

Gastzugriff und externe Freigaben härten

Es gibt zwei Sorten von Tenants. In der einen weiß jemand, wie viele Gastkonten existieren. In der anderen erfährt man es zum ersten Mal, wenn ein Auditor danach fragt – und die Zahl ist dann vierstellig, obwohl die Firma dreistellig viele Beschäftigte hat.

Das ist kein Zufall, sondern die logische Folge einer Voreinstellung. Microsoft 365 ist ab Werk auf Zusammenarbeit optimiert, nicht auf Kontrolle. Jeder darf einladen, auch Gäste dürfen Gäste einladen, Links funktionieren ohne Ablaufdatum, und Föderation mit der halben Welt ist eingeschaltet. Das ist für ein Startup mit vier Leuten eine vernünftige Entscheidung. Für eine Organisation mit Kundendaten, Bauplänen oder Personalakten ist es ein langsam wachsendes Problem, das sich hervorragend darin versteht, keine Symptome zu zeigen. Bis es welche zeigt.

Dieser Beitrag gehört zur Serie [Microsoft 365 Security](#) und behandelt das Handlungsfeld externe Zusammenarbeit: Entra B2B, SharePoint und OneDrive, Teams. Ich gehe die drei Ebenen der Reihe nach durch, sage jeweils, was ab Werk eingestellt ist, was ich stattdessen empfehle, und woran du merkst, dass du es zu streng gedreht hast. Denn das ist die andere Fehlerrichtung, über die selten jemand redet: Eine Freigabeeinstellung, die produktive Arbeit verhindert, wird nicht akzeptiert – sie wird umgangen. Meist über private Cloud-Speicher, und dann ist es wirklich vorbei.

Faktenkasten: Zahlen, die den Rahmen setzen

Die Standardschwelle im Inaktivitätsbericht für Gäste liegt bei 90 Tagen ohne Anmeldung. Wer nie angemeldet war, wird ab Erstellungsdatum gezählt.

Der Basistarif von Microsoft Entra External ID umfasst die ersten 50.000 monatlich aktiven externen Benutzer kostenfrei. Gastkonten kosten dich also in aller Regel kein Geld – was genau der Grund ist, warum niemand aufräumt.

Access Reviews mit automatischer Anwendung sperren abgelehnte Gäste 30 Tage lang und löschen sie danach. Nach der Löschung bleiben sie weitere 30 Tage wiederherstellbar.

Ein Team-Gast wartet im ungünstigen Fall bis zu zwölf Stunden, bis der Zugriff wirklich greift. Umgekehrt verlieren Gäste den Zugriff nach einer Verschärfung typischerweise innerhalb einer Stunde.

In Teams-Zugriffsrichtlinien sind Allow- und Blocklisten auf 100 Domänen je Richtlinie begrenzt. Der Domänenfilter in SharePoint verkraftet bis zu 5.000 Einträge.

Vier Türen, vier Schlösser, vier Schlüsselerhalter

Bevor irgendjemand an Schaltern dreht, muss klar sein, worüber wir reden. „Externer Zugriff“ ist in Microsoft 365 kein einzelner Mechanismus, sondern vier grundsätzlich verschiedene, die sich in einem Punkt entscheidend unterscheiden: ob am Ende ein Objekt in deinem Verzeichnis liegt, das du prüfen, ablaufen lassen und löschen kannst.

Vier Türen führen aus deinem Tenant nach draußen

Jede Tür hat ein eigenes Schloss – und einen eigenen Schlüsselverwalter.

Gastzugriff Entra B2B	Shared Channel B2B Direct Connect	External Access Föderation, Chat und Meeting	Anyone-Link unauthentifizierte Freigabe
Konto im Verzeichnis ja, UserType = Guest	Konto im Verzeichnis nein	Konto im Verzeichnis nein	Konto im Verzeichnis nein, niemand
Steuerung External Collaboration Settings	Steuerung Cross-Tenant Access Settings	Steuerung Teams Admin Center, Allowlist	Steuerung SharePoint Admin Center
Zugriff auf Teams, Sites, Dateien, Apps	Zugriff auf genau einen Kanal	Zugriff auf Chat, Anruf, Besprechung	Zugriff auf Datei oder Ordner, weiterleitbar
Ablauf Access Reviews, Gast-Ablauf	Ablauf Kanal-Mitgliedschaft entfernen	Ablauf kein Ablauf, nur Domänenliste	Ablauf Link-Ablauf in Tagen, Passwort

Merksatz:

Nur die erste Tür hinterlässt ein Konto, das du prüfen, ablaufen lassen und löschen kannst. Die anderen drei hinterlassen Protokolleinträge – und sonst nichts.

Skizze 1: Die vier Wege nach draußen – und was sie im Verzeichnis hinterlassen.

Diese Unterscheidung ist nicht akademisch. Sie entscheidet darüber, welches Admin Center zuständig ist, welche Lizenz du brauchst, und ob es überhaupt eine Aufräumfunktion gibt. Wer alles über einen Kamm schert, konfiguriert am Ende drei der vier Türen gar nicht.

Weg	Konto in deinem Verzeichnis	Steuerung liegt bei	Typische Fehlanwendung
Gastzugriff (Entra B2B)	Ja, UserType = Guest	External Collaboration Settings, Cross-Tenant Access, Access Reviews	Für eine einzelne Besprechung angelegt und nie wieder angefasst
Shared Channel (B2B Direct Connect)	Nein	Cross-Tenant Access Settings, beidseitig	Gar nicht genutzt, weil niemand die Cross-Tenant-Einstellungen kennt
External Access (Föderation)	Nein	Teams Admin Center, Föderationskonfiguration	Offen für alle Domänen, weil es die Voreinstellung ist
Anyone-Link (unauthentifziert)	Nein, gar kein Identitätsbezug	SharePoint Admin Center, Tenant- und Site-Ebene	Als Standard-Linktyp gesetzt, „damit es einfacher ist“

Der Entscheidungsbaum, der dir Arbeit spart

Die meisten Gastkonten in einem mittelständischen Tenant hätten nie entstehen müssen. Sie sind das Ergebnis der Frage „Wie kriege ich den schnell rein?“ statt der Frage „Was braucht der eigentlich?“. Vier Fragen, in dieser Reihenfolge gestellt, reduzieren den Bestand um einen erheblichen Anteil.

Welchen Weg nach draußen nimmst du? Vier Fragen, vier Antworten

In dieser Reihenfolge fragen – nicht in der Reihenfolge, in der es jemand eilig hat.

1

Braucht die Person nur Chat, Anruf oder eine Besprechung?

External Access mit Allowlist. Kein Konto, kein Dateizugriff, keine Nachpflege.

2

Arbeitet sie dauerhaft in genau einem Kanal mit?

Shared Channel über B2B Direct Connect. Sie bleibt in ihrem Tenant, unter ihren Richtlinien.

3

Braucht sie ein ganzes Team, eine Site oder mehrere Dateien?

Gastkonto in Entra B2B – mit Ablaufdatum und Access Review von Tag eins an.

4

Ist es genau eine Datei für genau eine Person?

Link für „Bestimmte Personen“. Anyone-Link nur, wenn die Empfängerseite technisch nichts anderes kann.

