

Tenant-Härtung: die 20 wichtigsten Schrauben

Ein frisch bestellter Microsoft-365-Tenant ist wie eine Mietwohnung mit Schlüssel unter der Fußmatte: Man kann sofort einziehen, und genau das ist das Problem. Die Standardeinstellungen sind darauf optimiert, dass am ersten Tag nichts hakt. Sie sind nicht darauf optimiert, dass am dreihundertsten Tag niemand deine Postfächer mitliest.

Dieser Artikel ist der Einstieg in das Handlungsfeld Tenant-Härtung. Er listet zwanzig Schrauben, die in der Praxis den größten Unterschied machen — mit Portal, Klickpfad, Lizenzbedarf, Priorität und dem entscheidenden Halbsatz, warum du das überhaupt anfassen sollst. Kein Framework, keine Reifegradmatrix, keine Selbstverwirklichung. Zwanzig Schalter, eine Reihenfolge, ein Nachmittag für die fünf wichtigsten davon.

Die Schrauben sind bewusst so gewählt, dass sie sich auch in einem Haus mit vier IT-Leuten und einem Budget umsetzen lassen, das nicht in Millionen gerechnet wird. Wo eine Einstellung eine bestimmte Lizenz verlangt, steht das dran. Und wo eine Schraube ein eigenes Kapitel verdient, verweist der Text auf den passenden Beitrag im Themenbereich [Microsoft 365 Security](#). Wer wissen will, wie ein solcher Tenant im Ernstfall aussieht, wenn niemand die Schrauben angezogen hat, findet die Langfassung im Dossier [TerminalFix und der Berlin-Hack](#).

FAKTEN · Warum Standardeinstellungen keine Sicherheitsentscheidung sind

Microsoft liefert Voreinstellungen aus, die für den kleinsten gemeinsamen Nenner aller Kundinnen und Kunden funktionieren müssen — vom Zwei-Personen-Betrieb bis zum Konzern mit Faxgerät im Keller. Das erzeugt systematisch weiche Defaults.

Drei Beispiele, alle belegt durch die Produktdokumentation: Die Überwachungsaufzeichnung ist bei den Business-Lizenzen nicht automatisch eingeschaltet. Die automatische Weiterleitung nach außen steht ab Werk auf „Automatisch – systemgesteuert“, was je nach Alter des Tenants Unterschiedliches bedeutet. Und die Teams-Föderation erlaubt standardmäßig Chats mit jeder beliebigen anderen Microsoft-365-Organisation.

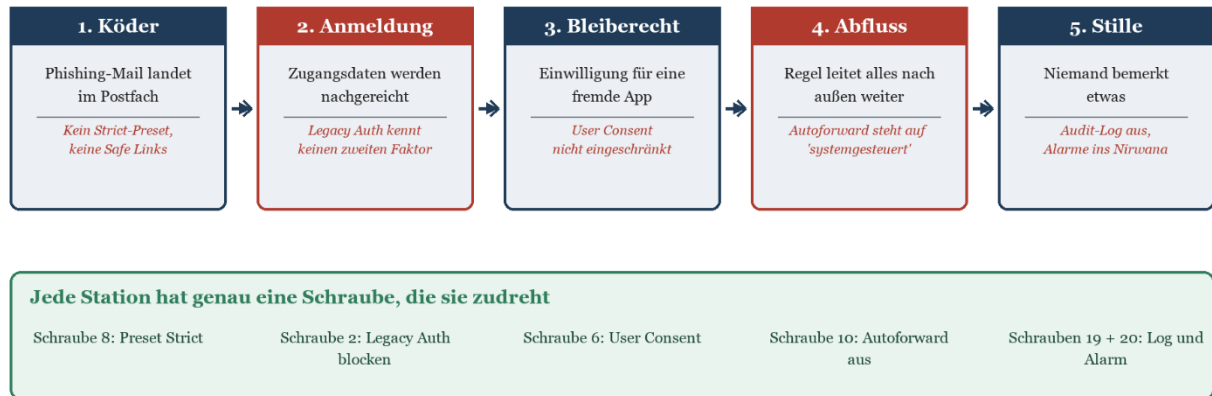
Keine dieser Einstellungen ist ein Fehler. Jede davon ist eine Entscheidung, die dir niemand abgenommen hat.

Der Tenant ab Werk: fünf Türen, keine einzige verschlossen

Bevor wir Schalter umlegen, lohnt ein Blick darauf, wie ein Angriff in einem unbearbeiteten Tenant tatsächlich abläuft. Nicht der Hollywood-Angriff mit Zero-Day und grünem Terminal, sondern der langweilige, der in der Statistik steht. Er benutzt ausschließlich Funktionen, die vorgesehen sind. Er bricht nichts auf. Er läuft die Standardeinstellungen entlang wie ein Kunde durch einen Möbelhausparcours.

Wie ein Tenant ab Werk übernommen wird

Fünf Stationen, fünf Standardeinstellungen, kein einziger Exploit



Skizze 1: Die typische Angriffskette in einem ungehärteten Tenant — und die Schraube, die jede Station zudreht.

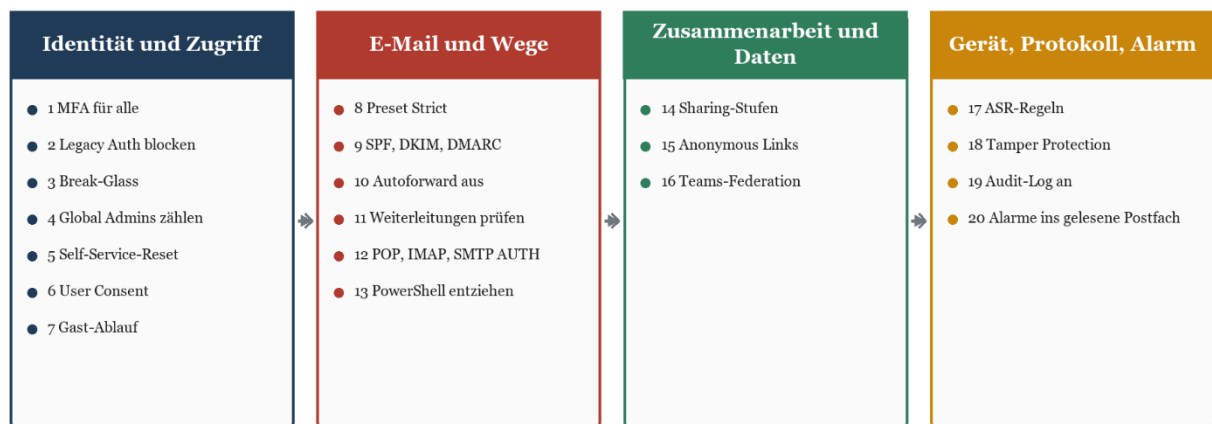
Bemerkenswert an dieser Kette ist, dass keine einzige Station einen Exploit braucht. Der Köder ist eine Mail, die durch den Filter kommt, weil der Filter auf der bequemen Stufe steht. Die Anmeldung gelingt, weil ein alter Client ohne zweiten Faktor spricht. Das Bleiberecht entsteht durch eine Einwilligung, die ein Mensch am Dienstagnachmittag freundlich weggeklickt hat. Der Abfluss läuft über eine Posteingangsregel. Und die Stille kommt daher, dass niemand ein Postfach benannt hat, in dem Alarme auflaufen.

