

Conditional Access: Baselines, die nicht nerven

Es gibt zwei Sorten von Conditional-Access-Installationen. Die eine besteht aus vier Richtlinien, die seit drei Jahren unverändert laufen, von denen niemand mehr weiß, wer sie angelegt hat, und die zusammen ungefähr so viel Schutz bieten wie ein Fahrradschloss am Panzerschrank. Die andere besteht aus siebenundachtzig Richtlinien mit Namen wie „Test neu 2 FINAL“, von denen sich vierzehn gegenseitig widersprechen, drei aus Versehen die Buchhaltung aussperren und eine seit 2022 auf Report-only steht, weil sich niemand traut, sie scharfzuschalten.

Beide Varianten haben denselben Ursprung: Es gab keine Baseline. Es gab Einzelfälle, die irgendwann Richtlinien wurden. Eine Baseline ist das Gegenteil davon — ein kleiner, bewusst gewählter Satz von Richtlinien, der für alle gilt, der begründet ist, der versioniert wird und der genau dort aufhört, wo der Nutzen kippt. Sieben Stück reichen. Nicht vierzig.

Dieser Beitrag beschreibt diese sieben Starttrichtlinien, die Reihenfolge, in der du sie einführst, und die drei Dinge, die den Unterschied zwischen einer Baseline und einem Sperrgebiet ausmachen: eine ordentliche Report-only-Phase, eine Namenskonvention mit Versionsnummer und eine Break-Glass-Ausnahme, die wirklich funktioniert. Er gehört in die Reihe [Microsoft 365 Security](#), in der die einzelnen Bausteine einer Microsoft-365-Absicherung zusammenlaufen.

Was Conditional Access tatsächlich tut — und warum das die Reihenfolge bestimmt

Bevor du Richtlinien schreibst, musst du wissen, wie sie ausgewertet werden. Sonst baust du Kombinationen, die auf dem Papier logisch aussehen und in der Praxis entweder gar nichts tun oder alles blockieren. Beides ist unangenehm, das zweite fällt schneller auf.

Eine Wenn-dann-Regel, keine Firewall-Regel

Eine Conditional-Access-Richtlinie ist eine Wenn-dann-Aussage aus Zuweisungen und Zugriffssteuerungen. Alle Zuweisungen innerhalb einer Richtlinie sind UND-verknüpft: Benutzer UND Zielressource UND Netzwerk UND Bedingung. Fehlt eines davon, greift die Richtlinie nicht. Und wenn mehrere Richtlinien auf dieselbe Anmeldung passen, müssen sie alle erfüllt werden. Verlangt eine MFA und eine andere ein konformes Gerät, dann brauchst du beides — nicht das eine oder das andere.

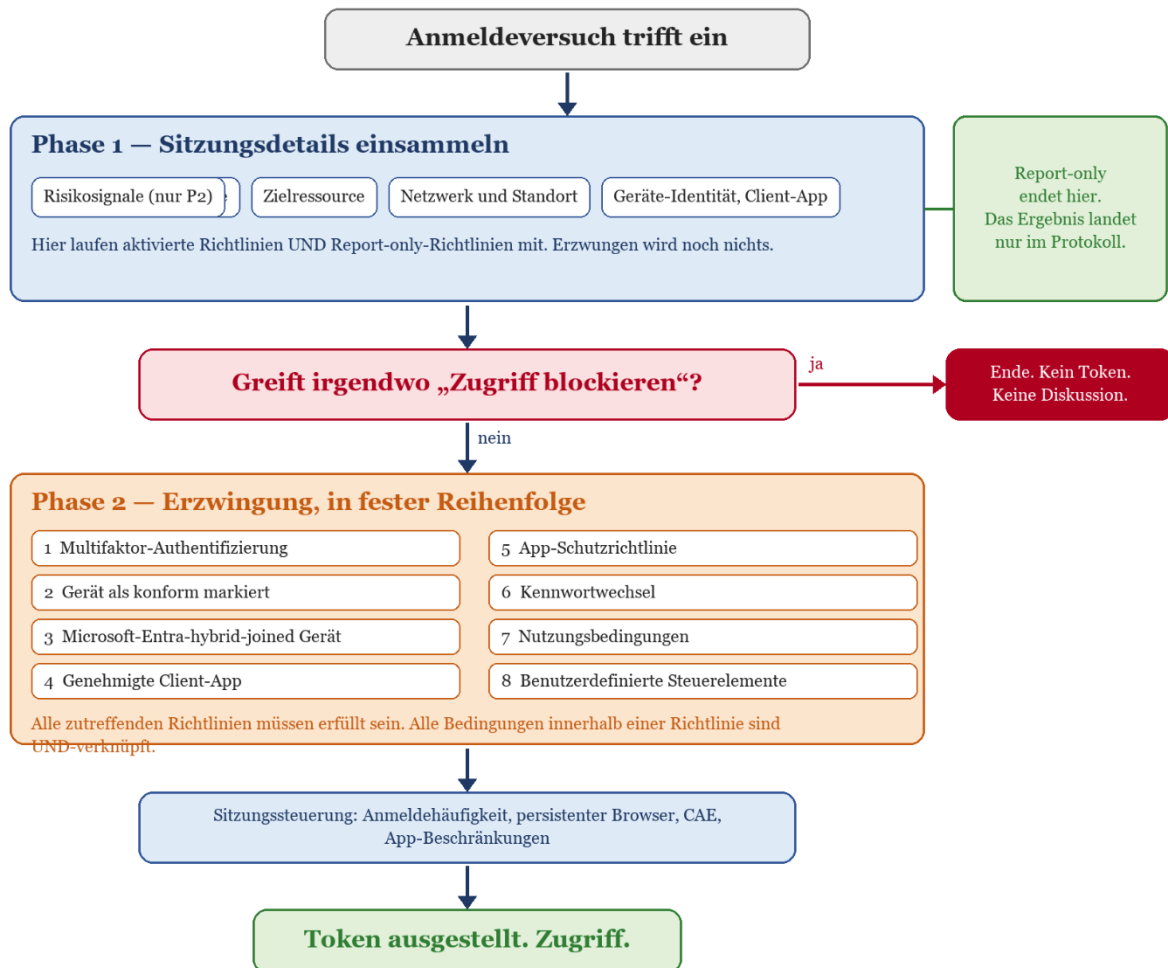
Der zweite entscheidende Punkt: Wer von keiner Richtlinie erfasst wird, bekommt sein Token. Conditional Access ist keine Firewall mit implizitem Deny am Ende. Wenn keine Bedingung zutrifft, wird der Zugriff gewährt. Das ist der Grund, warum eine Baseline immer mit einer Richtlinie für „alle Benutzer, alle Ressourcen“ beginnt und nicht mit einer Sammlung anwendungsspezifischer Sonderregeln.

