

CHECKLISTE · TOMORIS TOOLBOX

Microsoft 365 absichern: Checkliste für Entra ID, Exchange, SharePoint und Teams

Wichtige Einstellungen für Entra ID, Exchange Online, Defender, SharePoint, OneDrive und Teams, mit Kennungen der CISA-Baselines und Lizenzhinweisen

STAND

25.10.2026

UMFANG

PDF, 10 Seiten

ONLINE

tomoris.com/downloads/microsoft-365-sicherheitscheckliste

AUF EINEN BLICK

2 bis 8

Globale Administratoren
nach CISA SCuBA

30 Tage

laut CISA höchstens:
Gültigkeit von
„Jeder“-Links

6

Dienste im Überblick, von
Entra ID bis Teams

v2.0.0

Stand der CISA-Baselines
(ScubaGear)

FÜR WEN

- Administration von Microsoft 365 in kleinen und mittleren Unternehmen
- IT-Dienstleister, die Microsoft-365-Mandanten für Kunden betreuen
- Informationssicherheitsbeauftragte, die den Stand eines Mandanten prüfen

WORUM ES GEHT

Diese Checkliste fasst die wichtigsten Sicherheitseinstellungen für Microsoft 365 je Dienst zusammen: Entra ID, Exchange Online, Schutz vor Schadsoftware und Phishing, SharePoint und OneDrive, Teams sowie Protokolle. Grundlage sind die Baselines der US-Behörde CISA aus dem Projekt SCuBA (ScubaGear v2.0.0 vom 22.10.2026) und die Dokumentation von Microsoft. Jeder Punkt nennt die Kennung der Baseline, damit Sie ihn nachlesen und mit dem kostenlosen Werkzeug ScubaGear prüfen können.

Diese Checkliste ist eine Empfehlung von TOMORIS auf Grundlage der CISA-Baselines, die nur für US-Bundesbehörden verbindlich sind. Bezeichnungen, Standardwerte und Lizenzbedingungen von Microsoft ändern sich laufend; maßgeblich sind die aktuelle Dokumentation von Microsoft und die jeweils gültige Fassung der Baselines. Testen Sie Änderungen vor der Umsetzung, etwa mit Notfallzugang und Pilotgruppe.

INHALT

01	So nutzen Sie die Checkliste	2
02	Microsoft Entra ID: Anmeldung und Konten	3
03	Microsoft Entra ID: Rollen, Apps und Gäste	4
04	Exchange Online: E-Mail und Postfächer	5
05	Schutz vor Schadsoftware und Phishing	5
06	SharePoint und OneDrive: Freigaben	6
07	Microsoft Teams: Besprechungen und externe Kontakte	7
08	Protokolle, Warnungen und Messung	8
09	Lizenzhinweise	8
10	Quellen	9

01

So nutzen Sie die Checkliste

Woher die Punkte stammen, was „muss“ und „sollte“ heißt und wie Sie messen

Die CISA veröffentlicht im Projekt SCuBA sichere Grundkonfigurationen für Microsoft 365. Für US-Bundesbehörden sind die Muss-Vorgaben (SHALL) über BOD 25-01 verbindlich; anderen Organisationen stellt die CISA die Baselines als Referenz zur Verfügung. Die Baselines setzen mindestens eine Lizenz Microsoft 365 E3 voraus und nennen nur Lizenzen, die darüber hinausgehen. Mit ScubaGear stellt die CISA ein kostenloses Werkzeug bereit, das einen Mandanten gegen die Baselines prüft. Bei Punkten aus den Baselines steht die Kennung, etwa MS.AAD.1.1, und ob die Baseline den Punkt verlangt (muss) oder empfiehlt (sollte); Punkte ohne Kennung stammen aus Microsoft Learn oder sind Empfehlungen von TOMORIS.

Microsoft Secure Score	Die Microsoft-Sicherheitsbewertung misst den Sicherheitsstatus; eine höhere Zahl bedeutet mehr umgesetzte Empfehlungen. Sie steht im Microsoft Defender-Portal.
Sicherheitsstandards	Für Mandanten im kostenlosen Tarif von Entra ID: MFA-Registrierung für alle, MFA für Administratoren und bei Bedarf für alle Benutzer, Blockieren älterer Protokolle und des Gerätecodeflusses, Schutz privilegierter Aktivitäten.
Bedingter Zugriff	Mit Entra ID P1 oder P2 sind laut Microsoft Richtlinien für bedingten Zugriff meist die bessere Wahl als die Sicherheitsstandards.