Vier Felder, in dieser Reihenfolge

Die zwanzig Schrauben verteilen sich auf vier Felder. Die Reihenfolge ist keine Geschmacksfrage, sondern folgt der Angriffskette von innen nach außen: Wer die Identität nicht im Griff hat, braucht über Freigabeeinstellungen nicht nachzudenken. Ein Angreifer mit gültigem Konto teilt sich die Daten selbst frei — und zwar korrekt protokolliert, mit dem Namen deiner Kollegin daneben.

Vier Felder, zwanzig Schrauben

Die Reihenfolge ist keine Geschmacksfrage: von innen nach außen



Wer bei Feld 3 anfängt, hat hübsche Freigabeeinstellungen für einen Tenant, in dem längst jemand anderes mitliest.

Skizze 2: Die vier Härtungsfelder mit den zugehörigen Schrauben. Von links nach rechts abarbeiten.

WARNUNG · Die Reihenfolge ist der halbe Erfolg

Der häufigste Fehler in Härtungsprojekten ist nicht die falsche Einstellung, sondern die richtige Einstellung zum falschen Zeitpunkt. Wer Conditional Access scharf stellt, bevor Break-Glass-Konten existieren, sperrt sich mit beeindruckender Zuverlässigkeit selbst aus. Der Weg zurück führt dann über den Microsoft-Support, und der hat gerade viel zu tun.

Regel: Schraube 3 kommt vor Schraube 1 und 2. Immer. Auch wenn sie in der Tabelle weiter unten steht.

Die zwanzig Schrauben

Die folgenden vier Tabellen sind die eigentliche Checkliste. Die Spalte „Prio“ bedeutet: 1 heißt „diese Woche“, 2 heißt „diesen Monat“, 3 heißt „wenn die ersten beiden Stufen stehen“. Die Klickpfade entsprechen der aktuellen Oberfläche der jeweiligen Portale — Microsoft benennt Menüpunkte gelegentlich um, die Logik bleibt.

Feld A: Identität und Zugriff

Nr.	Schraube	Portal und Klickpfad	Lizenz	Prio	Warum
1	MFA für alle, nicht für die Hälfte	Entra Admin Center › Schutz › Bedingter Zugriff › Richtlinien › Neue Richtlinie (Gewähren: Multifaktor-Authentifizierung erforderlich)	Entra ID P1; ohne P1: Sicherheitssstandards	1	Der zweite Faktor ist die einzige Maßnahme mit dieser Wirkung pro Aufwand. Die Lücke sind fast nie die Nutzerkonten, sondern die Ausnahmen für Dienstkonto, Scanner und „den einen Kollegen“, die nie zurückgenommen wurden.
2	Legacy Authentication blockieren	Entra Admin Center › Schutz › Bedingter Zugriff › Neue Richtlinie › Bedingungen › Client-Apps › Andere Clients	Entra ID P1	1	Basic Auth kennt keinen zweiten Faktor. Eine MFA-Richtlinie neben einem offenen Legacy-Kanal ist ein verriegeltes Tor neben einem gekippten Fenster.
3	Break-Glass-Konten anlegen	Entra Admin Center › Identität › Benutzer › Neuer Benutzer (reines Cloud-Konto auf .onmicrosoft.com, aus allen CA-Richtlinien ausgenommen)	jede Lizenzstufe	1	Microsoft empfiehlt zwei dauerhaft berechnigte Notfallkonten. Ohne sie ist die erste schlecht gebaute Richtlinie zugleich die letzte Amtshandlung.
4	Globale Administratoren zählen	Entra Admin Center › Identität › Rollen und Administratoren › Globaler Administrator › Zuweisungen	jede Stufe; Just-in-Time über PIM: Entra ID P2	1	Microsoft empfiehlt weniger als fünf Personen in dieser Rolle. Alles darüber ist Angriffsfläche mit Vollzugriff — und in der Praxis oft ein Konto, das seit der Migration 2019 niemandem mehr gehört.
5	Self-Service-Kennwortzurücksetzung aktivieren	Entra Admin Center › Schutz › Kennwortzurücksetzung › Eigenschaften und Authentifizierungsmethoden	Entra ID P1 (auch für Rückschreiben ins AD)	3	Der Helpdesk ist der bequemste Social-Engineering-Kanal überhaupt. Wer das Zurücksetzen automatisiert, nimmt dem Anruf „hier ist der neue Kollege, ich komme nicht rein“ die Grundlage.
6	Benutzereinwilligung für Apps einschränken	Entra Admin Center › Identität › Anwendungen › Unternehmensanwendungen › Einwilligung und Berechtigungen › Benutzereinwilligungseinstellungen	jede Stufe	1	Ab Werk darf jeder Apps Berechtigungen erteilen, die keine Administratorfreigabe brauchen. Ein Klick genügt, damit eine fremde Anwendung dauerhaft Mail und Dateien liest — ohne Passwort, ohne MFA-Prompt, ohne Ende.
7	Ablauf für	Entra Admin Center ›	Zugriffsübe	2	Projekte enden, Gäste bleiben. Ein

	Gastkonten erzwingen	Identität › Externe Identitäten › Einstellungen für externe Zusammenarbeit; Zugriffsüberprüfungen unter Identity Governance	rprüfungen: Entra ID P2		Gastkonto ohne Ablaufdatum überlebt erfahrungsgemäß den Dienstleister, das Projekt und die Geschäftsbeziehung.
--	----------------------	---	-------------------------	--	--

Zu den Schrauben 1 und 2 gibt es jeweils einen eigenen Beitrag, weil beide mehr Fallstricke haben, als in eine Tabellenzelle passen: [MFA in Microsoft 365 richtig einführen](#) beschreibt den Rollout ohne Aufstand in der Belegschaft, [Legacy Authentication endgültig abschalten](#) den Weg von der Bestandsaufnahme über den Report-only-Modus bis zur harten Sperre. Die Richtlinienstruktur selbst – also welche Regeln du überhaupt bauen solltest – steht in [Conditional Access: Baselines, die nicht nerven](#). Wenn du keine Entra-ID-P1-Lizenzen hast, ist die Abwägung zwischen den Sicherheitsstandards und selbstgebauten Richtlinien in [Security Defaults oder Conditional Access?](#) ausgeführt.

