

Legacy Authentication endgültig abschalten

Es gibt in jedem Tenant diesen einen Gegenstand, über den niemand gern spricht. Er steht im Flur zwischen Teeküche und Kopierraum, hat vier Papierschächte, ein Display mit Touch-Verzögerung und eine Konfigurationsseite, die zuletzt 2017 jemand geöffnet hat. In dieser Konfigurationsseite steht ein Postfachname und ein Kennwort im Klartextfeld. Und dieses Kennwort gehört, in erschreckend vielen Häusern, nicht einem Dienstkonto, sondern der Kollegin aus der Buchhaltung, die 2017 zufällig danebenstand.

Genau dieses Gerät ist der Grund, warum die Multifaktor-Einführung im Haus nicht das gebracht hat, was sie bringen sollte. Denn solange irgendwo im Tenant noch ein Protokoll offen ist, das nichts anderes kann als Benutzername und Kennwort entgegenezunehmen, hat ein Angreifer eine Tür, an der niemand nach dem zweiten Faktor fragt. Er muss sie nur finden. Und er sucht automatisiert, rund um die Uhr, seit Jahren.

Dieser Beitrag gehört zum Handlungsfeld „Identitäten härten“ der Serie [Microsoft 365 Security](#) und behandelt den Teil, den man am liebsten aufschiebt, weil er nicht nach Sicherheitsarbeit aussieht, sondern nach Inventur: herausfinden, wer im Haus noch alte Anmeldeverfahren benutzt, diese Fälle einzeln umstellen — und die Tür danach so zumachen, dass sie auch zubleibt.

Die gute Nachricht vorweg: Den größten Teil der Arbeit hat Microsoft dir bereits abgenommen und die meisten Legacy-Protokolle in Exchange Online längst zwangsweise geschlossen. Die schlechte: Der Rest ist genau der Teil, der in deinem Haus produktiv im Einsatz ist. Sonst wäre er ja schon weg.

Was Legacy Auth eigentlich ist — und warum MFA daran abprallt

„Legacy Authentication“ ist kein einzelnes Protokoll, sondern eine Familie. Gemeinsam ist allen Mitgliedern ein einziges Merkmal: Der Client schickt Benutzername und Kennwort mit — bei manchen Verfahren sogar bei jeder einzelnen Anfrage — und der Server antwortet mit „ja“ oder „nein“. Das ist Basic Authentication. Sie ist bequem, sie ist uralte, sie funktioniert überall, und sie ist genau deshalb noch da.

Die Protokollfamilie im Überblick

Wenn im Sicherheitsbericht „Legacy Auth“ steht, ist meist eines der folgenden Verfahren gemeint. Die Tabelle sortiert sie nach dem, was dir in der Praxis begegnet — und nach dem, was heute noch davon übrig ist.

Protokoll	Wer es typischerweise nutzt	Zustand heute	Der Weg nach vorn
POP3 / IMAP4	Linux-Clients, Archivlösungen, Ticketsysteme, Thunderbird	Basic Auth abgeschaltet, OAuth möglich	OAuth 2.0 für IMAP und POP oder Umstieg auf Graph
SMTP AUTH	Drucker, Scanner,	Einziges Verfahren, bei	OAuth, Relay-Connector

	Fachanwendungen, Monitoring, Skripte	dem Basic Auth noch lebt	oder High Volume Email
Exchange ActiveSync	Native Mail-Apps auf Telefonen und Tablets	Basic Auth abgeschaltet	Outlook für iOS und Android oder aktuelle native App
Exchange Web Services	Raumsteuerungen, CRM- Anbindungen, Signaturlösungen, Archive	Basic Auth abgeschaltet, OAuth möglich, keine neuen Funktionen	Microsoft Graph, ersatzweise EWS mit OAuth
Remote PowerShell	Automatisierung, Verwaltungsskripte, Partnerzugriffe	Basic Auth abgeschaltet	Exchange-Online-Modul mit zertifikatbasierter Anmeldung
MAPI over HTTP, Outlook Anywhere, Adressbuch, Autodiscover	Ältere Outlook-Versionen und alles, was Postfächer sucht	Basic Auth abgeschaltet	Outlook ab 2016, moderne Authentifizierung aktiviert

Tabelle 1: Die Legacy-Protokolle und ihr heutiger Zustand in Exchange Online.

Wichtig ist die Unterscheidung zwischen Protokoll und Anmeldeverfahren. IMAP ist nicht per se unsicher — IMAP mit OAuth ist völlig in Ordnung. Unsicher ist die Kombination aus altem Protokoll und Basic Auth. Genau deshalb steht in den Berichten manchmal ein Protokollname, obwohl der Zugriff längst modern erfolgt: Wenn in den Anmeldeprotokollen „Browser“ oder „Mobile Apps and Desktop clients“ steht, ist alles gut. Steht dort ein konkreter Protokollname wie „Exchange ActiveSync“, dann nicht.

Warum der zweite Faktor nie gefragt wird

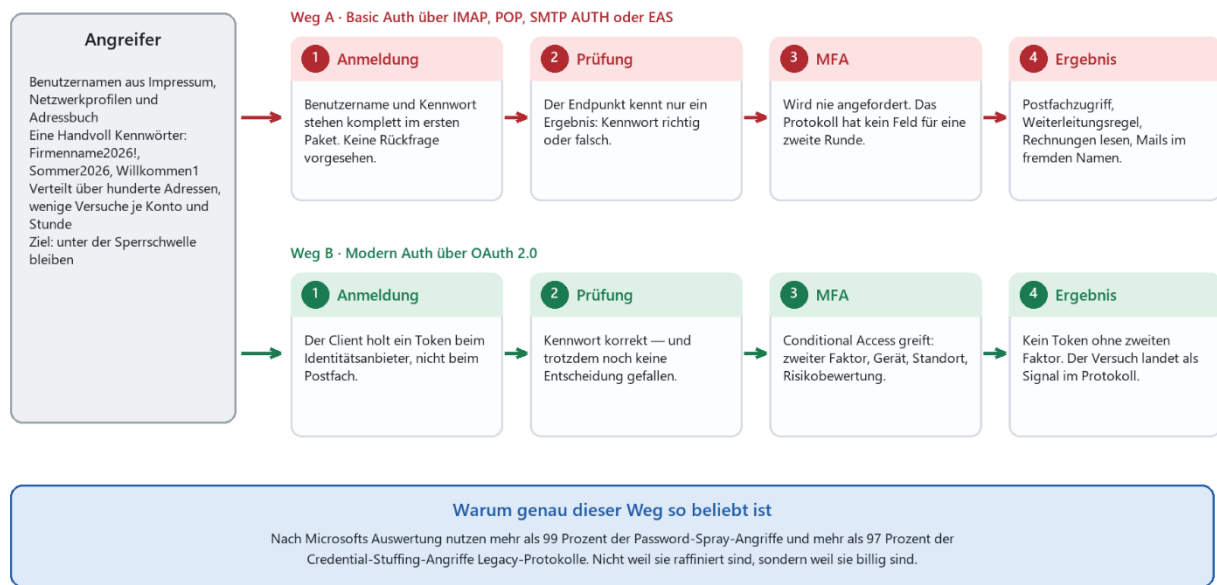
Der entscheidende Punkt ist kein Konfigurationsfehler, sondern Protokolldesign. Basic Auth kennt keinen Zwischenschritt. Der Client sagt „hier ist mein Kennwort“, der Server sagt „gut“ oder „nicht gut“. Es gibt in diesem Ablauf keine Stelle, an der ein Dienst zurückfragen könnte: „Bestätige das bitte auf deinem Telefon.“ Ein Drucker aus dem Jahr 2015 hätte auch gar nicht die Möglichkeit, so eine Rückfrage anzuzeigen.

