

MFA in Microsoft 365 richtig einführen

Es gibt zwei Sorten von Unternehmen: die, die MFA eingeführt haben, und die, die es nach dem ersten Vorfall in einer Nachtschicht einführen. Die zweite Variante ist technisch identisch, kostet aber deutlich mehr Nerven, weil parallel ein Forensiker im Besprechungsraum sitzt und die Geschäftsführung wissen will, warum das nicht längst an war.

Die gute Nachricht: Die Einführung von Multi-Faktor-Authentifizierung ist kein Großprojekt. Sie ist ein Rollout mit klarer Reihenfolge, einer Handvoll Sonderfälle und einem Kommunikationsplan. Die schlechte Nachricht: Genau an diesen drei Punkten scheitern die meisten Anläufe. Nicht an der Technik. Die Technik ist seit Jahren fertig, sie steht in deinem Tenant, sie wartet nur darauf, dass jemand die Verantwortung für die Reihenfolge übernimmt.

Dieser Beitrag gehört zur Reihe [Microsoft 365 Security](#) und beschreibt den Weg, den ich in Projekten tatsächlich gehe: erst die Administratoren, dann eine Pilotgruppe, dann die Belegschaft in Wellen. Dazu die Frage, was mit Dienstkonto, geteilten Postfächern und der Führungskraft passiert, die „aus terminlichen Gründen“ eine Ausnahme möchte. Und die unbequeme Wahrheit darüber, was MFA leistet und wogegen es überhaupt nichts ausrichtet.

Bevor du anfängst: Was MFA leistet — und was nicht

MFA wird gerne als Allheilmittel verkauft. Das ist es nicht. Es ist ein sehr wirksames Mittel gegen genau eine Angriffsklasse, und diese Angriffsklasse macht zufällig den überwiegenden Teil dessen aus, was täglich gegen deinen Tenant läuft. Verstehe die Grenze, bevor du dich in Sicherheit wiegst.

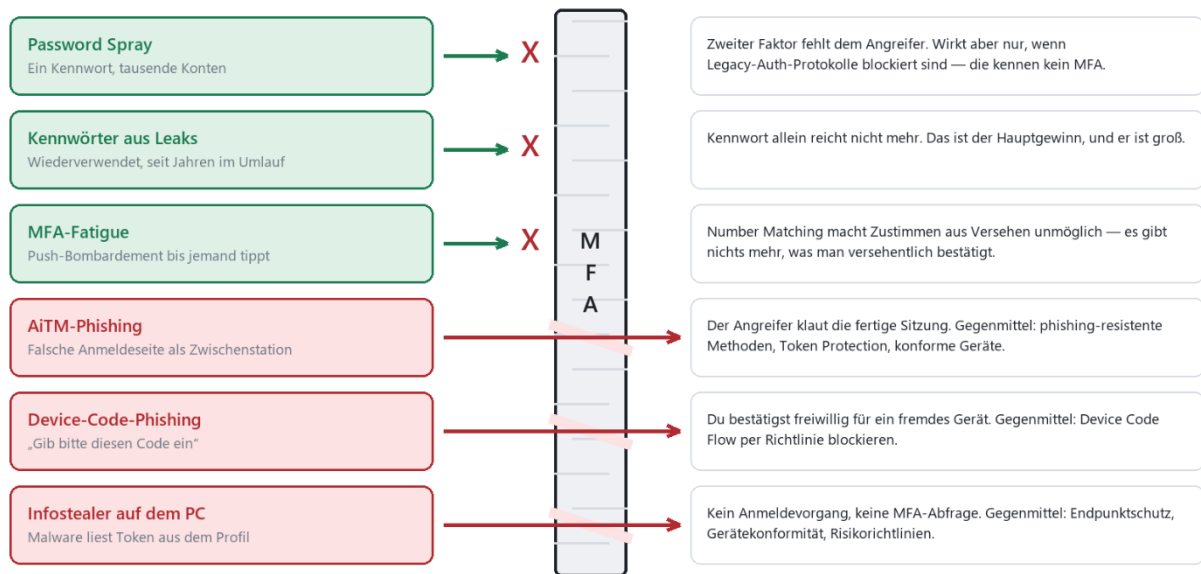
Password Spray: das Massengeschäft

Password Spray heißt: Ein Angreifer nimmt ein einziges, plausibles Kennwort — „Sommer2026!“ ist ein Klassiker — und probiert es gegen tausende Konten. Kein Konto wird oft genug falsch angemeldet, um eine Sperre auszulösen. Es reicht ein Treffer. In der Praxis ist das keine exotische Angriffsform, sondern der Normalfall: Im Microsoft Digital Defense Report 2025 entfallen 97 Prozent der Identitätsangriffe auf Password Spray, und die Zahl der identitätsbasierten Angriffe stieg im ersten Halbjahr 2025 um 32 Prozent.

Gegen diese Angriffsform wirkt MFA brutal effektiv, weil dem Angreifer schlicht der zweite Faktor fehlt. Microsoft beziffert die Wirkung auf über 99 Prozent der Kontoübernahmeversuche. Es gibt in der IT-Sicherheit sehr wenige Maßnahmen mit diesem Verhältnis von Aufwand zu Wirkung.

Was die MFA-Wand aufhält — und was einfach durchgeht

MFA ist eine Wand, kein Dach. Regen kommt trotzdem rein.



Merksatz: MFA erledigt die Massenangriffe. Gegen die gezielten brauchst du phishing-resistente Verfahren und gesunde Geräte.

Skizze: Drei Angriffsarten prallen an der MFA-Wand ab, drei laufen einfach daran vorbei.

FAKTEN · Was MFA gegen Password Spray leistet und wogegen nicht

MFA ist eine Wand, kein Dach. Sie steht dort, wo sich jemand mit Kennwort anmeldet — und nur dort.

- Wirkt: Password Spray, Credential Stuffing, Kennwörter aus alten Datenlecks. Der Angreifer hat das Kennwort, aber nicht das Gerät.
- Wirkt nur mit Zusatz: Password Spray über Legacy-Auth-Protokolle wie IMAP, POP3 oder SMTP. Diese Protokolle kennen keine MFA-Abfrage und gehen unter der Wand durch. Nach Microsofts Analyse laufen mehr als 99 Prozent der Password-Spray-Angriffe genau darüber.
- Wirkt halb: MFA-Fatigue, also Push-Bombardement, bis jemand entnervt auf „Genehmigen“ tippt. Mit Number Matching gibt es nichts mehr, was man versehentlich bestätigen kann.
- Wirkt nicht: AiTM-Phishing. Der Angreifer schaltet eine täuschend echte Anmeldeseite dazwischen, du machst brav deine MFA, und er greift die fertige Sitzung ab. Das Token interessiert sich nicht dafür, wie gut du dich authentifiziert hast.
- Wirkt nicht: Device-Code-Phishing. Du bekommst einen Code zugeschickt und bestätigst freiwillig eine Anmeldung für ein Gerät, das dem Angreifer gehört.
- Wirkt nicht: Infostealer-Malware, die Token direkt vom Rechner liest. Es findet gar keine Anmeldung statt, an der MFA greifen könnte.

