunkt, nicht nur beim Nachrichteneingang. Angreifer nutzen Time-of-Click-Angriffe: Die URL ist beim Empfang harmlos und wird erst Stunden später auf eine Phishing-Seite umgeleitet.

 High Impact · Lizenzabhängig | **Konfigurationsort:** `security.microsoft.com → Policies → Safe Links`

5.8 Safe Attachments konfiguriert (Defender P1/P2)

Safe Attachments ergänzt signaturbasierte Erkennung durch verhaltensbasierte Analyse in isolierten Umgebungen (Sandboxing). Wirksam bei unbekannter Malware und neu gepackten Dateiformaten. Zero-Day-Malware, die signaturbasierte Scanner nicht erkennen, wird so abgefangen.

 High Impact · Lizenzabhängig | **Konfigurationsort:** `security.microsoft.com → Policies → Safe Attachments`

5.9 Transport Rule: Externe E-Mails kennzeichnen

Die Maßnahme ist kein technischer Blocker, sondern eine Awareness-Verstärkung — visuelle Kontextinformation für den Benutzer. Das sensibilisiert User für potenzielle Phishing-Mails und reduziert die Erfolgsquote von Social Engineering.

 Quick Win | **Konfigurationsort:** `Exchange Admin Center → Mail flow → Rules`

Videos: Defender XDR: Anti-Phishing, Spam & Malware

Zwischenauswertung: E-Mail ist der primäre Angriffsvektor. Wenn SPF/DKIM/DMARC oder Safe Links/Attachments fehlen, ist der Tenant akut gefährdet. → **Tenant Security Check empfohlen**

6. Collaboration Security

#	Maßnahme	Status	Anmerkung
6.1	SharePoint External Sharing eingeschränkt		

Standardmäßig erlaubt SharePoint das Teilen mit externen Personen — auch anonym. Ohne Einschränkung können Mitarbeiter sensible Dokumente unkontrolliert nach außen teilen, was DSGVO-Verstöße und Datenverlust verursacht.

 High Impact ·· Betriebsrelevant | **Konfigurationsort:** `SharePoint Admin Center → Policies → Sharing`

6.2	"Anyone"-Links deaktiviert		

Anonyme Freigabelinks entkoppeln den Zugriff vollständig von Identität. Es gibt keine belastbare Zuordnung zu einem Benutzerkonto und damit nur eingeschränkte Nachvollziehbarkeit. Diese Links können weitergeleitet werden und stellen das größte Datenabflussrisiko in SharePoint dar.

 High Impact | **Konfigurationsort:** `SharePoint Admin Center → Policies → Sharing → „Anyone" Links deaktivieren`

6.3	Sensible Sites individuell eingeschränkt		

SharePoint Sites mit sensiblen Daten (HR, Finanzen, Geschäftsleitung) benötigen strengere Sharing-Einstellungen als die Org-weite Policy. Individuelle Einschränkungen verhindern, dass die allgemeine Regel zu permissiv für kritische Bereiche ist.

 Betriebsrelevant | **Konfigurationsort:** `SharePoint Admin Center → Sites → Active sites → [Site] → Sharing`

6.4	External Identities: Guest Invite Restrictions konfiguriert		

Je offener Gast-Einladungen geregelt sind, desto stärker wächst die externe Angriffsfläche über Zeit. Gastkonten leben oft in Gruppen, Teams, Sites und Dateien weiter, auch wenn die ursprüngliche Zusammenarbeit beendet ist. Die Einschränkung auf Admins oder bestimmte Gruppen verhindert unkontrolliertes Wachstum externer Identitäten im Tenant.

 High Impact | **Konfigurationsort:** `Entra Admin Center → External Identities → External collaboration settings`

6.5 Bestehende Gäste auditiert (inaktive entfernen)

Gäste-Accounts, die monatelang nicht genutzt wurden, sind ein Sicherheitsrisiko: Sie sind oft vergessen, aber weiterhin zugriffsberechtigt. Regelmäßiges Auditing und Entfernen inaktiver Gäste reduziert die Angriffsfläche.

 Quick Win | **Konfigurationsort:** `PowerShell (Get-MgUser -Filter "userType eq 'Guest'") oder Entra Admin Center → Users → Guest users`

6.6 Collaboration Restrictions: Domain Allow/Deny-List

Domain-basierte Einschränkungen steuern, mit welchen externen Organisationen zusammengearbeitet werden darf. Eine Allow-List begrenzt Sharing auf bekannte Partner, eine Deny-List blockiert bekannte Risiko-Domains.

