

MFA für SharePoint Online erzwingen

Es gibt diesen einen Moment in jedem Sicherheitsprojekt, in dem jemand aus der Geschäftsführung fragt: „Wir haben doch MFA, oder?“ Und dann antwortet die IT: „Ja, für die Administration.“ Kurze Pause. „Und für den Rest?“ Noch kürzere Pause. Genau in dieser Pause liegt das Problem, um das es hier geht — denn in SharePoint Online und OneDrive liegen nicht die Administrationskonten, sondern die Verträge, die Personalakten, die Konstruktionszeichnungen und das Angebot, das nächste Woche abgegeben wird.

Die gute Nachricht: SharePoint Online braucht keine eigene MFA-Konfiguration. Die schlechte: Genau deshalb suchen Administratorinnen und Administratoren im SharePoint Admin Center nach einem Schalter, den es dort nicht gibt, finden stattdessen einen ähnlich klingenden — „Zugriff von nicht verwalteten Geräten“ — und stellen ihn auf „eingeschränkt“. Danach ist das Häkchen gesetzt, das Ticket geschlossen und die Anmeldung nach wie vor mit einem einzigen Kennwort möglich. Das ist ungefähr so, als würdest du das Fenster verriegeln und die Haustür offen lassen, weil beides irgendwie mit Gebäudesicherheit zu tun hat.

Dieser Beitrag zeigt, wie du MFA für SharePoint Online und OneDrive wirklich erzwingst: mit einer Conditional-Access-Richtlinie an der richtigen Stelle, mit dem korrekten Verständnis dessen, was App-Enforced Restrictions zusätzlich leisten (und was eben nicht), mit einer belastbaren Antwort auf die Gastzugriffsfrage und mit einer ehrlichen Vorschau darauf, was der OneDrive-Sync-Client und die Office-Apps danach tun. Er gehört in die Reihe [Microsoft 365 Security](#), in der die Bausteine einer Microsoft-365-Absicherung zusammenlaufen.

Warum MFA in SharePoint gar nicht in SharePoint konfiguriert wird

Der wichtigste Satz zuerst: SharePoint Online besitzt keine eigene Anmeldelogik. Es besitzt auch keine Benutzerdatenbank, keine Kennwortrichtlinie und keinen zweiten Faktor. Alles, was mit Authentifizierung zu tun hat, delegiert der Dienst an Microsoft Entra ID. SharePoint bekommt am Ende ein Token gereicht und liest darin nach, was der Benutzer nachgewiesen hat. Wer also „MFA für SharePoint“ konfigurieren will, konfiguriert in Wahrheit Entra ID — und zwar mit einer Zielressource, die SharePoint einschließt.

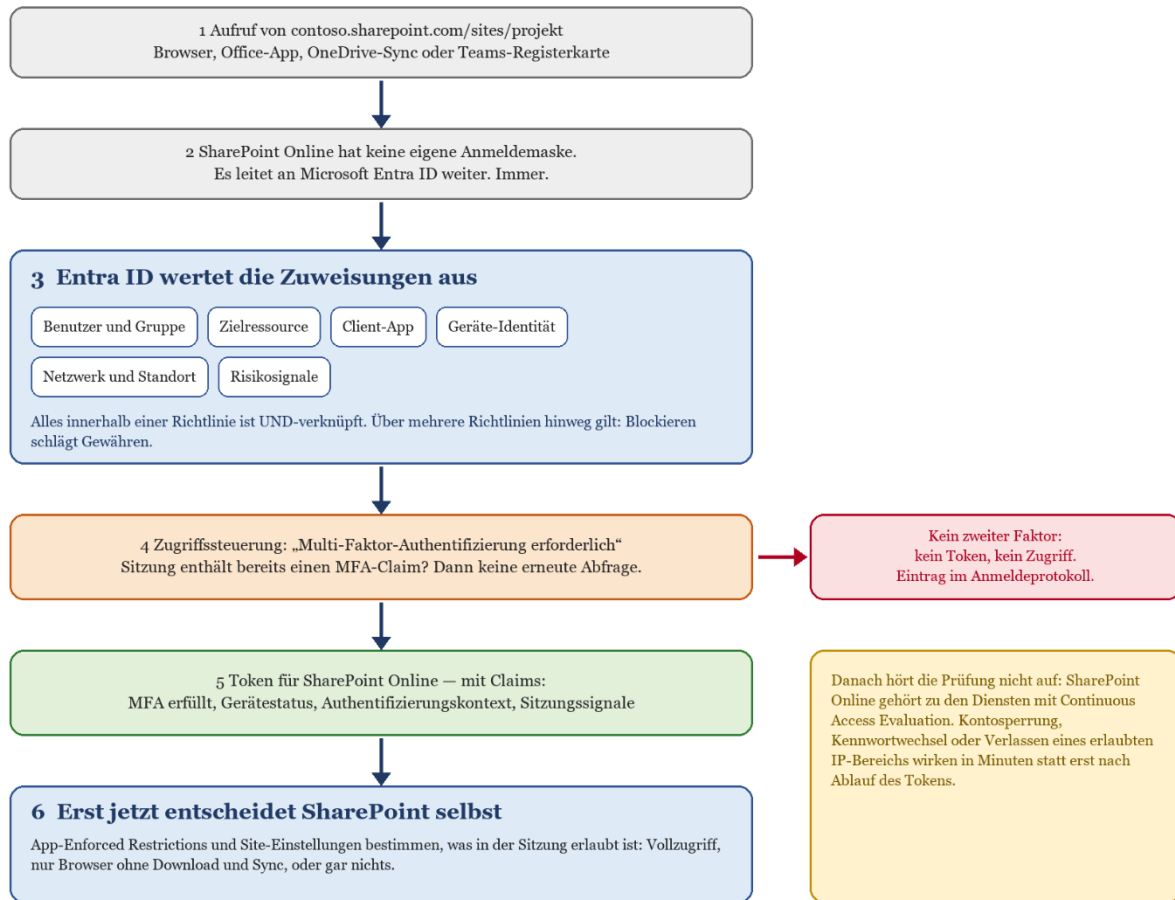
Der Anmeldefluss, Schritt für Schritt

Es lohnt sich, den Ablauf einmal komplett anzuschauen, weil sich daraus fast alle späteren Fehlersuchen von selbst erklären. Wenn jemand eine Website aufruft, passiert Folgendes:

- Der Client fragt die Ressource an, bekommt aber kein Formular, sondern eine Weiterleitung an den Anmeldedienst von Microsoft Entra ID.
- Entra ID sammelt die Sitzungsdetails ein: Benutzer, Gruppe, Rolle, angefragte Zielressource, Client-App, Geräte-Identität, Netzwerkstandort und — mit der passenden Lizenz — Risikosignale.
- Alle passenden Conditional-Access-Richtlinien werden ausgewertet. Innerhalb einer Richtlinie sind die Zuweisungen UND-verknüpft, über mehrere Richtlinien hinweg gewinnt jedes Blockieren.
- Ist MFA gefordert und noch nicht erfüllt, kommt die Aufforderung. Ist sie in der laufenden Sitzung bereits erfüllt, passiert an dieser Stelle gar nichts Sichtbares.
- Entra ID stellt ein Token aus, in dem der MFA-Nachweis, der Gerätestatus und gegebenenfalls der Authentifizierungskontext als Claims stehen.

- Erst jetzt entscheidet SharePoint Online selbst, was in dieser Sitzung erlaubt ist — und genau hier setzen die App-Enforced Restrictions an.