Die Konsequenz ist nicht, MFA sein zu lassen. Die Konsequenz ist, MFA als ersten Schritt zu begreifen und die Lücken bewusst zu schließen: Legacy-Authentifizierung abschalten (siehe [Legacy Authentication endgültig abschalten](#)), Device Code Flow per Richtlinie blockieren, Geräte gesund halten (siehe [Defender for Endpoint: Onboarding ohne Drama](#)) und mittelfristig auf phishing-resistente Verfahren umstellen, wie in [Passwordless: FIDO2 und Passkeys in der Praxis](#) beschrieben.

Microsoft entscheidet inzwischen mit

Falls du noch überlegst, ob MFA ein Thema für dieses Jahr ist: Microsoft hat dir die Entscheidung teilweise abgenommen. Seit Oktober 2024 wird MFA für Anmeldungen am Azure-Portal, am Microsoft Entra Admin Center und am Intune Admin Center erzwungen, seit Februar 2025 auch für das Microsoft 365 Admin Center. Die zweite Phase startete am 1. Oktober 2025 und erfasst Azure CLI, Azure PowerShell, die Azure-Mobile-App, Infrastructure-as-Code-Werkzeuge und die REST-Schnittstellen der Ressourcenverwaltung — dort allerdings nur für schreibende Operationen. Lesen geht weiterhin ohne.

Das ist keine Richtlinie in deinem Tenant, die du wegklicken kannst: Die Durchsetzung passiert serverseitig. Ein Aufschub war möglich, aber endlich — für Phase 2 bis zum 1. Juli 2026. Bemerkenswert daran: Auch Notfallzugänge sind erfasst. Break-Glass-Konten brauchen einen MFA-Weg, und der sollte kein Handy sein, das im Urlaub mit im Koffer liegt.

Bereich	Was passiert	Was das für dich heißt
Azure- und Admin-Portale	MFA-Pflicht seit Oktober 2024, Microsoft 365 Admin Center seit Februar 2025	Deine Administratoren sind ohnehin erfasst. Nimm die Umstellung selbst in die Hand, bevor sie dich überrascht.
Azure CLI, PowerShell, IaC, REST	MFA-Pflicht für schreibende Operationen seit 1. Oktober 2025	Automatisierung mit Benutzerkonten fliegt dir um die Ohren. Auf Workload Identities umstellen.
Workload Identities	Verwaltete Identitäten und Dienstprinzipale sind nicht betroffen	Der saubere Zielzustand für alles Automatisierte.
Break-Glass-Konten	Ebenfalls MFA-pflichtig, keine Ausnahme	Passkey oder zertifikatsbasierte Anmeldung hinterlegen, im Safe dokumentieren.
Microsoft-verwaltete Richtlinien	Erscheinen im Tenant zunächst im Nur-Bericht-Modus und werden frühestens nach 30 Tagen aktiviert	Prüfen, ausnehmen, gezielt aktivieren — statt sich überraschen zu lassen.

Tabelle 1: Was Microsoft ohne dein Zutun durchsetzt — und was du selbst regeln musst.

WARNUNG · Der 30-Tage-Automatismus

Microsoft legt Conditional-Access-Richtlinien direkt in deinem Tenant an — unter anderem MFA für Administratoren, MFA für alle Benutzer und das Blockieren von Device Code Flow. Sie starten im Nur-Bericht-Modus und werden aktiviert, wenn du nichts tust; angekündigt wird das zwei Wochen vorher per Nachrichtencenter und E-Mail. Wer diese Nachrichten nicht liest, erlebt die MFA-Einführung als Naturereignis statt als Projekt. Und die Break-Glass-Konten sind dann nicht ausgenommen, weil das niemand gemacht hat.

Ob du mit Security Defaults startest oder direkt mit Conditional Access arbeitest, hängt an Lizenz und Anspruch — die Abwägung steht in [Security Defaults oder Conditional Access?](#). Für alles, was danach kommt, brauchst du ein sauberes Regelwerk: [Conditional Access: Baselines, die nicht nerven](#).

Die Reihenfolge: Admins, Pilot, alle

Der häufigste Fehler ist der Stichtag. Jemand setzt eine Richtlinie auf „Alle Benutzer“, klickt am Freitagnachmittag auf Speichern und fährt ins Wochenende. Am Montag stehen 400 Leute vor

einem Registrierungsdialog, den sie nicht erwartet haben, das Telefon im Helpdesk glüht, und um 11 Uhr entscheidet jemand mit ausreichend Rangabzeichen, dass „das erstmal wieder ausgemacht wird“. Danach ist das Thema für zwei Jahre verbrannt.

Die Reihenfolge ist deshalb nicht Geschmackssache, sondern der Kern des Vorgehens. Sie sorgt dafür, dass Probleme dort auftreten, wo Leute sitzen, die sie lösen können.

Einführung in Phasen statt an einem Stichtag

Wer alle gleichzeitig umstellt, hat am Montag alle gleichzeitig am Telefon



Jede Phase hat ein Abbruchkriterium: mehr als 5 Prozent der Welle im Helpdesk, dann Welle stoppen statt durchziehen.

Skizze: Fünf Phasen mit Dauer, Inhalt und einem Abbruchkriterium je Welle.

Phase 0: Bestandsaufnahme, zwei Wochen

Bevor du irgendetwas einschaltest, willst du wissen, wie dein Tenant tatsächlich aussieht. Nicht, wie er im Konzept aussieht. Der Bericht über die Aktivität der Authentifizierungsmethoden im Entra Admin Center sagt dir, wer welche Methode registriert hat. Die Anmeldeprotokolle sagen dir, wer noch über Legacy-Protokolle hereinkommt und welche Konten sich verdächtig gleichmäßig alle fünf Minuten anmelden — das sind deine Dienstkunden, auch wenn sie „Peter Müller“ heißen.

- Welche Konten haben keine Methode registriert? Diese Liste ist dein Arbeitsvorrat für die Kommunikation.
- Welche Konten sind eigentlich keine Personen? Dienstkunden, Ressourcenkonten, Testkonten aus dem Projekt von 2019.
- Welche geteilten Postfächer haben ein aktives Kennwort und eine Anmeldeberechtigung?
- Welche Anwendungen melden sich noch mit Basisauthentifizierung an?
- Existieren zwei Break-Glass-Konten, sind sie getestet und aus allen Richtlinien ausgenommen?

