

Zero Trust im Mittelstand: pragmatisch statt dogmatisch

Es gibt einen sicheren Weg, ein Zero-Trust-Projekt im Mittelstand zum Scheitern zu bringen: Man beginnt mit einer Folie. Auf der Folie sind konzentrische Kreise, in der Mitte steht „Daten“, außen herum stehen sechs Säulen, und irgendwo unten läuft ein Pfeil im Kreis, der „Continuous Improvement“ heißt. Die Folie ist nicht falsch. Sie ist nur vollkommen wirkungslos, weil sie keiner einzigen Person sagt, was sie am Montagmorgen anklicken soll.

Zero Trust hat ein Übersetzungsproblem. Das Konzept ist gut, die Prinzipien sind richtig, und die Bedrohungslage gibt beiden recht. Aber zwischen dem Prinzip „explizit verifizieren“ und der Frage, ob deine Buchhaltung morgen noch an ihre DATEV-Schnittstelle kommt, liegt eine Lücke, die keine Beratungsfolie schließt. Genau diese Lücke ist das Thema dieses Beitrags.

Die Ausgangslage, die ich in mittelständischen Häusern regelmäßig antreffe: Microsoft 365 E3 ist lizenziert, weil es zum Office-Paket dazugehörte. Es gibt vier Conditional-Access-Richtlinien, von denen zwei auf Report-only stehen. Elf Personen sind Global Administrator, davon sind drei nicht mehr im Haus. Und es gibt eine Excel-Tabelle mit Ausnahmen, deren letzte Änderung aus dem Jahr 2022 stammt. Das ist kein Skandal, sondern der Normalzustand.

Dieser Beitrag übersetzt die drei Zero-Trust-Prinzipien in konkrete Microsoft-365-Funktionen und beschreibt, was du damit in sechs Monaten tatsächlich erreichst — ohne Zusatzlizenz, ohne Reifegradmodell und ohne einen einzigen Workshop, dessen Ergebnis ein weiterer Workshop ist. Er gehört in die Reihe [Microsoft 365 Security](#), in der die einzelnen Bausteine einer Microsoft-365-Absicherung zusammenlaufen.

FAKTEN — Die drei Prinzipien, wie Microsoft sie definiert

Explizit verifizieren: Jede Zugriffsanfrage wird anhand aller verfügbaren Signale authentifiziert und autorisiert — nicht einmal beim Eintritt, sondern fortlaufend.

Minimale Rechte: Personen und Arbeitslasten bekommen nur den Zugriff, den sie brauchen, und nur für die kürzestmögliche Zeit.

Kompromittierung annehmen: Die Kontrollen werden so entworfen, dass sie auch dann noch wirken, wenn ein Angreifer bereits innerhalb der Umgebung arbeitet.

Microsoft hat die Zero-Trust-Leitartikel im Mai 2026 überarbeitet und das Adoptionsmodell auf drei Ebenen gestellt: Geschäftsszenarien, Sicherheitsdisziplinen und Technologiesäulen. Der Mittelstand braucht davon vor allem die dritte Ebene.

Was Zero Trust ist — und was in Präsentationen daraus wird

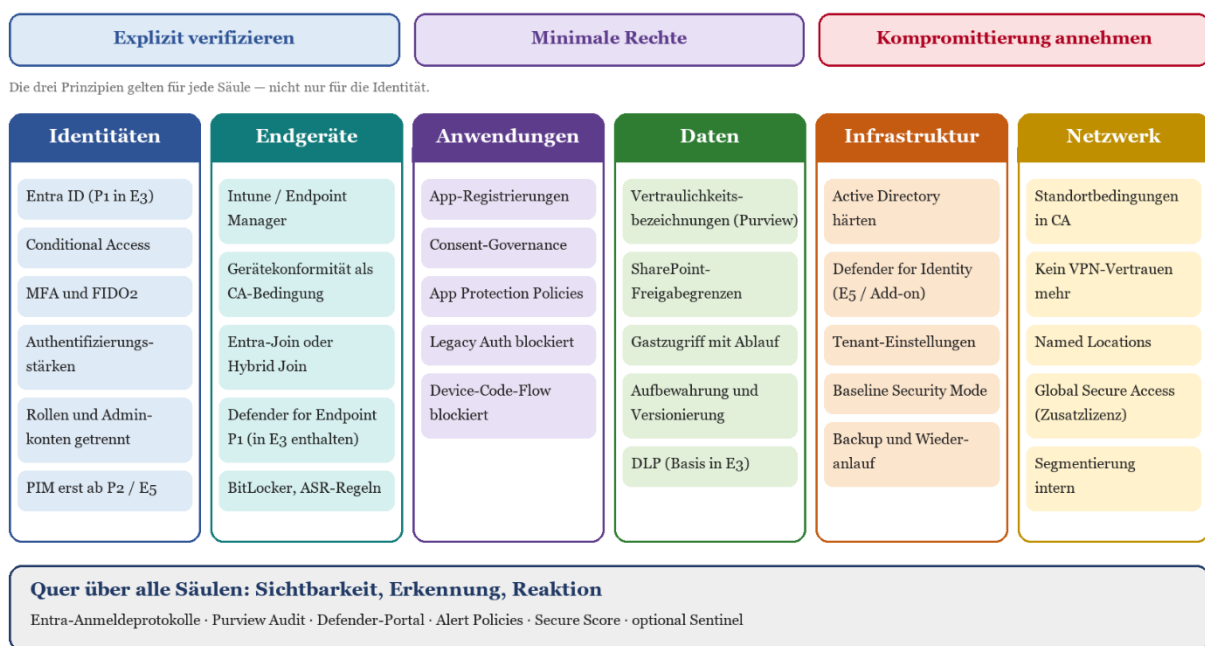
Der Kern von Zero Trust passt in einen Halbsatz: niemals vertrauen, immer prüfen. Das eigentliche Argument dahinter ist historisch. Das alte Modell ging davon aus, dass es ein Innen und ein Außen gibt, dass das Innen sicherer ist und dass Sicherheit die Aufgabe einer Abteilung ist. Alle drei Annahmen sind heute falsch. Moderne Angriffe laufen über Identitäten, Phishing und übernommene Sitzungen — sie interessieren sich nicht dafür, wo im Netz du gerade sitzt.