·· **Betriebsrelevant** | **Konfigurationsort:** `Entra Admin Center → External Identities → External collaboration settings → Collaboration restrictions`

6.7 Teams Guest Access eingeschränkt

Gäste in Teams können standardmäßig auf Chats, Dateien und Kanäle zugreifen. Ohne Einschränkung erhalten externe Personen möglicherweise Zugang zu internen Diskussionen und Dokumenten, die nicht für sie bestimmt sind.

 High Impact ·· Betriebsrelevant | **Konfigurationsort:** `Teams Admin Center → Users → Guest access`

6.8 Gastzugriff kontrolliert und eingeschränkt

Unkontrollierter Gastzugriff ist eine der häufigsten Schwachstellen in M365-Tenants. Ohne Einschränkungen können Gäste auf SharePoint-Sites, Teams-Kanäle und Gruppen zugreifen. Guest Access Policies müssen definieren: wer Gäste einladen darf, welche Berechtigungen Gäste erhalten und wie lange Gastzugriffe gültig sind.

 High Impact | **Konfigurationsort:** `Entra Admin Center → Identity → External Identities → External collaboration settings`

6.9 Gastzugriff regelmäßig auditiert (Access Reviews)

Ohne regelmäßige Access Reviews bleiben Gastkonten aktiv, lange nachdem die Zusammenarbeit beendet ist. Entra ID Access Reviews automatisieren die Überprüfung. Typischer Fehlzustand: Hunderte Gastkonten ohne letzte Anmeldung in 180+ Tagen, mit Zugriff auf sensible SharePoint-Sites.

 Lizenzabhängig | **Konfigurationsort:** `Entra Admin Center → Identity Governance → Access reviews`

6.10 Teams App Permission Policies konfiguriert

Apps in Teams sind nicht nur Komfortfunktionen, sondern Integrationen mit eigenem Berechtigungsmodell und API-Zugriff auf Tenant-Daten. Die Policy beschränkt verfügbare Apps auf geprüfte und freigegebene Anwendungen.

 High Impact | **Konfigurationsort:** `Teams Admin Center → Teams apps → Permission policies`

6.11 Teams-Erstellung auf Security Group beschränkt

Unkontrollierte Teams-Erstellung führt zu Wildwuchs: doppelte Teams, keine Namenskonvention, fehlende Governance. Die Beschränkung auf eine Security Group stellt sicher, dass Teams bewusst und strukturiert angelegt werden.

·· **Betriebsrelevant** | **Konfigurationsort:** `PowerShell (Set-MgGroupSetting) oder Entra Admin Center → Groups → General`

Videos: SharePoint Security | Datei-Sharing | External Identities | Sharing Policies

7. App Security & Governance

#	Maßnahme	Status	Anmerkung
7.1	User Consent für Enterprise Apps deaktiviert		

Bei OAuth-Consent-Phishing gibt der Benutzer einer scheinbar legitimen Anwendung direkt Zugriff auf Daten. Der Angriff zielt nicht auf Passwortdiebstahl, sondern auf autorisierte Token-Vergabe durch den User selbst. Ohne Deaktivierung von User Consent ist jeder User ein potenzielles Einfallstor.

 High Impact | **Konfigurationsort:** `Entra Admin Center → Identity → Applications → Enterprise applications → Consent and permissions → User consent settings`

7.2	Admin Consent Workflow konfiguriert		

Nach Deaktivierung von User Consent brauchen User einen Weg, Apps anzufordern. Der Admin Consent Workflow leitet Anfragen an Admins weiter, die Berechtigungen prüfen und genehmigen oder ablehnen. Ohne Workflow umgehen User die Einschränkung oder wenden sich an den Helpdesk.

 High Impact | **Konfigurationsort:** `Entra Admin Center → Identity → Applications → Enterprise applications → Consent and permissions → Admin consent settings`

7.3	Bestehende Enterprise Apps auditiert		

Wichtig ist die Unterscheidung zwischen Delegated Permissions und Application Permissions. Vor allem App-Rechte wie Mail.Read, Files.ReadWrite.All oder Directory.Read.All exponieren den Tenant auch ohne kompromittierten User. Ein Audit deckt überprivilegierte und verwaiste Apps auf.

