

Security Defaults oder Conditional Access? Der Umschaltpfad, bei dem du nicht selbst vor der Tür stehst

Es gibt zwei Arten, wie dieses Gespräch beginnt. Variante eins: „Wir haben Security Defaults an, das reicht doch.“ Variante zwei: „Wir haben Security Defaults ausgeschaltet, weil der Scanner im zweiten Stock keine Mails mehr verschicken konnte. Conditional Access wollten wir dann nächste Woche machen.“ Die zweite Variante ist deutlich häufiger, als irgendjemand zugeben möchte, und sie beschreibt einen Tenant, der seit acht Monaten ohne Mehrfaktorpflicht läuft, weil ein Multifunktionsgerät wichtiger war als die Anmeldung von zweihundert Leuten.

Security Defaults sind ein Geschenk. Sie kosten nichts, sie sind mit zwei Klicks aktiv, und Microsoft rechnet vor, dass Mehrfaktorauthentifizierung zusammen mit einem Riegel vor der Legacy-Authentifizierung mehr als 99,2 Prozent der üblichen identitätsbasierten Angriffe abfängt. Für einen Tenant ohne Premiumlizenzen gibt es dazu schlicht keine Alternative. Sie sind aber auch ein Kippschalter: an oder aus, für alle, ohne Ausnahme, ohne Bedingung, ohne Erklärung.

Genau daran scheitert der Betrieb. Nicht am Sicherheitsniveau — das ist ordentlich —, sondern an dem einen Sonderfall, den es in jedem Haus gibt und für den der Schalter kein Ventil hat. Dieser Beitrag gehört zur Serie [Microsoft 365 Security](#) und klärt drei Dinge: was Security Defaults tatsächlich erzwingen, wo ihre Grenze verläuft, und wie du auf Conditional Access umschaltest, ohne dich dabei selbst aus deinem eigenen Tenant auszusperrten. Letzteres passiert nämlich häufiger als jeder Angriff.

FAKTEN · Die Kurzfassung, falls du gleich weitermusst

Wenn du keine Lizenz für Conditional Access hast, lass Security Defaults an und lies den Rest später. Wenn du eine hast und der erste echte Sonderfall aufgetaucht ist, dann in dieser Reihenfolge:

- › Break-Glass-Konten anlegen, testen, überwachen — vor allem anderen.
- › Richtlinien in Report-only anlegen und mindestens eine Woche auswerten.
- › Conditional Access auf An schalten und erst danach, unmittelbar danach, Security Defaults aus.
- › Gerät, Standort, Sitzungsdauer und Risiko in den Wochen darauf ergänzen.

Was Security Defaults erzwingen — ohne dich vorher zu fragen

Security Defaults sind kein Regelwerk, sondern ein Paket. Du kannst es nehmen oder lassen, aber du kannst es nicht aufschnüren. Das ist gleichzeitig ihre größte Stärke: Es gibt keine Möglichkeit, sie versehentlich falsch zu konfigurieren, weil es nichts zu konfigurieren gibt.

Die sechs Regeln im Paket

Im Einzelnen erzwingt der Schalter Folgendes. Erstens die Registrierung für Mehrfaktorauthentifizierung für sämtliche Benutzer. Zweitens Mehrfaktorauthentifizierung bei jeder einzelnen Anmeldung für vierzehn privilegierte Rollen — vom Globalen Administrator über

den Exchange-Administrator bis hinunter zum Helpdesk-Administrator und zum Kennwortadministrator. Drittens Mehrfaktorauthentifizierung für alle übrigen Benutzer immer dann, wenn Microsoft es anhand eigener Signale für nötig hält. Viertens eine Blockade der Legacy-Authentifizierung, einschließlich Exchange ActiveSync mit Basisauthentifizierung. Fünftens eine Blockade des Device Code Flow. Und sechstens Mehrfaktorauthentifizierung für privilegierte Tätigkeiten: Azure-Portal, Entra Admin Center, Azure PowerShell und Azure CLI, und zwar für jeden, nicht nur für Administratoren.

Zwei Details lohnen den zweiten Blick. Die frühere Karenzfrist von vierzehn Tagen für die MFA-Registrierung gibt es seit dem 29. Juli 2024 nicht mehr — weder in neuen noch in bestehenden Tenants. Wer sich anmeldet, registriert sich, sofort. Und der Device Code Flow: Bei allen neuen Tenants seit dem 1. Juli 2026 blockieren Security Defaults dieses Verfahren mit. Das ist sicherheitstechnisch hervorragend, weil Angreifer den Ablauf gern für Phishing missbrauchen, und betrieblich schmerzhaft, wenn ein Besprechungsraumsystem oder ein Drucker genau darauf angewiesen ist.

Ein Schalter, sechs Regeln — und alles andere bleibt draußen

Security Defaults sind kein Regelwerk, sondern ein Kippschalter. Das ist die Stärke und zugleich die ganze Grenze.



Die rechte Spalte ist keine Kritik. Sie ist die Preisliste: Was nichts kostet, kann auch nichts unterscheiden.

Skizze 1: Der ganze Funktionsumfang auf einer Seite. Die linke Spalte ist der Grund, warum du den Schalter anlassen solltest. Die rechte ist der Grund, warum du irgendwann umsteigst.

Wahrscheinlich sind sie bei dir schon an

Tenants, die seit dem 22. Oktober 2019 angelegt wurden, bekommen Security Defaults bei der Erstellung mit — es gibt lediglich eine Karenz von 24 Stunden, damit du dein frisches Verzeichnis überhaupt erst einrichten kannst. Darüber hinaus schaltet Microsoft den Schalter bei Bestandstenants von sich aus ein, wenn drei Dinge zusammenkommen: keine Conditional-Access-Richtlinien, keine Premiumlizenzen und keine aktive Nutzung von Legacy-Clients. Du wirst darüber per E-Mail informiert. Ob jemand diese E-Mail liest, ist eine andere Frage.