Die Checkliste ist eine Empfehlung von TOMORIS auf Grundlage der CISA-Baselines; nicht jeder Punkt passt zu jedem Unternehmen. Prüfen Sie Änderungen vorab, damit Sie niemanden aussperren. Multi-Faktor-Authentifizierung und bedingten Zugriff behandelt die eigene Checkliste „MFA in Microsoft 365 einführen“ ausführlich, SPF, DKIM und DMARC der Leitfaden zur E-Mail-Sicherheit.

02

Microsoft Entra ID: Anmeldung und Konten

Ältere Protokolle sperren, starke Anmeldung, Notfallzugang

Microsoft empfiehlt, Anmeldungen mit älteren Protokollen zu blockieren, weil sie keine Multi-Faktor-Authentifizierung unterstützen. Laut Microsofts Analyse nutzen mehr als 97 Prozent der Credential-Stuffing-Angriffe und mehr als 99 Prozent der Passwort-Spray-Angriffe solche Protokolle.

- ☐ Ältere Authentifizierung blockiert (MS.AAD.1.1, muss).
- ☐ Phishingresistente MFA für alle Benutzer (MS.AAD.3.1, muss), etwa gerätegebundene Passkeys, FIDO2-Schlüssel, Windows Hello for Business oder zertifikatbasierte Authentifizierung; als Untergrenze MFA für alle Benutzer, etwa solange phishingresistente Verfahren noch nicht möglich sind (MS.AAD.3.2, muss); für hochprivilegierte Rollen immer phishingresistent (MS.AAD.3.6, muss).
- ☐ SMS, Sprachanruf und Einmalcode per E-Mail als Methoden deaktiviert (MS.AAD.3.5, muss); im Microsoft Authenticator Anmeldekontext angezeigt (MS.AAD.3.3, muss).
- ☐ Gerätecode-Anmeldung blockiert (MS.AAD.3.9, sollte).
- ☐ Benutzer mit hohem Risiko und Anmeldungen mit hohem Risiko blockiert (MS.AAD.2.1 und 2.3, muss; erfordert Entra ID P2).
- ☐ Kennwörter laufen nicht ab (MS.AAD.6.1, muss); Details in der Passwortrichtlinie.
- ☐ Mindestens zwei Notfallzugriffskonten, rein in der Cloud mit einer Domäne *.onmicrosoft.com, nicht synchronisiert, mit Passkey (FIDO2) oder Zertifikat geschützt (Microsoft Learn).

- ☐ Ohne Lizenz für bedingten Zugriff: Sicherheitsstandards aktiviert (Microsoft Learn).

03 —

Microsoft Entra ID: Rollen, Apps und Gäste

Wenige globale Administratoren, eingeschränkte App-Einwilligung, kontrollierte Gäste

- ☐ Zwei bis acht Personen mit der Rolle Globaler Administrator (MS.AAD.7.1, muss); Microsoft empfiehlt weniger als fünf, die CISA lässt weitere Konten etwa für den Notfallzugriff zu.
- ☐ Für Verwaltungsaufgaben feinere Rollen statt Globaler Administrator (MS.AAD.7.2, muss).
- ☐ Privilegierte Konten nur in der Cloud, getrennt vom lokalen Active Directory (MS.AAD.7.3, muss).
- ☐ Keine dauerhaft aktiven Zuweisungen hochprivilegierter Rollen, Aktivierung des Globalen Administrators nur mit Genehmigung, Warnungen bei Zuweisung und Aktivierung (MS.AAD.7.4 bis 7.8, muss; Warnung bei anderen hochprivilegierten Rollen 7.9, sollte; Entra ID P2 oder eine andere PAM-Lösung).
- ☐ Nur Administratoren registrieren Anwendungen (MS.AAD.5.1, muss).
- ☐ Benutzereinwilligung für Anwendungen eingeschränkt (MS.AAD.5.2, muss); Microsoft empfiehlt, sie höchstens für Apps verifizierter Herausgeber zuzulassen.
- ☐ Workflow für die Einwilligung durch Administratoren eingerichtet (MS.AAD.5.3, muss).
- ☐ Gäste mit eingeschränktem Zugriff auf Verzeichnisobjekte (MS.AAD.8.1, sollte); einladen dürfen nur Personen mit der Rolle Gasteinladender (MS.AAD.8.2, sollte), nur an freigegebene Domänen (MS.AAD.8.3, sollte).
- ☐ Neu in v2.0.0: riskante KI-Agenten blockiert (MS.AAD.9.1, muss; laut CISA mit Entra ID P2 und Microsoft Agent 365 oder Microsoft 365 E7).