 Quick Win | **Konfigurationsort:** `Entra Admin Center → Identity → Applications → Enterprise applications → All applications`

7.4	App Secrets und Certificates Expiry überwacht		

Abgelaufene Secrets führen zu Ausfällen, aber vergessene Secrets sind ein Sicherheitsrisiko: Wer den Secret-Wert hat, kann sich als die App authentifizieren. Monitoring mit automatischen Benachrichtigungen vor Ablauf verhindert beides.

 Quick Win | **Konfigurationsort:** `Entra Admin Center → Identity → Applications → App registrations → [App] → Certificates & secrets`

7.5	Cross-Tenant Access Settings konfiguriert

Diese Einstellungen steuern Vertrauen zwischen Entra-ID-Umgebungen. Inbound- und Outbound-Regeln müssen explizit definiert werden, da Standardwerte oft nicht zum tatsächlichen Kollaborationsmodell passen. Ohne Konfiguration gelten die Standardeinstellungen — die in vielen Fällen zu permissiv sind.

 High Impact | **Konfigurationsort:** `Entra Admin Center → External Identities → Cross-tenant access settings`

Zwischenauswertung: App-basierte Angriffe (OAuth Consent Phishing, Token Theft über Enterprise Apps) nehmen stark zu. Wenn User Consent noch aktiv ist, besteht unmittelbarer Handlungsbedarf. → **Tenant Security Check empfohlen**

8. Endpoint Security

#	Maßnahme	Status	Anmerkung
8.1	Geräteplattform-Einschränkungen konfiguriert		

Plattform-Einschränkungen definieren, welche Betriebssysteme auf M365-Ressourcen zugreifen dürfen. Ohne diese Einschränkung können ungemanagte oder unsichere Geräte (z.B. gerootete Android-Phones) auf Unternehmensdaten zugreifen.

·· **Betriebsrelevant** | **Konfigurationsort:** `Intune Admin Center → Devices → Enrollment restrictions`

8.2	Windows Compliance Policy erstellt

Compliance ist mehr als Geräteinventar. Der Status entscheidet direkt über Zugriff. Gerätesicherheit wird zum aktiven Bestandteil der Zugangskontrolle. Nur Geräte, die alle Compliance-Anforderungen erfüllen, gelten als compliant — Grundlage für gerätebasierte CA-Policies.

Abhängigkeit: Compliance Policies entfalten ihren vollen Wert erst zusammen mit Conditional Access (3.7 — Compliant Device erforderlich).

 High Impact | **Konfigurationsort:** `Intune Admin Center → Devices → Compliance policies`

8.3 BitLocker als Requirement aktiv

Verschlüsselung entfaltet ihren vollen Wert nur, wenn Recovery-Key-Prozesse, Geräteinventarisierung und Ausnahmeregeln sauber verwaltet werden. BitLocker verschlüsselt die gesamte Festplatte. Bei Verlust oder Diebstahl eines Geräts sind die Daten ohne den Recovery Key nicht lesbar — ein DSGVO-Risiko ohne Verschlüsselungspflicht.

 High Impact | **Konfigurationsort:** `Intune Admin Center → Devices → Configuration profiles → Endpoint protection → BitLocker`

8.4 Minimum OS-Version festgelegt

Veraltete Betriebssysteme erhalten keine Sicherheitsupdates und sind anfällig für bekannte Exploits. Eine Mindestversion stellt sicher, dass nur Geräte mit aktuellem Patchlevel auf Unternehmensressourcen zugreifen.

 Quick Win | **Konfigurationsort:** `Intune Admin Center → Devices → Compliance policies → Windows → System security`

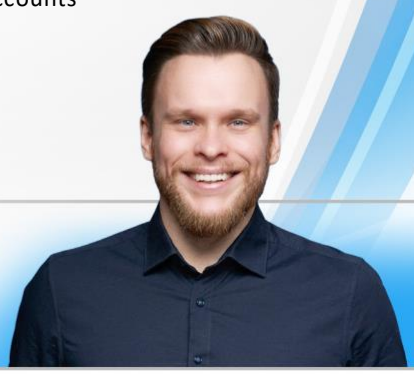
8.5 Windows Autopilot Deployment Profile konfiguriert

Autopilot standardisiert nicht nur das Onboarding, sondern reduziert Konfigurationsabweichungen. Geräte laufen vom ersten Start an in definierte Richtlinien, Apps und Sicherheitsprofile. Ohne Autopilot werden Geräte manuell eingerichtet — fehleranfällig und nicht standardisiert.