Das führt regelmäßig zu dem Anruf, der mit „bei uns fragt Outlook seit heute Morgen nach einer App“ beginnt. Kein Angriff, keine Störung — nur ein Schalter, den jemand anders umgelegt hat, weil du es selbst nicht getan hast.

WICHTIG · Der Schritt, den fast alle vergessen

Nach dem Einschalten solltest du die bestehenden Tokens entziehen, sonst laufen angemeldete Sitzungen ungestört weiter und niemand registriert sich für MFA. Microsoft nennt dafür ausdrücklich das Graph-PowerShell-Cmdlet `Revoke-MgUserSignInSession`. Ohne diesen Schritt hast du eine Richtlinie, die auf dem Papier greift und im Alltag wochenlang niemanden erreicht.

Was Security Defaults nicht können — und warum das der Punkt ist

Die Liste der Dinge, die Security Defaults nicht beherrschen, ist keine Mängelliste. Sie ist die Preisliste. Was nichts kostet und ohne Konfiguration auskommt, kann keine Unterscheidungen treffen. Genau das ist aber der eigentliche Zweck von Conditional Access: Unterscheidungen treffen.

Kein Gerät, kein Standort, kein Risiko

Security Defaults können nicht wissen, ob sich jemand von einem verwalteten Firmennotebook oder von einem Internetcafé aus anmeldet. Sie kennen kein konformes Gerät, keinen Hybrid Join, keine Geräteplattform. Sie kennen kein Land, keinen IP-Bereich, kein vertrauenswürdiges Netzwerk. Und sie werten kein Risiko aus: Wenn die Zugangsdaten eines Kontos in einem Datenleck auftauchen, passiert genau nichts. Der Benutzer bekommt beim nächsten Mal vielleicht eine MFA-Aufforderung, vielleicht auch nicht — die Entscheidung liegt bei Microsofts Signalen, nicht bei dir.

Ebenso wenig lässt sich die Sitzung steuern. Keine Anmeldehäufigkeit, keine Vorgabe zur Browserpersistenz, keine app-erzwungenen Einschränkungen für nicht verwaltete Geräte. Und du kannst nicht verlangen, dass deine Administratoren sich phishing-resistent anmelden. Ein Code aus einer Authenticator-App erfüllt die Anforderung genauso wie ein Sicherheitsschlüssel — auch wenn nur eines von beiden gegen einen ordentlich gemachten Adversary-in-the-Middle-Angriff hilft.

Keine Ausnahme — bis auf genau eine

Es gibt exakt eine eingebaute Ausnahme, und die hast du nicht gewählt: Das Synchronisierungskonto von Entra Connect beziehungsweise Cloud Sync — alles, was der Rolle „Verzeichnissynchronisierungskonten“ zugewiesen ist — bleibt außen vor. Sonst würde die Verzeichnissynchronisierung beim Umlegen des Schalters sofort stehen bleiben. Für alle anderen Konten gilt: keine Ausnahme, keine Ausrede.

Das trifft in der Praxis vier Gruppen. Dienstkonto, die als Benutzerkonto angelegt wurden und irgendein Skript betreiben. Multifunktionsgeräte, Scanner und Kopierer, die per SMTP Mails verschicken. Fachanwendungen, die per IMAP oder POP3 ein Postfach leerräumen. Und Geräte

ohne Tastatur, die den Device Code Flow benutzen. Jede dieser Gruppen fällt beim Einschalten um, und keine davon lässt sich mit Bordmitteln herausnehmen.

WARNUNG · Der klassische Fehler und seine Folgekosten

Weil eine einzelne Ausnahme nicht möglich ist, schalten viele Häuser den kompletten Schalter wieder aus — wegen eines Scanners. Damit fällt nicht nur die Ausnahme, sondern die gesamte Mehrfaktorpflicht für alle Benutzer und alle Administratoren.

- › Richtig wäre: Legacy-Authentifizierung sauber abschalten und das Gerät auf modernes SMTP umstellen.
- › Oder, wenn das nicht geht: auf Conditional Access wechseln und dort eine eng gefasste Ausnahme bauen — mit Standortbindung und ohne Postfachrechte.
- › Falsch ist immer: den Schutz für zweihundert Leute abschalten, damit ein Kopierer weiterhin Basisauthentifizierung sprechen darf.

Der Schalter kennt nur alle

Und weil das noch nicht reicht: Security Defaults und Conditional Access schließen sich gegenseitig aus. Du kannst nicht den Schalter anlassen und daneben zwei Richtlinien bauen, die die Lücken schließen. Solange Security Defaults aktiv sind, greifen deine Conditional-Access-Richtlinien nicht. Es gibt kein Sowohl-als-auch, es gibt nur ein Entweder-oder — und deshalb einen Moment des Umschaltens, den du planen musst.

Merkmal	Security Defaults	Conditional Access
Lizenz	keine, in jedem Tenant enthalten	mindestens Entra ID P1, auch in Microsoft 365 Business Premium
Konfiguration	an oder aus, sonst nichts	vollständig frei, Bedingungen und Kontrollen kombinierbar
MFA für Benutzer	ja, Zeitpunkt entscheidet Microsoft	ja, Zeitpunkt und Umfang entscheidest du
MFA für Administratoren	ja, 14 Rollen, bei jeder Anmeldung	ja, frei wählbare Rollen, auf Wunsch phishing-resistent
Legacy-Authentifizierung	wird blockiert, ohne Ausnahme	wird blockiert, Ausnahmen eng gefasst möglich
Device Code Flow	wird blockiert, ohne Ausnahme	blockierbar, Ausnahmen für Raumsysteme möglich
Gerätezustand	nicht auswertbar	konform, Hybrid Join, Plattform, verwaltete App
Standort und Netzwerk	nicht auswertbar	Land, IP-Bereich, benannte und vertrauenswürdige Netzwerke
Risikosignale	nicht auswertbar	Anmelde- und Benutzerrisiko, dafür allerdings P2 nötig
Sitzungssteuerung	nicht möglich	Anmeldehäufigkeit, Browserpersistenz, App-Einschränkungen
Ausnahmen	nur das Synchronisierungskonto	beliebige Konten und Gruppen, inklusive Break-Glass
Testbetrieb vorab	nicht vorgesehen	Report-only, Arbeitsmappe, Auswirkungsanalyse
Betriebsaufwand	praktisch null	spürbar: Dokumentation, Ausnahmen, regelmäßige Prüfung