Die Notfallzugänge sind die Voraussetzung für alles Weitere, nicht die Nacharbeit. Wie du sie anlegst, absicherst und überwachst, steht in [Break-Glass-Konten anlegen und überwachen](#). Wer ohne funktionierenden Notfallzugang eine tenantweite Richtlinie aktiviert, hat sich sein eigenes Ausfallszenario gebaut.

Phase 1: Administratoren, eine Woche

Administratoren zuerst. Nicht, weil sie es verdient hätten, sondern weil ihre Konten die wertvollsten im Haus sind und weil sie die einzige Gruppe sind, die einen Fehler im Rollout selbst beheben kann. Wenn im Registrierungsprozess etwas klemmt, merkt das jemand, der weiß, wo man nachschaut — und nicht jemand, der daraufhin die Personalabteilung anruft.

Für privilegierte Rollen gilt: Push-Benachrichtigung ist das Minimum, phishing-resistent ist das Ziel. Wer administrative Rechte hat, bekommt einen Passkey oder einen Sicherheitsschlüssel. Das kostet pro Person einmalig zwanzig Minuten und einen zweistelligen Eurobetrag und erspart dir die Diskussion, ob ein Admin-Konto per AiTM-Seite übernommen werden kann. Zwei Sicherheitsschlüssel je Person übrigens, sonst ist der verlorene Schlüssel dein nächster Notfall.

In dieser Phase testest du außerdem den Notfallweg. Wirklich testen: anmelden, nicht nur das Kennwort im Safe anschauen.

Phase 2: Pilotgruppe, zwei bis drei Wochen

Die Pilotgruppe ist keine Gruppe von Freiwilligen aus der IT. Das ist der zweithäufigste Fehler: Zwölf technikaffine Kollegen registrieren sich in vier Minuten, melden „lief super“ und man schließt daraus, dass der Rollout einfach wird. Dann trifft die Welle die Produktion, wo Handys im Spind liegen, und die Buchhaltung, wo ein Terminalserver von 25 Leuten geteilt wird.

Eine brauchbare Pilotgruppe hat 30 bis 80 Personen und bildet die Wirklichkeit ab: Außendienst mit schlechtem Empfang, Produktion ohne Diensthandy, Empfang mit geteiltem Arbeitsplatz, eine Führungskraft, eine Person kurz vor dem Ruhestand, die den Satz „Ich hab kein Smartphone“ nicht als Provokation meint, sondern als Tatsache. Genau diese Fälle willst du in Woche zwei lösen und nicht in Woche neun.

Phase 3: Belegschaft in Wellen, vier bis sechs Wochen

Wellen nach Organisationseinheit, nicht nach Alphabet. Der Grund ist banal: Innerhalb einer Abteilung helfen sich Leute gegenseitig. Wenn in einer Abteilung acht von zehn schon registriert sind, fragen die letzten beiden ihre Kollegin und nicht den Helpdesk. Verteilst du dagegen alphabetisch, sitzt in jeder Abteilung genau ein Betroffener, der niemanden fragen kann.

Pro Welle brauchst du einen Ansprechpartner vor Ort — nicht notwendigerweise aus der IT. Die Person, die in jeder Abteilung ohnehin gefragt wird, wenn der Drucker klemmt, ist deine wertvollste Ressource im gesamten Projekt. Sag ihr das ruhig auch.

Phase	Zielgruppe	Erfolgskriterium	Abbruchkriterium
Phase 0	Niemand, nur Analyse	Liste aller Konten ohne Methode, aller Dienstkontoen, aller geteilten Postfächer liegt vor	Break-Glass-Konten nicht getestet
Phase 1	Alle privilegierten Rollen	100 Prozent registriert, Administratoren möglichst mit Passkey	Ein Admin-Konto ohne funktionierende Methode
Phase 2	30 bis 80 Personen quer durchs Haus	Über 90 Prozent registriert, alle Sonderfälle benannt und gelöst	Mehr als 10 Prozent brauchen Helpdesk-Kontakt
Phase 3	Belegschaft, Welle für	Je Welle über 95 Prozent innerhalb	Mehr als 5 Prozent Ticketquote —

	Welle	einer Woche	Welle stoppen, Ursache klären
Phase 4	Tenant-Einstellungen	SMS und Sprachanruf deaktiviert, Ausnahmen befristet dokumentiert	Ausnahmen ohne Ablaufdatum im Bestand

Tabelle 2: Phasenplan mit Erfolgs- und Abbruchkriterien. Ohne Abbruchkriterium wird jede Welle durchgezogen, egal wie sie läuft.

TIPP • Wo es danach weitergeht

MFA ist der Anfang der Kette, nicht das Ende:

- › [Conditional Access: Baselines, die nicht nerven](#) — das Regelwerk, in dem deine MFA-Pflicht dauerhaft lebt
- › [Break-Glass-Konten anlegen und überwachen](#) — der Notausgang, den du vor der ersten Richtlinie brauchst
- › [Tenant-Härtung: die 20 wichtigsten Schrauben](#) — was du im selben Wartungsfenster gleich miterledigst

Methoden: Authenticator mit Number Matching, SMS und Sprachanruf raus

„Wir haben MFA“ ist eine Aussage ohne Informationsgehalt, solange nicht klar ist, welche Methoden erlaubt sind. Ein zweiter Faktor per SMS ist besser als nichts, aber er ist eben auch nur so sicher wie die Prozesse deines Mobilfunkanbieters und die Sorgfalt der Person im Callcenter, die eine Ersatz-SIM herausgibt.

Die Methodenleiter: oben hin, unten weg

Balkenlänge = Widerstand gegen echte Angriffe, nicht gegen das Sicherheitsgefühl



SMS und Sprachanruf erst deaktivieren, wenn die Alternative registriert ist — sonst sperrst du Leute aus, die nichts falsch gemacht haben.

Skizze: Die Methodenleiter. Der Balken zeigt den Widerstand gegen echte Angriffe, nicht die gefühlte Sicherheit.

Erst aufräumen: die Richtlinie für Authentifizierungsmethoden

In vielen Tenants existieren die Methoden dreifach: in der modernen Richtlinie für Authentifizierungsmethoden, in den alten MFA-Diensteinstellungen und in den Einstellungen für die Kennwortzurücksetzung. Diese Richtlinien wurden unabhängig voneinander ausgewertet — wer in irgendeiner davon für eine Methode freigeschaltet war, durfte sie nutzen. Das erklärt den Klassiker: „Wir haben SMS doch abgeschaltet, warum bekommen die Leute weiter SMS?“ Weil in der alten Kennwortzurücksetzung noch „Mobiltelefon“ steht, und das erlaubt Anruf und Textnachricht gleichzeitig.

