

Passwordless: FIDO2 und Passkeys in der Praxis

Der klassische Phishing-Angriff auf ein Microsoft-365-Konto ist inzwischen ein Handwerk mit Bausatzcharakter. Der Angreifer mietet ein Kit, das die echte Anmeldeseite in Echtzeit durchreicht. Der Nutzer tippt sein Passwort ein, bekommt brav die Push-Benachrichtigung auf sein Telefon, bestätigt sie — und der Angreifer sitzt in der Sitzung. Multifaktor-Authentifizierung war dabei aktiv. Sie hat funktioniert. Sie hat nur nichts genützt.

Der Grund ist unangenehm einfach: Alles, was der Nutzer eintippen, ablesen oder bestätigen kann, kann er auch an die falsche Stelle eintippen, ablesen oder bestätigen. Ein sechsstelliger Code ist ein Geheimnis, das durch einen Menschen hindurchgereicht wird — und Menschen unterscheiden unter Zeitdruck nicht zuverlässig zwischen der echten Anmeldeseite von Microsoft und einer Adresse, die genauso aussieht, nur ein bisschen anders geschrieben ist.

Phishing-resistente Verfahren lösen das Problem nicht dadurch, dass sie das Geheimnis besser verstecken. Sie lösen es dadurch, dass es kein übertragbares Geheimnis mehr gibt. Was der Nutzer besitzt, ist ein privater Schlüssel, der sein Gerät nie verlässt und der nur dann signiert, wenn die Gegenstelle wirklich die ist, für die er einmal angelegt wurde. Man kann diesen Schlüssel nicht weitergeben. Nicht aus Versehen, nicht unter Druck, nicht nach einem netten Anruf vom angeblichen IT-Support.

Dieser Beitrag gehört in die Reihe [Microsoft 365 Security](#) und beschreibt den praktischen Weg dorthin: wie der Anmeldefluss technisch funktioniert, worin sich FIDO2-Sicherheitsschlüssel, Passkeys im Microsoft Authenticator und Windows Hello for Business unterscheiden, in welcher Reihenfolge du ausrollst, wie du das Ganze über Authentifizierungsstärken im Conditional Access erzwingst — und was passiert, wenn jemand seinen Schlüssel in der Regionalbahn liegen lässt. Denn das passiert. Nicht vielleicht.

WICHTIG — Der Zeitplan ist keiner mehr, den du dir aussuchst

Seit dem 1. September 2026 sind Passkeys die Standard-Anmeldeerfahrung in Microsoft Entra ID. Konten, die für SMS oder Sprachanruf freigeschaltet sind, werden automatisch für Passkeys aktiviert und beim nächsten MFA-Vorgang zur Registrierung angestupst.

Zum 1. Februar 2027 stellt Microsoft die selbst betriebene SMS- und Sprachzustellung ein. Wer danach als einzige Methode SMS oder Anruf hat, bekommt bei der Anmeldung eine blockierende Aufforderung zur Passkey-Registrierung. Ein Abschalten dieses Verhaltens ist nicht vorgesehen.

Für den Zeitraum dazwischen gibt es eine befristete Ausstiegsmöglichkeit über die Authentifizierungsmethoden-Richtlinie. Sie verschiebt den Termin, sie ersetzt ihn nicht. Wer einen echten regulatorischen Bedarf an einem Telekommunikationskanal hat, bindet ab Ende Oktober 2026 einen eigenen Anbieter über den Microsoft Security Store an.

Warum phishing-resistent etwas anderes ist als „starke MFA“

Der Begriff wird gern als Steigerungsform verwendet: erst Passwort, dann MFA, dann eben besonders gute MFA. Das ist falsch. Es ist kein Unterschied im Grad, sondern in der Bauart.

Es gibt nichts zum Abfangen

Bei der Registrierung erzeugt der Authenticator — der Sicherheitsschlüssel, das Smartphone, der Windows-Hello-Container — ein Schlüsselpaar. Der öffentliche Teil geht an Entra ID und wird beim Konto hinterlegt. Der private Teil bleibt im Gerät, in Hardware, und ist so gebaut, dass er dort auch bleibt. Er wird nie übertragen, nie angezeigt, nie in ein Feld getippt.

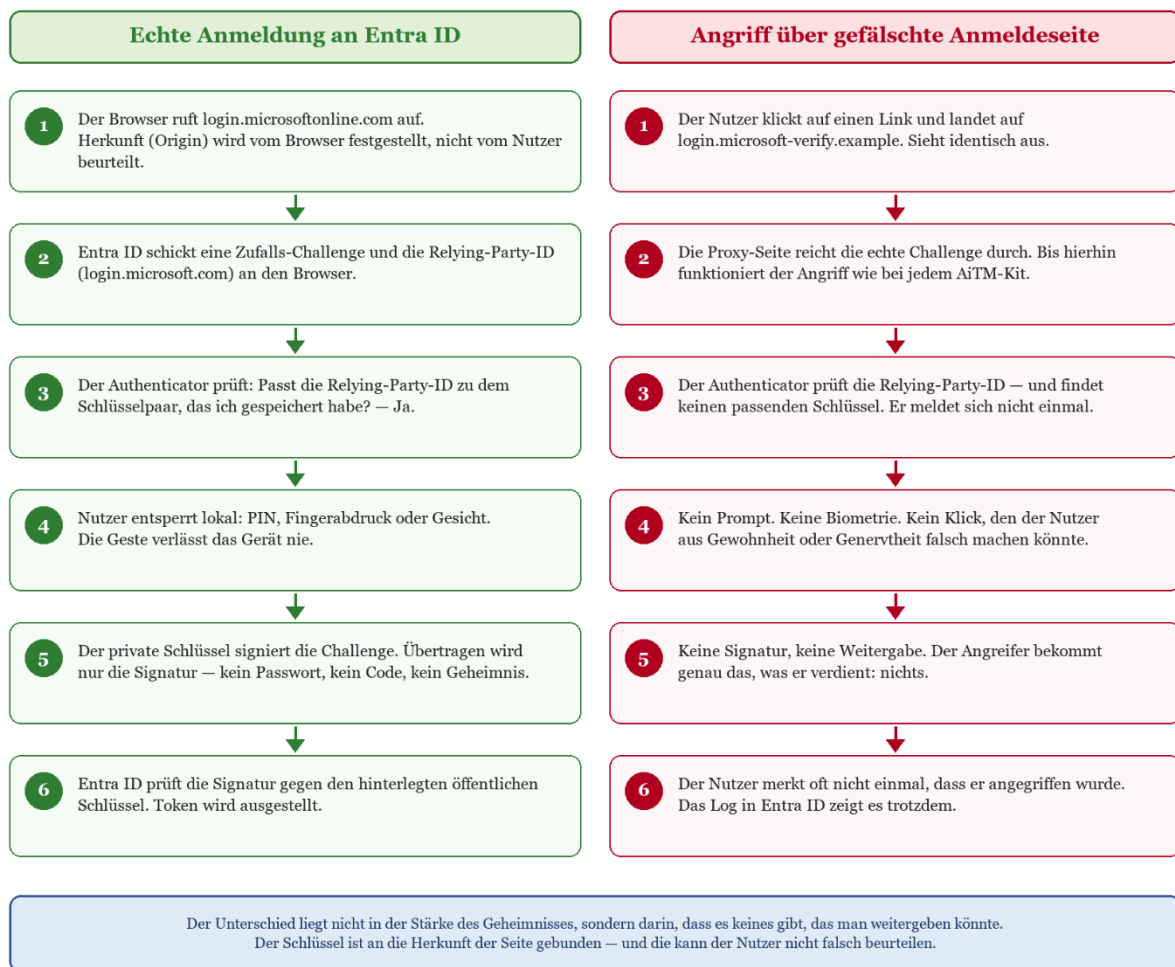
Bei jeder Anmeldung schickt Entra ID eine Zufalls-Challenge. Der Authenticator signiert sie und schickt die Signatur zurück. Diese Signatur ist genau einmal verwendbar und für genau diesen Vorgang gültig. Wer sie mitschneidet, hat einen wertlosen Datensatz. Es gibt keinen Code, der irgendwo weitergegeben werden könnte, weil es keinen Code gibt.