Tabelle 1: Die Gegenüberstellung, um die es eigentlich geht. Die letzte Zeile erklärt, warum die Entscheidung selten eine Frage der Sicherheit ist und meistens eine des Betriebs.

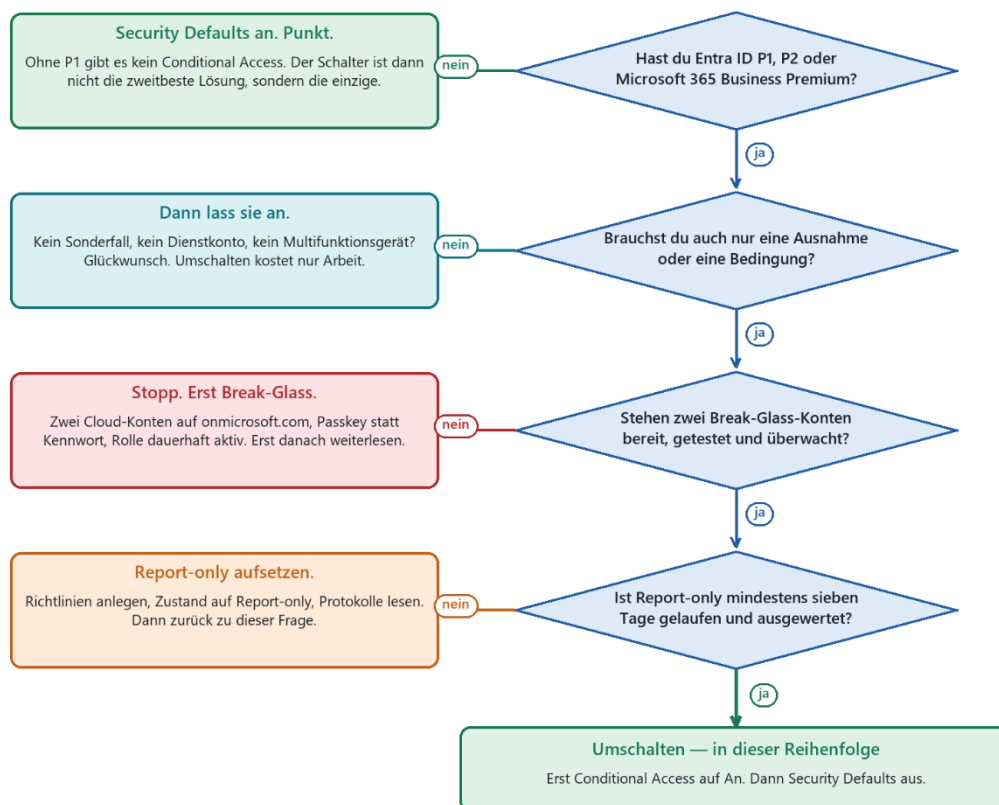
Wie ein tragfähiges Grundgerüst aus Richtlinien aussieht, das diesen Betriebsaufwand klein hält, steht ausführlich unter [Conditional Access: Baselines, die nicht nerven](#). Für den Umstieg genügen zunächst vier Richtlinien — dazu gleich mehr.

Der Entscheidungsbaum: bleiben oder umschalten?

Die Frage aus der Überschrift des Beitrags ist eigentlich falsch gestellt. Es ist keine Glaubensfrage und auch keine Frage der Reife. Es sind vier Fragen, die sich in dieser Reihenfolge stellen lassen, und drei davon haben eine unangenehm eindeutige Antwort.

Entscheidungsbaum: bleiben oder umschalten?

Vier Fragen. Wer bei der dritten hängen bleibt, schaltet heute noch nicht um — sondern legt erst Konten an.



Die dritte Frage ist die einzige, bei der ein Nein wirklich wehtut — aber erst später, im Ernstfall.

Skizze 2: Vier Fragen, vier mögliche Ausgänge. Wer bei Frage drei hängen bleibt, schaltet heute nicht um — sondern legt erst Konten an.

Frage 1: Hast du überhaupt eine Lizenz?

Conditional Access setzt mindestens Entra ID P1 voraus. Das steckt in Microsoft 365 E3 und E5, in Business Premium und in Entra ID P1 als Einzelprodukt. In Business Basic und Business Standard steckt es nicht. Riskobasierte Richtlinien — Anmelderisiko, Benutzerrisiko — verlangen darüber hinaus P2 mit Entra ID Protection.

Wenn die Antwort Nein lautet, endet die Diskussion hier. Security Defaults sind dann nicht die zweitbeste Lösung, sondern die einzige, und sie sind eine gute. Lass sie an, kümmere dich um die Bestandsaufnahme der Legacy-Clients und komm wieder, wenn die Lizenzfrage neu verhandelt

wird. Nebenbei: Für die verpflichtende Azure-MFA reichen Security Defaults als Nachweis vollkommen aus.

Frage 2: Ist der erste echte Sonderfall aufgetaucht?