Seit dem 30. September 2025 lassen sich Methoden in den alten MFA- und Kennwortzurücksetzungs-Richtlinien nicht mehr verwalten. Wenn deine Migration noch nicht auf „Migration abgeschlossen“ steht, ist das dein erster Handgriff. Vorher hat das Abschalten einer Methode keinen verlässlichen Effekt, und du debuggst Geistereinstellungen.

Number Matching und der Kontext in der Benachrichtigung

Number Matching ist für Push-Benachrichtigungen im Microsoft Authenticator Standardverhalten und lässt sich nicht mehr abwählen. Das ist gut so: Es beendet die Angriffsform, bei der jemand nachts um drei so lange Push-Anfragen schickt, bis der genervte Empfänger auf „Genehmigen“ tippt, um wieder schlafen zu können. Wer eine zweistellige Zahl vom Bildschirm abtippen muss, den er gar nicht vor sich hat, bestätigt nichts aus Versehen.

Was du zusätzlich einschaltest, weil es standardmäßig nicht an ist: Standort und Anwendungsname in der Benachrichtigung. Beides steht in der Methodenrichtlinie unter „Microsoft verwaltet“ auf deaktiviert. Der Unterschied in der Praxis ist erheblich. „Genehmigen Sie die Anmeldung?“ bestätigt man gedankenlos. „Anmeldung bei Outlook aus Lagos“ nicht. Ebenfalls empfehlenswert und ebenfalls standardmäßig aus: die Funktion, mit der Leute eine verdächtige Anfrage direkt in der App melden können. Damit bekommst du Meldungen von Angriffsversuchen, für die sonst niemand den Helpdesk anruft.

Methode	Phishing-resistant	Typische Schwäche	Empfehlung
Passkey (FIDO2), Sicherheitsschlüssel	Ja	Beschaffung und Verlust wollen organisiert sein	Pflicht für alle privilegierten Rollen
Windows Hello for Business	Ja	An das jeweilige Gerät gebunden	Ideal für feste Arbeitsplätze
Zertifikatsbasierte Anmeldung	Ja	Setzt eine funktionierende PKI voraus	Sinnvoll, wo Karten ohnehin existieren
Authenticator, Push mit Number Matching	Nein	AiTM-Phishing, Nutzung des Privatgeräts	Solide Standardmethode für die Belegschaft
Authenticator, Einmalcode (TOTP)	Nein	Code kann abgefragt und weitergegeben werden	Rückfallebene ohne Datenverbindung
OATH-Hardware-Token	Nein	Beschaffung, Inventarisierung, Batterie	Für Arbeitsplätze ohne Smartphone
SMS an Mobilnummer	Nein	SIM-Swap, Rufumleitung, Zustellprobleme	Deaktivieren
Sprachanruf	Nein	Anrufbeantworter, Weiterleitung, Zentrale	Deaktivieren

Tabelle 3: Methodenvergleich. Die rechte Spalte ist die Entscheidungsgrundlage, nicht das Sicherheitsgefühl.

Die Registrierungskampagne: der Weg weg von SMS

Der Übergang von SMS zu Authenticator ist der Punkt, an dem viele Projekte einen Umweg über die Holzhammermethode nehmen: Methode deaktivieren, warten, was passiert. Was passiert, ist ein Helpdesk mit Sperrmeldungen von Leuten, die nichts falsch gemacht haben. Der elegante Weg ist die Registrierungskampagne in Entra.

Die Mechanik ist simpel: Wer sich per SMS oder Sprachanruf erfolgreich authentifiziert hat, bekommt direkt anschließend die Aufforderung, den Authenticator einzurichten. Der Zeitpunkt ist der Trick — die Person ist ohnehin gerade am Anmelden und beschäftigt sich mit dem Thema. Eine E-Mail mit derselben Bitte wird gelesen, für später vorgemerkt und nie wieder angeschaut.

Einstellung	Zustand „Microsoft verwaltet“	Zustand „Aktiviert“
Zielmethode	Microsoft wählt nach Tenant-Konfiguration; bei aktivierten Passkeys werden Passkeys beworben	Du wählst: Authenticator oder Passkey
Aufschub in Tagen	1 Tag, nicht konfigurierbar	0 bis 14 Tage
Begrenzte Anzahl Aufschübe	Bei Authenticator: nach dreimal Aufschieben ist Schluss	Ein- oder ausschaltbar; eingeschaltet sind drei Aufschübe erlaubt
Zielgruppe	Konfigurierbar über Ein- und Ausschluss	Konfigurierbar über Ein- und Ausschluss
Wer wird angesprochen	Konten, die per Anruf oder Textnachricht authentifizieren und noch keine Push-Benachrichtigung eingerichtet haben	Gleiche Regel bei Authenticator; bei Passkey nach jeder MFA-Methode

Tabelle 4: Registrierungskampagne im Vergleich der beiden Zustände.

Ein paar Eigenheiten, an denen sonst die Erwartung scheitert: Die Kampagne kann immer nur eine Methode gleichzeitig bewerben. Sie greift nicht, wenn die Anmeldung über eine bestehende Einmalanmeldung läuft — es muss eine echte interaktive Anmeldung mit MFA sein. Eine Authenticator-Kampagne läuft nicht auf Mobilgeräten. Und wenn eine Conditional-Access-Richtlinie die Seite zur Registrierung von Sicherheitsinformationen einschränkt, erscheint auch keine Aufforderung. Wer das nicht weiß, sucht drei Tage nach einem Fehler, der keiner ist.

WARNUNG · Reihenfolge beim Abschalten

SMS und Sprachanruf werden nicht abgeschaltet, weil ein Datum erreicht ist, sondern weil die betroffenen Konten eine Alternative registriert haben. Erst die Kampagne laufen lassen, dann die Zahlen im Bericht über die Methodenaktivität prüfen, dann die Restgruppe persönlich ansprechen — das sind erfahrungsgemäß zwischen zwei und fünf Prozent —, und erst dann die Methode aus der Richtlinie nehmen. Wer die Reihenfolge dreht, sperrt Leute aus, die nichts falsch gemacht haben. Das merkt man sich im Unternehmen deutlich länger als jede gelungene Einführung.