Damit ist MFA an dieser Stelle nicht umgangen, sondern schlicht unerreichbar. Dasselbe gilt für alles, was Conditional Access sonst noch beisteuert: Gerätekonformität, Standortbewertung, Sitzungssteuerung, Risikoeinstufung. All diese Signale entstehen im Token-Fluss von OAuth. Wo kein Token fließt, gibt es auch nichts zu bewerten.

Angreifer wissen das seit Jahren, und sie haben ihre Werkzeuge entsprechend gebaut. Der Klassiker ist Password Spray: nicht tausend Kennwörter gegen ein Konto — das löst Sperren aus —, sondern ein plausibles Kennwort gegen tausend Konten, verteilt über viele Quelladressen und über Stunden gestreckt. Als Ziel nimmt man den Endpunkt, der am wenigsten zurückfragt.

Password Spray trifft auf Basic Auth

Dasselbe Kennwort gegen viele Konten — der Unterschied liegt im Protokoll, nicht im Kennwort.



Ein blockiertes Legacy-Protokoll nimmt dem Angriff nicht das Kennwort, aber den Türgriff.

Skizze 1: Derselbe Angriff, zwei Protokollwege. Der Unterschied entsteht nicht beim Kennwort, sondern in Schritt drei.

FAKTEN · Warum Legacy Auth das Lieblingsziel ist

Microsoft wertet die Angriffsversuche gegen Entra ID kontinuierlich aus und kommt zu einer bemerkenswert eindeutigen Verteilung:

- › Mehr als 99 Prozent aller Password-Spray-Angriffe laufen über Legacy-Protokolle.
- › Mehr als 97 Prozent aller Credential-Stuffing-Angriffe ebenfalls.
- › Beide Angriffsarten wären mit blockierter Basic Authentication schlicht wirkungslos.
- › Das ist keine Prognose, sondern eine Auswertung der tatsächlichen Anmeldeversuche.

Wenn ein Konto auf diesem Weg fällt, merkt es zunächst niemand. Es gibt keine ungewöhnliche Anmeldung im Browser, keinen MFA-Hinweis, keine Meldung. Der Angreifer liest still mit, legt eine Weiterleitungsregel an und wartet auf die nächste Rechnung mit Bankverbindung. Was dann zu tun ist, steht in [Kompromittiertes Konto erkennen und aufräumen](#) — der bessere Weg ist allerdings, es gar nicht so weit kommen zu lassen.

Was Microsoft bereits abgeräumt hat

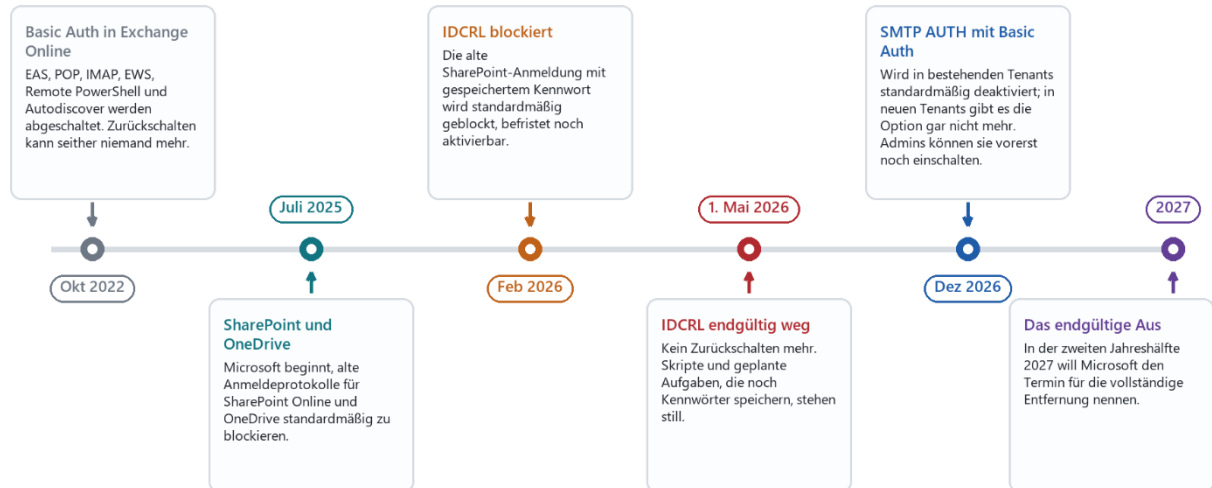
Ein großer Teil dieser Arbeit ist bereits erledigt, und zwar nicht freiwillig. Seit Oktober 2022 hat Microsoft Basic Authentication in Exchange Online für Exchange ActiveSync, POP, IMAP, Exchange Web Services, Remote PowerShell, das Offline-Adressbuch, Autodiscover sowie Outlook für Windows und Mac abgeschaltet. Seit dem 31. Dezember 2022 kann niemand mehr zurückschalten — weder du noch der Microsoft-Support. Wer damals nicht vorbereitet war, hat das Wochenende in Erinnerung.

Übrig geblieben ist genau eine Ausnahme, und die hat es in sich: SMTP AUTH. Weil daran die halbe Gerätewelt hängt, hat Microsoft diesen Fall mehrfach verschoben. Der aktuelle Plan wurde im Januar 2026 nachjustiert und sieht so aus: Bis Dezember 2026 ändert sich nichts. Zum

Jahresende 2026 wird SMTP AUTH mit Basic Authentication in bestehenden Tenants standardmäßig deaktiviert; Administratoren können es danach bei Bedarf noch einmal aktivieren. In Tenants, die nach diesem Zeitpunkt entstehen, gibt es die Option gar nicht mehr. Den Termin für die endgültige Entfernung will Microsoft in der zweiten Jahreshälfte 2027 nennen.

Was Microsoft schon abgeschaltet hat — und was noch kommt

Der Stichtag ist selten der Tag, an dem es wehtut. Wehtun tut der Tag danach.



Stand der Planung im September 2026. Termine dieser Art verschieben sich gelegentlich nach hinten — die Richtung bisher noch nie.

Skizze 2: Der Zeitstrahl der Abschaltungen. Die letzte Marke ist noch unbeschriftet — das macht sie nicht harmloser.

