

CHECKLISTE · TOMORIS TOOLBOX

MFA in Microsoft 365 einführen: Checkliste für den Rollout ohne Aussperren

Acht Schritte von der Ausgangslage bis zur Kontrolle, nach Microsoft Learn, CISA und BSI, mit den Phasen der verpflichtenden MFA für Azure und Admin-Portale

STAND

25.10.2026

UMFANG

PDF, 11 Seiten

ONLINE

tomoris.com/downloads/mfa-microsoft-365-checkliste

AUF EINEN BLICK

2

Notfallzugriffskonten
mindestens, nur in der
Cloud

90 Tage

Notfallkonten spätestens
erneut testen

Nur Bericht

Richtlinien erst testen,
dann einschalten

1.10.2025

Phase 2 der Pflicht-MFA
für die Azure-Verwaltung

FÜR WEN

- Administration von Microsoft 365 und Microsoft Entra ID in kleinen und mittleren Unternehmen
- IT-Dienstleister, die Mandanten ihrer Kunden einrichten und betreuen
- IT-Leitung, die den MFA-Rollout plant und gegenüber der Geschäftsführung vertritt

WORUM ES GEHT

Solange ein Konto nur mit Passwort geschützt ist, genügt Angreifern ein gestohlenes Passwort. Diese Checkliste führt die Administration von Microsoft 365 und Microsoft Entra ID in acht Schritten zur Multi-Faktor-Authentifizierung für alle: Ausgangslage und Lizenz prüfen, Notfallzugriffskonten anlegen, Methoden wählen, Registrierung und Kommunikation vorbereiten, Richtlinien im Modus „Nur Bericht“ testen, Legacy-Authentifizierung blockieren, Administratoren phishingresistent absichern und das Ergebnis kontrollieren. Dazu kommen die Phasen der verpflichtenden MFA, die Microsoft für Azure und die Admin-Portale durchsetzt.

Die Checkliste ist eine Empfehlung von TOMORIS und an die eigene Umgebung anzupassen; sie ersetzt keine Rechtsberatung. Microsoft ändert Funktionen, Bezeichnungen und Termine laufend; Maßgeblich sind die verlinkten Seiten von Microsoft Learn in der aktuellen Fassung, für NIS2-Pflichten der Gesetzestext des NISG 2026 in der geltenden Fassung. Testen Sie jede Richtlinie zuerst im Modus „Nur Bericht“.

INHALT

01	Worum es geht und was verpflichtend ist	3
02	Schritt 1: Ausgangslage und Lizenz prüfen	3
03	Schritt 2: Notfallzugriffskonten anlegen	4
04	Schritt 3: Methoden wählen	5
05	Schritt 4: Registrierung vorbereiten und informieren	6
06	Schritt 5: Schrittweise einführen mit „Nur Bericht“	7
07	Schritt 6: Legacy-Authentifizierung blockieren	7
08	Schritt 7: Administratoren phishingresistent absichern	8
09	Verpflichtende MFA von Microsoft für Azure und Admin-Portale	9
10	Schritt 8: Kontrollieren und nachhalten	10
11	Quellen	11

01

Worum es geht und was verpflichtend ist

Zwei Faktoren aus verschiedenen Kategorien, nicht jede MFA gleich stark; was das NISG 2026 vorgibt und was Microsoft durchsetzt.

Bei der Multi-Faktor-Authentifizierung (MFA) genügt das Passwort allein nicht. Die Faktoren stammen laut BSI aus verschiedenen Kategorien: Wissen (etwa Passwort oder PIN), Besitz (etwa Chipkarte, USB-Token oder Smartphone) oder Biometrie (etwa Fingerabdruck). Die US-Behörde CISA empfiehlt MFA für alle Benutzer und Dienste und nennt phishingresistente MFA den Goldstandard; jede MFA sei aber besser als keine.