TIPP • Break-Glass ohne Zettelwirtschaft

Zwei Konten, reine Cloud-Identitäten auf der .onmicrosoft.com-Domain, keine Personenbindung, kein gemeinsames Muster im Namen. Passwörter mit sechzig Zeichen, geteilt auf zwei Umschläge in zwei verschiedenen Safes, damit niemand allein einsteigen kann. Beide Konten aus allen Richtlinien für bedingten Zugriff ausnehmen – und danach eine Warnungsregel bauen, die anschlägt, sobald sich eines davon anmeldet.

Der letzte Halbsatz ist der wichtige. Ein Notfallkonto ohne Überwachung ist eine Hintertür, die du selbst eingebaut hast.

› [Break-Glass-Konten anlegen und überwachen](#)

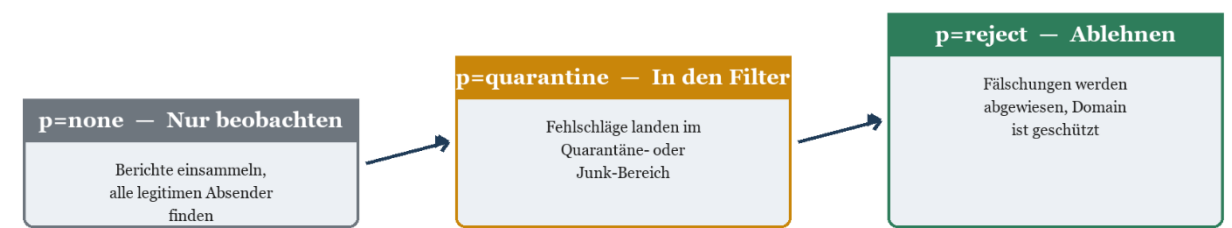
Feld B: E-Mail und Nachrichtenwege

Nr.	Schraube	Portal und Klickpfad	Lizenz	Pri o	Warum
8	Voreingestellte Sicherheitsrichtlinien auf „Strikt“	Defender-Portal › E-Mail und Zusammenarbeit › Richtlinien und Regeln › Bedrohungsrichtlinien › Voreingestellte Sicherheitsrichtlinien	EOP; Safe Links und Safe Attachments: Defender für Office 365 P1 oder P2	1	Microsoft pflegt die Schwellwerte nach, du nicht. Strikt stellt erkannten Spam in die Quarantäne statt in den Junk-Ordner – der Unterschied zwischen „weggeräumt“ und „einen Klick entfernt“.
9	SPF, DKIM und DMARC scharf stellen	Defender-Portal › E-Mail und Zusammenarbeit › Richtlinien › E-Mail-Authentifizierung › DKIM; die Einträge selbst beim DNS-Anbieter	EOP	2	Ohne veröffentlichte DMARC-Richtlinie ist deine Domain Freiwild für Absenderfälschung. Der Weg führt über p=none und p=quarantine zu p=reject – nie direkt, sonst stirbt die Rechnungsversand-Software als Erstes.
10	Automatische Weiterleitung nach außen abschalten	Defender-Portal › Bedrohungsrichtlinien › Anti-Spam › Ausgehende Spamfilterrichtlinie › Automatische Weiterleitung: „Aus“	EOP	1	Der Standardwert heißt „Automatisch – systemgesteuert“ und bedeutet je nach Alter des Tenants Unterschiedliches. Setze ihn explizit, dann weißt du, was gilt, ohne raten zu müssen.
11	Bestehende Weiterleitungen und Posteingangsregeln prüfen	Exchange Admin Center › Empfänger › Postfächer › Postfacheinstellungen › E-Mail-Weiterleitung; gründlicher per PowerShell über Get-Mailbox und Get-	EOP	1	Die Richtlinie aus Schraube 10 stoppt Neues. Sie räumt nicht weg, was ein Angreifer vor drei Monaten eingerichtet hat – und was seitdem still jede Angebotsmail kopiert.

		InboxRule			
12	Legacy-Protokolle am Postfach abschalten	Exchange Admin Center > Empfänger > Postfächer > E-Mail-Apps verwalten; flächendeckend über Set-CASMailbox und Authentifizierungsrichtlinien	EOP	2	POP und IMAP sind die letzten Türen, durch die Basic Auth noch geht. Für SMTP AUTH hat Microsoft angekündigt, die Basisauthentifizierung Ende Dezember 2026 bei bestehenden Tenants standardmäßig zu deaktivieren — freiwillig ist eleganter als überrascht.
13	PowerShell-Zugriff für normale Konten entziehen	Exchange Online PowerShell: Set-User -RemotePowerShellEnabled \$false, mit Ausnahmen für Administratoren, Dienst- und Überwachungskonten	EOP	3	Wer keine Verwaltungsaufgaben hat, braucht keine Verwaltungsschnittstelle. Angreifer mit gestohlenem Konto brauchen sie sehr wohl — sie automatisieren damit das Anlegen von Regeln und das Abziehen von Postfächern.

Die DMARC-Rampe: niemals mit p=reject anfangen

Drei Stufen, dazwischen jeweils Berichte lesen und Absender aufräumen



Zwischen den Stufen liegen Wochen, nicht Minuten. Ein Schlüsselwechsel bei DKIM braucht allein 96 Stunden.

Skizze 3: DMARC in drei Stufen. Wer die mittlere Stufe überspringt, lernt seine eigenen Absender auf die harte Tour kennen.

