

Secure Score: sinnvoll nutzen statt Punktejagd

Es gibt eine Sorte Kennzahl, die in Unternehmen ein erstaunliches Eigenleben entwickelt. Sie wird eingeführt, um etwas sichtbar zu machen, und nach sechs Monaten arbeiten alle daran, die Zahl zu bewegen, statt an dem, was die Zahl eigentlich abbilden sollte. Der Microsoft Secure Score ist ein Musterexemplar dieser Gattung. Er steht im Defender-Portal, er ist gut gemeint, er ist handwerklich solide gebaut – und er wird täglich missbraucht.

Der typische Verlauf sieht so aus: Die Geschäftsführung sieht in einer Präsentation die Zahl 38 Prozent, erschrickt, und fragt, wann denn 100 Prozent erreicht seien. Die IT antwortet pflichtbewusst mit einem Zeitplan. Vier Monate später steht der Score bei 71 Prozent, es hat niemand die Legacy-Authentifizierung abgeschaltet, dafür sind vierzig Richtlinien aktiv, die kein Mensch je geprüft hat, und beim nächsten Phishing-Vorfall fällt auf, dass die Angreifer über genau den Weg hereinkamen, den man aus Bequemlichkeit auf „Risiko akzeptiert“ gesetzt hatte. Der Score war die ganze Zeit grün. Das ist das Perfide daran: Er hat nicht gelogen. Er wurde nur falsch gelesen.

Dieser Beitrag zeigt dir, was der Score misst und was nicht, warum 100 Prozent kein sinnvolles Ziel ist, welche empfohlenen Aktionen tatsächlich Angriffe verhindern und welche reine Kosmetik sind, wie du den Status „Resolved through alternate mitigation“ benutzt, ohne dich selbst zu belügen, und wie du aus dem Score ein Berichtsinstrument machst, das in der Geschäftsführung eine echte Diskussion auslöst statt eines zufriedenen Nickens.

Dieser Beitrag gehört zum Handlungsfeld „Steuerung und Nachweis“ unserer Serie zum Thema [Microsoft 365 Security](#). Wenn du gerade erst anfängst und noch keine Baseline hast, dreh die Reihenfolge um: erst die Schrauben aus der [Tenant-Härtung: die 20 wichtigsten Schrauben](#), dann der Score als Kontrolle. Andersherum jagst du Punkte hinterher, statt Angriffswege zu schließen.

Was der Score wirklich misst – und was er dir verschweigt

Die Mechanik in drei Sätzen

Microsoft Secure Score ist eine Zusammenfassung deiner Sicherheitskonfiguration als Zahl. Du bekommst Punkte dafür, dass du empfohlene Sicherheitsfunktionen einschaltest, sicherheitsbezogene Tätigkeiten erledigst oder eine Empfehlung nachweislich mit einem Fremdprodukt beziehungsweise einer eigenen Maßnahme abdeckst. Jede einzelne empfohlene Aktion ist höchstens zehn Punkte wert, und die meisten werden binär bewertet: umgesetzt oder nicht. Ein Teil wird anteilig gerechnet – wenn du 50 von 100 Konten mit MFA schützt und die Aktion zehn Punkte wert ist, bekommst du fünf.

Der angezeigte Wert aktualisiert sich in der Oberfläche nahezu in Echtzeit, die tatsächliche Punkteverrechnung läuft über einen täglichen Abgleich. Rechne nach einer Änderung mit 24 bis 48 Stunden, bis der Punktwert steht. Bei Empfehlungen zu Microsoft Teams und Microsoft Entra kommt hinzu, dass der Zustand zusätzlich in einem monatlichen beziehungsweise wöchentlichen Rhythmus aufgefrischt wird. Wer eine Stunde nach dem Klick eine Krisensitzung einberuft, weil die Zahl sich nicht bewegt hat, hat zu viel Zeit.

Vier Kategorien, ein Zahlenwert

Die empfohlenen Aktionen sind in vier Gruppen sortiert: Identity für Konten und Rollen in Microsoft Entra ID, Device für Microsoft Defender for Endpoint, Apps für E-Mail und Cloud-

Anwendungen einschließlich Defender for Cloud Apps, und Data für die Informationsklassifizierung aus Microsoft Purview. Diese Aufteilung ist nicht statisch: Im April 2026 hat Microsoft mehrere Empfehlungen aus der Kategorie Cloud Apps als identitätsbezogen neu einsortiert. Die Gesamtsumme blieb gleich, die Teilwerte für Identity und Apps haben sich verschoben. Wer seine Berichte auf Kategoriewerte stützt, hatte an dem Tag eine unerklärliche Abweichung im Quartalsbericht.

Wichtiger als die Kategorien ist die Produktliste. Secure Score bewertet heute unter anderem Microsoft Entra ID, Exchange Online, SharePoint Online, Microsoft Teams, Defender for Endpoint, Defender for Identity, Defender for Office, Defender for Cloud Apps, App Governance und Microsoft Purview Information Protection – und dazu eine wachsende Liste von Fremdanwendungen wie Salesforce, ServiceNow, Okta, GitHub, Zoom, Docusign oder Citrix ShareFile, sofern du die entsprechenden Konnektoren angebunden hast, wie im Beitrag zu Defender for Cloud Apps beschrieben.

Nachzulesen unter [Defender for Cloud Apps im Mittelstand](#). Seit dem 30. Juni 2026 wirken zusätzlich über 200 neue AWS- und GCP-Empfehlungen aus der erweiterten Multicloud-Abdeckung auf den Score. Wenn dein Wert an dem Tag gefallen ist, ist nicht dein Tenant schlechter geworden – der Betrachtungsrahmen ist größer geworden.

Die blinden Flecken

Microsoft schreibt es selbst in die Dokumentation, und man kann es nicht oft genug wiederholen: Der Secure Score ist keine Aussage darüber, wie wahrscheinlich ein Einbruch in deine Systeme ist. Er misst, in welchem Umfang du Sicherheitsfunktionen in deiner Microsoft-Umgebung benutzt, die das Risiko senken können. Das ist etwas anderes. Alles, was außerhalb der bewerteten Produkte liegt, kommt in der Zahl schlicht nicht vor – und das ist in einem mittelständischen Unternehmen typischerweise die Hälfte des Problems.

Was der Secure Score abdeckt – und was außerhalb liegt



- | | | |
|--------------------------------|----------------------------------|---------------------------------|
| ✗ Backup und Wiederanlauf | ✗ Netzsegmentierung, OT, Drucker | ✗ Prozesse, Notfallplan, Übung |
| ✗ Patchstand von Fremdsoftware | ✗ Awareness und Meldekultur | ✗ Lieferanten und Dienstleister |

Skizze 1: Der Score bewertet einen Ausschnitt. Die Ränder deiner Sicherheitslage liegen außerhalb.

FAKTEN: Was der Score strukturell nicht sehen kann

Ob deine Sicherungen wiederherstellbar sind. Ein Backup, das nie zurückgespielt wurde, ist eine Hoffnung, keine Maßnahme.