Zwei Phasen: erst sammeln, dann erzwingen

Die Auswertung läuft in zwei Phasen. In Phase 1 sammelt Microsoft Entra die Sitzungsdetails ein — Benutzer, Rolle, Zielressource, Netzwerkstandort, Geräteidentität, Client-App und, wenn lizenziert, die Risikosignale. Hier laufen aktivierte Richtlinien und Report-only-Richtlinien gemeinsam mit. In Phase 2 wird erzwungen, und zwar nur für aktivierte Richtlinien. Gibt es irgendwo ein „Zugriff blockieren“, endet die Auswertung sofort. Block schlägt Grant, immer, ohne Verhandlung.

Erst danach fordert Entra die fehlenden Grant-Kontrollen an, und zwar in einer festen Reihenfolge: MFA, dann Gerätekonformität, dann Hybrid-Join, dann genehmigte Client-App, App-Schutzrichtlinie, Kennwortwechsel, Nutzungsbedingungen, benutzerdefinierte Steuerelemente. Sind alle erfüllt, greifen die Sitzungssteuerungen — Anmeldehäufigkeit, persistenter Browser, Continuous Access Evaluation. Dann erst gibt es ein Token.

Auswertungsreihenfolge einer Conditional-Access-Richtlinie



Skizze 1: Die zwei Phasen der Auswertung. Report-only-Richtlinien enden nach Phase 1 im Protokoll — sie sperren niemanden aus, aber sie zeigen dir, wen sie aussperren würden.

FAKTEN — Zahlen, die du im Kopf haben solltest

Ein Tenant verträgt maximal 240 Conditional-Access-Richtlinien — inklusive der Richtlinien, die auf „Aus“ oder „Report-only“ stehen. Das Limit erreicht man nicht durch Baselines, sondern durch Sonderfälle.

Microsoft beziffert die Wirkung von MFA auf über 99,2 Prozent der identitätsbasierten Angriffe. Über 99 Prozent der Password-Spray-Angriffe laufen über Legacy-Authentifizierung.

Gelöschte Richtlinien lassen sich innerhalb von 30 Tagen wiederherstellen. Das ist ein Sicherheitsnetz, keine Backup-Strategie.

Richtlinien, die auf Rollen oder Gruppen zielen, greifen erst bei der nächsten Tokenausstellung. Wer gerade ein gültiges Token hat, merkt von der neuen Gruppenmitgliedschaft zunächst nichts.

Security Defaults und Conditional Access schließen sich aus

Viele Tenants starten mit Security Defaults. Das ist völlig in Ordnung: Sie erzwingen MFA-Registrierung für alle, MFA für Administratoren, blockieren Legacy-Authentifizierung, schützen den Zugriff auf das Azure-Portal und blockieren seit dem 1. Juli 2026 in neuen Tenants auch den Geräteanmeldecode-Flow. Für null Euro Lizenzkosten ist das eine Menge.

Nur: Beides gleichzeitig geht nicht. Sobald du Conditional-Access-Richtlinien anlegst, kannst du Security Defaults nicht mehr aktivieren, und wer von Security Defaults auf Conditional Access wechselt, muss sie ausdrücklich deaktivieren. In dem Moment, in dem der Schalter umgelegt wird, ist der Schutz weg — und zwar sofort und vollständig, nicht schrittweise. Welche Variante für dich passt, steht ausführlich in [Security Defaults oder Conditional Access?](#).

WARNUNG — Der Moment, in dem der Tenant nackt dasteht

Beim Umstieg von Security Defaults auf Conditional Access gibt es ein Zeitfenster, in dem weder das eine noch das andere greift. Wer die Security Defaults abschaltet und dann in Ruhe anfängt, Richtlinien zu bauen, betreibt seinen Tenant in der Zwischenzeit ohne MFA-Zwang und mit offener Legacy-Authentifizierung.

Richtig ist die umgekehrte Reihenfolge: Erst alle sieben Richtlinien anlegen — im Zustand Report-only. Auswerten. Ausnahmen klären. Dann in einem einzigen Wartungsfenster die Security Defaults ausschalten und die Richtlinien scharfstellen. Dauer: Minuten, nicht Wochen.

Zweiter Stolperstein: Das Synchronisierungskonto von Entra Connect beziehungsweise Cloud Sync ist von Security Defaults automatisch ausgenommen. Von deinen eigenen Richtlinien ist es das nicht.

Wer das übersieht, bricht die Verzeichnissynchronisierung — meistens freitagabends.

Ein zweiter Effekt kommt hinzu, den viele erst bemerken, wenn er da ist: Microsoft legt in berechtigten Tenants eigene, verwaltete Richtlinien an. Sie erscheinen zunächst auf Report-only und werden frühestens 30 Tage später automatisch aktiviert, mit zwei Wochen Vorwarnung per E-Mail und Message Center. Du kannst sie ausschließen, ausschalten oder früher aktivieren — umbenennen oder löschen kannst du sie nicht. Wer seine eigene Baseline sauber gebaut hat, hat davon nichts zu befürchten. Wer keine hat, bekommt sie geschenkt, allerdings ohne Rücksicht auf sein Multifunktionsgerät im Kopierraum.

Die sieben Startrichtlinien

Sieben Richtlinien decken den Großteil dessen ab, was in einem mittelständischen Tenant schiefgehen kann. Sie sind bewusst breit geschnitten — je weniger Richtlinien, desto weniger Wechselwirkungen. Die Nummerierung ist keine Kosmetik, sondern Teil der Namenskonvention: Über CA03 kann man am Telefon reden, über „die mit dem Legacy-Zeug“ nicht.

Die sieben Startrichtlinien: wer, was, wogegen

CA01	Alle Benutzer, alle Ressourcen MFA erzwingen	P1
CA02	Privilegierte Rollen Phishing-resistente Stärke	P1
CA03	Alle Benutzer, Legacy-Clients Blockieren	P1
CA04	Alle Benutzer, Desktop-Zugriff Konformes oder hybrides Gerät	P1 + Intune
CA05	Alle Benutzer, Geräteanmeldecode Blockieren	P1
CA06	Privilegierte Rollen, Admin-Portale Anmeldehäufigkeit 4–12 h	P1
CA07	Alle Benutzer, hohes Risiko MFA, Kennwortwechsel, Sperre	P2

Jede dieser Richtlinien schließt dieselbe Break-Glass-Gruppe aus. Ausnahme: Sie ist keine Bequemlichkeit, sie ist die Feuerleiter.

Skizze 2: Die sieben Startrichtlinien mit Geltungsbereich, Steuerung und Lizenzbedarf. Sechs davon brauchen Entra ID P1, nur die letzte verlangt P2.