Die Details zu Schraube 9 — inklusive der Frage, welche Systeme in deinem Haus eigentlich in deinem Namen versenden — stehen in [SPF, DKIM, DMARC für Exchange Online](#). Was hinter den Presets aus Schraube 8 technisch passiert und wo Safe Links an seine Grenzen kommt, behandelt [Defender for Office 365: Safe Links und Safe Attachments](#). Und wenn du die Schrauben 10 und 11 anfasst, weil du bereits einen Verdacht hast: Der geordnete Ablauf steht in [Kompromittiertes Konto erkennen und aufräumen](#).

WARNUNG · Schraube 11 findet, was Schraube 10 nicht mehr erreicht

Eine ausgehende Spamfilterrichtlinie unterbindet künftige Weiterleitungen. Sie löscht keine bestehende Posteingangsregel. In fast jedem Tenant, den wir prüfen, existieren Regeln, die Mails in einen unauffälligen Unterordner verschieben und als gelesen markieren — angelegt nicht von Angreifern, sondern von Menschen, die vor sechs Jahren ihr Postfach sortieren wollten.

Der Punkt ist: Du kannst die harmlosen nicht von den bösartigen unterscheiden, ohne einmal alle anzusehen. Genau deshalb steht diese Schraube auf Prio 1 und nicht auf Prio 3.

Feld C: Zusammenarbeit und externe Freigaben

Nr.	Schraube	Portal und Klickpfad	Lizenz	Prio	Warum
-----	----------	----------------------	--------	------	-------

14	Freigabestufen für SharePoint und OneDrive festlegen	SharePoint Admin Center › Richtlinien › Freigabe › Externe Freigabe (Organisationsebene, danach je Site)	SharePoint Online	2	Die Organisationsebene ist die Obergrenze. Steht sie auf „Jeder“, ist jede restriktivere Einstellung darunter Dekoration, die eine einzige Site-Besitzerin wieder aufmachen kann.
15	Anonyme Links begrenzen und ablaufen lassen	SharePoint Admin Center › Richtlinien › Freigabe › erweiterte Einstellungen für „Jeder“-Links: Ablauf in Tagen, Berechtigung auf „Anzeigen“	SharePoint Online	2	Ein Link ohne Ablaufdatum ist ein Passwort, das nie geändert wird – und das in einem WhatsApp-Verlauf, einer Mail-Signatur und einem Ticketsystem gleichzeitig liegt. Dreißig Tage sind ein üblicher, verträglicher Wert.
16	Teams-Föderation nach außen eingrenzen	Teams Admin Center › Benutzer › Externer Zugriff (Modus „Kontrolliert“ oder Positivliste erlaubter Domänen)	Teams (in jedem M365-Plan enthalten)	2	Ab Werk darf jede fremde Microsoft-365-Organisation deine Belegschaft anschauen. Phishing über den Teams-Chat umgeht jeden Mailfilter, den du gerade so sorgfältig auf „strikt“ gestellt hast.

Feld C ist das Feld, in dem Sicherheit und Zusammenarbeit am härtesten aufeinandertreffen. Wer hier zu grob vorgeht, erzeugt Schatten-IT schneller, als die Richtlinie greift: Was per SharePoint nicht geht, geht dann eben per privatem Cloudspeicher. Die differenzierte Variante – Freigabe erlauben, aber mit Ablauf, Authentifizierung und Protokoll – steht in [Gastzugriff und externe Freigaben härten](#). Für die Frage, was von den Daten selbst geschützt gehört und nicht nur der Weg dorthin, ist der [Kompetenzbereich Microsoft Purview](#) der richtige Einstieg.

Feld D: Endgerät, Protokoll und Alarm

Nr.	Schraube	Portal und Klickpfad	Lizenz	Pri o	Warum
17	ASR-Regeln aus dem Audit- in den Blockmodus	Defender-Portal › Endpunkte › Konfigurationsverwaltung › Angriffsflächenreduzierung; alternativ Intune › Endpunktsicherheit › Angriffsflächenreduzierung	Defender für Endpunkt P1/P2 oder Defender for Business	2	Die Standardschutzregeln lassen sich laut Microsoft in der Regel ohne Vorabtest blockend setzen. Alle übrigen gehören erst in den Audit-Modus – sonst blockierst du am Montag das Warenwirtschaftssystem.
18	Manipulationsschutz einschalten	Defender-Portal › Einstellungen › Endpunkte › Erweiterte Features › Manipulationsschutz	Defender für Endpunkt oder Defender for Business	1	Ohne Manipulationsschutz schaltet die Schadsoftware den Virenschutz ab, bevor du die erste Warnung siehst. Ein Schalter, keine Nebenwirkungen, fünf Sekunden Arbeit.
19	Einheitliches Überwachungsprotokoll einschalten	Purview-Portal › Lösungen › Überwachung › Suchen (Schaltfläche zum Starten der Aufzeichnung)	Standard 180 Tage; mit E5 ein Jahr für Entra, Exchange und SharePoint	1	Bei den Business-Lizenzen und bei Testtenants ist die Aufzeichnung nicht automatisch aktiv. Ohne Protokoll gibt es im Ernstfall keine Forensik, sondern nur Vermutungen mit Zeitdruck.
20	Sicherheitswarnungen an ein Postfach, das jemand liest	Defender- bzw. Purview-Portal › Richtlinien › Warnungsrichtlinie › Empfänger auf ein gemeinsames Postfach mit klarer Zuständigkeit setzen	EOP (erweiterte Richtlinien: E5 bzw. Defender P2)	1	Warnungen an eine Adresse ohne Besitzer sind Selbstberuhigung mit Zeitstempel. Ein gemeinsames Postfach mit zwei benannten Personen und einer Vertretungsregel kostet zehn Minuten.

Schraube 20 ist die unspektakulärste der ganzen Liste und in der Praxis die, die am häufigsten fehlt. Wir haben Tenants gesehen, in denen die Warnungen seit achtzehn Monaten an eine Verteilerliste gingen, deren einziges Mitglied das Unternehmen verlassen hatte. Welche Richtlinien sich wirklich lohnen und welche nur Rauschen erzeugen, steht in [Alert Policies und Benachrichtigungen richtig aufsetzen](#). Für das Onboarding der Endgeräte, ohne dass die Belegschaft am nächsten Tag vor verschlossenen Anwendungen steht, gibt es [Defender for Endpoint: Onboarding ohne Drama](#).

WICHTIG · Protokollierung ist mitbestimmungsrelevant

Sobald du Anmeldeprotokolle, Alarme und Endgerätedaten zusammenführst, entsteht eine technische Einrichtung, die zur Verhaltens- und Leistungskontrolle geeignet ist. Ob du sie so nutzen willst, ist rechtlich unerheblich — geeignet genügt. In Betrieben mit Betriebsrat gehört das früh auf den Tisch, nicht nach dem Rollout.