Was vorgegeben ist und was empfohlen wird

VORGABE	FÜR WEN	GRUNDLAGE
Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung als Teil der Risikomanagementmaßnahmen	wesentliche und wichtige Einrichtungen, seit 1. Oktober 2026	§ 32 Abs. 4 lit. j NISG 2026; § 2 NISV 2026 mit Anhang Nr. 11.7 DVO 2024/2690
MFA für Azure-Portal und Admin Center von Entra, Intune und Microsoft 365, für ändernde Zugriffe auch über Azure CLI, PowerShell und API	alle Benutzerkonten, die diese Anwendungen nutzen	technische Durchsetzung durch Microsoft (Abschnitt 09)
alle weiteren Punkte dieser Checkliste	alle Mandanten	Empfehlung von TOMORIS nach Microsoft Learn, CISA und BSI

§ 32 NISG 2026 verlangt geeignete und verhältnismäßige Maßnahmen (Abs. 1 bis 3). Die NISV 2026 (BGBl. II Nr. 290/2026) erstreckt in § 2 den Anhang der Durchführungsverordnung (EU) 2024/2690 auf alle wesentlichen und wichtigen Einrichtungen: Nutzer sind, soweit angemessen und je nach Klassifizierung der Werte, mit mehreren Faktoren oder kontinuierlich zu authentifizieren (Anhang Nr. 11.7.1). Ein bestimmtes Verfahren schreiben beide nicht vor. Wer als wesentliche oder wichtige Einrichtung gilt, regeln §§ 24 bis 26. § 32 gilt seit 1. Oktober 2026 (§ 51 Abs. 2; kundgemacht am 23.12.2025).

02

Schritt 1: Ausgangslage und Lizenz prüfen

Sicherheitsstandards oder Conditional Access: welcher Weg zu Ihrer Lizenz passt und welche Konten Sie vorher erfassen.

Zwei Wege zur MFA in Microsoft Entra ID (Microsoft Learn: Sicherheitsstandards, MFA für alle Benutzer)

MERKMAL	SICHERHEITSSTANDARDS	CONDITIONAL ACCESS
Lizenz	keine zusätzliche	mindestens Microsoft Entra ID P1
MFA	alle registrieren sich; Administratoren bei jeder Anmeldung, andere, wenn Microsoft es für nötig hält	nach Richtlinie; Microsoft empfiehlt als Basis alle Benutzer, alle Ressourcen

Legacy-Authentifizierung	blockiert, ebenso der Gerätecodefluss	eigene Richtlinie (Schritt 6)
Ausnahmen	keine, nur ein oder aus; Synchronisierungskonten sind ausgenommen	gezielt, etwa für Notfallzugriffskonten

- ☐ Lizenz geklärt: Conditional Access setzt Microsoft Entra ID P1 oder P2 voraus; ohne diese Lizenz aktivieren Sie die Sicherheitsstandards.
- ☐ Status der Sicherheitsstandards geprüft (Entra ID > Übersicht > Eigenschaften > Sicherheitsstandards verwalten). Microsoft aktiviert sie auch selbst, wenn ein Mandant weder Richtlinien für bedingten Zugriff noch Premium-Lizenzen noch aktiv genutzte Legacy-Clients hat.
- ☐ Vorhandene Richtlinien für bedingten Zugriff erfasst. Wer die Sicherheitsstandards durch eigene Richtlinien ersetzt, muss sie deaktivieren und sofort passende Richtlinien aktivieren.
- ☐ Alte MFA pro Benutzer (per-user MFA) erfasst; sie wird nach der Umstellung auf Conditional Access manuell deaktiviert (Schritt 5).
- ☐ Sonderkonten erfasst: Administratorkonten samt Rollen, Benutzerkonten, mit denen Skripte laufen, und bei hybrider Identität das Synchronisierungskonto von Entra Connect oder Cloud Sync.

03

Schritt 2: Notfallzugriffskonten anlegen

Vor der ersten Richtlinie: mindestens zwei Konten nur in der Cloud, mit Passkey, getrennt verwahrt und überwacht.