Als hochprivilegiert nennt die CISA als Grundliste, die bei Bedarf um weitere Rollen zu ergänzen ist: Globaler Administrator, Administrator für privilegierte Rollen, Benutzeradministrator, SharePoint-Administrator, Exchange-Administrator, Administrator für Hybrididentität, Anwendungsadministrator und Cloudanwendungsadministrator.

04 —

Exchange Online: E-Mail und Postfächer

Weiterleitung, Absenderschutz, SMTP AUTH, Freigaben und Überwachung

- ☐ Automatische Weiterleitung an externe Domänen deaktiviert (MS.EXO.1.1, muss): Die CISA setzt das über die Remotedomäne „Default“ um, deren automatische Weiterleitung nicht zugelassen wird. Zusätzlich in der Richtlinie für ausgehenden Spam „Aus – Weiterleitung ist deaktiviert“ wählen: Der Standardwert „Automatisch – Systemgesteuert“ verhält sich je nach Mandant unterschiedlich.
- ☐ SPF mit Ablehnung nicht freigegebener Absender, DKIM für alle Domänen, DMARC mit p=reject (MS.EXO.2.2, 4.1, 4.2, muss; DKIM MS.EXO.3.1, sollte).
- ☐ SMTP AUTH organisationsweit deaktiviert (MS.EXO.5.1, muss); nur für einzelne Postfächer, die es nachweislich brauchen, ausnahmsweise erlaubt. Sind die Sicherheitsstandards aktiv, ist SMTP AUTH bereits deaktiviert.
- ☐ Kontakt- und Kalenderdetails nicht mit allen Domänen geteilt (MS.EXO.6.1 und 6.2, muss).
- ☐ Hinweis für Nachrichten externer Absender aktiviert (MS.EXO.7.1, muss).
- ☐ Postfachüberwachung aktiv (MS.EXO.13.1, muss); laut Microsoft in allen Organisationen standardmäßig eingeschaltet, trotzdem prüfen.

Wird die automatische Weiterleitung deaktiviert, wirken auch Posteingangsregeln von Benutzern und Weiterleitungen durch Administratoren nicht mehr, die Nachrichten an externe Adressen umleiten; der Absender erhält einen Unzustellbarkeitsbericht (Microsoft Learn).

05 —

Schutz vor Schadsoftware und Phishing

Voreingestellte Richtlinien, Anlagen, Links, Identitätswechsel und Ausnahmen

Mit den voreingestellten Sicherheitsrichtlinien Standard und Streng wendet Microsoft empfohlene Einstellungen für den E-Mail-Schutz an; sie sind praktisch nicht konfigurierbar. Die voreingestellte Richtlinie Integrierter Schutz gibt Benutzern ohne andere Zuweisung einen Grundschutz durch Sichere Anlagen und Sichere Links aus Defender for Office 365.

- ☐ Voreingestellte Sicherheitsrichtlinie Standard für die meisten Benutzer zugewiesen, Streng für ausgewählte, besonders gefährdete Konten (Microsoft Learn).
- ☐ Anhänge, die sich per Klick ausführen lassen, blockiert, mindestens .exe, .cmd und .vbe (MS.SECURITYSUITE.1.1, muss).

