

Demo GmbH — Microsoft 365



Geprüft am **19. Oktober 2026, 5 Uhr**

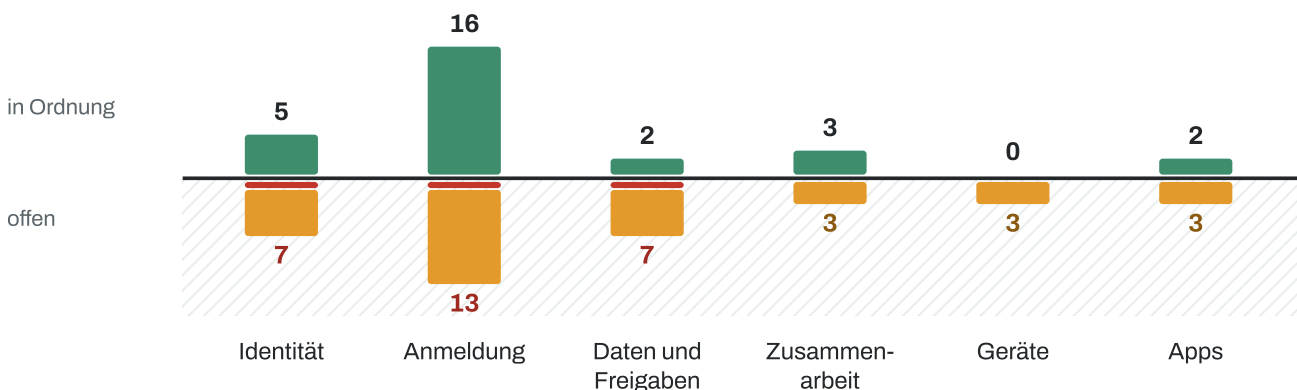
Bezug **SCuBA-Baselines der CISA (Version 2.0.0), BSI IT-Grundschutz, DSGVO
Art. 32**

Lizenzstand **Business Premium, 147 Benutzer**

Prüfumfang **73 von 144 Prüfpunkten automatisch ausgewertet. 71 Prüfpunkte nicht
automatisch ausgewertet, mit Grund im Abschnitt „Was wir nicht geprüft
haben“.**

Ergebnis auf einen Blick

Von den ausgewerteten Prüfungen sind 28 bestanden. 3 Befunde sind kritisch; wir empfehlen, sie innerhalb von zwei Wochen zu beheben. 33 weitere Punkte sollten eingeplant werden.



Grün, oben: bestanden (28) Rot, unten: kritisch (3) Orange, unten: Handlungsbedarf (33)

Nicht im Diagramm: Lizenz fehlt (7), nicht messbar (2)

Reihenfolge der Maßnahmen

- 1 ▲ MFA-Registrierung für alle Benutzer durchsetzen** bis zu +2 Punkte
 Für die restlichen 29 Konten genügt das Kennwort allein. BSI ORP.4.A21.
- 2 ▲ Anonyme Freigabelinks abschalten**
 Freigaben sind für beliebige Empfänger über anonyme Links möglich; 63 solcher Links sind aktiv, 41 davon ohne Ablaufdatum. BSI CON.9.A1.
- 3 ▲ Reine Cloud-Konten für globale Administratoren anlegen**
 2 der 5 Konten werden aus Ihrem lokalen Active Directory synchronisiert. SCuBA MS.AAD.7.3v1, BSI OPS.1.1.2.A22.

Ergebnis in Zahlen

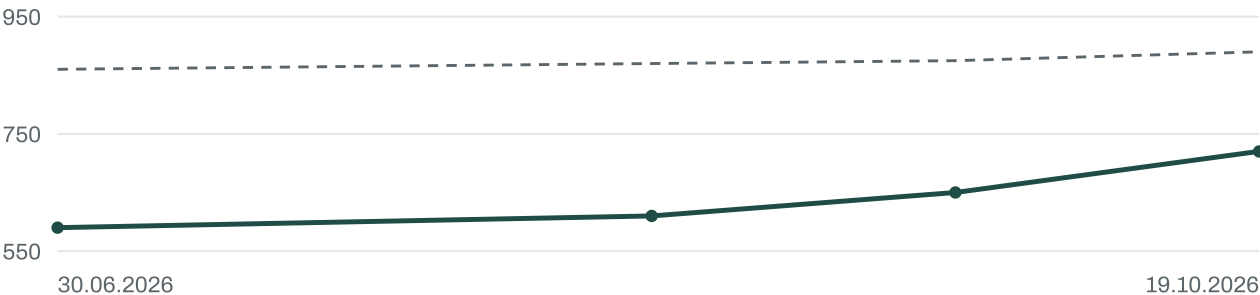
So verteilen sich die Bewertungen der geprüften Einstellungen.

Kritisch 3 sofort handeln	Handlungsbedarf 33 einplanen	Bestanden 28 belegt in Ordnung	Lizenz fehlt 7 kein Mangel	Nicht messbar 2 kein Urteil möglich
---	--	--	--	---

73 von 144 Prüfpunkten automatisch ausgewertet. Davon 7 ohne passende Lizenz und 2 nicht messbar.
71 Prüfpunkte nicht automatisch ausgewertet, jeweils mit Grund.

Microsoft Secure Score

720 von 890 möglichen Punkten am 19.10.2026



Durchgezogen: Ihr Secure Score. Gestrichelt: die in Ihrem Tenant erreichbaren Punkte.

Seit dem letzten Scan: 47 neu, 6 behoben, 3 verschlechtert.

Was wir nicht geprüft haben

71 Prüfpunkte nicht automatisch ausgewertet. Nicht jede Empfehlung lässt sich automatisch und nur lesend prüfen. Hier steht, was wir nicht automatisch ausgewertet haben, mit dem Grund je Gruppe.

Benötigt PowerShell-Zugriff (folgt in einer späteren Version) 53 Prüfpunkte

Diese Einstellungen von Exchange Online, Teams und SharePoint sind nur per PowerShell lesbar, nicht über Microsoft Graph. Wir nehmen sie in einer späteren Version auf.

Grund: Diese Schutzeinstellung für E-Mails ist nur über Exchange Online PowerShell auslesbar, nicht über die Microsoft-Schnittstelle, die Auditspiegel heute nutzt. Auditspiegel prüft sie in einer späteren Version automatisch. Bis dahin prüfen Sie sie bitte im Microsoft Defender Portal (security.microsoft.com) im Bereich „E-Mail & Zusammenarbeit“.

Prüf-ID	Prüfpunkt
AS-ZU-004	Sichere Links schützen auch Office-Anwendungen
AS-ZU-005	Der Filter für gefährliche Dateianhänge ist aktiv
AS-ZU-006	Admins werden benachrichtigt, wenn interne Benutzer Schadsoftware versenden
AS-ZU-007	Eine Richtlinie für sichere Anlagen ist aktiv
AS-ZU-008	Sichere Anlagen schützen auch SharePoint, OneDrive und Teams
AS-ZU-009	Spam-Richtlinien benachrichtigen Administratoren
AS-ZU-010	Eine Anti-Phishing-Richtlinie ist eingerichtet
AS-ZU-012	DKIM-Signierung ist für alle E-Mail-Domains aktiv
AS-ZU-017	Besonders gefährdete Konten (Geschäftsführung, Buchhaltung) sind als Prioritätskonten geschützt
AS-ZU-018	Für Prioritätskonten gilt die strenge Schutzvorlage
AS-ZU-020	Eine Liste blockierter Absender ist gepflegt

Grund: Diese Schutzeinstellung für E-Mails ist nur über Exchange Online PowerShell auslesbar, nicht über die Microsoft-Schnittstelle, die Auditspiegel heute nutzt. Auditspiegel prüft sie in einer späteren Version automatisch. Bis dahin prüfen Sie sie bitte im Microsoft Defender Portal (security.microsoft.com) im Bereich „E-Mail & Zusammenarbeit“.

Prüf-ID	Prüfpunkt
AS-ZU-023	Eine Anti-Malware-Richtlinie ist eingerichtet
AS-ZU-024	Die Anti-Phishing-Einstellungen sind vollständig konfiguriert
AS-ZU-025	Von Benutzern gemeldete Nachrichten landen in einem überwachten Postfach
AS-ZU-026	Die automatische Weiterleitung an externe Empfänger ist gesperrt
AS-ZU-027	Der Eingangs-Spamfilter ist konfiguriert
AS-ZU-028	Der Ausgangs-Spamfilter begrenzt den Massenversand
AS-ZU-032	Jede Form der E-Mail-Weiterleitung nach außen ist gesperrt

Grund: Diese Exchange-Einstellung ist nur über Exchange Online PowerShell auslesbar, nicht über die Microsoft-Schnittstelle, die Auditspiegel heute nutzt. Auditspiegel prüft sie in einer späteren Version automatisch. Bis dahin prüfen Sie sie bitte im Exchange Admin Center (admin.exchange.microsoft.com). Manche dieser Werte zeigt nur PowerShell; den Befehl nennt die Empfehlung zu diesem Punkt, Ihr IT-Dienstleister kann ihn für Sie ausführen.

AS-AP-008	Benutzer können keine Outlook-Add-ins selbst installieren
AS-DA-009	Externe Speicheranbieter sind in Outlook im Web gesperrt
AS-DA-010	Die Überwachungsrichtlinie der Organisation ist nicht deaktiviert
AS-ZU-019	E-Mail-Infos (MailTips) warnen Benutzer vor externen Empfängern
AS-ZU-021	Keine Transportregel nimmt ganze Absenderdomains von der Spamprüfung aus
AS-ZU-022	E-Mails von externen Absendern werden als „Extern“ gekennzeichnet
AS-ZU-029	Die Postfachüberwachung ist organisationsweit nicht abgeschaltet
AS-ZU-030	Die Postfachüberwachung ist für alle Benutzer aktiv
AS-ZU-031	Kein Benutzer ist von der Postfachüberwachung ausgenommen
AS-ZU-033	Outlook kennzeichnet externe Absender sichtbar
AS-ZU-034	Weiterleitungsregeln an externe Domains werden geprüft

Grund: Diese Teams-Einstellung ist nur über Teams PowerShell auslesbar, nicht über die Microsoft-Schnittstelle, die Auditspiegel heute nutzt. Auditspiegel prüft sie in einer späteren Version automatisch. Bis dahin prüfen Sie sie bitte im Teams Admin Center (admin.teams.microsoft.com).

AS-AP-011	Apps aus dem Teams-Store sind nur nach Freigabe nutzbar
AS-AP-012	Richtlinien für Teams-App-Berechtigungen sind eingeschränkt
AS-DA-020	Teams erlaubt nur freigegebene Cloud-Speicherdienste
AS-ZU-035	Der externe Zugriff in Teams ist auf freigegebene Organisationen beschränkt
AS-ZU-036	Kommunikation mit nicht verwalteten Teams-Konten ist gesperrt
AS-ZU-037	Kommunikation mit Skype-Konten ist gesperrt
AS-ZU-042	Mitarbeiter nehmen nicht am Chat von Besprechungen nicht vertrauenswürdiger Organisationen teil
AS-ZU-043	Anonyme Teilnehmer können den Besprechungschat nicht nutzen
AS-ZU-044	Die Cloudaufzeichnung von Teams-Besprechungen ist bewusst konfiguriert
AS-ZU-045	Benutzer können Sicherheitsbedenken direkt aus Teams melden

Grund: Diese SharePoint-Einstellung ist nur über SharePoint Online PowerShell auslesbar, nicht über die Microsoft-Schnittstelle, die Auditspiegel heute nutzt. Auditspiegel prüft sie in einer späteren Version automatisch. Bis dahin prüfen Sie sie bitte im SharePoint Admin Center (Adresse: <Ihr Mandantennamen>-admin.sharepoint.com).

AS-AP-009	Benutzerdefinierte Skripte auf persönlichen Websites sind gesperrt
AS-AP-010	Benutzerdefinierte Skripte auf selbst erstellten Websites sind gesperrt
AS-DA-013	Anonyme Freigabelinks laufen nach spätestens 30 Tagen ab
AS-DA-014	Freigabelinks erlauben standardmäßig nur das Ansehen

Grund: Diese SharePoint-Einstellung ist nur über SharePoint Online PowerShell auslesbar, nicht über die Microsoft-Schnittstelle, die Auditspiegel heute nutzt. Auditspiegel prüft sie in einer späteren Version automatisch. Bis dahin prüfen Sie sie bitte im SharePoint Admin Center (Adresse: <Ihr Mandantenname>-admin.sharepoint.com).

AS-DA-015	Freigabelinks gelten standardmäßig nur für bestimmte Personen
AS-DA-017	Gäste müssen sich regelmäßig per Bestätigungscode neu authentifizieren
AS-DA-018	Externe Freigaben in OneDrive sind eingeschränkt
AS-GE-004	Downloads aus SharePoint auf nicht verwaltete Geräte sind gesperrt

Grund: Diese Einstellung ist nur über Exchange Online PowerShell auslesbar, nicht über die Microsoft-Schnittstelle, die Auditspiegel heute nutzt. Auditspiegel prüft sie in einer späteren Version automatisch. Bis dahin prüfen Sie sie bitte im Microsoft 365 Admin Center (admin.microsoft.com) unter Einstellungen > Organisationseinstellungen > Dienste.

AS-AN-008	Exchange Online verlangt moderne Authentifizierung
AS-ZU-002	Kalender können nicht öffentlich mit externen Personen geteilt werden

Grund: Ob dieser DNS-Eintrag für alle Ihre E-Mail-Domains gesetzt ist, prüft Auditspiegel derzeit nicht automatisch; das folgt in einer späteren Version. Bis dahin prüfen Sie den Eintrag bitte in der DNS-Verwaltung Ihres Domain-Anbieters. Die Sollwerte zeigt das Microsoft 365 Admin Center (admin.microsoft.com) unter Einstellungen > Domänen.

AS-ZU-011	Für alle E-Mail-Domains ist ein SPF-Eintrag veröffentlicht
AS-ZU-013	Für alle E-Mail-Domains ist ein DMARC-Eintrag veröffentlicht

Grund: Welche Konten freigegebene Postfächer sind, lässt sich nur über Exchange Online PowerShell ermitteln, nicht über die Microsoft-Schnittstelle, die Auditspiegel heute nutzt. Auditspiegel prüft diesen Punkt in einer späteren Version automatisch. Bis dahin sehen Sie die Konten im Microsoft 365 Admin Center (admin.microsoft.com) unter Teams & Gruppen > Freigegebene Postfächer und blockieren unter Benutzer > Aktive Benutzer für jedes die Anmeldung.

AS-AN-005	Die direkte Anmeldung an freigegebenen Postfächern ist gesperrt
-----------	---

Grund: Der Pro-Benutzer-MFA-Status ist nur über eine Beta-Schnittstelle von Microsoft Graph und nur Konto für Konto abrufbar. Wir nehmen die Prüfung auf, sobald Microsoft die Schnittstelle allgemein freigibt. Bis dahin sehen Sie den Status im Microsoft Entra Admin Center (entra.microsoft.com) unter Benutzer > Alle Benutzer > „Pro-Benutzer-MFA“.

AS-AN-010	Die veraltete Pro-Benutzer-MFA ist abgeschaltet (MFA läuft zentral über Richtlinien)
-----------	--

Nur im Microsoft-Portal prüfbar

15 Prüfpunkte

Diese Punkte sehen Sie nur im Microsoft 365 Admin Center, oder es sind organisatorische Maßnahmen. Bitte prüfen Sie sie anhand der Empfehlung selbst.

Grund: Für diese Einstellung bietet Microsoft keine auslesbare Schnittstelle (nur im Admin-Center sichtbar). Bitte prüfen Sie sie manuell anhand der Empfehlung.

Prüf-ID	Prüfpunkt
AS-AN-007	Inaktive Sitzungen in Microsoft-365-Webanwendungen werden nach höchstens drei Stunden beendet
AS-AN-011	Die Option „Angemeldet bleiben?“ wird bei der Anmeldung nicht angeboten
AS-AP-002	Microsoft Defender for Cloud Apps ist eingerichtet
AS-DA-002	Speicherdienste von Drittanbietern sind in Microsoft 365 im Web gesperrt
AS-ID-007	Mitarbeiter können Gruppenfunktionen im Portal „Meine Gruppen“ nicht verwalten
AS-ID-013	Der Zugriff auf das Microsoft Entra Admin Center ist auf Administratoren beschränkt
AS-ID-022	Der Synchronisationsdienst Entra Connect wird per Connect Health überwacht

Grund: Organisatorische Maßnahme: Hier geht es um die regelmäßige Sichtung eines Berichts durch Ihr Team. Das lässt sich technisch nicht prüfen; bitte legen Sie dafür einen festen Termin fest.

AS-AP-005	Der Bericht zur App-Nutzung wird wöchentlich gesichtet
AS-ID-010	Der Bericht zur Kontobereitstellung wird wöchentlich gesichtet
AS-ID-011	Zuweisungen zu Exchange-Rollengruppen werden wöchentlich gesichtet
AS-ZU-014	Der Bericht zu gefälschten Absenderdomains wird wöchentlich gesichtet
AS-ZU-015	Der Bericht „Eingeschränkte Entitäten“ wird wöchentlich gesichtet
AS-ZU-016	Der Bedrohungsschutz-Statusbericht wird regelmäßig gesichtet

Grund: Die Domain-Zulassungsliste für Gasteinladungen ist über die allgemein freigegebene Microsoft-Graph-Schnittstelle nicht lesbar. Bitte prüfen Sie sie manuell anhand der Empfehlung.

AS-ID-015	Gasteinladungen sind nur an freigegebene Partnerdomains möglich
-----------	---

Grund: Ob Administratoren dedizierte, gehärtete Arbeitsplätze nutzen, ist eine organisatorische Maßnahme und technisch nicht aus Microsoft 365 auslesbar.