·· **Betriebsrelevant** | **Konfigurationsort:** `Intune Admin Center → Devices → Windows enrollment → Deployment profiles`

8.6 User Account Type auf Standard (keine lokalen Admins)

Lokale Admin-Rechte erlauben Usern, Software zu installieren, Sicherheitseinstellungen zu ändern und Malware mit erhöhten Rechten auszuführen. Standard-User-Accounts eliminieren diesen Angriffsvektor vollständig.



 High Impact ·· Betriebsrelevant | **Konfigurationsort:** `Intune Admin Center → Devices → Configuration profiles → Local admin`

8.7	BYOD App Protection Policies konfiguriert

App Protection Policies schützen Unternehmensdaten auf privaten Geräten ohne das Gerät vollständig zu managen. Daten in Outlook, Teams und OneDrive werden verschlüsselt, Copy-Paste wird eingeschränkt und Unternehmensdaten können remote gelöscht werden.

 High Impact ·· Betriebsrelevant | **Konfigurationsort:** `Intune Admin Center → Apps → App protection policies`

8.8	Defender for Endpoint angebunden (falls lizenziert)

Signale vom Endpunkt werden nicht isoliert betrachtet, sondern mit Identitäts-, Mail- und Cloud-Signalen im Defender XDR Dashboard korreliert. Defender for Endpoint liefert Endpoint Detection and Response (EDR): Erkennung von Angriffen auf Geräteebene und automatische Isolation kompromittierter Geräte.

 High Impact · Lizenzabhängig | **Konfigurationsort:** `security.microsoft.com → Settings → Endpoints → Onboarding`

Videos: Autopilot | Compliance Policies | Device Management | BYOD

9. Data Protection

#	Maßnahme	Status	Anmerkung
9.1	Sensitivity Labels erstellt (4 Stufen)		

Labels sind nicht nur sichtbare Klassifizierungen, sondern können Schutzmaßnahmen wie Verschlüsselung, Wasserzeichen oder Zugriffsbeschränkungen auslösen — eine Steuerungsschicht für Datenverwendung. Ohne Klassifizierung gibt es keine Grundlage für automatischen Schutz — alles wird gleich behandelt.

 High Impact ·· Betriebsrelevant | **Konfigurationsort:** `compliance.microsoft.com → Information protection → Labels`

9.2 Label Policy veröffentlicht

Die Label Policy macht die erstellten Labels für User verfügbar und definiert, welche Gruppen welche Labels sehen und verwenden können. Ohne veröffentlichte Policy existieren die Labels nur in der Konfiguration, nicht in der Praxis.

Abhängigkeit: Labels entfalten ihren vollen Schutzwert erst zusammen mit DLP-Policies (9.5).

 High Impact | **Konfigurationsort:** `compliance.microsoft.com → Information protection → Label policies`

9.3 Default-Label auf "Intern" gesetzt

Ein Default-Label stellt sicher, dass jedes neue Dokument automatisch eine Klassifizierung erhält. Ohne Default bleiben Dokumente unklassifiziert — DLP-Policies und Schutzmaßnahmen greifen nicht bei unlabeled Content.

 Quick Win | **Konfigurationsort:** `compliance.microsoft.com → Information protection → Label policies → [Policy] → Default label`

9.4 DLP-Policy für Germany PII aktiviert

DLP erkennt nicht nur Inhalte, sondern bewertet Kontexte wie Zielort, Benutzeraktion oder Kanal. Dadurch kann zwischen interner Nutzung und risikoreicher externer Freigabe unterschieden werden. Ohne DLP verlassen DSGVO-relevante Daten unkontrolliert die Organisation.

 High Impact | **Konfigurationsort:** `compliance.microsoft.com → Data loss prevention → Policies`

9.5 DLP-Policy für Sensitivity Labels konfiguriert

DLP-Policies auf Basis von Sensitivity Labels verhindern, dass als "Vertraulich" oder "Streng Vertraulich" gekennzeichnete Inhalte per E-Mail, Teams oder SharePoint nach extern geteilt werden. Label + DLP = durchgängiger Schutz.