Nr.	Richtlinie	Wirkung	Lizenz	Nervfaktor
CA01	MFA für alle Benutzer	Zweiter Faktor bei allen Ressourcen	P1	Gering — die Sitzung hält.
CA02	Phishing-resistente MFA für Admins	Nur FIDO2, Windows Hello, Zertifikat	P1	Hoch am ersten Tag, danach null.
CA03	Legacy-Authentifizierung blockieren	Basic Auth und alte Mailprotokolle raus	P1	Gering, wenn die Inventur stimmt.
CA04	Konformes oder hybrid-joined Gerät	Zugriff nur vom verwalteten Endgerät	P1 + Intune	Mittel — der Härtestest.
CA05	Geräteanmeldecode blockieren	Device Code Flow gesperrt	P1	Null, bis der Teams-Room streikt.
CA06	Anmeldehäufigkeit für Admins	Erneute Anmeldung nach 4 bis 12 Stunden	P1	Mittel, aber begründbar.
CA07	Risiko-Richtlinien	Reaktion auf Anmelde- und Benutzerrisiko	P2	Gering, wenn P2 vorhanden.

Tabelle 1: Die Baseline auf einen Blick. Der Nervfaktor ist Erfahrungswert, keine Metrik.

CA01 — MFA für alle Benutzer

Der Klassiker, und trotzdem der am häufigsten halbherzig umgesetzte. „MFA für alle“ heißt alle: Benutzer, Gäste, Dienstleister, der Geschäftsführer, das Konto der Werkstudentin. Zielressource ist „Alle Ressourcen“, nicht eine handverlesene App-Liste — sonst musst du bei jeder neuen Anwendung nachziehen und vergisst es beim dritten Mal.

Der Vorwurf, MFA nerve, hält der Realität nicht stand, wenn die Sitzungsdauer vernünftig konfiguriert ist. Bei Standardeinstellungen bleibt die Sitzung auf dem Gerät bestehen; der zweite Faktor ist eine Sache von wenigen Prompts pro Woche. Wer täglich zehnmal die App bestätigen muss, hat kein MFA-Problem, sondern ein Problem mit widersprüchlichen Sitzungseinstellungen.

Wie du die Einführung ohne Aufstand hinbekommst, steht in [MFA in Microsoft 365 richtig einführen](#).

Ein Detail, das bei der Kombination gern übersehen wird: Du kannst in einer Richtlinie nicht gleichzeitig „Multifaktor-Authentifizierung erforderlich“ und „Authentifizierungsstärke erforderlich“ setzen. Die eingebaute Stärke „Multifaktor-Authentifizierung“ ist inhaltlich dasselbe wie die Grant-Kontrolle. Entscheide dich für eine der beiden Schreibweisen und bleibe im ganzen Tenant dabei.

CA02 — Phishing-resistente MFA für Administratoren

Ein Push in der Authenticator-App ist MFA. Phishing-resistent ist er nicht: Ein Adversary-in-the-Middle-Proxy fängt die Anmeldung ab, der Benutzer bestätigt brav, der Angreifer hat das Token. Für privilegierte Rollen ist das zu wenig. Die eingebaute Authentifizierungsstärke „Phishing-resistente MFA“ erlaubt nur drei Kombinationen: FIDO2, Windows Hello for Business beziehungsweise Plattform-Anmeldeinformationen, und zertifikatsbasierte Authentifizierung als Multifaktor-Variante.

Methode	MFA-Stärke	Passwortlose Stärke	Phishing-resistent
FIDO2-Sicherheitsschlüssel / Passkey	ja	ja	ja
Windows Hello for Business	ja	ja	ja
Zertifikat (mehrstufig)	ja	ja	ja
Authenticator (Telefonanmeldung)	ja	ja	nein
Temporary Access Pass	ja	nein	nein
Kennwort plus Push, SMS oder OATH	ja	nein	nein
Zertifikat (einstufig), SMS-Anmeldung, QR-Code	nein	nein	nein

Tabelle 2: Was die drei eingebauten Authentifizierungsstärken jeweils zulassen. Wer für Admins die höchste Stufe verlangt, muss die Methoden vorher ausgerollt haben.

Praktisch heißt das: Bevor CA02 scharfgeschaltet wird, brauchen alle Rolleninhaber einen registrierten phishing-resistenten Faktor — und zwar zwei, denn ein einzelner Sicherheitsschlüssel in der Waschmaschine ist ein Ausfall, kein Ärgernis. Die Einführung von Schlüsseln und Passkeys behandelt [Passwordless: FIDO2 und Passkeys in der Praxis](#) im Detail.

WICHTIG — Rollen greifen erst beim nächsten Token

Richtlinien, die auf Verzeichnisrollen zielen, werden nur bei der Tokenausstellung ausgewertet. Wer eine Rolle frisch zugewiesen bekommt und noch ein gültiges Token hält, fällt zunächst nicht unter CA02.

Sauber wird das erst mit Privileged Identity Management: Bei der Rollenaktivierung wird MFA verlangt und die Auswertung neu ausgelöst. Dauerhaft zugewiesene Administratorrollen sind ohnehin die schlechtere Idee — sie sind auch nachts um drei aktiv, wenn niemand hinsieht.

CA03 — Legacy-Authentifizierung blockieren

Legacy-Authentifizierung kennt kein MFA. Das ist keine Schwäche, das ist Bauart. Ein Angreifer mit gültigem Kennwort und einem alten IMAP-Client umgeht jede noch so schön konfigurierte MFA-Richtlinie, weil das Protokoll den zweiten Faktor überhaupt nicht anbieten kann. Deshalb gehört CA03 zu den Richtlinien mit dem besten Verhältnis von Aufwand zu Wirkung.

Die Bedingung heißt „Client-Apps“ und umfasst „Exchange ActiveSync-Clients“ sowie „Andere Clients“. Die Steuerung ist „Zugriff blockieren“. Der ganze Aufwand steckt nicht in der Richtlinie, sondern in der Inventur davor: Multifunktionsgeräte, die per SMTP scannen,

Fakturierungssoftware mit hartcodiertem POP3-Abruf, ein Alarmierungsserver von 2013. Genau dafür ist die Report-only-Phase da. Der vollständige Weg inklusive Abschaltung der Basisauthentifizierung in Exchange Online steht in [Legacy Authentication endgültig abschalten](#).

CA04 — Konformes oder Microsoft-Entra-hybrid-joined Gerät

Das ist die Richtlinie, an der sich entscheidet, ob deine Baseline eine Zugangskontrolle ist oder eine Zugangskontrolle mit Substanz. Ein Kennwort plus zweiter Faktor beweist, wer da tippt. Erst die Gerätebedingung beweist, worauf getippt wird. Ohne sie darf sich der Benutzer vom ungepatchten Privatrechner mit vier Browsererweiterungen unbekannter Herkunft am Firmenpostfach anmelden — korrekt authentifiziert, versteht sich.