Solange dein Tenant ohne Ausnahme auskommt, kostet der Umstieg nur Arbeit. Ein sauber laufender Schalter ist besser als ein halbfertiges Richtlinienwerk. Die ehrliche Antwort in den meisten Häusern lautet allerdings: Der Sonderfall ist längst da, er heißt Scanner, Buchhaltungsimport oder Besprechungsraum, und er wird bislang durch kollektives Wegsehen gelöst.

Drei Auslöser, bei denen die Antwort feststeht

- Du willst Administratoren zwingend auf phishing-resistente Verfahren festlegen. Das geht mit Security Defaults nicht, mit Authentifizierungsstärken in Conditional Access schon.
- Du hast eine Anforderung an Standort oder Gerät — etwa aus einer Kundenvereinbarung, aus einer Zertifizierung oder aus einer Risikoanalyse. Der Schalter kann beides nicht.
- Du brauchst eine dokumentierte, begründete und zeitlich begrenzte Ausnahme, die ein Prüfer nachvollziehen kann. Mit Security Defaults gibt es nichts zu dokumentieren außer dem Zustand An.

TIPP · Ein sinnvoller Zwischenschritt

Wenn du eine P1-Lizenz hast, aber noch kein Richtlinienwerk, musst du nicht alles auf einmal bauen. Fang mit den vier Richtlinien an, die Security Defaults eins zu eins ersetzen. Gerät, Standort, Sitzungsdauer und Risiko kommen später dazu — jede einzeln, jede erst in Report-only. Ein Umstieg in vier Wochen mit vier Schritten ist besser als ein Umstieg an einem Freitagnachmittag mit zwölf.

Der Umschaltpfad, ohne dich selbst auszusperrern

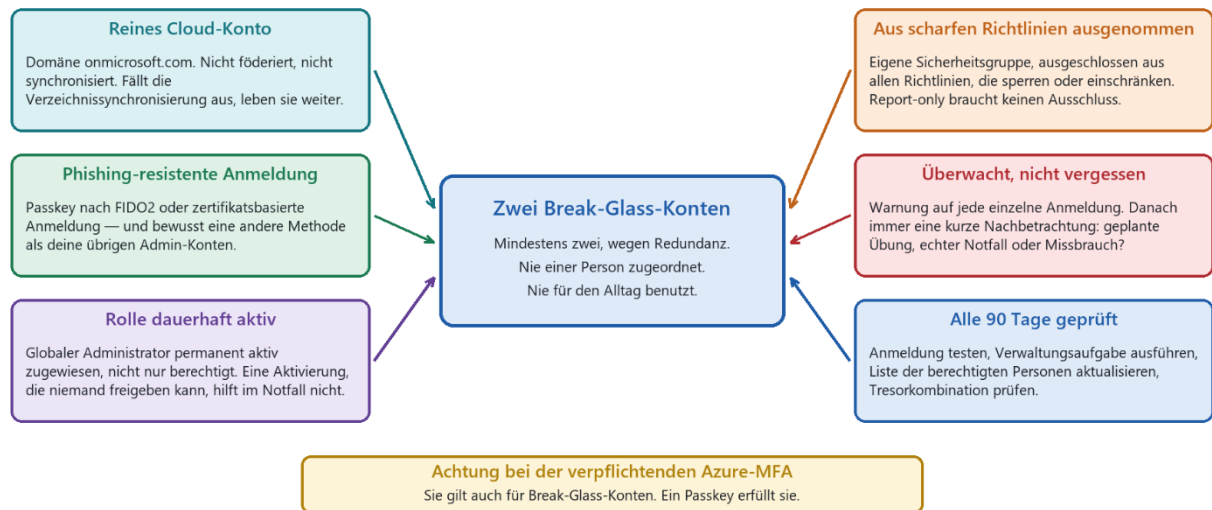
Jetzt zum eigentlich Interessanten. Der Umstieg ist kein Migrationsprojekt, sondern ein Ablauf von etwa zwei Wochen, in dem genau ein Schritt gefährlich ist — und der dauert dreißig Sekunden.

Schritt 0: Break-Glass, bevor irgendetwas anderes passiert

Bevor du eine einzige Richtlinie anlegst, brauchst du mindestens zwei Notfallzugänge. Microsoft empfiehlt dafür ausdrücklich zwei oder mehr reine Cloud-Konten auf der onmicrosoft.com-Domäne, die weder föderiert noch synchronisiert sind und die die Rolle Globaler Administrator dauerhaft aktiv zugewiesen bekommen — nicht nur berechtigt. Die vollständige Bauanleitung samt Überwachung findest du unter [Break-Glass-Konten anlegen und überwachen](#).

Anatomie der beiden Konten, die du nie brauchst

Bis zu dem einen Tag, an dem du sie brauchst. Dann entscheiden sie darüber, ob du noch Administrator bist.



Ein Break-Glass-Konto mit Kennwort auf einem Zettel im Serverraum ist kein Notfallkonzept, sondern ein Zweitschlüssel für Angreifer.

Skizze 3: Sechs Eigenschaften, ohne die ein Notfallkonto keines ist. Der Punkt unten rechts ist der, an dem die meisten Konzepte nach zwei Jahren scheitern.

Wichtig ist die Wahl des Anmeldeverfahrens: ein Passkey nach FIDO2 oder eine zertifikatsbasierte Anmeldung — und bewusst eine andere Methode als bei deinen normalen Administratorkonten. Wenn deine Admins die Authenticator-App benutzen und der Push-Dienst ausfällt, nützt dir ein Notfallkonto mit derselben App wenig. Beide Verfahren erfüllen zugleich die verpflichtende Azure-MFA, die auch für Break-Glass-Konten gilt. Wie du Passkeys ausrollst, steht unter [Passwordless: FIDO2 und Passkeys in der Praxis](#).