Notfallzugriffskonten (Break-Glass-Konten) verhindern, dass Sie sich durch eine fehlerhafte Richtlinie, einen Ausfall des Identitätsverbunds oder unerreichbare MFA-Geräte aus dem Mandanten aussperren. Die Punkte folgen Microsoft Learn, gelesen am 25. Oktober 2026.

- ☐ Mindestens zwei Konten nur in der Cloud, mit der Domäne *.onmicrosoft.com, weder im Verbund noch aus dem lokalen Active Directory synchronisiert.
- ☐ Rolle Globaler Administrator dauerhaft aktiv zugewiesen, in Privileged Identity Management nicht nur berechtigt.
- ☐ Anmeldung mit Passkey (FIDO2), von Microsoft empfohlen, oder mit zertifikatbasierter Authentifizierung, wenn bereits eine PKI besteht; mit einer anderen Methode als die normalen Administratorkonten. Anmelde- und Geräte laufen nicht ab und fallen nicht unter eine automatische Bereinigung.
- ☐ Keiner einzelnen Person und keinem Telefon von Mitarbeitenden zugeordnet; Schlüssel und Anmelde- und Geräte an getrennten, sicheren, feuerfesten Orten; Nutzung nur von einer dafür vorgesehenen, sicheren Arbeitsstation.

- ☐ Aus allen Richtlinien für bedingten Zugriff ausgeschlossen, die die Anmeldung blockieren oder einschränken, am besten über eine eigene Gruppe. Richtlinien im Modus „Nur Bericht“ blockieren nicht und brauchen keinen Ausschluss.
- ☐ Jede Anmeldung löst eine Benachrichtigung aus; jede Nutzung wird anhand der Protokolle nachbesprochen.
- ☐ Mindestens alle 90 Tage und nach Personalwechseln in der IT getestet: Anmeldung, Verwaltungsaufgaben, Liste der berechtigten Personen, dokumentierter Ablauf.

Der Ausschluss aus Ihren Richtlinien befreit nicht von der verpflichtenden MFA, die Microsoft für Azure und die Admin-Portale durchsetzt; sie gilt ausdrücklich auch für Notfallzugriffskonten. Passkey (FIDO2) und zertifikatbasierte Authentifizierung erfüllen sie.

04

Schritt 3: Methoden wählen

Phishingresistent, wo möglich, Microsoft Authenticator mit Zahlenabgleich als Mindeststandard, SMS und Anruf nur als Übergang.

Methoden in Microsoft Entra ID und ihre Einordnung (Microsoft Learn, CISA, BSI)

Passkey (FIDO2)	Phishingresistent: als FIDO2-Sicherheitsschlüssel per USB oder NFC, als Passkey in Microsoft Authenticator oder als synchronisierter Passkey. FIDO/WebAuthn ist laut CISA die einzige breit verfügbare phishingresistente Form.
Windows Hello for Business	Phishingresistent und als Erstanmeldung nutzbar; Microsoft empfiehlt es neben Passkeys und zertifikatbasierter Authentifizierung.
Zertifikatbasierte Authentifizierung	Phishingresistent (bei CISA: PKI-basierte MFA). Sinnvoll mit eigener Public-Key-Infrastruktur; CISA nennt eine reife Identitätsverwaltung als Voraussetzung.
Microsoft Authenticator mit Benachrichtigung	Standardmethode der Sicherheitsstandards: Die Person tippt eine angezeigte Zahl in die App (Zahlenabgleich), das erschwert MFA-Fatigue-Angriffe. Nicht phishingresistent; laut CISA gehört Push mit Zahlenabgleich, neben Einmalcodes aus App oder Token, zu den besten Optionen für KMU, die phishingresistente MFA nicht sofort einführen können.
Einmalcode aus einer App (OATH-TOTP)	Sechsstelliger Code aus Microsoft Authenticator oder einer anderen TOTP-App, auch unter Sicherheitsstandards zulässig; anfällig für Phishing, weil er auf einer gefälschten Anmeldeseite eingegeben werden kann (CISA).