Der teuerste Fehler:

Für Frage 1 ein Gastkonto anzulegen. Fünf Minuten gespart, drei Jahre Karteileiche im Verzeichnis.

Skizze 2: Vier Fragen, die vor jeder externen Einladung zu klären sind.

Tipp: Shared Channels sind unterschätzt

Ein Shared Channel über B2B Direct Connect ist in vielen Partnerkonstellationen die sauberere Lösung als ein Gastkonto. Die externe Person bleibt in ihrem Heimat-Tenant, unterliegt deren Conditional Access und deren Gerätesteuerung, und du legst nichts an, was du später wieder löschen musst. Der Preis: Es funktioniert nur, wenn beide Organisationen Microsoft Entra nutzen und beide die Cross-Tenant-Einstellungen entsprechend konfigurieren. Bei einem Steuerberater, der auf Google Workspace sitzt, kommst du damit nicht weiter.

Entra B2B: die Eingangskontrolle

Alles, was mit Gastkonten zu tun hat, beginnt an einer einzigen Stelle: den Einstellungen für die externe Zusammenarbeit im Microsoft Entra Admin Center, zu finden unter Externe Identitäten. Vier Blöcke, alle vier ab Werk großzügiger, als die meisten Organisationen es wollen, wenn man sie fragt.

Wer darf einladen

Die Voreinstellung erlaubt jedem im Tenant, Gäste einzuladen – ausdrücklich einschließlich der Gäste selbst. Das ist der Punkt, an dem die meisten Gesprächsrunden kurz still werden. Ein Gast, den du für ein Projekt eingeladen hast, darf seinerseits Leute einladen, die du nie gesehen hast, und die dann in deinem Verzeichnis stehen.

Stufe	Was sie bedeutet	Wann sie passt
Jeder in der Organisation, einschließlich Gästen	Voreinstellung. Auch Gastkonten dürfen weitere Gäste einladen.	Kleine Organisation ohne Compliance-Anforderungen. Sonst: nein.
Mitgliedsbenutzer und	Interne Beschäftigte dürfen einladen,	Der pragmatische Standard für die

bestimmte Administratorrollen	Gäste nicht mehr.	meisten Häuser.
Nur bestimmte Administratorrollen	Nur „Benutzeradministrator“ und „Gasteinladender“ (Guest Inviter) dürfen.	Regulierte Umgebungen, Behörden, alles mit Nachweispflicht.
Niemand, auch keine Administratoren	Einladungen sind vollständig aus. Bestehende Gäste bleiben.	Übergangszustand während einer Aufräumaktion, kein Dauerzustand.

Der mittlere Weg ist in der Praxis fast immer der richtige: Gäste dürfen nicht mehr einladen, Beschäftigte schon. Wer strenger fahren will, ohne den Helpdesk zu fluten, stellt auf „nur bestimmte Administratorrollen“ und verteilt die Rolle **Gasteinladender** gezielt an die Personen, die es tatsächlich brauchen – Projektleitung, Assistenz, Vertriebsinnendienst. Diese Rolle darf ausschließlich einladen und sonst nichts. Sie ist eine der wenigen Entra-Rollen, die man ohne Bauchschmerzen breit verteilen kann, und sie erspart dir die Diskussion, ob jemand „mal eben“ Benutzeradministrator wird. Wie sich das in eine Gesamtrollenstruktur einfügt, steht in der [Tenant-Härtung: die 20 wichtigsten Schrauben](#).

Warnung: Die Einladung ist nur die halbe Miete

Wer einladen darf, ist eine Frage. Wer Zugriff gewähren darf, ist eine andere. Ein Team-Besitzer kann einen bereits vorhandenen Gast jederzeit in sein Team holen, ganz ohne Einladungsrecht. Und jeder, der Vollzugriff auf eine Bibliothek hat, kann Inhalte freigeben. Die Einladungsbeschränkung verhindert also neue Konten, nicht neue Zugriffe. Beides muss zusammen betrachtet werden, sonst hast du ein sehr sauber kontrolliertes Verzeichnis mit sehr unkontrolliert verteilten Berechtigungen.

Was Gäste im Verzeichnis sehen dürfen

Der zweite Block regelt, wie viel ein Gast von deiner Organisation sieht, wenn er erst einmal drin ist. Die Voreinstellung ist ein Mittelweg, der Gästen eingeschränkten Blick auf Eigenschaften und Mitgliedschaften erlaubt – die Mitgliederlisten aller nicht ausgeblendeten Gruppen inklusive.

Einstellung	Sichtbar für den Gast	Nebenwirkung
Gleicher Zugriff wie Mitglieder	Verzeichnisdaten wie für interne Beschäftigte	Dein komplettes Adressbuch bei einem Partner. Praktisch nie sinnvoll.
Eingeschränkter Zugriff auf Eigenschaften und Mitgliedschaften	Voreinstellung. Keine Aufzählung von Benutzern und Gruppen, aber Mitgliedschaften nicht ausgeblendeter Gruppen sind sichtbar.	Guter Kompromiss, wenn Gäste in Teams mitarbeiten sollen.
Zugriff nur auf eigene Verzeichnisobjekte (restriktivste Stufe)	Nur das eigene Profil. Keine anderen Profile, Gruppen, Mitgliedschaften.	Kann Personenauswahl und einzelne Team-Funktionen für Gäste spürbar verschlechtern. Vorher testen, nicht freitagnachmittags ausrollen.

Domänen erlauben oder blockieren

Unter „Einschränkungen für die Zusammenarbeit“ liegt eine Allow- oder Blockliste für Domänen. Sie ist ein Entweder-oder: entweder du führst auf, mit wem Einladungen erlaubt sind, oder du führst auf, mit wem nicht. Beides gleichzeitig geht nicht, und das ist auch gut so, weil die Kombination unweigerlich zu Streit über die Auswertungsreihenfolge führen würde.