 High Impact | **Konfigurationsort:** `compliance.microsoft.com → Data loss prevention → Policies → Condition: Sensitivity label`

9.6 Retention Policy eingerichtet (7 Jahre)

Retention schützt nicht primär vor Angreifern, sondern vor Verlust von Nachvollziehbarkeit und rechtlich relevanten Daten. Der Wert liegt in kontrollierter Aufbewahrung und Löschlogik. Ohne Retention Policy können User geschäftsrelevante Daten löschen, die für Audits oder Rechtsstreitigkeiten benötigt werden.

·· **Betriebsrelevant** | **Konfigurationsort:** `compliance.microsoft.com → Data lifecycle management → Retention policies`

9.7 Datenklassifizierung implementiert

Ohne Datenklassifizierung fehlt die Grundlage für DLP-Policies und Sensitivity Labels. Mindestens 3 Klassifizierungsstufen: Öffentlich, Intern, Vertraulich. Purview Information Protection bietet vordefinierte Sensitive Information Types für DACH-relevante Daten (IBAN, Personalausweisnummern, Steuernummern).

 High Impact | **Konfigurationsort:** `Microsoft Purview → Information protection → Classifiers → Sensitive info types`

9.8 Auto-Labeling für sensible Inhalte konfiguriert

Manuelle Klassifizierung funktioniert in der Praxis nicht flächendeckend. Auto-Labeling erkennt sensible Inhalte automatisch und wendet Sensitivity Labels an. Ohne Auto-Labeling bleiben sensible Dokumente ungeschützt in SharePoint und OneDrive. Mindestens für regulierte Datentypen (Finanzdaten, Personaldaten) konfigurieren.

 Lizenzabhängig | **Konfigurationsort:** `Microsoft Purview → Information protection → Auto-labeling`

10. Monitoring & Response

#	Maßnahme	Status	Anmerkung
10.1	Unified Audit Log aktiviert		

Audit Logging ist die zentrale Forensikgrundlage. Ohne Logs ist weder Rekonstruktion noch belastbare Bewertung eines Vorfalls möglich. Sichtbarkeit kommt immer vor Reaktionsfähigkeit. Das Unified Audit Log erfasst alle sicherheitsrelevanten Aktivitäten im Tenant: Anmeldungen, Datenzugriffe, Admin-Aktionen, Mailbox-Zugriffe.

 High Impact · Quick Win | **Konfigurationsort:** `compliance.microsoft.com → Audit → Audit search (Aktivierung prüfen)`

10.2	Audit Log Aufbewahrungsdauer geprüft		

Standardmäßig werden Audit-Daten 180 Tage aufbewahrt. Für Compliance-Anforderungen und forensische Analysen nach Sicherheitsvorfällen reicht das oft nicht. Die Aufbewahrungsdauer muss an die regulatorischen Anforderungen angepasst werden.

 Quick Win | **Konfigurationsort:** `compliance.microsoft.com → Audit → Audit retention policies`

10.3	Advanced Audit aktiviert (E5)		

Der Mehrwert liegt in tieferen Detailereignissen wie MailItemsAccessed und SearchQueryInitiated. Besonders relevant bei Insider-Vorfällen und forensischer Analyse kompromittierter Konten. Standard-Audit erfasst diese Daten nicht.

 Lizenzabhängig | **Konfigurationsort:** `compliance.microsoft.com → Audit (E5-Lizenz erforderlich)`

10.4	Log-Export in SIEM/Log Analytics konfiguriert		

Erst durch zentrale Korrelation mit anderen Datenquellen entstehen belastbare Detektions- und Investigationsmöglichkeiten. Einzelne Portale liefern Sicht, ein SIEM liefert Zusammenhang. Der Export in Log Analytics, Microsoft Sentinel oder ein externes SIEM ermöglicht professionelle Incident Response.

Abhängigkeit: Audit Logs sind nur mit Export/SIEM langfristig nutzbar — Standard-Aufbewahrung endet nach 180 Tagen.

 High Impact · Lizenzabhängig | **Konfigurationsort:** `Entra Admin Center → Diagnostic settings → Log Analytics / Microsoft Sentinel`

10.5 Standard Alert Policies geprüft (alle kritischen aktiv)

Microsoft liefert vorkonfigurierte Alert Policies für kritische Ereignisse: ungewöhnliche Dateifreigaben, Malware-Erkennung, Admin-Rollenänderungen. Ohne Prüfung sind möglicherweise nicht alle relevanten Alerts aktiviert.