AS-GE-003	Administratoren arbeiten auf besonders gesicherten Admin-Arbeitsplätzen
-----------	---

Nicht automatisch auslesbar

1 Prüfpunkt

Für diese Einstellungen bietet Microsoft keine Schnittstelle, die sich nur lesend abfragen lässt.

Grund: Aufbewahrungsrichtlinien lassen sich nur über die Purview-Verwaltung von Microsoft auslesen, auf die Auditspiegel keinen automatischen Zugriff hat. Bitte prüfen Sie diesen Punkt selbst im Microsoft Purview Portal (purview.microsoft.com) unter Lösungen > Datenlebenszyklusverwaltung > Richtlinien > Aufbewahrungsrichtlinien.

Prüf-ID	Prüfpunkt
---------	-----------

AS-DA-019	SharePoint-Inhalte unterliegen einer mandantenweiten Aufbewahrungsrichtlinie
-----------	--

Zusätzliche Berechtigung nötig

2 Prüfpunkte

Dafür bräuchte Auditspiegel weitere Leseberechtigungen in Microsoft Graph. Wir fordern bewusst nur die nötigsten an.

Grund: Für diese Prüfung bräuchte Auditspiegel die zusätzliche Leseberechtigung „AccessReview.Read.All“. Wir fragen sie bewusst nicht an, solange sie nicht für mehrere Prüfungen nötig ist.

Prüf-ID	Prüfpunkt
---------	-----------

AS-ID-019	Gastkonten werden regelmäßig per Zugriffsüberprüfung bestätigt
-----------	--

AS-ID-020	Administratorrollen werden regelmäßig per Zugriffsüberprüfung bestätigt
-----------	---

Ausgewertet, aber ohne Urteil

Von den 73 ausgewerteten Prüfungen sind 7 ohne passende Lizenz und 2 nicht messbar. Diese Prüfungen hat der Scan angefasst, konnte sie aber nicht bewerten. Sie zählen weder als bestanden noch als Mangel.

Lizenz fehlt

7 Prüfpunkte

Diese Prüfungen setzen eine Microsoft-365-Lizenz voraus, die Ihr Tenant nicht hat. Das ist kein Mangel.

Grund: Erfordert Microsoft Entra ID P2 (enthalten z. B. in Microsoft 365 E5).

Prüf-ID	Prüfpunkt
---------	-----------

AS-AN-018	Risikante Anmeldungen werden per Richtlinie zur Multifaktor-Anmeldung gezwungen oder blockiert
-----------	--

AS-AN-019	Konten mit hohem Kompromittierungsrisiko müssen ihr Kennwort ändern oder werden gesperrt
-----------	--

AS-ID-018	Administratorrechte werden über Privileged Identity Management nur bei Bedarf vergeben
-----------	--

AS-ID-021	Die Aktivierung der Rolle „Globaler Administrator“ muss von einer zweiten Person genehmigt werden
-----------	---

AS-ID-023	Neue Zuweisungen hoch privilegierter Rollen werden per E-Mail an eine festgelegte Adresse gemeldet
-----------	--

AS-ID-024	Jede Aktivierung der Rolle „Globaler Administrator“ wird per E-Mail an eine festgelegte Adresse gemeldet
-----------	--

AS-ID-025	Aktivierungen weiterer hoch privilegierter Rollen werden per E-Mail an eine festgelegte Adresse gemeldet
-----------	--

Nicht messbar

2 Prüfpunkte

Die Daten ließen sich bei diesem Scan nicht vollständig lesen. Der nächste Scan versucht es erneut.

Grund: Microsoft hat den Datenabruf wegen zu hoher Lastrate gedrosselt. Bitte starten Sie den Audit in 30 Minuten erneut.

Prüf-ID	Prüfpunkt
---------	-----------

AS-DA-005	Die Aufbewahrungsdauer der Anmelde- und Audit-Protokolle reicht für eine Vorfallaufklärung aus
-----------	--

Grund: Für diesen Check lagen keine Daten vor (zum Beispiel keine Bedingte-Zugriff-Richtlinie definiert).

AS-DA-001	Customer Lockbox ist aktiv — Microsoft-Support greift nur nach Ihrer Freigabe auf Daten zu
-----------	--

Offene Befunde im Einzelnen

Alle Befunde mit Bewertung kritisch oder Handlungsbedarf, das Dringendste zuerst. Bestandene Prüfungen stehen in der Liste aller Prüfungen nach SCuBA-Baselines.

Schweregrad sehr hoch, 3 Befunde

▲ **Kritisch**, Schweregrad sehr hoch

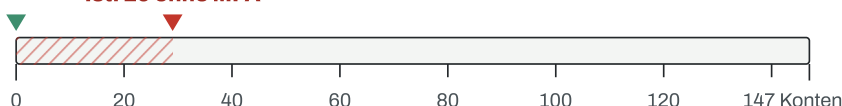
Pos. 58, AS-AN-013

Weniger als 95 % der Benutzer haben eine MFA-Methode registriert

Anforderung: Mindestens 95 % aller Benutzer haben eine Multifaktor-Methode registriert

Soll: 0

Ist: 29 ohne MFA



Gemessen am 19. Oktober 2026, 5 Uhr über Microsoft Graph, nur lesend.

Warum das wichtig ist

Multifaktor-Anmeldung schützt nur Konten, für die eine zweite Methode tatsächlich eingerichtet ist, etwa die Authenticator-App. Liegt die Registrierungsquote unter 95 %, gibt es noch Konten, die im Ernstfall nur durch ein Passwort geschützt sind oder bei der ersten Abfrage von einem Angreifer registriert werden könnten.

Wo Sie die Einstellung finden: Microsoft Entra Admin Center (entra.microsoft.com) > Entra ID > Authentifizierungsmethoden > Benutzerregistrierungsdetails

Hinweis für die IT: Microsoft Graph PowerShell: 'Get-MgReportAuthenticationMethodUserRegistrationDetail -All -Filter 'isMfaRegistered eq false' | ft UserPrincipalName,UserType'

BSI IT-Grundschutz	ORP.4.A21 Mehr-Faktor-Authentisierung
DSGVO	Art. 32 Abs. 1 lit. b
Secure Score	MFA für alle Benutzer, bis zu 2 Punkte
Benötigte Lizenz	Microsoft Entra ID P1 (enthalten z. B. in Microsoft 365 Business Premium, E3 und E5) oder Microsoft Entra ID P2 (enthalten z. B. in Microsoft 365 E5)

So beheben Sie es

MFA-Registrierung für alle Benutzer durchsetzen

Sorgen Sie dafür, dass mindestens 95 % aller Benutzer eine MFA-Methode registriert haben (Bericht erfordert Microsoft Entra ID P1).

1. Öffnen Sie Entra ID > Authentifizierungsmethoden > Benutzerregistrierungsdetails und filtern Sie auf „Nicht für MFA registriert“.
2. Klären Sie für jedes Konto: aktive Person, Funktions- oder Altkonto? Deaktivieren Sie nicht mehr benötigte Konten oder blockieren Sie deren Anmeldung.
3. Bitten Sie die übrigen Personen per Mail mit Anleitung, die Authenticator App unter mysignins.microsoft.com/security-info einzurichten.
4. Aktivieren Sie unter Authentifizierungsmethoden die „Registrierungskampagne“, damit Microsoft fehlende Registrierungen bei der Anmeldung einfordert.
5. Geben Sie neuen Mitarbeitenden einen befristeten Zugriffspass (Temporary Access Pass) für die sichere Ersteinrichtung.
6. Prüfen Sie den Bericht nach zwei Wochen erneut.

▲ **Kritisch**, Schweregrad sehr hoch

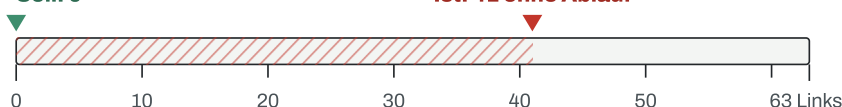
Pos. 70, AS-DA-011

Anonyme „Jeder mit dem Link“-Freigaben sind erlaubt

Anforderung: SharePoint erlaubt keine anonymen „Jeder mit dem Link“-Freigaben

Soll: 0

Ist: 41 ohne Ablauf



Gemessen am 19. Oktober 2026, 5 Uhr über Microsoft Graph, nur lesend.

Warum das wichtig ist

SharePoint und OneDrive können Links erzeugen, die ohne Anmeldung funktionieren („Jeder mit dem Link“). Solche Links werden weitergeleitet, landen in Suchmaschinen oder fremden Postfächern. Niemand kann nachvollziehen, wer die Datei geöffnet hat. Externe sollten sich daher immer als Gast anmelden müssen.

So beheben Sie es

Anonyme Freigabelinks abschalten

Beschränken Sie die externe Freigabe in SharePoint auf „Neue und vorhandene Gäste“ oder strenger, sodass anonyme Links nicht mehr möglich sind.

1. Prüfen Sie vorab, ob Abteilungen anonyme Links aktiv nutzen (z. B. für Kunden-Downloads), und klären Sie Alternativen wie Gastzugang.

Wo Sie die Einstellung finden: SharePoint Admin Center (<tenant>-admin.sharepoint.com) > Richtlinien > Freigabe > Externe Freigabe (SharePoint)

Hinweis für die IT: SharePoint Online PowerShell: Get-SPOTenant | fl SharingCapability – erwartet ExternalUserSharingOnly, ExistingExternalUserSharingOnly oder Disabled. Setzen: Set-SPOTenant -SharingCapability ExternalUserSharingOnly

BSI IT-Grundschutz	CON.9.A1 Festlegung zulässiger Empfangender
DSGVO	Art. 32 Abs. 1 lit. b
Benötigte Lizenz	Keine Zusatzlizenz erforderlich

2. Öffnen Sie im SharePoint Admin Center Richtlinien > Freigabe.
3. Stellen Sie den Regler für SharePoint auf „Neue und vorhandene Gäste“, „Vorhandene Gäste“ oder „Nur Personen in Ihrer Organisation“. OneDrive kann nicht großzügiger sein als SharePoint.
4. Speichern Sie. Hinweis: Bereits verschickte „Jeder“-Links funktionieren danach nicht mehr – informieren Sie betroffene Teams vorab.
5. Prüfen Sie einzelne Websites mit abweichenden Freigabeeinstellungen unter Websites > Aktive Websites.
6. Testen Sie: Beim Freigeben einer Datei darf die Option „Jeder mit dem Link“ nicht mehr angeboten werden.

▲ **Kritisch**, Schweregrad sehr hoch

Pos. 23, AS-ID-001

Globale Administratoren werden aus dem lokalen AD synchronisiert

Anforderung: Globale Administratoren sind reine Cloud-Konten (nicht aus dem lokalen AD synchronisiert)



Gemessen am 19. Oktober 2026, 5 Uhr über Microsoft Graph, nur lesend.

Warum das wichtig ist

Globale Administratoren haben vollen Zugriff auf alle Daten und Einstellungen in Microsoft 365. Werden diese Konten aus dem lokalen Active Directory synchronisiert, kann ein Angreifer, der Ihr Firmennetz oder Ihren Server übernimmt, damit auch Ihre gesamte Cloud übernehmen. Reine Cloud-Konten trennen diese beiden Welten.

Wo Sie die Einstellung finden: Microsoft Entra Admin Center (entra.microsoft.com) > Entra ID > Rollen und Administratoren > Globaler Administrator > Aktive Zuweisungen

Hinweis für die IT: Microsoft Graph PowerShell: Get-MgDirectoryRoleMember -DirectoryRoleId (Get-MgDirectoryRole -Filter "roleTemplateId eq '62e90394-69f5-4237-9190-012177145e10'").Id | % { Get-MgUser -UserId \$_.Id -Property UserPrincipalName,OnPremisesSyncEnabled }

SCuBA (CISA)	MS.AAD.7.3v1 Privilegierte Benutzer als reine Cloud-Konten
BSI IT-Grundschutz	OPS.1.1.2.A22 Trennung von administrativen und anderen Tätigkeiten; OPS.1.1.2.A6 Schutz administrativer Tätigkeiten
DSGVO	Art. 32 Abs. 1 lit. b
Secure Score	aad_admin_accounts_separate_unassigned_cloud_only
Benötigte Lizenz	Keine Zusatzlizenz erforderlich

So beheben Sie es

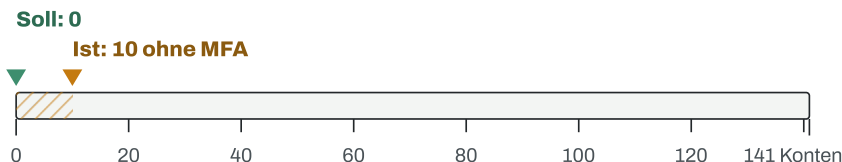
Reine Cloud-Konten für globale Administratoren anlegen

Die Rolle „Globaler Administrator“ wird nur an reine Cloud-Konten vergeben, die nicht aus dem lokalen AD synchronisiert werden.

1. Öffnen Sie im Microsoft Entra Admin Center die Rolle „Globaler Administrator“ und prüfen Sie bei jedem Mitglied die Spalte bzw. Eigenschaft „Lokal synchronisiert“ (On-premises sync enabled).
2. Legen Sie für jede betroffene Person ein neues reines Cloud-Konto an, z. B. admin.nachname@<firma>.onmicrosoft.com, und schützen Sie es mit MFA.
3. Weisen Sie dem neuen Cloud-Konto die Rolle „Globaler Administrator“ zu und testen Sie die Anmeldung im Admin Center.
4. Entfernen Sie danach die Rolle vom synchronisierten Konto. Nutzen Sie das synchronisierte Konto nur noch für die tägliche Arbeit.
5. Prüfen Sie, ob Skripte oder Dienste das alte Konto verwenden, und stellen Sie diese vorher um.
6. Kontrollieren Sie abschließend, dass kein Mitglied der Rolle mehr „onPremisesSyncEnabled = true“ aufweist.

Nicht alle Mitarbeiterkonten haben eine starke MFA-Methode

Anforderung: Alle Mitarbeiterkonten sind MFA-fähig (starke Methode registriert und zugelassen)



Gemessen am 19. Oktober 2026, 5 Uhr über Microsoft Graph, nur lesend.

Warum das wichtig ist

Ein Konto ist erst dann wirklich durch MFA geschützt, wenn eine starke Methode registriert und in Ihren Richtlinien auch zugelassen ist. Diese Prüfung zeigt, ob wirklich jedes Mitarbeiterkonto diese Voraussetzung erfüllt, damit MFA-Richtlinien niemanden aussperren und niemand durchrutscht.

Wo Sie die Einstellung finden: Microsoft Entra Admin Center (entra.microsoft.com) > Entra ID > Authentifizierungsmethoden > Benutzerregistrierungsdetails

Hinweis für die IT: Microsoft Graph PowerShell: ``Get-MgReportAuthenticationMethodUserRegistrationDetail -All -Filter "isMfaCapable eq false and userType eq 'member'" | ft UserPrincipalName,MethodsRegistered``

BSI IT-Grundschutz	ORP.4.A21 Mehr-Faktor-Authentisierung
DSGVO	Art. 32 Abs. 1 lit. b
Secure Score	MFA für alle Benutzer, bis zu 2 Punkte
Benötigte Lizenz	Microsoft Entra ID P1 (enthalten z. B. in Microsoft 365 Business Premium, E3 und E5) oder Microsoft Entra ID P2 (enthalten z. B. in Microsoft 365 E5)

So beheben Sie es

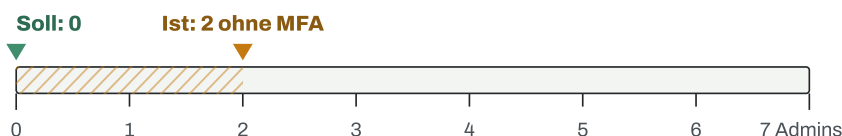
Starke MFA-Methode für alle Mitarbeiterkonten sicherstellen

Stellen Sie sicher, dass alle Mitarbeiterkonten eine starke, zugelassene MFA-Methode registriert haben (Bericht erfordert Entra ID P1).

1. Öffnen Sie Entra ID > Authentifizierungsmethoden > Benutzerregistrierungsdetails und filtern Sie auf Benutzertyp „Mitglied“ und „Nicht MFA-fähig“.
2. Prüfen Sie, ob die registrierte Methode in den Authentifizierungsmethoden-Richtlinien für diese Person überhaupt aktiviert ist.
3. Deaktivieren Sie verwaiste oder ungenutzte Konten; blockieren Sie die Anmeldung von Funktionspostfächern.
4. Unterstützen Sie die übrigen Personen bei der Einrichtung der Authenticator App oder eines Passkeys, ggf. mit befristetem Zugriffspass.
5. Aktivieren Sie die Registrierungskampagne und prüfen Sie den Bericht nach zwei Wochen erneut.

Nicht alle Administratoren haben eine MFA-Methode registriert

Anforderung: Alle Administratoren haben eine Multifaktor-Methode registriert



Gemessen am 19. Oktober 2026, 5 Uhr über Microsoft Graph, nur lesend.

Warum das wichtig ist

Ein Kennwort allein lässt sich erraten, abfangen oder per Phishing stehlen. Mit einer zweiten Anmeldemethode (z. B. Authenticator-App) reicht ein gestohlenes Kennwort nicht mehr aus. Für Administratoren ist das besonders wichtig, weil ihre Konten den Zugriff auf das ganze Unternehmen öffnen.

Wo Sie die Einstellung finden: Microsoft Entra Admin Center (entra.microsoft.com) > Entra ID > Authentifizierungsmethoden > Benutzerregistrierungsdetails

Hinweis für die IT: Microsoft Graph PowerShell: `Get-MgReportAuthenticationMethodUserRegistrationDetail -Filter "isAdmin eq true" | Select UserPrincipalName,IsMfaRegistered,MethodsRegistered`

So beheben Sie es

MFA für alle Administratorkonten registrieren und erzwingen

Alle Konten mit Administratorrolle registrieren eine Multifaktor-Methode und MFA wird für sie erzwungen.