Die Herkunft der Seite entscheidet, nicht das Auge des Nutzers

Der eigentliche Trick liegt eine Ebene tiefer. Das Schlüsselpaar wird bei der Registrierung fest an eine Relying-Party-ID gebunden, also an die Domäne des Dienstes. Vor jeder Signatur prüft der Browser beziehungsweise das Betriebssystem, ob die Herkunft der aufgerufenen Seite zu dieser gebundenen ID passt. Passt sie nicht, passiert nichts. Kein Prompt, keine Abfrage, keine Möglichkeit, es trotzdem zu tun.

Damit verschwindet die entscheidende Schwachstelle: die menschliche Beurteilung. Der Nutzer muss keine Adresse mehr lesen, keine Zertifikatswarnung interpretieren und nicht entscheiden, ob eine Push-Meldung um 23:40 Uhr wohl von ihm selbst ausgelöst wurde. Ein Angreifer-in-der-Mitte kann die Anmeldeseite perfekt nachbauen — er kann nur nichts damit anfangen.

Anmeldefluss FIDO2: warum es nichts zum Abfangen gibt



Skizze 1: Der FIDO2-Anmeldefluss im direkten Vergleich mit dem Angriffsversuch. Der Bruch passiert bei Schritt 3 — und zwar ohne Zutun des Nutzers.

FAKTEN — Was phishing-resistent konkret heißt

Kein übertragbares Geheimnis: kein Passwort, kein Einmalcode, kein Zahlenabgleich, der weitergesagt werden könnte.

Bindung an die Herkunft: der private Schlüssel signiert nur für die Domäne, für die er registriert wurde. Eine Nachbau-Seite bekommt keine Signatur.

Lokale Entsperrung: PIN, Fingerabdruck oder Gesicht entsperren nur den Authenticator. Die biometrischen Daten verlassen das Gerät nicht und liegen weder bei Microsoft noch bei dir.

Kein Ermüdungsangriff: es gibt keine Push-Benachrichtigung, die man aus Genervtheit wegbestätigen könnte. Der Angreifer kann keine Anfrage auslösen, die beim Nutzer ankommt.

In Entra ID erfüllen genau drei Methodenfamilien diese Definition: Passkey (FIDO2), Windows Hello for Business samt Entra-Passkey auf Windows, und die mehrstufige zertifikatsbasierte Anmeldung.

Was es nicht heißt

Phishing-resistent ist nicht angriffsresistent. Wenn die Anmeldeinformation nicht mehr zu holen ist, gehen Angreifer eine Etage höher und versuchen, das fertige Token vom Gerät zu stehlen — über Schadsoftware, über einen kompromittierten Browser, über eine Sitzung, die irgendwo offen

liegen geblieben ist. Passwortlos zu sein ersetzt weder Endpunktschutz noch eine vernünftige Gerätekonformität.

Es ersetzt auch nicht das Aufräumen an anderer Stelle. Solange irgendwo noch ein Protokoll lebt, das nur Benutzername und Passwort kennt, hast du eine Hintertür, die von deiner schönen neuen Anmeldearchitektur schlicht nicht berührt wird. Das ist der Grund, warum [Legacy Authentication endgültig abschalten](#) zeitlich vor dem Passwordless-Projekt liegt und nicht danach.

TIPP — Der nächste logische Schritt nach der Umstellung

Wenn die Anmeldeinformationen nicht mehr phishbar sind, verlagert sich der Angriff auf die Token. Die passende Antwort heißt Tokenschutz in Conditional Access: das Aktualisierungstoken wird an die Hardware des ausstellenden Geräts gebunden und ist auf einem anderen Rechner wertlos.

Dazu gehört Entra ID Protection mit den Erkennungen, die auch bei passwortlosen Konten noch greifen — anomale Token, Zugriffsversuch auf das Primary Refresh Token, Angreifer in der Mitte.

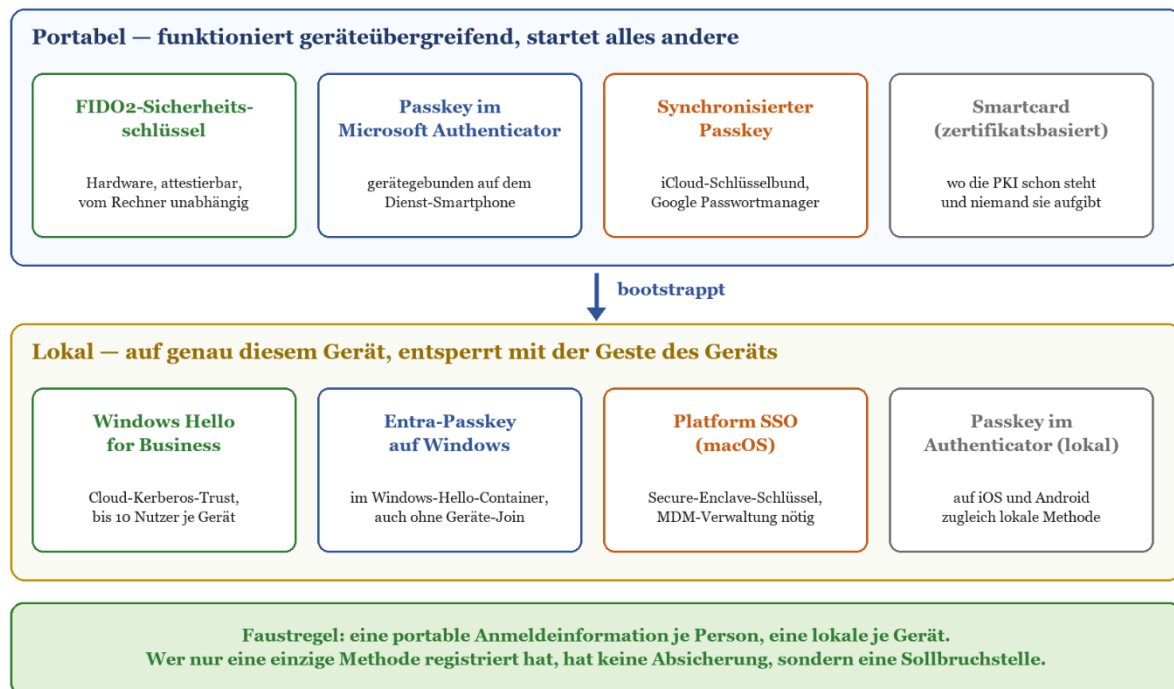
Was daraus im Ernstfall folgt, steht in [Kompromittiertes Konto erkennen und aufräumen](#) und in [Phishing-Vorfall: die ersten 60 Minuten](#).

