Microsoft 365 Security Check, Kurzreport

Musterfirma GmbH

20.10.2026

Geprüft wurden die Einstellungen Ihres Microsoft 365 anhand anerkannter Sicherheitsstandards: Anmeldung und Konten, Admin-Rechte, Gastzugänge, App-Berechtigungen und Zugriffsregeln im Microsoft Entra Admin Center, dazu ausgewählte Einstellungen für E-Mail und Teams. Der Bericht zeigt, was schon gut eingestellt ist und welche empfohlenen Einstellungen noch offen sind, sortiert nach Dringlichkeit und mit dem Portal, in dem Sie sie finden.

80	60	20
Prüfpunkte geprüft	in Ordnung	offen, 15 hoch und 5 mittel



Hoch: typisches Einfallstor, zeitnah umsetzen. Mittel: sinnvolle Verbesserung, einplanen. 595 weitere Prüfpunkte wurden nicht bewertet, warum, steht am Ende des Berichts.

Offene Einstellungen

Hoch — MFA ist nicht für alle Benutzer verpflichtend
Anmeldung und Konten, Microsoft Entra Admin Center, CISA.MS.AAD.3.2

Hoch — Admins melden sich ohne phishing-resistente MFA an
Anmeldung und Konten, Microsoft Entra Admin Center, CISA.MS.AAD.3.6

Hoch — Gruppenbesitzer dürfen Apps Zugriff auf Daten erteilen
Anmeldung und Konten, Microsoft Entra Admin Center, CISA.MS.AAD.5.4

Offene Einstellungen, Fortsetzung

Hoch	Kennwörter laufen regelmäßig ab	Anmeldung und Konten, Microsoft Entra Admin Center, CISA.MS.AAD.6.1
Hoch	Admin-Rollen sind dauerhaft aktiv statt nur bei Bedarf	Anmeldung und Konten, Microsoft Entra Admin Center, CISA.MS.AAD.7.4
Hoch	Anmeldung mit FIDO2-Sicherheitsschlüssel ist nicht aktiviert	Anmeldung und Konten, Microsoft Entra Admin Center, EIDSCA.AF01
Hoch	FIDO2-Schlüssel werden nicht auf Echtheit geprüft	Anmeldung und Konten, Microsoft Entra Admin Center, EIDSCA.AF03
Hoch	Kennwortschutz für das lokale Active Directory ist aus	Anmeldung und Konten, Microsoft Entra Admin Center, EIDSCA.PR02
Hoch	Ein synchronisiertes Konto hat eine dauerhafte Admin-Rolle	Anmeldung und Konten, Microsoft Entra Admin Center, MT.1026
Hoch	Veraltete Anmeldeverfahren sind nicht blockiert	Zugriffsregeln, Microsoft Entra Admin Center, CISA.MS.AAD.1.1
Hoch	Keine Zugriffsregel gilt für alle Apps	Zugriffsregeln, Microsoft Entra Admin Center, MT.1003
Hoch	Zugriffsregeln nehmen kein Notfallkonto aus	Zugriffsregeln, Microsoft Entra Admin Center, MT.1005
Hoch	Keine Zugriffsregel verlangt MFA für alle Benutzer	Zugriffsregeln, Microsoft Entra Admin Center, MT.1007
Hoch	Zugriffsregeln erfassen auch Synchronisierungskonten	Zugriffsregeln, Microsoft Entra Admin Center, MT.1020
Hoch	Benutzer- und Anmelderisiko sind nicht getrennt geregelt	Zugriffsregeln, Microsoft Entra Admin Center, MT.1049

Mittel

Globale Admins werden beim Geräte-Beitritt lokale Admins

Admin-Konten, Microsoft Entra Admin Center, MT.1090

Mittel

Authenticator zeigt bei der Anmeldung keinen Kontext an

Anmeldung und Konten, Microsoft Entra Admin Center, CISA.MS.AAD.3.3

Mittel

Telefon-Teilnehmer umgehen den Wartebereich in Teams

Teams-Besprechungen, Microsoft Teams Admin Center, MT.1042

Mittel

Anonyme Personen dürfen Teams-Besprechungen starten

Teams-Besprechungen, Microsoft Teams Admin Center, MT.1047

Mittel

Microsoft-365-Gruppen laufen nicht automatisch ab

Gruppen, Microsoft Entra Admin Center, MT.1058

Die Kennungen stammen aus internationalen Sicherheitsstandards (u. a. CIS und CISA). Was sie für Ihr Unternehmen bedeuten, erkläre ich Ihnen gern im Gespräch.

Bereits gut eingestellt (60)

CIS.M365.1.3.1 CIS.M365.1.3.3 CISA.MS.AAD.5.1 CISA.MS.AAD.5.2 CISA.MS.AAD.7.6 CISA.MS.AAD.7.8 CISA.MS.AAD.8.1 CISA.MS.AAD.8.2 CISA.MS.AAD.8.3 EIDSCA.AF02 EIDSCA.AF04 EIDSCA.AG01 EIDSCA.AG02 EIDSCA.AG03 EIDSCA.AM04 EIDSCA.AM06 EIDSCA.AM07 EIDSCA.AP05 EIDSCA.AP10 EIDSCA.AP14 EIDSCA.AS04 EIDSCA.AT01 EIDSCA.AV01 EIDSCA.CP01 EIDSCA.CR03 EIDSCA.CR04 EIDSCA.PR01 EIDSCA.ST09 MT.1001 MT.1006 MT.1008 MT.1013 MT.1016 MT.1017 MT.1021 MT.1022 MT.1025 MT.1029 MT.1031 MT.1032 MT.1036 MT.1037 MT.1045 MT.1051 MT.1053 MT.1054 MT.1062 MT.1063 MT.1064 MT.1065 MT.1069 MT.1071 MT.1073 MT.1078 MT.1080 MT.1081 MT.1092 MT.1096 MT.1097 MT.1099

Nicht bewertet (595)

58

Nicht in Ihrer Lizenz enthalten

Ob sich ein Upgrade lohnt oder Sie zu viel zahlen, zeigt der kostenlose Lizenz-Check.

196

Nicht im Umfang des kostenlosen Checks

Einstellungen einzelner Dienste wie Exchange Online oder Teams. Im Detail-Check sehe ich sie mir gern an.

341

Für Ihre Umgebung nicht anwendbar

Diese Prüfungen betreffen Konstellationen, die bei Ihnen nicht vorkommen.

Wie es weitergeht

20 offene Einstellungen. Sie entscheiden, wer sie umsetzt.

Umsetzen lassen

Ich setze die Empfehlungen um und dokumentiere jede Änderung. Festpreis, Angebot vorab.

Selbst umsetzen

Wenn Sie möchten, prüfe ich danach auf Anfrage noch einmal.

Kostenloses Erstgespräch: kontakt@kmitt-consulting.de

Erstellt von KMITT Consulting, kontakt@kmitt-consulting.de. Grundlage ist das Open-Source-Framework Maester (MIT-Lizenz). Der Bericht ist eine Momentaufnahme und keine Garantie für Sicherheit. Ausführliche Berichte mit personenbezogenen Daten löschen wir nach 30 Tagen automatisch. Den Kurzbericht und die Kennzahlen ohne Personennamen bewahren wir für Folgeprüfungen auf, auf Wunsch löschen wir alle Daten zu Ihrem Unternehmen.