1. Öffnen Sie „Benutzerregistrierungsdetails“ und filtern Sie auf Administratoren mit „MFA-fähig: Nein“ bzw. „Nicht registriert“ (der Bericht erfordert Microsoft Entra ID P1).
2. Bitten Sie jede betroffene Person, unter <https://aka.ms/mysecurityinfo> die Microsoft-Authenticator-App oder einen FIDO2-Schlüssel zu registrieren.
3. Ohne Entra ID P1: Aktivieren Sie die Sicherheitsstandards – damit ist MFA für Admins verpflichtend.

BSI IT-Grundschutz	ORP.4.A10 Schutz von Benutzendenkennungen mit weitreichenden Berechtigungen
DSGVO	Art. 32 Abs. 1 lit. b
Secure Score	MFA für alle Administratoren
Benötigte Lizenz	Microsoft Entra ID P1 (enthalten z. B. in Microsoft 365 Business Premium, E3 und E5) oder Microsoft Entra ID P2 (enthalten z. B. in Microsoft 365 E5)

4. Mit Entra ID P1: Erstellen Sie eine Richtlinie für bedingten Zugriff aus der Vorlage „MFA für Administratoren erforderlich“; schließen Sie ein Notfallkonto aus und testen Sie zuerst im Modus „Nur Bericht“.
5. Prüfen Sie nach einigen Tagen erneut den Bericht: Alle Admins müssen als MFA-registriert erscheinen.

 **Handlungsbedarf**, Schweregrad hoch

Pos. 10, AS-AN-016

Microsoft Authenticator zeigt weder App-Namen noch Standort an

Anforderung: Microsoft Authenticator zeigt App-Name und Standort an (Schutz vor MFA-Ermüdungsangriffen)

Authenticator-Anfragen zeigen nicht den Standort der Anmeldung an.

Warum das wichtig ist

Bei sogenannten MFA-Ermüdungsangriffen schicken Angreifer so lange Anmeldeanfragen aufs Handy, bis jemand genervt auf „Genehmigen“ tippt. Zeigt die Authenticator-App an, welche Anwendung sich anmeldet und von welchem Ort aus, fällt eine fremde Anfrage, etwa aus dem Ausland, sofort auf.

Wo Sie die Einstellung finden: Microsoft Entra Admin Center (entra.microsoft.com) > Entra ID > Authentifizierungsmethoden > Richtlinien > Microsoft Authenticator > Konfigurieren

Hinweis für die IT: Microsoft Graph PowerShell: `(Get-MgPolicyAuthenticationMethodPolicyAuthenticationMethodConfiguration -AuthenticationMethodConfigurationId MicrosoftAuthenticator).AdditionalProperties.featureSettings`

SCuBA (CISA)	MS.AAD.3.3v2 Microsoft Authenticator zeigt Anmeldekontext an
BSI IT-Grundschutz	ORP.4.A13 Geeignete Auswahl von Authentisierungsmechanismen
DSGVO	Art. 32 Abs. 1 lit. b
Benötigte Lizenz	Keine Zusatzlizenz erforderlich

So beheben Sie es

App-Name und Standort im Authenticator anzeigen lassen

Aktivieren Sie in der Microsoft-Authenticator-Richtlinie die Anzeige von Anwendungsname und geografischem Standort.

1. Öffnen Sie Entra ID > Authentifizierungsmethoden > Richtlinien > Microsoft Authenticator.
2. Stellen Sie sicher, dass die Methode aktiviert ist und für „Alle Benutzer“ gilt.
3. Setzen Sie auf der Registerkarte „Konfigurieren“ „Anwendungsname in Pushbenachrichtigungen anzeigen“ auf Status „Aktiviert“ für alle Benutzer – nicht „Von Microsoft verwaltet“.
4. Setzen Sie ebenso „Geografischen Standort in Pushbenachrichtigungen anzeigen“ auf „Aktiviert“ und speichern Sie.
5. Testen Sie mit einer Anmeldung, dass die App beides anzeigt, und bitten Sie Mitarbeitende, unerwartete Anfragen abzulehnen und zu melden.

 **Handlungsbedarf**, Schweregrad hoch

Pos. 17, AS-AN-022

Die Geräte-Code-Anmeldung (beliebtes Phishing-Werkzeug) ist erlaubt

Anforderung: Die Geräte-Code-Anmeldung (beliebtes Phishing-Werkzeug) ist blockiert

Keine Richtlinie für bedingten Zugriff blockiert die Geräte-Code-Anmeldung (4 Richtlinien im Tenant geprüft).

Warum das wichtig ist

Die Geräte-Code-Anmeldung ist für Geräte ohne Tastatur gedacht, etwa Konferenzraum-Systeme. Angreifer missbrauchen sie für Phishing: Sie schicken einen Code und bitten, ihn auf einer echten Microsoft-Seite einzugeben. Damit melden Mitarbeitende unwissentlich das Gerät des Angreifers an.

Wo Sie die Einstellung finden: Microsoft Entra Admin Center (entra.microsoft.com) > Entra ID > Bedingter Zugriff > Richtlinien

Hinweis für die IT: Microsoft Graph PowerShell: `Get-MgIdentityConditionalAccessPolicy | ? { \$\_.Conditions.AuthenticationFlows.TransferMethods -match 'deviceCodeFlow' } | ft DisplayName,State`

So beheben Sie es

Geräte-Code-Anmeldung per bedingtem Zugriff blockieren

Blockieren Sie die Geräte-Code-Anmeldung per bedingtem Zugriff für alle Benutzer (erfordert Entra ID P1).

1. Prüfen Sie im Anmeldeprotokoll (Filter „Authentifizierungsprotokoll: Gerätecodefluss“), ob Geräte wie Teams-Räume das Verfahren legitim nutzen.
2. Öffnen Sie im Entra Admin Center Entra ID > Bedingter Zugriff > Richtlinien und wählen Sie „Neue Richtlinie“ (oder „Neue Richtlinie aus Vorlage“).
3. Benutzer: „Alle Benutzer“. Schließen Sie unter „Ausschließen“ Ihre zwei Notfallkonten (Break-Glass) und das Synchronisierungskonto von Entra Connect aus. Nehmen Sie nur nachweislich nötige Gerätekonten zusätzlich aus.
4. Zielressourcen: „Alle Ressourcen“. Bedingungen > Authentifizierungsflüsse: „Gerätecodefluss“. Gewähren: „Zugriff blockieren“.

SCuBA (CISA)	MS.AAD.3.9v1 Gerätecode-Anmeldung blockieren
BSI IT-Grundschutz	ORP.4.A13 Geeignete Auswahl von Authentisierungsmechanismen
DSGVO	Art. 32 Abs. 1 lit. b
Benötigte Lizenz	Microsoft Entra ID P1 (enthalten z. B. in Microsoft 365 Business Premium, E3 und E5) oder Microsoft Entra ID P2 (enthalten z. B. in Microsoft 365 E5)

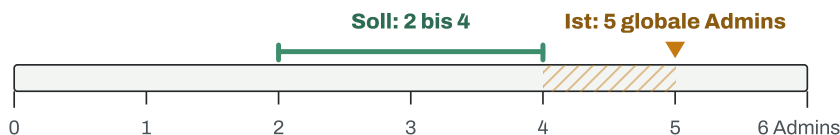
- Aktivieren Sie die Richtlinie zunächst im Modus „Nur Bericht“ und werten Sie das Anmeldeprotokoll einige Tage aus.
- Schalten Sie die Richtlinie danach auf „Ein“ und testen Sie mit einem betroffenen Konto in einem privaten Browserfenster.

⚠ **Handlungsbedarf**, Schweregrad hoch

Pos. 22, AS-ID-003

Die Zahl der globalen Administratoren liegt nicht zwischen zwei und vier

Anforderung: Zwischen zwei und vier Globale Administratoren sind benannt



Gemessen am 19. Oktober 2026, 5 Uhr über Microsoft Graph, nur lesend.

Warum das wichtig ist

Globale Administratoren dürfen in Microsoft 365 alles. Gibt es nur einen, fehlt bei Krankheit oder Urlaub die Vertretung. Gibt es zu viele, steigt die Zahl der Konten, über die ein Angreifer die volle Kontrolle erlangen kann. Zwei bis vier sind ein guter Kompromiss.

Wo Sie die Einstellung finden: Microsoft Entra Admin Center (entra.microsoft.com) > Entra ID > Rollen und Administratoren > Globaler Administrator

Hinweis für die IT: Microsoft Graph PowerShell: (Get-MgDirectoryRoleMember -DirectoryRoleId (Get-MgDirectoryRole -Filter "roleTemplateId eq '62e90394-69f5-4237-9190-012177145e10').Id).Count

SCuBA (CISA)	MS.AAD.7.1v1 Zwei bis acht Globale Administratoren
BSI IT-Grundschutz	OPS.1.1.2.A21 Regelung der IT-Administrationsrollen
DSGVO	Art. 32 Abs. 1 lit. b
Secure Score	OneAdmin
Benötigte Lizenz	Keine Zusatzlizenz erforderlich

So beheben Sie es

Globale Administratoren auf zwei bis vier Konten begrenzen

Die Anzahl der Globalen Administratoren wird auf zwei bis vier Konten begrenzt, alle übrigen Admins erhalten passende Teilrollen.

- Öffnen Sie die Rolle „Globaler Administrator“ und listen Sie alle aktiven Zuweisungen auf.
- Prüfen Sie für jedes Konto, welche Aufgaben die Person tatsächlich erledigt.
- Ersetzen Sie die Rolle, wo möglich, durch eingeschränkte Rollen wie „Benutzeradministrator“, „Exchange-Administrator“, „Teams-Administrator“ oder „Helpdeskadministrator“.
- Behalten Sie insgesamt zwei bis vier Global-Admins; die Notfallkonten zählen dabei mit.
- Wenn nur ein Global-Admin existiert, ernennen Sie eine zweite, vertrauenswürdige Person bzw. legen Sie ein Notfallkonto an.
- Prüfen Sie die Rollenzuweisungen künftig mindestens vierteljährlich.

Schweregrad mittel, 22 Befunde

⚠ **Handlungsbedarf**, Schweregrad mittel

Pos. 36, AS-DA-016

Externe Freigaben sind nicht auf Partnerdomains beschränkt

Anforderung: Externe Freigaben sind auf eine Liste erlaubter Partnerdomains beschränkt

Es ist keine Begrenzung hinterlegt.

Warum das wichtig ist

Die meisten KMU arbeiten mit einem überschaubaren Kreis externer Partner: Steuerberatung, Kanzlei, wichtige Kunden und Lieferanten. Wenn externe Freigaben nur an deren Domains möglich sind, kann niemand versehentlich oder absichtlich Dateien an private oder unbekannte Adressen teilen.

Wo Sie die Einstellung finden: SharePoint Admin Center (<tenant>-admin.sharepoint.com) > Richtlinien > Freigabe > Weitere Einstellungen für die externe Freigabe > Externe Freigabe nach Domäne einschränken

So beheben Sie es

Externe Freigaben auf Partnerdomains beschränken

Beschränken Sie externe Freigaben in SharePoint und OneDrive auf eine Positivliste zugelassener Partnerdomains.

- Erstellen Sie mit den Fachabteilungen eine Liste der Partnerdomains, mit denen tatsächlich Dateien geteilt werden (z. B. kanzlei-mustermann.de).
- Öffnen Sie im SharePoint Admin Center Richtlinien > Freigabe > Weitere Einstellungen für die externe Freigabe.

Hinweis für die IT: SharePoint Online PowerShell: Get-SPOTenant | fl SharingDomainRestrictionMode,SharingAllowedDomainList – erwartet AllowList. Setzen: Set-SPOTenant - SharingDomainRestrictionMode AllowList - SharingAllowedDomainList "partner1.de partner2.de"

SCuBA (CISA)	MS.SHAREPOINT.1.3v1 Externe Freigabe nur an freigegebene Domains oder Gruppen
BSI IT-Grundschutz	CON.9.A1 Festlegung zulässiger Empfangender
DSGVO	Art. 32 Abs. 1 lit. b
Secure Score	Externe Freigabe über Domainliste steuern, bis zu 2 Punkte
Benötigte Lizenz	Keine Zusatzlizenz erforderlich

3. Aktivieren Sie „Externe Freigabe nach Domäne einschränken“, wählen Sie „Nur bestimmte Domänen zulassen“ und tragen Sie die Domains ein.
4. Speichern Sie und kommunizieren Sie, wie neue Partnerdomains beantragt werden (fester Ansprechpartner, kurze Prüfung).
5. Testen Sie: Eine Freigabe an eine Adresse außerhalb der Liste muss abgelehnt werden. Überprüfen Sie die Liste halbjährlich.

 **Handlungsbedarf**, Schweregrad mittel

Pos. 50, AS-AN-004

Es gibt keine eigene Liste gesperrter Kennwörter

Anforderung: Eine eigene Liste gesperrter Kennwörter (z. B. Firmenname) ist aktiv

Es ist keine hinterlegt.

Warum das wichtig ist

Viele Mitarbeitende wählen Kennwörter, die den Firmennamen, den Ort oder Produktnamen enthalten. Genau diese Begriffe probieren Angreifer zuerst aus. Mit einer eigenen Sperrliste lehnt Microsoft 365 solche Kennwörter automatisch ab.

Wo Sie die Einstellung finden: Microsoft Entra Admin Center (entra.microsoft.com) > Entra ID > Authentifizierungsmethoden > Kennwortschutz

Hinweis für die IT: Microsoft Graph PowerShell: (Get-MgBetaDirectorySetting | ? DisplayName -eq 'Password Rule Settings').Values | ? Name -in 'EnableBannedPasswordCheck','BannedPasswordList'

BSI IT-Grundschutz	ORP.4.A8 Regelung des Passwortgebrauchs; ORP.4.A22 Regelung zur Passwortqualität
DSGVO	Art. 32 Abs. 1 lit. b
Secure Score	aad_custom_banned_passwords
Benötigte Lizenz	Microsoft Entra ID P1 (enthalten z. B. in Microsoft 365 Business Premium, E3 und E5) oder Microsoft Entra ID P2 (enthalten z. B. in Microsoft 365 E5)

So beheben Sie es

Eigene Liste gesperrter Kennwörter anlegen (z. B. Firmenname)

Die benutzerdefinierte Liste gesperrter Kennwörter wird aktiviert und mit firmenspezifischen Begriffen gefüllt.

1. Öffnen Sie Entra ID > Authentifizierungsmethoden > Kennwortschutz (erfordert Microsoft Entra ID P1).
2. Stellen Sie „Benutzerdefinierte Liste erzwingen“ auf „Ja“.
3. Tragen Sie unter „Benutzerdefinierte Liste gesperrter Kennwörter“ Begriffe ein: Firmenname, Abkürzungen, Ort, Produkt- und Markennamen, Sportverein (je 4–16 Zeichen, eine Zeile pro Begriff).
4. Speichern Sie. Die Liste greift bei der nächsten Kennwortänderung, bestehende Kennwörter bleiben gültig.
5. Bei lokalem AD: Prüfen Sie, ob der Entra-Kennwortschutz-Agent auf den Domänencontrollern eingesetzt werden soll.

 **Handlungsbedarf**, Schweregrad mittel

Pos. 16, AS-AN-021

Das Registrieren neuer MFA-Methoden ist nicht abgesichert

Anforderung: Das Registrieren neuer Sicherheitsinformationen (MFA-Methoden) ist durch bedingten Zugriff geschützt

Keine Richtlinie für bedingten Zugriff schützt das Registrieren neuer MFA-Methoden (4 Richtlinien im Tenant geprüft).

Warum das wichtig ist

Wer eine neue MFA-Methode zu einem Konto hinzufügen darf, kontrolliert das Konto. Kennt ein Angreifer nur das Passwort, könnte er sonst sein eigenes Handy als zweiten Faktor eintragen. Eine Richtlinie verlangt für diese Registrierung bereits MFA oder ein Firmengerät.

Wo Sie die Einstellung finden: Microsoft Entra Admin Center (entra.microsoft.com) > Entra ID > Bedingter Zugriff > Richtlinien

So beheben Sie es

Registrierung von MFA-Methoden per bedingtem Zugriff schützen

Schützen Sie die Registrierung von Sicherheitsinformationen per bedingtem Zugriff mit MFA oder Gerätevoraussetzung (erfordert Entra ID P1).

1. Öffnen Sie im Entra Admin Center Entra ID > Bedingter Zugriff > Richtlinien und wählen Sie „Neue Richtlinie“ (oder „Neue Richtlinie aus Vorlage“).

Hinweis für die IT: Microsoft Graph PowerShell: `Get-MgIdentityConditionalAccessPolicy | ? { \$\_.Conditions.Applications.IncludeUserActions -contains 'urn:user:registersecurityinfo' } | ft DisplayName,State`

SCuBA (CISA)	MS.AAD.3.8v1 MFA-Registrierung nur von verwalteten Geräten
BSI IT-Grundschrift	ORP.4.A13 Geeignete Auswahl von Authentisierungsmechanismen
DSGVO	Art. 32 Abs. 1 lit. b
Benötigte Lizenz	Microsoft Entra ID P1 (enthalten z. B. in Microsoft 365 Business Premium, E3 und E5) oder Microsoft Entra ID P2 (enthalten z. B. in Microsoft 365 E5)

2. Benutzer: „Alle Benutzer“. Schließen Sie unter „Ausschließen“ Ihre zwei Notfallkonten (Break-Glass) und das Synchronisierungskonto von Entra Connect aus.
3. Zielressourcen: „Benutzeraktionen“ > „Sicherheitsinformationen registrieren“.
4. Gewähren: MFA bzw. Authentifizierungsstärke, oder ein konformes bzw. hybrid eingebundenes Gerät.
5. Richten Sie für neue Mitarbeitende den befristeten Zugriffspass (Temporary Access Pass) ein, damit sie ihre erste Methode registrieren können.
6. Aktivieren Sie die Richtlinie zunächst im Modus „Nur Bericht“ und werten Sie das Anmeldeprotokoll einige Tage aus.
7. Schalten Sie die Richtlinie danach auf „Ein“ und testen Sie mit einem betroffenen Konto in einem privaten Browserfenster.