Warum die Säulen-Darstellung trotzdem nützlich ist

Ich schimpfe gern über Folien mit Säulen, aber die Struktur selbst hat einen praktischen Wert: Sie zwingt dich, jede Zone deiner Umgebung einmal anzuschauen und ehrlich aufzuschreiben, womit

du sie eigentlich absicherst. In dem Moment, in dem in einer Säule „nichts“ steht, hast du eine Erkenntnis — und die ist mehr wert als jedes Reifegraddiagramm.

Die Zero-Trust-Säulen und was Microsoft 365 dafür mitbringt



Die unbequeme Kurzfassung: Mit Microsoft 365 E3 deckst du die linken vier Säulen solide ab.

Die beiden rechten brauchen entweder Zusatzlizenzen oder Handarbeit — oder du lässt sie bewusst offen und schreibst das auf.

boddenberg.de

Skizze 1: Die Zero-Trust-Säulen mit den Microsoft-365-Funktionen, die tatsächlich dahinterstehen. Rechts wird es dünn — und das ist eine Aussage, keine Lücke im Bild.

Die drei Dogmen, die du getrost ignorieren darfst

Erstens: „Zero Trust ist ein Produkt.“ Nein. Es gibt kein Kästchen, das man kauft und einschaltet. Wer dir etwas anderes erzählt, verkauft dir gerade etwas.

Zweitens: „Zero Trust bedeutet, dass wir das VPN abschaffen.“ Auch nein — jedenfalls nicht als erster Schritt. Netzwerksegmentierung ist die teuerste und langsamste Säule. Sie ist zugleich die, in der du am wenigsten Angriffe verhinderst, solange elf Personen Global Administrator sind.

Drittens: „Zero Trust braucht E5.“ Das ist die hartnäckigste Behauptung, und sie ist höchstens zu einem Drittel wahr. Microsoft 365 E3 enthält Microsoft Entra ID P1 und damit Conditional Access, Authentifizierungsstärken, Gerätekonformität als Bedingung und Administrative Units. Was E3 nicht enthält, ist Entra ID P2 — also Privileged Identity Management, Identity Protection mit Risikosignalen, Zugriffsüberprüfungen und Entitlement Management. Das ist ein echter Unterschied, aber er betrifft die Kür, nicht die Pflicht.

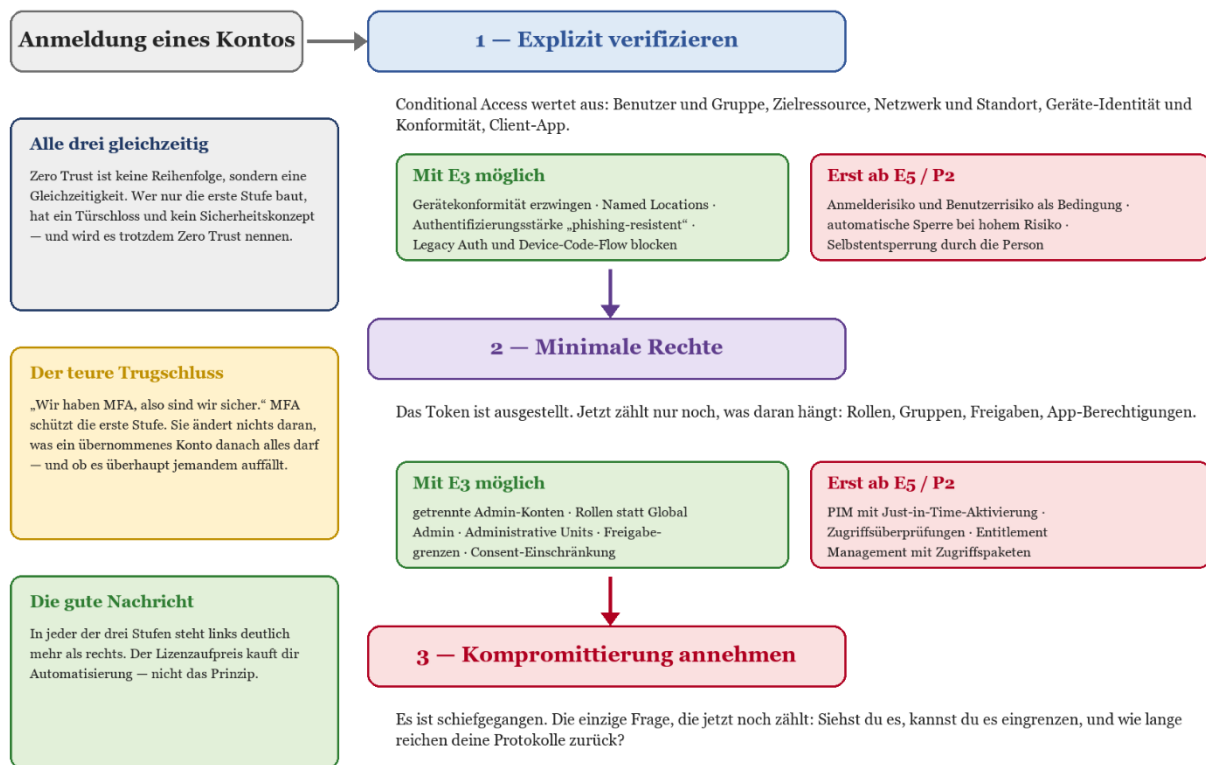
WICHTIG — Der Satz, der Zero-Trust-Projekte rettet

Zero Trust ist kein Zustand, den man erreicht, sondern eine Reihenfolge von Entscheidungen. Du wirst nie „fertig“ sein. Du kannst aber nach sechs Monaten sagen: Diese fünf Dinge sind jetzt anders, und hier ist der Nachweis. Das reicht für die Geschäftsführung, für den Versicherer und für jeden Auditor, der nicht nach Punkten, sondern nach Wirksamkeit fragt.

Prinzip 1 in der Praxis: explizit verifizieren mit Conditional Access

Conditional Access ist die Stelle, an der Zero Trust in Microsoft 365 aufhört, ein Konzept zu sein, und anfängt, eine Konfiguration zu sein. Jede Anmeldung wird gegen einen Satz von Bedingungen geprüft, und erst danach entscheidet sich, ob ein Token ausgestellt wird, mit welchen Auflagen und für wie lange. Das ist die technische Übersetzung von „explizit verifizieren“ — es gibt keine zweite.