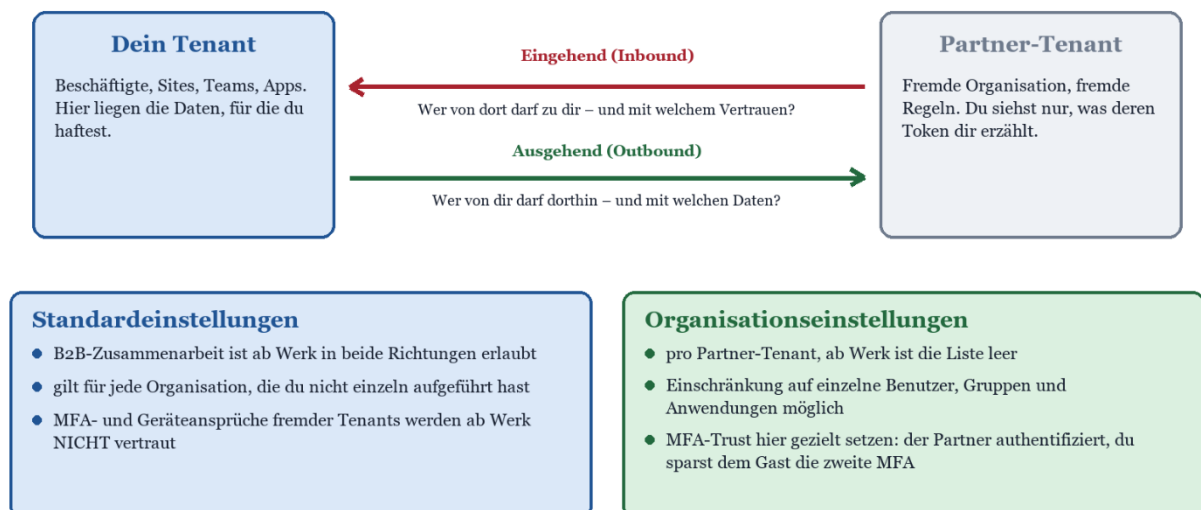
Eine Allowliste ist stark, aber pflegeintensiv und in einer Organisation mit wechselnden Projektpartnern schnell ein Ticket-Generator. Eine Blockliste ist schwächer, aber sinnvoll für Fälle, in denen ein bestimmter Wettbewerber oder ein ehemaliger Dienstleister ausdrücklich draußen bleiben soll. Wichtig: Diese Liste wirkt auf Entra-Einladungen und damit auch auf SharePoint-Site-Freigaben und – sobald die B2B-Integration aktiv ist – auf Datei- und Ordnerfreigaben. Der Domänenfilter im SharePoint Admin Center ist eine zweite, davon getrennte Liste. Wer nur eine von beiden pflegt, wundert sich später über inkonsistente Ergebnisse.

Cross-Tenant Access Settings: der Schalter, den kaum jemand kennt

Die Einstellungen für den mandantenübergreifenden Zugriff sind der modernere und deutlich präzisere Hebel. Sie trennen zwei Richtungen: eingehend, also wer aus fremden Entra-Organisationen zu dir darf, und ausgehend, also wohin deine Leute als Gäste dürfen. Beides lässt sich auf einzelne Benutzer, Gruppen und Anwendungen einschränken.

Cross-Tenant Access Settings: zwei Richtungen, zwei Ebenen

Standardeinstellungen gelten für alle. Organisationseinstellungen schlagen sie.



Skizze 3: Eingehend, ausgehend, Standard- und Organisationseinstellungen.

Der praktisch wertvollste Punkt darin ist der MFA-Trust. Ab Werk vertraut dein Tenant den Multifaktor-Ansprüchen fremder Organisationen **nicht**. Wenn deine Conditional-Access-Richtlinie also MFA für Gäste verlangt – und das sollte sie –, dann muss ein Gast, der sich in seinem eigenen Haus längst stark authentifiziert hat, bei dir noch einmal eine zweite Methode registrieren. Das ist der häufigste Grund, warum Gastzugriff als „kompliziert“ gilt. Für Partner, denen du organisatorisch vertraust, setzt du in den Organisationseinstellungen den MFA-Trust – und der Gast kommt mit dem MFA aus seinem Heimat-Tenant durch. Dieselbe Mechanik gibt es für Ansprüche zu konformen und Entra-hybrid eingebundenen Geräten. Wie du die dazugehörige Richtlinienseite baust, steht in [Conditional Access: Baselines, die nicht nerven](#); die Grundlagen zur Methodenwahl in [MFA in Microsoft 365 richtig einführen](#).

Wichtig: MFA-Trust ist eine Vertrauensentscheidung, keine Bequemlichkeit

Wenn du den MFA-Trust setzt, verlässt du dich darauf, dass der Partner-Tenant sein MFA ordentlich betreibt – dass dort keine SMS-Methode als einziger Faktor läuft, dass Break-Glass-Konten nicht als

Alltagskonten missbraucht werden, dass kompromittierte Konten zeitnah gesperrt werden. Bei einem Konzern mit eigenem SOC ist das eine vertretbare Annahme. Bei einem Zweimannbüro, das Microsoft 365 Business Basic bei einem Reseller gebucht hat, ist es Wunschdenken. Setze den Trust je Organisation, nie global.

Gast-Ablauf und Access Reviews

Ein Gastkonto ohne Ablaufmechanik ist ein Konto auf Lebenszeit. Das Projekt endet, die Rechnung wird bezahlt, der Kontakt schläft ein – und das Konto bleibt, mit Zugriff auf jedes Team und jede Site, in die es je aufgenommen wurde. Vier Jahre später ist der Mensch dahinter längst bei einem Wettbewerber, aber die E-Mail-Adresse funktioniert vielleicht noch, und der Zugriff funktioniert ganz sicher noch.

Lebenszyklus eines Gastkontos – mit Ablaufdatum statt Ewigkeitsgarantie

Ohne Schritt 4 bis 7 endet jeder Tenant als Museum ehemaliger Projektpartner.



Skizze 4: Vom Einladen bis zum Löschen – mit Rückkehrpfad für aktive Gäste.

Der Einstieg ist der Bericht zu inaktiven Gästen im Bereich ID Governance. Er zeigt Gesamtzahl, Verteilung nach Tagen seit der letzten Anmeldung und – die unangenehmste Kennzahl – wie viele Gäste sich *nie* angemeldet haben. Diese Gruppe ist meist überraschend groß: Einladungen, die im Spamfilter der Gegenseite hängen blieben, Kollegen, die den Link nie geöffnet haben, Adressen mit Tippfehler. Alles Konten, die dir nichts nützen und trotzdem in jeder Zugriffsliste auftauchen. Der Bericht lässt sich exportieren, was für die Erstinventur die schnellste Variante ist. Für die Geschäftsführung ist genau dieser Export übrigens die eine Zahl, die ohne Erklärung wirkt – dazu passt [Security-Reporting für die Geschäftsführung](#).

Der Betrieb läuft dann über Access Reviews. Zwei Muster haben sich bewährt, und sie schließen einander nicht aus:

Muster	Prüfende Instanz	Ergebnis bei Ablehnung	Aufwand
Selbstauskunft mit zweiter Stufe	Erste Stufe: der Gast selbst. Zweite Stufe: Gruppenbesitzer oder benannte Person.	Anmeldung 30 Tage gesperrt, danach Löschung aus dem Tenant	Mittel. Braucht Kommunikation, liefert aber die belastbarste Begründung.
Inaktivitätsprüfung ohne Menschen	Formal eine prüfende Person, die bewusst nicht reagiert; „Ergebnisse	Identisch: 30 Tage Sperre, dann Löschung	Niedrig. Läuft nach der

	automatisch anwenden“ und „bei fehlender Antwort: Zugriff entziehen“.		Einrichtung von allein.
--	---	--	-------------------------

Beim zweiten Muster gibt es eine eingebaute Höflichkeit, die man kennen sollte: Die Inaktivitätsprüfung ignoriert Konten, die jünger sind als die konfigurierte Inaktivitätsfrist. Wer 90 Tage einstellt, löscht also keinen Gast, der vor 20 Tagen eingeladen wurde und noch nicht dazu kam, sich anzumelden. Jeder bekommt mindestens eine faire Chance.