Das ist kein Grund, auf Schraube 19 zu verzichten. Es ist ein Grund, die Auswertungszwecke schriftlich zu begrenzen, bevor jemand anders sie für dich definiert.

› [Security-Monitoring und Betriebsrat: was mitbestimmungspflichtig ist](#)

Ein Nachmittag: die fünf mit der größten Wirkung

Zwanzig Schrauben klingen nach einem Quartal. Sind sie auch, wenn man alles sauber macht. Aber fünf davon lassen sich an einem Nachmittag drehen und verschieben das Risiko so deutlich, dass sich der Rest danach in Ruhe planen lässt. Die Auswahl folgt einem einfachen Kriterium: hohe Wirkung, überschaubarer Abstimmungsbedarf, keine harte Abhängigkeit von einem Projektplan.

Ein Nachmittag: die fünf mit der größten Wirkung

Realistischer Zeitplan für einen mittelständischen Tenant, inklusive Kaffee und einer Panik



Danach: Audit-Log prüfen, Warnungsrichtlinie auf ein Postfach legen, das jemand liest. Das ist der sechste Punkt, der eigentlich der erste war.

Skizze 4: Ein realistischer Nachmittag. Die Reihenfolge ist nicht verhandelbar — Break-Glass zuerst.

13:30 Uhr — Break-Glass, bevor irgendetwas anderes passiert

Zwei reine Cloud-Konten auf der onmicrosoft-Domain, keine Namen, die auf Personen schließen lassen, sehr lange Passwörter, ausgenommen von allen Richtlinien für bedingten Zugriff. Anschließend eine Warnungsregel, die bei jeder Anmeldung dieser Konten anschlägt. Microsoft empfiehlt phishing-resistente Verfahren für diese Konten, also FIDO2-Sicherheitsschlüssel oder zertifikatsbasierte Anmeldung — und zwar bewusst ein anderes Verfahren als bei den normalen Administratorkonten, damit ein Ausfall des einen nicht beide lahmlegt.

Das dauert zwanzig Minuten und ist die Versicherung für alles, was danach kommt. Wer diesen Schritt überspringt, weil er „nur schnell“ eine Richtlinie bauen will, hat statistisch gute Chancen, den Rest des Nachmittags in einer Support-Warteschleife zu verbringen.

14:00 Uhr — Legacy Authentication blockieren

Zuerst nachsehen, wer das überhaupt noch benutzt: In den Anmeldeprotokollen lässt sich nach Clientanwendungen filtern, die nicht auf modernem Weg authentifizieren. Die Trefferliste ist erfahrungsgemäß kurz und besteht aus einem Multifunktionsgerät im dritten Stock, einer Zeiterfassung und einem Skript, das jemand 2018 geschrieben hat. Dann die Richtlinie im Report-only-Modus anlegen, ein bis zwei Tage beobachten, danach aktivieren.

Wer schneller sein will, kann die Richtlinie sofort aktivieren und die gefundenen Ausnahmen einzeln freistellen. Das ist die ehrlichere Variante, weil sie die Ausnahmen sichtbar macht statt sie unter einem Report-only-Modus zu begraben, der nie ausgewertet wird.

15:00 Uhr — MFA für alle, inklusive der Administratoren

Eine Richtlinie, alle Benutzer, alle Cloud-Apps, Gewährungssteuerung auf Multifaktor-Authentifizierung. Die Break-Glass-Konten sind ausgenommen, sonst niemand. Für Azure- und Verwaltungszugriffe hat Microsoft die Frage ohnehin entschieden: Seit Oktober 2024 gilt MFA-Pflicht für die Anmeldung an den Verwaltungsportalen, und seit Oktober 2025 wird sie schrittweise auch für schreibende Zugriffe über Azure CLI, Azure PowerShell, SDKs, Infrastructure-as-Code-Werkzeuge und die REST-Schnittstellen durchgesetzt. Lesende Zugriffe bleiben ausgenommen. Wer dafür mehr Zeit brauchte, konnte eine Verschiebung bis Juli 2026 beantragen — dieser Zug ist inzwischen abgefahren.

Das Nutzererlebnis entscheidet über den Erfolg. Wer die Registrierung der Methoden ohne Vorwarnung erzwingt, erzeugt am Montagmorgen eine Telefonlawine. Wer zwei Wochen vorher informiert, eine Kurzanleitung mit drei Bildern verschickt und in der ersten Woche eine Sprechstunde anbietet, kommt mit erstaunlich wenig Reibung durch. Details dazu in [MFA in Microsoft 365 richtig einführen](#); wenn du gleich einen Schritt weiter gehen willst, ist [Passwordless: FIDO2 und Passkeys in der Praxis](#) der Anschluss.

16:15 Uhr — Voreingestellte Sicherheitsrichtlinien auf „Strikt“

Im Defender-Portal die voreingestellten Sicherheitsrichtlinien öffnen und alle Empfänger in „Strikt“ aufnehmen. Das ist die seltene Situation, in der die aggressivere Einstellung weniger Arbeit macht als die vorsichtige: Microsoft pflegt die Schwellwerte nach, du musst keine eigenen Anti-Spam- und Anti-Phishing-Richtlinien mehr betreuen, und die Voreinstellungen haben Vorrang vor allen selbstgebaute Regeln.

Der spürbare Unterschied zwischen „Standard“ und „Strikt“ liegt beim Umgang mit erkanntem Spam: Standard verschiebt in den Junk-Ordner, Strikt stellt in die Quarantäne. Das bedeutet, dass jemand die Quarantäne betreuen muss. Genau deshalb steht Schraube 20 auf derselben Prioritätsstufe.

17:00 Uhr — automatische Weiterleitung nach außen abschalten

In der ausgehenden Spamfilterrichtlinie die automatische Weiterleitung explizit auf „Aus“ setzen, statt es beim systemgesteuerten Standard zu belassen. Microsoft selbst empfiehlt, den Wert bewusst zu setzen, weil das Verhalten sonst je nach Organisation abweicht. Wer legitime Weiterleitungen hat — typischerweise Funktionspostfächer, die an einen Dienstleister gehen —, legt dafür eine zweite Richtlinie mit engem Geltungsbereich an. Nicht umgekehrt.