WICHTIG · Ausschließen heißt nicht ungeschützt

Break-Glass-Konten werden aus allen Richtlinien ausgenommen, die sperren oder einschränken — dafür legst du eine eigene Sicherheitsgruppe an. Aus Richtlinien im Zustand Report-only müssen sie nicht ausgeschlossen werden, weil dort nichts erzwungen wird. Der Schutz dieser Konten kommt nicht aus der Richtlinie, sondern aus dem phishing-resistenten Verfahren, dem Tresor und der Überwachung.

- › Warnung auf jede einzelne Anmeldung, mit anschließender kurzer Nachbetrachtung: geplante Übung, echter Notfall oder Missbrauch?
- › Funktionsprüfung mindestens alle 90 Tage, ebenso nach jedem Personalwechsel im Administrationsteam.
- › Zugangsdaten an zwei getrennten, gesicherten Orten — nicht im Kennwortspeicher, auf den ein kompromittiertes Adminkonto Zugriff hat.

Für die Alarmierung selbst brauchst du eine Regel, die zuverlässig bei einem Menschen ankommt. Wie du solche Meldungen aufsetzt, ohne im Rauschen unterzugehen, steht unter [Alert Policies und Benachrichtigungen richtig aufsetzen](#); wenn die Anmeldeprotokolle ohnehin in einem Arbeitsbereich landen, ist der Weg über [Microsoft Sentinel anbinden: wann es sich lohnt](#) der bequemere.

Schritt 1: Bestandsaufnahme, damit du weißt, was umfällt

Bevor du irgendetwas scharf schaltest, brauchst du eine Liste. Filtere die Anmeldeprotokolle nach Legacy-Authentifizierung und notiere jedes Konto, jede Anwendung und jede IP-Adresse, die dort auftaucht. Das Vorgehen im Detail — inklusive der Frage, welche Protokolle in Exchange Online überhaupt noch aktiv sein können — steht unter [Legacy Authentication endgültig abschalten](#).

Dazu kommen drei weitere Listen: alle Benutzerkonten, die eigentlich Dienstkonten sind; alle Geräte, die per SMTP Mails verschicken; und alles, was den Device Code Flow benutzt. Für den letzten Punkt gibt es in Conditional Access inzwischen eine eigene Bedingung, sodass du Raumsysteme gezielt herausnehmen kannst, während der Ablauf für alle übrigen Konten blockiert bleibt. Mit Security Defaults hast du diese Wahl nicht.

Und schließlich: Wenn deine Leute noch gar nicht flächendeckend für MFA registriert sind, ist der Umstieg auf Conditional Access nicht dein erstes Problem. Dann brauchst du zuerst eine ordentliche Einführung, mit Ankündigung, Registrierungsfenster und Rückfallebene — siehe [MFA in Microsoft 365 richtig einführen](#).

Schritt 2: Report-only, und zwar lange genug

Report-only ist der Grund, warum ein Umstieg auf Conditional Access beherrschbar ist. Eine Richtlinie in diesem Zustand wird bei jeder Anmeldung vollständig ausgewertet, aber nicht durchgesetzt. Niemand wird gesperrt, niemand bekommt eine zusätzliche Aufforderung — und im Anmeldeprotokoll steht trotzdem, was passiert wäre.

Report-only lesen, bevor du scharf schaltest

Vier Ergebnisse stehen im Anmeldeprotokoll. Nur eines davon darfst du ignorieren.

Ergebnis im Protokoll	Was tatsächlich passiert ist	Was du damit machst
Report-only: Success	Alle Bedingungen trafen zu, die geforderte Kontrolle war im Token bereits erfüllt.	Nichts. Das ist der Beleg dafür, dass die Richtlinie im Alltag nicht stört.
Report-only: Failure	Bedingungen trafen zu, die Kontrolle wurde nicht erfüllt — oder es greift eine Blockade.	Jeden Treffer einzeln erklären. Das sind genau die Anmeldungen, die am Tag T aussetzen.
Report-only: User action required	Es hätte eine Aufforderung gegeben, etwa zu MFA. Im Report-only wird niemand gefragt.	Bei MFA-Richtlinien erwartbar. Interessant wird die Menge: Wie viele Leute trifft es am ersten Morgen?
Report-only: Not applied	Eine Bedingung traf nicht zu, oder das Konto ist ausgeschlossen.	Zuweisung prüfen. Wenn hier fast alles landet, ist die Richtlinie zu eng gefasst.
Ausnahme: Richtlinien mit dem Bereich Benutzeraktionen lassen sich in Report-only nicht auswerten. Und Richtlinien, die ein konformes Gerät verlangen, fragen auf macOS, iOS und Android trotzdem nach einem Zertifikat.		

Report-only erzwingt nichts — deshalb müssen Break-Glass-Konten dort auch noch nicht ausgeschlossen sein. Beim Umschalten auf An schon.

Skizze 4: Die vier Ergebnisse im Anmeldeprotokoll und was du jeweils damit machst. Die zweite Zeile ist die einzige, die Arbeit macht — und die einzige, die zählt.

Sieben Tage sind das Minimum, zwei Wochen sind ehrlicher: Erst dann hast du den Monatsabschluss der Buchhaltung, den Außendienst nach der Rückkehr und den Kollegen

gesehen, der nur alle zehn Tage ein bestimmtes System benutzt. Ausgewertet wird an drei Stellen: in den Anmeldeprotokollen selbst, in der Registerkarte zur Richtlinienauswirkung und — falls die Protokolle in einem Log-Analytics-Arbeitsbereich landen — in der Arbeitsmappe zu Conditional Access.

WARNUNG · Zwei Grenzen von Report-only, die du kennen musst

Report-only ist gut, aber nicht allwissend. Richtlinien, die den Bereich Benutzeraktionen verwenden, lassen sich damit nicht auswerten. Und Richtlinien, die ein konformes Gerät verlangen, können auf macOS, iOS und Android trotzdem eine Zertifikatsauswahl auslösen — obwohl gar nichts erzwungen wird. Nimm diese Plattformen in Report-only-Richtlinien mit Gerätebedingung heraus, sonst erklärst du dem Helpdesk eine Woche lang eine Abfrage, die es eigentlich nicht geben dürfte.