Ob deine Netzwerksegmentierung existiert, ob die Produktionsanlage im selben Broadcast-Segment hängt wie die Buchhaltung, ob der Drucker noch SNMP mit „public“ spricht.

Ob deine Belegschaft weiß, wo sie einen Verdachtsfall meldet, und ob die Meldung außerhalb der Kernarbeitszeit jemanden erreicht.

Ob deine Lieferanten und Dienstleister Zugriff auf Daten haben, den niemand mehr überprüft hat.

Ob die Richtlinie, für die du Punkte bekommen hast, auch die richtigen Konten erfasst – der Score sieht das Vorhandensein, nicht die Wirksamkeit im Ausschluss.

Der letzte Punkt ist der teuerste. Eine Conditional-Access-Richtlinie, die MFA verlangt, aber vierzehn Ausnahmen für „Projektkonten“ enthält, ist im Score eine erfolgreich umgesetzte Aktion. In der Realität ist sie ein Türsteher, der jeden durchwinkt, der behauptet, auf der Liste zu stehen.

Wie man Ausnahmen sauber baut und wieder loswird, steht im Beitrag [Conditional Access: Baselines, die nicht nerven](#). Wer zusätzlich einen Alarm auf genau solche Ausnahmen legen will, findet den Weg in [Alert Policies und Benachrichtigungen richtig aufsetzen](#).

Warum 100 Prozent kein Ziel ist

Der Nenner ist beweglich

Der Score wird als Prozentwert dargestellt: erreichte Punkte geteilt durch erreichbare Punkte. Der Zähler liegt in deiner Hand. Der Nenner nicht. Microsoft zeigt dir grundsätzlich den vollständigen Satz möglicher Empfehlungen für ein Produkt, unabhängig davon, welche Lizenzedition du hast. Das ist bewusst so gebaut, damit du siehst, was gute Praxis wäre – aber es bedeutet, dass ein Tenant mit Business Premium strukturell niemals dieselbe Prozentzahl erreichen kann wie einer mit E5 plus vollständig angebundenen Konnektoren.

Dazu kommt die zeitliche Komponente. Microsoft ergänzt laufend neue empfohlene Aktionen. Im Februar 2026 kamen etwa Empfehlungen dazu, den Dienst Remoteregistrierung auf Windows-Systemen abzuschalten und die NTLM-Authentifizierung für Windows-Arbeitsplätze zu deaktivieren. Beides sind sinnvolle Maßnahmen – und beides hat bei allen, die sie noch nicht umgesetzt hatten, den Prozentwert gesenkt, ohne dass sich im Tenant irgendetwas verschlechtert hätte. Wenn dein Score im Quartalsbericht fällt, ist die erste Frage nicht „Was haben wir kaputt gemacht?“, sondern „Was hat Microsoft ergänzt?“.

WARNUNG: Punkte für aktivierte Lizenzen, die nichts tun

Der häufigste und unangenehmste Selbstbetrug beim Secure Score ist der Lizenz-Reflex. Eine Empfehlung lautet sinngemäß „Stelle sicher, dass Defender for Cloud Apps aktiviert ist“. Du klickst auf Aktivieren, der Dienst ist vorhanden, die Punkte werden gutgeschrieben. Was tatsächlich passiert ist: nichts. Kein Konnektor konfiguriert, keine Richtlinie definiert, kein Alarm verkabelt, niemand zuständig.

Dasselbe Muster gibt es an mehreren Stellen: Defender for Identity mit installiertem Sensor, aber ohne dass jemand die Meldungen liest. Eine Safe-Attachments-Richtlinie, die existiert, aber im Überwachungsmodus statt im Blockiermodus läuft. Eine DLP-Richtlinie, die nur für eine Testgruppe

von drei Personen greift. Purview-Kennzeichnungen, die veröffentlicht sind, aber die niemand vergibt.

In allen Fällen hältst du Punkte in der Hand, die dir vorspiegeln, ein Risiko sei behandelt. Das ist schlechter als gar keine Punkte, weil du in der nächsten Runde der Priorisierung nicht mehr hinschaust. Merke: Der Score bewertet, dass ein Schalter umgelegt ist. Ob dahinter jemand steht, der die Ausgabe liest, kann er nicht wissen.

Gegenmittel: Bei jeder Aktion, die durch reines Aktivieren einer Lizenz Punkte bringt, trägst du in die Notiz ein, wer die Ausgabe wie oft ansieht und wohin die Meldung geht. Wenn dir dazu nichts einfällt, hast du keine Maßnahme, sondern eine Rechnungsposition.

Drei Vergleichswerte, die ehrlicher sind als der Rohwert

Im Portal kannst du neben deinem aktuellen Wert weitere Sichten einblenden, und genau die gehören in jeden Bericht. Der nackte Rohwert allein gehört dort nämlich nicht hin.

Sicht im Portal	Was sie zeigt	Wofür du sie im Bericht brauchst
Your secure score	Erreichte Punkte im Verhältnis zu allen theoretisch möglichen Punkten, lizenzunabhängig.	Rohwert. Allein aussagelos, weil der Nenner Dinge enthält, die du gar nicht kaufen kannst.
Current license score	Was mit den tatsächlich vorhandenen Microsoft-Lizenzen erreichbar wäre.	Der einzig faire Maßstab für die Leistung des Betriebs. Diese Zahl gehört auf die Führungsfolie.
Achievable score	Erreichbar mit den vorhandenen Lizenzen unter Berücksichtigung der bewusst akzeptierten Risiken.	Zeigt, wie viel Luft nach oben tatsächlich noch da ist – ohne die Punkte, die ihr aus guten Gründen nie holen werdet.
Planned score	Prognose, wenn alle als „Planned“ markierten Aktionen fertig sind.	Verbindlichkeit. Wer hier eine Zahl nennt, hat sich auf einen Termin festgelegt.

Die Differenz zwischen „Current license score“ und „Achievable score“ ist übrigens die interessanteste Zahl im ganzen Portal. Sie ist die Summe der Risiken, die dein Unternehmen bewusst trägt. Wenn diese Differenz groß ist und niemand in der Geschäftsführung sie je gesehen hat, habt ihr ein Governance-Problem, kein Technikproblem.

Setz dir eine Zone, kein Maximum

Im Reiter Metrics & trends kannst du eine eigene Secure-Score-Zone definieren, also selbst festlegen, welcher Bereich für euch gut, akzeptabel und schlecht ist. Nutze das. Ein Mittelständler mit Microsoft 365 Business Premium, abgeschalteter Legacy-Authentifizierung, phishing-resistenter MFA für Administratoren und sauber gepflegten Defender-Richtlinien landet je nach Tenant-Zuschnitt irgendwo im Bereich zwischen 55 und 75 Prozent – und ist damit in der Praxis besser aufgestellt als ein E5-Kunde bei 80 Prozent, dessen Punkte überwiegend aus eingeschalteten, aber unbeaufsichtigten Diensten stammen.