Drei Wege, ein Ziel: Schlüssel, Passkey im Authenticator, Windows Hello

In der Diskussion werden diese drei gern gegeneinander ausgespielt, als müsste man sich entscheiden. Muss man nicht. Sie erfüllen unterschiedliche Aufgaben, und eine ordentliche Installation nutzt mindestens zwei davon nebeneinander. Die nützlichste Unterscheidung ist nicht die nach Hersteller, sondern die nach portabel und lokal.

Portable Anmeldeinformationen funktionieren geräteübergreifend. Sie sind das, womit eine Person zum ersten Mal ins System kommt, und das, womit sie sich auf einem fremden oder neuen Gerät anmeldet. Lokale Anmeldeinformationen liegen auf genau einem Gerät und werden mit dessen eigener Entsperrgeste benutzt. Sie sind bequem und schnell, aber sie helfen nichts, wenn das Gerät nicht verfügbar ist. Deshalb die Reihenfolge: erst portabel, dann lokal.

Portable und lokale Anmeldeinformationen: wer was bekommt



Skizze 2: Die Landkarte der Anmeldeinformationen. Die portable Methode startet die lokale — nicht umgekehrt.

FIDO2-Sicherheitsschlüssel

Das Stück Hardware am Schlüsselbund oder im USB-Anschluss. Es hat drei Eigenschaften, die es für Administratoren konkurrenzlos machen: Es ist vom Rechner unabhängig, es ist attestierbar, und es funktioniert auch dort, wo es kein persönliches Smartphone gibt — in der Produktion, im Krankenhaus, im Fahrzeug, hinter einer Tür, an der Telefone abgegeben werden.

Attestierung heißt: Der Schlüssel weist bei der Registrierung nach, welches Fabrikat und Modell er ist. Entra ID kann das gegen hinterlegte Metadaten prüfen. Damit lässt sich durchsetzen, dass privilegierte Konten nur mit geprüfter Hardware arbeiten — und nicht mit einem Passkey, der irgendwo in einer Cloud eines beliebigen Anbieters liegt. Der Preis dafür sind Beschaffung, Logistik und ein Ersatzvorrat im Schrank.

Passkeys im Microsoft Authenticator und synchronisierte Passkeys

Der Passkey in der Authenticator-App ist gerätegebunden: Der private Schlüssel entsteht auf dem Telefon und bleibt dort. Er ist attestierbar, kostet keine zusätzliche Hardware und lässt sich über Passkey-Profilen gezielt für einzelne Gruppen erlauben oder sperren. Für die Breite der Belegschaft ist er meist der pragmatischste Einstieg — vorausgesetzt, es gibt ein dienstliches oder freiwillig genutztes Smartphone, und ihr habt geklärt, wie ihr mit denen umgeht, die keines haben oder keines nutzen wollen.

Synchronisierte Passkeys sind der andere Fall: Der Schlüssel wird verschlüsselt im Anbieterspeicher abgelegt — iCloud-Schlüsselbund, Google Passwortmanager, ein Passwortmanager eines Drittanbieters — und steht auf allen Geräten dieses Kontos zur Verfügung. Das ist bequem, überlebt einen Gerätewechsel und ist trotzdem phishing-resistent. Es ist aber nicht attestierbar: Microsoft sagt dazu unmissverständlich, dass synchronisierte Passkeys wie andere

nicht attestierte Authenticatoren zu behandeln sind. Für Verzeichnisrollen ist das die falsche Wahl, für den Vertriebsinnendienst eine sehr gute.

Windows Hello for Business und der Entra-Passkey auf Windows

Windows Hello for Business ist die lokale Methode auf dem Arbeitsgerät und damit die, die im Alltag am häufigsten benutzt wird. Der Nutzer sieht keinen Anmeldevorgang mehr, sondern nur seine Kamera oder den Fingerabdrucksensor. Für Umgebungen mit einem Active Directory im Rücken ist Cloud-Kerberos-Trust der empfohlene Weg — er spart die komplette Zertifikatsinfrastruktur und funktioniert für Entra-ID-eingebundene wie hybrid eingebundene Geräte. Wer wissen will, was da im Hintergrund passiert, findet die Grundlagen im [Kompetenzbereich Kerberos](#).

Windows Hello for Business unterstützt bis zu zehn Nutzer je Gerät und ist ausdrücklich nicht für Kioskgeräte mit einem gemeinsamen Konto gedacht. Für geteilte Arbeitsplätze nimmst du portable Anmeldeinformationen — also den Sicherheitsschlüssel.

Seit Mai 2026 kommt der Entra-Passkey auf Windows dazu: ein gerätegebundener Passkey direkt im Windows-Hello-Container. Er wird nicht synchronisiert, das Gerät muss weder eingebunden noch registriert sein, und auf einem PC können mehrere Entra-Konten je einen eigenen Passkey ablegen. Für gemeinsam genutzte Rechner und für Beratungssituationen mit fremden Tenants ist das die praktischste Neuerung der letzten Jahre.

Kriterium	FIDO2-Sicherheitsschlüssel	Passkey im Authenticator	Windows Hello for Business
Typ	portabel, gerätegebunden	portabel, gerätegebunden	lokal, gerätegebunden
Attestierung	ja, Fabrikat und Modell prüfbar	ja, über AAGUID	nicht anwendbar, an das Gerät gebunden
Zusatzkosten	Hardware plus Ersatzvorrat	keine, wenn ein Smartphone da ist	keine, wenn die Geräte passen
Geteilte Geräte	sehr gut geeignet	geeignet	nur bis zehn Nutzer, kein Kiosk
Ohne Smartphone	funktioniert	funktioniert nicht	funktioniert
Verlustfolge	Ersatzschlüssel aus dem Vorrat	neues Telefon, neu registrieren	nur dieses Gerät betroffen
Bevorzugt für	Administratoren, stark regulierte Rollen, Produktion	breite Belegschaft, mobile Rollen	jedes persönliche Windows-Arbeitsgerät

Tabelle 1: Die drei Wege im Vergleich. Sie schließen sich nicht aus — die meisten Häuser brauchen zwei davon parallel.

WARNUNG — Zwei Sachen, die im Pilotbetrieb regelmäßig übersehen werden

Gäste können keine Passkeys registrieren. Die Registrierung von Passkey-Anmeldeinformationen wird für interne wie externe Gastkonten nicht unterstützt. Wenn deine externen Beteiligten phishing-resistent anmelden sollen, muss das über die Vertrauensstellung zum Heimattenant laufen — Details dazu in [Gastzugriff und externe Freigaben härten](#).

Ändert sich der Benutzerprinzipalname einer Person, lassen sich ihre vorhandenen Passkeys nicht nachziehen. Sie muss den alten löschen und einen neuen anlegen. Plane das bei Namensänderungen und bei Domänenenumstellungen mit ein, sonst wird die Heirat einer Kollegin zum Helpdesk-Ticket mit Sperrwirkung.

Rollout-Reihenfolge: Administratoren zuerst, und zwar aus gutem Grund

Die Versuchung ist groß, mit einer freiwilligen Pilotgruppe aus technikaffinen Kollegen zu starten. Das fühlt sich gut an und bringt sicherheitlich nichts. Die Konten, die ein Angreifer haben will, sind nicht die der Begeisterten, sondern die mit Verzeichnisrollen. Und es sind genau die Konten, bei denen ein Ausrollversehen am wenigsten Schaden anrichtet — weil die Betroffenen wissen, was sie tun, und im Zweifel selbst den Weg zurück finden.