WARNUNG · Das Datum ist ein Angebot, kein Rettungsanker

Wer bis Dezember 2026 wartet, verhandelt am 2. Januar 2027 mit der Personalabteilung darüber, warum die Lohnabrechnung nicht verschickt wurde. Drei Gründe, früher anzufangen:

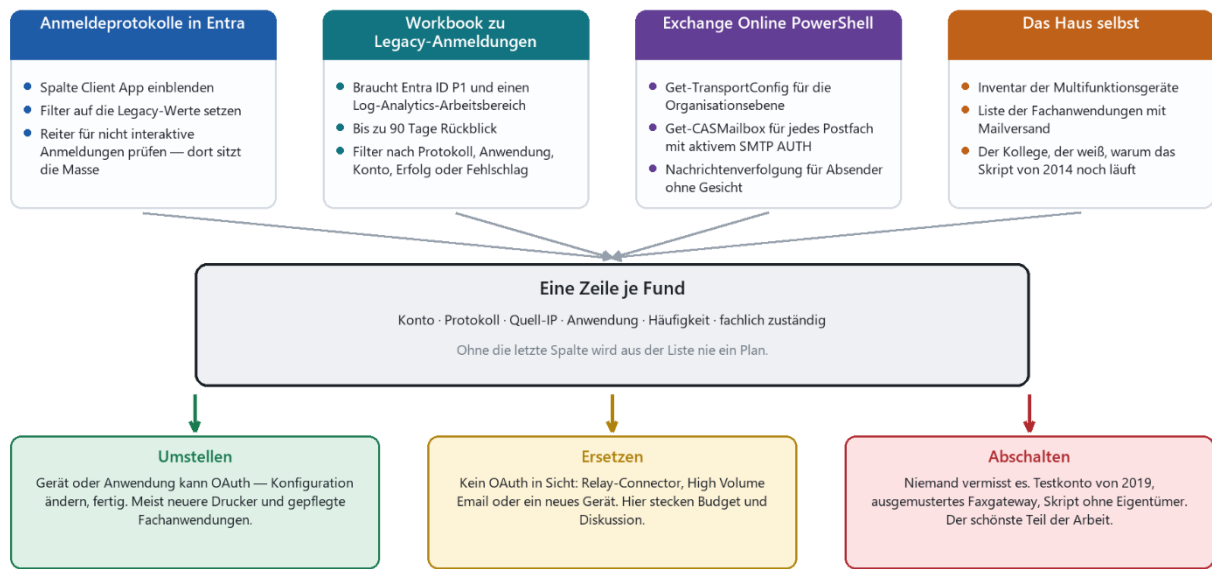
- › Die Umstellung eines Multifunktionsgeräts dauert zehn Minuten — die Klärung, wem es gehört und wer den Wartungsvertrag hat, gern drei Wochen.
- › Ältere Geräte können weder OAuth noch TLS 1.2. Dann steht keine Konfigurationsänderung an, sondern eine Beschaffung.
- › Die Abschaltung erfolgt nach Microsofts Zeitplan, nicht nach deinem Wartungsfenster.

Finden statt raten: die Bestandsaufnahme

Die Versuchung ist groß, die Blockade einfach scharf zu schalten und abzuwarten, wer sich meldet. Das ist tatsächlich eine Vorgehensweise — sie heißt nur nicht Projekt, sondern Störung. Solange du nicht weißt, was da eigentlich passiert, blockierst du möglicherweise die Alarmierung der Betriebstechnik. Also erst zählen.

Bestandsaufnahme: vier Quellen, eine Liste

Erst zählen, dann zumachen. Wer die Reihenfolge tauscht, lernt seine Fachbereiche von einer neuen Seite kennen.



Faustregel aus der Praxis: ein Drittel umstellen, ein Drittel ersetzen, ein Drittel darf einfach gehen.

Skizze 3: Vier Quellen ergeben eine Liste. Die letzte Spalte dieser Liste ist die wichtigste.

Die Anmeldeprotokolle richtig filtern

Der schnellste Einstieg liegt im Microsoft Entra Admin Center unter „Monitoring & Health“ in den Anmeldeprotokollen. Dafür genügt die Rolle „Reports Reader“. Zwei Handgriffe sind entscheidend und werden regelmäßig vergessen:

- Blende über „Columns“ die Spalte „Client App“ ein. Ohne sie siehst du zwar Anmeldungen, aber nicht das verwendete Verfahren.
- Setze über „Add filters“ den Filter „Client App“ und wähle sämtliche Legacy-Werte aus. Die Oberfläche gruppiert sie praktischerweise bereits als Legacy-Authentifizierungs-Clients.
- Und dann der Punkt, an dem die meisten Auswertungen zu optimistisch ausfallen: Wiederhole das Ganze im Reiter für nicht interaktive Benutzeranmeldungen. Genau dort sitzen Drucker, Skripte und Fachanwendungen — also praktisch alles, worum es hier geht.

In der Detailansicht eines Treffers steht unter „Basic Info“ das Feld „Client App“ mit dem konkreten Protokoll. Diese Werte sind deine Landkarte:

Wert im Protokoll	Bedeutung	Wer dahintersteckt (meistens)
Authenticated SMTP	SMTP AUTH auf Port 587, mit Kennwort angemeldet	Multifunktionsgeräte, Fachanwendungen, Monitoring-Systeme
Exchange ActiveSync	EAS ohne modernes Anmeldeverfahren	Alte Telefone, Tablets im Lager, zertifikatbasierte Profile
IMAP4 / POP3	Postfachabruf über die klassischen Abrufprotokolle	Archivlösungen, Ticketsysteme, Linux-Clients
Exchange Web Services	Programmierschnittstelle für Postfach- und Kalenderdaten	Raumbuchung, Signaturlösungen, CRM-Anbindungen
MAPI over HTTP / Outlook Anywhere	Outlook-Zugriff ohne moderne Authentifizierung	Sehr alte Outlook-Installationen, Terminalserver-Altlasten

Exchange Online PowerShell	Verwaltungszugriff per Remote PowerShell	Automatisierungsskripte, Partner- und Dienstleisterzugriffe
Other clients	Sammelposten für alles Übrige mit Basic Auth	Der spannendste Eintrag der Liste — hier lohnt das Nachsehen

Tabelle 2: Was die Werte in der Spalte „Client App“ bedeuten und worauf sie in der Praxis hindeuten.

Das Workbook für den Überblick über 90 Tage

Für die Auswertung über einen längeren Zeitraum gibt es im Entra Admin Center unter „Monitoring & Health“ das Workbook „Sign-ins using legacy authentication“ im Abschnitt „Usage“. Es beantwortet genau die Frage, um die es hier geht: Ist es sicher, Legacy Auth abzuschalten? Du wählst ein Protokoll, dann eine Anwendung, dann ein Konto — und siehst am Ende alle Legacy-Anmeldungen dieses Kontos. Interaktive und nicht interaktive Anmeldungen werden getrennt ausgewiesen, gefiltert wird nach Zeitraum bis 90 Tage, Konto, Anwendung sowie Erfolg oder Fehlschlag.

Zwei Voraussetzungen musst du kennen, bevor du im Portal suchst: Das Workbook braucht eine Entra-ID-P1-Lizenz und einen Log-Analytics-Arbeitsbereich, in den die Anmeldeprotokolle über eine Diagnoseeinstellung geschrieben werden. Wer diese Einstellung erst heute anlegt, hat morgen einen Tag Daten und nicht 90. Auch das ist ein Argument, früh anzufangen.