 Quick Win | **Konfigurationsort:** `security.microsoft.com → Policies → Alert policy`

10.6 Custom Alert: Admin-Rollenzuweisung erstellt

Standard-Alerts decken nicht jede organisationsspezifische Gefährdung ab. Custom Alerts schaffen Überwachung für kritische Ereignisse wie privilegierte Rechteänderungen, Massenfreigaben oder App-Zustimmungen. Ohne diesen Alert können Angreifer sich unbemerkt zum Global Admin hochstufen.

 High Impact | **Konfigurationsort:** `security.microsoft.com → Policies → Alert policy → New alert policy`

10.7 Monitoring und Alerting für kritische Ereignisse eingerichtet

Ohne definierte Alerts werden Sicherheitsvorfälle erst bei sichtbarem Schaden entdeckt. Mindestens Alerts für: Global Admin Rollenzuweisung, Conditional Access Policy-Änderungen, Mail-Weiterleitungsregeln, Mass File Downloads. Microsoft Defender und Sentinel bieten vordefinierte Alert-Templates.

 High Impact | **Konfigurationsort:** `security.microsoft.com → Incidents & alerts → Alert policies`

10.8 Security Operations Prozess definiert

Technische Alerts ohne definierten Prozess erzeugen Alert Fatigue. Für jeden Alert-Typ muss klar sein: wer wird informiert, welche Erstmaßnahmen sind zu ergreifen, wann wird eskaliert. Ohne definierten Prozess bleiben kritische Alerts tagelang unbearbeitet.

·· **Betriebsrelevant** | **Konfigurationsort:** `Organisationsinterne Dokumentation / Runbook`

10.9 Identity Secure Score geprüft und dokumentiert

Der Identity Secure Score zeigt den aktuellen Sicherheitsstatus des Tenants als Prozentwert mit konkreten Verbesserungsvorschlägen. Regelmäßige Dokumentation macht den Fortschritt sichtbar und identifiziert Rückschritte.

 Quick Win | **Konfigurationsort:** `security.microsoft.com → Secure Score`

10.10 Defender XDR Dashboard als Routine eingerichtet

Das Defender XDR Dashboard konsolidiert Sicherheits-Events aus E-Mail, Identity, Endpoints und Cloud Apps. Ohne regelmäßige Dashboard-Prüfung bleiben Incidents unbearbeitet und Angriffe eskalieren unbemerkt.

 Quick Win | **Konfigurationsort:** `security.microsoft.com → Incidents & alerts`

10.11 Service Health Notifications aktiviert

Service Health Notifications informieren über Ausfälle, Änderungen und Sicherheits-Advisories von Microsoft. Ohne Benachrichtigungen erfährt das IT-Team von Problemen erst, wenn User sich melden — *zu spät für proaktives Handeln.*

 Quick Win | **Konfigurationsort:** `Microsoft 365 Admin Center → Health → Service health → Preferences`

10.12 Incident-Response-Rhythmus definiert

Ein definierter Rhythmus (z.B. tägliche Alert-Prüfung, wöchentliches Dashboard-Review) stellt sicher, dass Sicherheits-Events nicht übersehen werden. Ohne festen Prozess ist Monitoring reaktiv statt proaktiv — Vorfälle werden erst bearbeitet, wenn sie eskalieren.

·· **Betriebsrelevant** | **Konfigurationsort:** `Organisatorische Maßnahme (kein Portal-Konfigurationsort)`

Videos: Alert Policies | Identity Secure Score | Defender XDR

11. Defender XDR & Automatisierung

#	Maßnahme	Status	Anmerkung
11.1	Automatic Attack Disruption aktiviert		

Unterbricht erkannte Angriffsketten automatisiert, bevor sich ein Vorfall lateral ausbreitet. Der Mehrwert liegt in der Reaktionsgeschwindigkeit und der Verknüpfung mehrerer Signale statt isolierter Einzelerkennung. Ohne diese Funktion muss ein Analyst den Angriff manuell stoppen, was bei schnellen Angriffen zu spät sein kann.