TIPP: Die Zielzone einmal jährlich neu verhandeln

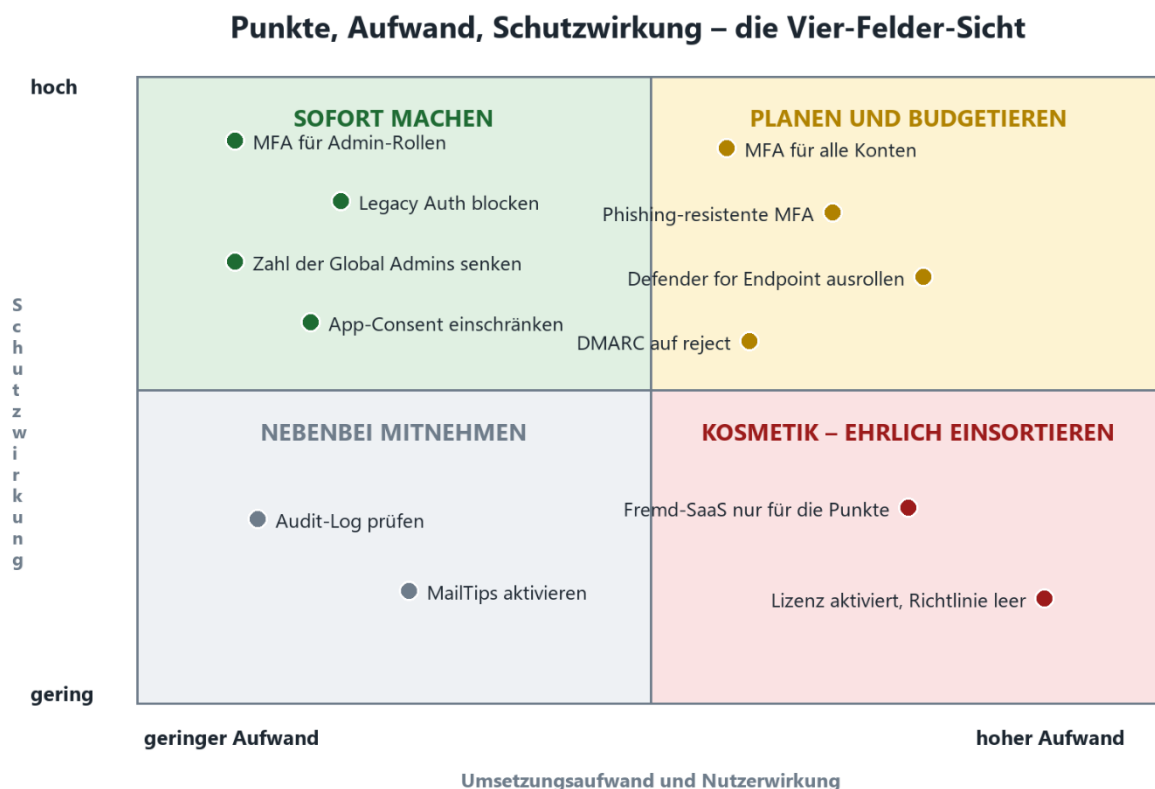
Definiere die Zone gemeinsam mit der Geschäftsführung und schreib den Beschluss auf: „Wir halten den Wert unter Berücksichtigung unserer Lizenzen zwischen X und Y Prozent. Unterhalb von X gibt es eine Sondermeldung.“ Damit ist die Frage nach den 100 Prozent ein für alle Mal beantwortet, und zwar bevor sie das erste Mal gestellt wird.

Überprüf die Zone einmal im Jahr. Wenn Microsoft den Nenner spürbar erweitert hat oder ihr Lizenzen gewechselt habt, ist die alte Zone nicht mehr die gleiche Aussage.

Welche Aktionen echten Schutz bringen – und welche Kosmetik sind

Die Rangfolge des Portals ist nicht deine Rangfolge

Das Portal sortiert die empfohlenen Aktionen nach verbleibenden Punkten, Umsetzungsschwierigkeit, Nutzerwirkung und Komplexität. Ganz oben landet also, was viele Punkte bringt und leicht ist. Das ist eine brauchbare Heuristik und genau deshalb gefährlich: Sie optimiert auf Punkte pro Aufwand, nicht auf verhinderten Schaden pro Aufwand. Diese beiden Größen fallen oft, aber eben nicht immer zusammen.



Skizze 2: Punkte allein sind eine Achse. Erst Schutzwirkung und Aufwand ergeben eine Entscheidung.

Die harte Wahrheit dahinter: Ein sehr kleiner Teil der Aktionen verhindert einen sehr großen Teil der real beobachteten Angriffe. Kontenmissbrauch über gestohlene Kennwörter, Legacy-Protokolle ohne zweiten Faktor, überprivilegierte Administratorkonten und bösartige App-Zustimmungen decken die Mehrheit dessen ab, was in mittelständischen Umgebungen tatsächlich schiefliegt. Alles andere ist wichtig, aber nachgeordnet.

Die 15 Aktionen mit dem besten Verhältnis von Punkten zu Aufwand

Die folgende Tabelle ist die Liste, die wir in Projekten tatsächlich abarbeiten. Die Punktzahlen sind Größenordnungen: Der exakte Wert hängt an deinem Tenant, an der anteiligen Bewertung und daran, was Microsoft zuletzt geändert hat. Die Reihenfolge ist bewusst nicht die des Portals.

Nr.	Empfohlene Aktion	Punkte (Größenordnung)	Aufwand	Was du vorher klären musst
1	MFA für alle Administratorrollen erzwingen	10	niedrig	Break-Glass-Konten vorher anlegen und ausnehmen
2	Legacy-Authentifizierung blockieren	7	niedrig bis mittel	Anmeldeprotokolle 30 Tage auswerten, Multifunktionsgeräte und Scan-to-Mail finden
3	Alle Benutzerkonten für MFA registrieren und erzwingen	bis 9, anteilig	mittel	Registrierungskampagne, Rufbereitschaft am Stichtag, Ersatzverfahren
4	Phishing-resistente MFA-Stärke für Administratoren fordern	bis 10	mittel	Schlüssel oder Passkeys beschaffen, Ersatzgerät je Person einplanen
5	Zahl der Konten mit Rolle Globaler Administrator senken	bis 10	niedrig	Rollen fachlich neu schneiden statt pauschal entziehen
6	Administrative Konten getrennt, cloudbasiert und ohne Postfach führen	bis 10	mittel	Notfallzugang und Kennwortablage vorher klären
7	Benutzerzustimmung für Anwendungen einschränken	bis 10	niedrig	Zustimmungsworkflow braucht Prüfer mit Reaktionszeit, sonst staut es sich
8	Administrator-Zustimmungsworkflow aktivieren	bis 10	niedrig	Ohne benannte Prüfer wird daraus ein Ticketfriedhof
9	Safe Links für E-Mail, Office-Anwendungen und Teams aktivieren	bis 10	niedrig	Ausnahmelisten aus der Altkonfiguration überprüfen
10	Safe Attachments einschließlich SharePoint, OneDrive und Teams	bis 10	niedrig	Blockiermodus statt Überwachung, sonst reine Punktebeschaffung
11	Anti-Phishing-Richtlinie mit Identitätswechsel-Schutz einrichten	mehrere Aktionen zu je 1 bis 5	mittel	Geschützte Personen und eigene Domänen sauber pflegen
12	Automatische externe Weiterleitung unterbinden	bis 10	niedrig	Bestehende Weiterleitungen vorher inventarisieren und einzeln klären
13	SPF, DKIM und DMARC für alle Domänen veröffentlichen	je Domäne mehrere Punkte	mittel	Alle sendenden Systeme finden, sonst kippt der Rechnungsversand
14	Gastfreigaben in SharePoint begrenzen, Weitergabe durch Gäste unterbinden	je 1 bis 8	niedrig	Bestehende Freigabelinks laufen weiter, separat aufräumen
15	Manipulationsschutz und Angriffsflächenreduzierung auf Endgeräten	je Regel wenige Punkte, in Summe zweistellig	mittel	Regeln zuerst im Überwachungsmodus, sonst blockierst du die Fachanwendung