In der Praxis formulierst du CA04 als „Konformes Gerät ODER hybrid-joined Gerät ODER MFA“, solange die Geräteflotte noch nicht vollständig verwaltet ist, und ziehst das ODER-MFA später heraus. Die Geräteauswertung setzt voraus, dass die Endpunkte in Intune oder per Hybrid-Join bekannt sind; wie das ohne Drama gelingt, beschreibt [Defender for Endpoint: Onboarding ohne Drama](#). Für den Browserzugriff auf SharePoint und Exchange lässt sich der Zwischenschritt über app-erzwungene Beschränkungen gehen — Details in [MFA für SharePoint Online erzwingen](#).

WARNUNG — „Blockieren“ plus „Alle Ressourcen“ ist eine geladene Waffe

Die Kombination aus Block-Steuerung und „Alle Ressourcen“ in einer Richtlinie kann Administratoren komplett aussperren. Für zentrale Endpunkte wie Microsoft Graph lassen sich keine Ausnahmen konfigurieren.

Wenn du mit Blockieren arbeitest — bei CA03 und CA05 kommst du nicht darum herum — dann grenze die Bedingung so eng wie möglich ein und prüfe die Ausschlussgruppe zweimal. Und teste die Ausschlüsse tatsächlich: Ein ausgeschlossener Benutzer kann durch eine andere Richtlinie trotzdem zur MFA gezwungen werden.

CA05 — Geräteanmeldecode-Flow blockieren

Der Device Code Flow existiert für Geräte ohne Tastatur und Browser: Fernseher, Teams-Raumsysteme, Drucker. Der Benutzer bekommt einen Code angezeigt und tippt ihn auf einem zweiten Gerät ein. Legitime Nutzung ist selten. Angreifer dagegen lieben ihn, weil er sich hervorragend in Phishing verpacken lässt: eine überzeugende Mail, ein Code, ein arglos eingetippter Bestätigungsschritt — und das Token wandert an eine Infrastruktur, die niemals im Firmennetz war.

In Conditional Access findest du das unter den Bedingungen als „Authentifizierungsflüsse“. Blockiere den Geräteanmeldecode-Flow tenantweit und schneide Ausnahmen ausschließlich auf die konkreten Raumgerätekonto zu — nicht auf eine Gruppe „IT“, in der über die Jahre erfahrungsgemäß alle landen, die einmal etwas dringend brauchten.

CA06 — Anmeldehäufigkeit für Administratoren

Gestohlene Token sind der bequemste Zugang, den ein Angreifer bekommen kann: kein Kennwort, kein MFA-Prompt, einfach eine gültige Sitzung. Die Anmeldehäufigkeit begrenzt, wie lange so ein Diebstahl trägt. Für privilegierte Rollen beim Zugriff auf die Administrationsportale sind vier bis zwölf Stunden ein vernünftiger Wert.

„Jedes Mal“ solltest du dagegen nur mit echtem Anlass setzen — etwa in der Risiko-Richtlinie. Microsoft rechnet dabei mit fünf Minuten Uhrentoleranz, mehr als einmal alle fünf Minuten wird also niemand gefragt. Trotzdem gilt: Wer permanent bestätigen muss, bestätigt irgendwann auch

die Anfrage, die er nicht selbst ausgelöst hat. Genau das ist der Angriff, gegen den du eigentlich arbeitest.

TIPP — Zwei Schalter, die sich gegenseitig sabotieren

Bevor du die Anmeldehäufigkeit einführst, schalte die alte Einstellung „MFA auf vertrauenswürdigen Geräten merken“ im Tenant ab. Beide zusammen führen zu Prompts, die niemand erklären kann — und die Beschwerden landen bei dir, nicht bei Microsoft.

Ebenfalls prüfen: Konfigurierbare Tokenlebensdauern für Aktualisierungs- und Sitzungstoken sind seit dem 30. Januar 2021 zurückgezogen. Wer noch Reste davon im Tenant hat, mischt zwei Mechanismen, die sich nicht vertragen.

Für mobile Geräte kann die erneute Authentifizierung nach Ablauf des Intervalls spürbar dauern. Das ist bekannt und kein Fehler in deiner Konfiguration.

CA07 — Risiko-Richtlinien, aber nur mit P2

Anmelderisiko und Benutzerrisiko sind die einzigen Signale in dieser Liste, die eine Entra-ID-P2-Lizenz voraussetzen. Ohne P2 gibt es keine Risikobewertung, und eine Richtlinie, die auf ein Signal reagiert, das nie gesetzt wird, ist Dekoration. Deshalb steht CA07 an siebter Stelle und nicht an erster: Sie ist die Kür, nicht die Pflicht.

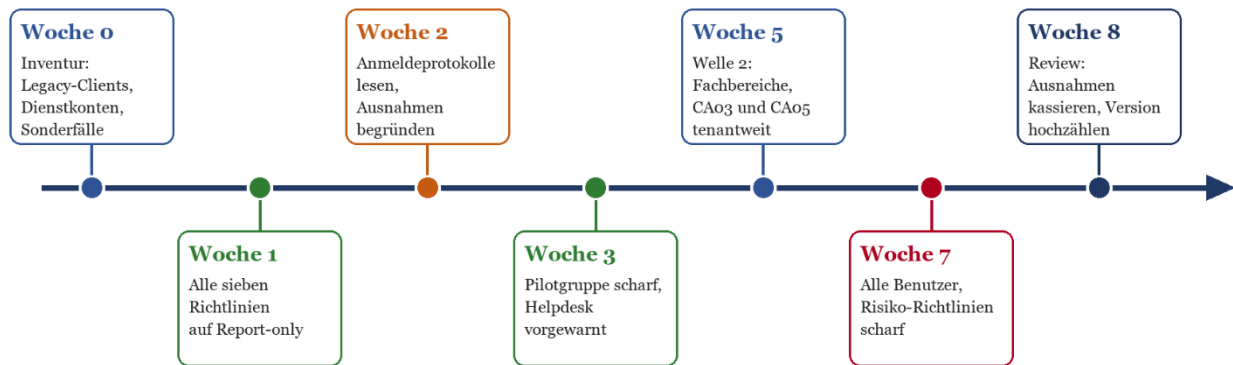
Mit P2 baust du zwei Richtlinien. Bei hohem Anmelderisiko: MFA erzwingen und Anmeldehäufigkeit auf „jedes Mal“. Bei hohem Benutzerrisiko: sichere Kennwortänderung erzwingen oder blockieren, je nachdem, wie viel Selbstheilung du den Benutzern zutraust. Wichtig ist die Vorrangregel: Blockieren schlägt alles andere, und die Anforderung zur Risikobehhebung schlägt die reine Kennwortänderung. Was danach zu tun ist, wenn ein Konto tatsächlich übernommen wurde, steht in [Kompromittiertes Konto erkennen und aufräumen](#).