TIPP • Fehlschläge sind die interessantere Hälfte

Filtere nicht nur auf erfolgreiche Anmeldungen. Die fehlgeschlagenen Legacy-Anmeldungen erzählen zwei Geschichten gleichzeitig:

- › Häufen sich Fehlversuche über IMAP oder SMTP aus wechselnden Ländern auf viele verschiedene Konten, siehst du gerade einem Password Spray zu.
- › Häufen sie sich auf ein einziges Konto von einer festen internen Adresse, hat jemand das Kennwort im Drucker nach dem letzten Wechsel nicht nachgezogen.
- › Beides gehört auf die Liste — das eine als Vorfall, das andere als Aufgabe.

Die Exchange-Seite der Inventur

Die Anmeldeprotokolle zeigen dir, was tatsächlich passiert ist. Die Exchange-Konfiguration zeigt dir, was möglich wäre. Beides gehört zusammen, denn ein Postfach mit aktiviertem SMTP AUTH ist auch dann eine offene Tür, wenn sie gerade niemand benutzt. Die folgenden Zeilen liefern in wenigen Minuten den Bestand:

```
# Ist SMTP AUTH auf Organisationsebene noch erlaubt?
Get-TransportConfig | Format-List SmtClientAuthenticationDisabled

# Welche Postfächer haben SMTP AUTH ausdrücklich aktiviert?
$Users = Get-CASMailbox -ResultSize unlimited
$Users | Where-Object { $_.SmtClientAuthenticationDisabled -eq $false } |
    Select-Object DisplayName, PrimarySmtAddress

# Und welche folgen einfach der Organisationseinstellung?
$Users | Where-Object { $_.SmtClientAuthenticationDisabled -eq $null } |
    Measure-Object
```

Der dritte Block ist der unangenehme. Wenn die Organisationseinstellung SMTP AUTH erlaubt und die meisten Postfächer keinen eigenen Wert gesetzt haben, dann ist SMTP AUTH faktisch für alle offen — auch für die 400 Konten, die es nie gebraucht haben. Das ist der übliche Ausgangszustand in gewachsenen Umgebungen und gleichzeitig die schnellste Verbesserung, die du in diesem Projekt erzielen kannst.

Ergänzend hilft die Nachrichtenverfolgung im Exchange Admin Center. Suche nach Absendern, die keine Menschen sind: noreply@, scan@, alarm@, erp@. Jede dieser Adressen ist ein Eintrag auf deiner Liste. Wenn du das Thema gleich mit dem Blick auf den gesamten Tenant verbinden willst, findest du die Nachbarthemen in [Tenant-Härtung: die 20 wichtigsten Schrauben](#).

Die üblichen Verdächtigen

Nach zwei Wochen Messen hast du eine Liste. Erfahrungsgemäß stehen darauf immer dieselben vier Kategorien, unabhängig von Branche und Größe des Hauses. Es ist fast tröstlich.

Multifunktionsgeräte und Scanner

Der Dauerbrenner. „Scan to Mail“ ist die meistgenutzte Funktion nach dem Kopieren, und eingerichtet wurde sie vom Techniker des Händlers, der dafür ein Postfach und ein Kennwort brauchte. Ob dieses Kennwort noch gilt, weiß niemand — es funktioniert ja. Bei neueren Geräten lohnt der Blick in die Firmware-Beschreibung: Viele Hersteller unterstützen inzwischen OAuth für den Mailversand. Bei älteren Geräten wird es die Entscheidung zwischen Relay-Connector und Neubeschaffung.

Fachanwendungen, Alarmserver und Zeiterfassung

Das Warenwirtschaftssystem verschickt Auftragsbestätigungen, die Zeiterfassung meldet fehlende Buchungen, die Gebäudeleittechnik meldet den Ausfall der Lüftung, und der Backup-Server meldet seit elf Monaten jeden Morgen um 6:15 Uhr, dass alles in Ordnung ist. Diese Systeme sind selten dokumentiert, oft geschäftskritisch und praktisch immer außerhalb der Zuständigkeit der IT beschafft worden. Genau deshalb brauchst du in deiner Liste die Spalte „fachlich zuständig“ — nicht aus Bürokratie, sondern weil du jemanden brauchst, der die Umstellung testet und die Abschaltung verantwortet.

Skripte, Dienstkonten und der ehemalige Kollege

Der PowerShell-Einzeiler mit gespeichertem Kennwort im Klartext, der die Urlaubsliste verschickt. Die geplante Aufgabe auf dem Terminalserver, die niemand mehr anfassen möchte. Das Dienstkonto mit dem Namen „svc-mail-alt“, das seit 2019 kein Kennwort mehr geändert hat und, weil es Basic Auth benutzt, auch von keiner Richtlinie erfasst wird. Diese Fälle sind die undankbarsten, weil sie meist Restarbeit sind — und die dankbarsten, weil man ungefähr die Hälfte davon ersatzlos abschalten kann.

Fundstelle	Symptom im Protokoll	Erste Maßnahme
Multifunktionsgerät, Scanner	Authenticated SMTP von einer festen internen Adresse, regelmäßig zur Bürozeit	Firmware prüfen, OAuth aktivieren; sonst Relay-Connector oder High Volume Email

Fachanwendung mit Mailversand	Authenticated SMTP oder EWS, oft nachts in Blöcken	Hersteller nach OAuth-Unterstützung fragen, Versionsstand prüfen
Archiv- oder Ticketsystem	IMAP4 oder POP3, im Minutentakt	Auf OAuth oder Graph umstellen; Herstellerdokumentation verlangen
Skript oder geplante Aufgabe	Authenticated SMTP oder Exchange Online PowerShell von einem Serverkonto	Auf zertifikatbasierte Anmeldung oder verwaltete Identität umbauen
Altes Telefon oder Tablet	Exchange ActiveSync, unregelmäßig, meist ein einzelnes Konto	Outlook-App einrichten; wenn das Gerät zu alt ist, ist es zu alt
Herrenloses Dienstkonto	Anmeldeversuche ohne erkennbaren Zweck oder gar keine mehr	Eigentümer suchen, sonst deaktivieren und 30 Tage beobachten

Tabelle 3: Die vier Fundstellen, an denen du in fast jedem Haus fündig wirst.

WARNUNG • Der Klassiker mit Ansage

Wenn ein Multifunktionsgerät mit dem persönlichen Konto einer Person angemeldet ist, hast du drei Probleme auf einmal:

- › Das Kennwort dieser Person steht im Klartext in einer Weboberfläche, die jeder im Netz erreicht, der die IP-Adresse kennt.
- › Die Person kann ihr Kennwort nicht ändern, ohne das Scannen im Haus lahmzulegen — also ändert sie es nicht.
- › Verlässt die Person das Unternehmen, wird das Konto deaktiviert, und niemand kann mehr scannen. Diese Störung wird zuverlässig an einem Freitagnachmittag entdeckt.