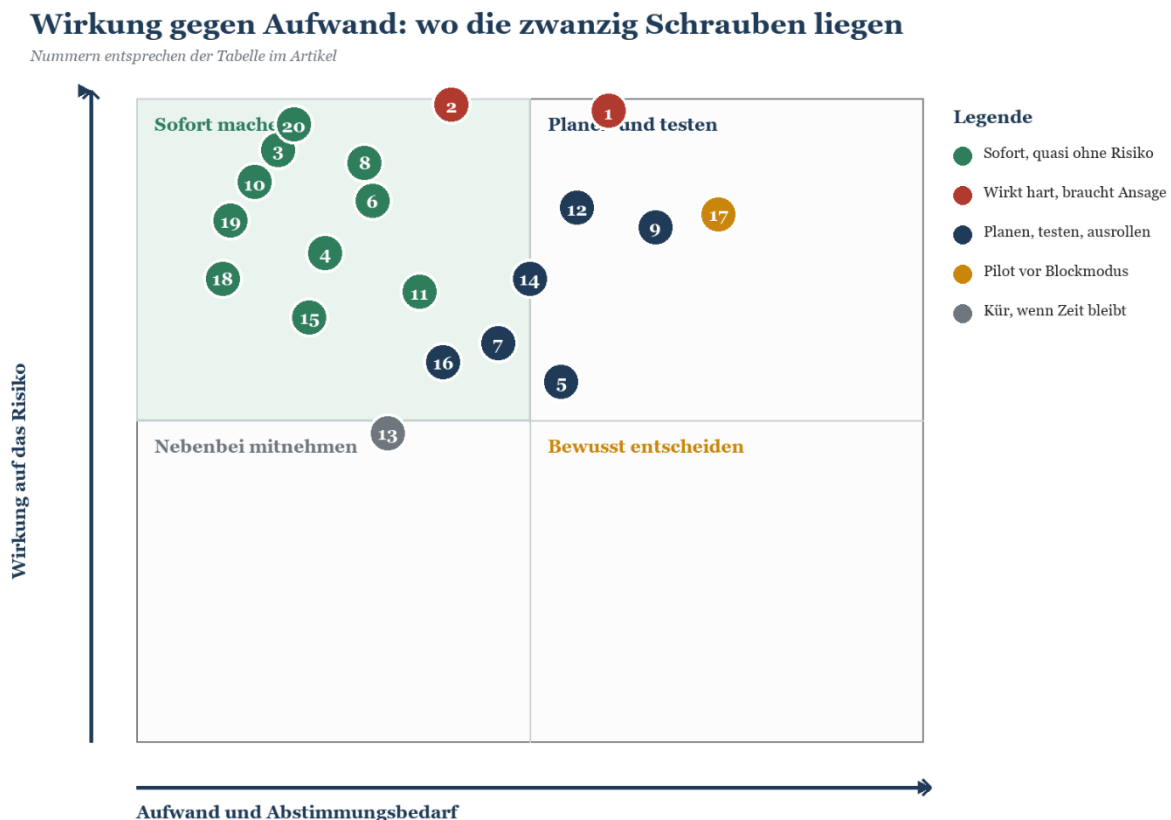
TIPP · Der sechste Punkt, der eigentlich der erste ist

Wenn der Nachmittag gut läuft, bleibt noch eine halbe Stunde. Nutze sie für Schraube 19 und 20: nachsehen, ob das einheitliche Überwachungsprotokoll läuft, und die Warnungsrichtlinien auf ein Postfach legen, in das tatsächlich jemand schaut. Beides zusammen kostet weniger Zeit als die Kaffeepause, entscheidet aber darüber, ob du einen späteren Vorfall rekonstruieren kannst oder ob du raten musst.

Ohne Protokoll ist jede Untersuchung eine Meinungsäußerung mit Rechnungsstellung.

Wirkung gegen Aufwand: was wann drankommt

Nicht jede Schraube verdient dieselbe Aufmerksamkeit. Manche wirken sofort und kosten nichts außer einem Klick — Manipulationsschutz und Überwachungsprotokoll gehören dazu. Andere wirken ebenso stark, brauchen aber eine Ansage an die Belegschaft und einen Termin: MFA und Legacy Auth. Und wieder andere verlangen einen Pilotbetrieb, bevor du sie blockend setzt, weil sie sonst Produktion verhindern statt Angriffe.



Skizze 5: Die zwanzig Schrauben nach Wirkung und Aufwand. Links oben wird zuerst gedreht.

Was du in der ersten Woche schaffst

- Break-Glass-Konten anlegen und mit einer Warnungsregel versehen (Schraube 3).
- Zählen, wie viele globale Administratoren existieren, und begründen, warum jeder Einzelne die Rolle braucht (Schraube 4).
- Manipulationsschutz einschalten und Überwachungsprotokoll prüfen (Schrauben 18 und 19).
- Automatische Weiterleitung nach außen explizit abschalten und bestehende Regeln durchsehen (Schrauben 10 und 11).

- Benutzereinwilligung für Apps einschränken und den Genehmigungsablauf aktivieren (Schraube 6).
- Warnungsrichtlinien auf ein betreutes Postfach legen (Schraube 20).

Was einen Termin und eine Ansage braucht

MFA für alle, das Abschalten von Legacy Authentication, die Umstellung der Freigabestufen und die DMARC-Rampe verändern Arbeitsabläufe. Für diese Schrauben brauchst du zwei Dinge: einen Zeitpunkt, der nicht auf den Quartalsabschluss fällt, und eine Nachricht, die erklärt, was passiert, ohne die Belegschaft zu belehren. Der Satz „ab Dienstag brauchst du dein Handy beim Anmelden, hier sind drei Bilder“ wirkt besser als jede Schulungsfolie über Bedrohungslagen.

Wenn du das Ganze regelmäßig überprüfen willst, ohne dich an einer Punktzahl festzubeißen, hilft [Secure Score: sinnvoll nutzen statt Punktejagd](#). Die Härtung ist außerdem die technische Grundlage für mehrere Nachweispflichten — welche Maßnahmen in Microsoft 365 sich konkret auf die Anforderungen abbilden lassen, steht in [NIS2 aus Security-Sicht: technische Maßnahmen in M365](#). Und für die Frage, wie du das Ergebnis nach oben verkaufst, ohne in Fachjargon zu verfallen: [Security-Reporting für die Geschäftsführung](#).