Anmeldefluss SharePoint Online mit Conditional Access



Merksatz: Conditional Access entscheidet, wer die Tür aufbekommt. SharePoint entscheidet, was drinnen erlaubt ist. Das sind zwei Ebenen, keine Alternative.

Skizze 1: Anmeldefluss SharePoint Online mit Conditional Access. Die Authentifizierung passiert in Entra ID, die Feinsteuerung der Sitzung in SharePoint.

Was in SharePoint auffällt, wenn MFA fehlt

SharePoint ist im Schadensfall selten der Einstiegspunkt, aber fast immer die zweite Station. Ein abgephischtes Kennwort führt zuerst ins Postfach, dann in OneDrive, dann in die Teamsites — nicht weil Angreifer besonders kreativ wären, sondern weil die Suche in SharePoint hervorragend funktioniert und „Gehalt“, „Kündigung“ und „Angebot“ genau die Begriffe sind, die dort Treffer liefern. Wer erlebt hat, wie schnell ein einziges kompromittiertes Konto ein Delta-Sync-Protokoll für eine halbe Terabyte an Dokumenten erzeugt, diskutiert danach nicht mehr über den zweiten Faktor.

FAKTEN — Zahlen, die die Diskussion abkürzen

Microsoft beziffert die Wirkung von MFA auf über 99 Prozent verhinderte Kontoübernahmen — eine Zahl, die seit Jahren stabil bleibt und die Grundlage für die Microsoft-verwalteten Richtlinien in Entra ID bildet.

Über 99 Prozent der beobachteten Password-Spray-Angriffe laufen laut Microsofts Analyse über Legacy-Authentifizierungsprotokolle — also über Wege, die MFA konstruktionsbedingt nicht

unterstützen.

Seit Februar 2025 erzwingt Microsoft MFA schrittweise für die Anmeldung am Microsoft 365 Admin Center, seit Oktober 2025 in der zweiten Phase auch für Azure CLI, Azure PowerShell und schreibende Aufrufe der Azure-Verwaltungs-API. Für die Endbenutzeranmeldung an SharePoint Online gilt das ausdrücklich nicht — dafür bist du selbst zuständig.

Der letzte Punkt wird regelmäßig missverstanden. Die verpflichtende MFA von Microsoft betrifft Verwaltungsportale und Verwaltungsschnittstellen, nicht die tägliche Arbeit deiner Belegschaft in SharePoint. Wenn du dich darauf verlässt, dass Microsoft das schon regeln wird, bleibt dein Dokumentenbestand exakt so geschützt wie vorher: durch ein Kennwort, das jemand aus dem Team im Zweifel auch für ein Online-Kochforum benutzt.

Die Grundlagen der Einführung — Methodenwahl, Registrierung, Kommunikation, Rollout in Wellen — behandelt der Beitrag [MFA in Microsoft 365 richtig einführen](#) ausführlich. Hier geht es um die SharePoint-spezifische Ebene darüber.

Die CA-Richtlinie gezielt auf SharePoint Online und OneDrive

Jetzt wird gebaut. Und die erste Entscheidung ist zugleich die folgenreichste: Auf welche Zielressource richtest du die Richtlinie aus? Es gibt drei sinnvolle Antworten und ungefähr fünfzehn, die sich später als Ticketquelle erweisen.

Zielressource: Office 365 statt SharePoint Online allein

Im Auswahldialog findest du sowohl die App-Gruppe „Office 365“ als auch die Einzel-App „Office 365 SharePoint Online“. Der Reflex, möglichst gezielt vorzugehen und nur SharePoint auszuwählen, ist verständlich und in den meisten Fällen falsch. Der Grund heißt Dienstabhängigkeit: Microsoft Teams greift auf SharePoint zu, das Microsoft-365-Portal greift auf SharePoint zu, Power Apps greift auf SharePoint zu, Microsoft Forms greift auf SharePoint zu. Diese Abhängigkeiten werden überwiegend früh gebunden ausgewertet, das heißt: Die SharePoint-Richtlinie muss erfüllt sein, bevor die aufrufende App überhaupt startet.

Wenn du nur SharePoint adressierst, erzeugst du damit ein Verhalten, das dein Helpdesk hassen wird: Teams startet, der Chat funktioniert, die Registerkarte „Dateien“ verlangt plötzlich eine zusätzliche Anmeldung. Technisch korrekt, für Anwenderinnen und Anwender aber vollkommen unerklärlich. Microsoft empfiehlt daher ausdrücklich, für gemeinsame Anforderungen die App-Gruppe „Office 365“ zu verwenden, damit Exchange Online, SharePoint Online und Teams dieselbe Anforderung sehen und die Zahl der Aufforderungen sinkt.

Zielressource	Wann sinnvoll	Nebenwirkung
Office 365 (App-Gruppe)	Der Normalfall für eine MFA-Baseline. Deckt SharePoint, OneDrive, Exchange, Teams und die Portale gemeinsam ab.	Keine. Genau das ist die Empfehlung, weil Dienstabhängigkeiten sauber aufgelöst werden.
Office 365 SharePoint Online (Einzel-App)	Wenn SharePoint und OneDrive strenger behandelt werden sollen als der Rest, etwa mit höherer Authentifizierungsstärke.	Zusätzliche Aufforderungen in Teams, Forms, Power Apps und im Portal. Vorher testen.
Alle Ressourcen	Für die tenantweite MFA-Grundrichtlinie, die ohnehin für alles gelten soll.	Trifft auch Registrierungsvorgänge und Dienstprinzipale — Ausschlüsse gut dokumentieren.
Authentifizierungskontext	Für einzelne, besonders heikle Sites:	Erfordert zusätzliche Lizenzen und

	Vorstand, Personal, Projekt „Nordstern“.	schließt einige Clients aus. Siehe Kapitel 3.
--	--	---

Tabelle 1: Zielressourcen im Vergleich. Die App-Gruppe „Office 365“ ist für die MFA-Baseline fast immer die richtige Wahl.

Dienstabhängigkeiten, die du kennen solltest

Damit die Auswahl nicht abstrakt bleibt: Die folgende Übersicht zeigt, welche Anwendungen SharePoint im Hintergrund mitziehen. Früh gebunden bedeutet, dass die Anforderung vor der Anmeldung an der aufrufenden App erfüllt sein muss. Spät gebunden bedeutet, dass sie erst greift, wenn wirklich ein Token für den nachgelagerten Dienst angefordert wird.

Aufrufende Anwendung	Nachgelagerter Dienst	Bindung
Microsoft Teams	SharePoint, Exchange	früh gebunden
Microsoft Teams	Planner, Stream, Whiteboard	spät gebunden
Microsoft-365-Portal	SharePoint, Exchange, Teams-Dienste	früh gebunden
Power Apps	SharePoint, Exchange, Azure-Verwaltungs-API	früh gebunden
Microsoft Forms	SharePoint, Exchange	früh gebunden
SharePoint	SharePoint Online Web Client Extensibility	früh gebunden

Tabelle 2: Auszug aus den Dienstabhängigkeiten. Wer nur SharePoint adressiert, trifft trotzdem Teams, Forms und Power Apps — nur unvorhersehbarer.

Die letzte Zeile verdient einen Kommentar, weil sie regelmäßig für Verwirrung sorgt: „SharePoint Online Web Client Extensibility“ ist ein interner Dienstprinzipal, über den moderne Seiten und SharePoint-Framework-Erweiterungen ihre Aufrufe abwickeln. Wenn du in den Anmeldeprotokollen Einträge zu dieser Anwendung siehst, ist das kein Angriff, sondern SharePoint beim Rendern der eigenen Startseite.