SMS und Sprachanruf

Nur als letzte Möglichkeit und Übergang (CISA): anfällig für Phishing, Angriffe auf SS7 und SIM-Swapping. Microsoft nennt SMS als Beispiel für die am wenigsten sicheren Methoden, die man sperren kann, und für den Umstieg auf sicherere wie Authenticator. Das BSI rät, den Code nicht auf dem Anmeldegerät zu empfangen.

- ☐ Zielbild: phishingresistent für Administratoren und gefährdete Konten, sonst mindestens Authenticator mit Zahlenabgleich; SMS und Anruf nur befristet; je Person zwei Methoden.

05

Schritt 4: Registrierung vorbereiten und informieren

Registrierung absichern, Termine ankündigen und erklären, woran echte Anfragen zu erkennen sind.

Ohne Microsoft Entra ID Protection werden Personen bei der nächsten Anmeldung, die MFA verlangt, zur Registrierung aufgefordert. Mit einem bereits gestohlenen Passwort könnte dann ein Angreifer seine eigene Methode registrieren. Microsoft empfiehlt deshalb, die Registrierung per Conditional Access an vertrauenswürdige Geräte und Standorte zu binden; zusätzlich lässt sich ein befristeter Zugriffspass (TAP) verlangen, ein zeitlich begrenzter Code von der Administration. Unter Sicherheitsstandards gibt es seit 29. Juli 2024 keine 14-tägige Schonfrist für die Registrierung mehr.

- ☐ Termine festgelegt: Pilot, Wellen, Stichtag für die Registrierung; Helpdesk und Vertretung eingeplant.
- ☐ Mitarbeitende rechtzeitig informiert, was sich ändert, was sie tun müssen und bis wann; Microsoft stellt Kommunikationsvorlagen bereit (aka.ms/mfatemplates).
- ☐ Ablauf bei Verlust oder Wechsel des Smartphones festgelegt: befristeter Zugriffspass oder Pflege der Methoden durch die Administration.
- ☐ Nach dem Aktivieren der Sicherheitsstandards bestehende Sitzungen widerrufen, etwa per `Revoke-MgUserSignInSession`, damit sich alle neu anmelden und registrieren.

Mustertext zum Anpassen. Die Verhaltenshinweise empfiehlt TOMORIS, weil CISA Angriffe mit gehäuften Push-Anfragen (Push Bombing) und Phishing-Seiten für Passwort und Einmalcode beschreibt: „Ab [Datum] bestätigen Sie jede Anmeldung bei Microsoft 365 zusätzlich mit [Microsoft Authenticator oder Passkey]. Bitte richten Sie die Methode bis [Datum] unter <https://myprofile.microsoft.com> im Bereich Sicherheitsinformationen ein, wenn möglich auch eine zweite. Bestätigen Sie nur Anmeldungen, die Sie gerade selbst durchführen; unerwartete Anfragen lehnen Sie ab und melden sie an [Name, Funktion, Telefon]. Wir fragen Sie nie per Telefon oder E-Mail nach einem Code. Ist Ihr Smartphone verloren, melden Sie sich sofort bei [Kontakt].“

06 —

Schritt 5: Schrittweise einführen mit „Nur Bericht“

Pilotgruppe, Richtlinie im Modus „Nur Bericht“, Wirkung prüfen, einschalten und in Wellen erweitern.

1 Pilotgruppe bestimmen und registrieren lassen

Beginnen Sie mit einer kleinen Gruppe, etwa der IT selbst, und aktivieren Sie die gewählten Methoden. Danach erweitern Sie in Wellen, die Ihr Support bewältigen kann.

2 Richtlinie „MFA für alle“ anlegen

Einschließen: zuerst die Pilotgruppe, im Endausbau Alle Benutzer. Ausschließen: Notfallzugriffskonten, bei hybrider Identität die Rolle Directory-Synchronisierungskonten. Zielressourcen: Alle Ressourcen. Erteilen: Authentifizierungsstärke Multi-Faktor-Authentifizierung. Richtlinie aktivieren: Nur Bericht (Report-only).