Die drei häufigsten Bremsen

Bremse	Wie sie klingt	Was tatsächlich hilft
Der Dienstleister	„Unsere Branchensoftware kann kein OAuth, da müssen wir Basic Auth anlassen.“	Terminierte Ausnahme mit Namen, Datum und Ticketnummer. Eine Ausnahme ohne Enddatum ist keine Ausnahme, sondern der neue Normalzustand. Der Hersteller bekommt eine schriftliche Frist.
Der Vorstand	„Das darf die Arbeit nicht behindern, wir haben gerade Hochsaison.“	Die fünf Nachmittagsschrauben behindern niemanden außer Angreifern. Für den Rest einen Termin nach der Saison verbindlich festlegen — schriftlich, mit Datum.
Die eigene Gründlichkeit	„Wir machen das richtig, sobald das Konzept steht.“	Schraube 18 dauert fünf Sekunden. Ein Konzept, das das Einschalten des Manipulationsschutzes um vier Monate verzögert, ist kein Konzept, sondern ein Alibi.

Nach der Härtung: dranbleiben, ohne zu ersticken

Ein gehärteter Tenant bleibt nicht von allein gehärtet. Microsoft liefert neue Funktionen aus, Kolleginnen und Kollegen bekommen Ausnahmen, Projekte legen Gastkonten an, und irgendwann steht die Freigabestufe wieder auf „Jeder“, weil es für eine Ausschreibung schnell gehen musste. Härtung ist deshalb kein Projekt mit Abschlussbericht, sondern ein wiederkehrender Termin.

Ein Quartalstermin, neunzig Minuten

- Wie viele globale Administratoren gibt es heute? Sind es mehr als beim letzten Mal?
- Welche Ausnahmen stehen in den Richtlinien für bedingten Zugriff, und welche davon haben ein abgelaufenes Enddatum?
- Wie viele Gastkonten sind seit über neunzig Tagen ohne Anmeldung?
- Welche Apps haben im letzten Quartal Berechtigungen erhalten, und wer hat zugestimmt?
- Laufen die Warnungsrichtlinien noch in ein Postfach, das jemand liest — und ist diese Person noch im Unternehmen?

- Steht die automatische Weiterleitung nach außen noch auf „Aus“?

Wenn du diese sechs Fragen viermal im Jahr ehrlich beantwortest, bist du weiter als die meisten Häuser mit einem dreistelligen Werkzeugbudget. Der nächste Reifegrad ist dann nicht die nächste Lizenz, sondern die Übung: einen Vorfall einmal durchspielen, bevor er echt ist. Wie das aussieht, steht in [Phishing-Vorfall: die ersten 60 Minuten](#) und in [Incident-Response-Plan für Microsoft 365](#). Wer das Thema pragmatisch statt dogmatisch weiterdenken will, findet den Rahmen in [Zero Trust im Mittelstand: pragmatisch statt dogmatisch](#).

FAKTEN · Härtung ersetzt keine Wiederherstellung

Alle zwanzig Schrauben zusammen senken die Wahrscheinlichkeit eines Vorfalls erheblich. Sie senken sie nicht auf null, und sie ersetzen kein Backup. Die Aufbewahrungsfunktionen in Microsoft 365 sind Aufbewahrung, keine Sicherung: Sie schützen vor dem versehentlichen Löschen, nicht vor einem Angreifer mit Administratorrechten und Zeit.

Wer die Härtung ernst nimmt, klärt im selben Zug die Frage, wie lange die Wiederherstellung dauert und wer sie schon einmal geübt hat.

› [Ransomware-Vorsorge in Microsoft 365](#)

Häufige Fragen

Reichen die Sicherheitsstandards nicht aus, wenn wir keine P1-Lizenzen haben?

Für einen kleinen Tenant ohne Sonderfälle sind die Sicherheitsstandards ein guter Anfang: Sie erzwingen MFA-Registrierung, blockieren Legacy Authentication und verlangen MFA für privilegierte Aktionen. Ihr Nachteil ist die Alles-oder-nichts-Logik — du kannst keine Ausnahmen definieren, außer den Standards komplett abzuschalten. Sobald du ein Dienstkonto, einen Standortfilter oder ein abweichendes Verhalten für Administratoren brauchst, führt der Weg zu Entra ID P1 und eigenen Richtlinien. Die Abwägung ist ausführlich beschrieben, der Kurzsatz lautet: Sicherheitsstandards sind besser als nichts und schlechter als eine durchdachte Baseline.

Wie viele der zwanzig Schrauben brauchen zusätzliche Lizenzen?

Rund die Hälfte funktioniert mit jeder Lizenzstufe: Break-Glass-Konten, Administratorenzahl, Einwilligungseinstellungen, Freigabestufen, anonyme Links, Teams-Föderation, Weiterleitungen, Legacy-Protokolle, PowerShell-Zugriff, Überwachungsprotokoll und Warnungsrichtlinien in der Grundvariante. Für den bedingten Zugriff — und damit für die Schrauben 1 und 2 in ihrer sauberen Form — brauchst du Entra ID P1. Zugriffsüberprüfungen für Gastkonten setzen P2 voraus. Manipulationsschutz und ASR-Regeln setzen Defender für Endpunkt oder Defender for Business voraus, was in Microsoft 365 Business Premium enthalten ist.

Wir haben Business Premium. Ist das genug?

Für den Mittelstand ist Business Premium erstaunlich vollständig: bedingter Zugriff, Defender for Business, Intune und Defender für Office 365 Plan 1 sind enthalten. Achte auf zwei Dinge. Erstens ist die Überwachungsaufzeichnung bei den Business-Lizenzen nicht automatisch aktiv — Schraube 19 ist bei dir also keine Formalität, sondern echte Arbeit. Zweitens fehlen die Zugriffsüberprüfungen aus Entra ID P2, sodass der Gästebefugnis aus Schraube 7 über eine manuelle Routine oder ein Skript laufen muss. Beides ist lösbar, aber beides muss jemand wissen.

Was passiert, wenn wir Legacy Authentication einfach abschalten?

In einem typischen Mittelstandstenant fallen drei bis fünf Dinge aus, und zwar zuverlässig dieselben: ein Multifunktionsdrucker, der per SMTP an Postfächer sendet, eine Fachanwendung mit fest verdrahtetem Postausgang, ein altes Mobilgerät mit dem eingebauten Mailprogramm, und ein Skript ohne Besitzer. Deshalb der Report-only-Modus vor der Aktivierung: Er zeigt dir die Liste, bevor sie sich am Telefon meldet. Wichtig ist die Unterscheidung zwischen Legacy Authentication im bedingten Zugriff und SMTP AUTH für den Versand — das sind zwei verschiedene Baustellen, und die zweite hat ihren eigenen Zeitplan.