Wenn du unsicher bist, ob P2 sich rechnet: In den meisten mittelständischen Tenants ist die Antwort ja, sobald ein einziger ernsthafter Vorfall verhindert wird. Wie so eine Rechnung aussieht und was sie mit dem Rest der Sicherheitsarchitektur zu tun hat, ordnet [Zero Trust im Mittelstand: pragmatisch statt dogmatisch](#) ein. Für die konkrete Auslegung im eigenen Tenant lohnt ein Blick auf die [Microsoft 365 Security Beratung](#).

Report-only: die Phase, in der du noch Fehler machen darfst

Report-only ist die wichtigste Erfindung im Conditional-Access-Umfeld, und sie wird regelmäßig übersprungen, weil sie sich anfühlt wie Zeitverschwendung. Ist sie nicht. Sie ist die einzige Gelegenheit, den Unterschied zwischen deinem Modell der Organisation und der tatsächlichen Organisation zu erfahren, ohne dass jemand dabei zu Schaden kommt.

Rollout in acht Wochen: Report-only zuerst, Reue später nie



Zeitraum für den Mittelstand. Wer 20 000 Konten und drei Rechenzentren hat, verdoppelt jede Zahl und schläft trotzdem schlecht.

Skizze 3: Ein realistischer Rollout-Plan. Die Report-only-Phase ist kein Puffer, sondern Arbeitszeit — sie besteht aus Protokolle lesen und Ausnahmen begründen.

Was Report-only zeigt — und was nicht

Eine Richtlinie im Zustand Report-only wird in Phase 1 vollständig ausgewertet und in Phase 2 nicht erzwungen. Das Ergebnis landet in den Anmeldeprotokollen im Reiter „Nur Bericht“. Du siehst also für jede reale Anmeldung, ob die Richtlinie gegriffen hätte und mit welchem Ergebnis. Bei mehreren Richtlinien gleichzeitig siehst du auch das Zusammenspiel — was wichtig ist, weil sich Wirkungen addieren.

Frage	Report-only beantwortet sie	Anmerkung
Wer wäre blockiert worden?	ja, vollständig	Der wichtigste Wert. Vor dem Scharfschalten muss diese Liste erklärbar sein.
Welche Legacy-Clients sind aktiv?	ja	Client-App und Benutzeragent stehen im Protokoll.
Wären Dienstkonten betroffen?	nur wenn sie sich anmelden	Ein Konto, das monatlich läuft, taucht in einer Woche nicht auf.
Wie reagieren Dienstprinzipale?	nein	Benutzerbezogene Richtlinien greifen nicht für Dienstprinzipale. Dafür braucht es Workload Identities.
Wie fühlt sich das für Benutzer an?	nein	Prompts werden nicht ausgelöst. Akzeptanz misst du erst im Pilotbetrieb.
Klappt der Ausschluss?	eingeschränkt	Ausschlüsse musst du aktiv testen — eine andere Richtlinie kann dieselbe Anforderung stellen.

Tabelle 3: Report-only ist ein starkes Werkzeug mit klaren Grenzen. Die untere Hälfte der Tabelle enthält die Fälle, die Projekte reihenweise überraschen.

Mindestens eine Woche, besser zwei

Microsoft empfiehlt, jede Richtlinie mindestens eine Woche im Report-only-Zustand laufen zu lassen, bevor sie erzwungen wird. Das ist die Untergrenze und passt zu Organisationen mit gleichmäßigem Wochenrhythmus. Sobald Monatsabschluss, Schichtbetrieb, Außendienst oder Saisongeschäft im Spiel sind, brauchst du länger — mindestens einen vollständigen Geschäftszyklus. Der Monatsabschluss ist erfahrungsgemäß der Termin, an dem die exotischste Software des Hauses aufwacht.

TIPP — Auswertung ohne Klickorgie

Für den Überblick über alle Richtlinien gleichzeitig gibt es die Arbeitsmappe „Conditional Access Insights and Reporting“. Sie braucht Entra ID P1 und einen Log-Analytics-Arbeitsbereich, in den die Anmeldeprotokolle gestreamt werden.

Für Einzelfälle nimm das What-If-Werkzeug: Benutzer, App, Bedingungen eingeben, Ergebnis ablesen. Es ersetzt keinen echten Test, spart aber die Hälfte der Rückfragen aus dem Helpdesk.

Der Reiter „Richtlinienauswirkung“ an der Richtlinie selbst zeigt die Wirkung zusammengefasst — auch für Richtlinien im Report-only-Zustand.

Wenn Anmeldeprotokolle systematisch ausgewertet werden, ist das in Deutschland kein rein technisches Thema. Was dabei mitbestimmungspflichtig ist, klärt [Security-Monitoring und Betriebsrat: was mitbestimmungspflichtig ist](#) — am besten vor dem Rollout, nicht danach.

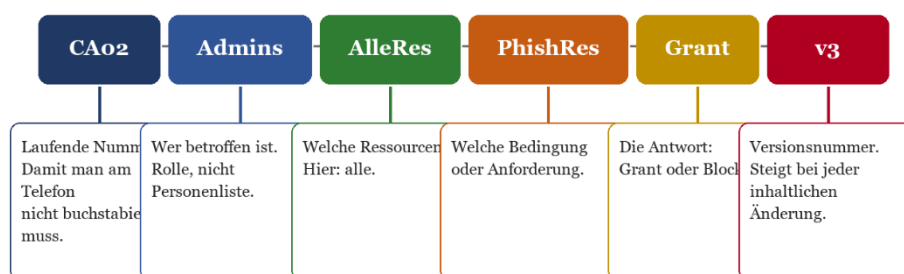
Namenskonvention und Break-Glass: die zwei Dinge, die man später nicht nachrüstet

Report-only rettet dich beim Einführen. Die Namenskonvention und die Break-Glass-Ausnahme retten dich in den Jahren danach — und beide lassen sich nachträglich nur mit erheblichem Aufwand einziehen, weil dann schon dreißig Richtlinien existieren, die niemand anfassen will.

Namen, die man am Telefon vorlesen kann

Conditional-Access-Richtlinien haben kein Eigentümerfeld. Es gibt keine Beschreibung, kein Änderungsdatum im Namen, keine Begründung. Alles, was du hast, ist der Name — also muss er arbeiten. Ein brauchbares Schema besteht aus laufender Nummer, Zielgruppe, Ressourcen, Bedingung, Antwort und Versionsnummer.

Anatomie eines Richtliniennamens



Notfallrichtlinien beginnen mit „EM01 - NUR IM NOTFALL AKTIVIEREN“ — im Ernstfall zählt jede Sekunde, die niemand mit Suchen verbringt.

Skizze 4: Sechs Bestandteile, ein Name. Die Versionsnummer ganz hinten ist der Teil, den die meisten Konventionen weglassen — und genau der, den man später vermisst.