Die Richtlinie im Detail

Für die Baseline reicht eine überschaubare Konfiguration. Lege sie im Microsoft Entra Admin Center unter Conditional Access an, gib ihr einen Namen, den man am Telefon vorlesen kann, und konfiguriere sie so:

- Benutzer: alle Benutzer einschließen. Ausschließen: die Break-Glass-Konten und, falls vorhanden, das Synchronisierungskonto von Entra Connect.
- Zielressourcen: die App-Gruppe „Office 365“ auswählen.
- Bedingungen: zunächst keine. Standort- und Geräteinschränkungen kommen später, nicht gleichzeitig mit der MFA-Einführung.
- Gewähren: „Zugriff gewähren“ mit „Multi-Faktor-Authentifizierung erforderlich“ oder — besser — mit einer Authentifizierungsstärke.
- Sitzung: vorerst nichts. Anmeldehäufigkeit und Browserpersistenz sind eigene Entscheidungen mit eigenen Nebenwirkungen.
- Zustand: „Nur berichten“. Nicht „Ein“. Noch nicht.

Authentifizierungsstärken sind der lohnendste Detailgewinn an dieser Stelle. Statt pauschal „irgendein zweiter Faktor“ kannst du eine der drei eingebauten Stärken verlangen — Multi-Faktor, kennwortlose MFA oder phishing-resistente MFA — oder eine eigene Kombination definieren. Für den ersten Wurf reicht die eingebaute MFA-Stärke; für Administrationsrollen und besonders schützenswerte Sites lohnt der Sprung zur phishing-resistenten Variante. Wie du dahin kommst, ohne die halbe Belegschaft mit Sicherheitsschlüsseln auszustatten, beschreibt [Passwordless: FIDO2 und Passkeys in der Praxis](#).

TIPP — Report-only ist keine Formalie, sondern die halbe Miete

Lass die Richtlinie mindestens eine volle Arbeitswoche im Zustand „Nur berichten“ laufen. Eine Woche deshalb, weil erst dann die Monatsabschlüsse, die Heimarbeitsstage, das Multifunktionsgerät im Keller und der eine Kollege mit dem Mac in der Auswertung auftauchen.

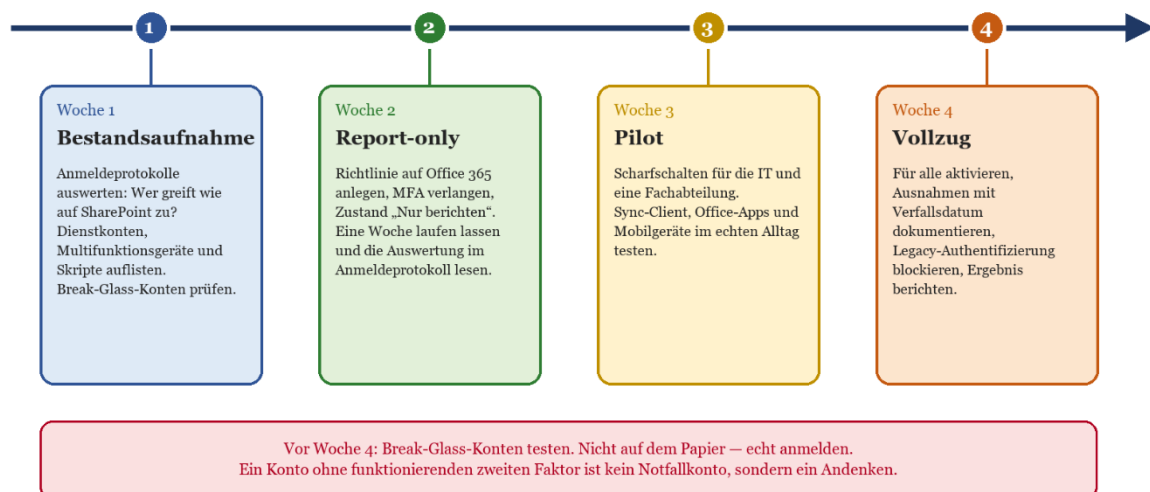
Filtere die Anmeldeprotokolle anschließend nach der Richtlinie und sortiere nach dem Ergebnis. Interessant sind nicht die Erfolge, sondern die Einträge „Fehler“ und „Nicht angewendet“ — dort stehen die Fälle, die dich am Tag des Scharfschaltens anrufen.

Die Registerkarte „Richtlinienauswirkung“ liefert dieselbe Auswertung als Zusammenfassung und eignet sich gut für die Vorlage in der Betriebsbesprechung.

Die Reihenfolge beim Scharfschalten

MFA für SharePoint einzuführen ist selten ein technisches Problem und fast immer ein Terminproblem. Wer am Dienstagvormittag ohne Ankündigung aktiviert, bekommt am Dienstagnachmittag eine sehr direkte Rückmeldung aus dem Vertrieb. Der folgende Fahrplan hat sich bewährt, weil er jede Woche genau eine Frage beantwortet und keine zwei gleichzeitig.

Vier Wochen bis zur erzwungenen MFA für SharePoint Online



Skizze 2: Vier Wochen von der Bestandsaufnahme bis zum Vollzug. Jede Woche beantwortet genau eine Frage.

WARNUNG — Break-Glass-Konten vor dem Scharfschalten testen

Jede Richtlinie, die MFA erzwingt, braucht Ausschlüsse für die Notfallkonten. Das ist keine Bequemlichkeit, sondern Schutz vor der Aussperrung des gesamten Tenants durch eine Fehlkonfiguration.

Ausschluss allein reicht nicht: Seit der verpflichtenden MFA für die Verwaltungsportale müssen auch Notfallkonten stark authentifizieren können. Microsoft empfiehlt dafür ausdrücklich Passkeys nach FIDO2 oder zertifikatbasierte Authentifizierung.

Wie viele Konten du brauchst, wie du sie überwachst und warum sie nicht im selben Safe liegen sollten wie der Serverraumschlüssel, steht in [Break-Glass-Konten anlegen und überwachen](#).

Und noch ein Hinweis zur Wirkzeit: Änderungen an Conditional-Access-Richtlinien und an Gruppenmitgliedschaften brauchen bis zu einen Tag, bis sie in nachgelagerten Diensten wie SharePoint Online vollständig repliziert sind; für Richtlinienänderungen ist die Latenz auf etwa

zwei Stunden optimiert. Wenn eine Änderung sofort greifen muss, widerrufe die Aktualisierungstoken der betroffenen Konten. Wer das nicht weiß, testet zehn Minuten nach der Änderung, sieht das alte Verhalten und beginnt eine Fehlersuche, die es nicht braucht.

Wenn du gerade dabei bist, deine Richtlinienlandschaft insgesamt zu ordnen: Der Beitrag [Conditional Access: Baselines, die nicht nerven](#) beschreibt den Satz von Startrichtlinien, in den diese SharePoint-Regel hineingehört, samt Namenskonvention, Ausnahmeverwaltung und Reihenfolge. Falls dein Tenant noch mit Security Defaults läuft, klärt [Security Defaults oder Conditional Access?](#) zuerst die Frage, ob und wann der Wechsel überhaupt lohnt.

App-Enforced Restrictions gegen Conditional Access

Kommen wir zu der Verwechslung, die diesem Beitrag seinen praktischen Nutzen gibt. Im SharePoint Admin Center gibt es unter „Zugriffssteuerung“ den Eintrag „Nicht verwaltete Geräte“ mit drei Optionen: Vollzugriff zulassen, eingeschränkten webbasierten Zugriff zulassen, Zugriff blockieren. Das sieht nach Sicherheitskonfiguration aus, fühlt sich nach Sicherheitskonfiguration an — und ist auch eine. Nur eben keine Authentifizierung.