3 Wirkung prüfen

Im Modus „Nur Bericht“ blockiert die Richtlinie nichts, zeigt aber, wen sie treffen würde. Prüfen Sie Richtlinienauswirkung und Anmeldeprotokolle.

4 Einschalten, erweitern, aufräumen

Stellen Sie die Richtlinie auf „Ein“ und nehmen Sie Welle für Welle weitere Gruppen auf, bis sie für alle gilt. Danach deaktivieren Sie die alte MFA pro Benutzer manuell, wie Microsoft es empfiehlt.

Sicherheitsstandards kennen keinen Testmodus, nur Ein oder Aus für den ganzen Mandanten. Informieren Sie vorher alle und stellen Sie sicher, dass Administratoren keine älteren Authentifizierungsprotokolle verwenden, wie Microsoft es verlangt. Deaktivieren Sie unter Sicherheitsstandards keine Methoden: Microsoft warnt, dass Sie sich damit aussperren können.

07 —

Schritt 6: Legacy-Authentifizierung blockieren

Alte Protokolle beherrschen keine MFA und umgehen sie. Erst die Nutzung finden, dann blockieren.

Legacy-Authentifizierung nennt Microsoft Anmeldungen von Clients ohne moderne Authentifizierung, etwa Office 2010, und über ältere E-Mail-Protokolle wie IMAP, SMTP oder POP3. Sie unterstützt keine MFA, ein Angreifer kann eine MFA-Richtlinie damit umgehen. Nach Microsofts Analyse nutzen mehr als 97 Prozent der Credential-Stuffing- und mehr als 99 Prozent der Password-Spray-Angriffe Legacy-Authentifizierung.

1 Nutzung ermitteln

Entra ID > Monitoring & health > Anmeldeprotokolle: Spalte Client-App einblenden und nach allen älteren Authentifizierungsprotokollen filtern, auch auf der Registerkarte für nicht interaktive Anmeldungen. Betroffene Clients umstellen oder ersetzen.

2

Blockieren, erst im Modus „Nur Bericht“

Alle Benutzer, Alle Ressourcen, Bedingungen > Client-Apps: nur Exchange ActiveSync-Clients und Andere Clients; Erteilen: Zugriff blockieren. Ausschließen nur Konten, die Legacy-Authentifizierung noch brauchen; Microsoft empfiehlt, mindestens ein Konto auszuschließen, um sich bei einem Fehler nicht auszusperrern. Nach Prüfung auf „Ein“ stellen, Ausnahmen abbauen.

Sicherheitsstandards blockieren Legacy-Authentifizierung, die Standardauthentifizierung für Exchange ActiveSync und den Gerätecodefluss; für neue Mandanten gilt die Sperre des Gerätecodeflusses seit 1. Juli 2026.

08

Schritt 7: Administratoren phishingresistent absichern

Für privilegierte Rollen die Authentifizierungsstärke „Phishingresistente MFA“: erst registrieren, dann erzwingen.

Wer ein Administratorkonto übernimmt, erreicht oft jedes System und alle Daten. CISA fordert Administratoren und andere besonders wertvolle Ziele deshalb auf, phishingresistente MFA einzuführen oder die Umstellung zu planen, beginnend mit Helpdesk und IT-Administration. Conditional Access bietet dafür die integrierte Authentifizierungsstärke „Phishingresistente MFA“. Als Rollen eignen sich jene, für die schon die Sicherheitsstandards MFA bei jeder Anmeldung verlangen, etwa Global Administrator, Privileged Role Administrator, Security Administrator, Exchange Administrator und User Administrator.