 **Handlungsbedarf**, Schweregrad mittel

Pos. 14, AS-AN-023

Administratoren müssen sich nicht phishing-resistent anmelden

Anforderung: Administratoren müssen sich phishing-resistent anmelden (Passkey, Windows Hello, Zertifikat)

Keine Richtlinie verlangt von Administratoren eine phishing-resistente Anmeldung (Passkey, Windows Hello).

Warum das wichtig ist

Auch normale MFA per App-Bestätigung lässt sich mit modernen Phishing-Seiten aushebeln, die Anmeldung und Bestätigung in Echtzeit weiterreichen. Passkeys, Windows Hello for Business oder Zertifikate sind fest an die echte Microsoft-Seite gebunden und lassen sich so nicht abfangen. Für Administratoren lohnt sich dieser Schutz besonders.

Wo Sie die Einstellung finden: Microsoft Entra Admin Center (entra.microsoft.com) > Entra ID > Bedingter Zugriff > Richtlinien

Hinweis für die IT: Microsoft Graph PowerShell: `Get-MgIdentityConditionalAccessPolicy | ? { \$\_.GrantControls.AuthenticationStrength.Id -eq '00000000-0000-0000-0000-000000000004' } | ft DisplayName,State`

SCuBA (CISA)	MS.AAD.3.6v1 Phishing-resistente MFA für hoch privilegierte Rollen
BSI IT-Grundschrift	ORP.4.A10 Schutz von Benutzendenkennungen mit weitreichenden Berechtigungen
DSGVO	Art. 32 Abs. 1 lit. b
Secure Score	aad_phishing_MFA_strength
Benötigte Lizenz	Microsoft Entra ID P1 (enthalten z. B. in Microsoft 365 Business Premium, E3 und E5) oder Microsoft Entra ID P2 (enthalten z. B. in Microsoft 365 E5)

So beheben Sie es

Phishing-resistente MFA für Administratoren verlangen

Verlangen Sie per bedingtem Zugriff für Administratoren die Authentifizierungsstärke „Phishing-resistente MFA“ (erfordert Entra ID P1).

1. Statten Sie alle Administratoren zuerst mit einer phishing-resistenten Methode aus (Passkey/FIDO2-Schlüssel, Passkey in Authenticator oder Windows Hello for Business) und testen Sie die Anmeldung.
2. Öffnen Sie im Entra Admin Center Entra ID > Bedingter Zugriff > Richtlinien und wählen Sie „Neue Richtlinie“ (oder „Neue Richtlinie aus Vorlage“).
3. Benutzer: unter „Verzeichnisrollen“ alle Administratorrollen einschließen. Schließen Sie unter „Ausschließen“ Ihre zwei Notfallkonten (Break-Glass) und das Synchronisierungskonto von Entra Connect aus.
4. Zielressourcen: „Alle Ressourcen“. Gewähren: „Authentifizierungsstärke erforderlich“ > „Phishing-resistente MFA“.
5. Aktivieren Sie die Richtlinie zunächst im Modus „Nur Bericht“ und werten Sie das Anmeldeprotokoll einige Tage aus.
6. Schalten Sie die Richtlinie danach auf „Ein“ und testen Sie mit einem betroffenen Konto in einem privaten Browserfenster. Halten Sie für jedes Adminkonto eine zweite registrierte Methode als Reserve bereit.

Gastbenutzer müssen sich nicht mit MFA anmelden

Anforderung: Gastbenutzer müssen sich mit Multifaktor anmelden

Keine Richtlinie verlangt von Gastbenutzern eine Multifaktor-Anmeldung.

Warum das wichtig ist

Gäste aus Partnerfirmen haben Zugriff auf Ihre Teams und Dateien, doch deren Konten verwalten Sie nicht selbst. Verlangen Sie für Gäste ebenfalls einen zweiten Faktor, schützen Sie Ihre Daten auch dann, wenn das Passwort eines Gastes in fremde Hände gerät.

Wo Sie die Einstellung finden: Microsoft Entra Admin Center (entra.microsoft.com) > Entra ID > Bedingter Zugriff > Richtlinien

Hinweis für die IT: Microsoft Graph PowerShell: `Get-MgIdentityConditionalAccessPolicy | ? { $_.Conditions.Users.IncludeGuestsOrExternalUsers -or $_.Conditions.Users.IncludeUsers -contains 'GuestsOrExternalUsers' } | ft DisplayName, State``

SCuBA (CISA)	MS.AAD.3.2v2 MFA für alle Benutzer erzwingen
BSI IT-Grundschutz DSGVO	ORP.4.A21 Mehr-Faktor-Authentisierung Art. 32 Abs. 1 lit. b
Benötigte Lizenz	Microsoft Entra ID P1 (enthalten z. B. in Microsoft 365 Business Premium, E3 und E5) oder Microsoft Entra ID P2 (enthalten z. B. in Microsoft 365 E5)

So beheben Sie es

MFA für Gast- und externe Benutzer verlangen

Erstellen Sie eine Richtlinie für bedingten Zugriff, die für alle Gast- und externen Benutzer MFA verlangt (erfordert Entra ID P1).

1. Öffnen Sie im Entra Admin Center Entra ID > Bedingter Zugriff > Richtlinien und wählen Sie „Neue Richtlinie“ (oder „Neue Richtlinie aus Vorlage“).
2. Benutzer: Einschließen > „Gast- oder externe Benutzer“ und alle Typen auswählen.
3. Zielressourcen: „Alle Ressourcen“. Gewähren: „Authentifizierungsstärke erforderlich“ (Multi-Faktor-Authentifizierung) oder „Multi-Faktor-Authentifizierung erforderlich“.
4. Optional: Vertrauen Sie unter Externe Identitäten > Mandantenübergreifende Zugriffseinstellungen der MFA bekannter Partner-Tenants, um Doppelabfragen zu vermeiden.
5. Aktivieren Sie die Richtlinie zunächst im Modus „Nur Bericht“ und werten Sie das Anmeldeprotokoll einige Tage aus.
6. Schalten Sie die Richtlinie danach auf „Ein“ und testen Sie mit einem betroffenen Konto in einem privaten Browserfenster. Informieren Sie Ihre wichtigsten Partner über die neue Anforderung.

SMS ist als Anmeldemethode erlaubt

Anforderung: Die Anmeldemethode SMS ist deaktiviert

SMS und Sprachanruf sind aktiv, und 12 Benutzer haben ausschließlich eines davon hinterlegt.

Warum das wichtig ist

SMS-Codes waren lange der Standard für den zweiten Faktor, gelten heute aber als schwach. Über SIM-Tausch beim Mobilfunkanbieter oder abgefangene Nachrichten können Angreifer den Code erhalten. Die Authenticator App oder Passkeys bieten deutlich mehr Schutz.

Wo Sie die Einstellung finden: Microsoft Entra Admin Center (entra.microsoft.com) > Entra ID > Authentifizierungsmethoden > Richtlinien > SMS

Hinweis für die IT: Microsoft Graph PowerShell: `(Get-MgPolicyAuthenticationMethodPolicy).AuthenticationMethodConfigurations | ? Id -eq 'Sms' | ft Id, State`` – Sollwert: disabled.

SCuBA (CISA)	MS.AAD.3.5v2 SMS, Sprachanruf und E-Mail-Einmalcode deaktivieren
BSI IT-Grundschutz DSGVO	ORP.4.A13 Geeignete Auswahl von Authentisierungsmechanismen Art. 32 Abs. 1 lit. b
Benötigte Lizenz	Keine Zusatzlizenz erforderlich

So beheben Sie es

SMS als Anmeldemethode abschalten

Deaktivieren Sie SMS als Anmeldemethode in den Authentifizierungsmethoden-Richtlinien.

1. Ermitteln Sie unter Authentifizierungsmethoden > Benutzerregistrierungsdetails, wer ausschließlich SMS registriert hat.
2. Begleiten Sie diese Personen bei der Einrichtung der Authenticator App oder eines Passkeys und geben Sie eine Frist vor.
3. Öffnen Sie Entra ID > Authentifizierungsmethoden > Richtlinien > SMS und setzen Sie „Aktivieren“ auf „Aus“; speichern Sie.
4. Prüfen Sie, dass die Self-Service-Kennwortzurücksetzung weiterhin mit anderen Methoden funktioniert.
5. Testen Sie mit einem Pilotkonto, dass SMS bei der Anmeldung nicht mehr angeboten wird.

Passkeys (FIDO2) sind als Anmeldemethode nicht freigegeben

Anforderung: Phishing-resistente Anmeldung mit Passkeys (FIDO2) ist freigegeben

Passkeys (FIDO2) sind nicht freigegeben.

Warum das wichtig ist

Passkeys sind der sicherste Weg, sich anzumelden: Sie sind an die echte Microsoft-Seite gebunden und können von Phishing-Seiten nicht abgefangen werden. Sie funktionieren mit Sicherheitsschlüsseln (z. B. USB-Token) oder auf dem Smartphone in der Authenticator App und ersetzen oft sogar das Passwort.

Wo Sie die Einstellung finden: Microsoft Entra Admin Center (entra.microsoft.com) > Entra ID > Authentifizierungsmethoden > Richtlinien > „Passkey (FIDO2)“

Hinweis für die IT: Microsoft Graph PowerShell: `Get-MgPolicyAuthenticationMethodPolicyAuthenticationMethodConfiguration -AuthenticationMethodConfigurationId Fido2 | fl Id,State` – Sollwert: enabled.

BSI IT-Grundschutz	ORP.4.A13 Geeignete Auswahl von Authentisierungsmechanismen
DSGVO	Art. 32 Abs. 1 lit. b
Benötigte Lizenz	Keine Zusatzlizenz erforderlich

So beheben Sie es

Passkeys (FIDO2) als Anmeldemethode freigeben

Aktivieren Sie die Anmeldemethode „Passkey (FIDO2)“ in den Authentifizierungsmethoden-Richtlinien.

1. Öffnen Sie Entra ID > Authentifizierungsmethoden > Richtlinien > „Passkey (FIDO2)“.
2. Aktivieren Sie die Methode, zunächst für eine Pilotgruppe (z. B. Administratoren), später für „Alle Benutzer“.
3. Prüfen Sie auf der Registerkarte „Konfigurieren“, ob gerätegebundene Passkeys in der Authenticator App und Sicherheitsschlüssel erlaubt sind; speichern Sie.
4. Lassen Sie die Pilotgruppe unter mysignins.microsoft.com/security-info einen Passkey registrieren und die Anmeldung testen.
5. Nutzen Sie die Passkeys anschließend für eine Richtlinie „Phishing-resistente MFA“ für Administratoren.

Inaktive Sitzungen in SharePoint und OneDrive bleiben angemeldet

Anforderung: Inaktive Sitzungen in SharePoint und OneDrive werden automatisch abgemeldet

Die Abmeldung ist abgeschaltet.

Warum das wichtig ist

Wird an einem fremden oder gemeinsam genutzten Rechner vergessen, sich abzumelden, bleibt der Zugriff auf SharePoint und OneDrive offen. Die automatische Abmeldung nach Inaktivität schließt solche Sitzungen. Sie greift im Browser auf nicht verwalteten Geräten, also typischerweise auf privaten oder fremden PCs.

Wo Sie die Einstellung finden: SharePoint Admin Center (<tenant>-admin.sharepoint.com) > Richtlinien > Zugriffssteuerung > Abmeldung bei Leerlaufsitzung

Hinweis für die IT: SharePoint Online PowerShell: Get-SPOBrowserIdleSignOut – erwartet Enabled = True. Setzen: Set-SPOBrowserIdleSignOut -Enabled \$true -WarnAfter (New-TimeSpan -Minutes 45) -SignOutAfter (New-TimeSpan -Hours 1)

BSI IT-Grundschutz	SYS.2.1.A1 Sichere Authentisierung von Benutzenden
DSGVO	Art. 32 Abs. 1 lit. b
Secure Score	spo_idle_session_timeout
Benötigte Lizenz	Keine Zusatzlizenz erforderlich

So beheben Sie es

Automatische Abmeldung bei Inaktivität einschalten

Aktivieren Sie die automatische Abmeldung inaktiver Browser-Sitzungen in SharePoint und OneDrive.

1. Prüfen Sie die Voraussetzung: Die Funktion nutzt Conditional Access und erfordert Microsoft Entra ID P1 oder P2.
2. Öffnen Sie im SharePoint Admin Center Richtlinien > Zugriffssteuerung > Abmeldung bei Leerlaufsitzung.
3. Aktivieren Sie „Inaktive Benutzer automatisch abmelden“ und wählen Sie z. B. Warnung nach 45 Minuten und Abmeldung nach 1 Stunde. Speichern Sie.
4. Beachten Sie: Auf verwalteten (konformen oder domänengebundenen) Geräten und bei „Angemeldet bleiben“ greift die Abmeldung nicht. Blenden Sie diese Option ggf. über das Unternehmensbranding aus.
5. Testen Sie nach etwa 15 Minuten Wartezeit auf einem nicht verwalteten Gerät, ob die Warnung erscheint.

Nicht alle Benutzer müssen sich phishing-resistent anmelden

Anforderung: Bedingter Zugriff verlangt von allen Benutzern eine phishing-resistente Anmeldung (Passkey, Windows Hello, Zertifikat)

Keine der 4 Richtlinien tut das; alle Benutzer melden sich mit Kennwort und Authenticator-Bestätigung an.

Warum das wichtig ist

Multifaktor per App-Bestätigung oder Einmalcode lässt sich mit heutigen Phishing-Werkzeugen aushebeln: Eine gefälschte Anmeldeseite reicht Kennwort und Bestätigung in Echtzeit an Microsoft weiter und übernimmt die Sitzung. Passkeys (FIDO2), Windows Hello for Business und die Anmeldung per Zertifikat sind an die echte Microsoft-Adresse gebunden und funktionieren auf einer gefälschten Seite nicht. Für Administratoren prüft Auditspiegel das gesondert; diese Prüfung betrifft alle Benutzer.

Wo Sie die Einstellung finden: Microsoft Entra Admin Center (entra.microsoft.com) > Entra ID > Bedingter Zugriff > Richtlinien

Hinweis für die IT: Microsoft Graph PowerShell: `'Get-MgIdentityConditionalAccessPolicy | ? { $_.GrantControls.AuthenticationStrength.Id -eq '00000000-0000-0000-0000-000000000004' -and $_.Conditions.Users.IncludeUsers -contains 'All' } | ft DisplayName,State'`. Ausgewertet wird die integrierte Authentifizierungsstärke „Phishing-resistente MFA“; eine selbst angelegte Stärke erkennt die Prüfung nicht.

SCuBA (CISA)	MS.AAD.3.1v1 Phishing-resistente MFA für alle Benutzer erzwingen
BSI IT-Grundschutz	ORP.4.A21 Mehr-Faktor-Authentisierung; ORP.4.A13 Geeignete Auswahl von Authentisierungsmechanismen
DSGVO	Art. 32 Abs. 1 lit. b
Benötigte Lizenz	Microsoft Entra ID P1 (enthalten z. B. in Microsoft 365 Business Premium, E3 und E5) oder Microsoft Entra ID P2 (enthalten z. B. in Microsoft 365 E5)

So beheben Sie es

Phishing-resistente MFA für alle Benutzer verlangen

Verlangen Sie per bedingtem Zugriff für alle Benutzer und alle Ressourcen die Authentifizierungsstärke „Phishing-resistente MFA“ (erfordert Microsoft Entra ID P1). Führen Sie das schrittweise ein, zuerst für Administratoren, dann Abteilung für Abteilung.

1. Geben Sie im Entra Admin Center unter Entra ID > Authentifizierungsmethoden > Richtlinien die Methode „Passkey (FIDO2)“ frei, bei Bedarf auch Windows Hello for Business. Passkeys lassen sich auch in Microsoft Authenticator auf dem Smartphone speichern.
2. Lassen Sie alle Mitarbeitenden eine phishing-resistente Methode registrieren (Mein Konto > Sicherheitsinformationen, aka.ms/mysecurityinfo) und verfolgen Sie den Fortschritt im Bericht „Registrierungsdetails der Benutzer“.
3. Öffnen Sie Entra ID > Bedingter Zugriff > Richtlinien > „Neue Richtlinie“. Benutzer: „Alle Benutzer“ einschließen; unter „Ausschließen“ Ihre zwei Notfallkonten (Break-Glass) und das Synchronisierungskonto von Entra Connect.
4. Zielressourcen: „Alle Ressourcen (früher „Alle Cloud-Apps“)“. Gewähren: „Authentifizierungsstärke erforderlich“ > „Phishing-resistente MFA“.
5. Aktivieren Sie die Richtlinie zunächst im Modus „Nur Bericht“ und sehen Sie im Anmeldeprotokoll nach, wer noch keine passende Methode hat.
6. Schalten Sie die Richtlinie auf „Ein“, sobald alle Benutzer eine passende Methode registriert haben, und testen Sie mit einem Testkonto in einem privaten Browserfenster.

Mitarbeitende können eigene Apps, Testversionen und Dienste aktivieren

Anforderung: Mitarbeiter können keine eigenen Apps, Testversionen oder Dienste in Microsoft 365 aktivieren

Laut Microsoft Secure Score dürfen Beschäftigte Testversionen und eigene Apps in Microsoft 365 selbst aktivieren (0 % erfüllt).