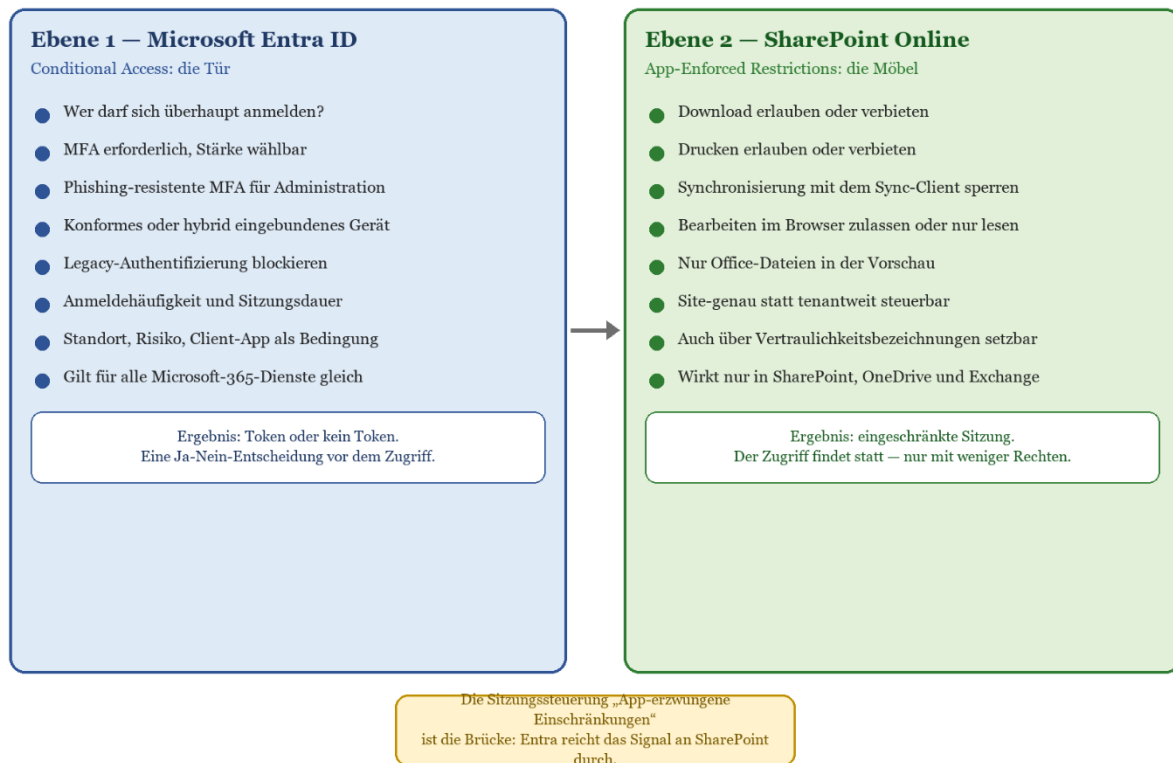
Was App-Enforced Restrictions tatsächlich tun

App-erzwungene Einschränkungen sind eine Sitzungssteuerung in Conditional Access. Entra ID trifft dabei keine eigene Entscheidung über die Sitzung, sondern reicht ein Signal an die Anwendung durch: „Dieser Benutzer kommt von einem nicht verwalteten Gerät.“ Was daraufhin passiert, entscheidet die Anwendung selbst. SharePoint Online, OneDrive und Exchange Online werten dieses Signal aus, andere Dienste nicht.

In SharePoint bedeutet der eingeschränkte Modus konkret: Zugriff nur über den Browser, kein Herunterladen, kein Drucken, keine Synchronisierung und kein Zugriff über Apps einschließlich der Office-Desktopanwendungen. Ob im Browser bearbeitet werden darf, entscheidest du zusätzlich. Anwenderinnen und Anwender sehen dann oben auf der Website einen Hinweiskasten; im blockierten Modus stattdessen die Meldung, dass der Zugriff von einem nicht vertrauenswürdigen Gerät aus abgelehnt wurde.

Der entscheidende Punkt: All das passiert, nachdem sich jemand erfolgreich angemeldet hat. App-Enforced Restrictions verlangen keinen zweiten Faktor. Sie verlangen überhaupt keine bestimmte Authentifizierung. Sie sortieren nur, wie großzügig die Sitzung ausfällt.

Zwei Ebenen: Conditional Access und App-Enforced Restrictions



Skizze 3: Conditional Access entscheidet über den Zutritt, App-Enforced Restrictions über die Möblierung. Beide Ebenen brauchst du.

Kriterium	Conditional Access (MFA)	App-Enforced Restrictions
Wirkt wann?	Vor der Tokenausstellung	Nach der Anmeldung, innerhalb der Sitzung
Wirkt worauf?	Alle Microsoft-365-Dienste, je nach Zielressource	Nur SharePoint, OneDrive und Exchange Online
Fragt einen zweiten Faktor ab?	Ja, das ist der Zweck	Nein, niemals
Verhindert Kontoübernahme?	Ja, das ist der Hauptnutzen	Nein, nur die Folgen auf nicht verwalteten Geräten
Steuerbar je Website?	Nur über Authentifizierungskontexte	Ja, tenantweit und je Site oder OneDrive
Konfigurationsort	Microsoft Entra Admin Center	Entra (Sitzungssteuerung) plus SharePoint Admin Center oder PowerShell
Umgehbar durch Legacy-Clients?	Ja, wenn Legacy-Auth nicht blockiert ist	Ja, ausdrücklich — ältere Clients erzwingen keine gerätebasierten Einschränkungen
Wirkt auf „Jeder“-Links?	Nein, dort meldet sich niemand an	Nein, ausdrücklich nicht

Tabelle 3: Der Unterschied in acht Zeilen. Wer nur die rechte Spalte konfiguriert, hat den Zugriff verfeinert, aber nicht abgesichert.

Die PowerShell-Ebene: tenantweit und je Website

Im Admin Center gilt die Einstellung für die gesamte Organisation. Feiner wird es mit der SharePoint Online Management Shell. Tenantweit setzt du den eingeschränkten Zugriff so:

`Set-SPOtenant -ConditionalAccessPolicy AllowLimitedAccess`

Für einzelne Websites — inklusive der persönlichen OneDrive-Ablagen — geht es gezielter. Wichtig dabei: Die Einstellung auf Site-Ebene muss mindestens so streng sein wie die organisationsweite. Lockerer geht nicht, und das ist auch gut so.

```
$site = "<vollständige Adresse der Website>"
Set-SPOsite -Identity $site -ConditionalAccessPolicy BlockAccess
```

```
Get-SPOsite -IncludePersonalSite $true -Limit all `
    -Filter "Url -like '/personal/'" |
Set-SPOsite -ConditionalAccessPolicy AllowLimitedAccess
```

Die Feinsteuerung erfolgt über zusätzliche Parameter, die sowohl tenantweit als auch je Website gelten. Sie entscheiden darüber, ob dein „eingeschränkter Zugriff“ am Ende produktiv nutzbar bleibt oder ob dein Ticketsystem in Flammen steht.