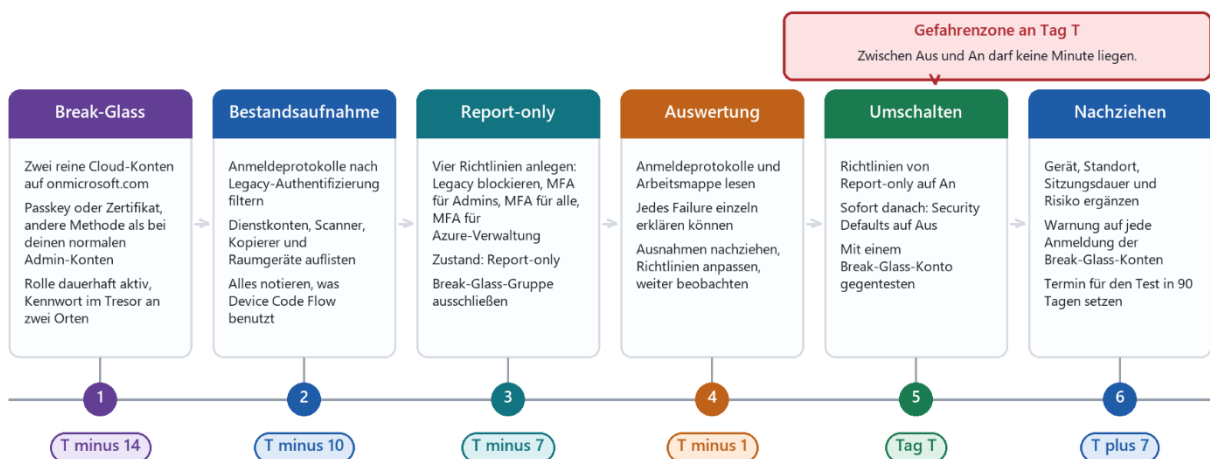
Schritt 3: Tag T und die gefährlichen dreißig Sekunden

Und jetzt der einzige Moment, in dem etwas schiefgehen kann. Die Reihenfolge lautet: zuerst die Conditional-Access-Richtlinien von Report-only auf An, dann — unmittelbar danach — Security Defaults auf Aus. Nicht umgekehrt.

Der Grund ist banal und wird trotzdem regelmäßig falsch gemacht. Solange Security Defaults aktiv sind, greifen deine Richtlinien nicht. Viele schalten deshalb erst den Schalter aus, um „freie Bahn“ zu haben, und stellen dann in Ruhe die Richtlinien scharf. In der Zwischenzeit läuft der Tenant ohne jede Mehrfaktorpflicht und mit offener Legacy-Authentifizierung. Aus „gleich mal eben“ werden erfahrungsgemäß zwei Stunden, weil noch jemand anruft. Zwei Stunden reichen für ein Password-Spraying-Skript vollkommen aus.

Umschaltpfad in sechs Stationen

Zwei Wochen reichen. Der einzige Schritt, der wirklich gefährlich ist, dauert dreißig Sekunden.



Wer Security Defaults zuerst ausschaltet und dann in Ruhe Richtlinien baut, betreibt seinen Tenant zwischendurch ohne jeden Schutz.

Skizze 5: Der gesamte Ablauf über zwei Wochen. Station fünf ist die einzige, bei der die Reihenfolge über den Ausgang entscheidet.

Direkt nach dem Umschalten gehört ein Gegentest dazu: Melde dich mit einem Break-Glass-Konto an und prüfe, ob es tatsächlich durchkommt. Danach eine normale Benutzeranmeldung und eine Administratoranmeldung. Drei Minuten Arbeit, die dir den Abend retten.

Richtlinie	Umfang	Kontrolle	Ausnahmen einplanen für
Legacy-Authentifizierung blockieren	alle Benutzer	Zugriff blockieren	Geräte, die zwingend SMTP mit Basisauthentifizierung brauchen — eng gefasst und befristet
MFA für Administratoren	14 privilegierte Rollen	MFA erzwingen, auf Wunsch phishing-resistent	Break-Glass-Konten
MFA für alle Benutzer	alle Benutzer	MFA erzwingen	Break-Glass-Konten, echte Dienstkanten in der Übergangsphase
MFA für die Azure-Verwaltung	alle Benutzer	MFA erzwingen für Azure-Portal, Entra Admin Center, Azure PowerShell und Azure CLI	Break-Glass-Konten

Tabelle 2: Die vier Richtlinien, die Security Defaults eins zu eins ersetzen. Microsoft stellt sie beim Umstieg als vorbereitete Richtlinien bereit; du kannst sie auch selbst aus den Vorlagen der Kategorie sichere Grundlagen bauen.

Schritt 4: Nachziehen, sonst war es nur ein Lizenzwechsel

Wenn du nach dem Umstieg bei diesen vier Richtlinien stehen bleibst, hast du dasselbe Sicherheitsniveau wie vorher — nur mit mehr Verwaltungsaufwand. Der Gewinn entsteht erst in den Wochen danach: Gerätebedingungen für den Zugriff auf Postfach und Dateiablage, Sitzungssteuerung für nicht verwaltete Geräte, Authentifizierungsstärken für Administratoren und, falls P2 vorhanden ist, risikobasierte Richtlinien. Jede einzeln, jede erst in Report-only. Die weiteren Schrauben am Tenant findest du in der [Tenant-Härtung: die 20 wichtigsten Schrauben](#), und die Frage, wie weit du das Ganze treiben solltest, beantwortet [Zero Trust im Mittelstand: pragmatisch statt dogmatisch](#).