Warum das wichtig ist

Standardmäßig dürfen Mitarbeitende Apps aus dem Office Store hinzufügen und Testversionen von Microsoft-Diensten im Namen der Firma starten. Damit gelangen Anwendungen in Ihre Umgebung, die die IT weder kennt noch geprüft hat und die auf Firmendaten zugreifen können.

Wo Sie die Einstellung finden: Microsoft 365 Admin Center (admin.microsoft.com) > Einstellungen > Organisationseinstellungen > Dienste > Benutzereigene Apps und Dienste

Hinweis für die IT: Microsoft Graph PowerShell: `Invoke-MgGraphRequest -Uri 'https://graph.microsoft.com/beta/admin/appsAndServices' (Felder isOfficeStoreEnabled, isAppAndServicesTrialEnabled)`

So beheben Sie es

Office Store und Testversionen für Mitarbeitende sperren

Der Zugriff auf den Office Store und das Starten von Testversionen durch Mitarbeitende wird deaktiviert.

1. Öffnen Sie im Microsoft 365 Admin Center Einstellungen > Organisationseinstellungen > Dienste > „Benutzereigene Apps und Dienste“.
2. Deaktivieren Sie „Benutzern den Zugriff auf den Office Store erlauben“.
3. Deaktivieren Sie „Benutzern das Starten von Testversionen von Apps und Diensten erlauben“ und speichern Sie.
4. Prüfen Sie zusätzlich, ob Self-Service-Käufe deaktiviert werden sollen (MSCommerce-PowerShell-Modul).

BSI IT-Grundschutz	APP.6.A4 Regelung für die Installation und Konfiguration von Software
DSGVO	Art. 32 Abs. 1 lit. b
Secure Score	admincenter_owned_apps_and_services
Benötigte Lizenz	Keine Zusatzlizenz erforderlich

5. Legen Sie einen Weg fest, über den Mitarbeitende neue Apps bei der IT beantragen.
6. Die Änderung erscheint im Microsoft Secure Score und damit in Auditspiegel oft erst nach 24–48 Stunden.

 **Handlungsbedarf**, Schweregrad mittel

Pos. 18, AS-AP-003

Mitarbeitende dürfen eigene App-Registrierungen anlegen

Anforderung: Mitarbeiter dürfen keine eigenen App-Registrierungen anlegen

Jeder Mitarbeiter darf Anwendungen in Ihrem Tenant registrieren.

Warum das wichtig ist

Eine App-Registrierung ist eine Art Eintrittskarte, mit der eine Software auf Daten in Ihrem Microsoft 365 zugreifen kann. Dürfen alle Mitarbeitenden solche Registrierungen anlegen, entstehen unkontrollierte Zugänge, die niemand überblickt. Das sollte Administratoren vorbehalten sein.

Wo Sie die Einstellung finden: Microsoft Entra Admin Center (entra.microsoft.com) > Entra ID > Benutzer > Benutzereinstellungen > „Benutzer können Anwendungen registrieren“

Hinweis für die IT: Microsoft Graph PowerShell: `(Get-MgPolicyAuthorizationPolicy).DefaultUserRolePermissions.AllowedToCreateApps` – ändern mit `Update-MgPolicyAuthorizationPolicy -DefaultUserRolePermissions @{AllowedToCreateApps=\$false}`.

SCuBA (CISA)	MS.AAD.5.1v1 Nur Administratoren registrieren Anwendungen
BSI IT-Grundschutz	APP.6.A4 Regelung für die Installation und Konfiguration von Software
DSGVO	Art. 32 Abs. 1 lit. b
Secure Score	aad_third_party_apps
Benötigte Lizenz	Keine Zusatzlizenz erforderlich

So beheben Sie es

App-Registrierungen auf Administratoren beschränken

Erlauben Sie nur Administratoren, Anwendungen in Ihrem Tenant zu registrieren.

1. Öffnen Sie Entra ID > Benutzer > Benutzereinstellungen.
2. Setzen Sie „Benutzer können Anwendungen registrieren“ auf „Nein“ und speichern Sie.
3. Prüfen Sie unter Entra ID > App-Registrierungen > Alle Anwendungen, welche Apps von normalen Mitarbeitenden angelegt wurden, und entfernen Sie nicht benötigte.
4. Weisen Sie Personen, die tatsächlich Apps entwickeln, gezielt die Rolle „Anwendungsentwickler“ zu.
5. Prüfen Sie mit einem normalen Konto, dass „Neue Registrierung“ nicht mehr möglich ist.

 **Handlungsbedarf**, Schweregrad mittel

Pos. 31, AS-DA-006

Es ist keine Richtlinie zur Verhinderung von Datenverlust (DLP) aktiv

Anforderung: Richtlinien zur Verhinderung von Datenverlust (DLP) sind aktiv

Laut Microsoft Secure Score ist keine Richtlinie zur Verhinderung von Datenverlust aktiv (0 % erfüllt).

Warum das wichtig ist

Richtlinien zur Verhinderung von Datenverlust (DLP) erkennen automatisch, wenn sensible Daten wie IBANs, Ausweis- oder Steuernummern per E-Mail verschickt oder extern geteilt werden. Sie können warnen, blockieren oder die IT informieren, bevor Daten das Unternehmen verlassen.

Wo Sie die Einstellung finden: Microsoft Purview Portal (purview.microsoft.com) > Lösungen > Verhinderung von Datenverlust > Richtlinien

Hinweis für die IT: Security & Compliance PowerShell (Connect-IPPSSession): Get-DlpCompliancePolicy | fl Name,Mode,Enabled,ExchangeLocation,SharePointLocation,OneDriveLocation

So beheben Sie es

DLP-Richtlinie für E-Mail, SharePoint und OneDrive einrichten

Mindestens eine DLP-Richtlinie für Exchange, SharePoint und OneDrive ist aktiv.

1. Öffnen Sie im Microsoft Purview Portal Lösungen > Verhinderung von Datenverlust > Richtlinien und wählen Sie „Richtlinie erstellen“.
2. Wählen Sie eine passende Vorlage, z. B. für deutsche personenbezogene Daten oder Finanzdaten (Kategorie „Datenschutz“ bzw. „Finanzen“, Region Deutschland).
3. Wählen Sie als Speicherorte Exchange-E-Mail, SharePoint-Websites und OneDrive-Konten.
4. Starten Sie die Richtlinie im Simulationsmodus mit Richtlinienertipps, werten Sie die Treffer zwei Wochen aus und aktivieren Sie sie dann.
5. Informieren Sie die Mitarbeitenden über die neuen Warnhinweise.

SCuBA (CISA)	MS.SECURITYSUITE.3.1v1 DLP-Richtlinie für personenbezogene und sensible Daten
BSI IT-Grundschutz	CON.9.A2 Regelung des Informationsaustausches
DSGVO	Art. 32 Abs. 1 lit. b
Secure Score	dlp_datalossprevention
Benötigte Lizenz	Keine Zusatzlizenz erforderlich

6. Der Status erscheint im Microsoft Secure Score und in Auditspiegel nach 24–48 Stunden.

 **Handlungsbedarf**, Schweregrad mittel

Pos. 32, AS-DA-007

DLP-Richtlinien schützen keine Chats und Kanäle in Teams

Anforderung: DLP-Richtlinien schützen auch Chats und Kanäle in Microsoft Teams

Laut Microsoft Secure Score schützt keine DLP-Richtlinie die Chats und Kanäle in Teams (0 % erfüllt).

Warum das wichtig ist

Viele Mitarbeitende teilen Informationen heute eher im Teams-Chat als per E-Mail. Gilt die DLP-Richtlinie dort nicht, können sensible Daten wie Kundenlisten oder Bankverbindungen ungeprüft an Gäste und externe Chatpartner gehen.

Wo Sie die Einstellung finden: Microsoft Purview Portal (purview.microsoft.com) > Lösungen > Verhinderung von Datenverlust > Richtlinien

Hinweis für die IT: Security & Compliance PowerShell (Connect-IPPSSession): Get-DlpCompliancePolicy | fl Name,Mode,TeamsLocation

SCuBA (CISA)	MS.SECURITYSUITE.3.2v1 DLP für Exchange, OneDrive, SharePoint, Teams und Geräte
BSI IT-Grundschutz	CON.9.A2 Regelung des Informationsaustausches
DSGVO	Art. 32 Abs. 1 lit. b
Secure Score	mip_DLP_policies_Teams
Benötigte Lizenz	Keine Zusatzlizenz erforderlich

So beheben Sie es

DLP-Richtlinien auf Teams-Chats und -Kanäle ausweiten

Die DLP-Richtlinien werden auf Teams-Chat- und Kanalnachrichten ausgeweitet.

1. Prüfen Sie die Lizenz: DLP für Teams-Chats erfordert z. B. Microsoft 365 E5, E5 Compliance oder ein passendes Add-on.
2. Öffnen Sie im Purview Portal Verhinderung von Datenverlust > Richtlinien und bearbeiten Sie Ihre bestehende Richtlinie oder legen Sie eine neue an.
3. Aktivieren Sie unter „Speicherorte“ „Teams-Chat- und Kanalnachrichten“.
4. Testen Sie die Richtlinie zunächst im Simulationsmodus und prüfen Sie mit einem Pilotbenutzer, ob eine Testnachricht mit z. B. einer Test-IBAN erkannt wird.
5. Aktivieren Sie die Richtlinie und prüfen Sie nach 24–48 Stunden den Secure-Score-Status.

 **Handlungsbedarf**, Schweregrad mittel

Pos. 72, AS-DA-008

Es sind keine Vertraulichkeitsbezeichnungen veröffentlicht

Anforderung: Vertraulichkeitsbezeichnungen (z. B. „Intern“, „Vertraulich“) sind veröffentlicht

Laut Microsoft Secure Score sind keine Vertraulichkeitsbezeichnungen veröffentlicht (0 % erfüllt).

Warum das wichtig ist

Mit Vertraulichkeitsbezeichnungen wie „Intern“ oder „Vertraulich“ kennzeichnen Mitarbeitende Dokumente und E-Mails. Je nach Stufe kann Microsoft 365 automatisch verschlüsseln, eine Kennzeichnung einblenden oder die Weitergabe an Externe verhindern. So bleibt der Schutz auch beim Weiterleiten erhalten.

Wo Sie die Einstellung finden: Microsoft Purview Portal (purview.microsoft.com) > Lösungen > Information Protection > Vertraulichkeitsbezeichnungen

Hinweis für die IT: Security & Compliance PowerShell (Connect-IPPSSession): Get-Label | Select DisplayName,Priority; Get-LabelPolicy | fl Name,Labels,Mode

BSI IT-Grundschutz	CON.9.A2 Regelung des Informationsaustausches
DSGVO	Art. 32 Abs. 1 lit. a; Art. 32 Abs. 1 lit. b
Secure Score	mip_sensitivitylabelspolicies
Benötigte Lizenz	Keine Zusatzlizenz erforderlich

So beheben Sie es

Vertraulichkeitsbezeichnungen anlegen und veröffentlichen

Vertraulichkeitsbezeichnungen werden erstellt und über eine Bezeichnungsrichtlinie an die Mitarbeitenden veröffentlicht.

1. Legen Sie ein einfaches Schema mit drei bis vier Stufen fest, z. B. „Öffentlich“, „Intern“, „Vertraulich“, „Streng vertraulich“.
2. Erstellen Sie im Purview Portal unter Information Protection > Vertraulichkeitsbezeichnungen die Bezeichnungen mit Kennzeichnung und ggf. Verschlüsselung.
3. Veröffentlichen Sie die Bezeichnungen über „Bezeichnungen veröffentlichen“ an alle Benutzer oder zunächst eine Pilotgruppe.
4. Legen Sie eine Standardbezeichnung (z. B. „Intern“) fest und schulen Sie die Mitarbeitenden kurz.
5. Prüfen Sie in Word/Outlook, ob die Schaltfläche „Vertraulichkeit“ erscheint (Verteilung kann bis zu 24 Stunden dauern).

Gäste dürfen Dateien weiterteilen, die ihnen nicht gehören

Anforderung: Gäste dürfen Dateien, die ihnen nicht gehören, nicht weiterteilen

Gäste dürfen Ihre Dateien an weitere Personen weitergeben.

Warum das wichtig ist

Wenn Sie eine Datei mit einem externen Partner teilen, sollte dieser sie nicht ohne Ihr Wissen an weitere Personen weitergeben können. Diese Einstellung sorgt dafür, dass nur Ihre eigenen Mitarbeitenden entscheiden, wer Zugriff auf Ihre Inhalte erhält.

Wo Sie die Einstellung finden: SharePoint Admin Center (<tenant>-admin.sharepoint.com) > Richtlinien > Freigabe > Weitere Einstellungen für die externe Freigabe

Hinweis für die IT: SharePoint Online PowerShell: Get-SPOTenant | fl PreventExternalUsersFromResharing – erwartet True. Setzen: Set-SPOTenant - PreventExternalUsersFromResharing \$true

BSI IT-Grundschutz	CON.9.A1 Festlegung zulässiger Empfangender
DSGVO	Art. 32 Abs. 1 lit. b
Secure Score	spo_external_users_sharing
Benötigte Lizenz	Keine Zusatzlizenz erforderlich

So beheben Sie es

Weiterteilen durch Gäste untersagen

Untersagen Sie Gästen in SharePoint und OneDrive, Elemente weiterzugeben, die ihnen nicht gehören.

1. Öffnen Sie im SharePoint Admin Center Richtlinien > Freigabe.
2. Klappen Sie „Weitere Einstellungen für die externe Freigabe“ auf.
3. Deaktivieren Sie die Option „Gästen das Freigeben von Elementen erlauben, die sie nicht besitzen“ und speichern Sie.
4. Testen Sie mit einem Gastkonto, dass die Schaltfläche zum Teilen bei fremden Dateien nicht mehr zur Verfügung steht.

SharePoint erlaubt Freigaben an neue externe Personen

Anforderung: Externe Freigaben in SharePoint sind höchstens an bereits vorhandene Gäste möglich

Die Einstellung steht auf „Jeder“: Mitarbeitende können Dateien an beliebige neue Adressen und sogar per anonymem Link freigeben.

Warum das wichtig ist

„Vorhandene Gäste“ heißt: Nach außen teilen lässt sich nur mit Personen, die bereits als Gast in Ihrem Verzeichnis stehen. Neue externe Empfänger kommen dann nicht mehr per Klick eines einzelnen Mitarbeitenden hinzu, sondern über einen bewussten Schritt, etwa eine Gast-Einladung durch die IT oder einen Teams-Besitzer.

Wo Sie die Einstellung finden: SharePoint Admin Center (<tenant>-admin.sharepoint.com) > Richtlinien > Freigabe > Externe Freigabe

Hinweis für die IT: SharePoint Online PowerShell: Get-SPOTenant | fl SharingCapability – erwartet ExistingExternalUserSharingOnly oder Disabled. Setzen: Set-SPOTenant -SharingCapability ExistingExternalUserSharingOnly

SCuBA (CISA)	MS.SHAREPOINT.1.1v1 Externe Freigabe in SharePoint höchstens an vorhandene Gäste
BSI IT-Grundschutz	CON.9.A1 Festlegung zulässiger Empfangender
DSGVO	Art. 32 Abs. 1 lit. b
Benötigte Lizenz	Keine Zusatzlizenz erforderlich

So beheben Sie es

Externe Freigabe in SharePoint auf vorhandene Gäste beschränken

Stellen Sie die externe Freigabe für SharePoint im SharePoint Admin Center auf „Vorhandene Gäste“ oder „Nur Personen in Ihrer Organisation“.

1. Klären Sie mit den Fachabteilungen, mit welchen externen Partnern heute Dateien geteilt werden (z. B. Steuerberatung, Kanzlei, Lieferanten).
2. Laden Sie diese Partner als Gäste ein (Entra ID > Benutzer > Externen Benutzer einladen) oder nehmen Sie sie in die passenden Teams auf, damit die laufende Zusammenarbeit weitergeht.
3. Öffnen Sie im SharePoint Admin Center Richtlinien > Freigabe und stellen Sie den Regler für SharePoint auf „Vorhandene Gäste“ oder „Nur Personen in Ihrer Organisation“. OneDrive kann nicht großzügiger sein als SharePoint.
4. Legen Sie fest, wer künftig neue Gäste einlädt (z. B. IT oder Teams-Besitzer), und teilen Sie das den Mitarbeitenden mit.
5. Testen Sie: Eine Freigabe an eine noch unbekannte externe Adresse muss abgelehnt werden.

Die Anmeldung ist auch von nicht verwalteten Geräten möglich

Anforderung: Bedingter Zugriff erlaubt die Anmeldung nur von verwalteten Geräten

Die Richtlinie läuft im Nur-Berichtsmodus und blockiert damit nichts.

Warum das wichtig ist

Mit dieser Richtlinie sind Anmeldungen nur von Geräten möglich, die Ihr Unternehmen verwaltet, also von Firmenlaptops mit aktuellem Virenschutz und Verschlüsselung. Private oder fremde Rechner bleiben außen vor, selbst wenn jemand Passwort und zweiten Faktor kennt.

Wo Sie die Einstellung finden: Microsoft Entra Admin Center (entra.microsoft.com) > Entra ID > Bedingter Zugriff > Richtlinien

Hinweis für die IT: Microsoft Graph PowerShell: ``Get-MgIdentityConditionalAccessPolicy | ? { $_.GrantControls.BuiltInControls -match 'Device' } | ft DisplayName,State``

SCuBA (CISA)	MS.AAD.3.7v1 Anmeldung nur von verwalteten Geräten
BSI IT-Grundschutz	SYS.3.2.2.A4 Verteilung der Grundkonfiguration auf mobile Endgeräte
DSGVO	Art. 32 Abs. 1 lit. b
Benötigte Lizenz	Microsoft Entra ID P1 (enthalten z. B. in Microsoft 365 Business Premium, E3 und E5) oder Microsoft Entra ID P2 (enthalten z. B. in Microsoft 365 E5)

So beheben Sie es

Anmeldung nur von verwalteten Geräten zulassen

Verlangen Sie per bedingtem Zugriff ein konformes (Intune) oder hybrid eingebundenes Gerät für die Anmeldung (erfordert Entra ID P1 und in der Regel Intune).

