

Security-Reporting für die Geschäftsführung: der Quartalsreport auf einer Seite

Es gibt zwei Sorten von Sicherheitsberichten. Die eine landet in der Sitzung, wird drei Minuten lang gelobt und danach nie wieder geöffnet. Die andere landet nach dem Vorfall beim Anwalt, und dann interessiert sich plötzlich sehr genau jemand dafür, was du wann gemeldet hast und wer es abgezeichnet hat. Das Unangenehme daran: Es ist derselbe Bericht. Du weißt nur zum Zeitpunkt des Schreibens noch nicht, in welcher Rolle er später auftritt.

Dieser Beitrag gehört zum Handlungsfeld „Führung und Nachweis“ und beschreibt einen Quartalsreport, der auf eine Seite passt. Eine Seite ist keine Koketterie, sondern eine Konstruktionsbedingung: Was nicht auf die Seite passt, wird auch nicht gelesen. Sechs Kennzahlen, jeweils mit Trend, Ampel und einem Satz Deutung — Punktestand deiner Sicherheitseinstellungen, Abdeckung mit starker Anmeldung, offene kritische Befunde, Vorfälle und Reaktionszeiten, Übungsstand und Lizenz-Lücken. Dazu eine fertige Vorlage zum Abtippen, ein Beispiel-Dashboard und eine Übersetzungstabelle, mit der du dir das Fachchinesisch selbst austreibst.

Vorweg die zwei Regeln, die alles andere tragen: keine Abfragesprache im Bericht — keine Zeile KQL, kein Screenshot aus einem Analysewerkzeug, keine Regelnamen. Und kein Fachbegriff ohne Übersetzung. Wenn du „MFA-Coverage“ schreibst, hast du verloren. Wenn du „Anteil der Konten, die sich nur mit zweitem Faktor anmelden können“ schreibst, hast du gewonnen. Es ist wirklich so simpel und wirklich so selten.

Fakten: Warum die Geschäftsführung das lesen muss, nicht darf

Das deutsche NIS2-Umsetzungsgesetz wurde am 6. Dezember 2025 verkündet und gilt seitdem ohne Übergangsfrist für rund 29.500 Einrichtungen in 18 Sektoren.

§ 38 BSIG verpflichtet Geschäftsführung und Vorstand persönlich: Risikomanagementmaßnahmen billigen, ihre Umsetzung überwachen, sich regelmäßig schulen lassen. Die Pflicht ist nicht delegierbar, ein Haftungsverzicht per Gesellschaftsvertrag oder Satzung ist ausgeschlossen.

„Überwachen“ heißt: wiederkehrend, nachweisbar, mit Datum. Genau dafür ist ein Quartalsreport da — er ist kein Berichtswesen-Hobby, sondern das Beweisstück, dass jemand hingesehen hat.

Der Bußgeldrahmen reicht bis 10 Millionen Euro oder 2 Prozent des weltweiten Jahresumsatzes, je nachdem, was höher ist.

Warum dein aktueller Bericht niemanden erreicht

Ich habe eine Menge dieser Berichte gesehen. Der Klassiker ist ein Bildschirmfoto aus dem Defender-Portal, darunter vierzehn Aufzählungspunkte mit Produktnamen, und ganz unten ein Satz, der mit „Wir empfehlen, zeitnah ...“ beginnt. Das ist kein Bericht, das ist ein Alibi in PowerPoint-Form. Die Geschäftsführung liest daraus genau eine Botschaft: Die IT hat viel zu tun. Was sie nicht liest: ob das Haus sicherer geworden ist, ob es irgendwo brennt und was sie selbst entscheiden soll.

Die drei Todsünden

Erstens: zu viele Zahlen. Der Punktestand kennt mehrere hundert Empfehlungen, das Anmeldeprotokoll hat Millionen Zeilen, das Ticketsystem hat vierstellige Rückstände. Wer daraus nicht auswählt, delegiert die Auswahl an den Leser — und der wählt aus, indem er das Dokument schließt.