Die Positionen 1 bis 6 sind der Kern. Wenn du nur eine Woche hast, machst du die und hörst dann auf. Details zur Einführung stehen in [MFA in Microsoft 365 richtig einführen](#), zum sauberen Abschalten der Altprotokolle in [Legacy Authentication endgültig abschalten](#), zu Schlüsseln und Passkeys in [Passwordless: FIDO2 und Passkeys in der Praxis](#) und zum Notfallzugang in [Break-Glass-Konten anlegen und überwachen](#). Positionen 7 und 8 behandelt [App-Registrierungen und Consent-Governance](#), die Positionen 9 bis 12 der Beitrag zu [Defender for Office 365: Safe Links und Safe Attachments](#) sowie [SPF, DKIM, DMARC für Exchange Online](#).

Kosmetik: Aktionen, die du gelassen einsortieren darfst

Nicht jede empfohlene Aktion verdient einen Sprint. Es gibt eine ganze Klasse von Empfehlungen, deren Schutzwirkung im Verhältnis zum organisatorischen Aufwand gering ist, und es ist völlig in

Ordnung, sie als „Planned“ mit großzügigem Termin oder als bewusst akzeptiertes Restrisiko zu führen. Der Fehler wäre, so zu tun, als gäbe es sie nicht.

Typ von Empfehlung	Warum sie im Score steht	Warum sie selten oben gehört
Kennwortablauf, Komplexitätsregeln und ähnliche Klassiker	Historisch gewachsene Empfehlungen aus Standardkatalogen.	Bringt wenig, wenn MFA und phishing-resistente Verfahren stehen. Kann die Belegschaft sogar zu schlechteren Kennwörtern treiben.
Empfehlungen für Fremd-SaaS, die du gar nicht nutzt	Konnektoren machen Produkte sichtbar, sobald sie angebunden sind.	Punkte für eine Anwendung, die bei euch drei Personen benutzen, verschieben die Prozentzahl, nicht das Risiko.
Einzelne Sicherheitshinweise und Anzeigoptionen in Outlook	Kleine Aktionen mit ein bis zwei Punkten, leicht umzusetzen.	Sinnvoll als Beifang, wenn du ohnehin in der Richtlinie bist. Kein eigenes Projekt wert.
Mobilgeräte-Empfehlungen aus dem Cloud-Apps-Konnektor	Kommen über die Geräteverwaltung mit, oft dutzendweise.	Wenn eure Geräteverwaltung ohnehin über Intune-Konfigurationsprofile läuft, ist das doppelte Buchführung. Alternative Mitigation mit Nachweis.
Empfehlungen mit hohem Nutzereingriff und geringem Angriffsbezug	Vollständigkeit des Katalogs.	Jede Maßnahme, die täglich Reibung erzeugt, kostet dich Akzeptanz, die du später für etwas Wichtigeres brauchst.

WICHTIG: Sicherheit gegen Benutzbarkeit – und wer das entscheidet

Microsoft formuliert es unaufgeregt: Sicherheit sollte immer gegen Benutzbarkeit abgewogen werden, und nicht jede Empfehlung passt in jede Umgebung. Genau das ist der Grund, warum „Risk accepted“ existiert. Der Fehler liegt nie im Akzeptieren, sondern darin, wer es tut: Wenn eine Person aus der IT-Administration im Alleingang Risiken akzeptiert, ist das keine Entscheidung, sondern eine Notlösung mit Haftungsfolge. Risiken akzeptiert die Leitung, dokumentiert, mit Datum und Wiedervorlage.

„Alternative Mitigation“ richtig nutzen

Die sechs Status im Klartext

Jede empfohlene Aktion trägt einen Status. Diese Statuswerte sind nicht Dekoration, sondern das eigentliche Steuerungsinstrument – sie verändern den Score und dokumentieren gleichzeitig eine Entscheidung.

Status	Bedeutung	Punkte	Wofür du ihn wirklich einsetzt
To address	Du erkennst die Aktion als notwendig an und willst sie irgendwann angehen. Gilt auch für teilweise umgesetzte Aktionen.	keine bzw. anteilig	Der Standardzustand. Wenn hier nach zwölf Monaten noch alles steht, ist das dein eigentlicher Befund.
Planned	Es gibt konkrete Pläne zur Umsetzung.	keine	Nur mit Termin und Namen in der Notiz. Sonst ist es „To address“ mit besserem Selbstbild.
Risk accepted	Ihr verzichtet bewusst auf die Umsetzung und tragt das Restrisiko.	keine	Die ehrlichste Kategorie. Braucht eine Freigabe außerhalb der IT und ein Wiedervorlagedatum.
Resolved through third party	Ein Fremdprodukt deckt die Anforderung ab.	volle Punktzahl	Fremdes Mail-Gateway, fremdes Endpunktschutzprodukt, fremdes Identitätsmanagement. Hersteller und

			Version in die Notiz.
Resolved through alternate mitigation	Eine eigene oder interne Maßnahme deckt die Anforderung ab.	volle Punktzahl	Der Status für organisatorische oder anders gebaute technische Lösungen. Verlangt den härtesten Nachweis.
Completed	Alle erreichbaren Punkte sind erreicht, bestätigt durch Microsoft-Daten.	volle Punktzahl	Nicht manuell setzbar und nicht änderbar. Genau deshalb der einzige Status mit echter Beweiskraft.

FAKTEN: Was Microsoft bei „Resolved through“ prüft

Nichts. Das ist keine Polemik, sondern steht so in der Dokumentation: Microsoft hat keinerlei Einblick in die Vollständigkeit der Umsetzung, wenn eine empfohlene Aktion als „Resolved through third party“ oder „Resolved through alternate mitigation“ markiert ist. Die Punkte werden trotzdem voll gutgeschrieben.