- ☐ E-Mails auch nach der Zustellung geprüft, Schadsoftware in Quarantäne oder verworfen (MS.SECURITYSUITE.1.2 und 1.3, muss).
- ☐ Anhänge in SharePoint, OneDrive und Teams auf Schadsoftware geprüft (MS.SECURITYSUITE.1.4, sollte).
- ☐ Schutz vor Identitätswechsel für besonders gefährdete Konten, eigene Domänen sowie wichtige Lieferanten und Partner (MS.SECURITYSUITE.2.1 bis 2.3, sollte; Defender for Office 365).
- ☐ Spam und Phishing nicht im Posteingang zugestellt, keine zugelassenen Domänen im Anti-Spam-Schutz (MS.SECURITYSUITE.6.1 und 6.2, muss).
- ☐ Links in E-Mails, Teams und Office-Dokumenten gegen Sperrlisten geprüft, Klicks protokolliert (MS.SECURITYSUITE.7.1 und 7.3, sollte; Defender for Office 365).
- ☐ Keine IP-Zulassungslisten und keine sicheren Listen (MS.SECURITYSUITE.8.1 und 8.2, sollte).
- ☐ Richtlinie zur Verhinderung von Datenverlust für Ihre sensiblen Datenarten eingerichtet (MS.SECURITYSUITE.3.1, muss; 3.2 bis 3.5, sollte).

06 —

SharePoint und OneDrive: Freigaben

Externe Freigabe begrenzen, sichere Standardlinks, Ablauf für „Jeder“-Links

Stufen der externen Freigabe (Microsoft Learn), von offen bis geschlossen

Jeder	Links, mit denen jeder ohne Anmeldung auf Dateien oder Ordner zugreift.
Neue und vorhandene Gäste	Eingeladene melden sich mit ihrem Konto an oder bestätigen ihre Identität mit einem Code.
Vorhandene Gäste	Freigabe nur an Gäste, die bereits im Verzeichnis stehen.
Nur Personen in Ihrer Organisation	Externe Freigabe ist deaktiviert.

- ☐ Externe Freigabe für SharePoint und OneDrive auf „Vorhandene Gäste“ oder „Nur Personen in Ihrer Organisation“ begrenzt (MS.SHAREPOINT.1.1 und 1.2, muss) oder bewusst und dokumentiert offener eingestellt.
- ☐ Externe Freigabe auf freigegebene Domänen oder Sicherheitsgruppen beschränkt (MS.SHAREPOINT.1.3, muss).
- ☐ Standardlink „Bestimmte Personen“ mit Leserechten (MS.SHAREPOINT.2.1 und 2.2, muss).

- ☐ Wo „Jeder“-Links erlaubt sind: Ablauf nach höchstens 30 Tagen, nur Leserechte (MS.SHAREPOINT.3.1 und 3.2, muss).
- ☐ Gäste mit Bestätigungscode melden sich spätestens nach 30 Tagen erneut an (MS.SHAREPOINT.3.3, muss).

07 —

Microsoft Teams: Besprechungen und externe Kontakte

Wer Besprechungen starten, beitreten und Kontakt aufnehmen darf

Für den externen Zugriff sind in Teams laut Microsoft standardmäßig alle externen Domänen zulässig. Mit einer Zulassungsliste beschränken Sie Chats und Besprechungen auf die Organisationen, mit denen Sie tatsächlich zusammenarbeiten; alle anderen Domänen sind dann gesperrt.

- ☐ Externer Zugriff nur für freigegebene Domänen (MS.TEAMS.2.1, muss).
- ☐ Nicht verwaltete Teams-Konten können keinen Kontakt zu internen Benutzern aufnehmen (MS.TEAMS.2.2, muss); interne Benutzer kontaktieren sie nicht von sich aus (MS.TEAMS.2.3, sollte).
- ☐ Anonyme Benutzer können keine Besprechungen starten (MS.TEAMS.1.2, muss); anonyme Teilnehmende und Einwahl landen im Wartebereich (MS.TEAMS.1.3 und 1.5, sollte).
- ☐ Externe Teilnehmende können keine Steuerung geteilter Bildschirme anfordern (MS.TEAMS.1.1, sollte).
- ☐ Aufzeichnung von Besprechungen nach eigener Regel; die CISA empfiehlt, sie zu deaktivieren (MS.TEAMS.1.6, sollte).
- ☐ E-Mail-Integration von Teams deaktiviert (MS.TEAMS.4.1, muss).
- ☐ Nur freigegebene Microsoft-, Dritt- und eigene Apps installierbar (MS.TEAMS.5.1 bis 5.3, sollte).

08

Protokolle, Warnungen und Messung

Audit einschalten, Warnungen weiterleiten, Fortschritt messen

Achtung bei Business-Tarifen: Laut Microsoft ist die Überwachungsprotokollierung für Microsoft 365 Business Basic, Business Standard und Business Premium nicht standardmäßig aktiviert und muss manuell eingeschaltet werden.