Wo die drei Prinzipien im Tagesgeschäft tatsächlich zuschlagen



boddenberg.de

Skizze 2: Dieselbe Anmeldung, dreimal betrachtet. Links, was in Microsoft 365 E3 geht, rechts, wofür du E5 oder Entra ID P2 brauchst.

Die Signale, die du in E3 schon hast

Conditional Access wertet bei jeder Anmeldung eine ganze Reihe von Signalen aus: wer sich anmeldet, auf welche Ressource, aus welchem Netz, mit welchem Gerät und mit welcher Client-Anwendung. In E3 sind davon alle bis auf eines verfügbar — es fehlt nur das Risikosignal aus Entra ID Protection. Praktisch heißt das: Du kannst Gerätekonformität erzwingen, benannte Standorte definieren, Legacy Authentication blockieren und für administrative Rollen eine phishing-resistente Anmeldung verlangen. Du kannst nur nicht sagen: „Wenn diese Anmeldung ungewöhnlich aussieht, dann ...“.

Signal	In Microsoft 365 E3	Was du damit baust
Benutzer, Gruppe, Rolle	Ja (Entra ID P1)	Getrennte Richtlinien für Belegschaft, Administration, Dienstkonten und Gäste
Zielressource	Ja	Strengere Regeln für Admin-Portale und für die Azure-Ressourcenverwaltung

Netzwerk und Standort	Ja	Benannte Standorte, Ausschluss unmöglicher Regionen, abgestufte Sitzungsdauer
Geräte-Identität und Konformität	Ja (mit Intune)	Zugriff auf Unternehmensdaten nur von verwalteten, konformen Geräten
Client-Anwendung	Ja	Legacy Authentication und Device-Code-Flow gezielt blockieren
Authentifizierungsstärke	Ja	Phishing-resistente Anmeldung für alle administrativen Rollen erzwingen
Anmelderisiko und Benutzerrisiko	Nein (Entra ID P2)	Risikobasierte Richtlinien, automatische Sperre und Selbstentsperrung
Sitzungssteuerung über Cloud Apps	Eingeschränkt	Vollständige Sitzungskontrolle erst mit Defender for Cloud Apps

Tabelle 1: Welche Conditional-Access-Signale in E3 verfügbar sind — und was daraus praktisch folgt.

Wer dabei bei null anfängt, sollte nicht mit einer eigenen Architektur starten, sondern mit einem kleinen, begründeten Satz von Startrichtlinien. Wie der aussieht, welche Reihenfolge sich bewährt hat und wie du die Report-only-Phase nutzt, ohne sie zu einer Dauerlösung zu machen, steht ausführlich in [Conditional Access: Baselines, die nicht nerven](#).

Was Microsoft dir inzwischen abnimmt — ob du willst oder nicht

Ein Punkt, der in vielen Häusern noch nicht angekommen ist: Microsoft legt inzwischen eigene Conditional-Access-Richtlinien direkt in Tenants an. Diese von Microsoft verwalteten Richtlinien erscheinen zunächst im Report-only-Zustand, und Microsoft aktiviert sie frühestens dreißig Tage nach ihrer Einführung von selbst, wenn du sie in diesem Zustand lässt. Zwei Wochen vorher gibt es eine Ankündigung per E-Mail und im Message Center. Löschen oder umbenennen kannst du diese Richtlinien nicht; du kannst sie aber ausschalten, Ausnahmen eintragen oder sie duplizieren und die Kopie frei anpassen.

Der Katalog ist inzwischen umfangreich: MFA für alle Benutzer, MFA für Administration in den Microsoft-Admin-Portalen, Blockade von Legacy Authentication, Blockade des Device-Code-Flows und — mit Entra ID P2 — risikobasierte Varianten bis hin zur Sperre von Konten mit hohem Risiko. Neuerdings gibt es sogar eine Vorschau-Richtlinie, die Agent-Identitäten mit hohem Risiko blockiert. Wer das nicht verfolgt, wird irgendwann überrascht — und zwar immer an einem Freitagnachmittag.

WARNUNG — Der Freitagnachmittag-Effekt

Von Microsoft verwaltete Richtlinien greifen auch dann, wenn niemand bei dir hingeschaut hat. Das ist im Ergebnis gut und im Ablauf unangenehm. Zwei Konsequenzen: Erstens gehören eure Break-Glass-Konten in die Ausnahmeliste jeder dieser Richtlinien — auch der von Microsoft angelegten. Zweitens braucht jemand bei euch die Aufgabe, den Message Center einmal pro Woche zu lesen. Nicht als Projekt, sondern als Termin im Kalender.

Wie Break-Glass-Konten aussehen müssen, damit sie im Ernstfall funktionieren und im Alltag nicht vergessen werden, steht in [Break-Glass-Konten anlegen und überwachen](#).

Legacy Authentication: der billigste Sicherheitsgewinn, den es gibt

Nach Microsofts eigener Auswertung nutzen über neunundneunzig Prozent aller Password-Spray-Angriffe Legacy-Authentifizierungsprotokolle. Diese Protokolle können kein MFA. Solange sie offen sind, ist jede MFA-Richtlinie in deinem Tenant eine Empfehlung und keine Vorgabe — der Angreifer nimmt einfach die Tür daneben.

Gleichzeitig gilt: Multifaktor-Authentifizierung senkt nach Microsofts Zahlen das Risiko einer Kontoübernahme um mehr als neunundneunzig Prozent. Diese beiden Zahlen zusammen sind das gesamte Argument für die ersten beiden Monate deines Fahrplans. Wenn du in einem halben Jahr nur zwei Dinge schaffst, dann diese: [MFA in Microsoft 365 richtig einführen](#) und [Legacy Authentication endgültig abschalten](#).

FAKTEN — Verpflichtende MFA ist keine Zukunftsmusik mehr

Seit Oktober 2024 verlangt Microsoft MFA für Anmeldungen am Azure-Portal, am Entra-Admin-Center und am Intune-Admin-Center. Ab Februar 2025 kam das Microsoft-365-Admin-Center hinzu. Seit dem 1. Oktober 2025 läuft Phase 2: MFA für Azure CLI, Azure PowerShell, die mobile Azure-App, Infrastructure-as-Code-Werkzeuge und REST-Endpunkte bei allen schreibenden Vorgängen. Lesende Zugriffe sind ausgenommen.