High Impact · Lizenzabhängig | **Konfigurationsort:** `security.microsoft.com → Settings → Microsoft Defender XDR → Automatic attack disruption`

11.2	Automated Investigation and Response (AIR) konfiguriert		

AIR reduziert manuelle Analystenarbeit: Alarme werden automatisch untersucht, zusammengeführt und mit Handlungsempfehlungen versehen. Entscheidend bei hohem Alert-Volumen. Ohne AIR muss jeder Alert manuell untersucht werden.

High Impact · Lizenzabhängig | **Konfigurationsort:** `security.microsoft.com → Settings → Email & collaboration → Automated investigation`

11.3	Attack Simulation Training eingerichtet		

Der Nutzen ist nicht nur Awareness, sondern messbare Resilienz — ein wiederholbarer Prüfmechanismus für Benutzerverhalten gegen Phishing. Die Ergebnisse zeigen, wo Awareness-Training notwendig ist. Ohne regelmäßige Simulationen ist die tatsächliche Phishing-Resilienz der Organisation unbekannt.

Lizenzabhängig ·· Betriebsrelevant | **Konfigurationsort:** `security.microsoft.com → Email & collaboration → Attack simulation training`

Zwischenauswertung: Monitoring ohne Automatisierung skaliert nicht. Wenn weder Attack Disruption noch AIR aktiv sind, bleibt die Reaktion auf Angriffe manuell und damit zu langsam. → **Tenant Security Check empfohlen**

12. Backup & Ransomware-Schutz

#	Maßnahme	Status	Anmerkung
12.1	SharePoint/OneDrive Versionierung geprüft		

Versionierung hilft gegen logische Datenveränderung, ersetzt aber kein unabhängiges Backup. Der Unterschied muss klar sein. Ohne ausreichende Versionshistorie (mindestens 100 Versionen) ist eine Wiederherstellung nach einem Angriff nicht möglich.

 Quick Win | **Konfigurationsort:** `SharePoint Admin Center → Settings → Default storage limit / Versioning`

12.2	Microsoft 365 Backup konfiguriert		

Der Mehrwert liegt in der Unabhängigkeit von Produktivdaten, Aufbewahrungslogik und Tenant-Zustand. Relevant bei Fehlbedienung, Ransomware oder administrativer Kompromittierung. Ohne Backup sind Daten bei einem Ransomware-Angriff, versehentlicher Löschung oder einer Tenant-Kompromittierung unwiederbringlich verloren.

 High Impact | **Konfigurationsort:** `Microsoft 365 Admin Center → Settings → Microsoft 365 Backup (oder Drittanbieter-Lösung)`

12.3	Backup-Wiederherstellung getestet		

Wiederherstellbarkeit ist keine Eigenschaft des Backups, sondern des getesteten Prozesses. Regelmäßige Wiederherstellungstests stellen sicher, dass die Daten tatsächlich wiederherstellbar sind und der Prozess im Ernstfall funktioniert.

Abhängigkeit: Backup ohne Restore-Test ist organisatorisch unvollständig.

 High Impact | **Konfigurationsort:** `Organisatorische Maßnahme – regelmäßiger Test der Wiederherstellung`

12.4 Ransomware-Reaktionsplan dokumentiert

Ein dokumentierter Ransomware-Reaktionsplan definiert: Sofortmaßnahmen (Device Isolation, Account Disable), Kommunikationskette, Forensik-Schritte, Wiederherstellungsreihenfolge. Ohne Plan verliert das Team im Ernstfall kritische Minuten mit Abstimmung statt Eindämmung.

·· **Betriebsrelevant** | **Konfigurationsort:** `Organisationsinterne Dokumentation`

12.5 Backup-Restore regelmäßig getestet

Ein Backup ohne getestete Wiederherstellung ist kein Backup. Quartalsweise Restore-Tests für: Exchange-Postfächer, SharePoint-Sites, OneDrive-Daten, Teams-Kanäle. Typischer Fehlzustand: Backup läuft seit Monaten, aber niemand hat je geprüft ob die Wiederherstellung funktioniert.