1. Stellen Sie sicher, dass alle Firmengeräte in Intune registriert sind und Konformitätsrichtlinien haben oder hybrid in Entra eingebunden sind.
2. Öffnen Sie im Entra Admin Center Entra ID > Bedingter Zugriff > Richtlinien und wählen Sie „Neue Richtlinie“ (oder „Neue Richtlinie aus Vorlage“).
3. Benutzer: „Alle Benutzer“. Schließen Sie unter „Ausschließen“ Ihre zwei Notfallkonten (Break-Glass) und das Synchronisierungskonto von Entra Connect aus. Zielressourcen: „Alle Ressourcen“.
4. Gewähren: „Markieren des Geräts als kompatibel erforderlich“ und/oder „In Microsoft Entra Hybrid eingebundenes Gerät erforderlich“ mit „Eines der ausgewählten Steuerelemente anfordern“.
5. Aktivieren Sie die Richtlinie zunächst im Modus „Nur Bericht“ und werten Sie das Anmeldeprotokoll einige Tage aus. Achten Sie besonders auf Smartphones und Gäste.
6. Schalten Sie die Richtlinie danach auf „Ein“ und testen Sie mit einem betroffenen Konto in einem privaten Browserfenster. Planen Sie für Mobilgeräte und Gäste bei Bedarf eigene Richtlinien.

OneDrive synchronisiert auch auf fremde, nicht verbundene Geräte

Anforderung: OneDrive synchronisiert nur auf firmeneigene (domänenverbundene) Geräte

OneDrive kann Firmendaten auf beliebige private Geräte synchronisieren.

Warum das wichtig ist

Der OneDrive-Client synchronisiert Firmendateien auf die lokale Festplatte. Ist das auf jedem beliebigen Rechner möglich, landen vollständige Kopien von Firmendaten auf privaten Laptops. Beschränken Sie die Synchronisierung auf Firmengeräte, die zu Ihrer Domäne gehören.

Wo Sie die Einstellung finden: SharePoint Admin Center (<tenant>-admin.sharepoint.com) > Einstellungen > OneDrive – „Synchronisierung“

Hinweis für die IT: SharePoint Online PowerShell: Get-SPOTenantSyncClientRestriction | fl TenantRestrictionEnabled,AllowedDomainList – erwartet True. Setzen: Set-SPOTenantSyncClientRestriction -Enable -DomainGuids "<GUID>"

BSI IT-Grundschutz	ORP.4.A16 Richtlinien für die Zugriffs- und Zugangskontrolle
DSGVO	Art. 32 Abs. 1 lit. b
Secure Score	spo_block_onedrive_sync_unmanaged_devices
Benötigte Lizenz	Keine Zusatzlizenz erforderlich

So beheben Sie es

OneDrive-Sync auf domänenverbundene Geräte beschränken

Erlauben Sie die OneDrive-Synchronisierung nur auf Rechnern, die Mitglied Ihrer Active-Directory-Domäne sind.

1. Prüfen Sie, ob Sie ein lokales Active Directory haben. Ermitteln Sie die Domänen-GUID mit Get-ADDomain | select ObjectGUID.
2. Reine Cloud-Umgebung ohne lokale Domäne? Steuern Sie das Ziel dann besser über Conditional Access mit „konformes Gerät“ und notieren Sie die Abweichung.
3. Öffnen Sie im SharePoint Admin Center Einstellungen > OneDrive „Synchronisierung“ und aktivieren Sie „Synchronisierung nur auf PCs zulassen, die bestimmten Domänen angehören“.
4. Tragen Sie die Domänen-GUID(s) ein, ggf. auch „Synchronisierung auf Mac blockieren“, und speichern Sie.
5. Testen Sie auf einem privaten PC, dass der OneDrive-Client keine Firmenbibliotheken mehr synchronisiert.

 **Handlungsbedarf**, Schweregrad mittel

Pos. 52, AS-ID-002

Es fehlen zwei erkennbare Notfallzugangs-Konten (Break-Glass)

Anforderung: Es gibt zwei erkennbare Notfallzugangs-Konten (Break-Glass) mit Globaler-Administrator-Rolle

Es wurden 0 von mindestens 2 Notfallzugangs-Konten erkannt.

Warum das wichtig ist

Notfallzugangs-Konten (Break-Glass) sind zwei reservierte Administratorkonten, mit denen Sie wieder in Ihren Tenant gelangen, wenn alle anderen Admins ausgesperrt sind, etwa durch eine fehlerhafte Richtlinie oder einen MFA-Ausfall. Ohne sie kann eine Fehlkonfiguration Sie dauerhaft aus Ihrer eigenen Umgebung aussperren.

Wo Sie die Einstellung finden: Microsoft Entra Admin Center (entra.microsoft.com) > Entra ID > Benutzer > Alle Benutzer > Neuer Benutzer; danach Entra ID > Rollen und Administratoren > Globaler Administrator > Zuweisungen hinzufügen

Hinweis für die IT: Auditspiegel erkennt Notfallkonten am Namen (UPN beginnt z. B. mit „breakglass“, „emergency“, „notfall“ oder Anzeigename enthält „Notfallzugang“). Anders benannte Konten bitte manuell bestätigen.

BSI IT-Grundschutz	ORP.4.A20 Notfallvorsorge für das Identitäts- und Berechtigungsmanagement-System
DSGVO	Art. 32 Abs. 1 lit. b; Art. 32 Abs. 1 lit. c
Benötigte Lizenz	Keine Zusatzlizenz erforderlich

So beheben Sie es

Zwei Notfallzugangs-Konten einrichten und sicher verwahren

Zwei eindeutig benannte, reine Cloud-Notfallkonten mit der Rolle „Globaler Administrator“ werden eingerichtet und sicher verwahrt.

1. Legen Sie zwei reine Cloud-Konten auf der Domain <firma>.onmicrosoft.com an, z. B. breakglass01@ und breakglass02@ oder mit Anzeigename „Notfallzugang 1/2“ – so erkennt Auditspiegel sie automatisch.
2. Weisen Sie beiden Konten dauerhaft die Rolle „Globaler Administrator“ zu; vergeben Sie keine Lizenzen.
3. Vergeben Sie lange, zufällige Kennwörter und schützen Sie die Konten mit phishingresistenten Methoden (z. B. FIDO2-Sicherheitsschlüssel); Microsoft verlangt für Admin-Portale ohnehin MFA.
4. Schließen Sie mindestens ein Notfallkonto aus allen Richtlinien für bedingten Zugriff aus, damit es bei Fehlkonfigurationen funktioniert.
5. Verwahren Sie Zugangsdaten und Schlüssel getrennt und versiegelt (z. B. Tresor), dokumentieren Sie, wer sie im Notfall nutzen darf.
6. Testen Sie die Anmeldung beider Konten mindestens halbjährlich und richten Sie eine Warnung für jede Anmeldung dieser Konten ein.

Nicht nur Administratoren und Gasteinladende dürfen Gäste einladen

Anforderung: Nur Administratoren und Gasteinladende dürfen Gäste einladen

Jeder Benutzer, auch Gäste, darf weitere Gäste einladen (Microsoft-Standard).

Warum das wichtig ist

Wenn jede Person Gäste einladen darf, wächst die Zahl externer Konten unkontrolliert. Legen Sie fest, dass nur Administratoren und Personen mit der Rolle „Gasteinladender“ einladen dürfen. Dann gibt es eine bewusste Entscheidung pro Gast und einen klaren Überblick.

Wo Sie die Einstellung finden: Microsoft Entra Admin Center (entra.microsoft.com) > Entra ID > Externe Identitäten > Einstellungen für externe Zusammenarbeit > Einstellungen für Gasteinladungen

Hinweis für die IT: Microsoft Graph PowerShell: `(Get-MgPolicyAuthorizationPolicy).AllowInvitesFrom` – Sollwert `adminsAndGuestInviters` oder `none`; ändern mit `Update-MgPolicyAuthorizationPolicy -AllowInvitesFrom adminsAndGuestInviters``.

SCuBA (CISA)	MS.AAD.8.2v1 Nur Gasteinladende dürfen Gäste einladen
BSI IT-Grundschutz	ORP.4.A1 Regelung für die Einrichtung und Löschung von Benutzenden und Benutzendengruppen
DSGVO	Art. 32 Abs. 1 lit. b
Benötigte Lizenz	Keine Zusatzlizenz erforderlich

So beheben Sie es

Gasteinladungen auf Admins und Gasteinladende beschränken

Beschränken Sie Gasteinladungen auf Administratoren und die Rolle „Gasteinladender“.

1. Öffnen Sie Entra ID > Externe Identitäten > Einstellungen für externe Zusammenarbeit.
2. Wählen Sie unter „Einstellungen für Gasteinladungen“ die Option „Nur Benutzer mit bestimmten Administratorrollen können Gastbenutzer einladen“.
3. Weisen Sie Personen, die regelmäßig Gäste einladen müssen (z. B. Projektleitung), die Rolle „Gasteinladender“ zu.
4. Kommunizieren Sie den neuen Ablauf für Gastanfragen an die Belegschaft.
5. Prüfen Sie mit einem normalen Konto, dass eine Gasteinladung in Teams oder Entra nicht mehr möglich ist.

Es gibt öffentliche Microsoft-365-Gruppen, denen jeder beitreten kann

Anforderung: Es gibt keine öffentlichen Microsoft-365-Gruppen, denen jeder beitreten kann



Gemessen am 19. Oktober 2026, 5 Uhr über Microsoft Graph, nur lesend.

Warum das wichtig ist

Öffentliche Microsoft-365-Gruppen und Teams kann jeder Mitarbeitende ohne Freigabe betreten und dann alle Dateien, Mails und Chats darin lesen. Oft ist das bei der Erstellung nicht bewusst gewählt worden, etwa bei Teams für Personal, Geschäftsführung oder Projekte mit Kundendaten.

Wo Sie die Einstellung finden: Microsoft 365 Admin Center (admin.microsoft.com) > Teams & Gruppen > Aktive Teams & Gruppen > [Gruppe] > Einstellungen > Datenschutz

Hinweis für die IT: Microsoft Graph PowerShell: `Get-MgGroup -Filter "groupTypes/any(c:c eq 'Unified')"` -All -Property `Id,DisplayName,Visibility` | ? `Visibility -eq 'Public'`; ändern mit `Update-MgGroup -GroupId <id> -Visibility Private`

BSI IT-Grundschutz	ORP.4.A2 Einrichtung, Änderung und Entzug von Berechtigungen
DSGVO	Art. 32 Abs. 1 lit. b
Secure Score	aad_managed_approved_public_groups_only
Benötigte Lizenz	Keine Zusatzlizenz erforderlich

So beheben Sie es

Öffentliche Gruppen und Teams auf „Privat“ umstellen

Microsoft-365-Gruppen und Teams werden auf „Privat“ gestellt, sofern kein bewusster Grund für eine öffentliche Gruppe besteht.

1. Öffnen Sie im Microsoft 365 Admin Center Teams & Gruppen > Aktive Teams & Gruppen und filtern Sie nach Datenschutz „Öffentlich“.
2. Klären Sie mit den Besitzern jeder Gruppe, ob der Inhalt wirklich für alle Mitarbeitenden gedacht ist.
3. Öffnen Sie bei nicht gewollten Fällen die Gruppe, wechseln Sie zu „Einstellungen“ und setzen Sie den Datenschutz auf „Privat“.
4. Prüfen Sie danach die Mitgliederliste: Personen, die zuvor beigetreten sind, bleiben Mitglied und müssen ggf. entfernt werden.
5. Legen Sie fest, dass neue Teams standardmäßig privat erstellt werden, und informieren Sie die Mitarbeitenden.

Anonyme Personen können Teams-Besprechungen beitreten

Anforderung: Anonyme Personen können Teams-Besprechungen nicht beitreten

Laut Microsoft Secure Score können anonyme Personen Teams-Besprechungen beitreten (0 % erfüllt).

Warum das wichtig ist

Anonyme Teilnehmende treten einer Teams-Besprechung ohne Anmeldung bei, also nur mit einem frei gewählten Namen. Wer den Besprechungslink hat, kann so unerkant zuhören. Ist anonymen Beitritt aus, müssen sich Externe mit einem Microsoft-Konto anmelden und sind damit erkennbar.

Wo Sie die Einstellung finden: Teams Admin Center (admin.teams.microsoft.com) > Besprechungen > Besprechungsrichtlinien > Global (organisationsweiter Standard) > „Besprechungsbeitritt & Wartebereich“

Hinweis für die IT: Teams PowerShell: Get-CsTeamsMeetingPolicy -Identity Global | fl AllowAnonymousUsersToJoinMeeting – erwartet False. Setzen: Set-CsTeamsMeetingPolicy -Identity Global -AllowAnonymousUsersToJoinMeeting \$false

BSI IT-Grundschutz	APP.5.4.A7 Regelungen für eine sichere Benutzung der UCC-Dienste
DSGVO	Art. 32 Abs. 1 lit. b
Secure Score	meeting_restrictanonymoujoin_v1
Benötigte Lizenz	Keine Zusatzlizenz erforderlich

So beheben Sie es

Anonymen Beitritt zu Teams-Besprechungen abschalten

Deaktivieren Sie in der globalen Teams-Besprechungsrichtlinie den Beitritt anonymer Personen.

1. Klären Sie vorab, ob Kunden ohne Microsoft-Konto regelmäßig an Ihren Besprechungen teilnehmen. Dann ggf. nur für einzelne Gruppen eine eigene Richtlinie mit anonymem Beitritt plus Lobby nutzen.
2. Öffnen Sie im Teams Admin Center Besprechungen > Besprechungsrichtlinien > Global (organisationsweiter Standard).
3. Schalten Sie unter „Besprechungsbeitritt & Wartebereich“ die Option „Anonyme Benutzer können an einer Besprechung teilnehmen“ aus und speichern Sie.
4. Prüfen Sie weitere eigene Besprechungsrichtlinien auf dieselbe Einstellung.
5. Testen Sie mit einem privaten Browserfenster ohne Anmeldung, dass ein Beitritt nicht mehr möglich ist. Microsoft Secure Score übernimmt die Änderung meist nach 24–48 Stunden.

Schweregrad gering, 6 Befunde

MFA- und SSPR-Einstellungen sind nicht in die zentrale Richtlinie migriert

Anforderung: Die MFA- und SSPR-Einstellungen sind in die zentrale Richtlinie für Authentifizierungsmethoden migriert

Die Migration der MFA- und SSPR-Einstellungen in die zentrale Richtlinie ist nicht abgeschlossen (Status: migrationInProgress).

Warum das wichtig ist

Microsoft hat die alten, getrennten Einstellungen für MFA und Self-Service-Kennwörterücksetzung (SSPR) abgekündigt. Solange die Migration nicht abgeschlossen ist, gelten alte und neue Einstellungen parallel. Dadurch bleiben schwache Methoden wie SMS oft unbemerkt erlaubt, obwohl sie in der neuen Richtlinie bereits abgeschaltet sind.

Wo Sie die Einstellung finden: Microsoft Entra Admin Center (entra.microsoft.com) > Entra ID > Authentifizierungsmethoden > Richtlinien > „Migration verwalten“

Hinweis für die IT: Microsoft Graph PowerShell: (Get-MgPolicyAuthenticationMethodPolicy).PolicyMigrationState – erwartet wird „migrationComplete“. Graph: GET /v1.0/policies/authenticationMethodsPolicy.

SCuBA (CISA)	MS.AAD.3.4v1 Migration der Authentifizierungsmethoden abgeschlossen
BSI IT-Grundschutz	ORP.4.A12 Entwicklung eines Authentisierungskonzeptes für IT-Systeme und Anwendungen
DSGVO	Art. 32 Abs. 1 lit. b
Benötigte Lizenz	Keine Zusatzlizenz erforderlich

So beheben Sie es

MFA- und SSPR-Einstellungen in die zentrale Richtlinie migrieren

Übertragen Sie die alten MFA- und SSPR-Einstellungen in die zentrale Richtlinie für Authentifizierungsmethoden und setzen Sie den Status auf „Migration abgeschlossen“.

1. Dokumentieren Sie die Altrichtlinien: Entra ID > Benutzer > „Per-user MFA“ > Dienstinstellungen sowie Entra ID > Benutzer > Kennwörterücksetzung > Authentifizierungsmethoden.
2. Öffnen Sie Entra ID > Authentifizierungsmethoden > Richtlinien und starten Sie den Migrationsassistenten oder wählen Sie „Migration verwalten“ > „Migration wird ausgeführt“.
3. Aktivieren Sie in der neuen Richtlinie die benötigten Methoden (Microsoft Authenticator, Passkeys, ggf. Befristeter Zugriffspass). SMS und Anruf nur für eine kleine Ausnahmegruppe zulassen.
4. Testen Sie mit einigen Pilotkonten Anmeldung und Kennwörterücksetzung, bevor Sie die Methoden in den Altrichtlinien abschalten.

5. Setzen Sie unter „Migration verwalten“ den Status auf „Migration abgeschlossen“. Ab dann gilt nur noch die neue Richtlinie (Sicherheitsfragen bleiben in SSPR).
6. Bei Problemen können Sie den Status jederzeit auf „Migration wird ausgeführt“ zurücksetzen.