Ein Aufschub war möglich, endete aber am 1. Juli 2026. Diese Frist ist vorbei — wer jetzt noch Automatisierung mit reinen Kennwortkonten betreibt, betreibt sie auf Zeit.

Prinzip 2 in der Praxis: minimale Rechte ohne PIM

Hier wird es unbequem, denn hier trifft das Prinzip auf die Lizenz. Privileged Identity Management — also die zeitlich begrenzte Aktivierung administrativer Rollen mit Begründung, Genehmigung und Protokoll — steckt in Entra ID P2 und damit in Microsoft 365 E5. In E3 hast du es nicht. Punkt.

Was du aber hast, ist der weitaus größere Teil der Wirkung. Der eigentliche Schaden im Mittelstand entsteht selten daran, dass jemand eine Rolle vierundzwanzig statt vier Stunden aktiv hatte. Er entsteht daran, dass elf Konten dauerhaft Global Administrator sind, dass diese Konten gleichzeitig E-Mails lesen und im Internet surfen, und dass drei davon Personen gehören, die das Haus vor zwei Jahren verlassen haben.

Der PIM-Ersatz, der nichts kostet

PIM-Funktion (E5 / Entra ID P2)	Behelf mit Microsoft 365 E3	Restrisiko
Just-in-Time-Aktivierung einer Rolle	Getrennte Admin-Konten, die nur für administrative Arbeit angemeldet werden	Rolle bleibt dauerhaft zugewiesen; die Trennung ist organisatorisch
Genehmigung durch eine zweite Person	Vier-Augen-Prinzip per Prozess, dokumentiert im Ticketsystem	Nicht technisch erzwungen, also disziplinarabhängig
Zeitlich begrenzte Zuweisung	Quartalsweise manuelle Durchsicht der Rollenzuweisungen per PowerShell-Export	Zwischen zwei Durchsichten liegen bis zu drei Monate
Zugriffsüberprüfungen (Access Reviews)	Exportierte Liste an die Fachbereiche mit Rückmeldefrist	Aufwand liegt bei dir statt beim System
Begründungspflicht bei Aktivierung	Conditional Access mit Authentifizierungsstärke für administrative Rollen	Keine Begründung, aber deutlich höhere Anmeldehürde
Lückenlose Protokollierung der Aktivierungen	Entra-Auditprotokoll und Purview-Audit auswerten	Aufbewahrungsdauer wird zum begrenzenden Faktor

Tabelle 2: Was PIM leistet, was du in E3 stattdessen tust — und was dabei offen bleibt. Die dritte Spalte gehört ins Risikoregister, nicht ins Vergessen.

Die wichtigste Maßnahme dieser ganzen Tabelle steht in keiner Zeile: Reduziere die Zahl der Global Administrators auf unter fünf. Das ist kein Lizenzthema, sondern eine Nachmittagsaufgabe.

Microsoft Entra kennt über sechzig eingebaute Rollen mit begrenztem Umfang; für fast jede Aufgabe gibt es eine, die weniger kann als „alles“. Der Grund, warum das nicht passiert, ist nie technisch. Er heißt „dann funktioniert vielleicht etwas nicht mehr“.

Eine Falle, die viele erst im Betrieb bemerken

Conditional Access kann auf Verzeichnisrollen als Bedingung reagieren — aber nur auf eingebaute Rollen. Rollen, die über eine Administrative Unit begrenzt sind, und selbst definierte Rollen werden von dieser Bedingung nicht erfasst. Wer also seine Administration sauber nach Standorten segmentiert und sich darauf verlässt, dass die strenge Admin-Richtlinie dann automatisch greift, hat eine Lücke, die im Portal nicht rot leuchtet. Der Ausweg ist unspektakulär: Adressiere solche Konten zusätzlich über eine Sicherheitsgruppe.

Segmentierung heißt nicht nur Netzwerk

Wenn im Zero-Trust-Kontext von Segmentierung die Rede ist, denken die meisten an VLANs. Im Microsoft-365-Alltag ist die wirksamere Segmentierung eine andere: Wer darf welche Daten sehen, wer darf sie nach außen geben, und wie lange gilt das. Externe Freigaben ohne Ablaufdatum, Teams ohne Eigentümer und Gastkonten aus abgeschlossenen Projekten sind der eigentliche laterale Bewegungsraum in einer Cloud-Umgebung. Wie du das sauber begrenzt, ohne die Zusammenarbeit lahmzulegen, beschreibt [Gastzugriff und externe Freigaben härten](#).

Der zweite Segmentierungshebel sind Anwendungen. Jede App-Registrierung mit weitreichenden Berechtigungen ist ein dauerhafter Zugang, der kein MFA kennt und keine Sitzung ablaufen lässt. Genau deshalb ist Consent-Governance kein Verwaltungsthema, sondern eine Zero-Trust-Maßnahme ersten Ranges — nachzulesen in [App-Registrierungen und Consent-Governance](#).

TIPP — Die Fünf-Minuten-Übung für die nächste Leitungsrunde

Öffne das Entra-Admin-Center, zeige die Liste der Konten mit der Rolle Global Administrator auf dem Beamer und lies die Namen vor. Nicht kommentieren, nur vorlesen. Diese Übung ersetzt in der Regel drei Folien Argumentation und beschleunigt Entscheidungen erheblich.

Wenn du dieselbe Wirkung mit Zahlen statt mit Namen erzielen möchtest, hilft [Security-Reporting für die Geschäftsführung](#).

Prinzip 3 in der Praxis: Kompromittierung annehmen

Das dritte Prinzip ist das, an dem die meisten Zero-Trust-Vorhaben stillschweigend vorbeigehen, weil es unangenehm ist. „Kompromittierung annehmen“ bedeutet nämlich, dass man den eigenen Erfolg nicht daran misst, ob etwas passiert, sondern daran, wie schnell man es merkt und wie klein man den Schaden hält. Das ist eine andere Art von Kennzahl, und sie lässt sich schlechter feiern.