Daraus folgt zweierlei. Erstens: Der Status ist ein sinnvolles Werkzeug, damit der Score deine reale Lage abbildet und nicht nur deine Microsoft-Lage. Zweitens: Er ist die eleganteste Methode, sich selbst in die Tasche zu lügen, wenn du ihn ohne Nachweis benutzt. Bei einer Prüfung nach NIS2 oder in einer Cyberversicherungs-Fragerunde ist „steht so im Portal“ keine Antwort.

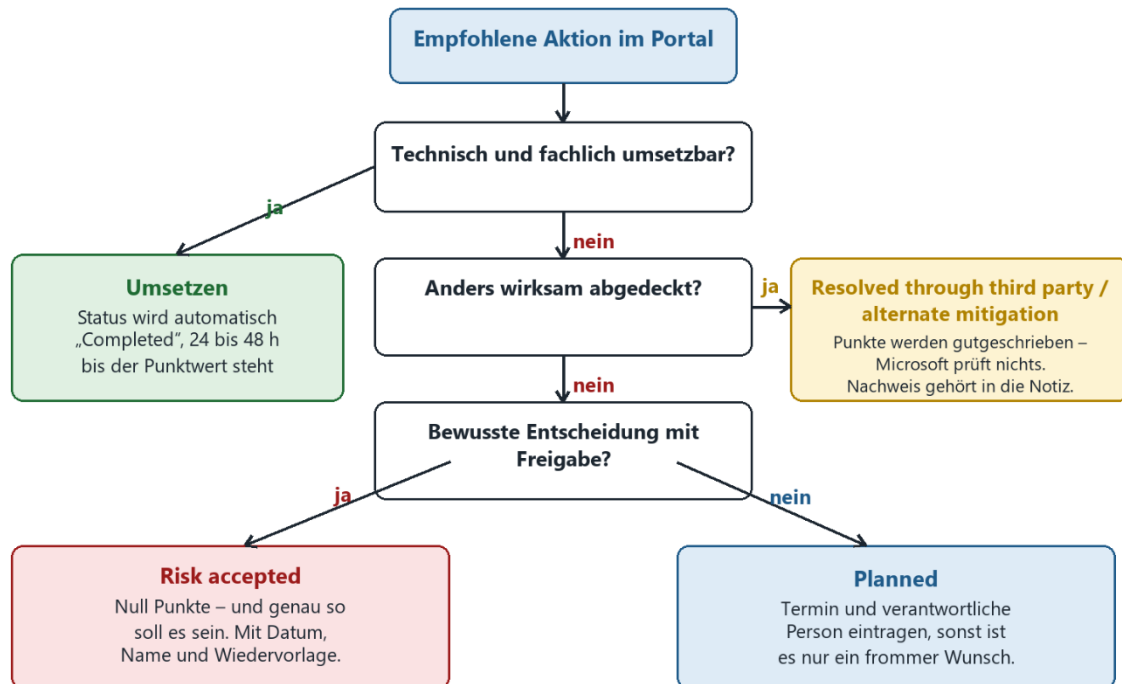
Wann Alternative Mitigation ehrlich ist – und wann nicht

Es gibt drei saubere Anwendungsfälle, und die decken in der Praxis fast alles ab.

- **Das Ziel wird technisch anders erreicht.** Klassiker: Du hast Security Defaults aktiviert, und Microsoft empfiehlt zusätzlich eine Anmelderrisiko- und Benutzerrisiko-Richtlinie. Microsoft selbst rät hier ausdrücklich dazu, den Status auf „Resolved through alternative mitigation“ zu setzen, statt beide Verfahren übereinanderzulegen.
- **Ein Fremdprodukt übernimmt die Funktion.** Ein vorgeschaltetes Mail-Gateway filtert Anhänge, eine bestehende Endpunktschutzlösung deckt die Geräte ab, ein anderer Identity Provider erzwingt die starke Anmeldung. Dann gehört Hersteller, Produktname und der Ort des Nachweises in die Notiz.
- **Die Maßnahme ist organisatorisch gelöst.** Etwa wenn eine Freigabe technisch möglich bleibt, aber durch einen verbindlichen, geprüften Prozess und regelmäßige Kontrolle abgesichert ist. Das ist die schwierigste Variante, weil der Nachweis nicht im System liegt.

Und die unehrliche Variante, die man in Tenants regelmäßig findet: Der Status wird gesetzt, weil die Aktion lästig ist, die Notiz lautet „intern gelöst“, und niemand kann drei Monate später sagen, was damit gemeint war. Das ist keine Mitigation, das ist eine Punktebeschaffungsmaßnahme mit Ansage.

Statuslogik: was du mit einer empfohlenen Aktion wirklich tust



Jeder Weg endet in einem Status mit Begründung. Kein Weg endet in „irgendwann mal“.

Skizze 3: Jede empfohlene Aktion endet in einem Status mit Begründung – auch die, die du nicht umsetzt.

Die Begründung ist das eigentliche Artefakt

Zu jeder empfohlenen Aktion kannst du Notizen und eigene Kennzeichnungen hinterlegen und nach diesen Kennzeichnungen filtern. Das ist die unspektakulärste und zugleich wertvollste Funktion des ganzen Werkzeugs. Etabliere ein festes Notizformat und halte es durch:

- Datum der Entscheidung und Name der Person, die sie getroffen hat.
- Warum die Microsoft-Empfehlung in eurer Umgebung nicht oder anders greift.
- Welche Maßnahme stattdessen wirkt – konkret, mit Produkt, Richtlinienname oder Prozessdokument.
- Wo der Nachweis liegt und wer ihn auf Nachfrage vorzeigen kann.
- Datum der Wiedervorlage. Ohne dieses Feld verweist jede Entscheidung.

Ergibt in Summe: Wenn ein Prüfer, eine Versicherung oder ein Kunde fragt, warum Punkt X nicht umgesetzt ist, hast du die Antwort im System stehen statt in der Erinnerung eines Kollegen, der inzwischen woanders arbeitet.

Wie das in einen Nachweis nach NIS2 eingeht, behandelt der Beitrag [NIS2 aus Security-Sicht: technische Maßnahmen in M365](#). Zur Einordnung, was der Score bei Vorfällen tatsächlich beiträgt – nämlich nichts, wenn der Ernstfall läuft – lohnt der Blick in [Incident-Response-Plan für Microsoft 365](#).

TIPP: Zuständigkeiten über Defender Unified RBAC schneiden

Die Berechtigungen für Secure Score liegen in Microsoft Defender Unified RBAC unter der Kategorie „Security posture“ und heißen „Exposure Management (read)“ für lesenden und „Exposure Management (manage)“ für verwaltenden Zugriff. Damit kannst du Lesezugriff breit verteilen – an

die Revision, an das Qualitätsmanagement, an die IT-Leitung – ohne dass jemand Statuswerte ändern kann.