- ☐ Getrennte Konten für Verwaltung und tägliche Arbeit; das senkt auch die Zahl der MFA-Abfragen (Microsoft).
- ☐ Alle mit Admin-Rolle haben eine phishingresistente Methode registriert, etwa einen Passkey mit Hilfe eines befristeten Zugriffspasses, und die Notfallzugriffskonten sind getestet, bevor die Richtlinie greift; sonst sperren Sie Administratoren aus.
- ☐ Richtlinie (Empfehlung von TOMORIS): Verzeichnisrollen einschließen, Notfallzugriffskonten ausschließen, Alle Ressourcen, Authentifizierungsstärke „Phishingresistente MFA“, zuerst „Nur Bericht“.
- ☐ Danach weitere gefährdete Gruppen, etwa Personal- oder Rechtsabteilung mit weitreichenden Lese-rechten; Systeme ohne MFA-Unterstützung der Geschäftsleitung als Risiko melden und ablösen (CISA).

09 —

Verpflichtende MFA von Microsoft für Azure und Admin-Portale

Microsoft erzwingt MFA für Admin-Portale und die Azure-Verwaltung in zwei Phasen; ausnehmen lässt sich kein Benutzerkonto.

Unabhängig von Ihren Richtlinien verlangt Microsoft MFA für die Verwaltung über Azure und die Admin-Portale. Die Phasen und Termine stammen von Microsoft Learn, gelesen am 25. Oktober 2026.

- Gilt für alle Benutzerkonten, auch für Notfallzugriffskonten, Administratoren mit berechtigten Rollen und Testmandanten. Ausschlüsse in Ihren Richtlinien wirken nicht, ein Opt-out gibt es nicht; auch „Angemeldet bleiben“ befreit nicht.
- Nicht betroffen sind Workload-Identitäten wie verwaltete Identitäten und Dienstprinzipale sowie das Synchronisierungskonto von Entra Connect oder Cloud Sync. Benutzerkonten, mit denen Skripte laufen, müssen MFA erfüllen; Microsoft empfiehlt den Umstieg auf Workload-Identitäten.
- Anmeldungen per ROPC (Benutzername und Kennwort über OAuth) sind mit MFA nicht vereinbar; Azure CLI ab 2.76 und Azure PowerShell ab 14.3 verwenden.
- Status prüfen als Global Administrator unter aka.ms/managementfaforazure (Phase 1) und aka.ms/postponePhase2MFA (Phase 2).

Phasen der verpflichtenden MFA



Okt. 2024

Phase 1: Portale

MFA für Lese- und Schreibvorgänge im Azure-Portal, im Microsoft Entra Admin Center und im Intune Admin Center, schrittweise weltweit.



Feb. 2025

Microsoft 365 Admin Center

Schrittweise Durchsetzung für die Anmeldung am Microsoft 365 Admin Center.



1.10.2025

Phase 2: Werkzeuge

MFA für Erstellen, Ändern und Löschen über Azure CLI, Azure PowerShell, Azure-App, IaC-Werkzeuge und REST-API; Lesen bleibt ohne MFA.



1.7.2026

Aufschub abgelaufen

Bis dahin ließ sich Phase 2 verschieben, Phase 1 bis 30.9.2025. Nach Beginn der Durchsetzung von Phase 2 kann ein Global Administrator beim Microsoft-Support beantragen, sie vorübergehend aufzuheben.

Die verpflichtende MFA ersetzt keine eigene Richtlinie: Sie gilt nur für die genannten Anwendungen. E-Mail, Teams und alle anderen Anwendungen sichern Sie mit Sicherheitsstandards oder Conditional Access ab.

10 —

Schritt 8: Kontrollieren und nachhalten

Registrierung und Nutzung auswerten, Ausnahmen abbauen, Notfallkonten testen, typische Fehler vermeiden.