Personas statt Abteilungen

Microsoft unterscheidet im Bereitstellungsleitfaden lediglich zwei Personas: Administratoren samt stark regulierten Rollen einerseits, alle anderen andererseits. Diese Grobheit ist Absicht. Je feiner du die Gruppen schneidest, desto länger diskutierst du über Zuordnungen und desto später hast du das erste privilegierte Konto abgesichert.

Praktisch legst du je Persona eine Sicherheitsgruppe an. Diese Gruppen benutzt du dreimal: für das Passkey-Profil, für die Registrierungskampagne und später für die Erzwingung. Wenn du sie gleich zu Anfang sauber schneidest, sparst du dir das Nachziehen an drei Stellen.

Persona	Empfohlene portable Methode	Empfohlene lokale Methode (Windows)	Ausweichoption
Administratoren und stark regulierte Rollen	FIDO2-Sicherheitsschlüssel, attestiert	Windows Hello for Business oder Entra-Passkey auf Windows	Passkey im Authenticator, Smartcard
Alle übrigen Rollen	synchronisierter Passkey	Windows Hello for Business oder Entra-Passkey auf Windows	FIDO2-Schlüssel, Passkey im Authenticator
Geteilte Arbeitsplätze und Produktion	FIDO2-Sicherheitsschlüssel	keine, bewusst nur portabel	Smartcard, wo die PKI schon läuft
Altgeräte, Terminaldienste, Linux	FIDO2-Sicherheitsschlüssel	nicht verfügbar	Smartcard, Passkey über geräteübergreifenden Anmeldefluss

Tabelle 2: Zuordnung von Methoden zu Personas. Der Grundsatz bleibt: eine portable Methode je Person, eine lokale je Gerät.

Der Temporary Access Pass ist das Startkabel

Die erste passwortlose Anmeldeinformation muss irgendwie in die Welt kommen. Wer schon eine klassische MFA-Methode registriert hat, kann sie dafür benutzen — wie das aufgesetzt wird, steht in [MFA in Microsoft 365 richtig einführen](#). Für alle anderen, für neue Kolleginnen und Kollegen und für jeden Wiederherstellungsfall gibt es den Temporary Access Pass: einen zeitlich begrenzten Code, mit dem sich jemand einmal oder mehrfach anmelden kann, um dort die richtigen Methoden zu registrieren.

Der TAP erfüllt die Multifaktor-Stärke, aber ausdrücklich nicht die kennwortlose und nicht die phishing-resistente Stärke. Das ist gut so und muss dir bewusst sein: Wenn deine Erzwingungsrichtlinie für alle Ressourcen phishing-resistente Anmeldung verlangt, sperrst du damit auch den Wiederherstellungsweg zu. Die Registrierungsoberfläche gehört deshalb aus der harten Richtlinie ausgenommen — sonst hast du einen sehr sicheren Tenant, in den niemand mehr hineinkommt.

Einstellung	Standardwert	Zulässiger Bereich	Praxisempfehlung
Mindestlaufzeit	1 Stunde	10 Minuten bis 30 Tage	60 Minuten
Maximallaufzeit	8 Stunden	10 Minuten bis 30 Tage	8 Stunden, für Neueintritte am

			ersten Tag
Standardlaufzeit	1 Stunde	10 Minuten bis 30 Tage	60 Minuten für Wiederherstellungsfälle
Einmalige Verwendung	aus	ein oder aus	aus, aber Nutzung überwachen
Länge des Codes	8 Zeichen	8 bis 48 Zeichen	mindestens 12 Zeichen

Tabelle 3: Die Richtlinie für den Temporary Access Pass. Nur wer in der Richtlinie enthalten ist, kann sich damit auch anmelden.

TIPP — TAP im Alltag: die vier Dinge, die den Unterschied machen

Einmal-TAP und Geräteeinrichtung vertragen sich schlecht. Wer mit einem Einmal-TAP eine passwortlose Methode registriert, muss das binnen zehn Minuten schaffen. Dauert die Geräteeinrichtung länger, braucht es einen zweiten TAP. Ein mehrfach nutzbarer TAP mit kurzer Laufzeit erspart dem Service Desk diesen Ärger.

Je Konto existiert immer nur ein TAP. Ein neuer überschreibt den alten — auch den noch gültigen.

Rollen sauber trennen: Authentifizierungsadministratoren können TAPs für normale Konten ausstellen, für privilegierte Konten braucht es die Rolle Privilegierter Authentifizierungsadministrator. Niemand kann sich selbst einen ausstellen.

Tokens aus einer TAP-Anmeldung sind zunächst auf die TAP-Laufzeit begrenzt, die Sitzung danach aber nicht automatisch. Wenn du das kurz halten willst, brauchst du eine Anmeldehäufigkeit in Conditional Access.

Wellen statt Stichtag

Der wichtigste Satz zum Ausrollen steht nicht in der Dokumentation, sondern im Ticketsystem: Das Aufkommen am Service Desk ist dein Tempomacher. Steigt es, verlangsamt du. Fällt es, gehst du weiter. Deshalb arbeitest du mit Zeitfenstern statt mit Stichtagen und mit einer Sicherheitsgruppe je Welle, die du einzeln in die Richtlinien aufnimmst.

Rollout in Wellen: Admins zuerst, Erzwingung zuletzt

Vorlauf Wochen 1–2	Personas festlegen und in Gruppen abbilden. Passkey-Profile anlegen. TAP-Richtlinie aktivieren. Report-only-Richtlinie mit phishing-resistenter Stärke scharfstellen — sie erzwingt nichts, sie protokolliert.
Welle 1 Wochen 3–5	Alle mit Verzeichnisrollen: Global Administrator, Privileged Role Administrator, Exchange, SharePoint, Sicherheit. Zwei Sicherheitsschlüssel je Person. Break-Glass-Konten bekommen ihre eigene Behandlung und bleiben ausgenommen.
Welle 2 Wochen 5–8	Geschäftsführung, Finanzen, Personal, Entwicklung, alle mit Zugriff auf sensible Daten. Sicherheitsschlüssel oder Passkey im Authenticator, dazu Windows Hello for Business auf dem Arbeitsgerät.
Welle 3 Wochen 8–14	Die Breite der Belegschaft. Synchronisierte Passkeys oder Passkey im Authenticator, lokale Methode je Gerät. Registrierungskampagne statt Einzelansprache.
Welle 4 ab Woche 14	Sonderfälle: geteilte Geräte, Produktion, Fahrzeuge, Terminalserver, alte Betriebssysteme. Hier gewinnt fast immer der Sicherheitsschlüssel — er braucht kein persönliches Gerät.
Die Erzwingung folgt der Registrierung immer mit Abstand — Welle für Welle, je Betriebssystem, nie als tenantweiter Stichtag. Tempomacher ist nicht der Projektplan, sondern das Ticketaufkommen am Service Desk.	

Skizze 3: Ein Rollout, der sich am Ticketaufkommen orientiert statt am Wunschtermin der Geschäftsführung.

Die Registrierungskampagne in der Authentifizierungsmethoden-Richtlinie nimmt dir dabei den größten Teil der Einzelansprache ab: Nutzer werden nach erfolgreicher MFA-Anmeldung zur Passkey-Registrierung aufgefordert. Im Microsoft-verwalteten Zustand läuft das ohnehin bereits für alle, die noch für SMS oder Anruf freigeschaltet sind. Du kannst diese Kampagne aber gezielt vorziehen und auf deine eigenen Wellen-Gruppen richten — was deutlich angenehmer ist, als sie ungesteuert über die gesamte Belegschaft hereinbrechen zu lassen.