- ☐ Einheitliches Überwachungsprotokoll aktiviert (MS.SECURITYSUITE.5.1, muss) und der Status im Microsoft Purview-Portal geprüft.
- ☐ Protokolle mindestens 3 Monate durchsuchbar und 12 Monate abrufbar (MS.SECURITYSUITE.5.2, muss); länger als 180 Tage in Microsoft 365 erfordert laut CISA E5, Microsoft Purview Suite oder den Zusatz E5 eDiscovery and Audit.
- ☐ Sicherheitswarnungen aktiviert und an ein überwachtes Postfach oder ein SIEM gesendet (MS.SECURITYSUITE.4.1, muss; 4.2, sollte).
- ☐ Anmelde- und Überwachungsprotokolle von Entra ID an die Stelle weitergeleitet, die Sicherheitsereignisse auswertet (MS.AAD.4.1, muss).
- ☐ Microsoft Secure Score als Ausgangswert festgehalten und regelmäßig überprüft.
- ☐ ScubaGear-Prüfung durchgeführt und Abweichungen begründet dokumentiert.

09

Lizenzhinweise

Welche Punkte laut CISA mehr als Microsoft 365 E3 brauchen

Zusätzliche Lizenzen laut CISA SCuBA v2.0.0 (Annahme: mindestens E3)

FUNKTION	LIZENZ LAUT QUELLE	KENNUNG
Risikobasierte Richtlinien	Microsoft Entra ID P2	MS.AAD.2
Verwaltete Geräte für Anmeldung und MFA-Registrierung	Microsoft Intune	MS.AAD.3.7, 3.8
Rollen nur bei Bedarf aktivieren, Genehmigung, Warnungen	Microsoft Entra ID P2 oder eine andere PAM-Lösung	MS.AAD.7.4 bis 7.9
Riskante KI-Agenten blockieren	Entra ID P2 und Microsoft Agent 365 oder Microsoft 365 E7	MS.AAD.9.1

Sichere Anlagen, Sichere Links, Schutz vor Identitätswechsel	Defender for Office 365 Plan 1 oder 2 (in E5 enthalten, für E3 als Zusatz)	MS.SECURITYSUITE.1.3, 1.4, 2, 7
Verhinderung von Datenverlust in Teams und auf Geräten	E5 oder eine vergleichbare Drittlösung	MS.SECURITYSUITE.3, 3.5
Eigene Aufbewahrungsrichtlinie für Audit	E5 oder E3 mit Compliance-Zusatz	MS.SECURITYSUITE.5
Audit-Aufbewahrung über 180 Tage	E5, Microsoft Purview Suite oder Zusatz E5 eDiscovery and Audit	MS.SECURITYSUITE.5
Entra-Protokolle an ein externes System senden	unter Umständen ein Azure-Abonnement	MS.AAD.4.1

Welche dieser Funktionen in Ihrem Tarif enthalten sind, etwa in Microsoft 365 Business Premium, steht in den Dienstbeschreibungen von Microsoft; prüfen Sie das vor der Umsetzung. Preise und Lizenzzuschnitte ändern sich laufend und sind nicht Teil dieser Checkliste.