Warnung: Access Reviews sind lizenzpflichtig

Die hier beschriebenen Funktionen – Inaktivitätsberichte für Gäste, Reviews mit Inaktivitätsfilter, mehrstufige Reviews, Empfehlungen anhand des letzten Anmeldezeitpunkts – setzen Microsoft Entra ID Governance beziehungsweise die Entra Suite voraus. Entra ID P2 allein deckt Access Reviews in ihrer Grundform ab, aber nicht die Ausbaustufen. Prüfe das vor der Konzeption, nicht danach. Es ist ausgesprochen unangenehm, einen fertigen Governance-Prozess vorzustellen und dann zu erfahren, dass die Lizenzen dafür nicht eingekauft sind.

Wenn die Lizenz fehlt, bleibt der manuelle Weg: eine dynamische Gruppe auf **userType -eq "Guest"**, ein Quartalstermin im Kalender, eine Liste aus dem Verzeichnis, und ein Mensch, der Gruppenbesitzer anschreibt. Unbequem, aber deutlich besser als nichts. Und ehrlicherweise: Der Prozess ist ohnehin die schwierigere Hälfte, die Lizenz automatisiert nur die Ausführung.

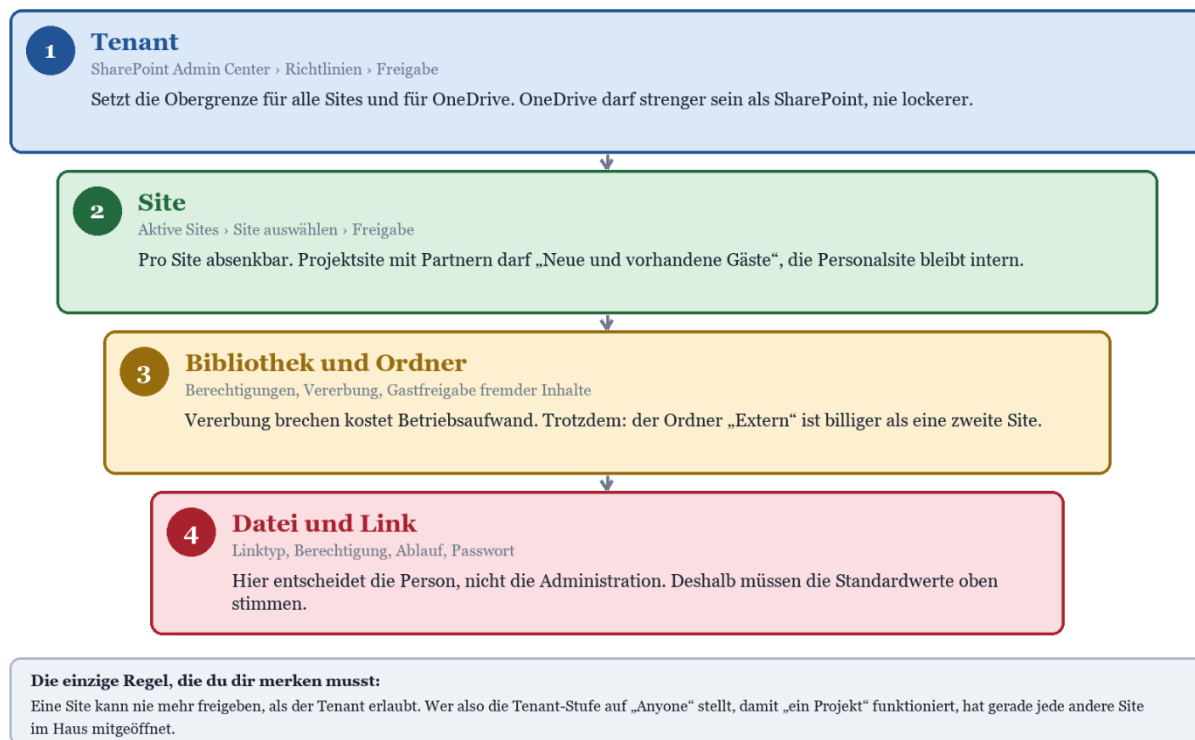
Ergänzend lohnt der Blick auf die Einstellung zum Selbstaustritt externer Benutzer. Ist sie aktiv, können Gäste deine Organisation eigenständig verlassen, ohne dass jemand ein Ticket schreibt. Sie setzt voraus, dass du Datenschutzinformationen im Tenant hinterlegt hast – ohne die ist der Schalter gar nicht verfügbar. Ein kleiner Punkt, der in Datenschutzgesprächen überdurchschnittlich gut ankommt.

SharePoint und OneDrive: die Kaskade der Freigabestufen

Hier liegt der eigentliche Hebel, denn hier liegen die Dokumente. Und hier ist die Mechanik am ehesten missverständlich, weil vier Ebenen ineinandergreifen und jede Ebene nur in eine Richtung wirken darf.

Freigabestufen: vom Tenant bis zum einzelnen Dokument

Jede Ebene darf strenger sein als die Ebene darüber. Lockerer darf keine.



Skizze 5: Die Freigabekaskade – jede Ebene darf nur strenger werden, nie lockerer.

Die vier Stufen auf Tenant- und Site-Ebene

Im SharePoint Admin Center unter Richtlinien und dann Freigabe stehen vier Stufen zur Wahl. Sie gelten für SharePoint und – separat einstellbar, aber niemals lockerer – für OneDrive.

Stufe	Was möglich ist	Bewertung
Jeder (Anyone)	Links, die ohne jede Anmeldung funktionieren. Weiterleitbar, nicht personenbezogen nachvollziehbar.	Nur mit Ablauf, Passwort und Ansichtsbeschränkung, und möglichst nicht auf Tenant-Ebene, sondern gezielt auf einer dafür gebauten Site.
Neue und vorhandene Gäste	Empfänger müssen sich mit Geschäfts-, Schul- oder Microsoft-Konto anmelden oder einen Bestätigungscode eingeben. Es entsteht ein Gastkonto.	Der sinnvolle Tenant-Standard für die meisten Organisationen. Jeder Zugriff hat eine Identität und taucht im Audit auf.
Vorhandene Gäste	Freigabe nur an Gäste, die bereits im Verzeichnis stehen.	Gut für Häuser mit kontrolliertem Onboarding-Prozess, in denen Einladungen zentral laufen. Erhöht die Last auf den Einladungsprozess.
Nur Personen in deiner Organisation	Externe Freigabe ist aus.	Richtig für OneDrive in vielen Häusern, richtig für Sites mit Personal-, Rechts- oder Vorstandsinhalten.

Die entscheidende Regel steht in keiner Oberfläche fett gedruckt: Die Tenant-Stufe ist die Obergrenze. Eine einzelne Site darf strenger sein, nie lockerer. Wer also die Tenant-Einstellung auf „Jeder“ hochdreht, weil ein einziges Projekt unauthentifizierte Links braucht, hat damit nicht dieses Projekt freigeschaltet, sondern die Möglichkeit für jede Site im Haus. Der saubere Weg

lautet: Tenant auf „Neue und vorhandene Gäste“, und die eine Projektsite, die wirklich Anyone-Links braucht, bekommt – nein, auch das geht nicht, weil die Site nicht über den Tenant hinaus darf. Genau das ist der Punkt, an dem ehrliche Beratung nötig wird: Entweder du hebst den Tenant an und senkst konsequent jede Site einzeln ab, oder du verzichtest auf unauthentifizierte Links. Ein bequemer dritter Weg existiert nicht.