Kommunikation gehört mit Vorlauf dazu, und zwar mehrfach: sechzig Tage vor der Erzwingung die Ankündigung, dann in abnehmenden Abständen bis zum Vortag. Wer nur einmal informiert, informiert praktisch niemanden. Wenn ihr die Belegschaft ohnehin schon mit simulierten Phishing-Mails trainiert — siehe [Attack Simulation Training: Phishing-Übungen richtig aufsetzen](#) —, ist das der ideale Aufhänger: Ihr könnt erklären, warum diese Übungen nach der Umstellung an Bedeutung verlieren.

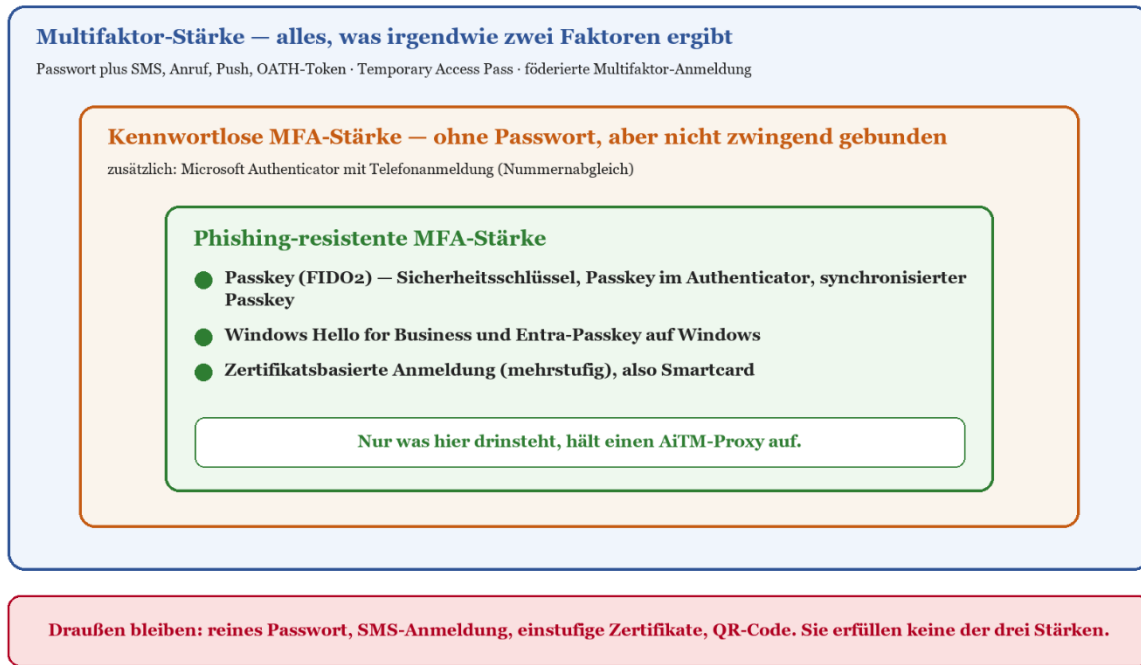
Erzwingen: Authentifizierungsstärken im Conditional Access

Registrierung allein ändert nichts. Solange das Passwort weiterhin funktioniert, benutzen Nutzer weiterhin das Passwort — nicht aus Bosheit, sondern aus Gewohnheit. Der Hebel für die Durchsetzung heißt Authentifizierungsstärke und ist eine Zugriffssteuerung in Conditional Access. Die Voraussetzung ist Entra ID P1.

Drei eingebaute Stärken, und wann du eine eigene brauchst

Microsoft liefert drei Stärken mit, die sich nicht verändern lassen und die automatisch wachsen, wenn neue Methoden dazukommen. Das ist ein Vorteil: Deine Richtlinie muss nicht angefasst werden, wenn Microsoft eine neue phishing-resistente Methode freigibt.

Die drei eingebauten Authentifizierungsstärken



Skizze 4: Die drei eingebauten Stärken als ineinanderliegende Mengen. Je weiter innen, desto weniger lässt sich weitergeben.

Methode	Multifaktor-Stärke	Kennwortlose MFA	Phishing-resistente MFA
Passkey (FIDO2), Sicherheitsschlüssel oder App	erfüllt	erfüllt	erfüllt
Windows Hello for Business, Plattform-Anmeldeinformation	erfüllt	erfüllt	erfüllt
Zertifikatsbasiert, mehrstufig	erfüllt	erfüllt	erfüllt
Microsoft Authenticator, Telefonanmeldung	erfüllt	erfüllt	erfüllt nicht
Temporary Access Pass	erfüllt	erfüllt nicht	erfüllt nicht
Passwort plus SMS, Anruf, Push oder OATH-Token	erfüllt	erfüllt nicht	erfüllt nicht
Föderierte mehrstufige Anmeldung	erfüllt	erfüllt nicht	erfüllt nicht
Passwort allein, SMS-Anmeldung, einstufiges Zertifikat, QR-Code	erfüllt nicht	erfüllt nicht	erfüllt nicht

Tabelle 4: Welche Methode welche Stärke erfüllt. Die Zeile mit dem Temporary Access Pass ist die, die den Wiederherstellungsweg bestimmt.

Eine eigene Stärke brauchst du im Wesentlichen dann, wenn du auf bestimmte Schlüsselmodelle einschränken willst. In den erweiterten Optionen einer eigenen Stärke lassen sich einzelne AAGUIDs zulassen — also genau die Fabrikate, die ihr beschafft habt. Für den Regelfall reicht die eingebaute phishing-resistente Stärke völlig aus.

Report-only zuerst, und zwar früh

Lege die Erzwingungsrichtlinie an, bevor du mit der Registrierung anfängst — im Modus Nur-Bericht, für alle Nutzer außer den Break-Glass-Konten, für alle Ressourcen, mit der phishing-resistenten Stärke als Zugriffssteuerung. Sie blockiert nichts. Sie schreibt in die Anmeldeprotokolle, wer blockiert worden wäre. Nach vier Wochen hast du eine belastbare Liste statt einer Vermutung.

Das ist dieselbe Disziplin wie bei jeder anderen Richtlinie und aus demselben Grund: Die Sonderfälle deines Hauses stehen in keiner Dokumentation. Wie eine Baseline aussieht, in die sich diese Richtlinie einfügt, beschreibt [Conditional Access: Baselines, die nicht nerven](#).

Erzwingung je Betriebssystem, nicht je Abteilung

Der wichtigste Kniff bei der Erzwingung ist die Schnittdimension. Nicht die Abteilung entscheidet, ob jemand bereit ist, sondern das Paar aus Nutzer und Gerät. Jemand mit einem aktuellen Windows-Notebook kann längst erzwungen werden, während dieselbe Person auf einem Android 13 noch scheitert. Deshalb legst du je Geräteplattform eine Gruppe und eine Richtlinie an und füllst die Gruppen nach und nach.