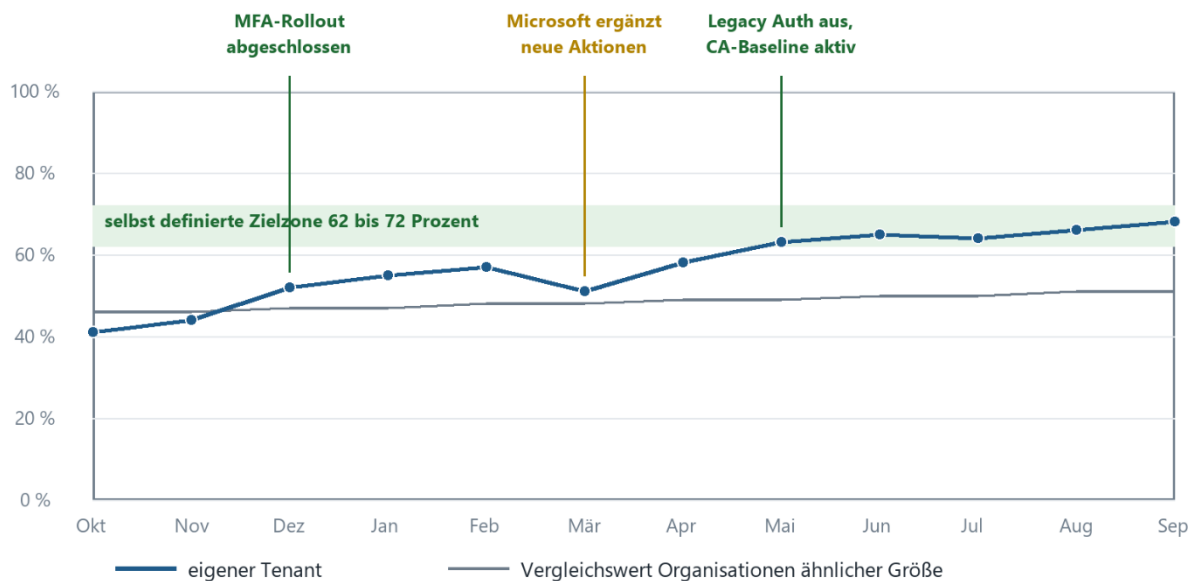
Wichtig: Wer klassische Entra-Rollen wie Sicherheitsadministrator, Exchange-Administrator oder SharePoint-Administrator hat, darf weiterhin ändern. Wenn du das Berechtigungsmodell wirklich schneiden willst, müssen die alten erhöhten Rollen weg. Und beachte: Der Zugriff über die Graph-API läuft weiterhin über Entra-Rollen, nicht über das neue Modell – relevant, wenn du eigene Dashboards baust.

Der Score als Berichtsinstrument für die Geschäftsführung

Eine Zahl ist keine Aussage

„Wir sind bei 64 Prozent“ ist keine Information, sondern ein Geräusch. Wer damit in eine Geschäftsführungssitzung geht, bekommt entweder ein gleichgültiges Nicken oder die Frage nach den fehlenden 36 Prozent – und beides hilft niemandem. Ein brauchbarer Bericht besteht aus vier Elementen: dem Wert im Verhältnis zur selbst gesetzten Zielzone, der Veränderung seit dem letzten Bericht mit Begründung, dem Vergleich mit ähnlichen Organisationen und der Liste der bewusst akzeptierten Risiken.

Score-Verlauf als Berichtsgrafik – mit Kontext statt nackter Zahl



Der Knick im März ist kein Versagen: Microsoft hat den Nenner vergrößert.

Skizze 4: Verlauf, Zielzone, Vergleichswert und Ereignisse in einer Grafik – so wird aus der Zahl eine Diskussion.

Die Ereignismarkierungen sind der wichtigste Teil. Jeder Knick nach oben oder unten braucht eine Beschriftung. Der Reiter History im Portal liefert dir die Rohdaten dafür: eine Grafik des Verlaufs und darunter die Liste aller Aktivitäten im gewählten Zeitraum mit den jeweils resultierenden Punkten und Kategorien. Wer diese Liste einmal im Quartal durchgeht, kann jede Bewegung erklären – und wer sie nicht durchgeht, wird von der ersten Nachfrage überrascht.

Vergleichswerte richtig einordnen

Das Portal bietet dir zwei Vergleichsdarstellungen: ein Balkendiagramm auf der Übersichtsseite und einen Vergleichsverlauf im Reiter Metrics & trends, in dem eine Linie den Durchschnitt von Organisationen mit ähnlicher Nutzerzahl zeigt. Zusätzlich kannst du einen eigenen Vergleich definieren. Die Vergleichsdaten sind anonymisiert; Microsoft weiß selbst nicht, welche Tenants konkret in der Auswertung stecken.

WARNUNG: Der Vergleichswert ist kein Gütesiegel

„Wir liegen über dem Durchschnitt vergleichbarer Organisationen“ klingt hervorragend und bedeutet fast nichts. Der Durchschnitt enthält Tenants mit völlig anderen Lizenzen, anderen Konnektoren und anderer Risikolage. Er enthält vor allem auch alle, die dasselbe Spiel spielen und Punkte optimiert haben.

Der Vergleich taugt für genau eine Aussage: als Warnlampe, wenn ihr deutlich darunter liegt. Nach oben hin ist er wertlos. Wer den Vergleichswert als Erfolgsnachweis in eine Führungsfolie schreibt, verkauft eine Wohlfühlgrafik und wird sie beim nächsten Vorfall wiedersehen – dann mit ganz anderem Publikum.

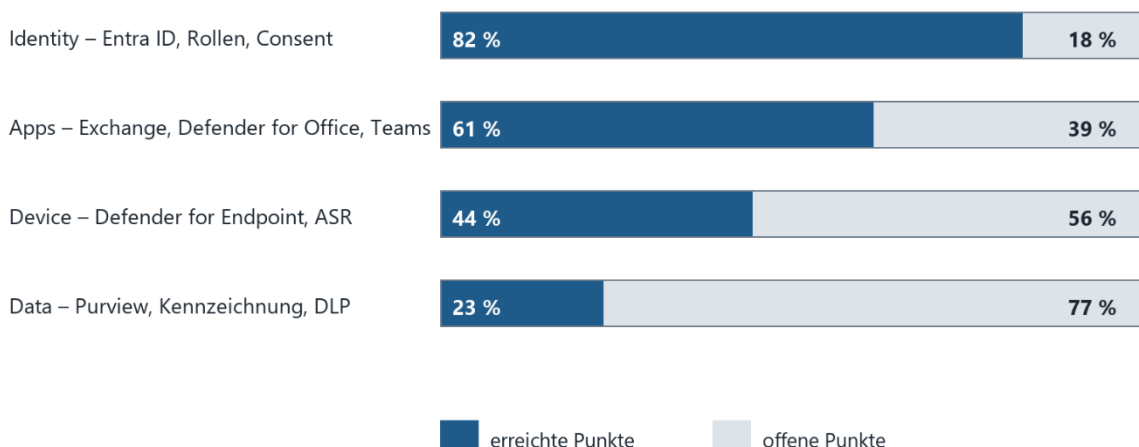
Vier Kennzahlen, die besser sind als der Score allein

Der Score gehört in den Bericht, aber nicht allein. Diese Begleitzahlen machen aus einer Prozentangabe eine Steuerungsgrundlage – und sie sind alle direkt aus dem Portal ablesbar oder über die Graph-API abrufbar.