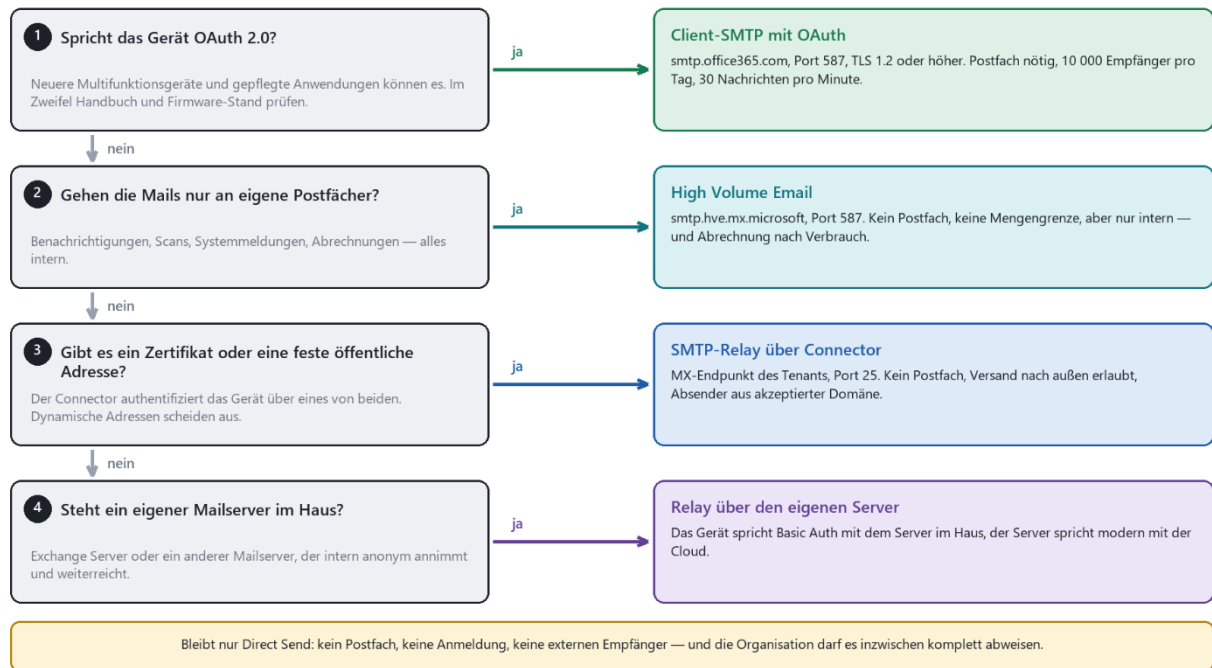
Diese Inventur ist die Sorte Arbeit, die kaum jemand nebenbei erledigt. Wenn du dabei Unterstützung brauchst — für die Auswertung, für die Gespräche mit den Fachbereichen oder für die Umbauten an Connector und Geräten —, findest du sie in der [Beratung zu Microsoft 365 Security](#).

Alternativen: OAuth, Relay-Connector, High Volume Email

Jetzt der konstruktive Teil. Für jeden Fund auf deiner Liste gibt es einen Weg, der ohne Basic Auth auskommt. Welcher es ist, hängt an vier Fragen — und die kannst du meist in zwei Minuten beantworten.

Welcher Versandweg passt zum Gerät?

Vier Fragen, vier Antworten — und ein Weg, den du nur im Notfall nimmst.



Skizze 4: Der Entscheidungsweg für Geräte und Anwendungen, die Mails verschicken.

Merkmal	Client-SMTP	SMTP-Relay	High Volume Email	Direct Send
Endpunkt	smtp.office365.com	MX-Endpunkt des Tenants	smtp.hve.mx.microsoft	MX-Endpunkt des Tenants
Port	587 (oder 25)	25	587	25
Anmeldung	Postfachkonto, OAuth empfohlen	Connector mit Zertifikat oder fester IP	HVE-Konto oder OAuth-Token	keine
TLS	erforderlich (1.2 oder 1.3)	optional, dringend empfohlen	erforderlich	optional
Postfach nötig	ja, lizenziert	nein	nein, keine Lizenz	nein
Externe Empfänger	ja	ja	nein	nein
Mengengrenzen	10 000 Empfänger pro Tag, 30 Nachrichten pro Minute	angemessene Grenzen des Dienstes	kein Empfänger- oder Nachrichtenlimit	Drosselung wie bei anonymer Post
Kosten	Postfachlizenz	keine zusätzlichen	Abrechnung nach Verbrauch	keine
Typischer Einsatz	Gerät mit OAuth, wenig Volumen	Gerät ohne OAuth, Versand nach außen	Massenversand an eigene Postfächer	Notlösung, möglichst gar nicht

Tabelle 4: Die vier Versandwege für Geräte und Anwendungen im Vergleich.

OAuth für Geräte und Anwendungen

Der saubere Weg. Exchange Online unterstützt OAuth 2.0 für IMAP, POP und SMTP AUTH seit 2020. Das Gerät oder die Anwendung authentifiziert sich dann nicht mehr mit einem Kennwort, sondern mit einem Token, das eine begrenzte Lebensdauer hat und nur für die registrierte Anwendung und die freigegebene Berechtigung gilt. Ein abgegriffenes Token ist damit deutlich weniger wert als ein abgegriffenes Kennwort.

Dazu registrierst du eine Anwendung in Entra ID, vergibst die notwendigen Berechtigungen und hinterlegst die Zugangsdaten im Gerät. Zwei Dinge sind dabei wichtig: Vergib nur die Berechtigungen, die tatsächlich gebraucht werden — für einen Scanner ist das der Versand, nicht der Vollzugriff auf alle Postfächer. Und behandle diese Registrierungen wie Konten, inklusive Ablaufdatum und Verantwortlichkeit. Wie du das systematisch aufsetzt, steht in [App-Registrierungen und Consent-Governance](#).

SMTP-Relay über einen eigenen Connector

Wenn das Gerät kein OAuth kann, aber trotzdem nach außen senden muss, ist der eingehende Connector der Standardweg. Das Gerät sendet auf Port 25 an den MX-Endpunkt deines Tenants — also an etwas in der Form contoso-com.mail.protection.outlook.com —, und Exchange Online erkennt es nicht am Kennwort, sondern am Zertifikat oder an der festen öffentlichen IP-Adresse.

Microsoft empfiehlt ausdrücklich die Variante mit Zertifikat: Im Feld „Subject“ oder „Subject Alternative Name“ muss eine akzeptierte Domäne deines Tenants stehen, im Connector trägst du dieselbe Domäne ein. Die IP-Variante funktioniert ebenfalls, verlangt aber eine statische Adresse, die nicht mit anderen Organisationen geteilt wird — dynamische Adressen sind nicht zulässig. Ein Vorteil dieses Wegs: Das Gerät braucht kein Postfach und keine Lizenz und darf mit jeder Adresse aus einer akzeptierten Domäne senden, auch mit einer, die gar kein Postfach hat.

Ein Nachteil, den du einplanen solltest: Post über den Relay-Weg durchläuft die Spamfilterung wie normale Post. Ohne sauberen SPF-Eintrag für die sendende Adresse landet die Auftragsbestätigung im Junk-Ordner des Kunden. Wie du Absenderauthentifizierung vollständig aufsetzt, steht in [SPF, DKIM, DMARC für Exchange Online](#).

Und noch eine Randnotiz für alle, die den Relay lieber im eigenen Haus betreiben: Windows Server 2022 ist die letzte Version, die das SMTP-Server-Feature der IIS-Rolle enthält. Für die Weiterleitung an Microsoft 365 war es ohnehin nie unterstützt. Wer diesen Weg gehen will, braucht einen unterstützten Exchange Server oder einen anderen gepflegten Mailserver.