Parameter	Wirkung	Praxishinweis
-AllowEditing \$false	Bearbeiten von Office-Dateien im Browser wird unterbunden.	Sinnvoll für Archiv- und Nachweisbereiche, unpraktisch für Projektarbeit.
-ReadOnlyForUnmanagedDevices \$true	Die gesamte Website wird für Betroffene schreibgeschützt.	Klare Ansage, wenig Diskussion. Gut für Ablagen mit Revisionscharakter.
-LimitedAccessFileType OfficeOnlineFilesOnly	Nur Office-Dateien lassen sich in der Vorschau öffnen.	Höchste Sicherheit, spürbarster Produktivitätsverlust.
-LimitedAccessFileType WebPreviewableFiles	Standardwert. Vorschau für alle im Web darstellbaren Dateien.	Achtung: PDF- und Bilddateien müssen zum Rendern teils geladen werden — das erzeugt unerwartete Zugriffsfehler.
-LimitedAccessFileType OtherFiles	Auch nicht darstellbare Dateien wie ZIP oder EXE dürfen geladen werden.	Die schwächste Variante. Wer sie braucht, braucht meist einen anderen Ansatz.

Tabelle 4: Die Parameter zu AllowLimitedAccess. Der Standardwert ist produktivitätsfreundlich, nicht sicherheitsmaximal.

WARNUNG — Die zwei Lücken, die alles aushebeln

„Jeder“-Links funktionieren ohne Anmeldung. Wo niemand authentifiziert wird, greift weder MFA noch eine gerätebasierte Einschränkung. Wenn du Conditional Access für SharePoint ernst meinst, deaktivierst du diese Linkart für die betroffenen Sites — sonst ist die gesamte Konstruktion eine sehr aufwendige Dekoration.

Clients ohne moderne Authentifizierung können gerätebasierte Einschränkungen nicht erzwingen und umgehen damit die Richtlinie. Microsoft empfiehlt deshalb, im SharePoint Admin Center zusätzlich „Apps, die keine moderne Authentifizierung verwenden“ zu blockieren.

Wie du Legacy-Protokolle tenantweit loswirst, ohne die Faxsoftware aus dem Jahr 2009 zu übersehen, steht in [Legacy Authentication endgültig abschalten](#).

Authentifizierungskontexte: MFA nur für die heiklen Websites

Es gibt einen dritten Weg, der oft übersehen wird und für den Mittelstand erstaunlich gut passt: Authentifizierungskontexte. Damit kannst du eine Conditional-Access-Richtlinie nicht an eine Anwendung, sondern an eine einzelne SharePoint-Website binden. Der Ablauf ist dreistufig: Kontext in Entra ID anlegen und für Apps veröffentlichen, eine Richtlinie auf diesen Kontext ausrichten, den Kontext anschließend an die Website hängen — entweder direkt per PowerShell oder über eine Vertraulichkeitsbezeichnung.

```
$site = "<vollständige Adresse der Website>"
Set-SPOSite -Identity $site `
    -ConditionalAccessPolicy AuthenticationContext `
    -AuthenticationContextName "Vertrauliche Projekte"
```

Damit lässt sich sauber abbilden, was in Sicherheitsworkshops immer wieder gewünscht wird: MFA für alle, phishing-resistente MFA nur für die Vorstands- und Personalbereiche, Nutzungsbedingungen nur für Gäste auf einer bestimmten Projektsite. Die Steuerung über Vertraulichkeitsbezeichnungen ist dabei die elegantere Variante, weil sie sich in die übrige Klassifizierung einfügt statt daneben zu stehen — mehr dazu im [Kompetenzbereich Microsoft Purview](#).

WICHTIG — Authentifizierungskontexte haben eine echte Ausschlussliste

Der OneDrive-Sync-Client synchronisiert Websites mit Authentifizierungskontext nicht.
 Die SharePoint-Apps für iOS und Android unterstützen Authentifizierungskontexte nicht, ebenso wenig Viva Engage.
 Outlook unter Windows, Mac, Android und iOS kann nicht mit Sites kommunizieren, die durch einen Authentifizierungskontext geschützt sind.
 Der Upload von Aufzeichnungen aus Teams-Kanalbesprechungen schlägt auf solchen Sites fehl; die Terminplanung für Teams-Webinare scheitert, wenn OneDrive einen Kontext trägt.
 Die Stammwebsite des Tenants lässt sich nicht mit einem Authentifizierungskontext versehen.
 Fazit: ein hervorragendes Werkzeug für einzelne, klar abgegrenzte Bereiche — und ein denkbar schlechtes für die Fläche. Teste vor dem Ausrollen, nicht danach.

Gastzugriff und MFA für externe Nutzer

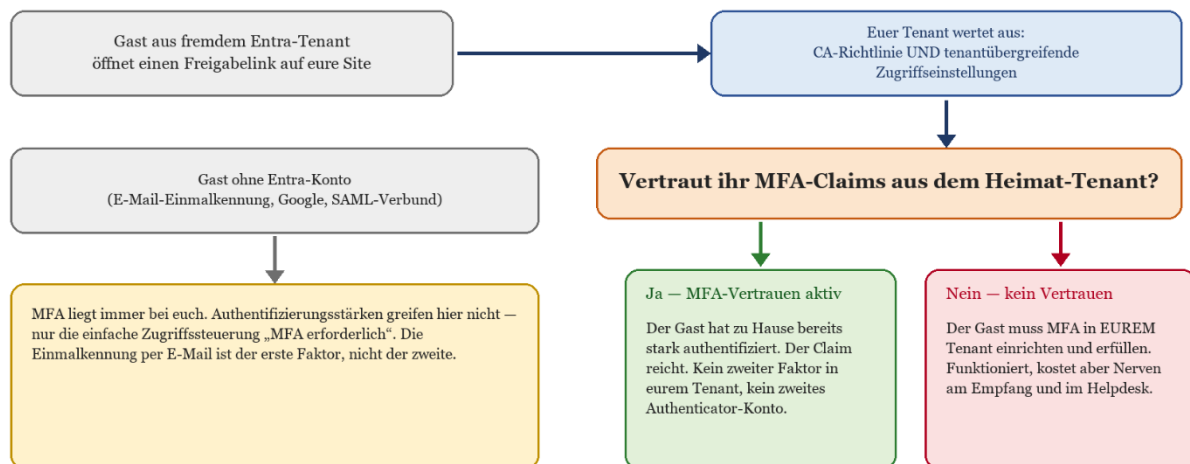
Sobald die interne Richtlinie steht, kommt die Frage, die jedes Projekt einmal aufhält: Was ist mit den Gästen? Der Steuerberater, die Anwaltskanzlei, das Ingenieurbüro, die Werbeagentur — alle haben Zugriff auf mindestens eine Teamsite, und niemand von ihnen gehört zu deinem Tenant. Die kurze Antwort lautet: MFA gilt auch für sie, und du entscheidest, wo sie den zweiten Faktor leisten.

MFA-Vertrauen: der Unterschied zwischen elegant und mühsam

Wenn ein Gast aus einem anderen Entra-Tenant auf deine Ressourcen zugreift, prüft Entra ID zwei Dinge gleichzeitig: deine Conditional-Access-Richtlinien und die tenantübergreifenden Zugriffseinstellungen — die ausgehenden des Heimat-Tenants und die eingehenden deines eigenen. In den eingehenden Einstellungen legst du fest, ob du MFA-Claims und Geräteangaben aus dem fremden Tenant akzeptierst.