 **Handlungsbedarf**, Schweregrad gering

Pos. 60, AS-AP-004

Mitarbeitende können ihr Firmenkonto mit LinkedIn verbinden

Anforderung: Mitarbeiter können ihr Firmenkonto nicht mit LinkedIn verbinden

Laut Microsoft Secure Score können Beschäftigte ihr Firmenkonto mit LinkedIn verbinden (0 % erfüllt).

Warum das wichtig ist

Mitarbeitende können ihr Firmenkonto mit ihrem LinkedIn-Profil verknüpfen. Dann sieht LinkedIn Kontakte und Informationen aus Microsoft 365 und umgekehrt. Firmendaten fließen damit in ein privates Netzwerk, ohne dass das Unternehmen darüber entscheidet.

Wo Sie die Einstellung finden: Microsoft Entra Admin Center (entra.microsoft.com) > Entra ID > Benutzer > Benutzereinstellungen > LinkedIn-Kontoverbindungen

Hinweis für die IT: Microsoft Graph: ``GET /security/secureScores?$top=1`` – Kontrolle ``aad_linkedin_connection_disables`` zeigt den Status. Der Secure Score wird etwa täglich aktualisiert.

BSI IT-Grundschutz	APP.6.A4 Regelung für die Installation und Konfiguration von Software
DSGVO	Art. 32 Abs. 1 lit. b
Secure Score	<code>aad_linkedin_connection_disables</code>
Benötigte Lizenz	Keine Zusatzlizenz erforderlich

So beheben Sie es

Verknüpfung von Firmenkonten mit LinkedIn abschalten

Deaktivieren Sie die Verknüpfung von Firmenkonten mit LinkedIn-Konten.

1. Öffnen Sie Entra ID > Benutzer > Benutzereinstellungen.
2. Setzen Sie „LinkedIn-Kontoverbindungen“ auf „Nein“ und speichern Sie.
3. Bereits bestehende Verknüpfungen werden damit nicht mehr genutzt; informieren Sie betroffene Mitarbeitende kurz.
4. Prüfen Sie nach einigen Tagen im Microsoft Secure Score, dass die Empfehlung zu LinkedIn-Verbindungen als erledigt angezeigt wird.

 **Handlungsbedarf**, Schweregrad gering

Pos. 59, AS-GE-001

Mitarbeitende können BitLocker-Wiederherstellungsschlüssel selbst auslesen

Anforderung: Mitarbeiter können BitLocker-Wiederherstellungsschlüssel nicht selbst auslesen

Mitarbeiter können die BitLocker-Wiederherstellungsschlüssel ihrer eigenen Geräte selbst abrufen.

Warum das wichtig ist

BitLocker verschlüsselt die Festplatten Ihrer Windows-Geräte. Der Wiederherstellungsschlüssel ist der Generalschlüssel dafür. Können Mitarbeitende ihn selbst im Portal abrufen, kann das auch jeder, der ihr Konto übernommen hat. Die Ausgabe sollte deshalb über die IT laufen.

Wo Sie die Einstellung finden: Microsoft Entra Admin Center (entra.microsoft.com) > Entra ID > Geräte > Geräteeinstellungen > „Restrict users from recovering the BitLocker key(s) for their owned devices“

Hinweis für die IT: Microsoft Graph PowerShell: ``(Get-MgPolicyAuthorizationPolicy).DefaultUserRolePermissions.AllowedToReadBitlockerKeysForOwnedDevice`` – Sollwert: False.

BSI IT-Grundschutz	ORP.4.A2 Einrichtung, Änderung und Entzug von Berechtigungen
DSGVO	Art. 32 Abs. 1 lit. b
Benötigte Lizenz	Keine Zusatzlizenz erforderlich

So beheben Sie es

Selbstabruf von BitLocker-Schlüsseln sperren

Hindern Sie Benutzer daran, BitLocker-Wiederherstellungsschlüssel ihrer eigenen Geräte selbst abzurufen.

1. Öffnen Sie Entra ID > Geräte > Geräteeinstellungen.
2. Setzen Sie „Benutzer daran hindern, die BitLocker-Schlüssel für ihre eigenen Geräte wiederherzustellen“ (Restrict users from recovering the BitLocker key(s) ...) auf „Ja“ und speichern Sie.
3. Legen Sie einen Ablauf fest, wie Mitarbeitende im Notfall den Schlüssel von der IT erhalten (z. B. telefonisch mit Rückruf zur Identitätsprüfung).
4. Prüfen Sie mit einem normalen Konto unter `myaccount.microsoft.com` > Geräte, dass kein Schlüssel mehr angezeigt wird.

Alle Mitarbeitenden dürfen Microsoft-365-Gruppen und Teams anlegen

Anforderung: Nur ausgewählte Personen dürfen Microsoft-365-Gruppen und Teams anlegen

Jeder Mitarbeiter darf Microsoft-365-Gruppen und Teams anlegen (Microsoft-Standard).

Warum das wichtig ist

Standardmäßig darf jeder Mitarbeitende neue Teams und Microsoft-365-Gruppen anlegen. In der Praxis entstehen so viele verwaiste Teams mit unklaren Besitzern und Berechtigungen. Eine kleine, berechtigte Gruppe von Personen sorgt für Ordnung und Übersicht.

Wo Sie die Einstellung finden: Microsoft Entra Admin Center (entra.microsoft.com) > Entra ID > Gruppen > Einstellungen > Allgemein; Ausnahmegruppe nur per Microsoft Graph PowerShell (Verzeichniseinstellung „Group.Unified“)

Hinweis für die IT: Microsoft Graph PowerShell: (Get-MgBetaDirectorySetting | ? DisplayName -eq 'Group.Unified').Values | ? Name -in 'EnableGroupCreation','GroupCreationAllowedGroupId'

BSI IT-Grundschutz	ORP.4.A1 Regelung für die Einrichtung und Löschung von Benutzenden und Benutzendengruppen
DSGVO	Art. 32 Abs. 1 lit. b
Benötigte Lizenz	Keine Zusatzlizenz erforderlich

So beheben Sie es

Anlegen von Gruppen und Teams auf eine Sicherheitsgruppe beschränken

Das Anlegen von Microsoft-365-Gruppen und Teams wird auf Mitglieder einer festgelegten Sicherheitsgruppe beschränkt.

1. Legen Sie eine Sicherheitsgruppe an, z. B. „M365-Gruppenersteller“, und nehmen Sie die berechtigten Personen auf.
2. Setzen Sie per Graph PowerShell in der Verzeichniseinstellung „Group.Unified“ EnableGroupCreation auf „false“ und GroupCreationAllowedGroupId auf die ID dieser Gruppe (Microsoft-Skriptvorlage).
3. Alternativ ohne Ausnahmegruppe: Stellen Sie in Entra ID > Gruppen > Einstellungen > Allgemein „Benutzer können Microsoft 365-Gruppen ... erstellen“ auf „Nein“.
4. Testen Sie mit einem normalen Konto, dass in Teams „Team erstellen“ nicht mehr möglich ist, und mit einem Mitglied der Gruppe, dass es funktioniert.
5. Teilen Sie den Mitarbeitenden mit, wie sie künftig ein neues Team beantragen.

Es gibt keine dynamische Gruppe, die alle Gastkonten erfasst

Anforderung: Eine dynamische Gruppe fasst alle Gastkonten automatisch zusammen

Keine dynamische Gruppe für Gastkonten gefunden.

Warum das wichtig ist

Gäste wie externe Berater oder Partner erhalten oft Zugriff auf Teams und Dateien. Eine dynamische Gruppe sammelt automatisch alle Gastkonten. So lassen sich für Gäste gezielt Regeln festlegen und Zugriffe regelmäßig überprüfen, ohne Listen von Hand zu pflegen.

Wo Sie die Einstellung finden: Microsoft Entra Admin Center (entra.microsoft.com) > Entra ID > Gruppen > Alle Gruppen > Neue Gruppe

Hinweis für die IT: Microsoft Graph PowerShell: `Get-MgGroup -Filter "groupTypes/any(c:c eq 'DynamicMembership')"-All | ft DisplayName,MembershipRule` – Regel muss user.userType -eq Guest enthalten.

BSI IT-Grundschutz	ORP.4.A3 Dokumentation der Benutzendenkennungen und Rechteprofile
DSGVO	Art. 32 Abs. 1 lit. b
Benötigte Lizenz	Microsoft Entra ID P1 (enthalten z. B. in Microsoft 365 Business Premium, E3 und E5) oder Microsoft Entra ID P2 (enthalten z. B. in Microsoft 365 E5)

So beheben Sie es

Dynamische Gruppe für alle Gastkonten anlegen

Legen Sie eine dynamische Sicherheitsgruppe an, die automatisch alle Gastkonten enthält (erfordert Microsoft Entra ID P1).

1. Öffnen Sie Entra ID > Gruppen > Alle Gruppen > Neue Gruppe.
2. Wählen Sie Gruppentyp „Sicherheit“, einen klaren Namen (z. B. „Alle Gäste – dynamisch“) und Mitgliedschaftstyp „Dynamischer Benutzer“.
3. Fügen Sie unter „Dynamische Abfrage hinzufügen“ die Regel `(user.userType -eq "Guest")` ein.
4. Speichern Sie und prüfen Sie nach einigen Minuten, dass die Mitgliederliste alle Gäste enthält.
5. Nutzen Sie die Gruppe für Richtlinien (z. B. MFA für Gäste) und für regelmäßige Zugriffsüberprüfungen.

In Teams-Besprechungen darf jeder präsentieren

Anforderung: Nur Organisatoren und Mitorganisatoren dürfen in Teams-Besprechungen präsentieren

Laut Microsoft Secure Score darf in Teams-Besprechungen jeder Teilnehmer präsentieren (0 % erfüllt).

Warum das wichtig ist

Standardmäßig darf in Teams-Besprechungen jede teilnehmende Person ihren Bildschirm teilen. Das kann zu Störungen führen oder dazu, dass Externe unerwünschte Inhalte zeigen. Sind nur Organisatoren und Mitorganisatoren Präsentierende, behalten Sie die Kontrolle; weitere Personen lassen sich in der Besprechung bei Bedarf freischalten.

Wo Sie die Einstellung finden: Teams Admin Center (admin.teams.microsoft.com) > Besprechungen > Besprechungsrichtlinien > Global (organisationsweiter Standard) > „Inhaltsfreigabe“

Hinweis für die IT: Teams PowerShell: Get-CsTeamsMeetingPolicy -Identity Global | fl DesignatedPresenterRoleMode – erwartet OrganizerOnlyUserOverride. Setzen: Set-CsTeamsMeetingPolicy -Identity Global - DesignatedPresenterRoleMode OrganizerOnlyUserOverride

BSI IT-Grundschutz	APP.5.4.A7 Regelungen für eine sichere Benutzung der UCC-Dienste
DSGVO	Art. 32 Abs. 1 lit. b
Secure Score	meeting_designatedpresenter_v1
Benötigte Lizenz	Keine Zusatzlizenz erforderlich

So beheben Sie es

Präsentieren auf Organisatoren beschränken

Stellen Sie in der globalen Besprechungsrichtlinie ein, dass standardmäßig nur Organisatoren und Mitorganisatoren präsentieren dürfen.

1. Öffnen Sie im Teams Admin Center Besprechungen > Besprechungsrichtlinien > Global (organisationsweiter Standard).
2. Setzen Sie unter „Inhaltsfreigabe“ die Option „Wer präsentieren kann“ auf Organisatoren und Mitorganisatoren (engl. „Only organizers and co-organizers“) und speichern Sie.
3. Prüfen Sie weitere Besprechungsrichtlinien auf dieselbe Einstellung.
4. Informieren Sie die Mitarbeitenden, dass sie in den Besprechungsoptionen einzelnen Personen die Präsentationsrolle geben können.
5. Testen Sie in einer neuen Besprechung, dass Teilnehmende ohne Rolle nicht teilen können. Secure Score übernimmt die Änderung nach 24–48 Stunden.

SCuBA-Baselines (CISA)

Alle ausgewerteten Prüfungen, geordnet nach den Microsoft-365-Sicherheitsbaselines der US-Behörde CISA (SCuBA, Version 2.0.0); Prüfungen ohne entsprechende SCuBA-Richtlinie stehen am Ende. Die Zuordnung stammt von Auditspiegel. Die Positionsnummer (Pos.) verweist aus den folgenden Sichten hierher.

Pos.	SCuBA	Prüfpunkt	Bewertung
Microsoft Entra ID (MS.AAD)			
1	MS.AAD.1.1v1	Bedingter Zugriff blockiert veraltete Authentifizierung für alle Benutzer	● Bestanden
2	MS.AAD.1.1v1	Veraltete Anmeldeprotokolle (POP, IMAP, SMTP-Auth) sind tenantweit gesperrt	● Bestanden
3	MS.AAD.2.1v1	Konten mit hohem Kompromittierungsrisiko müssen ihr Kennwort ändern oder werden gesperrt	⚠ Lizenz fehlt
4	MS.AAD.2.3v1	Risikante Anmeldungen werden per Richtlinie zur Multifaktor-Anmeldung gezwungen oder blockiert	⚠ Lizenz fehlt
5	MS.AAD.3.1v1	Bedingter Zugriff verlangt von allen Benutzern eine phishing-resistente Anmeldung (Passkey, Windows Hello, Zertifikat)	⚠ Handlungsbedarf
6	MS.AAD.3.2v2	Bedingter Zugriff verlangt Multifaktor für alle Administratoren	● Bestanden
7	MS.AAD.3.2v2	Bedingter Zugriff verlangt Multifaktor für alle Benutzer und alle Anwendungen	● Bestanden
8	MS.AAD.3.2v2	Gastbenutzer müssen sich mit Multifaktor anmelden	⚠ Handlungsbedarf
9	MS.AAD.3.2v2	Jeder Benutzer muss sich mit Multifaktor anmelden (Sicherheitsstandards oder bedingter Zugriff)	● Bestanden

Pos.	SCuBA	Prüfpunkt	Bewertung
10	MS.AAD.3.3v2	Microsoft Authenticator zeigt App-Name und Standort an (Schutz vor MFA-Ermüdungsangriffen)	⚠ Handlungsbedarf
11	MS.AAD.3.4v1	Die MFA- und SSPR-Einstellungen sind in die zentrale Richtlinie für Authentifizierungsmethoden migriert	⚠ Handlungsbedarf
12	MS.AAD.3.5v2	Die Anmeldemethode SMS ist deaktiviert	⚠ Handlungsbedarf
13	MS.AAD.3.5v2	Die schwachen Methoden Sprachanruf und E-Mail-Einmalcode sind deaktiviert	● Bestanden
14	MS.AAD.3.6v1	Administratoren müssen sich phishing-resistent anmelden (Passkey, Windows Hello, Zertifikat)	⚠ Handlungsbedarf
15	MS.AAD.3.7v1	Bedingter Zugriff erlaubt die Anmeldung nur von verwalteten Geräten	⚠ Handlungsbedarf
16	MS.AAD.3.8v1	Das Registrieren neuer Sicherheitsinformationen (MFA-Methoden) ist durch bedingten Zugriff geschützt	⚠ Handlungsbedarf
17	MS.AAD.3.9v1	Die Geräte-Code-Anmeldung (beliebtes Phishing-Werkzeug) ist blockiert	⚠ Handlungsbedarf
18	MS.AAD.5.1v1	Mitarbeiter dürfen keine eigenen App-Registrierungen anlegen	⚠ Handlungsbedarf
19	MS.AAD.5.2v1	Mitarbeiter können Drittanbieter-Apps keinen Zugriff auf Firmendaten erteilen	● Bestanden
20	MS.AAD.5.3v1	Der Admin-Zustimmungs-Workflow für App-Anfragen ist aktiviert	● Bestanden
21	MS.AAD.6.1v1	Kennwörter laufen auf keiner verifizierten Domain zwangsweise ab	● Bestanden
22	MS.AAD.7.1v1	Zwischen zwei und vier Globale Administratoren sind benannt	⚠ Handlungsbedarf
23	MS.AAD.7.3v1	Globale Administratoren sind reine Cloud-Konten (nicht aus dem lokalen AD synchronisiert)	▲ Kritisch
24	MS.AAD.7.4v1 MS.AAD.7.5v1	Administratorrechte werden über Privileged Identity Management nur bei Bedarf vergeben	⚠ Lizenz fehlt
25	MS.AAD.7.6v1	Die Aktivierung der Rolle „Globaler Administrator“ muss von einer zweiten Person genehmigt werden	⚠ Lizenz fehlt
26	MS.AAD.7.7v1	Neue Zuweisungen hoch privilegierter Rollen werden per E-Mail an eine festgelegte Adresse gemeldet	⚠ Lizenz fehlt
27	MS.AAD.7.8v1	Jede Aktivierung der Rolle „Globaler Administrator“ wird per E-Mail an eine festgelegte Adresse gemeldet	⚠ Lizenz fehlt
28	MS.AAD.7.9v1	Aktivierungen weiterer hoch privilegierter Rollen werden per E-Mail an eine festgelegte Adresse gemeldet	⚠ Lizenz fehlt
29	MS.AAD.8.1v1	Gastbenutzer haben nur eingeschränkten Lesezugriff auf das Verzeichnis	● Bestanden
30	MS.AAD.8.2v1	Nur Administratoren und Gasteinladende dürfen Gäste einladen	⚠ Handlungsbedarf
Security Suite (Defender for Office 365 und Purview) (MS.SECURITYSUITE)			
31	MS.SECURITYSUITE.3.1v1	Richtlinien zur Verhinderung von Datenverlust (DLP) sind aktiv	⚠ Handlungsbedarf
32	MS.SECURITYSUITE.3.2v1	DLP-Richtlinien schützen auch Chats und Kanäle in Microsoft Teams	⚠ Handlungsbedarf
33	MS.SECURITYSUITE.5.1v1	Die Microsoft-365-Überwachungsprotokollierung (Audit-Log) ist eingeschaltet	● Bestanden
34	MS.SECURITYSUITE.5.2v1	Die Aufbewahrungsdauer der Anmelde- und Audit-Protokolle reicht für eine Vorfallaufklärung aus	⚠ Nicht messbar
SharePoint Online und OneDrive (MS.SHAREPOINT)			
35	MS.SHAREPOINT.1.1v1	Externe Freigaben in SharePoint sind höchstens an bereits vorhandene Gäste möglich	⚠ Handlungsbedarf