Tipp: Absenken lässt sich delegieren, Anheben nicht

Wenn du den Tenant doch auf „Jeder“ setzen musst, dann setze im selben Arbeitsgang alle bestehenden Sites per PowerShell auf die restriktivere Stufe herunter und lege für neue Sites einen Bereitstellungsprozess fest, der die Freigabestufe direkt mitsetzt. Eine manuell gepflegte Ausnahmeliste hält keine zwei Quartale.

Anyone-Links zähmen: Ablauf, Passwort, Berechtigung

Wer unauthentifizierte Links zulässt, hat drei Stellschrauben, und alle drei sollten gesetzt sein. Erstens ein erzwungener Ablauf in Tagen. Zweitens die Beschränkung auf reine Ansicht, sofern der Anwendungsfall nichts anderes verlangt. Drittens ein Passwort, das ausschließlich für anonyme Links zur Verfügung steht und dem Empfänger auf einem anderen Kanal mitgeteilt werden muss.

Stellschraube	Wirkung	Empfehlung
Ablauf in Tagen	Beim Verkürzen werden bestehende Links auf den neuen, kürzeren Wert gezogen. Beim Verlängern behalten bestehende Links ihren alten Wert.	30 Tage auf Tenant-Ebene, 7 bis 14 Tage auf Sites mit sensiblen Inhalten. Das Verkürzen wirkt rückwirkend – ein seltener Glücksfall.
Berechtigung des Links	Anyone-Links lassen sich auf „Ansicht“ beschränken.	Standard auf Ansicht. Ausnahme: Dateianforderungen brauchen Bearbeiten oder Hochladen, sonst funktionieren sie nicht.
Passwortschutz	Nur für anonyme Links verfügbar, Passwort muss separat übermittelt werden.	Für alles, was den Namen eines Kunden trägt. Und bitte nicht in derselben E-Mail.
Ablauf des Gastzugriffs je Site	Gäste verlieren nach einer festgelegten Anzahl Tage den Zugriff auf die Site oder das OneDrive.	Ergänzt die Access Reviews auf Inhaltsebene. Besonders wirksam bei Projektsites mit klarem Enddatum.
Erneute Authentifizierung bei Bestätigungscode	Wer sich per Code angemeldet und „angemeldet bleiben“ gewählt hat, muss nach N Tagen erneut beweisen, dass er das Postfach noch erreicht.	Bei aktiver B2B-Integration greift stattdessen die Entra-Einstellung zum Einmalkennwort. Beide kennen, eine pflegen.

Der Standard-Linktyp ist der stillste und wirksamste Schalter von allen. Er bestimmt, was voreingestellt ist, wenn jemand auf „Teilen“ klickt – und die Mehrheit klickt auf „Kopieren“, ohne den Typ anzusehen. Steht dort „Jeder mit dem Link“, dann ist das die faktische Freigabepaxis deines Hauses, unabhängig von jeder Richtlinie im Intranet. Setze ihn auf „Bestimmte Personen“. Der Nutzungsverlust ist gering, der Gewinn an Nachvollziehbarkeit erheblich – und es ist eine der wenigen Maßnahmen, die im [Secure Score: sinnvoll nutzen statt Punktejagd](#) Punkte bringt und gleichzeitig wirklich etwas ändert.

Warnung: Anyone-Links sind der bevorzugte Exfiltrationsweg

Ein Angreifer, der ein Konto übernommen hat, braucht keine Malware, um Daten herauszuziehen. Er erzeugt Anyone-Links auf die interessanten Bibliotheken und ruft sie später von einer beliebigen

Adresse ab – ohne Anmeldung, ohne Conditional Access, ohne Geräteprüfung. Genau deshalb gehört „ungewöhnlich viele externe Freigaben in kurzer Zeit“ in die Alarmierung. Wie du solche Fälle erkennst und abräumst, steht in der Aufarbeitung eines kompromittierten Kontos.

Weiter: [Kompromittiertes Konto erkennen und aufräumen](#) sowie [Alert Policies und Benachrichtigungen richtig aufsetzen](#).

Der Stichtag: SharePoint-Authentifizierung wandert nach Entra B2B

Das ist die Änderung, die 2026 die meisten Rückfragen produziert hat. SharePoint und OneDrive kannten historisch zwei Freigabemodelle: die eigene SharePoint-Authentifizierung mit Einmalkennwort, bei der für Datei- und Ordnerfreigaben kein Gastkonto entstand, und die Integration mit Entra B2B, bei der immer ein Gastkonto angelegt wird und die Entra-Einstellungen greifen.

Dieses Nebeneinander endet. Die Integration wird für alle Tenants ausgerollt, ein Abwählen ist nicht vorgesehen, und den Zeitpunkt bestimmen die Rollout-Systeme, nicht du. Das manuelle Vorziehen war bis Ende April 2026 möglich. Der harte Punkt kommt danach: Externe, für die kein Entra-B2B-Gastkonto existiert, sehen ab Juli 2026 eine Zugriffsverweigerung auf zuvor geteilte Inhalte.

Wichtig: Was du dazu konkret tun solltest

Der Freigabebericht auf Site-Ebene listet Gäste, die über die alte SharePoint-Authentifizierung eingeladen wurden und noch kein Entra-B2B-Gastkonto haben. Die Spalte mit der E-Mail-Adresse ist deine Arbeitsliste.

Für diese Personen kannst du das Gastkonto vorab im Verzeichnis anlegen; dann bleiben alle bisherigen Links funktionsfähig. Alternativ entsteht das Konto automatisch, sobald erneut etwas mit ihnen geteilt wird.

Doppelte Konten entstehen dabei nicht: Existiert bereits ein B2B-Gastkonto für die Adresse, wird es verwendet.

Bereits geteilte Links müssen nicht neu verschickt werden, solange ein Gastkonto vorhanden ist.

Einmalkennwörter verschwinden nicht – sie sind weiterhin die Standardmethode für Gäste, nur eben in Entra statt in SharePoint.

Anyone- beziehungsweise anonyme Links sind von der Umstellung nicht betroffen. Das ist die schlechte Nachricht in einer guten: Ausgerechnet der ungeschützteste Weg bleibt, wie er war.

Praktisch bedeutet die Umstellung vor allem eines: Deine Entra-Einstellungen zur externen Zusammenarbeit werden jetzt auch für einfache Dateifreigaben scharf geschaltet. Wer bisher eine strenge Einladungsrichtlinie hatte und sich wunderte, warum trotzdem munter Dateien nach draußen gingen, bekommt zum ersten Mal ein konsistentes Bild. Wer umgekehrt seine Entra-Einstellungen nie angefasst hat, wird feststellen, dass jetzt für jede Dateifreigabe ein Verzeichnisobjekt entsteht – und die Gastzahlen entsprechend steigen. Beides ist beabsichtigt.