·· **Betriebsrelevant** | **Konfigurationsort:** `Backup-Lösung → Restore-Test-Dokumentation`

Ergebnis

Bereich	Punkte	Umgesetzt	Offen
1. Organisationseinstellungen	3		
2. Identity & MFA	11		
3. Conditional Access	17		
4. Admin-Rollen & PIM	8		
5. E-Mail-Security	9		
6. Collaboration Security	11		
7. App Security & Governance	5		
8. Endpoint Security	8		
9. Data Protection	8		
10. Monitoring & Response	12		
11. Defender XDR & Automatisierung	3		
12. Backup & Ransomware-Schutz	5		
Gesamt	**100**		

Ergebnisinterpretation

Score	Bewertung	Typische Lage	Mögliche Folgen	Nächster Schritt
0–25	**Kritisch**	Grundlegende Schutzmaßnahmen fehlen	Kontoübernahmen, Ransomware, Datenverlust	Sofort Identity-Baseline umsetzen, professionelle Analyse empfohlen
26–45	**Hohes Risiko**	MFA teilweise, fehlende App-/Guest-Governance	Credential Stuffing, OAuth-Angriffe, Datenabfluss	CA-Baseline und App Consent priorisieren
46–65	**Mittleres Risiko**	Basis vorhanden, Monitoring und DLP fehlen	Späte Erkennung, unsichere Recovery	Monitoring und Data Protection ausbauen
66–80	**Gute Basis**	Kernbereiche umgesetzt, Automatisierung fehlt	Manuelle Reaktion zu langsam	Defender XDR und Automatisierung aktivieren
81–100	**Stark abgesichert**	Umfassend geschützt	Restrisiko durch Konfigurationsdrift	Regelmäßige Reviews und Anpassung

Typische Schwachstellen aus realen Tenant-Audits

Diese Werte stammen aus Hardening-Projekten bei mittelständischen Unternehmen im DACH-Raum:

Schwachstelle	Häufigkeit
MFA nicht für alle User erzwungen	ca. 40 % der Tenants
Kein PIM für privilegierte Rollen	ca. 60 % der Tenants
Safe Links / Safe Attachments nicht konfiguriert	ca. 70 % der Tenants
Keine Guest Governance (kein Audit, keine Einschränkungen)	ca. 80 % der Tenants
User Consent für Apps aktiv	ca. 75 % der Tenants
Kein Backup für M365-Daten	ca. 85 % der Tenants
Fehlende Conditional Access Baselines	ca. 65 % der Tenants
Unkontrollierter Gastzugriff ohne Access Reviews	ca. 80 % der Tenants
Keine Datenklassifizierung implementiert	ca. 90 % der Tenants
Fehlendes Monitoring / Alerting für kritische Events	ca. 75 % der Tenants
Legacy Authentication nicht vollständig blockiert	ca. 55 % der Tenants
Kein Emergency Access Account konfiguriert	ca. 50 % der Tenants
Admin-Rollen permanent statt über PIM zugewiesen	ca. 60 % der Tenants
Kein dokumentierter Ransomware-Reaktionsplan	ca. 90 % der Tenants

Professionelle Unterstützung

Microsoft 365 Security ist komplex — und wird mit jedem Update komplexer. Neue Features, geänderte Defaults, erweiterte Angriffsflächen: Selbst erfahrene IT-Teams stehen vor der Herausforderung, alle Konfigurationen aktuell und sicher zu halten. Externe Unterstützung durch spezialisierte Security-Berater

siller.consulting
INTELLIGENCE FOR IT

spart nicht nur Zeit, sondern deckt Risiken auf, die intern oft übersehen werden — weil sie außerhalb des Tagesgeschäfts liegen.

M365 Security Checkup

- Strukturierte Prüfung, wo Ihr Tenant steht:
- **https://www.siller.consulting/m365-security-checkup/**

Microsoft 365 Hardening & DSGVO

- Vollständige Analyse und Umsetzung:
- **https://www.siller.consulting/microsoft-365-hardening-und-dsgvo/**

M365 Tenant Hardening — Nächster Schritt

Diese Checkliste gibt den Überblick — aber die Umsetzung entscheidet. Jeder offene Punkt ist eine konkrete Schwachstelle, die Angreifer ausnutzen können. Das M365 Tenant Hardening von siller.consulting deckt alle 100 Maßnahmen dieser Checkliste ab — von der Ist-Analyse über die Konfiguration bis zur Dokumentation.

Jetzt Tenant Hardening anfragen »

https://www.siller.consulting/microsoft-365-hardening-und-dsgvo/

Aaron Siller

Microsoft MVP | siller.consulting

Autor: *Microsoft 365 absichern*

Golem Lead Trainer & Trainer Heise Academy

siller.consulting
INTELLIGENCE FOR IT