High Volume Email für den internen Massenversand

Der Neuzugang unter den Versandwegen und für viele Häuser die eleganteste Lösung. High Volume Email ist genau für den Fall gebaut, um den es hier meistens geht: Anwendungen und Geräte, die viele Nachrichten an die eigene Belegschaft schicken. Lohnabrechnungen, Systemmeldungen, Scans, Benachrichtigungen aus Fachanwendungen.

Dafür legst du im Exchange Admin Center unter „Mail flow“ ein HVE-Konto an. Das ist kein Postfach und braucht keine Lizenz, sondern ein reines Absenderobjekt. Es kann selbst keine Post empfangen; wenn Antworten möglich sein sollen, hinterlegst du eine Antwortadresse. Die

Anmeldung erfolgt wahlweise mit Kontoanmeldedaten oder — empfohlen — mit einem OAuth-Token.

Grenze	Wert	Bedeutung für die Praxis
Empfängerrate	keine Begrenzung	Der Grund, warum es diesen Dienst gibt
Nachrichtenrate	keine Begrenzung	Auch Lastspitzen zum Monatsende sind unkritisch
HVE-Konten je Tenant	bis zu 100	Reicht, um je Anwendung ein eigenes Konto zu vergeben — genau so ist es gedacht
Empfänger je Nachricht	bis zu 50	Größere Verteiler über Verteilerlisten oder in Blöcken lösen
Nachrichtengröße	10 MB	Für Scans mit hoher Auflösung gelegentlich knapp
Empfängerkreis	nur intern	Sobald ein einziger externer Empfänger dabei ist, brauchst du einen anderen Weg
Abrechnung	nutzungsabhängig über eine Azure-Zahlungsmethode	Ohne zugewiesene Abrechnungsrichtlinie versendet das Konto nichts

Tabelle 5: Die Grenzen von High Volume Email, die du vor der Umstellung kennen musst.

Die Kosten sind überschaubar und werden nach zugestellten Empfängern abgerechnet — rund 42 US-Dollar je Million Empfänger. Für ein mittelständisches Haus mit ein paar zehntausend internen Systemnachrichten pro Monat bewegt sich das im Bereich von Rundungsfehlern. Wichtig ist nur, die Abrechnung überhaupt einzurichten: Ein HVE-Konto ohne gültige Abrechnungsrichtlinie steht auf „nicht aktiv“ und verschickt gar nichts.

WICHTIG · High Volume Email hat einen eigenen Eingang

Ein Detail, das in Sicherheitskonzepten regelmäßig übersehen wird: HVE-Konten können sich auch dann anmelden, wenn SMTP AUTH auf Organisationsebene deaktiviert ist. Der Dienst benutzt einen eigenen Endpunkt.

- › Das ist praktisch, weil du SMTP AUTH global abschalten und trotzdem Geräte versorgen kannst.
- › Es bedeutet aber auch, dass HVE-Konten mit Basic Auth eine eigene Tür sind, die du bewusst schließen musst.
- › Vergib deshalb OAuth statt Kennwort und begrenze den Zugriff auf die dafür zugelassenen Anwendungen.
- › Sind Security Defaults aktiv, ist Basic Auth für HVE ohnehin nicht verfügbar — dann bleibt nur OAuth.

Direct Send: der Weg, den du eher zumachst

Direct Send ist die Variante ganz ohne Anmeldung: Das Gerät sendet wie ein fremder Mailserver aus dem Internet an deinen MX-Endpunkt. Das funktioniert, hat aber Nebenwirkungen. Externe Empfänger sind nicht möglich, die Post wird wie anonyme Internetpost geprüft, und die Absenderadresse muss lediglich zu einer akzeptierten Domäne gehören — mehr nicht.

Genau dieses „mehr nicht“ ist im Jahr 2025 zum Problem geworden: Angreifer haben Direct Send genutzt, um Phishing-Mails mit hauseigenen Absenderadressen an die eigene Belegschaft zuzustellen, ohne sich jemals anmelden zu müssen. Microsoft hat daraufhin einen Schalter nachgeliefert, mit dem die Organisation solche Zustellungen ablehnt. Der Standardwert ist noch „aus“, das soll sich künftig ändern. Warte nicht darauf:

```
# Direct Send für die Organisation abweisen
Set-OrganizationConfig -RejectDirectSend $true

# Aktuellen Stand prüfen
Get-OrganizationConfig | Format-List RejectDirectSend
```

Abgewiesene Versuche quittiert der Dienst mit einer eindeutigen Meldung, die mit „550 5.7.68“ beginnt — praktisch für die Fehlersuche, wenn sich doch noch ein vergessenes Gerät meldet. Prüfe vor dem Umlegen des Schalters die Nachrichtenverfolgung auf unauthentifizierte interne Zustellungen. Wie du solche Vorfälle sonst behandelst, beschreibt [Phishing-Vorfall: die ersten 60 Minuten](#).

Zumachen: Conditional Access, Exchange-Schalter, Baseline Security Mode

Wenn die Liste abgearbeitet ist, kommt der Teil, für den du das alles gemacht hast. Und weil eine einzelne Maßnahme nie alles abdeckt, arbeitest du hier mit drei Schichten, die sich gegenseitig absichern.

Schicht 1: die Conditional-Access-Richtlinie

Die Richtlinie zum Blockieren von Legacy Authentication ist eine der wenigen, die man ohne große Diskussion empfehlen kann. Sie ist in wenigen Minuten gebaut — Microsoft liefert sie auch als Vorlage mit:

1. Benutzer: alle Benutzer einschließen. Ausschließen: die Break-Glass-Konten und, für den Übergang, eine benannte Ausnahmegruppe.
2. Zielressourcen: alle Ressourcen beziehungsweise alle Cloud-Apps.
3. Bedingungen, Client-Apps: „Configure“ auf „Ja“, dann ausschließlich die beiden Häkchen „Exchange ActiveSync clients“ und „Other clients“ setzen. Die modernen Client-Typen bleiben unangetastet.
4. Zugriffssteuerung, Gewähren: „Zugriff blockieren“.
5. Richtlinie zunächst auf „Nur Bericht“ stellen und ein bis zwei Wochen laufen lassen.
6. Auswertung prüfen, dann auf „Ein“ schalten — erst für eine Pilotgruppe, dann für alle.

Hinter „Other clients“ verbirgt sich der ganze Zoo: SMTP, Autodiscover, Exchange Online PowerShell, EWS, IMAP4, MAPI over HTTP, das Offline-Adressbuch, Outlook Anywhere, POP3 und die Reporting-Webdienste. Deshalb genügen diese zwei Häkchen — mehr brauchst du nicht anzuklicken, und mehr solltest du auch nicht.

Der Nur-Bericht-Modus ist kein optionaler Zwischenschritt, sondern der eigentliche Kern der Übung. Er zeigt dir für jede reale Anmeldung, ob die Richtlinie sie blockiert hätte — ohne dass jemand ausgesperrt wird. Wie du solche Richtlinien sauber aufbaust, benennst und ausrollst, ohne dass daraus ein Flickenteppich wird, steht in [Conditional Access: Baselines, die nicht nerven](#). Und wie die Notfallkonten aussehen, die du hier ausnimmst, in [Break-Glass-Konten anlegen und überwachen](#).