Vertraulichkeitsbezeichnungen auf Sites

Die eleganteste Steuerung sitzt nicht im SharePoint Admin Center, sondern in Microsoft Purview. Vertraulichkeitsbezeichnungen lassen sich nicht nur auf Dokumente anwenden, sondern auch auf Container – also auf Teams, Microsoft-365-Gruppen und SharePoint-Sites. Eine solche Bezeichnung kann festlegen, ob Gastzugriff auf dem verbundenen Team erlaubt ist und welche

externe Freigabestufe die Site haben darf. Damit wird aus einer technischen Einstellung eine fachliche Entscheidung: Wer eine Site als „Vertraulich – nur intern“ kennzeichnet, hat damit den Gastzugriff abgeschaltet, ohne je ein Admin Center zu öffnen. Das ist genau die Art von Steuerung, die man sich für den Alltag wünscht, und es ist ein eigenes Thema – die Konzeption von Bezeichnungen, Reichweiten und Veröffentlichungsrichtlinien gehört in den [Kompetenzbereich Microsoft Purview](#) und nicht in einen Absatz über Freigabeeinstellungen.

Eine Randbemerkung, die im Betrieb regelmäßig wichtig wird: Wenn du Gastzugriff über Bezeichnungen steuerst, dann steuere ihn *nur* darüber. Zwei parallele Steuerungswege – Bezeichnung hier, manuelle Gruppeneinstellung dort – führen verlässlich zu Fällen, in denen niemand mehr erklären kann, warum ein Team Gäste akzeptiert und das Nachbarteam nicht.

Teams: Gastzugriff, External Access und die Allowlist

Teams ist die Oberfläche, in der externe Zusammenarbeit für die meisten Menschen tatsächlich stattfindet – und gleichzeitig die Stelle, an der die Begriffe am gründlichsten durcheinandergehen. „Gastzugriff“ und „Externer Zugriff“ klingen ähnlich, sind aber zwei völlig verschiedene Funktionen mit verschiedenen Schaltern, verschiedenen Risiken und verschiedenen Zuständigkeiten.

Gastzugriff: ein Schalter für die ganze Organisation

Gastzugriff in Teams ist eine organisationsweite Einstellung. Es gibt keinen Schalter „Gäste erlaubt“ pro Team im Teams Admin Center. Wer ihn einschaltet, schaltet ihn für alle Teams ein – und muss danach differenzieren. Genau dafür sind Vertraulichkeitsbezeichnungen der vorgesehene Weg.

Was ein Gast in Teams darf, ist bewusst eingeschränkt. Er sieht das Etikett „Gast“ hinter seinem Namen, das Team zeigt ein Symbol für die Anwesenheit von Gästen, und eine ganze Reihe von Funktionen bleibt ihm verschlossen. Wichtig für die Erwartungshaltung: Ein Gast muss mindestens einem Team angehören, damit die Gastfunktionen überhaupt zur Verfügung stehen. Und nach dem Hinzufügen kann es bis zu zwölf Stunden dauern, bis der Zugriff vollständig greift – ein Umstand, der bei kurzfristigen Terminen regelmäßig für Aufregung sorgt. Wer am Montagmorgen einen Workshop hat, lädt nicht am Montagmorgen ein.

Verlässt ein Gast das Team von sich aus, bleibt sein Konto im Verzeichnis stehen. Das Entfernen aus dem Team ist keine Kontolöschung. Auch dieser Punkt spricht dafür, den Lebenszyklus über Access Reviews zu regeln statt über die Hoffnung, dass Team-Besitzer aufräumen.

Faktenkasten: Gastlizenzen in Teams

Gastzugriff funktioniert mit Microsoft 365 Business Standard, den Enterprise-Plänen und den Education-Plänen. Eine zusätzliche Microsoft-365-Lizenz je Gast ist nicht nötig; es gilt das Abrechnungsmodell von Microsoft Entra External ID über monatlich aktive Benutzer. Nur Personen von außerhalb deiner Organisation können als Gäste eingeladen werden – interne Konten lassen sich nicht zu Gästen umdeklarieren, um Lizenzkosten zu sparen. Diese Idee kommt in Beratungsgesprächen erstaunlich oft.

External Access: die Allowlist ist die eigentliche Maßnahme

External Access – im Deutschen „Externer Zugriff“, technisch Föderation – regelt Chat, Anrufe und Besprechungen mit Menschen außerhalb deiner Organisation, die Microsoft als Identitätsanbieter

nutzen. Es entsteht kein Konto, es gibt keinen Zugriff auf Teams, Sites oder Dateien. Die Voreinstellung ist: alle externen Domänen erlaubt.

Szenario	Was passiert	PowerShell-Parameter
Alle externen Domänen zulassen	Voreinstellung. Kommunikation mit jeder Organisation, die ihrerseits Föderation erlaubt.	AllowFederatedUsers
Nur bestimmte Domänen zulassen	Allowliste. Alles, was nicht auf der Liste steht, ist blockiert.	AllowedDomains
Bestimmte Domänen blockieren	Blockliste. Alles andere ist erlaubt. Unterdomänen sind dabei nicht automatisch mitblockiert.	BlockedDomains, BlockAllSubdomains
Alle externen Domänen blockieren	Keine Föderation. Externe können weiterhin anonym an Besprechungen teilnehmen, sofern anonymen Zugriff erlaubt ist.	AllowFederatedUsers

Alle vier Szenarien werden über **Set-CsTenantFederationConfiguration** gesetzt. Der Fallstrick mit den Unterdomänen ist der, den ich am häufigsten sehe: Wer contoso.com blockiert, hat marketing.contoso.com nicht blockiert. Der Parameter **BlockAllSubdomains** korrigiert das. Wer eine Blockliste pflegt und diesen Schalter nicht kennt, pflegt im Grunde eine Sammlung von Vorschlägen.

Für eine Allowliste spricht viel, wenn deine externe Kommunikation überschaubar ist – ein Dutzend Lieferanten, drei Kanzleien, zwei Prüfgesellschaften. Sie ist unbequem, wenn Vertrieb und Einkauf ständig mit neuen Häusern sprechen. Ein Kompromiss, den man selten diskutiert: Seit die Föderation auch über Zugriffsrichtlinien granular steuerbar ist, kannst du die Organisation offen lassen und für einzelne Gruppen – Entwicklung, Forschung, Vorstandsbüro – eine eigene Richtlinie mit eigener Domänenliste vergeben. Die Richtlinie schlägt dabei die Organisationseinstellung; die globale Standardrichtlinie selbst lässt sich nicht ändern und erbt immer die Organisationseinstellung.

Unverwaltete Teams-Konten, Skype und Testmandanten

Drei weitere Schalter verdienen Aufmerksamkeit, weil sie Wege eröffnen, an die im Konzept selten jemand denkt.