Richtlinie	Zielgruppe	Bedingung Geräteplattform	Zugriffssteuerung
PR-01	Windows-bereite Nutzer	Windows	Authentifizierungsstärke: phishing-resistente MFA
PR-02	macOS-bereite Nutzer	macOS	Authentifizierungsstärke: phishing-resistente MFA
PR-03	iOS-bereite Nutzer	iOS	Authentifizierungsstärke: phishing-resistente MFA
PR-04	Android-bereite Nutzer	Android	Authentifizierungsstärke: phishing-resistente MFA
PR-05	übrige bereite Nutzer	alle außer den vier oben	Authentifizierungsstärke: phishing-resistente MFA

Tabelle 5: Fünf Richtlinien für die schrittweise Erzwingung. Am Ende, wenn alle Gruppen voll sind, ersetzt du sie durch eine einzige Richtlinie für alle.

Als Faustregel für die Bereitschaft gilt: Windows 10 und neuer, iOS 17 und neuer, Android 14 und neuer, macOS 13 Ventura und neuer. Alles darunter, dazu virtuelle Arbeitsplätze, Terminaldienste und Linux, löst du über externe Hardware — Sicherheitsschlüssel oder Smartcard — oder über den geräteübergreifenden Anmeldefluss mit einem Passkey.

Passkey-Profile: Feinsteuerung je Gruppe

Statt einer tenantweiten Einstellung gibt es heute Passkey-Profile: benannte Regelsätze, die je Zielgruppe festlegen, welche Passkey-Arten erlaubt sind, ob Attestierung erzwungen wird und welche Fabrikate über ihre AAGUID zugelassen oder gesperrt sind. Damit lässt sich das trennen, was fachlich getrennt gehört.

Profil	Zielgruppe	Passkey-Arten	Attestierung	Schlüsselbeschränkung
Nur attestierte Hardware	IT-Administration, Geschäftsführung, Entwicklung	nur gerätegebunden	erzwungen	nur die beschafften Modelle zulassen
Gerätegebunden ohne Einschränkung	Personal, Finanzen, Vertrieb	nur gerätegebunden	erzwungen	aus
Alles erlaubt	übrige Belegschaft	gerätegebunden und	aus	aus

		synchronisiert		
--	--	----------------	--	--

Tabelle 6: Ein tragfähiger Schnitt für drei Profile. Mehr als drei Profile inklusive des Standardprofils werden derzeit nicht unterstützt.

WARNUNG — Die AAGUID-Falle und das Kleingedruckte zur Attestierung

Schlüsselbeschränkungen wirken auf Registrierung UND Anmeldung. Wenn du eine AAGUID aus der Zulassungsliste entfernst, können Personen, die dieses Modell bereits registriert haben, sich damit nicht mehr anmelden. Vor jeder Änderung an der Liste gehört ein Blick darauf, wer betroffen wäre. Attestierung wirkt nur zum Zeitpunkt der Registrierung. Wer sich ohne Attestierung registriert hat und bei dem du später die Erzwingung einschaltest, wird nicht ausgesperrt — die alte Anmeldeinformation bleibt gültig. Nachträgliches Aufräumen musst du selbst machen. Ohne erzwungene Attestierung ist eine AAGUID-Liste eine Empfehlung, keine Kontrolle. Microsoft formuliert das ungewohnt deutlich: Ist die Attestierung aus, kann Entra ID über einen Passkey keine einzige Eigenschaft garantieren — auch nicht, ob er synchronisiert oder gerätegebunden ist. Die Ausschlussliste in der Passkey-Richtlinie schlägt jede Einschlussliste. Wer dort steht, ist vollständig von Registrierung und Anmeldung ausgeschlossen.

Wenn der Schlüssel weg ist

Jedes Passwordless-Projekt bekommt irgendwann dieselbe Frage gestellt, meistens von jemandem, der bis dahin geschwiegen hat: Und was ist, wenn ich den verliere? Die Frage ist berechtigt, und die schlechteste Antwort darauf ist Improvisation. Die zweitschlechteste ist ein Passwort, das man für den Notfall doch noch behält.

FAKTEN — Was beim Verlust eines Schlüssels tatsächlich passiert

Der Finder kann damit nichts anfangen. Der private Schlüssel liegt in Hardware und ist ohne die zugehörige PIN oder Biometrie nicht benutzbar. Nach mehreren Fehleingaben sperrt sich der Schlüssel; bei den meisten Modellen wird er dann zurückgesetzt und das Schlüsselmaterial gelöscht. Es steht kein Benutzername darauf und kein Firmenname.

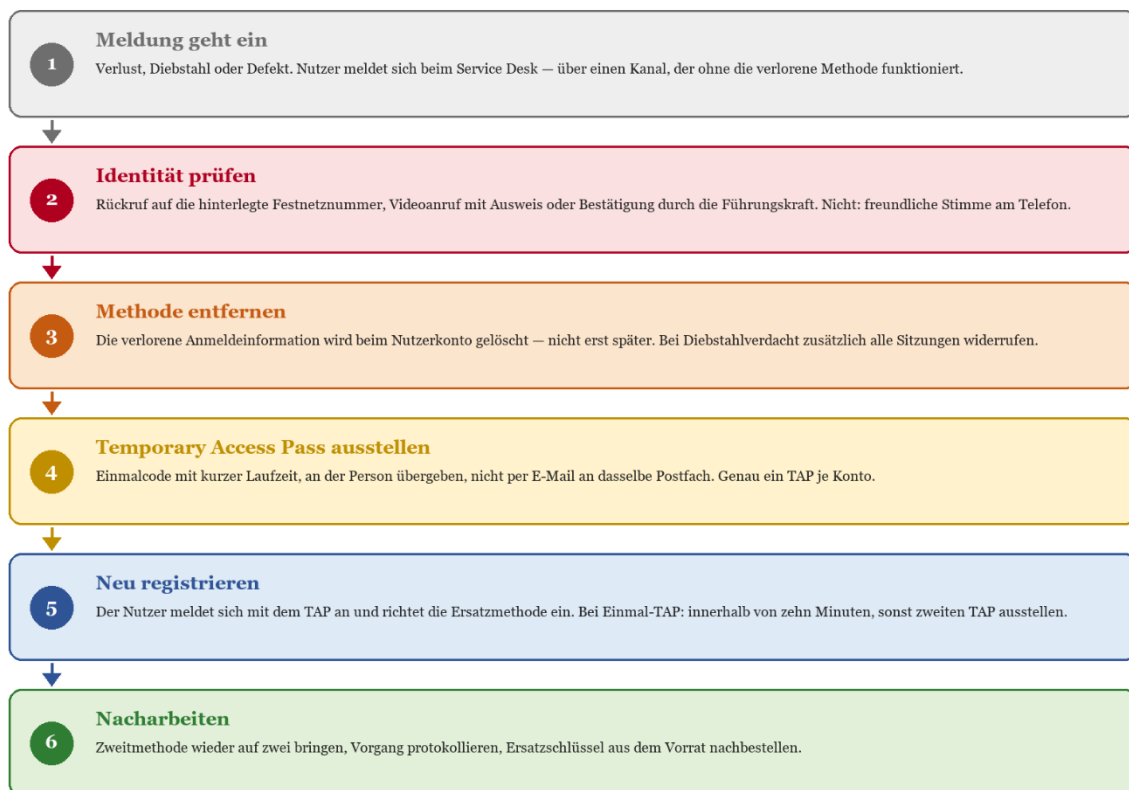
Es gibt nichts, was aus dem Schlüssel ausgelesen werden könnte, was anderswo nützt. Ein Passkey ist für genau eine Domäne registriert und lässt sich nicht auf einen anderen Dienst umbiegen.