Name	Bedeutung
CA01-Alle-AlleRes-MFA-Grant-v2	MFA für alle Benutzer auf alle Ressourcen, zweite Fassung.
CA02-Admins-AlleRes-PhishRes-Grant-v3	Phishing-resistente Stärke für privilegierte Rollen.
CA03-Alle-AlleRes-LegacyAuth-Block-v1	Legacy-Clients werden blockiert, unverändert seit Einführung.
CA04-Alle-M365-GeraetKonform-Grant-v4	Gerätekonformität für die Microsoft-365-Dienste.

CA05-Alle-AlleRes-DeviceCode-Block-v2	Geräteanmeldecode gesperrt, Raumgeräte ausgenommen.
EM01 - NUR IM NOTFALL AKTIVIEREN: MFA-Störung [1/3]	Deaktivierte Ausweichrichtlinie für den Störfall.

Tabelle 4: Beispiele. Wichtig ist nicht dieses Schema, sondern dass es genau eines gibt und alle sich daran halten.

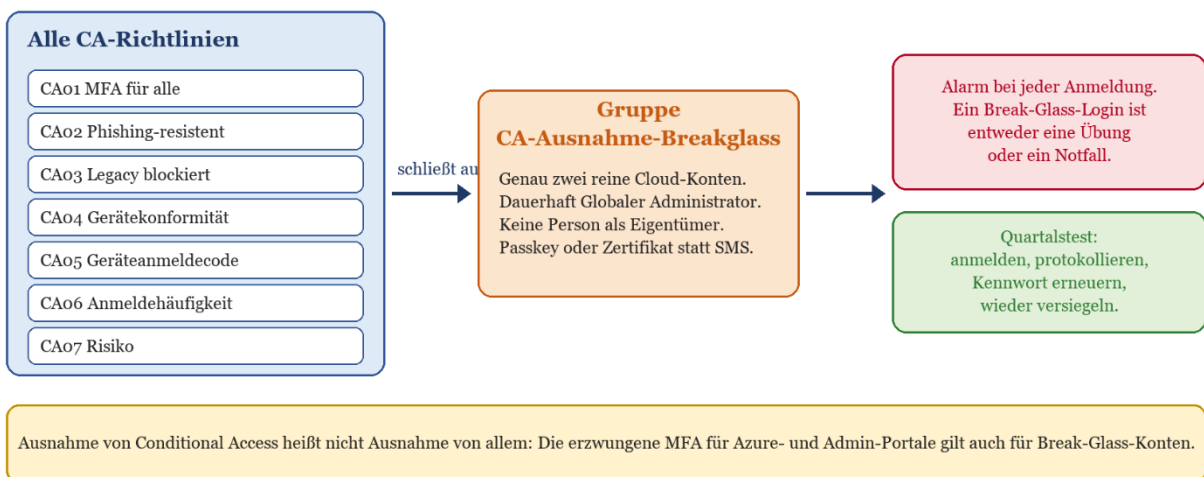
Die Versionsnummer verdient einen eigenen Absatz, weil sie so oft fehlt. Sie steigt bei jeder inhaltlichen Änderung: neue Ausnahme, geänderte Bedingung, andere Steuerung. Damit hast du erstens im Änderungsprotokoll einen Anker, zweitens in der Kommunikation mit dem Fachbereich eine Referenz und drittens beim Troubleshooting die Antwort auf die Frage, ob die Richtlinie, die gestern noch funktionierte, dieselbe ist wie heute. Wer es ernst meint, führt die Richtlinien ohnehin als Code über Microsoft Graph und legt sie in ein Repository — dann ergibt sich die Version fast von selbst.

Dazu gehört ein Register außerhalb des Tenants: eine Liste, welche Richtlinie welchem Team gehört, warum sie existiert und wann sie zuletzt überprüft wurde. Eine Tabelle reicht. Sie ist der Unterschied zwischen einer gepflegten Baseline und einem Sedimentgestein aus Einzelentscheidungen. Dieselbe Systematik empfiehlt sich für den restlichen Tenant — die Sammlung dazu findest du in [Tenant-Härtung: die 20 wichtigsten Schrauben](#).

Break-Glass: die Ausnahme, die überall gilt

Jede der sieben Richtlinien schließt dieselbe Gruppe aus, und in dieser Gruppe sind genau zwei reine Cloud-Konten mit dauerhafter Zuweisung der Rolle Globaler Administrator. Keine Person als Eigentümer, kein Namensbezug zu einem Menschen, keine Verknüpfung mit der lokalen Verzeichnissynchronisierung. Diese Konten existieren für den Fall, dass eine Fehlkonfiguration alle Administratoren aussperrt — ein Fall, der seltener eintritt, als man denkt, aber wenn er eintritt, dann vollständig.

Break-Glass: die einzige Ausnahme, die überall gilt



Skizze 5: Eine Gruppe, zwei Konten, überall ausgeschlossen — und mit Alarmierung auf jede einzelne Anmeldung. Ohne Überwachung ist ein Break-Glass-Konto nur ein Hintertürchen.

WARNUNG — Ausnahme heißt nicht Ausnahme von allem

Die erzwungene MFA für Azure- und Administrationsportale kennt keine Ausnahmen. Seit Oktober 2024 gilt sie für Azure-Portal, Entra Admin Center und Intune Admin Center, seit dem 1. Oktober

2025 zusätzlich für Azure CLI, Azure PowerShell, die mobile App, IaC-Werkzeuge und die REST-API bei schreibenden Operationen. Break-Glass-Konten sind ausdrücklich eingeschlossen. Ein Opt-out gibt es nicht, nur eine befristete Verschiebung des Starttermins, die spätestens am 1. Juli 2026 endete.

Konsequenz: Ein Break-Glass-Konto ohne registrierten MFA-Faktor ist im Ernstfall genauso ausgesperrt wie alle anderen. Microsoft empfiehlt für diese Konten Passkey (FIDO2) oder zertifikatsbasierte Authentifizierung — beides erfüllt die Anforderung und lässt sich physisch im Tresor deponieren.

Ein Zettel mit einem 40 Zeichen langen Kennwort im Umschlag ist ein hübsches Ritual, aber ohne zweiten Faktor ist er im Zweifel wertlos.

Zur Break-Glass-Ausnahme gehört zwingend die Überwachung: Jede Anmeldung eines dieser Konten löst einen Alarm aus, der bei einem Menschen ankommt und nicht in einem Sammelpostfach verhungert. Ein Break-Glass-Login ist entweder eine geplante Übung oder ein Notfall — beide Fälle wollen bemerkt werden. Wie du solche Alarmer sinnvoll schneidest, ohne im Rauschen unterzugehen, steht in [Alert Policies und Benachrichtigungen richtig aufsetzen](#); die Einrichtung und Pflege der Konten selbst behandelt [Break-Glass-Konten anlegen und überwachen](#) ausführlich.