Was du in E3 tatsächlich siehst

Mehr, als die meisten glauben. Microsoft Defender for Endpoint Plan 1 ist seit Anfang 2022 in Microsoft 365 E3 und A3 enthalten — damit hast du Verhaltensschutz, Angriffsflächenreduzierung und zentrale Sichtbarkeit auf den Endgeräten, wenn du die Geräte onboardest. Wie das ohne Betriebsunterbrechung gelingt, steht in [Defender for Endpoint: Onboarding ohne Drama](#). Für die Postfächer hat Microsoft 2026 begonnen, Defender for Office 365 Plan 1 in Microsoft 365 E3 und Office 365 E3 auszurollen; damit kommen Safe Links und Safe Attachments in Reichweite, ohne dass ein Add-on nötig ist — mehr dazu in [Defender for Office 365: Safe Links und Safe Attachments](#).

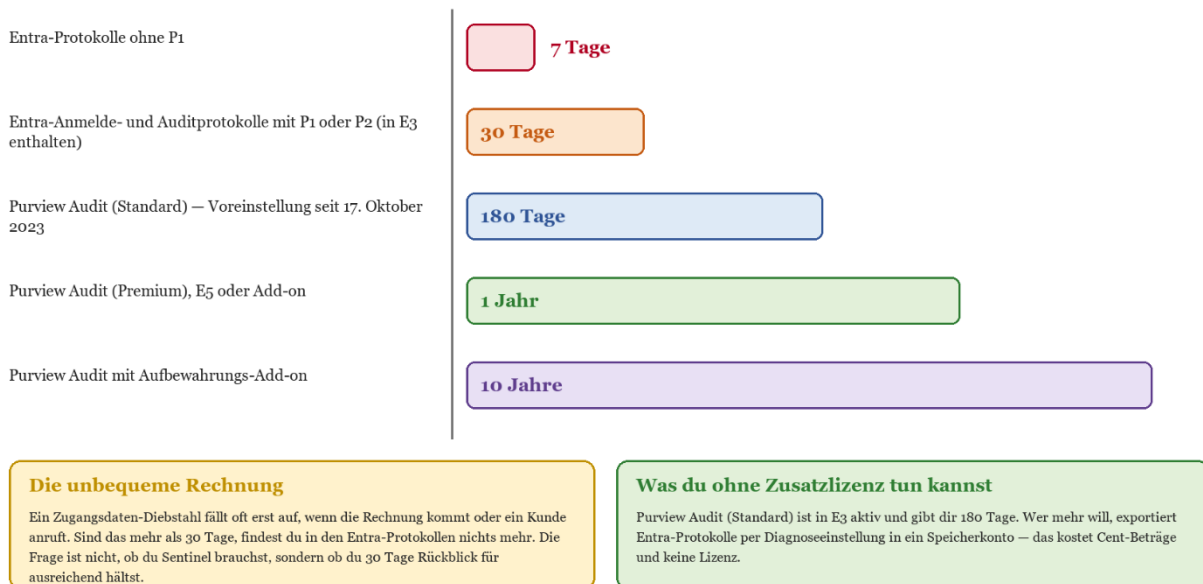
Dazu kommen Dinge, die schon immer da waren und trotzdem in vielen Häusern brachliegen: die Alert Policies im Microsoft-365-Defender-Portal, die Entra-Anmeldeprotokolle und die einheitliche Überwachungsprotokollierung in Microsoft Purview. Der Grund, warum sie brachliegen, ist meistens banal: Es gibt keinen Empfänger. Warnungen laufen in ein Sammelpostfach, in das niemand schaut. Wie du das ändern kannst, ohne im Alarmrauschen zu ertrinken, beschreibt [Alert Policies und Benachrichtigungen richtig aufsetzen](#).

Die Aufbewahrungsdauer ist die eigentliche Grenze

Hier liegt der praktisch wichtigste Unterschied zwischen „wir haben Protokolle“ und „wir können einen Vorfall aufklären“. Microsoft Entra bewahrt Anmelde- und Auditprotokolle sieben Tage lang auf, wenn keine Premium-Lizenz vorliegt, und dreißig Tage mit P1 oder P2. Die einheitliche Überwachungsprotokollierung in Purview Audit (Standard) reicht weiter: Seit dem 17. Oktober 2023 liegt die Voreinstellung bei 180 Tagen statt bei 90. Ein Jahr oder mehr bekommst du nur mit Audit (Premium) beziehungsweise einem Aufbewahrungs-Add-on.

Wie weit deine Protokolle zurückreichen — und warum das entscheidet

Balkenlänge logarithmisch: sonst wäre der oberste Balken ein Punkt.



boddenberg.de

Skizze 3: Der Rückblick, den deine Protokolle erlauben. Die Skala ist logarithmisch, damit der oberste Balken überhaupt sichtbar bleibt.

Warum das zählt: Der Zeitraum zwischen dem ersten erfolgreichen Phishing-Klick und dem Moment, in dem jemand im Haus stutzig wird, ist in der Praxis selten kürzer als ein paar Wochen. Wenn deine Entra-Protokolle nur dreißig Tage zurückreichen, ist die Frage „Von welcher IP-Adresse hat sich das Konto zuerst angemeldet?“ dann nicht mehr beantwortbar. Der Ausweg kostet fast nichts: Diagnoseeinstellungen in Entra einschalten und die Protokolle in ein Speicherkonto oder einen Log-Analytics-Arbeitsbereich schreiben. Ob daraus irgendwann eine vollständige SIEM-Anbindung wird, kannst du später entscheiden — die Abwägung steht in [Microsoft Sentinel anbinden: wann es sich lohnt](#).

Ein Wort zur Mitbestimmung, weil es an dieser Stelle immer kommt: Protokollierung, die personenbezogene Auswertungen ermöglicht, ist in Betrieben mit Betriebsrat nicht einfach eine technische Einstellung. Das ist kein Grund, es zu lassen, sondern ein Grund, es früh und sauber zu

besprechen. Was mitbestimmungspflichtig ist und was nicht, ordnet [Security-Monitoring und Betriebsrat: was mitbestimmungspflichtig ist](#) ein.

Erkennung ist wertlos ohne geprobte Reaktion

Der häufigste Fehler nach einer gelungenen Erkennung ist die hektische Improvisation: Kennwort zurücksetzen, fertig. Dabei bleiben Sitzungstoken gültig, Weiterleitungsregeln im Postfach bestehen und die angemeldete mobile App weiter verbunden. Die Reihenfolge, in der man ein übernommenes Konto tatsächlich aufräumt, steht in [Kompromittiertes Konto erkennen und aufräumen](#); was in den ersten sechzig Minuten nach einem Phishing-Vorfall zu tun ist, in [Phishing-Vorfall: die ersten 60 Minuten](#).