TIPP · Der Zugangscode für den Notfall

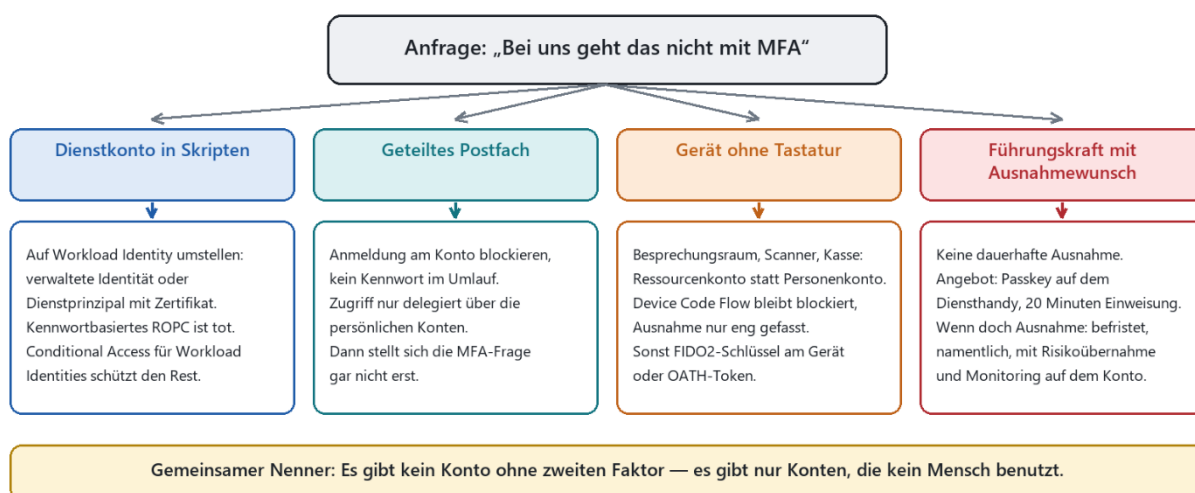
Der befristete Zugangscode (Temporary Access Pass) ist dein Werkzeug für Neueinstellungen, verlorene Geräte und die Registrierung des ersten Passkeys. Standardmäßig gilt eine Lebensdauer von einer Stunde bei einer maximalen Lebensdauer von acht Stunden; der zulässige Rahmen reicht von 10 Minuten bis 30 Tage. Für den Helpdesk ist die einmalige Verwendung mit kurzer Laufzeit die richtige Wahl. Achtung bei der Einrichtung kennwortloser Verfahren: Nach der Anmeldung mit einem Einmalcode muss die Registrierung binnen zehn Minuten abgeschlossen sein.

Sonderfälle: Dienstkonten, geteilte Postfächer und der Ausnahmewunsch

Jedes MFA-Projekt produziert eine Liste von Konten, bei denen „das nicht geht“. Diese Liste ist wertvoll, denn sie zeigt dir die Stellen, an denen über Jahre Abkürzungen genommen wurden. Drei der vier typischen Fälle sind technische Fragen mit klaren Antworten. Der vierte ist eine Führungsfrage.

„Dieses Konto kann kein MFA“ — vier Fälle, vier Antworten

Drei davon sind technische Fragen, einer ist eine Gehaltsfrage



Jede Ausnahme bekommt einen Namen, ein Ablaufdatum und einen Kalendereintrag für die Überprüfung.

Skizze: Vier Standardfälle und die jeweils richtige Antwort darauf.

Dienstkonten: das falsche Werkzeug seit Jahren

Das klassische Dienstkonto ist ein Benutzerkonto mit einem Kennwort, das seit 2018 nicht geändert wurde, weil niemand weiß, in wie vielen Skripten es steht. Es ist von MFA nicht ausgenommen, weil es besonders sicher wäre, sondern weil es sonst nicht mehr funktioniert. Genau diese Konten sind das bevorzugte Ziel bei Password Spray: hohe Rechte, altes Kennwort, keine zweite Hürde, und niemand schaut in die Anmeldeprotokolle.

Der Zielzustand heißt Workload Identity: verwaltete Identität, wo die Automatisierung in Azure läuft, sonst ein Dienstprinzipal mit Zertifikat. Beide sind von der MFA-Pflicht nicht betroffen, weil sie sich gar nicht als Mensch anmelden. Der kennwortbasierte Anmeldefluss über Benutzername und Kennwort — technisch ROPC — ist mit MFA grundsätzlich unvereinbar; die entsprechenden Programmierschnittstellen sind bei Microsoft inzwischen als veraltet markiert. Wenn irgendwo eine Anwendung dranhängt, die das noch braucht, ist die Ablösung dieser Anwendung ein eigenständiges Projekt — es fängt aber genau jetzt an und nicht irgendwann.

Für die Übergangszeit gilt: Dienstkonten, die noch Benutzerkonten sind, bekommen eine benannte Ausnahme mit Netzwerkbedingung, ein sehr langes Kennwort, keine interaktive

Anmeldeberechtigung für Menschen und ein Ablaufdatum im Ticketsystem. Nicht: einen Eintrag in einer Ausschlussgruppe, die „Sonderfälle“ heißt und in der nach zwei Jahren 60 Konten stehen.

Geteilte Postfächer: gar kein MFA-Thema

Geteilte Postfächer sind der einfachste Punkt auf der Liste, sobald man die Frage richtig stellt. Ein geteiltes Postfach braucht keine Anmeldung. Es hat zwar ein zugrundeliegendes Konto, aber die Anmeldung an diesem Konto gehört blockiert, und der Zugriff läuft über die persönlichen Konten der berechtigten Personen. Dann stellt sich die MFA-Frage nicht — der zweite Faktor sitzt beim Menschen, nicht beim Postfach.

Der Ärger entsteht immer dann, wenn ein geteiltes Postfach wie ein Sammelkonto benutzt wird: Kennwort im Umlauf, Anmeldung erlaubt, eventuell noch eine Lizenz drauf und ein Outlook-Profil auf fünf Rechnern. Solche Konten sind aus Sicht eines Angreifers hervorragende Ziele, weil sie oft weitreichende Berechtigungen haben und niemandem persönlich zugeordnet sind. Die Umstellung auf delegierten Zugriff ist Aufräumarbeit von ein bis zwei Tagen und löst gleichzeitig ein Nachvollziehbarkeitsproblem, das dir spätestens bei der nächsten Untersuchung eines Vorfalls begegnet.

Der Ausnahmewunsch aus der Chefetage

Er kommt. Er kommt zuverlässig, meistens per Telefon, und er beginnt mit „Ich verstehe ja, dass das für die anderen wichtig ist, aber ich bin ständig unterwegs.“ Die Begründungen sind austauschbar: zu viele Termine, kein privates Handy für dienstliche Zwecke, das Tablet des Vorstandsassistenten, die Sitzung im Ausland ohne Empfang.