Was Microsoft inzwischen von sich aus tut

Ein Detail, das die Entscheidung in den letzten Jahren verschoben hat: Microsoft baut inzwischen selbst Richtlinien in deinen Tenant. Diese Microsoft-verwalteten Richtlinien erscheinen in derselben Liste wie deine eigenen, tragen in der Spalte „Erstellt von“ den Eintrag Microsoft und starten grundsätzlich im Zustand Report-only.

Danach passiert Folgendes: Frühestens 30 Tage nach dem Erscheinen schaltet Microsoft sie selbst auf An, sofern du sie im Zustand Report-only stehen lässt. Zwei Wochen vorher wirst du per E-Mail und über das Nachrichtencenter informiert. Du kannst sie jederzeit früher aktivieren oder auf Aus stellen, du kannst Konten ausschließen — aber du kannst sie weder umbenennen noch löschen. Wenn du mehr ändern willst, duplizierst du sie und arbeitest mit der Kopie weiter.

Richtlinie	Zielgruppe	Voraussetzung
Legacy-Authentifizierung blockieren	alle Benutzer	auch als Richtlinie im Baseline-Sicherheitsmodus verfügbar
Device Code Flow blockieren	alle Benutzer	Ausnahmen für Teams-Raumsysteme gesondert vorgesehen

MFA für Administratoren in Microsoft-Verwaltungsportalen	14 privilegierte Rollen	P1 oder P2, Security Defaults ausgeschaltet
MFA für alle Benutzer	alle Benutzer	P1 oder P2, Security Defaults ausgeschaltet
MFA für Konten mit benutzerbezogener MFA	Konten mit alter Per-User-MFA	P1 oder P2, weniger als 500 betroffene Konten
MFA und erneute Anmeldung bei riskanten Anmeldungen	alle Benutzer oder eine lizenzbegrenzte Gruppe	P2 mit Entra ID Protection
Zugriff für Benutzer mit hohem Risiko blockieren	risikobehaftete Konten	P2 mit Entra ID Protection
Phishing-resistente Anmeldung für Administratoren	privilegierte Rollen	Baseline-Sicherheitsmodus, im Microsoft 365 Admin Center verwaltet

Tabelle 3: Die wichtigsten Microsoft-verwalteten Richtlinien und ihre Voraussetzungen. Auffällig: Der Großteil greift ausdrücklich nur dann, wenn Security Defaults ausgeschaltet sind.

FAKTEN · Die verpflichtende MFA läuft parallel und unabhängig

Unabhängig von Security Defaults und Conditional Access erzwingt Microsoft seit Oktober 2024 MFA für Azure-Portal, Entra Admin Center und Intune Admin Center, seit Februar 2025 zusätzlich für das Microsoft 365 Admin Center und seit dem 1. Oktober 2025 für Azure CLI, Azure PowerShell, die Azure-App, Infrastructure-as-Code-Werkzeuge und die REST-Schnittstellen bei jedem schreibenden Zugriff.

- › Diese Durchsetzung sitzt auf der Serverseite. Ausnahmen aus deinen eigenen Richtlinien greifen dort nicht — auch nicht für Break-Glass-Konten.
- › Die Möglichkeit, den Start für Phase 2 aufzuschieben, endete am 1. Juli 2026. Ein Opt-out gibt es nicht.
- › Workload-Identitäten wie verwaltete Identitäten und Dienstprinzipale sind nicht betroffen. Benutzerkonten, die als Dienstkonten laufen, sehr wohl — das ist der Anlass, sie endlich umzustellen.

Der praktische Effekt: Ein Teil dessen, was du früher selbst erzwingen musstest, kommt inzwischen ohnehin. Das entwertet Conditional Access nicht — im Gegenteil, es verschiebt den Wert dahin, wo Microsoft nicht für dich entscheiden kann: Ausnahmen, Geräte, Standorte, Sitzungen und die Frage, wie stark die Anmeldung deiner Administratoren sein muss. Wenn du bei der Einordnung dieser Themen eine zweite Meinung brauchst, ist das genau der Gegenstand meiner [Beratung zu Microsoft 365 Security](#); wer es lieber im Team erarbeiten möchte, findet den passenden Rahmen in der [Schulung Microsoft 365 Security](#).

Häufige Fragen

Kann ich Security Defaults und Conditional Access parallel betreiben?

Nein. Die beiden schließen sich gegenseitig aus. Solange Security Defaults aktiv sind, werden deine Conditional-Access-Richtlinien nicht durchgesetzt. Du kannst sie zwar anlegen und in Report-only betreiben — das ist sogar ausdrücklich der empfohlene Weg —, aber scharf werden sie erst, wenn der Schalter aus ist.

Wie lange sollte ich Report-only laufen lassen?

Mindestens sieben Tage, besser zwei Wochen. Entscheidend ist nicht die Dauer an sich, sondern ob ein vollständiger Arbeitszyklus abgebildet ist: Monatsabschluss, Außendienst, Urlaubsrückkehrer, selten genutzte Fachanwendungen. Wenn du jedes einzelne Ergebnis vom Typ Failure erklären kannst, bist du fertig — nicht wenn eine bestimmte Zahl von Tagen um ist.

Muss ich Break-Glass-Konten auch aus Report-only-Richtlinien ausschließen?

Nein, dort ist es nicht nötig, weil Report-only nichts erzwingt. Sobald du eine Richtlinie auf An schaltest, muss der Ausschluss allerdings stehen. Am saubersten löst du das mit einer eigenen Sicherheitsgruppe, die von Anfang an in jeder sperrenden oder einschränkenden Richtlinie als Ausnahme eingetragen ist. Dann kannst du beim Umschalten nichts vergessen.

Was passiert mit meinem Scanner, wenn ich Security Defaults einschalte?