Was gesperrt werden muss, ist nicht der Schlüssel, sondern seine Registrierung. Du löschst die Anmeldeinformation beim Nutzerkonto in Entra ID. Ab diesem Moment ist der Gegenstand elektronischer Restmüll.

Wer eine zweite Methode registriert hat, meldet sich normal weiter an und meldet den Verlust in Ruhe. Wer nur eine hatte, steht vor der Tür und braucht den Service Desk. Genau das ist der Grund für die Regel: mindestens zwei Methoden je Person, immer.

Bei Diebstahlverdacht und bei privilegierten Konten kommt der Widerruf aller aktiven Sitzungen dazu. Eine gelöschte Anmeldeinformation beendet bestehende Sitzungen nicht von selbst.

Schlüssel weg: der Ablauf, der vorher aufgeschrieben sein muss



Skizze 5: Der Wiederherstellungsablauf. Er gehört aufgeschrieben, bevor er gebraucht wird — nicht währenddessen.

Der Service Desk ist ab jetzt die Angriffsfläche

Das ist die unbequeme Wahrheit jeder passwortlosen Umgebung. Wenn die Anmeldung selbst nicht mehr angreifbar ist, wird der Wiederherstellungsweg zum lohnendsten Ziel. Ein Anruf, eine glaubwürdige Geschichte über ein verlorenes Telefon vor einem wichtigen Termin, ein hilfsbereiter Kollege am Telefon — und der Angreifer hat einen Temporary Access Pass für ein Konto, das er nie phishen konnte. Das ist keine Theorie, das ist der Standardweg gegen Organisationen, die ihre Anmeldung gehärtet und ihren Service Desk vergessen haben.

Die Gegenmaßnahmen sind organisatorisch, nicht technisch: eine festgelegte Identitätsprüfung vor jeder Ausstellung, ein zweiter Kanal, der nicht das Postfach der betroffenen Person ist, bei privilegierten Konten ein Vieraugenprinzip, und ein Protokoll über jede Ausstellung, das regelmäßig jemand liest. Eine Benachrichtigung auf ausgestellte TAPs für Inhaber von Verzeichnisrollen gehört in die Überwachung — wie das aufgesetzt wird, steht in [Alert Policies und Benachrichtigungen richtig aufsetzen](#).

Break-Glass bleibt Break-Glass

Die Notfallkonten sind der eine Ort, an dem du bewusst nicht mitziehst. Sie werden aus jeder Erzwingungsrichtlinie ausgenommen, ihre Anmeldeinformationen liegen physisch getrennt und aufgeteilt, und sie werden regelmäßig getestet. Ein reines Passwordless-Break-Glass-Konto klingt konsequent, ist aber riskant: Es macht dich von genau der Hardware abhängig, die im Ernstfall im verschlossenen Schrank des abwesenden Kollegen liegt. Ein sinnvoller Kompromiss sind zwei Notfallkonten mit unterschiedlichen Verfahren. Die vollständige Argumentation dazu steht in [Break-Glass-Konten anlegen und überwachen](#).

Und weil sich das erfahrungsgemäß niemand freiwillig ansieht: Der Wiederherstellungsweg gehört einmal geübt, mit echtem Konto und echter Uhr. Das passende Format dafür ist die [Feuerwehrübung: Security-Notfälle im Team trainieren](#), und die Anschlussstelle ist der [Incident-Response-Plan für Microsoft 365](#).

TIPP — Vier Regeln, die den Verlustfall entschärfen, bevor er eintritt

Zwei registrierte Methoden je Person sind Pflicht, nicht Empfehlung. Üblich und gut: eine portable und eine lokale — oder bei Administratoren zwei Sicherheitsschlüssel, von denen einer zu Hause oder im Tresor liegt.

Ersatzschlüssel im Schrank vorhalten, mindestens fünf Prozent der ausgegebenen Menge.

Beschaffungsvorgänge dauern in der Regel länger als die Geduld einer Führungskraft.

Den Wiederherstellungsablauf als Ablaufplan schreiben, nicht als Prosa. Wer prüft was, wer darf was ausstellen, was wird protokolliert, wann werden Sitzungen widerrufen.

Die Registrierungsoberfläche aus der harten Erzwingungsrichtlinie ausnehmen. Sonst schließt du genau den Weg, über den sich jemand wieder handlungsfähig macht.

Was das Ganze kostet und was es einspart

Passkeys selbst sind lizenzfrei: Sie stehen in allen Entra-ID-Editionen zur Verfügung, auch in der kostenlosen. Geld kostet die Erzwingung, weil dafür Conditional Access und damit Entra ID P1 nötig ist — was in den gängigen Microsoft-365-Paketen für Unternehmen ohnehin enthalten ist. Der zweite Kostenblock ist Hardware, und der ist überschaubar: Zwei ordentliche Sicherheitsschlüssel je Administrator liegen im niedrigen dreistelligen Bereich, Ersatzvorrat eingerechnet.

Der eigentliche Aufwand steckt woanders: in der Kommunikation, im Service Desk während der Umstellungswellen und in der Bereinigung der Altlasten, die vorher niemand sehen wollte. Rechne mit einer Projektlaufzeit von drei bis fünf Monaten für ein mittelständisches Haus, davon deutlich mehr Zeit für Abstimmung als für Konfiguration.

Dem gegenüber steht eine Ersparnis, die selten in die Rechnung kommt: Passwortrücksetzungen verschwinden weitgehend, MFA-Ermüdungsangriffe verschwinden vollständig, und die Anmeldung dauert im Alltag Sekundenbruchteile statt eines halben Vorgangs mit Telefon in der Hand. Wer den Nutzen gegenüber der Geschäftsführung darstellen muss, findet in [Security-Reporting für die Geschäftsführung](#) die passenden Kennzahlen — und in [Secure Score: sinnvoll nutzen statt Punktejagd](#) den Punktestand, der sich dabei ganz nebenbei bewegt.

Für die regulatorische Seite ist der Vorgang ebenfalls dankbar: Phishing-resistente Authentifizierung privilegierter Zugänge ist eine der wenigen technischen Maßnahmen, die sich in [NIS2 aus Security-Sicht: technische Maßnahmen in M365](#) ohne Interpretationsakrobatik direkt belegen lässt. Und sie ist einer der wenigen Bausteine aus [Zero Trust im Mittelstand: pragmatisch statt dogmatisch](#), bei dem die Wirkung so unmittelbar ist, dass die Diskussion über den Begriff sich erübrigt. Wenn du dir die Reihenfolge und den Schnitt für dein Haus nicht selbst zusammensuchen willst, ist das ein typischer Fall für die [Microsoft 365 Security Beratung](#); wenn das Team es hinterher selbst betreiben soll, für die [Schulung Microsoft 365 Security](#).

Häufige Fragen

Können wir das Passwort danach löschen?

Nicht wirklich, und das ist der Punkt, an dem viele Projekte enttäuscht sind. Das Kennwort bleibt im Konto vorhanden, es wird nur nicht mehr benutzt. Solange Conditional Access die phishing-resistente Stärke verlangt, kann jemand zwar noch ein Passwort eintippen, kommt damit aber nicht ans Ziel. Was du erreichen kannst, ist Bedeutungslosigkeit — nicht Abwesenheit. Praktisch heißt das: Passwortrichtlinien bleiben bestehen, aber sie hören auf, sicherheitsrelevant zu sein.