Die Antwort darauf ist keine technische, sondern eine sachliche: Führungskräfte sind die am gezieltesten angegriffene Gruppe im Unternehmen. Wer Zahlungen freigeben, Verträge zeichnen und im Namen des Hauses sprechen kann, ist für einen Angreifer erheblich mehr wert als ein beliebiger Zugang zum Dateiablagensystem. Eine Ausnahme an dieser Stelle ist ungefähr so sinnvoll wie ein Tresor, dessen Tür man offen lässt, damit der Geschäftsführer schneller drankommt.

Was in der Praxis funktioniert, ist nicht die Diskussion über Risiko, sondern das bessere Angebot. Ein Passkey auf dem Diensthandy oder ein Sicherheitsschlüssel am Schlüsselbund ist schneller als jede Kennworteingabe: einmal Gesicht oder Finger, fertig. Zwanzig Minuten persönliche Einweisung, ein zweiter Schlüssel als Reserve, und die Beschwerde verwandelt sich meistens in die Frage, warum das nicht längst so läuft. Ich habe noch keine Führungskraft erlebt, die nach zwei Wochen mit Passkey zurück zum Kennwort wollte.

WICHTIG · Wenn es doch eine Ausnahme sein muss

Manche Ausnahmen sind unvermeidlich. Dann aber nach Regeln, sonst wächst aus einer Ausnahme eine Schattenpolitik:

- Namentlich: eine Person, ein Konto, kein „Geschäftsleitung“ als Sammelgruppe.
- Befristet: maximal 90 Tage, mit Wiedervorlage. Läuft die Frist ab, endet die Ausnahme automatisch, nicht nach Diskussion.
- Kompensiert: engere Bedingungen an Standort und Gerät, kürzere Sitzungsdauer, Alarm auf dem Konto.
- Dokumentiert: mit Datum, Begründung und dem Namen der Person, die das Risiko übernimmt.

Nicht als Schuldzuweisung, sondern weil eine Ausnahme eine Entscheidung ist und Entscheidungen einen Absender haben.

Für Nachweispflichten ist dieser letzte Punkt mehr als Papierkram: Wer unter die NIS2-Regulierung fällt, muss belegen können, dass Zugriffsschutz nicht nur gedacht, sondern umgesetzt ist — siehe [NIS2 aus Security-Sicht: technische Maßnahmen in M365](#). Eine unbefristete, undokumentierte Ausnahme für die Geschäftsleitung ist in diesem Zusammenhang das denkbar ungünstigste Fundstück.

Wunsch	Tragfähig?	Bessere Lösung	Frist
Führungskraft ohne Zeit	Nein	Passkey oder Sicherheitsschlüssel, persönliche Einweisung	Keine Ausnahme
Kein privates Gerät nutzen wollen	Ja, berechtigt	Hardware-Token oder Diensthandy stellen	Dauerhafte Alternative
Dienstkonto in Skripten	Übergangsweise	Umstellung auf Workload Identity	90 Tage, dann Prüfung
Besprechungsraum, Kasse, Scanner	Ja, eng gefasst	Ressourcenkonto mit Gerätebindung, Device Code Flow bleibt blockiert	Jährliche Prüfung
Geteiltes Postfach	Nein	Anmeldung blockieren, delegierter Zugriff	Keine Ausnahme
Externe Partner und Gäste	Nein	MFA über das Heimatverzeichnis oder eigene Anforderung im Ressourcen-Tenant	Keine Ausnahme

Tabelle 5: Ausnahmewünsche und die jeweils tragfähige Antwort.

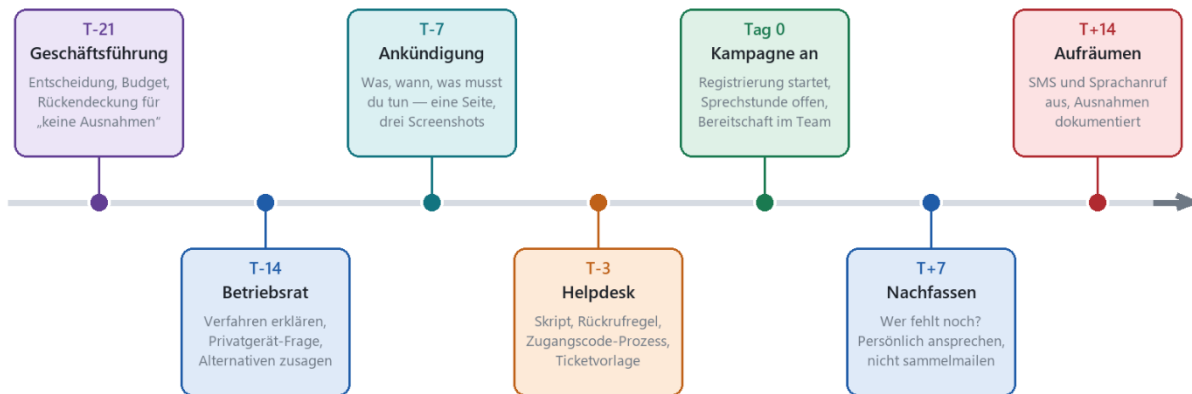
Der letzte Punkt wird gerne übersehen: Gastkonten sind vollwertige Zugänge zu deinen Daten. Wie du sie einhegst, steht in [Gastzugriff und externe Freigaben härten](#). Und wenn du dich fragst, ob deine Dateiablage nach der Einführung wirklich geschützt ist: [MFA für SharePoint Online erzwingen](#) geht auf die Besonderheiten dieses Dienstes ein.

Kommunikation: die Belegschaft mitnehmen statt überfahren

Der technische Teil der MFA-Einführung dauert ein paar Stunden. Der menschliche Teil dauert Wochen, und an ihm entscheidet sich, ob das Projekt als „notwendige Maßnahme“ oder als „diese Aktion von der IT“ in die Firmengeschichte eingeht. Der Unterschied kostet dich beim nächsten Sicherheitsthema entweder Rückenwind oder Widerstand.

Kommunikationsplan: sieben Termine, kein Überraschungsangriff

Die Belegschaft verzeiht Aufwand. Sie verzeiht nicht, überrumpelt zu werden.



Absender ist nicht die IT allein: Die Ankündigung kommt aus der Geschäftsführung, die Anleitung aus der IT.

Skizze: Sieben Termine von der Entscheidung bis zum Aufräumen.