Und weil ein Plan, den niemand geübt hat, nur ein gut formatiertes Dokument ist: Plane die erste Übung ein, bevor der Plan fertig ist. Eine Trockenübung im Team deckt in zwei Stunden mehr Lücken auf als ein Quartal Konzeptarbeit — siehe [Feuerwehübung: Security-Notfälle im Team trainieren](#). Der strukturelle Rahmen dafür ist [Incident-Response-Plan für Microsoft 365](#).

WARNUNG — Der Denkfehler, der Ransomware groß macht

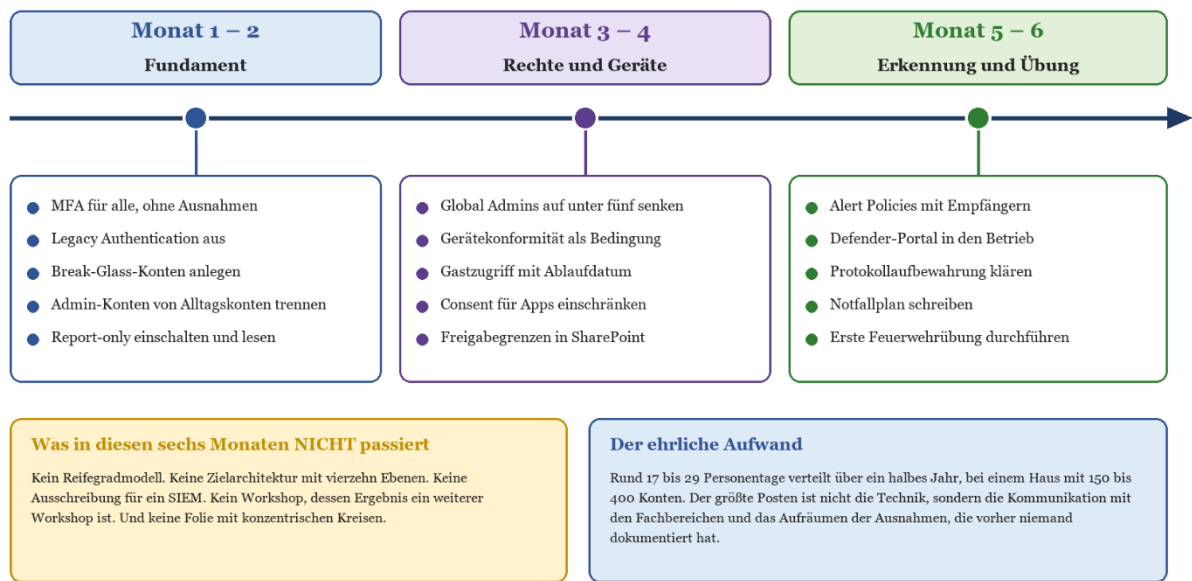
„Kompromittierung annehmen“ heißt auch: Deine Sicherungen müssen einen Angriff überleben, der mit administrativen Rechten geführt wird. Wenn dieselben Konten, die deine Umgebung verwalten, auch die Aufbewahrungsrichtlinien und die Sicherungen ändern können, hast du keine Sicherung, sondern eine Kopie mit Zeitverzögerung.

Die konkreten Maßnahmen dazu stehen in [Ransomware-Vorsorge in Microsoft 365](#); die Datenseite — Bezeichnungen, Aufbewahrung, Auswertung — im [Kompetenzbereich Microsoft Purview](#).

Sechs Monate, ein Fahrplan, keine Folien

Jetzt der Teil, wegen dessen du bis hierher gelesen hast. Der folgende Fahrplan setzt Microsoft 365 E3 voraus, ein Haus mit ungefähr 150 bis 400 Konten, eine IT mit zwei bis vier Personen und keine Zusatzlizenzen. Er ist absichtlich unaufgeregt.

Sechs Monate Zero Trust mit Microsoft 365 E3



Der Fahrplan ist bewusst langweilig. Langweilig ist die Eigenschaft, die Sicherheitsmaßnahmen im Betrieb überleben lässt.

boddenberg.de

Skizze 4: Sechs Monate in drei Etappen. Jede Etappe endet mit etwas, das man vorzeigen kann — das ist kein Zufall, sondern Voraussetzung dafür, dass die nächste Etappe bewilligt wird.

Monat 1 und 2: das Fundament, das alles andere trägt

MFA für alle. Ohne Ausnahmeliste, die länger ist als fünf Zeilen. Parallel dazu Legacy Authentication abschalten, denn ohne diesen Schritt ist der erste wertlos. Break-Glass-Konten anlegen, dokumentieren und aus jeder Richtlinie ausschließen. Administrative Konten von Alltagskonten trennen. Und alle neuen Richtlinien zuerst in Report-only laufen lassen, mindestens zwei Wochen, mit tatsächlicher Auswertung — nicht mit Hoffnung.

Wenn dein Tenant heute noch mit Security Defaults läuft, ist die Frage nach dem Umstieg Teil dieser Etappe und nicht später. Die Abwägung dazu steht in [Security Defaults oder Conditional Access?](#).

Monat 3 und 4: Rechte einsammeln, Geräte einbeziehen

Die Zahl der Global Administrators auf unter fünf senken und für den Rest die passende eingeschränkte Rolle finden. Gerätekonformität als Bedingung in die Conditional-Access-Baseline aufnehmen — zunächst nur für die sensiblen Anwendungen, dann breiter. Gastzugriff mit Ablaufdatum versehen und die Altlasten aufräumen. Benutzer-Consent für Anwendungen einschränken. Freigabegrenzen in SharePoint und OneDrive setzen. Diese Etappe ist die politisch anstrengendste, weil sie Menschen etwas wegnimmt.

Wer parallel die Tenant-Grundeinstellungen einmal systematisch durchgeht, spart sich später viel Einzelfalldiskussion: [Tenant-Härtung: die 20 wichtigsten Schrauben](#) liefert dafür die Reihenfolge. Wenn ihr noch eine SharePoint-Server-Umgebung im Haus habt, gehört sie in dieselbe Betrachtung — Hinweise dazu in [MFA für SharePoint Server on-premises](#) und, für die Kerberos-Seite dahinter, im [Kompetenzbereich Kerberos](#).