- Chat mit unverwalteten Teams-Konten, also mit privaten Microsoft-Konten. Praktisch für Kontakte ohne Firmen-Tenant, gleichzeitig ein bequemer Kanal für Social Engineering. Wenn du ihn zulässt, dann zumindest ohne die Erlaubnis, dass die Gegenseite den Kontakt beginnt – dann kann niemand deine Leute per E-Mail-Adresse finden und anschreiben.
- Chat und Anrufe mit Skype-Nutzern. In den meisten Häusern schlicht Altlast. Ausschalten, wenn kein konkreter Anwendungsfall existiert.
- Föderation mit reinen Testmandanten ohne gekaufte Lizenzen ist ab Werk blockiert. Das ist eine gute Voreinstellung, denn ein kostenloser Testmandant ist in Minuten eingerichtet und eignet sich hervorragend als Absender für plausibel wirkende Nachrichten. Lass sie blockiert, außer du hast einen echten Grund.
- Eine Sperrliste für einzelne externe Personen, unabhängig von deren Domäne. Maximal 200 Einträge. Wird jemand aufgenommen, verschwindet er auch aus bestehenden Chats. Nützlich nach einem konkreten Vorfall.

Seit dem Ausbau der Zusammenarbeit zwischen Teams und Defender lassen sich blockierte Domänen auch von der Sicherheitsseite aus pflegen: Ist der entsprechende Schalter im Teams Admin Center aktiv, verwalten Personen mit Sicherheitsadministrator-Rolle die Liste im Defender-

Portal über die Tenant-Allow-Block-Liste. Beide Listen sind dieselbe. Das ist genau dann sinnvoll, wenn die Sicherheitsabteilung im Ernstfall handeln können soll, ohne den Teams-Betrieb zu wecken. Vorausgesetzt wird Defender für Office 365 in Plan 1 oder 2 – siehe [Defender for Office 365: Safe Links und Safe Attachments](#).

Tipp: Der Lobby-Schalter gehört mit auf die Liste

Wer External Access streng konfiguriert und die Besprechungslobby vergisst, hat wenig gewonnen: Auch Personen aus blockierten Domänen können anonym an Besprechungen teilnehmen, solange anonymer Zugriff erlaubt ist. Für sensible Termine gehört die Lobby-Einstellung deshalb zur Härtung dazu – und zwar als eigene Richtlinie für die Personenkreise, die solche Termine tatsächlich halten.

Vom Projekt in den Betrieb

Härtung ist kein Projekt mit Abschlussbericht, sondern ein Rhythmus. Die Einstellungen von heute sind in achtzehn Monaten teils umbenannt, teils durch neue Mechanismen ersetzt, und der Gastbestand wächst in jedem Fall weiter. Was du brauchst, ist ein kleiner, ehrlicher Turnus, den du auch dann durchhältst, wenn gerade nichts brennt.

Was	Wie oft	Wer	Woran du merkst, dass es klemmt
Bericht zu inaktiven Gästen ansehen	Monatlich	Identitätsbetrieb	Der Anteil der Gäste ohne jede Anmeldung steigt – dein Einladungsprozess erzeugt Leichen.
Access Review für Gäste	Quartalsweise, automatisch angewendet	Gruppenbesitzer, Rückfall auf benannte Person	Besitzer klicken pauschal auf „genehmigen“ – dann fehlt die Begründungspflicht.
Freigabeeinstellungen prüfen (Tenant und Sites)	Halbjährlich, zusätzlich nach jeder größeren Änderung durch Microsoft	SharePoint-Betrieb	Neue Sites entstehen mit der Tenant-Standardstufe – dein Bereitstellungsprozess setzt sie nicht mit.
Anyone-Links inventarisieren	Quartalsweise	SharePoint-Betrieb gemeinsam mit Security	Die Zahl steigt, obwohl der Standard-Linktyp „Bestimmte Personen“ ist – jemand hat einen Weg gefunden, den er bequemer findet.
Föderationsliste und Sperrliste durchsehen	Halbjährlich	Teams-Betrieb	Auf der Allowliste stehen Domänen ehemaliger Partner – die Liste wird ergänzt, aber nie gekürzt.
Cross-Tenant-Einstellungen je Partner prüfen	Jährlich und beim Ende jeder Partnerschaft	Identitätsbetrieb	MFA-Trust steht noch für eine Organisation, mit der seit zwei Jahren nichts mehr läuft.

Wer diese sechs Zeilen ernst nimmt, hat mehr für die externe Angriffsfläche getan als mit jedem zusätzlichen Werkzeug. Und wer wissen will, wie sich das in eine größere Ordnung einfügt – Identität, Geräte, Daten, Netz –, findet den Rahmen unter [Zero Trust im Mittelstand: pragmatisch statt dogmatisch](#). Für Organisationen mit Berichtspflichten ist externe Zusammenarbeit außerdem ein Thema mit Prüfrelevanz; welche technischen Maßnahmen dabei erwartet werden, steht in [NIS2 aus Security-Sicht: technische Maßnahmen in M365](#).

Und wenn es doch passiert ist

Externe Freigaben sind selten der Einstiegspunkt eines Angriffs, aber sehr oft der Ausgang. Ein übernommenes Konto erzeugt Links, ein manipulierter Gast greift auf eine Site zu, ein Ordner mit Kundendaten ist plötzlich in einer fremden Suchmaschine auffindbar. Was das im Ernstfall bedeutet und wie schnell die Uhr läuft, ist im Dossier [TerminalFix und der Berlin-Hack](#) nachzulesen. Die ersten Schritte gehören in einen geübten Ablauf – dazu [Incident-Response-Plan für Microsoft 365](#) und, für den akuten Fall, [Phishing-Vorfall: die ersten 60 Minuten](#).

Wenn du diese Themen nicht nebenbei erledigen willst: Bei der Bestandsaufnahme, der Konzeption der Freigabestufen und der Einführung von Access Reviews unterstütze ich in der [Microsoft 365 Security Beratung](#). Wenn dein Team die Zusammenhänge selbst beherrschen soll – und das ist langfristig die bessere Investition –, dann ist die [Schulung Microsoft 365 Security](#) der passendere Weg.

Weiter im Thema

- › [Tenant-Härtung: die 20 wichtigsten Schrauben](#) – der Rahmen, in den dieses Handlungsfeld gehört
- › [Kompetenzbereich Microsoft Purview](#) – Vertraulichkeitsbezeichnungen für Sites, Teams und Dokumente
- › [Conditional Access: Baselines, die nicht nerven](#) – die Richtlinie, die für Gäste MFA verlangt
- › [App-Registrierungen und Consent-Governance](#) – der andere Weg, auf dem Externe an deine Daten kommen
- › [Defender for Cloud Apps im Mittelstand](#) – Übersicht über Freigaben und auffällige Dateiaktivität
- › [Ransomware-Vorsorge in Microsoft 365](#) – warum externe Schreibrechte in der Wiederherstellung wehtun
- › [MFA für SharePoint Online erzwingen](#) – die Ebene unter den Freigabestufen
- › [Security-Monitoring und Betriebsrat: was mitbestimmungspflichtig ist](#) – bevor du Freigabeberichte auswertest

Häufige Fragen

Wie finde ich heraus, wie viele Gastkonten wir überhaupt haben?

Die schnellste Antwort liefert die Gästeseite im Microsoft 365 Admin Center. Die aussagekräftigere kommt aus dem Bericht zu inaktiven Gästen im Bereich ID Governance: Er zeigt nicht nur die Gesamtzahl, sondern die Aufteilung in Gäste, die sich mindestens einmal angemeldet haben, und solche, die es nie taten. Der Export verkraftet bis zu einer Million Konten – eine Grenze, die du hoffentlich nicht brauchst. Rechne damit, dass die Zahl höher ist, als der Bauch sagt. Sie ist es eigentlich immer.