Und dann testest du sie. Einmal im Quartal: anmelden, protokollieren, Kennwort erneuern, wieder versiegeln. Ein ungetestetes Break-Glass-Konto ist eine Annahme, keine Maßnahme. Erfahrungsgemäß scheitert der erste Test — abgelaufene Lizenz, abgelaufenes Kennwort, versehentlich in eine Richtlinie geraten. Genau deshalb testet man.

Notfallrichtlinien für den Tag, an dem MFA streikt

Neben der Break-Glass-Gruppe lohnt sich ein Satz deaktivierter Ausweichrichtlinien für Störungsszenarien. Sie beginnen mit „EM“ und einem deutlichen „NUR IM NOTFALL AKTIVIEREN“, enthalten die Art der Störung und eine Reihenfolgennummer. Wenn der MFA-Dienst ausfällt oder ein Anbieter für externe Authentifizierungsmethoden nicht erreichbar ist, aktivierst du die Kette in der dokumentierten Reihenfolge — statt unter Zeitdruck neue Richtlinien zu bauen, was regelmäßig zu genau der Fehlkonfiguration führt, für die es dann wieder das Break-Glass-Konto braucht.

Ergänzend gehört der Schutz der Richtlinien selbst dazu. Mit geschützten Aktionen kannst du verlangen, dass jemand vor dem Anlegen, Ändern oder Löschen einer Conditional-Access-Richtlinie eine frische MFA vorlegt. Das kostet zwei Sekunden und verhindert, dass ein übernommenes Administratorkonto die Baseline im Vorbeigehen abräumt. In dieselbe Kategorie gehört die Kontrolle darüber, welche Anwendungen sich überhaupt Berechtigungen im Tenant holen dürfen — siehe [App-Registrierungen und Consent-Governance](#).

Betrieb: damit die Baseline nicht doch noch nervt

Eine Baseline ist kein Projekt mit Abschlussbericht, sondern ein Zustand, der gepflegt wird. Der Verfall beginnt harmlos: eine Ausnahme für einen Fachbereich, eine zweite für ein Projekt, eine dritte, weil der Vertrieb kurz vor Quartalsende keine Zeit für Diskussionen hat. Nach zwei Jahren sind es vierzig Richtlinien und die Baseline ist eine Erinnerung.

Ausnahmen mit Verfallsdatum

Die einzige Ausnahme ohne Ablaufdatum ist die Break-Glass-Gruppe. Alle anderen bekommen ein Datum, einen Verantwortlichen und einen Grund. Nicht als Bürokratie, sondern weil eine

Ausnahme ohne Ablaufdatum nach zwei Jahren niemandem mehr erklärbar ist — und niemand sie dann noch zu entfernen wagt.

Feld	Beispiel	Warum es gebraucht wird
Richtlinie	CA03-Alle-AlleRes-LegacyAuth-Block-v1	Ohne Bezug lässt sich die Ausnahme später nicht zuordnen.
Betroffenes Konto	sve-scan-mfp-halle3	Konto, nicht Gruppe. Gruppen wachsen unbemerkt.
Grund	Multifunktionsgerät ohne Modern-Auth-Unterstützung	Der Grund entscheidet, wann die Ausnahme wegfällt.
Ausgleichsmaßnahme	Nur SMTP, IP-Beschränkung, kein Postfachzugriff	Eine Ausnahme ohne Ausgleich ist ein offenes Loch.
Befristet bis	31.03.2027 (Gerätetausch)	Das Datum bindet die Ausnahme an ein Ereignis.
Verantwortlich	Team Client-Management	Jemand muss die Frist im Blick haben.

Tabelle 5: Das Ausnahmeregister. Sechs Spalten, eine Tabelle, ein Quartalstermin — mehr Prozess braucht es nicht.

Regelmäßig konsolidieren statt ergänzen

Wenn eine neue Anforderung kommt, ist die erste Frage nicht „Welche Richtlinie brauche ich dafür?“, sondern „In welche bestehende passt sie?“. Bei 240 möglichen Richtlinien klingt das übervorsichtig, aber das Problem ist nie das Limit, sondern die Übersicht: Jede zusätzliche Richtlinie multipliziert die Zahl der Wechselwirkungen, die man beim Troubleshooting im Kopf haben muss.

Hilfreich sind Filter statt Aufzählungen — Filter für Anwendungen und Gruppen statt langer GUID-Listen, die irgendwann an die Größenbegrenzung einer einzelnen Richtlinie stoßen. Wo Microsoft Security Copilot mit bereitgestellten Compute-Einheiten vorhanden ist, kann der Optimierungsagent für Conditional Access bestehende Richtlinien analysieren, Lücken zeigen und Zusammenlegungen vorschlagen. Vorhanden ist er in den wenigsten mittelständischen Tenants — die halbjährliche manuelle Durchsicht ersetzt er ohnehin nicht.

Wirkung berichten, nicht Aktivität

Wenn die Baseline steht, kommt irgendwann die Frage aus der Geschäftsführung, was das gebracht hat. Die schlechte Antwort ist eine Zahl aus dem Secure Score. Die gute Antwort besteht aus zwei Sätzen: wie viele Anmeldungen mit Legacy-Protokollen im Monat blockiert wurden, und wie viele Konten trotz gestohlener Kennwörter nicht übernommen werden konnten. Wie man den Punktestand richtig einordnet, statt ihn zum Ziel zu erklären, steht in [Secure Score: sinnvoll nutzen statt Punktejagd](#); die Aufbereitung für das Management behandelt [Security-Reporting für die Geschäftsführung](#).

Für regulierte Umgebungen kommt ein zweiter Aspekt dazu: Zugriffskontrolle und Multifaktor-Authentifizierung sind in den einschlägigen Anforderungskatalogen keine Empfehlung, sondern Erwartung. Die Zuordnung technischer Maßnahmen zu den Pflichten aus NIS2 ist Thema von [NIS2 aus Security-Sicht: technische Maßnahmen in M365](#). Und wenn es doch passiert ist, hilft ein vorbereiteter Ablauf mehr als jede Richtlinie — siehe [Incident-Response-Plan für Microsoft 365](#).

FAKTEN — Was Conditional Access nicht abdeckt

Dienstprinzipale und verwaltete Identitäten werden von benutzerbezogenen Richtlinien nicht erfasst. Aufrufe von Dienstprinzipalen laufen daran vorbei; dafür gibt es Conditional Access für Workload Identities mit eigener Lizenz.

Benutzerkonten, die als Dienstkonten missbraucht werden, sind dagegen voll betroffen — inklusive der erzwungenen MFA für Azure-Verwaltungsoperationen. Der Ausweg heißt Migration auf

verwaltete Identitäten, nicht Ausnahme.

Gäste aus Partnerorganisationen bringen ihre Authentifizierung aus dem Heimtenant mit, sofern die tenantübergreifenden Zugriffseinstellungen das erlauben. Ohne diese Vertrauensstellung müssen Gäste im Ziellant erneut MFA leisten.