- ☐ Registrierung und Nutzung der Methoden regelmäßig im Dashboard „Authentifizierungsmethodenaktivität“ geprüft; Personen mit SMS oder Anruf schrittweise auf Microsoft Authenticator oder sicherere Methoden umgestellt.
- ☐ Anmeldeprotokolle ausgewertet: Sie zeigen, wann MFA verlangt wurde und welche Richtlinien für bedingten Zugriff griffen; bei der verpflichtenden MFA nennen sie die Anwendung, die MFA erzwungen hat.
- ☐ Legacy-Anmeldungen (Spalte Client-App) gegengeprüft; Ausschlüsse aus Richtlinien dokumentiert, begründet und abgebaut.
- ☐ Notfallzugriffskonten mindestens alle 90 Tage getestet; neue Mitarbeitende registrieren ihre Methoden beim Eintritt, etwa mit befristetem Zugriffspass.

Häufige Fehler: kein oder nur ein Notfallzugriffskonto; Richtlinien sofort auf „Ein“ statt „Nur Bericht“; phishingresistente MFA vor der Registrierung erzwungen; unter Sicherheitsstandards Methoden deaktiviert; Legacy-Authentifizierung blockiert, ohne Scanner und Altanwendungen zu erfassen; Skripte unter Benutzerkonten; nur eine Methode je Person.

NÄCHSTER SCHRITT

Selbst prüfen oder gemeinsam umsetzen

UMSETZUNG BESPRECHEN

Kontakt aufnehmen

tomoris.com/contact

contact@tomoris.com

11 —

Quellen

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

- 1 Microsoft Learn: Sicherheitsstandards**
Richtlinien, Methoden, Vergleich mit Conditional Access; 25.10.2026
learn.microsoft.com/de-de/entra/fundamentals/security-defaults
- 2 Microsoft Learn: Obligatorische MFA**
Phasen, Konten, ROPC, Aufschub, Bestätigung, FAQ; 25.10.2026
learn.microsoft.com/de-de/entra/identity/authentication/concept...
- 3 Microsoft Learn: Notfallzugriffskonten**
Erstellen, Anforderungen, bedingter Zugriff, Prüfung; 25.10.2026
learn.microsoft.com/de-de/entra/identity/role-based-access-cont...
- 4 Microsoft Learn: MFA-Bereitstellung planen**
Methoden, Registrierung, Rollout, Berichte; 25.10.2026
learn.microsoft.com/de-de/entra/identity/authentication/howto-m...
- 5 Microsoft Learn: Übersicht Authentifizierung**
Methoden, phishingresistente Methoden; 25.10.2026
learn.microsoft.com/de-de/entra/identity/authentication/concept...
- 6 Microsoft Learn: MFA für alle Benutzer**
Stärken, Ausschlüsse, Richtlinie, „Nur Bericht“; 25.10.2026
learn.microsoft.com/de-de/entra/identity/conditional-access/pol...
- 7 Microsoft Learn: Legacy-Authentifizierung blockieren**
Richtlinie, Nutzung in Anmeldeprotokollen; 25.10.2026
learn.microsoft.com/de-de/entra/identity/conditional-access/pol...
- 8 CISA: Implementing Phishing-Resistant MFA (2022)**
Threats to MFA, Table 1, Implementations, Areas of Focus
www.cisa.gov/sites/default/files/publications/fact-sheet-implem...
- 9 BSI: Zwei-Faktor-Authentisierung**
Faktoren, Verfahren, Empfehlungen; 25.10.2026
www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Info...
- 10 NISG 2026, BGBl. I Nr. 94/2025 (RIS)**
§§ 24–26, 32, 51; Fassung vom 25.10.2026
www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gese...
- 11 NISV 2026, BGBl. II Nr. 290/2026, authentische Kundmachung im RIS**
§§ 2, 4 bis 7 und 9, kundgemacht am 1.10.2026, gelesen am 25.10.2026
www.ris.bka.gv.at/eli/bgbl/II/2026/290
- 12 Durchführungsverordnung (EU) 2024/2690, Anhang Nr. 11.6 und 11.7 (Authentifizierung)**
für alle wesentlichen und wichtigen Einrichtungen anwendbar nach § 2 NISV 2026
eur-lex.europa.eu/eli/reg_impl/2024/2690/oj/deu