Akzeptierst du sie, prüft Entra ID die Anmeldesitzung des Gastes auf einen entsprechenden Claim. Ist er vorhanden, entfällt eine zweite Abfrage. Akzeptierst du sie nicht, muss der Gast MFA in deinem Tenant einrichten und erfüllen — mit allem, was dazugehört: eigene Registrierung, zweiter Eintrag in der Authenticator-App, Rückfragen beim Helpdesk. Für B2B-Direktverbindungen, etwa in freigegebenen Teams-Kanälen, ist das MFA-Vertrauen sogar zwingend: Ohne diese Einstellung wird der Zugriff bei geforderter MFA schlicht blockiert.

Wo ein Gast seinen zweiten Faktor leistet



Was bei Gästen NICHT funktioniert

- Konformes Gerät verlangen — ein Gastgerät kann sich in eurem Tenant nicht registrieren.
- App-Schutzrichtlinien verlangen — dasselbe Problem, Geräte gehören dem Heimat-Tenant.
- Benutzerrisiko-Richtlinien mit Kennwortwechsel — der Gast kann bei euch kein Kennwort setzen.
- Continuous Access Evaluation — Gastkonten werden davon nicht erfasst.
- „Jeder“-Links: Sie erfordern keine Anmeldung. Wo nichts angemeldet wird, greift auch kein MFA.

Skizze 4: Der Weg eines Gastes durch deine Richtlinien — und die Liste dessen, was bei Gastkonten nicht funktioniert.

Gäste ohne Entra-Konto

Nicht jeder Gast bringt ein Entra-Konto mit. Für Gäste mit E-Mail-Einmalkennung, mit Google-Konto oder aus einem SAML-Verbund gilt: Die MFA-Verantwortung liegt immer bei dir als Ressourcen-Tenant. Und eine Einschränkung ist dabei wichtig genug für einen eigenen Satz: Authentifizierungsstärken lassen sich derzeit nur auf externe Benutzer anwenden, die sich mit Entra ID authentifizieren. Für Einmalkennungen, SAML/WS-Fed und Google-Verbund musst du die einfache Zugriffssteuerung „MFA erforderlich“ verwenden.

Der zweite Satz, der Verwirrung vermeidet: Die per E-Mail zugestellte Einmalkennung ist der erste Faktor, nicht der zweite. Sie ersetzt das Kennwort, nicht die MFA. Wer glaubt, mit Einmalkennungen sei die Gastanmeldung automatisch mehrstufig, irrt — und zwar in einer Richtung, die im Auditbericht auffällt.

Zugriffssteuerung	B2B-Gastbenutzer	B2B-Direktverbindung
Zugriff blockieren	unterstützt	unterstützt
MFA erforderlich	unterstützt	nur mit eingehendem MFA-Vertrauen
Konformes Gerät erforderlich	nur mit eingehendem Gerätevertrauen	nur mit eingehendem Gerätevertrauen
Genehmigte Client-App erforderlich	nicht unterstützt	nicht unterstützt
App-Schutzrichtlinie erforderlich	nicht unterstützt	nicht unterstützt
Nutzungsbedingungen	unterstützt	nicht unterstützt

App-erzwungene Einschränkungen	unterstützt	nicht unterstützt
Anmeldehäufigkeit	unterstützt	nicht unterstützt

Tabelle 5: Was bei externen Benutzern greift. Alles, was ein registriertes Gerät im eigenen Tenant voraussetzt, funktioniert für Gäste grundsätzlich nicht.

Fallstricke, die zuverlässig auftreten

Drei Punkte sorgen bei Gastzugriffen regelmäßig für Überraschungen, und alle drei lassen sich vorher wissen:

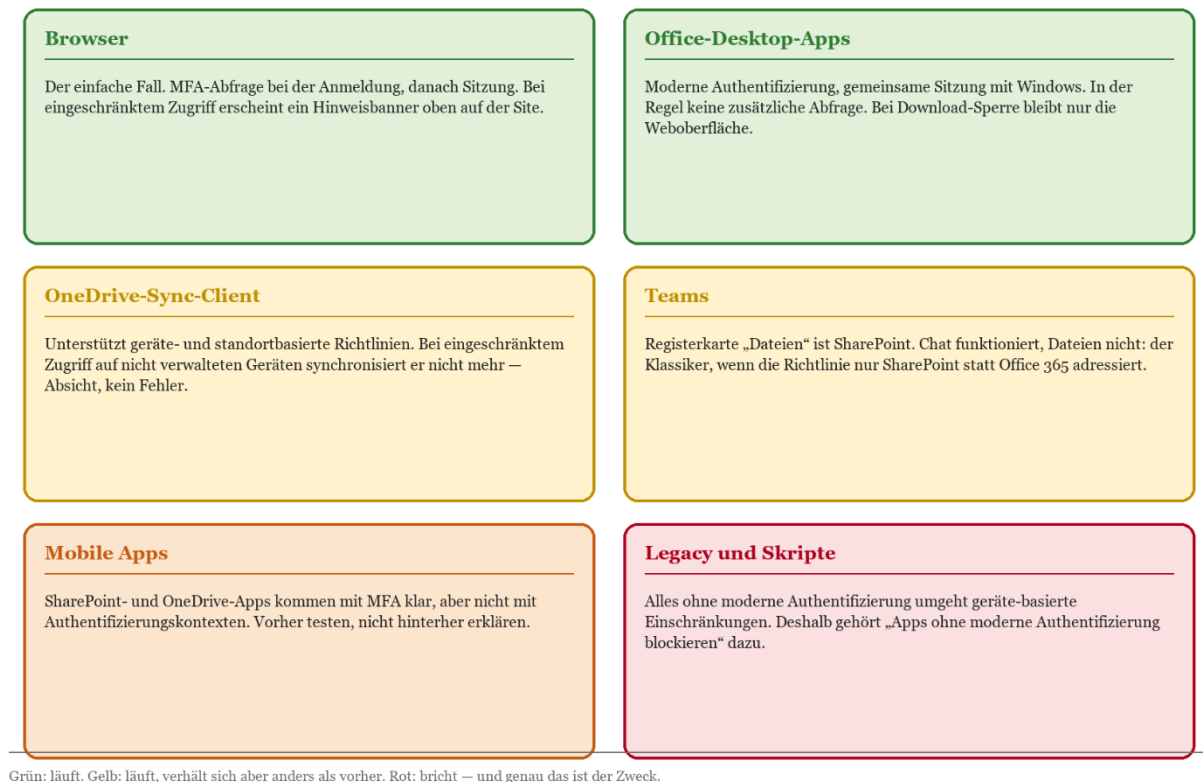
- Continuous Access Evaluation erfasst Gastkonten nicht. Widerrufereignisse und IP-basierte Richtlinien wirken bei Gästen also nicht nahezu in Echtzeit, sondern erst mit dem nächsten regulären Tokenwechsel.
- Benutzerrisiko-Richtlinien laufen bei Gästen ins Leere: Das Risiko wird im Heimatverzeichnis bewertet, ein erzwungener Kennwortwechsel im Ressourcen-Tenant ist nicht möglich. Ergebnis ist eine Blockade ohne Ausweg. Nimm Gäste aus risikobasierten Richtlinien heraus.
- Bei aktiven App-Enforced Restrictions sind auch Personen betroffen, die per Verifizierungscode auf einzelne Elemente zugreifen. Wenn das stört, lässt sich diese Gruppe mit Set-SPOTenant -ApplyAppEnforcedRestrictionsToAdHocRecipients \$false ausnehmen — eine bewusste Abwägung, keine Standardeinstellung.

Die vollständige Behandlung von Freigaberichtlinien, Ablaufdaten für Gastkonten, Domänenlisten und Zugriffsüberprüfungen steht in [Gastzugriff und externe Freigaben härten](#). Für diesen Beitrag genügt der Kern: Gäste bekommen MFA, und du entscheidest lediglich, ob sie ihn zu Hause oder bei dir leisten.