Häufige Fragen

Reichen die sieben Richtlinien wirklich für den Anfang?

Für den Anfang ja. Sie decken die Angriffswege ab, die in der Praxis tatsächlich genutzt werden: fehlende zweite Faktoren, Legacy-Protokolle, unverwaltete Geräte, Geräteanmeldecode-Phishing und zu lange Sitzungen für privilegierte Konten. Was danach kommt — Standortfilter, Token-Schutz, Richtlinien für privilegierte Arbeitsstationen, Sperrung von Ländern, aus denen nie eine Anmeldung erwartet wird — baust du auf einem Fundament auf, das du verstanden hast. Umgekehrt funktioniert es nicht.

Was passiert, wenn ich Security Defaults einfach anlasse?

Dann kannst du keine eigenen Richtlinien aktivieren, und du hast keine Möglichkeit, Ausnahmen zu definieren — Security Defaults sind an oder aus, nichts dazwischen. Für kleine Tenants ohne P1-Lizenzen ist das die richtige Wahl. Sobald es das erste Multifunktionsgerät, den ersten Sonderfall oder die erste Anforderung nach abgestuften Schutz gibt, brauchst du Conditional Access. Die Gegenüberstellung im Detail liefert [Security Defaults oder Conditional Access?](#).

Kann ich alle sieben Richtlinien am selben Tag scharfschalten?

Technisch ja. Empfehlenswert ist es nicht, mit zwei Ausnahmen: CA03 und CA05 kannst du nach einer sauberen Report-only-Phase gemeinsam aktivieren, weil sie nur bereits identifizierte Sonderfälle treffen. CA01, CA02, CA04 und CA06 verändern den Alltag spürbar und gehören in getrennte Wellen — schon damit der Helpdesk bei einer Beschwerdewelle weiß, welche Änderung sie ausgelöst hat.

Wie viele Break-Glass-Konten brauche ich?

Zwei. Eines ist zu wenig, weil ein einzelnes Konto genau einen Ausfall braucht, um wirkungslos zu sein. Mehr als zwei erhöhen die Angriffsfläche, ohne die Verfügbarkeit wesentlich zu verbessern. Beide sind reine Cloud-Konten, beide dauerhaft Globaler Administrator, beide mit unterschiedlichen phishing-resistenten Faktoren und getrennt verwahrt.

Was mache ich mit dem Multifunktionsgerät, das nur SMTP kann?

Nicht die Legacy-Richtlinie aufweichen. Stattdessen den Scan-to-Mail-Weg auf einen authentifizierten Übermittlungsweg oder ein internes Relay umstellen und das Gerätekonto so eng wie möglich schneiden: kein Postfachzugriff, keine Anmeldung an anderen Diensten, IP-Beschränkung. Wenn eine Ausnahme unumgänglich ist, kommt sie ins Ausnahmeregister mit Ablaufdatum und Ausgleichsmaßnahme.

Warum wird ein ausgeschlossener Benutzer trotzdem zur MFA aufgefordert?

Weil Ausschlüsse pro Richtlinie gelten, nicht pro Benutzer. Wenn du jemanden aus CA01 ausschließt, aber CA04 verlangt für dieselbe Ressource ein konformes Gerät oder MFA, dann greift eben CA04. Deshalb gehört zum Test einer Ausnahme immer die Frage, welche anderen Richtlinien auf dieselbe Anmeldung passen. Das What-If-Werkzeug beantwortet das in Sekunden.

Muss ich Gäste in die Baseline aufnehmen?

Ja, und zwar in CA01 ausdrücklich. Gastkonten sind ein beliebter Umweg, weil sie oft vergessen werden. Ob ein Gast seine MFA aus dem Heimattenant mitbringen darf, steuerst du über die tenantübergreifenden Zugriffseinstellungen — eine bewusste Entscheidung, keine Voreinstellung. Das gesamte Umfeld externer Zusammenarbeit behandelt [Gastzugriff und externe Freigaben härten](#).

Wie oft überprüfe ich die Baseline?

Halbjährlich vollständig, quartalsweise die Ausnahmen. Zusätzlich anlassbezogen: bei Lizenzwechsel, nach einem Sicherheitsvorfall, bei größeren Änderungen an der Geräteverwaltung und immer dann, wenn Microsoft eine neue verwaltete Richtlinie in den Tenant stellt. Bei jeder inhaltlichen Änderung steigt die Versionsnummer im Richtlinienamen.

Fazit

Eine Conditional-Access-Baseline, die nicht nervt, ist keine besonders clevere Baseline. Sie ist eine kleine. Sieben Richtlinien, die für alle gelten, breit geschnitten, sauber benannt, versioniert und mit genau einer dauerhaften Ausnahme. Der Rest ist Betriebsdisziplin: Report-only vor jeder Aktivierung, Ausnahmen mit Ablaufdatum, halbjährliche Durchsicht, vierteljährlicher Break-Glass-Test.

Der häufigste Fehler ist nicht die falsche Richtlinie, sondern die fehlende Reihenfolge. Wer die Security Defaults abschaltet, bevor die Baseline steht, tauscht mittelmäßigen Schutz gegen gar keinen. Wer ohne Report-only aktiviert, lernt die Sonderfälle seines Hauses am Montagmorgen über die Telefonanlage kennen. Und wer die Break-Glass-Konten anlegt, ohne sie je zu testen, hat eine Feuerleiter gebaut, die im Brandfall zum ersten Mal benutzt wird.

Der Aufwand für eine ordentliche Einführung liegt bei wenigen Tagen, verteilt über acht Wochen. Der Aufwand für die Aufräumarbeiten nach einer übernommenen Identität liegt deutlich darüber — und wird selten von denen bezahlt, die vorher die Zeit nicht hatten. Wie so ein Verlauf in der Realität aussieht, zeigt das [Dossier TerminalFix und der Berlin-Hack](#).

WEITER — Passende Beiträge aus dieser Reihe

- › [Microsoft 365 Security](#) — die Übersicht über alle Bausteine
- › [MFA in Microsoft 365 richtig einführen](#) — der Faktor, auf dem die halbe Baseline steht
- › [Legacy Authentication endgültig abschalten](#) — die Vorarbeit für CA03
- › [Tenant-Härtung: die 20 wichtigsten Schrauben](#) — was außerhalb von Conditional Access noch zu tun ist
- › [Break-Glass-Konten anlegen und überwachen](#) — Einrichtung, Verwahrung, Überwachung
- › [Security Defaults oder Conditional Access?](#) — die Entscheidung vor der Entscheidung
- › [Microsoft 365 Security Beratung](#) — Unterstützung bei Auslegung und Rollout
- › [Schulung Microsoft 365 Security](#) — wenn das Team es selbst können soll