WARNUNG · Was diese Richtlinie nicht kann

Conditional Access ist mächtig, aber sie ist kein Türsteher vor der Tür, sondern hinter ihr. Drei

Grenzen, die du kennen musst:

- › Die Richtlinie wird erst nach dem ersten Faktor ausgewertet. Der Angreifer erfährt also weiterhin, ob ein Kennwort korrekt war — er kann es nur nicht verwenden.
- › Aufrufe von Dienstprinzipalen werden von Richtlinien, die auf Benutzer angewendet werden, gar nicht erfasst. Dafür gibt es Conditional Access für Workload-Identitäten.
- › Auch zertifikatbasierte Authentifizierung für Exchange ActiveSync gilt als Legacy und wird von dieser Richtlinie blockiert. Das trifft gelegentlich verwaltete Tablets, die über Profile eingerichtet wurden.

Schicht 2: die Schalter in Exchange Online

Conditional Access blockiert die Anmeldung. Die Exchange-Schalter sorgen dafür, dass es gar nicht erst einen Dienst gibt, an dem sich jemand anmelden könnte. Das ist Tiefenverteidigung im Wortsinn — und es hilft in dem Moment, in dem eine CA-Richtlinie versehentlich gelöscht oder umkonfiguriert wird.

```
# SMTP AUTH organisationsweit abschalten
Set-TransportConfig -SmtpClientAuthenticationDisabled $true

# ... und ausschließlich dort wieder freigeben, wo es gebraucht wird
Set-CASMailbox -Identity scanner-empfang@contoso.de `
  -SmtpClientAuthenticationDisabled $false

# Ein Postfach wieder der Organisationseinstellung unterstellen
Set-CASMailbox -Identity altsystem@contoso.de `
  -SmtpClientAuthenticationDisabled $null
```

Die Reihenfolge ist entscheidend: erst global abschalten, dann gezielt einzelne Postfächer freigeben. Die Postfacheinstellung hat Vorrang vor der Organisationseinstellung. Für Tenants, die nach Januar 2020 entstanden sind, ist SMTP AUTH übrigens von Haus aus deaktiviert — dort besteht die Aufgabe eher darin, es nicht versehentlich einzuschalten.

Für Häuser ohne Lizenzen für Conditional Access sind die Security Defaults die passende Antwort: Sie blockieren Legacy Auth tenantweit und schalten dabei auch SMTP AUTH ab. Weniger fein steuerbar, aber wirksam — die Abwägung zwischen beiden Wegen steht in [Security Defaults oder Conditional Access?](#).

Schicht 3: Baseline Security Mode im Admin Center

Seit einiger Zeit fasst Microsoft eine Reihe dieser Einstellungen im Microsoft 365 Admin Center unter „Baseline Security Mode“ zusammen, zu finden unter „Org Settings“ im Reiter „Security and Privacy“. Interessant sind daran zwei Dinge. Erstens gibt es dort Schalter, die es früher nur in PowerShell gab — etwa das Blockieren alter Anmeldeverfahren für SharePoint und OneDrive oder das organisationsweite Abschalten der Exchange Web Services. Zweitens, und das ist der eigentliche Gewinn, gibt es je Einstellung einen Wirkungsbericht.

Das Verfahren ist entsprechend simpel: Bericht laufen lassen, und wenn er null Betroffene meldet, den Schalter umlegen. Meldet er Abhängigkeiten, bleibt der Schalter aus, bis diese Abhängigkeiten abgeräumt sind. Bei den Exchange Web Services lohnt der Blick besonders: Sie werden auch von Office-Add-Ins und einigen Erweiterungen benutzt, außerdem hängen daran je nach Umgebung

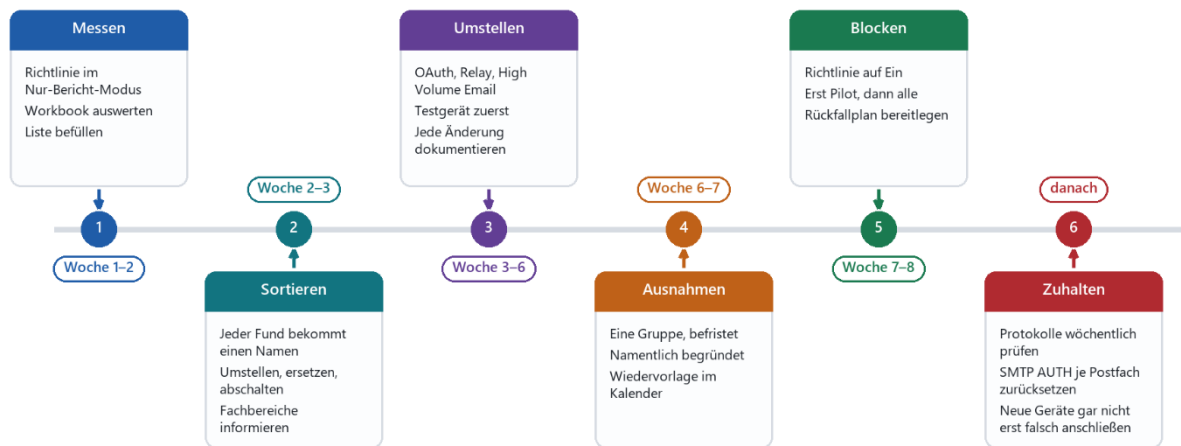
die organisationsübergreifende Frei-/Belegt-Zeit, MailTips und bestimmte Power-Query-Verbindungen. Abschalten ja — aber mit Bericht in der Hand.

Der Fahrplan

Zum Schluss die Reihenfolge, die sich in der Praxis bewährt hat. Acht Wochen sind realistisch, wenn niemand dazwischenfunkt; planerisch solltest du eher mit zwölf rechnen, weil immer jemand dazwischenfunkt.

Sechs Wellen bis zum harten Block

Acht bis zwölf Wochen, wenn niemand dazwischenfunkt. Zwölf bis zwanzig, wenn doch — also immer.



Die einzige Welle, die man auslassen kann, ist die erste. Man merkt es dann in Welle fünf.

Skizze 5: Sechs Wellen. Die sechste hat kein Ende — das ist keine Nachlässigkeit im Plan, sondern der Punkt.

TIPP • Die Ausnahmegruppe mit eingebautem Ablaufdatum

Du wirst Ausnahmen brauchen. Der Unterschied zwischen einer sauberen Umstellung und einer, die nie fertig wird, liegt in der Art, wie du sie verwaltest:

- › Genau eine Gruppe, nicht drei. Der Name sagt, worum es geht: „CA-Ausnahme-LegacyAuth-befristet“.
- › Jeder Eintrag hat einen Namen, einen Grund und ein Datum — notiert in der Gruppenbeschreibung oder im Ticket.
- › Alle vier Wochen Wiedervorlage. Ohne Wiedervorlage ist die Ausnahme keine Ausnahme, sondern der neue Normalzustand.
- › Wer die Gruppe verlässt, verlässt sie endgültig: Postfach auf SMTP AUTH prüfen und den Schalter mit zurückdrehen.