Monat 5 und 6: sehen, melden, üben

Alert Policies scharfstellen und jeder Warnung einen realen Empfänger mit Namen zuordnen. Das Defender-Portal in den Betriebsalltag einbauen, also einen festen Termin pro Woche. Die Frage der Protokollaufbewahrung entscheiden und dokumentieren. Den Notfallplan auf zwei Seiten schreiben – mehr liest im Ernstfall niemand. Und dann die erste Übung durchführen.

Wenn ihr an diesem Punkt Lust auf mehr habt, ist eine kontrollierte Angriffssimulation der nächste sinnvolle Schritt; wie man so etwas beauftragt, ohne dass es zur Show wird, beschreibt [Red-Team-Übung: der kontrollierte Angriff](#). Für die Belegschaft ist die günstigere Variante das [Attack Simulation Training: Phishing-Übungen richtig aufsetzen](#).

Etappe	Maßnahme	Aufwand	Wirkung
Monat 1–2	MFA für alle Konten	3–5 Tage	Sehr hoch – deckt den mit Abstand häufigsten Angriffsweg ab
Monat 1–2	Legacy Authentication abschalten	2–4 Tage	Sehr hoch – ohne diesen Schritt ist MFA umgehbar
Monat 1–2	Break-Glass-Konten einrichten	0,5 Tage	Hoch – verhindert die Totalaussperrung
Monat 3–4	Global Admins reduzieren	1–2 Tage	Hoch – begrenzt den Schaden jeder einzelnen Übernahme
Monat 3–4	Gerätekonformität als Bedingung	4–8 Tage	Hoch – setzt Intune und saubere Geräteverwaltung voraus
Monat 3–4	Gastzugriff und Freigaben härten	2–3 Tage	Mittel bis hoch – abhängig von der Altlastenmenge
Monat 5–6	Alert Policies mit Empfängern	1–2 Tage	Mittel – Wirkung entsteht erst durch Bearbeitung
Monat 5–6	Protokollaufbewahrung klären	1 Tag	Mittel – zahlt sich erst im Ernstfall aus, dann aber vollständig
Monat 5–6	Notfallplan und erste Übung	2–3 Tage	Hoch – verkürzt die Reaktionszeit im Ernstfall dramatisch

Tabelle 3: Der Fahrplan mit ehrlichen Aufwänden. Summe: rund 17 bis 29 Personentage über sechs Monate, ohne Zusatzlizenzen.

Was du in diesen sechs Monaten bewusst weglässt

Mindestens genauso wichtig wie die Liste oben ist die Liste der Dinge, die nicht stattfinden. Keine Netzwerksegmentierung im Rechenzentrum – zu teuer, zu langsam, zu wenig Wirkung im Verhältnis. Keine SIEM-Ausschreibung. Kein Reifegradmodell mit fünf Stufen und vierundsechzig Kriterien. Keine Vertraulichkeitsbezeichnungen für alle Dokumente, solange noch elf Personen Global Administrator sind. Und kein Passwordless-Rollout für die gesamte Belegschaft – für die administrativen Konten dagegen sehr wohl, siehe [Passwordless: FIDO2 und Passkeys in der Praxis](#).

Diese Weglassliste gehört ins Protokoll. Nicht als Versäumnis, sondern als bewusste Entscheidung mit Datum. Wenn in achtzehn Monaten jemand fragt, warum ihr das eine getan und das andere gelassen habt, ist dieser Eintrag die Antwort – und in einem NIS2-Kontext ist genau diese nachvollziehbare Priorisierung das, wonach gefragt wird. Was daraus konkret an technischen Maßnahmen folgt, ordnet [NIS2 aus Security-Sicht: technische Maßnahmen in M365](#) ein.

TIPP – Der Punkt, an dem externe Unterstützung tatsächlich hilft

Nicht bei der Strategie – die steht oben und passt auf eine Seite. Sondern bei den zwei Wochen Report-only-Auswertung, in denen jemand mit Erfahrung die Ausnahmen von den echten Problemen unterscheiden muss. Das ist die Stelle, an der interne Teams am häufigsten steckenbleiben, weil sie die Signale nicht einordnen können.

Für diese Etappe gibt es die [Microsoft 365 Security Beratung](#); wenn das Team die Grundlagen selbst aufbauen soll, ist die [Schulung Microsoft 365 Security](#) der günstigere Weg.

Warum das keine Übervorsicht ist

Es gibt in Deutschland eine anhaltende Neigung, Angriffe auf öffentliche und mittelständische Einrichtungen als Ausnahmefälle zu betrachten. Wer sich einmal ansieht, wie eine Kette aus einem übernommenen Zugang, unzureichend begrenzten Rechten und fehlender Erkennung tatsächlich abläuft, verliert diese Neigung recht schnell. Genau diese Kette beschreibt das [Dossier TerminalFix und der Berlin-Hack](#) an einem realen Fall.

Der Punkt daran ist nicht die Dramatik, sondern die Banalität der einzelnen Glieder. In keiner dieser Ketten steckt ein Angriff, für den man E5 gebraucht hätte, um ihn zu verhindern. Es steckt fast immer ein Konto darin, das mehr durfte, als es brauchte, und ein Protokoll, das niemand gelesen hat.

Wer wissen will, wo er steht, ohne sich in Punktejagd zu verlieren, findet im Secure Score einen brauchbaren Ausgangspunkt — mit der wichtigen Einschränkung, dass eine hohe Punktzahl kein Sicherheitsnachweis ist. Wie man ihn sinnvoll liest, steht in [Secure Score: sinnvoll nutzen statt Punktejagd](#). Wenn eure Postfächer noch ohne saubere Absenderauthentifizierung laufen, ist auch das ein Teil des Bildes: [SPF, DKIM, DMARC für Exchange Online](#).

Häufige Fragen

Brauchen wir für Zero Trust Microsoft 365 E5?

Nein, aber du kommst mit E3 nicht überall hin. E3 enthält Entra ID P1 und damit Conditional Access, Authentifizierungsstärken, Gerätekonformität als Bedingung und Administrative Units. Was fehlt, ist Entra ID P2: Privileged Identity Management, Identity Protection mit Risikosignalen, Zugriffsüberprüfungen und Entitlement Management. Meine Erfahrung: Die ersten achtzig Prozent der Wirkung stecken in dem, was E3 schon kann. Die Lizenzdiskussion ist meistens ein bequemer Grund, nicht anzufangen.