Kennzahl	Woher	Welche Frage sie beantwortet
Abstand zur Zielzone	Eigener Wert gegen selbst definierte Secure-Score-Zone	Sind wir dort, wo wir sein wollten – nach unserem eigenen, dokumentierten Maßstab?
Zahl und Alter der akzeptierten Risiken	Reiter Metrics & trends, Risk acceptance trend	Welche Risiken tragen wir bewusst, seit wann, und hat das noch jemand bestätigt?
Rückläufige Punkte	Reiter Metrics & trends, Regression trend und Score changes	Wo verfallen Maßnahmen wieder – durch Konfigurationsänderungen, neue Konten oder neue Geräte?
Abstand zwischen Planned score und aktuellem Wert	Score-Ansichten auf der Übersichtsseite	Wie viel haben wir uns vorgenommen, und wie lange steht das schon so da?

Besonders unterbewertet ist der Regressionsverlauf. Punkte gehen nicht nur verloren, weil jemand etwas abschaltet, sondern schleichend: Neue Konten werden angelegt und nicht in die MFA-Gruppe aufgenommen, neue Geräte kommen ohne Grundkonfiguration ins Netz, eine Ausnahme wird für ein Projekt eingerichtet und nie zurückgenommen. Genau das ist der Wert, den du in der Geschäftsführung zeigen willst, wenn du Argumente für Betriebsprozesse statt für Projekte brauchst.

Punkteherkunft je Kategorie – der Blick, der die Diskussion trägt



Vier Balken sagen mehr als eine Prozentzahl – und führen direkt zur nächsten Maßnahme.

Skizze 5: Die Aufteilung nach Kategorien führt zur nächsten Maßnahme. Die Gesamtzahl führt nur zu Rückfragen.

Der Quartalsrhythmus

Wir empfehlen einen festen Ablauf, der ohne Werkzeugbastelei auskommt und in zwei Stunden pro Quartal erledigt ist:

- **Woche 1:** History-Liste des Quartals durchgehen, jede Veränderung über fünf Punkte mit einer Zeile Begründung versehen.
- **Woche 1:** Alle Aktionen im Status „Risk accepted“ mit Wiedervorlagedatum im Quartal prüfen. Weiter tragen oder umsetzen – Verlängerung braucht eine neue Unterschrift.
- **Woche 2:** Alle Aktionen im Status „Resolved through third party“ und „alternate mitigation“ stichprobenartig gegen die Wirklichkeit prüfen. Drei pro Quartal reichen, wenn sie zufällig gezogen werden.
- **Woche 2:** Zwei bis vier neue Aktionen aus der oberen Hälfte der Prioritätsliste auf „Planned“ setzen – mit Termin und Namen.
- **Woche 3:** Eine Seite Bericht: Wert, Zielzone, Veränderung mit Begründung, akzeptierte Risiken, nächste Schritte. Mehr nicht.

Wie diese eine Seite konkret aussieht und welche Formulierungen in der Geschäftsführung ankommen, steht ausführlich in [Security-Reporting für die Geschäftsführung](#). Wenn du die Daten automatisiert abgreifen willst: Der Score ist über die Microsoft-Graph-Sicherheits-API unter secureScores verfügbar, mitsamt aktuellem Wert, Maximalwert, den Einzelwerten je Steuerung und den anonymisierten Vergleichswerten – in PowerShell etwa über Get-MgSecuritySecureScore. Damit lassen sich Verläufe länger aufbewahren, als die Oberfläche sie anzeigt.

WICHTIG: Secure Score ist nicht der einzige Score im Portal

Im Defender-Portal liegt inzwischen mehreres nebeneinander: der Microsoft Secure Score, die Initiativen und Metriken aus Microsoft Security Exposure Management, der Exposure Score aus dem Schwachstellenmanagement und der Cloud Secure Score aus Defender for Cloud. Exposure Management führt Empfehlungen aus mehreren Quellen – darunter Secure Score und Defender for Cloud – in einem gemeinsamen Empfehlungskatalog zusammen, sortiert nach Angriffsfläche.

Praktische Konsequenz für den Bericht: Nenne immer, welchen Score du meinst, und mische die Zahlen nie in einer Grafik. Zwei Prozentwerte nebeneinander, die verschiedene Dinge messen, sind der zuverlässigste Weg, Vertrauen in die gesamte Berichterstattung zu verlieren.

Häufige Fragen zum Microsoft Secure Score

Welcher Secure Score ist ein guter Wert?

Es gibt keinen allgemeingültigen guten Wert, weil der Nenner von deinen Lizenzen, deinen angebundenen Konnektoren und dem jeweils aktuellen Empfehlungskatalog abhängt. Sinnvoll ist die Frage anders herum: Wie hoch ist dein Wert im Verhältnis zu dem, was mit deinen Lizenzen erreichbar wäre, und wie viele der wirklich wirksamen Aktionen aus den oberen Rängen sind erledigt? Ein Tenant mit 58 Prozent, bei dem MFA flächendeckend erzwungen, Legacy-Auth abgeschaltet und die Zahl der globalen Administratoren einstellig ist, steht besser da als einer mit 78 Prozent ohne diese Grundlagen.

Warum ist mein Score gefallen, obwohl wir nichts geändert haben?

Drei häufige Ursachen. Erstens: Microsoft hat neue empfohlene Aktionen ergänzt – der Nenner wächst, dein Prozentwert fällt. Zweitens: Anteilig bewertete Aktionen haben sich verschlechtert, weil neue Konten oder Geräte dazugekommen sind, die noch nicht in den Richtlinien stehen. Drittens: Eine Konfiguration hat sich geändert, ohne dass es jemand als sicherheitsrelevant wahrgenommen hat. Der Regressionsverlauf im Reiter Metrics & trends zeigt dir genau, welcher Fall vorliegt.

Bringen Security Defaults Punkte?

Ja, und zwar sofort. Wenn du Security Defaults in Microsoft Entra ID aktivierst, bekommst du die volle Punktzahl für drei Aktionen: alle Konten können MFA nutzen (neun Punkte), MFA für Administratorrollen (zehn Punkte) und Blockieren der Legacy-Authentifizierung (sieben Punkte). Das ist für kleine Umgebungen ein hervorragendes Preis-Leistungs-Verhältnis. Der Preis: Du verlierst die Feinsteuerung, und sobald du eine einzige Ausnahme brauchst, musst du auf Conditional Access wechseln.