Wenn er per SMTP mit Basisauthentifizierung sendet: Er hört auf zu senden. Die saubere Lösung ist, ihn auf modernes SMTP oder auf einen Weiterleitungsconnector umzustellen, der nicht an einem Benutzerkonto mit Kennwort hängt. Die unsaubere Lösung — Security Defaults abschalten — kostet dich die Mehrfaktorpflicht für den gesamten Tenant. Das ist ein sehr teurer Scanner.

Reichen Security Defaults für die verpflichtende Azure-MFA?

Ja. Microsoft nennt sie ausdrücklich als gangbaren Weg für Tenants ohne Premiumlizenz. Wer den Schalter an hat, erfüllt die Anforderung. Umgekehrt gilt aber auch: Wer ihn ausschaltet, ohne sofort Conditional Access scharf zu stellen, erfüllt sie nicht mehr und läuft in Fehlermeldungen, sobald jemand in Azure etwas anlegen oder ändern will.

Was ist der Baseline-Sicherheitsmodus, und brauche ich den?

Das ist ein Bündel empfohlener Sicherheitseinstellungen, das im Microsoft 365 Admin Center verwaltet wird. Zwei davon erscheinen als Conditional-Access-Richtlinien: die Blockade der Legacy-Authentifizierung und die phishing-resistente Anmeldung für Administratoren. Anders als die Microsoft-verwalteten Richtlinien gelten sie formal als von dir erstellt. Für kleinere Häuser ohne eigenes Richtlinienwerk ist das ein brauchbarer Einstieg, für gewachsene Umgebungen eher ein weiterer Ort, an dem Regeln stehen.

Wir haben nur Business Standard. Ist das ein Sicherheitsproblem?

Es ist eine Einschränkung, kein Problem — solange du die Konsequenzen kennst. Security Defaults decken die Grundlagen ab. Was dir fehlt, sind Ausnahmen, Gerätebedingungen und Risikoauswertung. Für viele kleine Organisationen ist das vertretbar. Sobald du regulatorisch nachweisen musst, unter welchen Bedingungen Zugriff gewährt wird, wird der Schritt auf Business Premium schwer vermeidbar.

Wie erkenne ich, ob Microsoft in meinem Tenant Richtlinien verändert hat?

Die Überwachungsprotokolle führen Änderungen des Microsoft-verwalteten Richtlinienmanagers als eigenen Initiator in der Kategorie Richtlinie. Wer sich das regelmäßig ansehen will, filtert im Entra Admin Center unter Überwachungsprotokolle nach dem Dienst Conditional Access; Namen von Microsoft-verwalteten Richtlinien beginnen erkennbar mit einem eigenen Präfix. Praktischer ist es allerdings, die Nachrichtencenter-Meldungen ernst zu nehmen — die kommen zwei Wochen vor der Aktivierung.

Und wenn ich mich trotz allem aussperre?

Dann brauchst du das Break-Glass-Konto, das du hoffentlich in Schritt 0 angelegt hast. Falls nicht, bleibt der Weg über den Microsoft-Support, und der dauert — im schlechtesten Fall Tage, in denen niemand Konten anlegen, Kennwörter zurücksetzen oder Richtlinien ändern kann. Das ist übrigens ein Szenario, das in einen Notfallplan gehört; wie so einer aussieht, steht unter [Incident-Response-Plan für Microsoft 365](#).

Fazit

Security Defaults sind besser als ihr Ruf und deutlich besser als das, was in vielen Tenants stattdessen läuft. Sie erzwingen Mehrfaktorauthentifizierung für alle, sie schließen die Legacy-Authentifizierung, sie schützen die Administratorrollen und die Azure-Verwaltung, und sie kosten keinen Cent. Wenn du keine P1-Lizenz hast, ist die Diskussion damit beendet: Schalter an, Tokens entziehen, weitermachen.

Wenn du eine Lizenz hast, ist die Frage nicht, ob Conditional Access besser ist — das ist es —, sondern ob du den Betriebsaufwand tragen willst. Die ehrliche Antwort lautet in den meisten Fällen ja, weil der erste Sonderfall längst da ist und bisher durch Wegsehen gelöst wird. Ein Kopierer, der Basisauthentifizierung spricht, ist kein Argument gegen Mehrfaktorauthentifizierung. Er ist ein Argument für eine Richtlinie, die zwischen einem Kopierer und einem Menschen unterscheiden kann.

Und wenn du umschaltest, dann in dieser Reihenfolge: Break-Glass zuerst, Report-only als Zweites, und am Tag T erst Conditional Access auf An und dann Security Defaults aus. Die dreißig Sekunden dazwischen sind der einzige Teil dieses Projekts, bei dem Reihenfolge über Erfolg und Misserfolg entscheidet. Alles andere ist Fleißarbeit — und die lässt sich planen.

Weiter im Thema

- › [Conditional Access: Baselines, die nicht nerven](#) — das Richtlinienwerk, das nach dem Umstieg entsteht
- › [Break-Glass-Konten anlegen und überwachen](#) — Schritt 0, ohne den du nicht anfangen solltest
- › [MFA in Microsoft 365 richtig einführen](#) — wenn die Registrierung noch nicht flächendeckend steht
- › [Legacy Authentication endgültig abschalten](#) — die Bestandsaufnahme vor dem Umschalten
- › [Tenant-Härtung: die 20 wichtigsten Schrauben](#) — was nach den vier Grundrichtlinien kommt
- › [Secure Score: sinnvoll nutzen statt Punktejagd](#) — wie du den Fortschritt misst, ohne dich zu

belügen

- › [NIS2 aus Security-Sicht: technische Maßnahmen in M365](#) — wenn der Nachweis gegenüber Dritten dazukommt
- › [Beratung zu Microsoft 365 Security](#) — wenn du den Umschalttag nicht allein fahren möchtest