Ab wann darf SMTP AUTH mit Basisauthentifizierung nicht mehr benutzt werden?

Microsoft hat den Zeitplan mehrfach verlängert. Der aktuelle Stand: Bis einschließlich Dezember 2026 bleibt das Verhalten unverändert. Ende Dezember 2026 wird die Basisauthentifizierung für SMTP AUTH bei bestehenden Tenants standardmäßig deaktiviert, lässt sich von Administratoren aber weiterhin einschalten. Für Tenants, die danach neu angelegt werden, steht sie gar nicht mehr zur Verfügung. Ein endgültiges Abschaltdatum will Microsoft in der zweiten Jahreshälfte 2027 nennen. Übersetzt heißt das: Du hast noch Zeit, aber nicht beliebig viel, und das Umstellen von Geräten und Fachanwendungen auf OAuth dauert länger, als der Hersteller behauptet.

Sollen wir DMARC direkt auf p=reject setzen?

Nein. Microsoft empfiehlt ausdrücklich den stufenweisen Weg über p=none und p=quarantine, und dieser Rat ist keine Höflichkeit. In fast jedem Unternehmen versenden mehr Systeme in eigenem Namen als bekannt ist: das Newsletter-Werkzeug, das Bewerbungsportal, die Buchhaltungssoftware, der Ticketdienst. Mit p=none sammelst du die Berichte ein und findest heraus, wer das alles ist. Erst danach ziehst du an. Wer direkt auf p=reject springt, erfährt es daran, dass die Rechnungen nicht mehr ankommen — meistens am Monatsende.

Wie viele globale Administratoren sind vertretbar?

Microsoft empfiehlt weniger als fünf Personen in dieser Rolle, dazu die zwei Notfallkonten. In der Praxis kommen Häuser bis etwa fünfhundert Beschäftigte mit zwei bis drei benannten Personen aus, wenn die übrigen Aufgaben über spezialisierte Rollen laufen — Exchange-Administrator, Sicherheitsadministrator, Helpdesk-Administrator. Der Test ist simpel: Wenn du bei einem Konto überlegen musst, warum es die Rolle hat, hat es sie zu Unrecht.

Müssen wir die ASR-Regeln wirklich einzeln testen?

Nicht alle. Microsoft benennt eine Gruppe von Standardschutzregeln, die sich in der Regel ohne Vorabtest direkt im Block- oder Warnmodus aktivieren lassen. Für die übrigen gilt: erst Audit-Modus, dann die Berichte ansehen, dann blockend setzen. Die Regeln, die erfahrungsgemäß am ehesten legitime Abläufe treffen, sind die zu Office-Kindprozessen und zu Skripten — genau dort, wo Fachanwendungen gerne mit Makros und generierten Dokumenten arbeiten. Zwei Wochen Audit-Modus sind ein guter Kompromiss zwischen Gründlichkeit und Geduld.

Was ist mit dem Betriebsrat?

Die Härtingsmaßnahmen selbst sind überwiegend unkritisch — eine Freigabeeinstellung überwacht niemanden. Kritisch wird es bei den Schrauben 19 und 20 sowie beim Endgeräteschutz, weil dort Daten entstehen, die geeignet sind, Verhalten und Leistung zu kontrollieren. Der pragmatische Weg: früh informieren, die Auswertungszwecke schriftlich begrenzen, Zugriff auf die Protokolle auf benannte Rollen beschränken und protokollieren, wer auswertet. Das kostet zwei Sitzungen und erspart dir eine Einigungsstelle.

Wir haben schon einen Vorfall gehabt. Ist die Liste trotzdem richtig?

Die Reihenfolge ändert sich. Nach einem Vorfall gehören zuerst die Fragen geklärt, ob der Zugang wirklich geschlossen ist: bestehende Regeln und Weiterleitungen, erteilte App-Berechtigungen, angelegte Zusatzkonten, geänderte MFA-Methoden. Erst danach kommt die Grundhärtung. Der Grund ist unangenehm einfach — wer härtet, ohne den Zugang zu schließen, sperrt den Angreifer mit ein, nicht aus.

Fazit

Tenant-Härtung ist unspektakulär. Es gibt keinen Moment, in dem ein Balken grün wird und jemand klatscht. Es gibt zwanzig Einstellungen, von denen fünfzehn in einer Woche zu schaffen sind, und fünf, die einen Termin und eine freundliche Ansage brauchen. Zusammen verschieben sie die Frage von „wann trifft es uns“ zu „wie teuer wird es, wenn es uns trifft“ — und das ist der einzige Fortschritt, den man in diesem Feld realistisch anbieten kann.

Wenn du nur drei Dinge aus diesem Text mitnimmst: Lege zuerst die Break-Glass-Konten an. Schalte das Überwachungsprotokoll ein, bevor du es brauchst. Und Sorge dafür, dass die Warnungen in einem Postfach landen, das ein Mensch mit Namen und Vertretung liest. Alles andere ist wichtig. Diese drei sind die Voraussetzung dafür, dass „alles andere“ überhaupt etwas nützt.

Und ja, die Liste ist nicht vollständig. Sie ist absichtlich nicht vollständig. Eine vollständige Liste wird nicht abgearbeitet, sondern abgeheftet. Zwanzig Schrauben werden gedreht.

TIPP • Weiterlesen und weiterkommen

Dieser Beitrag ist der Einstieg in das Handlungsfeld Tenant-Härtung. Die einzelnen Schrauben haben eigene Beiträge, in denen die Fallstricke stehen, die hier keinen Platz hatten:

- › [Legacy Authentication endgültig abschalten](#)
- › [Conditional Access: Baselines, die nicht nerven](#)
- › [App-Registrierungen und Consent-Governance](#)
- › [Gastzugriff und externe Freigaben härten](#)
- › [Dossier: TerminalFix und der Berlin-Hack](#)

Wenn die zwanzig Schrauben in deinem Haus auf zwanzig Diskussionen hinauslaufen, statt auf zwanzig erledigte Punkte, liegt das selten an der Technik. Dafür gibt es die [Beratung zu Microsoft 365 Security](#) — und wenn das Team die Zusammenhänge selbst beherrschen soll, statt sie sich erklären zu lassen, die [Schulung Microsoft 365 Security](#).