Auswirkungen auf Sync-Client und Office-Apps

Und jetzt der Teil, der über Erfolg und Misserfolg entscheidet — nicht technisch, sondern im Empfinden der Belegschaft. Eine MFA-Einführung, die im Browser einwandfrei läuft und beim OneDrive-Symbol in der Taskleiste ein rotes Kreuz hinterlässt, gilt intern als gescheitert. Auch wenn sie es fachlich nicht ist.

Client-Landkarte: was nach dem Scharfschalten passiert



Skizze 5: Die Client-Landkarte nach dem Scharfschalten. Gelb heißt nicht kaputt, sondern anders als vorher.

Der OneDrive-Sync-Client

Der Sync-Client kommt mit Conditional Access zurecht: Er unterstützt sowohl geräte- als auch standortbasierte Richtlinien. Für Windows empfiehlt Microsoft die Kombination mit der automatischen Kontokonfiguration, weil die Anmeldung dann still im Hintergrund läuft. Drei Verhaltensweisen solltest du trotzdem kennen, bevor du sie erklären musst:

- Eine neu angelegte Zugriffsrichtlinie kann bis zu 24 Stunden brauchen, bis sie auf einem bereits authentifizierten Gerät wirkt. Das ist der häufigste Grund für „bei mir geht es noch“ am Tag nach dem Scharfschalten.
- Bei standortbasierten Richtlinien erscheint eine Aufforderung etwa alle 90 bis 120 Minuten, sobald jemand die freigegebenen IP-Bereiche verlässt. Wer viel im Zug arbeitet, merkt das sehr deutlich.
- Im eingeschränkten Zugriff auf nicht verwalteten Geräten synchronisiert der Client überhaupt nicht mehr. Das ist kein Fehler, sondern der ausdrückliche Zweck der Einstellung — und der Punkt, an dem du die Kommunikation vorbereitet haben solltest.

Der letzte Punkt hat einen erfreulichen Nebeneffekt, den man in der Argumentation gegenüber der Geschäftsführung ruhig verwenden darf: Ein Sync-Client, der auf privaten Geräten nicht läuft, ist ein Verschlüsselungstrojaner weniger, der über die Synchronisierung in die Cloud-Ablage schreibt. Wie du diesen Gedanken zu einer belastbaren Vorsorge ausbaust, beschreibt [Ransomware-Vorsorge in Microsoft 365](#).

Office-Desktop-Apps und die Tokenfrage

Word, Excel und PowerPoint verwenden moderne Authentifizierung und teilen sich die Sitzung mit der Windows-Anmeldung. In der Praxis heißt das: Nach dem Scharfschalten passiert dort meistens nichts Sichtbares. Interessanter wird es beim Zusammenspiel mit Continuous Access Evaluation. SharePoint Online gehört neben Exchange Online und Teams zu den Diensten, die kritische Ereignisse aus Entra ID abonnieren und nahezu in Echtzeit auswerten: gelöschte oder deaktivierte Konten, Kennwortwechsel, aktivierte MFA, explizit widerrufenen Aktualisierungstoken, hohes Benutzerrisiko — wobei SharePoint Online Benutzerrisikoereignisse ausdrücklich nicht auswertet.

Für CAE-fähige Clients verlängert sich die Lebensdauer der Zugriffstoken auf bis zu 28 Stunden, weil nicht mehr der Ablauf, sondern das Ereignis die Sperre auslöst. Das klingt zunächst nach weniger Sicherheit und ist das Gegenteil davon: Statt stündlich blind zu erneuern, reagiert die Sitzung auf tatsächliche Änderungen. Ohne CAE-fähigen Client bleibt es bei der Standardlebensdauer von einer Stunde. Bei Office-Web-Apps sinkt die Tokenlebensdauer auf eine Stunde, sobald überhaupt eine Conditional-Access-Richtlinie greift.

FAKTEN — Gemeinsames Bearbeiten und die 15-Minuten-Schraube

Wenn mehrere Personen gleichzeitig an einem Dokument arbeiten, kann CAE den Zugriff nicht sofort entziehen. Der vollständige Entzug greift beim Schließen des Dokuments, beim Beenden der Office-Anwendung oder nach einer Stunde, sofern eine IP-basierte Richtlinie gesetzt ist.

Wer das verkürzen will, konfiguriert in SharePoint eine Richtlinie für den Netzwerkstandort. Damit sinkt die maximale Lebensdauer von Sitzungen zur gemeinsamen Bearbeitung auf 15 Minuten; feiner justieren lässt sie sich über Set-SPOTenant mit dem Parameter IPAddressWACTokenLifetime.

CAE kennt ausschließlich IP-basierte benannte Standorte. Länder- und Regionsbedingungen sowie die alten vertrauenswürdigen MFA-IP-Adressen werden dabei nicht in Echtzeit ausgewertet.

Mobilgeräte, Explorer und die Reste

Die SharePoint- und OneDrive-Apps für iOS und Android kommen mit MFA problemlos zurecht. Ihre Grenze liegt, wie oben beschrieben, bei Authentifizierungskontexten. Der klassische Weg „Im Explorer öffnen“ über WebDAV ist der unangenehmste Kandidat der Liste: Er hängt an Mechanismen, die mit modernen Sitzungssteuerungen nicht sauber zusammenspielen, und verhält sich nach dem Scharfschalten häufig unzuverlässig. Die ehrliche Empfehlung lautet, ihn im Zuge dieses Projekts abzukündigen und durch die Synchronisierung oder Verknüpfungen auf OneDrive zu ersetzen.

Bleiben die Skripte. Jeder Tenant hat sie: das nächtliche Berichtsskript, den Archivierungsjob, die Schnittstelle zum ERP. Wenn sie mit einem Benutzerkonto und hinterlegtem Kennwort arbeiten, brechen sie beim Scharfschalten — und zwar zu Recht. Der Weg heraus führt über App-Registrierungen mit Zertifikat oder über verwaltete Identitäten. Der Ressourcenbesitzer-Kennwortfluss ist mit MFA grundsätzlich unvereinbar, entsprechende Programmierschnittstellen der Microsoft-Authentifizierungsbibliotheken sind inzwischen als veraltet gekennzeichnet. Wie du dabei nicht versehentlich einen neuen Wildwuchs an Anwendungsberechtigungen erzeugst, steht in [App-Registrierungen und Consent-Governance](#).

TIPP — Die drei Abfragen, die niemand vermisst

Deaktiviere alte, per Benutzer aktivierte MFA-Einstellungen, sobald die Conditional-Access-Richtlinie läuft. Beides parallel zu betreiben erzeugt genau die doppelten Aufforderungen, die dem Verfahren den Ruf ruinieren.

Setze eine gemeinsame Richtlinie über Exchange Online, SharePoint Online und Teams statt drei

verschiedene. Unterschiedliche Anforderungen an nachgelagerte Dienste sind die häufigste Ursache für scheinbar grundlose Zusatzabfragen.

Lass die Option „Angemeldet bleiben“ aktiviert. Sie reduziert die Zahl der Abfragen deutlich, ohne die MFA-Anforderung selbst aufzuweichen — beim Zugriff auf die Verwaltungsportale wird MFA ohnehin unabhängig davon verlangt.

Häufige Fragen

Gibt es im SharePoint Admin Center wirklich keinen MFA-Schalter?