Muss ich für jeden Gast eine Lizenz kaufen?

Nein. Für die Nutzung von Teams, SharePoint und den üblichen Diensten als Gast ist keine zusätzliche Microsoft-365-Lizenz nötig. Es gilt das Abrechnungsmodell von Microsoft Entra External ID nach monatlich aktiven Benutzern, und der Basistarif deckt die ersten 50.000 davon ab. Etwas anderes ist die Governance-Seite: Access Reviews mit Inaktivitätsfilter, mehrstufige Reviews und die Inaktivitätsberichte setzen Entra ID Governance oder die Entra Suite voraus. Die Gäste sind kostenlos, das Aufräumen ist es nicht.

Was ist der Unterschied zwischen Gastzugriff und External Access in Teams?

Gastzugriff bedeutet: Es entsteht ein Konto in deinem Verzeichnis, die Person kann einem Team beitreten, in Kanälen mitarbeiten und auf Dateien zugreifen. External Access bedeutet: Chat, Anruf und Besprechung mit jemandem, der bei sich zu Hause bleibt – kein Konto bei dir, kein Zugriff auf Teams, Sites oder Dateien. Wer nur reden will, braucht kein Gastkonto. Diese eine Unterscheidung spart den meisten Organisationen einen dreistelligen Kontobestand.

Warum muss ein Gast bei uns noch einmal MFA einrichten, obwohl seine Firma längst MFA hat?

Weil dein Tenant den Multifaktor-Ansprüchen fremder Organisationen ab Werk nicht vertraut. Die Lösung heißt MFA-Trust in den Cross-Tenant Access Settings, gesetzt je Partnerorganisation in den Organisationseinstellungen. Danach akzeptiert deine Conditional-Access-Richtlinie das MFA aus dem Heimat-Tenant. Setze ihn bewusst und einzeln – global ist er eine Vertrauenserklärung an jede Organisation der Welt, und die haben nicht alle ein SOC.

Kann ich Gastzugriff nur für bestimmte Teams erlauben?

Nicht über den Teams-Schalter – der gilt organisationsweit. Der vorgesehene Weg führt über Vertraulichkeitsbezeichnungen auf Containern: Eine Bezeichnung legt fest, ob das Team Gäste akzeptiert und welche externe Freigabestufe die verbundene Site haben darf. Damit trifft die fachlich verantwortliche Person die Entscheidung beim Anlegen des Teams, nicht die Administration im Nachhinein. Die Konzeption dazu gehört in den [Kompetenzbereich Microsoft Purview](#).

Was passiert im Juli 2026 mit unseren bestehenden externen Freigaben?

Externe, für die kein Entra-B2B-Gastkonto in deinem Verzeichnis existiert, bekommen ab diesem Zeitpunkt eine Zugriffsverweigerung auf zuvor geteilte Inhalte. Betroffen sind Personen, die über die alte SharePoint-Authentifizierung per Einmalkennwort eingeladen wurden. Der Freigabebericht auf Site-Ebene listet sie auf. Du kannst die Gastkonten vorab anlegen oder die Inhalte erneut teilen, dann entsteht das Konto automatisch. Anonyme Links sind von der Umstellung nicht betroffen, und Einmalkennwörter als Anmeldemethode bleiben erhalten – sie ziehen nur von SharePoint nach Entra um.

Ist es schlimm, wenn wir den Standard-Linktyp auf „Jeder mit dem Link“ lassen?

Ja, und zwar aus einem Grund, der wenig mit Technik zu tun hat: Der Standard-Linktyp ist die faktische Freigabepaxis deines Hauses. Menschen klicken auf „Kopieren“ und prüfen den Typ nicht. Wenn dort „Jeder“ steht, entstehen unauthentifizierte, weiterleitbare Links für Inhalte, für die niemand das je vorgesehen hat – einschließlich der Angebotskalkulation, die dann in der E-Mail-Signaturkette eines Kunden weiterwandert. Setze ihn auf „Bestimmte Personen“. Das ist eine Fünf-Minuten-Änderung mit dem besten Verhältnis von Aufwand zu Wirkung in diesem ganzen Beitrag.

Wir wollen aufräumen. Wo fangen wir an, ohne Betrieb zu stören?

In dieser Reihenfolge: erst messen, dann die Standardwerte für neue Vorgänge korrigieren, dann den Bestand angehen. Konkret: Bericht zu inaktiven Gästen exportieren. Standard-Linktyp und Link-Ablauf setzen. Einladungsrecht von „jeder inklusive Gäste“ auf „Mitgliedsbenutzer“ ziehen.

Föderation von „alle Domänen“ auf eine bewusste Entscheidung bringen. Erst danach den ersten Access Review starten – und den mit Selbstauskunft, nicht mit stiller automatischer Löschung. Wer als erste Amtshandlung 400 Konten löscht, hat am nächsten Tag 400 Tickets und die dauerhafte Reputation, dass Security die Arbeit verhindert.

Reicht es nicht, externe Freigaben einfach ganz abzuschalten?

Wenn deine Organisation tatsächlich nicht extern zusammenarbeitet: ja, und dann tu es. In allen anderen Fällen ist es die Maßnahme mit der höchsten Rückfallquote. Externe Zusammenarbeit verschwindet nicht, wenn du sie im Tenant abschaltest – sie zieht auf private Cloud-Speicher, in E-Mail-Anhänge und auf USB-Sticks um. Dort hast du weder Protokoll noch Ablauf noch Rückholmöglichkeit. Ein kontrollierter Weg nach draußen ist fast immer sicherer als ein verbotener.

Fazit

Gastzugriff und externe Freigaben sind das Handlungsfeld, in dem sich Sicherheit und Arbeitsfähigkeit am unmittelbarsten in die Quere kommen. Genau deshalb funktioniert hier weder die reine Verbotslösung noch das Laufenlassen. Was funktioniert, ist eine bewusste Entscheidung auf jeder der vier Ebenen: welcher Weg nach draußen für welchen Anlass, wer einladen darf, welche Freigabestufe der Tenant und die einzelne Site zulassen, und wann ein Zugang von allein wieder erlischt.

Wenn du aus diesem Beitrag drei Dinge mitnimmst, dann diese. Erstens: Der Standard-Linktyp ist die Einstellung mit dem besten Verhältnis von Aufwand zu Wirkung – fünf Minuten, und die tägliche Freigabepaxis ändert sich. Zweitens: Ein Gastkonto ohne Ablaufmechanik ist ein Konto auf Lebenszeit, und Access Reviews sind der einzige Weg, der nicht auf menschlicher Disziplin beruht. Drittens: Die Umstellung auf Entra B2B für SharePoint-Freigaben macht deine Entra-Einstellungen erstmals für alles scharf – wer sie nie angefasst hat, sollte das jetzt tun, nicht im Sommer nach der ersten Zugriffsverweigerung.

Und wenn dir die Zahl der Gastkonten in deinem Tenant gerade unangenehm ist: Das ist keine Schande, das ist die Voreinstellung. Unangenehm wird es erst, wenn du die Zahl kennst und nichts damit machst.