Pos.	SCuBA	Prüfpunkt	Bewertung
36	MS.SHAREPOINT.1.3v1	Externe Freigaben sind auf eine Liste erlaubter Partnerdomains beschränkt	⚠ Handlungsbedarf
Microsoft Teams (MS.TEAMS)			
37	MS.TEAMS.1.1v1	Externe Teilnehmer können in Teams-Besprechungen keine Bildschirmsteuerung übernehmen	● Bestanden
38	MS.TEAMS.1.2v2	Anonyme Personen können keine Teams-Besprechungen starten	● Bestanden
Ergänzende Prüfungen ohne entsprechende SCuBA-Richtlinie			
39		Administratoren müssen sich regelmäßig neu anmelden; Browsersitzungen bleiben nicht dauerhaft bestehen	● Bestanden
40		Administratorkonten haben keine Lizenz mit E-Mail, SharePoint oder Teams (getrennte Admin-Konten)	● Bestanden
41		Alle Administratoren haben eine Multifaktor-Methode registriert	⚠ Handlungsbedarf
42		Alle Mitarbeiterkonten sind MFA-fähig (starke Methode registriert und zugelassen)	⚠ Handlungsbedarf
43		Anonyme Personen können Teams-Besprechungen nicht beitreten	⚠ Handlungsbedarf
44		Bei Synchronisation aus dem lokalen AD ist die Kennwort-Hash-Synchronisierung aktiv	● Bestanden
45		Benutzer ohne starke MFA-Methode werden bei der Anmeldung zur Registrierung aufgefordert	● Bestanden
46		Customer Lockbox ist aktiv — Microsoft-Support greift nur nach Ihrer Freigabe auf Daten zu	⚙ Nicht messbar
47		Der Kennwortschutz gilt auch für das lokale Active Directory (Modus „Erzwungen“)	● Bestanden
48		Der Tenant ist für Microsoft Entra ID P1 (inkl. MFA Premium) lizenziert	● Bestanden
49		Eine dynamische Gruppe fasst alle Gastkonten automatisch zusammen	⚠ Handlungsbedarf
50		Eine eigene Liste gesperrter Kennwörter (z. B. Firmenname) ist aktiv	⚠ Handlungsbedarf
51		Es gibt keine öffentlichen Microsoft-365-Gruppen, denen jeder beitreten kann	⚠ Handlungsbedarf
52		Es gibt zwei erkennbare Notfallzugangs-Konten (Break-Glass) mit Globaler-Administrator-Rolle	⚠ Handlungsbedarf
53		Fremde Personen können sich nicht per E-Mail-Bestätigung selbst in Ihren Tenant registrieren	● Bestanden
54		Gäste dürfen Dateien, die ihnen nicht gehören, nicht weiterteilen	⚠ Handlungsbedarf
55		Inaktive Sitzungen in SharePoint und OneDrive werden automatisch abgemeldet	⚠ Handlungsbedarf
56		Microsoft Authenticator ist als Anmeldemethode freigegeben	● Bestanden
57		Microsoft Forms prüft Formulare automatisch auf Phishing	● Bestanden
58		Mindestens 95 % aller Benutzer haben eine Multifaktor-Methode registriert	▲ Kritisch
59		Mitarbeiter können BitLocker-Wiederherstellungsschlüssel nicht selbst auslesen	⚠ Handlungsbedarf
60		Mitarbeiter können ihr Firmenkonto nicht mit LinkedIn verbinden	⚠ Handlungsbedarf
61		Mitarbeiter können keine eigenen Apps, Testversionen oder Dienste in Microsoft 365 aktivieren	⚠ Handlungsbedarf

Pos.	SCuBA	Prüfpunkt	Bewertung
62		Mitarbeiter ohne Adminrolle dürfen keine neuen Microsoft-Entra-Tenants anlegen	● Bestanden
63		Mitarbeiter ohne Adminrolle dürfen keine Sicherheitsgruppen anlegen	● Bestanden
64		Nur ausgewählte Personen dürfen Microsoft-365-Gruppen und Teams anlegen	△ Handlungsbedarf
65		Nur Organisatoren und Mitorganisatoren dürfen in Teams-Besprechungen präsentieren	△ Handlungsbedarf
66		OneDrive synchronisiert nur auf firmeneigene (domänenverbundene) Geräte	△ Handlungsbedarf
67		Phishing-resistente Anmeldung mit Passkeys (FIDO2) ist freigegeben	△ Handlungsbedarf
68		Self-Service-Kennwortzurücksetzung ist für alle Mitarbeiter freigeschaltet	● Bestanden
69		SharePoint akzeptiert keine veralteten Anmeldeprotokolle	● Bestanden
70		SharePoint erlaubt keine anonymen „Jeder mit dem Link“-Freigaben	▲ Kritisch
71		Sway-Präsentationen können nicht mit Personen außerhalb Ihrer Organisation geteilt werden	● Bestanden
72		Vertraulichkeitsbezeichnungen (z. B. „Intern“, „Vertraulich“) sind veröffentlicht	△ Handlungsbedarf
73		Zugriff auf Azure-Verwaltungsportale erfordert Multifaktor	● Bestanden

BSI Grundschutz

Bezug der Prüfungen zu Anforderungen des BSI IT-Grundschutz-Kompendiums (Edition 2023). Eine Prüfung kann mehrere Anforderungen berühren.

Anforderung	Ergebnis	Prüfungen (Pos.)
APP.5.3.A2 Sicherer Betrieb von E-Mail-Servern	● 1	● 2
APP.5.4.A5 Rollen- und Berechtigungskonzept für UCC	● 1	● 37
APP.5.4.A7 Regelungen für eine sichere Benutzung der UCC-Dienste	△ 2 ● 1	● 38 △ 43 △ 65
APP.6.A4 Regelung für die Installation und Konfiguration von Software	△ 3	△ 18 △ 60 △ 61
CON.9.A1 Festlegung zulässiger Empfangender	▲ 1 △ 3 ● 1	△ 35 △ 36 △ 54 ▲ 70 ● 71
CON.9.A2 Regelung des Informationsaustausches	△ 3	△ 31 △ 32 △ 72
DER.1.A5 Einsatz von mitgelieferten Systemfunktionen zur Detektion	⊖ 4	⊖ 4 ⊖ 26 ⊖ 27 ⊖ 28
OPS.1.1.2.A6 Schutz administrativer Tätigkeiten	▲ 1 ● 1	▲ 23 ● 39
OPS.1.1.2.A16 Erweiterte Sicherheitsmaßnahmen für Administrationszugänge	● 1	● 73
OPS.1.1.2.A17 IT-Administration im Vier-Augen-Prinzip	⊖ 1	⊖ 25
OPS.1.1.2.A21 Regelung der IT-Administrationsrollen	△ 1 ⊖ 1	△ 22 ⊖ 24
OPS.1.1.2.A22 Trennung von administrativen und anderen Tätigkeiten	▲ 1 ● 1	▲ 23 ● 40
OPS.1.1.4.A2 Nutzung systemspezifischer Schutzmechanismen	● 1	● 57

Anforderung	Ergebnis	Prüfungen (Pos.)
OPS.1.1.5.A3 Konfiguration der Protokollierung auf System- und Netzebene	● 1	● 33
OPS.1.1.5.A8 Archivierung von Protokollierungsdaten	○ 1	○ 34
OPS.2.2.A1 Erstellung einer Strategie für die Cloud-Nutzung	● 1	● 62
OPS.2.2.A2 Erstellung einer Sicherheitsrichtlinie für die Cloud-Nutzung	○ 1	○ 46
ORP.4.A1 Regelung für die Einrichtung und Löschung von Benutzenden und Benutzendengruppen	△ 2 ● 2	△ 30 ● 53 ● 63 △ 64
ORP.4.A2 Einrichtung, Änderung und Entzug von Berechtigungen	△ 2 ● 3 ☹ 1	● 19 ● 20 ☹ 26 ● 29 △ 51 △ 59
ORP.4.A3 Dokumentation der Benutzendenkennungen und Rechteprofile	△ 1	△ 49
ORP.4.A8 Regelung des Passwortgebrauchs	△ 1 ● 1	● 47 △ 50
ORP.4.A10 Schutz von Benutzendenkennungen mit weitreichenden Berechtigungen	△ 2 ● 1 ☹ 2	● 6 △ 14 ☹ 27 ☹ 28 △ 41
ORP.4.A11 Zurücksetzen von Passwörtern	● 1	● 68
ORP.4.A12 Entwicklung eines Authentisierungskonzeptes für IT-Systeme und Anwendungen	△ 1	△ 11
ORP.4.A13 Geeignete Auswahl von Authentisierungsmechanismen	△ 6 ● 5	● 1 ● 2 △ 5 △ 10 △ 12 ● 13 △ 16 △ 17 ● 56 △ 67 ● 69
ORP.4.A16 Richtlinien für die Zugriffs- und Zugangskontrolle	△ 1	△ 66
ORP.4.A17 Geeignete Auswahl von Identitäts- und Berechtigungsmanagement-Systemen	● 1	● 48
ORP.4.A20 Notfallvorsorge für das Identitäts- und Berechtigungsmanagement-System	△ 1 ● 1	● 44 △ 52
ORP.4.A21 Mehr-Faktor-Authentisierung	▲ 1 △ 3 ● 3	△ 5 ● 7 △ 8 ● 9 △ 42 ● 45 ▲ 58
ORP.4.A22 Regelung zur Passwortqualität	△ 1 ● 1	● 47 △ 50
ORP.4.A23 Regelung für passwortverarbeitende Anwendungen und IT-Systeme	● 2 ☹ 1	☹ 3 ● 21 ● 44
ORP.4.A24 Vier-Augen-Prinzip für administrative Tätigkeiten	☹ 1	☹ 25
SYS.2.1.A1 Sichere Authentisierung von Benutzenden	△ 1	△ 55
SYS.3.2.2.A4 Verteilung der Grundkonfiguration auf mobile Endgeräte	△ 1	△ 15

DSGVO Art. 32

Bezug der Prüfungen zu DSGVO Art. 32 Abs. 1 (Sicherheit der Verarbeitung).

Art. 32 Abs. 1	Ergebnis	Prüfungen (Pos.)
lit. a Pseudonymisierung und Verschlüsselung	△ 1	△ 72

Art. 32 Abs. 1	Ergebnis	Prüfungen (Pos.)
lit. b Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit	▲ 3 ▲ 33 ● 28 ☐ 7 ○ 2	● 1 ● 2 ☐ 3 ☐ 4 ▲ 5 ● 6 ● 7 ▲ 8 ● 9 ▲ 10 ▲ 11 ▲ 12 ● 13 ▲ 14 ▲ 15 ▲ 16 ▲ 17 ▲ 18 ● 19 ● 20 ● 21 ▲ 22 ▲ 23 ☐ 24 ☐ 25 ☐ 26 ☐ 27 ☐ 28 ● 29 ▲ 30 ▲ 31 ▲ 32 ● 33 ○ 34 ▲ 35 ▲ 36 ● 37 ● 38 ● 39 ● 40 ▲ 41 ▲ 42 ▲ 43 ● 44 ● 45 ○ 46 ● 47 ● 48 ▲ 49 ▲ 50 ▲ 51 ▲ 52 ● 53 ▲ 54 ▲ 55 ● 56 ● 57 ▲ 58 ▲ 59 ▲ 60 ▲ 61 ● 62 ● 63 ▲ 64 ▲ 65 ▲ 66 ▲ 67 ● 68 ● 69 ▲ 70 ● 71 ▲ 72 ● 73
lit. c Wiederherstellbarkeit nach Zwischenfall	▲ 1 ● 1	● 44 ▲ 52

Secure Score

Prüfungen, die einer Kontrolle des Microsoft Secure Score entsprechen, nach Kategorie.

Kontrolle	Ergebnis	Prüfungen (Pos.)
Kategorie Apps		
Keine Benutzer-Zustimmung zu Apps 4 von 4 Punkten erreicht	● 1	● 19
Kategorie Data		
Externe Freigabe über Domainliste steuern 0 von 2 Punkten erreicht	▲ 1	▲ 36
Kategorie Identity		
MFA für alle Administratoren 40 von 40 Punkten erreicht	▲ 1 ● 1	● 6 ▲ 41
Legacy-Authentifizierung blockieren 30 von 30 Punkten erreicht	● 2	● 1 ● 2
MFA für alle Benutzer 7 von 9 Punkten erreicht	▲ 1 ▲ 1 ● 1	● 7 ▲ 42 ▲ 58
Selbstständiges Zurücksetzen von Kennwörtern 20 von 20 Punkten erreicht	● 1	● 68
Ohne Wert im Secure-Score-Abruf dieses Scans		
aad_admin_accounts_separate_unassigned_cloud_o nly	▲ 1 ● 1	▲ 23 ● 40
aad_admin_consent_workflow	● 1	● 20
aad_custom_banned_passwords	▲ 1	▲ 50
aad_limited_administrative_roles	● 1	● 73
aad_linkedin_connection_disables	▲ 1	▲ 60
aad_managed_approved_public_groups_only	▲ 1	▲ 51
aad_password_protection	● 1	● 47
aad_phishing_MFA_strength	▲ 1	▲ 14
aad_sign_in_freq_session_timeout	● 1	● 39
aad_third_party_apps	▲ 1	▲ 18
admincenter_owned_apps_and_services	▲ 1	▲ 61

Kontrolle	Ergebnis	Prüfungen (Pos.)
CustomerLockBoxEnabled	 1	 46
dlp_datalossprevention	 1	 31
forms_phishing_protection	 1	 57
meeting_anonymousstartmeeting_v1	 1	 38
meeting_designatedpresenter_v1	 1	 65
meeting_externalrequestcontrol_v1	 1	 37
meeting_restrictanonymousjoin_v1	 1	 43
mip_DLP_policies_Teams	 1	 32
mip_search_auditlog	 1	 33
mip_sensitivitylabelspolicies	 1	 72
OneAdmin	 1	 22
PasswordHashSync	 1	 44
PWAgePolicyNew	 1	 21
SigninRiskPolicy	 1	 4
spo_block_onedrive_sync_unmanaged_devices	 1	 66
spo_external_users_sharing	 1	 54
spo_idle_session_timeout	 1	 55
spo_legacy_auth	 1	 69
sway_block_sharing_with_outside_users	 1	 71
UserRiskPolicy	 1	 3

Über diesen Bericht

Dies ist eine technische Konfigurationsprüfung mit Bezug zu den SCuBA-Baselines der CISA, BSI Grundschatz und DSGVO Art. 32. Es handelt sich nicht um ein vollständiges Sicherheits-Audit und nicht um eine ISO-27001-Zertifizierung. Die Empfehlungen ersetzen keine individuelle rechtliche oder sicherheitstechnische Beratung.

Methodik

Auditspiegel prüft technisch lesbare Konfigurationseinstellungen Ihres Microsoft-365-Tenants über Microsoft Graph, nur lesend und mit einer App-Anmeldung ohne Benutzerkennwort. Jede Prüfung trägt die benötigte Microsoft-365-Lizenz als Merkmal; fehlt sie, zählt die Prüfung nie als bestanden und steht im Abschnitt „Was wir nicht geprüft haben“. Welche Einstellungen geprüft und wie sie bewertet werden, legt Auditspiegel fest. Die Bezüge zu den Microsoft-365-Sicherheitsbaselines der US-Behörde CISA (SCuBA, Version 2.0.0), zu Anforderungen des BSI IT-Grundschatz-Kompendiums (Edition 2023) und zu DSGVO Art. 32 Abs. 1 lit. a–d sind Zuordnungen von Auditspiegel.

Quellen

Die Secure Configuration Baselines für Microsoft 365 veröffentlicht die US-Behörde CISA im Projekt SCuBA (Secure Cloud Business Applications) unter CC0 1.0, gemeinfrei: github.com/cisagov/ScubaGear, Version 2.0.0. Auditspiegel ist ein unabhängiges Angebot; CISA hat diesen Bericht weder geprüft noch bestätigt und empfiehlt keine kommerziellen Produkte.

Datenschutz

Erstellt auf Servern in Deutschland (Hetzner, Rechenzentren Falkenstein und Nürnberg). Gelesen wurden ausschließlich Konfigurationsdaten; Inhalte aus Postfächern, SharePoint-Sites oder OneDrive-Ordern Ihres Tenants hat Auditspiegel zu keinem Zeitpunkt verarbeitet. Grundlage ist die Auftragsverarbeitungsvereinbarung (AVV) gemäß Art. 28 DSGVO.

Auftragsverarbeitungsvereinbarung (AVV)

Die Auftragsverarbeitungsvereinbarung (AVV) zwischen Auditspiegel und Ihrem Unternehmen haben Sie in Ihrem Konto elektronisch abgeschlossen; Text und Annahme-Verlauf finden Sie dort jederzeit. Bei Fragen oder Änderungswünschen wenden Sie sich an die Adresse unten.

Angaben zum Bericht

Art der Prüfung	Technische Konfigurationsprüfung des Microsoft-365-Tenants
Prüfgegenstand	Demo GmbH — Microsoft 365
Prüfzeitpunkt	19. Oktober 2026, 5 Uhr
Scan-ID	00000000-0000-0000-0000-0000000d3e12

Herausgeber

Auditspiegel, ein Angebot von Gläser IT-Solutions, Inhaber Daniel Gläser
Georgstrasse 46 · 09111 Chemnitz
Einzelunternehmen — keine Handelsregistereintragung
USt-IdNr: DE409251798