Was in die Ankündigung gehört — und was nicht

Eine Ankündigung, die funktioniert, beantwortet drei Fragen und hört dann auf: Was ändert sich? Ab wann? Was musst du konkret tun? Eine Seite, drei Bildschirmfotos, ein Termin. Keine Erläuterung des OAuth-Ablaufs, keine Bedrohungslage-Präsentation mit Weltkarte, keine Aufzählung von Compliance-Anforderungen. Das interessiert an dieser Stelle niemanden, und jede zusätzliche Zeile senkt die Wahrscheinlichkeit, dass die entscheidenden drei gelesen werden.

Was hingegen sehr wohl hineingehört: der Satz, dass das für alle gilt, inklusive Geschäftsführung. Dieser eine Satz erspart dir ungefähr die Hälfte der Diskussionen. Und der Absender ist wichtig: Die Ankündigung kommt aus der Geschäftsführung, die Anleitung aus der IT. Kommt beides aus der IT, ist es eine Bitte. Kommt es von oben, ist es eine Entscheidung.

Das Privatgerät-Thema ernst nehmen

„Ich installiere keine Firmen-App auf meinem privaten Handy“ ist kein Sabotageversuch, sondern eine legitime Position. Sie kommt in jedem Projekt, und wer sie als Bockigkeit abtut, hat spätestens dann ein Problem, wenn sich der Betriebsrat einschaltet — was er zu Recht tut.

Die Antwort ist eine Alternative, nicht ein Argument. Ein OATH-Hardware-Token kostet ungefähr so viel wie ein Mittagessen und löst den Fall vollständig. Ein FIDO2-Sicherheitsschlüssel kostet etwas mehr und ist gleichzeitig die bessere Methode. Rechne die Alternative von vornherein ins Budget: fünf bis zehn Prozent der Belegschaft, dann bist du auf der sicheren Seite und musst nicht mitten im Rollout eine Beschaffung anstoßen.

Wichtig für die Gespräche mit der Arbeitnehmervertretung: Die Authenticator-App ist kein Überwachungswerkzeug, sie überträgt keine Standortdaten des Geräts an den Arbeitgeber. Was tatsächlich protokolliert wird und wo die Mitbestimmung wirklich beginnt, ist ein eigenes Thema

— [Security-Monitoring und Betriebsrat: was mitbestimmungspflichtig ist](#) geht es im Detail durch. Wer diese Unterscheidung sauber erklären kann, hat die Sitzung in zwanzig Minuten hinter sich.

Den Helpdesk vorbereiten

Rechne mit fünf bis fünfzehn Prozent Ticketquote je Welle — abhängig davon, wie gut die Ankündigung war und wie viele Leute schon eine Methode registriert haben. Die Tickets sind fast alle gleich: Handy neu, Authenticator weg, Registrierung abgebrochen, Code kommt nicht an. Dafür brauchst du genau einen sauberen Prozess.

1. Identität prüfen. Rückruf auf die im Personalsystem hinterlegte Nummer oder Bestätigung durch die Führungskraft. Nicht: „Klingt plausibel.“
2. Befristeten Zugangscode ausstellen, einmalig verwendbar, kurze Laufzeit.
3. Die betroffene Person registriert die Methode selbst — der Helpdesk registriert nie im Namen einer anderen Person.
4. Alte, nicht mehr nutzbare Methoden entfernen.
5. Ticket mit Kategorie schließen, damit du nach zwei Wochen weißt, welche Ursache wie oft aufgetreten ist.

WARNUNG · Der Helpdesk ist jetzt ein Angriffsziel

Sobald MFA steht, verlagert sich der Angriff dorthin, wo MFA zurückgesetzt wird. Der Anruf „Hier ist Herr Weber aus dem Vertrieb, mein Handy ist im Zug liegen geblieben, ich brauche dringend Zugang für einen Kundentermin“ ist ein Standardmuster, kein Einzelfall. Ohne verbindliche Rückrufregel hast du eine sehr teure Authentifizierung eingeführt und die Hintertür weit offen gelassen. Die Rückrufregel steht schriftlich im Prozess, gilt ohne Ausnahme und gilt besonders dann, wenn der Anrufer Druck macht — Druck ist Teil des Angriffs, nicht ein Zeichen von Dringlichkeit.

Wie ein Vorfall dieser Art abläuft und welche Schritte in der ersten Stunde zählen, steht in [Phishing-Vorfall: die ersten 60 Minuten](#) und in [Kompromittiertes Konto erkennen und aufräumen](#). Wer das Muster vorher üben will, findet in [Attack Simulation Training: Phishing-Übungen richtig aufsetzen](#) den passenden Rahmen.

Zeitpunkt	Empfänger	Inhalt	Absender
T minus 21 Tage	Geschäftsführung	Entscheidung, Budget für Hardware-Token, Zusage „keine Ausnahmen“	IT-Leitung
T minus 14 Tage	Betriebsrat	Verfahren, Privatgerät-Frage, zugesagte Alternativen	IT-Leitung und Personal
T minus 7 Tage	Alle	Eine Seite: was, wann, was ist zu tun, drei Bildschirmfotos	Geschäftsführung
T minus 3 Tage	Helpdesk und Ansprechpartner vor Ort	Skript, Rückrufregel, Prozess für Zugangscode, Ticketkategorien	IT
Tag 0	Welle 1	Kampagne aktiv, offene Sprechstunde, Bereitschaft im Team	IT
T plus 7 Tage	Nicht registrierte Personen	Persönliche Ansprache statt Sammelmail	Führungskraft
T plus 14 Tage	Alle	Kurzes Ergebnis, Dank, Hinweis auf abgeschaltete Methoden	IT

Tabelle 6: Kommunikationsplan. Sieben Termine, jeweils mit Absender — denn der Absender entscheidet über die Wirkung.

Nach dem Rollout: was in den Regelbetrieb übergeht

Ein Rollout endet nicht, wenn die letzte Welle durch ist, sondern wenn die Kontrolle in den Regelbetrieb übergeht. Drei Berichte gehören dauerhaft auf den Tisch: der Bericht über registrierte Methoden, die Liste der Ausnahmen mit Ablaufdatum und die Zahl der Anmeldungen ohne MFA. Letztere sollte gegen null gehen — tut sie das nicht, hast du irgendwo noch eine Lücke, meistens ein altes Protokoll oder eine vergessene Ausschlussgruppe.

Für die Berichterstattung nach oben taugt der Secure Score als grober Kompass, solange man ihn nicht mit dem Ziel verwechselt — dazu [Secure Score: sinnvoll nutzen statt Punktejagd](#). Wie eine Kompromittierung in der Praxis abläuft und welche Rolle fehlende Faktoren dabei spielen, zeigt das Dossier [TerminalFix und der Berlin-Hack](#). Wenn du die Einführung nicht allein stemmen willst: Die [Beratung zu Microsoft 365 Security](#) begleitet genau diese Rollouts, und für den Wissensaufbau im eigenen Team gibt es die [Schulung Microsoft 365 Security](#).