Nein, und das ist kein Versehen. SharePoint Online authentifiziert nicht selbst, sondern verlässt sich vollständig auf Microsoft Entra ID. Die Einstellungen unter „Zugriffssteuerung“ steuern die Sitzung nach der Anmeldung, nicht die Anmeldung selbst. Wer dort etwas sucht, sucht am falschen Ort — mit dem unangenehmen Nebeneffekt, dass er etwas Plausibles findet.

Soll ich die Richtlinie auf SharePoint Online oder auf Office 365 richten?

Auf Office 365, solange du keinen ausdrücklichen Grund für das Gegenteil hast. Die App-Gruppe löst die Dienstabhängigkeiten sauber auf und verhindert das Muster „Teams-Chat läuft, Dateien nicht“. Eine gezielte Richtlinie nur auf SharePoint Online ergibt Sinn, wenn du dort strenger sein willst als anderswo — etwa mit phishing-resistenter MFA.

Reicht „eingeschränkter webbasierter Zugriff“ nicht als Schutz?

Nein. Diese Einstellung verhindert Download, Druck und Synchronisierung auf nicht verwalteten Geräten. Sie verhindert nicht, dass sich jemand mit einem abgephischten Kennwort anmeldet, in aller Ruhe durch die Dokumente liest und über die Weboberfläche kopiert, was er braucht. Sie ist eine sinnvolle zweite Ebene, aber niemals ein Ersatz für die erste.

Was passiert mit dem OneDrive-Sync-Client?

Er läuft weiter, solange nur MFA verlangt wird. Er unterstützt geräte- und standortbasierte Richtlinien. Er stellt die Synchronisierung ein, wenn du den eingeschränkten Zugriff für nicht verwaltete Geräte aktivierst, und er synchronisiert keine Websites mit Authentifizierungskontext. Rechne außerdem damit, dass neue Richtlinien auf bereits authentifizierten Geräten bis zu 24 Stunden brauchen.

Müssen Gäste auch MFA machen?

Ja, sofern deine Richtlinie sie einschließt — und das sollte sie. Die einzige Frage ist, wo sie den zweiten Faktor leisten. Mit eingehendem MFA-Vertrauen in den tenantübergreifenden Zugriffseinstellungen akzeptierst du den Nachweis aus dem Heimat-Tenant. Ohne dieses Vertrauen müssen Gäste MFA in deinem Tenant einrichten. Beides ist vertretbar, das erste ist deutlich angenehmer für alle Beteiligten.

Wie sichere ich eine einzelne, besonders heikle Website stärker ab?

Mit einem Authentifizierungskontext. Du legst ihn in Entra ID an, richtest eine Conditional-Access-Richtlinie darauf aus und verbindest ihn per Set-SPOSite oder über eine Vertraulichkeitsbezeichnung mit der Website. Beachte die Einschränkungen: kein Sync, keine

mobilen SharePoint-Apps, kein Outlook, keine Stammwebsite. Für einzelne Bereiche hervorragend, für die Fläche ungeeignet.

Warum werden Benutzer trotz Ausschluss zur MFA aufgefordert?

Meistens greift eine zweite Richtlinie, an die niemand mehr gedacht hat — nicht selten eine Microsoft-verwaltete. Microsoft legt solche Richtlinien in Entra-Tenants selbst an, zunächst im Modus „Nur berichten“, und aktiviert sie frühestens 30 Tage später, sofern sie nicht ausdrücklich abgeschaltet wurden. Der Blick ins Anmeldeprotokoll auf die Registerkarte „Bedingter Zugriff“ zeigt in wenigen Sekunden, welche Richtlinie tatsächlich gegriffen hat.

Und was ist mit SharePoint Server im eigenen Rechenzentrum?

Das ist eine andere Welt mit anderen Werkzeugen. On-premises gibt es keine Conditional-Access-Richtlinie, sondern Verbundanmeldung, Ansprüche und im klassischen Fall Kerberos mit korrekt gesetzten Dienstprinzipalnamen. Wie du MFA dort erzwingst und welche Rolle die Anmeldeanbieter dabei spielen, beschreibt [MFA für SharePoint Server on-premises](#); die Kerberos-Grundlagen dazu findest du im [Kompetenzbereich Kerberos](#).

Wie weise ich nach, dass MFA für SharePoint tatsächlich greift?

Über die Anmeldeprotokolle in Entra ID, gefiltert nach der Anwendung „Office 365 SharePoint Online“ und der Spalte für den bedingten Zugriff. Jeder Eintrag zeigt, welche Richtlinien ausgewertet wurden und mit welchem Ergebnis. Für die regelmäßige Berichterstattung eignet sich diese Auswertung besser als jede Prozentzahl aus einem Bewertungswerkzeug — mehr dazu in [Security-Reporting für die Geschäftsführung](#).

Fazit

MFA für SharePoint Online zu erzwingen ist technisch eine Sache von zwanzig Minuten und organisatorisch eine Sache von vier Wochen. Der Unterschied zwischen beiden Zahlen ist genau das, was am Ende darüber entscheidet, ob die Maßnahme hält oder ob sie nach drei Tagen mit einem Ausnahmeeintrag für „die Vertriebsabteilung, vorübergehend“ wieder aufgeweicht wird.

Die vier Punkte, die du mitnehmen solltest: Erstens wird MFA in Entra ID konfiguriert, nicht in SharePoint — und die Zielressource heißt in aller Regel „Office 365“, nicht „SharePoint Online“. Zweitens sind App-Enforced Restrictions eine wertvolle zweite Ebene für nicht verwaltete Geräte, aber kein Authentifizierungsmittel; wer sie mit MFA verwechselt, hat die Fenster verriegelt und die Tür offen gelassen. Drittens sind Gäste kein Sonderfall, sondern eine Entscheidung: MFA-Vertrauen aus dem Heimat-Tenant oder eigene Registrierung bei dir. Und viertens entscheidet sich der Erfolg am OneDrive-Symbol in der Taskleiste, nicht im Richtlinieneditor.

Wer zusätzlich die tenantweiten Schrauben nachziehen will, findet die Reihenfolge in [Tenant-Härtung: die 20 wichtigsten Schrauben](#). Und wenn die Frage im Raum steht, wie viel Zero Trust ein Unternehmen mit 180 Beschäftigten wirklich braucht, ohne dass daraus ein Dauerprojekt wird, hilft [Zero Trust im Mittelstand: pragmatisch statt dogmatisch](#) beim Sortieren.

WEITER — Passende Beiträge und Angebote

- › [MFA in Microsoft 365 richtig einführen](#) — die Grundlagen der Einführung, von der Methodenwahl bis zur Kommunikation.
- › [Conditional Access: Baselines, die nicht nerven](#) — der Satz von Startrichtlinien, in den diese Regel gehört.
- › [MFA für SharePoint Server on-premises](#) — dieselbe Frage für SharePoint im eigenen

Rechenzentrum.

- › [Gastzugriff und externe Freigaben härten](#) — Freigaberichtlinien, Ablaufdaten und Zugriffsüberprüfungen für Externe.
- › [Legacy Authentication endgültig abschalten](#) — die Voraussetzung dafür, dass deine Richtlinie nicht umgangen wird.
- › [Kompromittiertes Konto erkennen und aufräumen](#) — was zu tun ist, wenn es trotzdem jemanden erwischt hat.
- › [Dossier TerminalFix und der Berlin-Hack](#) — wie ein realer Vorfall abläuft, wenn die Grundlagen fehlen.
- › [Microsoft 365 Security Beratung](#) — Unterstützung bei Entwurf, Report-only-Auswertung und Rollout.
- › [Schulung Microsoft 365 Security](#) — für Teams, die das künftig selbst betreiben wollen.