Wie viele Conditional-Access-Richtlinien brauchen wir wirklich?

Weniger, als du denkst. Ein durchdachter Startsatz von sechs bis acht Richtlinien deckt den allergrößten Teil ab. Alles darüber entsteht in der Regel aus Einzelfällen, die nie aufgeräumt wurden. Wenn du in deinem Tenant vierzig Richtlinien hast und niemand mehr erklären kann, was Richtlinie 23 tut, ist das kein Zeichen von Reife, sondern von fehlender Pflege.

Wir haben kein Intune. Können wir trotzdem anfangen?

Ja. Die ersten beiden Monate des Fahrplans brauchen kein Intune: MFA, Legacy Authentication, Break-Glass-Konten und getrennte Admin-Konten sind reine Identitätsthemen. Ohne Geräteverwaltung fällt allerdings die Bedingung „konformes Gerät“ weg, und damit ein wesentlicher Baustein der zweiten Etappe. Das ist kein Grund zu warten, aber ein Grund, die Geräteverwaltung als nächstes Projekt einzuplanen.

Was passiert, wenn wir gar nichts tun?

Interessanterweise nicht nichts. Microsoft legt inzwischen selbst Richtlinien in Tenants an und aktiviert sie nach einer Ankündigungsfrist. Auch die verpflichtende MFA für Verwaltungsportale läuft unabhängig von deiner Planung weiter. Wer nichts tut, bekommt trotzdem Veränderungen —

nur eben zu Microsofts Zeitpunkt und ohne vorherige Auswirkungenanalyse im eigenen Haus. Das ist der schlechtere Weg zum selben Ziel.

Wie überzeugen wir die Geschäftsführung?

Nicht mit Zero Trust. Der Begriff hilft dir dort nicht, weil er nach Projekt klingt und nach Kosten. Was hilft: zwei konkrete Zahlen und ein Szenario. Die Zahlen sind die Anzahl eurer Konten mit dauerhaften Administrationsrechten und die Anzahl der Tage, die eure Protokolle zurückreichen. Das Szenario ist die Frage, wer am Samstagmorgen um sieben entscheidet, ob der Tenant vom Netz geht. Wer darauf keine Antwort hat, versteht das Problem in zwei Minuten.

Reicht MFA per SMS?

Es ist besser als kein zweiter Faktor und schlechter als alles andere. SMS-Codes lassen sich abfangen und in Echtzeit weiterreichen — moderne Phishing-Werkzeuge tun genau das. Für die allgemeine Belegschaft ist die Authenticator-App mit Nummernabgleich ein vernünftiger Ausgangspunkt. Für alle administrativen Konten solltest du auf phishing-resistente Verfahren gehen, also FIDO2-Schlüssel oder Passkeys. Conditional Access kennt dafür eine eigene Authentifizierungsstärke; du musst sie nur zuweisen.

Wie lange dauert das wirklich?

Der Fahrplan oben umfasst rund 17 bis 29 Personentage über sechs Monate. Die reine Konfigurationszeit ist dabei der kleinere Teil. Der größere geht in Abstimmung, in das Aufräumen undokumentierter Ausnahmen und in das Gespräch mit den Fachbereichen, deren Spezialanwendung noch Basisauthentifizierung spricht. Wer diese Anteile in der Planung unterschlägt, landet im vierten Monat in der Diskussion, warum das Projekt hinterherhinkt.

Was ist der häufigste Fehler in Zero-Trust-Projekten im Mittelstand?

Die Reihenfolge. Es wird mit der Säule begonnen, die am interessantesten klingt — meistens Netzwerk oder Daten — statt mit der, in der die Angriffe tatsächlich stattfinden. Das ist die Identität. Der zweithäufigste Fehler: Man baut Erkennung auf, ohne vorher festzulegen, wer die Meldungen liest. Eine Warnung ohne Empfänger ist kein Sicherheitsgewinn, sondern nur ein zusätzlicher Eintrag in einem Protokoll, das niemand öffnet.

Fazit

Zero Trust im Mittelstand scheitert selten an der Technik und fast nie an der Lizenz. Es scheitert an der Übersetzung — daran, dass zwischen dem Prinzip und der ersten Konfiguration ein Berg aus Folien liegt, den niemand wegräumt. Die drei Prinzipien sind einfach genug, dass man sie sich merken kann, und sie lassen sich vollständig in Microsoft-365-Funktionen übersetzen: Conditional Access für das explizite Verifizieren, getrennte Konten und eingeschränkte Rollen für die minimalen Rechte, Protokollierung und geübte Reaktion für die Annahme, dass es schiefgeht.

Mit Microsoft 365 E3 erreichst du in sechs Monaten einen Zustand, in dem die häufigsten Angriffswege geschlossen sind, in dem der Schaden einer einzelnen Kontoübernahme begrenzt bleibt und in dem jemand merkt, wenn etwas passiert. Das ist kein Endzustand und kein Zertifikat. Es ist der Unterschied zwischen einem Vorfall, den man am Montag aufräumt, und einem, der in der Lokalpresse steht.

Und wenn du am Ende der sechs Monate immer noch keine Folie mit konzentrischen Kreisen hast: umso besser. Die Kreise haben noch nie jemanden aufgehalten.

WEITER — Passend zu diesem Beitrag

- › [Conditional Access: Baselines, die nicht nerven](#) — der konkrete Startsatze an Richtlinien
- › [Tenant-Härtung: die 20 wichtigsten Schrauben](#) — die Grundeinstellungen, die vorher stimmen müssen
- › [MFA in Microsoft 365 richtig einführen](#) und [Legacy Authentication endgültig abschalten](#) — die beiden Schritte aus Monat 1 und 2
- › [Break-Glass-Konten anlegen und überwachen](#) — bevor du die erste Richtlinie scharfstellst
- › [Incident-Response-Plan für Microsoft 365](#) und [Feuerwehübung: Security-Notfälle im Team trainieren](#) — für das dritte Prinzip
- › [Microsoft 365 Security](#) — die Roadmap der gesamten Reihe
- › [Microsoft 365 Security Beratung](#) und [Schulung Microsoft 365 Security](#) — wenn ihr Unterstützung braucht