NÄCHSTER SCHRITT

Selbst prüfen oder gemeinsam umsetzen

KOSTENLOS PRÜFEN

Microsoft-365-Domain-Check

tomoris.com/tools/microsoft-365-check

E-Mail-Sicherheits-Check

tomoris.com/tools/email-security-check

DMARC-Generator

tomoris.com/tools/dmarc-generator

UMSETZUNG BESPRECHEN

Kontakt aufnehmen

tomoris.com/contact

contact@tomoris.com

10

Quellen

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

- CISA SCuBA-Baseline Microsoft Entra ID (ScubaGear v2.0.0, 22.10.2026)**
MS.AAD.1 bis 9, Liste hochprivilegierter Rollen, Lizenzanforderungen, gelesen am 25.10.2026
github.com/cisagov/ScubaGear/blob/v2.0.0/PowerShell/ScubaGear/b...
- CISA SCuBA-Baseline Exchange Online (v2.0.0)**
MS.EXO.1 bis 7 und 13, gelesen am 25.10.2026
github.com/cisagov/ScubaGear/blob/v2.0.0/PowerShell/ScubaGear/b...
- CISA SCuBA-Baseline Security Suite (v2.0.0)**
MS.SECURITYSUITE.1 bis 8, Lizenzanforderungen, gelesen am 25.10.2026
github.com/cisagov/ScubaGear/blob/v2.0.0/PowerShell/ScubaGear/b...
- CISA SCuBA-Baseline SharePoint und OneDrive (v2.0.0)**
MS.SHAREPOINT.1 bis 3, gelesen am 25.10.2026
github.com/cisagov/ScubaGear/blob/v2.0.0/PowerShell/ScubaGear/b...
- CISA SCuBA-Baseline Microsoft Teams (v2.0.0)**
MS.TEAMS.1, 2, 4, 5, gelesen am 25.10.2026
github.com/cisagov/ScubaGear/blob/v2.0.0/PowerShell/ScubaGear/b...
- CISA: Secure Cloud Business Applications (SCuBA) Project**
Projekt, ScubaGear als kostenloses Prüfwerkzeug, gelesen am 25.10.2026
www.cisa.gov/resources-tools/services/secure-cloud-business-app...

- | | |
|--|--|
| <p>7 Microsoft Learn: Microsoft-Sicherheitsbewertung (Secure Score)
Einleitung, gelesen am 25.10.2026
learn.microsoft.com/de-de/defender-xdr/microsoft-secure-score</p> <p>9 Microsoft Learn: Legacy-Authentifizierung blockieren
Übersicht, gelesen am 25.10.2026
learn.microsoft.com/de-de/entra/identity/conditional-access/policies</p> <p>11 Microsoft Learn: Automatische externe E-Mail-Weiterleitung
Drei Einstellungen und ihre Wirkung, gelesen am 25.10.2026
learn.microsoft.com/de-de/defender-office-365/outbound-spam-policies</p> <p>13 Microsoft Learn: Bewährte Methoden für Microsoft Entra-Rollen
Nr. 5, weniger als fünf globale Administratoren, gelesen am 25.10.2026
learn.microsoft.com/de-de/entra/identity/role-based-access-control</p> <p>15 Microsoft Learn: Voreingestellte Sicherheitsrichtlinien
Standard, Streng, Integrierter Schutz, gelesen am 25.10.2026
learn.microsoft.com/de-de/defender-office-365/preset-security-policies</p> <p>17 Microsoft Learn: Postfachüberwachung
Standardmäßig aktiviert, gelesen am 25.10.2026
learn.microsoft.com/de-de/purview/audit-mailboxes</p> <p>19 Microsoft Learn: Externer Zugriff in Microsoft Teams
Standard: alle externen Domänen, Zulassungsliste, gelesen am 25.10.2026
learn.microsoft.com/de-de/microsoftteams/trusted-organizations</p> | <p>8 Microsoft Learn: Sicherheitsstandards in Microsoft Entra ID
Inhalt, Zielgruppe, bedingter Zugriff bei P1/P2, gelesen am 25.10.2026
learn.microsoft.com/de-de/entra/fundamentals/security-defaults</p> <p>10 Microsoft Learn: Konten für den Notfallzugriff
Anzahl, Cloudkonten, Authentifizierung, gelesen am 25.10.2026
learn.microsoft.com/de-de/entra/identity/role-based-access-control</p> <p>12 Microsoft Learn: Überwachung aktivieren (Microsoft Purview)
Standardstatus, Ausnahme Business-Tarife, gelesen am 25.10.2026
learn.microsoft.com/de-de/purview/audit-log-enable-disable</p> <p>14 Microsoft Learn: Benutzereinwilligung für Anwendungen
Empfehlung verifizierte Herausgeber, gelesen am 25.10.2026
learn.microsoft.com/de-de/entra/identity/enterprise-apps/config</p> <p>16 Microsoft Learn: SMTP AUTH aktivieren oder deaktivieren
Organisations- und Postfacheinstellung, gelesen am 25.10.2026
learn.microsoft.com/de-de/exchange/clients-and-mobile-in-exchange</p> <p>18 Microsoft Learn: Externe Freigabe in SharePoint und OneDrive
Freigabestufen, gelesen am 25.10.2026
learn.microsoft.com/de-de/sharepoint/turn-external-sharing-on-off</p> |
|--|--|