Ein Wort zur Kommunikation, weil sie in Projekten dieser Art über Erfolg und Misserfolg entscheidet: Die Ankündigung „wir schalten unsichere Anmeldeverfahren ab“ erzeugt Widerstand. Die Ankündigung „ab dem 15. Oktober scannt das Gerät im dritten Stock über einen neuen Weg, ihr müsst nichts tun, bei Problemen ruft ihr diese Nummer an“ erzeugt keinen. Und wenn du dabei Anmeldedaten auswertest, kläre früh, was davon mitbestimmungspflichtig ist — die Kriterien dafür stehen in [Security-Monitoring und Betriebsrat: was mitbestimmungspflichtig ist](#).

Häufige Fragen

Ist Legacy Auth nicht ohnehin schon überall abgeschaltet?

In Exchange Online zum größten Teil ja: EAS, POP, IMAP, EWS, Remote PowerShell, Adressbuch, Autodiscover und die Outlook-Protokolle wurden seit Oktober 2022 zwangsweise geschlossen und lassen sich nicht mehr reaktivieren. Offen ist SMTP AUTH, und offen sind alle Dienste außerhalb von Exchange. Deshalb reicht es nicht, sich auf die Abschaltung durch Microsoft zu verlassen: Deine CA-Richtlinie deckt auch das ab, was Microsoft noch nicht angefasst hat.

Wir haben noch Geräte, die kein OAuth können. Was jetzt?

Dann fällst du auf den Relay-Connector oder auf High Volume Email zurück, je nachdem, ob nach außen gesendet werden muss. Beide Wege kommen ohne Basic Auth des Geräts aus. Wenn das Gerät nicht einmal TLS 1.2 beherrscht, ist die Umstellung keine Konfigurationsfrage mehr: Dann sendet es über einen Mailserver im eigenen Haus — oder es wird ersetzt.

Blockiert die Richtlinie auch unsere Dienstkonten?

Nur teilweise, und das ist eine der häufigsten Fehlannahmen. Richtlinien, die auf Benutzer angewendet werden, greifen nicht bei Aufrufen von Dienstprinzipalen. Wenn eine Anwendung mit eigener Identität arbeitet, brauchst du Conditional Access für Workload-Identitäten. Dienstkonten, die schlicht Benutzerkonten sind, werden dagegen ganz normal erfasst — und genau die stehen meist in den Skripten.

Was passiert mit den Nutzern, wenn ich die Richtlinie scharf schalte?

Bei Exchange ActiveSync bekommt die betroffene Person eine einzelne Quarantäne-Mail mit Erklärung und Hinweisen. Bei den übrigen Protokollen kommt schlicht eine Anmeldefehlermeldung des jeweiligen Clients, die selten hilfreich ist. Deshalb der Nur-Bericht-Modus vorher und deshalb die Ankündigung mit Datum, Ansprechpartner und Telefonnummer.

Reicht MFA nicht aus, wenn wir es überall erzwingen?

Nein — das ist der Kern dieses Themas. MFA wird über Protokolle erzwungen, die eine Rückfrage kennen. Ein Legacy-Protokoll kennt keine. Eine MFA-Pflicht ohne Legacy-Blockade ist wie eine Sicherheitstür neben einem offenen Fenster. Wie du beides zusammenbringst, steht in [MFA in Microsoft 365 richtig einführen](#) — und wenn du danach ganz vom Kennwort weg willst, in [Passwordless: FIDO2 und Passkeys in der Praxis](#).

Wie hängen SharePoint und OneDrive mit dieser Sache zusammen?

Über dieselbe Logik, nur mit eigenen Protokollen. Microsoft blockiert seit Juli 2025 alte Anmeldeverfahren für SharePoint Online und OneDrive standardmäßig; das ältere Verfahren mit gespeicherten Kennwörtern wurde im Februar 2026 standardmäßig geblockt und zum 1. Mai 2026 endgültig entfernt. Betroffen sind vor allem Skripte, geplante Aufgaben, Datenaktualisierungen und Drittwerkzeuge, die Benutzername und Kennwort speichern. Mehr zur Absicherung dieser Dienste in [MFA für SharePoint Online erzwingen](#).

Wie merken wir, dass sich wieder etwas eingeschlichen hat?

Über die Blockade selbst. Sobald die Richtlinie aktiv ist, erscheint jeder neue Legacy-Versuch als blockierte Anmeldung im Protokoll — inklusive Konto, Protokoll und Quelladresse. Baue dir eine wöchentliche Auswertung oder eine Benachrichtigung darauf; wie du das aufsetzt, ohne im Meldungsrauschen zu ertrinken, steht in [Alert Policies und Benachrichtigungen richtig aufsetzen](#).

Bringt uns das auch Punkte im Secure Score?

Ja, das Blockieren von Legacy Authentication ist dort eine der höher gewichteten Empfehlungen. Der Punktestand ist aber der Nebeneffekt, nicht das Ziel — die Maßnahme lohnt sich, weil sie die am häufigsten genutzte Angriffsroute schließt. Wie man diese Zahl sinnvoll liest, steht in [Secure Score: sinnvoll nutzen statt Punktejagd](#).

Fazit

Legacy Authentication abzuschalten ist keine besonders anspruchsvolle technische Aufgabe. Die Richtlinie ist in zehn Minuten gebaut, die PowerShell-Zeilen sind kurz, und die Alternativen für Geräte sind dokumentiert und erprobt. Anspruchsvoll ist etwas anderes: herauszufinden, was im Haus eigentlich läuft, für jeden Fund einen Verantwortlichen zu finden, und die Umstellung so zu planen, dass am Montagmorgen niemand vor einem stummen Scanner steht.

Deshalb lautet die Reihenfolge: messen, sortieren, umstellen, befristet ausnehmen, blockieren, zuhalten. Wer bei Schritt fünf anfängt, lernt seine Fachbereiche von einer neuen Seite kennen — und verliert das Vertrauen, das er für die nächsten Maßnahmen braucht.

Der Zeitdruck kommt diesmal nicht aus dem Sicherheitskonzept, sondern aus dem Kalender. Ende 2026 deaktiviert Microsoft SMTP AUTH mit Basic Authentication in bestehenden Tenants standardmäßig, und das endgültige Aus wird 2027 terminiert. Bis dahin ist reichlich Zeit — vorausgesetzt, man fängt an, solange sie noch reichlich ist. Und die Kollegin aus der Buchhaltung kann endlich ihr Kennwort ändern.

Weiter im Handlungsfeld Identitäten und Tenant-Härtung

- › [Conditional Access: Baselines, die nicht nerven](#) — der Rahmen, in den die Legacy-Blockade gehört
- › [Tenant-Härtung: die 20 wichtigsten Schrauben](#) — die übrigen Schalter, die zum selben Bild gehören
- › [Gastzugriff und externe Freigaben härten](#) — die zweite große Tür neben den Protokollen
- › [Microsoft 365 Security Beratung](#) — Inventur, Umstellung und Rollout im Projekt
- › [Schulung Microsoft 365 Security](#) — wenn das Team die Zusammenhänge selbst beherrschen soll
- › [Dossier: TerminalFix und der Berlin-Hack](#) — wie so ein Angriff in der Praxis abläuft