Die Abwägung im Detail steht in [Security Defaults oder Conditional Access?](#). Und wenn du die Registrierungswelle mit einem Anlass verbinden willst, hilft [Attack Simulation Training: Phishing-Übungen richtig aufsetzen](#).

Sollten wir Aktionen einfach auf „Resolved through alternate mitigation“ setzen, um den Bericht schöner zu machen?

Nein – aber nicht aus moralischen Gründen, sondern aus praktischen. Der Status schreibt die Punkte gut, ohne dass Microsoft die Umsetzung prüft. Genau deshalb verlierst du damit die einzige Funktion, die der Score für dich hat: dich an offene Punkte zu erinnern. Sechs Monate später steht eine unbelegte Zahl im Portal, die niemand mehr auflösen kann. Setz den Status, wenn du den Nachweis in der Notiz hast, und sonst nicht.

Kann ich den Score exportieren oder historisieren?

Ja. Über die Microsoft-Graph-Sicherheits-API liest du unter secureScores den aktuellen Wert, den Maximalwert, die Zahl der aktiven und lizenzierten Konten, die Einzelwerte je Steuerung und die anonymisierten Vergleichswerte aus. In PowerShell geht das über das Microsoft-Graph-Modul mit Get-MgSecuritySecureScore. Beachte, dass der API-Zugriff über Entra-Rollen gesteuert wird und nicht über das neuere Unified-RBAC-Modell im Defender-Portal.

Warum kann ich bei Geräte-Empfehlungen keinen Status setzen?

Empfohlene Aktionen in der Kategorie Device werden nicht im Secure Score selbst verwaltet, sondern über die zugehörige Sicherheitsempfehlung im Defender Vulnerability Management. Wichtiger Fallstrick: Legst du dort eine globale Ausnahme an, wird der Status im Secure Score mit der Begründung aktualisiert – das kann bis zu zwei Stunden dauern. Legst du dagegen eine Ausnahme pro Gerätegruppe an, passiert im Secure Score gar nichts, und die Aktion bleibt auf „To address“ stehen. Wer sich darüber wundert, hat meist die falsche Ausnahmeart gewählt.

Wie lange dauert es, bis eine Umsetzung sichtbar wird?

Rechne mit 24 bis 48 Stunden, bis eine abgeschlossene Aktion im Score erscheint. Bei Empfehlungen zu Microsoft Teams und Microsoft Entra kommt die zusätzliche Auffrischung im monatlichen beziehungsweise wöchentlichen Takt dazu. Plane das ein, wenn ein Umsetzungsstichtag kurz vor einem Berichtstermin liegt – sonst berichtest du über einen Stand, den es schon nicht mehr gibt.

Ersetzt Exposure Management den Secure Score?

Nicht kurzfristig. Microsoft Security Exposure Management ist breiter angelegt und arbeitet mit Initiativen, Metriken, Angriffspfaden und einem unternehmensweiten Expositionsgraph über Endpunkte, Identitäten, Cloud- und SaaS-Ressourcen. Bei Initiativen ohne eigene Metriken wird der Initiativwert sogar nach derselben Logik berechnet wie der Secure Score. Der Secure Score bleibt vorerst die konkretere, leichter erklärbare Zahl für Konfigurationsdisziplin in Microsoft 365. Beachte allerdings: Exposure Management ist nur in der öffentlichen Cloud verfügbar, nicht in souveränen Umgebungen.

Fazit

Der Microsoft Secure Score ist ein gutes Werkzeug mit einer schlechten Eigenschaft: Er sieht aus wie ein Ergebnis, ist aber nur eine Zwischenmeldung. Wer ihn als Ergebnis behandelt, optimiert auf die Zahl und wundert sich, wenn der Angriff durch die Tür kommt, an der niemand gemessen hat. Wer ihn als Arbeitsvorrat behandelt – als eine gepflegte, priorisierte, kommentierte Liste offener Entscheidungen – hat eines der wenigen Instrumente in der Hand, die IT-Sicherheit für Nichttechniker greifbar machen.

Praktisch heißt das: Setz dir eine Zielzone statt eines Maximums. Arbeite die sechs Aktionen mit dem größten Schutzeffekt ab, bevor du dich um Punkte im einstelligen Bereich kümmerst. Benutze die Status ehrlich, mit Datum, Name und Nachweis in der Notiz – besonders bei „Alternative Mitigation“, wo Microsoft dir vertraut, ohne zu prüfen. Erkläre jeden Knick im Verlauf. Und behandle den Vergleich mit ähnlichen Organisationen als Warnlampe nach unten, nicht als Auszeichnung nach oben.

Der beste Satz, den du in einer Geschäftsführungssitzung zum Score sagen kannst, lautet nicht „Wir sind bei 71 Prozent“. Er lautet: „Wir tragen aktuell vier bewusst akzeptierte Risiken, hier sind sie, hier ist der Grund, und diese zwei wollen wir im nächsten Quartal auflösen.“ Das ist eine Aussage, an der man arbeiten kann. Eine Prozentzahl ist es nicht.

WEITER IM THEMA

- › [Microsoft 365 Security](#) – der Überblick über die gesamte Serie mit allen Handlungsfeldern.
- › [Tenant-Härtung: die 20 wichtigsten Schrauben](#) – die Maßnahmenliste, die du abarbeitest, bevor du den Score als Steuerung benutzt.
- › [MFA in Microsoft 365 richtig einführen](#) und › [Conditional Access: Baselines, die nicht nerven](#) – die beiden Aktionen mit dem größten Effekt auf Score und Realität.
- › [Security-Reporting für die Geschäftsführung](#) – wie aus Kennzahlen eine Entscheidungsvorlage wird.
- › [Zero Trust im Mittelstand: pragmatisch statt dogmatisch](#) – der größere Rahmen, in den die einzelnen Punkte gehören.
- › [Defender for Endpoint: Onboarding ohne Drama](#) und › [Defender for Identity: das Active Directory im Blick](#) – damit aus aktivierten Lizenzen wirksame Sensorik wird.
- › [Gastzugriff und externe Freigaben härten](#) und › [Ransomware-Vorsorge in Microsoft 365](#) – zwei Bereiche, in denen der Score nur die halbe Miete zeigt.
- › [Dossier: TerminalFix und der Berlin-Hack](#) – was passiert, wenn die Grundlagen fehlen und die Kennzahl trotzdem grün war.
- › [Microsoft 365 Security Beratung](#) – wenn ihr die Priorisierung, die Zielzone und den Berichtsrhythmus einmal gemeinsam aufsetzen wollt, statt sie über zwei Jahre zu erfinden.
- › [Schulung Microsoft 365 Security](#) – für Teams, die den Portalumgang und die Statuslogik im eigenen Tenant üben wollen.