Häufige Fragen

Wie lange dauert die Einführung realistisch?

Im Mittelstand mit 200 bis 1.000 Konten sind acht bis zwölf Wochen ein realistischer Rahmen — zwei Wochen Bestandsaufnahme, eine Woche Administratoren, zwei bis drei Wochen Pilot, vier bis sechs Wochen Wellen. Der technische Aufwand daran beträgt vielleicht drei Tage. Alles andere ist Kommunikation, Sonderfälle und das geduldige Einsammeln der letzten fünf Prozent. Wer schneller sein will, kann das machen; er verlagert den Aufwand dann nur in den Helpdesk.

Reichen die Security Defaults, oder brauche ich Conditional Access?

Die Security Defaults sind besser als nichts und für sehr kleine Umgebungen ohne Entra-ID-P1-Lizenz die richtige Wahl. Sie erzwingen MFA für alle, kennen aber keine Ausnahmen, keine Bedingungen und keine Abstufung nach Standort oder Gerät. Sobald du Dienstkonten, Ausnahmen mit Kompensation oder unterschiedliche Anforderungen für Administratoren brauchst, führt kein Weg an Conditional Access vorbei. Und wer die Sonderfälle aus diesem Beitrag kennt, weiß, dass er sie braucht.

Was mache ich mit Leuten, die kein privates Handy nutzen wollen?

Eine Alternative stellen, nicht diskutieren. OATH-Hardware-Token oder FIDO2-Sicherheitsschlüssel lösen den Fall vollständig, kosten wenig und sind organisatorisch beherrschbar. Fünf bis zehn Prozent der Belegschaft sollte man dafür einplanen. Der Versuch, die Position wegzuzugraben, kostet mehr Zeit als die Beschaffung — und endet erfahrungsgemäß trotzdem bei der Beschaffung.

Können wir SMS nicht wenigstens als Notfallmethode behalten?

Kann man, sollte man aber nicht. Eine Methode, die als Rückfallebene verfügbar ist, wird zur Methode, die ein Angreifer als Rückfallebene nutzt — er meldet sich an, wählt bei der Methodenauswahl den bequemen Weg und umgeht damit die stärkere Methode. Die bessere

Notfallmethode ist der befristete Zugangscode über den Helpdesk: Er ist begrenzt gültig, protokolliert und an einen Prozess mit Identitätsprüfung gebunden.

Müssen Break-Glass-Konten wirklich auch MFA haben?

Ja. Die verpflichtende MFA für Azure- und Admin-Portale kennt für Notfallzugänge keine Ausnahme, ausdrücklich auch nicht für Konten mit hinterlegten Ausschlüssen. Der praktikable Weg ist ein Passkey oder eine zertifikatsbasierte Anmeldung, physisch getrennt aufbewahrt und regelmäßig getestet. Ein Notfallzugang, der im Notfall nicht funktioniert, ist kein Notfallzugang, sondern eine Beruhigungspille.

Was ist mit Gästen und externen Partnern?

Gastkonten sind erfasst. Die Anforderung kann entweder im Heimatverzeichnis des Gastes erfüllt werden — dann muss die tenantübergreifende Zugriffseinstellung so konfiguriert sein, dass du dieser MFA vertraust — oder der Gast erfüllt sie in deinem Tenant. Beides ist eine bewusste Entscheidung. Nichts zu entscheiden führt dazu, dass externe Zugänge die schwächste Stelle im sonst sauber abgesicherten Tenant sind.

Wir haben MFA. Sind wir jetzt sicher?

Ihr habt das Massengeschäft erledigt, und das ist viel. Gegen einen gezielten Angriff mit einer täuschend echten Anmeldeseite hilft Push-MFA aber nicht. Die nächsten Schritte heißen deshalb: phishing-resistente Methoden für alles Privilegierte, Device Code Flow blockieren, Gerätekonformität als Bedingung, Risikorichtlinien scharf stellen. In dieser Reihenfolge, und jeweils mit derselben Ruhe wie bei der MFA-Einführung.

Und wenn wir die Registrierungskampagne einfach Microsoft überlassen?

Der Zustand „Microsoft verwaltet“ ist eine vernünftige Wahl für Tenants ohne eigenes Konzept: Microsoft wählt Zielmethode und Aufschubverhalten und passt beides an die aktuelle Empfehlung an — inzwischen mit Tendenz zu Passkeys, wo diese aktiviert sind. Wenn du aber selbst steuern willst, welche Gruppe wann angesprochen wird, brauchst du den Zustand „Aktiviert“ mit eigener Zielgruppe. Der Unterschied ist keine Sicherheitsfrage, sondern eine Frage der Planbarkeit deines Helpdesk-Aufkommens.

Fazit

MFA einzuführen ist kein technisches Problem. Der Tenant kann das seit Jahren, die Methoden sind da, die Richtlinien sind vorbereitet, Microsoft schaltet inzwischen selbst Teile davon scharf. Was fehlt, ist meistens die Reihenfolge und jemand, der die unbequemen Gespräche führt.

Halte dich an drei Dinge, dann läuft es: Administratoren zuerst, weil sie Fehler selbst beheben können. Eine ehrliche Pilotgruppe, weil die Wirklichkeit im Lager anders aussieht als in der IT. Und eine Ankündigung aus der Geschäftsführung mit dem Satz, dass es für alle gilt — dieser eine Satz spart dir mehr Arbeit als jede technische Optimierung.

Alles andere ist Handwerk: Number Matching ist ohnehin Standard, Standort und Anwendungsname schaltest du zusätzlich ein, die Registrierungskampagne holt die SMS-Nutzer ab, und erst danach fliegen SMS und Sprachanruf aus der Richtlinie. Dienstkonten werden zu Workload Identities, geteilte Postfächer verlieren ihre Anmeldeberechtigung, und Ausnahmen bekommen einen Namen und ein Ablaufdatum.

Und dann fängst du an, die zweite Hälfte zu bauen: das Regelwerk in [Conditional Access: Baselines, die nicht nerven](#), den Notausgang in [Break-Glass-Konten anlegen und überwachen](#) und den Weg zu phishing-resistenter Anmeldung in [Passwordless: FIDO2 und Passkeys in der Praxis](#). MFA ist nicht das Ziel. Es ist die Eintrittskarte dafür, dass die restlichen Maßnahmen überhaupt Sinn ergeben.