Wir haben Leute ohne Diensthandy. Was machen wir mit denen?

FIDO2-Sicherheitsschlüssel. Sie sind genau für diesen Fall die richtige Antwort und der Grund, warum eine reine Passkey-im-Authenticator-Strategie in Betrieben mit Produktion, Pflege oder Außendienst regelmäßig scheitert. Ein Schlüssel kostet weniger als eine Stunde Diskussion darüber, ob man private Telefone dienstlich einbinden darf. Und die Frage, ob man das darf, ist in mitbestimmten Betrieben ohnehin keine, die die IT allein entscheidet.

Ist ein synchronisierter Passkey im iCloud-Schlüsselbund sicher genug?

Für die breite Belegschaft: ja. Er ist phishing-resistent, er überlebt einen Gerätewechsel, und er kostet nichts. Für Verzeichnisrollen: nein. Der Grund ist nicht die Sicherheit des Anbieters, sondern die fehlende Attestierung — Entra ID kann über einen synchronisierten Passkey keine Eigenschaft garantieren und kann nicht unterscheiden, auf wie vielen Geräten er am Ende liegt. Für privilegierte Konten willst du genau diese Gewissheit, deshalb dort attestierte, gerätegebundene Hardware.

Was passiert mit unseren Dienstkonten und Skripten?

Nichts, und das ist ein Problem für sich. Passkeys sind eine Methode für Menschen. Nicht interaktive Zugriffe laufen über Anwendungsregistrierungen, verwaltete Identitäten und Zertifikate — und die sind nach einem erfolgreichen Passwordless-Projekt oft der am schlechtesten gesicherte Rest im Tenant. Setze das Aufräumen der Dienstkonten direkt hinter das Passwordless-Projekt auf die Liste, nicht irgendwann.

Wie viele Sicherheitsschlüssel braucht eine Person?

Zwei. Einer am Schlüsselbund, einer an einem sicheren Ort, der nicht derselbe Ort ist. Die Rechnung ist unromantisch: Der zweite Schlüssel kostet einmalig einen kleinen Betrag, ein Wiederherstellungsvorgang über den Service Desk kostet jedes Mal Arbeitszeit auf beiden Seiten und schafft eine Gelegenheit für einen Social-Engineering-Angriff. Bei Administratoren ist der zweite Schlüssel nicht verhandelbar.

Können wir das schrittweise machen, oder muss der ganze Tenant auf einmal?

Schrittweise, unbedingt. Genau dafür gibt es die Trennung zwischen Authentifizierungsmethoden-Richtlinie und Authentifizierungsstärke: Die erste bestimmt, wer eine Methode überhaupt registrieren darf, die zweite, wo sie verlangt wird. Du kannst Passkeys für alle freigeben, aber nur für die Administratorengruppe erzwingen — und diese Gruppe dann Welle für Welle vergrößern.

Unsere alte Branchenapplication kann kein FIDO2. Und jetzt?

Erst prüfen, ob das stimmt. Häufig kann nicht die Anwendung kein FIDO2, sondern sie hat einen eingebetteten Browser aus einer anderen Zeit oder benutzt noch ein altes Anmeldeprotokoll. Im ersten Fall hilft ein Update, im zweiten ist es ohnehin ein Fall für [Legacy Authentication endgültig abschalten](#). Bleibt eine echte Lücke, grenzt du sie ein: eigene Richtlinie, benannte Nutzergruppe, Netzwerkbedingung, Ablaufdatum im Namen der Richtlinie und ein Verantwortlicher, der den Ablauf im Kalender hat.

Wie merken wir, ob es wirkt?

Über zwei Berichte. Die Registrierung zeigt dir die Aktivität der Authentifizierungsmethoden: wie viele Personen überhaupt zu phishing-resistenter Anmeldung fähig sind. Die Nutzung zeigt dir in den Anmeldeprotokollen, womit tatsächlich angemeldet wurde. Die Lücke zwischen beiden Zahlen ist die interessante Kennzahl — sie sagt dir, wie viele Menschen die neue Methode registriert haben und trotzdem weiter das Passwort benutzen. Diese Lücke schließt keine Kommunikation, sondern nur die Erzwingung.

Wir haben Security Defaults aktiv. Reicht das nicht?

Nein. Security Defaults verlangen MFA, aber sie kennen keine Authentifizierungsstärken und können daher phishing-resistente Verfahren nicht erzwingen. Sie sind ein guter Grundsatz für kleine Umgebungen und ein Hindernis, sobald du differenzieren willst. Die Abwägung im Detail steht in [Security Defaults oder Conditional Access?](#).

Fazit

Passwordless ist kein Komfortprojekt mit sicherheitlichem Nebeneffekt, sondern der einzige Schritt in der Anmeldearchitektur, der eine ganze Angriffsklasse entfernt statt sie zu erschweren. Wer phishing-resistent anmeldet, kann keinen Code weitergeben, weil es keinen gibt — und keine Anmeldeseite verwechseln, weil der Schlüssel die Verwechslung nicht mitmacht.

Die Reihenfolge ist wichtiger als die Technik. Erst die Personas und Gruppen, dann die Passkey-Profile, dann der Temporary Access Pass als Startkabel, dann die Report-only-Richtlinie möglichst früh — und erst danach die Registrierung in Wellen, mit den privilegierten Konten vorneweg. Die Erzwingung folgt der Registrierung mit Abstand, je Betriebssystem, gesteuert vom Ticketaufkommen und nicht vom Wunschtermin.

Der Teil, der am häufigsten fehlt, ist der unspektakulärste: der aufgeschriebene Wiederherstellungsweg. Zwei Methoden je Person, Ersatzschlüssel im Schrank, eine Identitätsprüfung, die diesen Namen verdient, und ein Protokoll, das jemand liest. Sonst hast du die Haustür durch eine Panzertür ersetzt und den Schlüsseldienst im Telefonbuch stehen lassen.

Und der Zeitdruck ist diesmal keiner, den man wegdiskutieren kann. Seit Anfang September 2026 sind Passkeys der Standard, ab Februar 2027 gibt es die von Microsoft betriebene SMS- und Sprachzustellung nicht mehr. Wer erst dann anfängt, macht den Rollout nicht in Wellen, sondern an einem Montagmorgen — gemeinsam mit allen anderen, die auch erst dann angefangen haben. Wie so etwas endet, wenn zusätzlich noch jemand von außen mitliest, zeigt das [Dossier TerminalFix und der Berlin-Hack](#).

WEITER — Passende Beiträge aus dieser Reihe

- › [MFA in Microsoft 365 richtig einführen](#) — die Vorstufe, auf der dieses Projekt aufsetzt
- › [Conditional Access: Baselines, die nicht nerven](#) — der Rahmen, in dem die Erzwingung lebt

- › [Break-Glass-Konten anlegen und überwachen](#) — die Ausnahme, die nie mitwandert
- › [Legacy Authentication endgültig abschalten](#) — die Vorarbeit, ohne die alles andere Kosmetik bleibt
- › [Tenant-Härtung: die 20 wichtigsten Schrauben](#) — was rund um die Anmeldung noch zu tun ist
- › [Gastzugriff und externe Freigaben härten](#) — warum externe Konten hier eine Sonderrolle haben
- › [Microsoft 365 Security Beratung](#) — Unterstützung bei Schnitt, Reihenfolge und Rollout
- › [Schulung Microsoft 365 Security](#) — wenn das Team es selbst können soll