Zweitens: keine Bewertung. „Der Punktestand liegt bei 68 Prozent“ ist eine Zahl ohne Aussage. Ist das gut? Im Vergleich wozu? Verglichen mit dem Vorquartal, mit dem Ziel, mit ähnlich großen Häusern? Erst der Vergleich macht aus einer Messung eine Information.

Drittens: keine Entscheidung. Ein Bericht, der nichts von der Geschäftsführung will, war die Zeit nicht wert. Am Ende jeder Seite gehören zwei bis drei Punkte, die eine Entscheidung brauchen: ein Budget, ein Termin, eine akzeptierte Restgefahr mit Namen darunter. Wer nichts fordert, bekommt nichts — und darf sich später nicht beschweren, dass „ja niemand etwas gesagt“ habe.

Vom Datenberg zur einen Seite: was auf dem Weg wegfällt

Was die Systeme liefern

Secure Score: 412 Empfehlungen

Entra ID: Anmeldeprotokoll, Millionen Zeilen

Defender XDR: Vorfälle, Warnungen, Geräte

Purview: Richtlinienetreffer, Kennzeichnungen

Sentinel: Analyseregeln, Arbeitsmappen

Lizenzbericht: zugewiesen, genutzt, ungenutzt

Übungen: Klickraten, Meldequoten

Ticketsystem: 1.284 offene Vorgänge

Drei Filterfragen

1. Kann die Geschäftsführung darüber entscheiden?
2. Ändert sich die Zahl im Quartalsrhythmus?
3. Gibt es eine Ampelregel, die vorher feststand?

Alles andere:
Anhang oder Papierkorb

Quartalsreport Q3/2026

- Sicherheitsniveau (Punktestand)
- Anteil Konten mit starker Anmeldung
- Offene kritische Befunde
- Vorfälle und Reaktionszeit
- Übungsstand
- Lizenz-Lücken

Empfehlung an die Geschäftsführung:

eine Entscheidung, ein Budget,
ein Termin.

Skizze 1: Drei Filterfragen entscheiden, was aus dem Datenberg auf die eine Seite kommt. Alles andere gehört in den Anhang — oder gar nicht ins Dokument.

Die stille Erwartung an dich

Seit § 38 BSIg gilt, sitzt in jeder Sitzung eine unausgesprochene Frage mit am Tisch: Kann ich als Geschäftsführung später belegen, dass ich überwacht habe? Diese Frage beantwortest nicht du, sondern dein Bericht — und zwar durch seine Existenz, seine Regelmäßigkeit und seine Nachvollziehbarkeit. Vier datierte Seiten pro Jahr mit denselben sechs Kennzahlen sind vor jedem Prüfer mehr wert als eine dreißigseitige Sonderauswertung, die es genau einmal gab.

Welche technischen Maßnahmen die Richtlinie konkret verlangt und wie du sie in Microsoft 365 abbildest, steht ausführlich im Beitrag [NIS2 aus Security-Sicht: technische Maßnahmen in M365](#). Den Überblick über alle Handlungsfelder findest du auf der Themenseite [Microsoft 365 Security](#).

Die sechs Kennzahlen, die auf die Seite gehören

Sechs ist keine magische Zahl, aber eine praktikable. Sie decken die vier Fragen ab, die eine Geschäftsführung tatsächlich hat: Wird es besser? Sind die Grundlagen da? Brennt gerade etwas? Können wir im Ernstfall handeln? Alles darüber hinaus ist Anhang.

Erstens: das Sicherheitsniveau als Punktestand

Microsoft rechnet die Konfiguration deines Mandanten in eine Prozentzahl um — den Secure Score. Er bewertet Empfehlungen aus Entra ID, Exchange Online, SharePoint Online, Teams, Defender für Endgeräte, Identitäten, Office und Cloud-Apps sowie Purview; jede Empfehlung ist

höchstens zehn Punkte wert, viele werden anteilig vergeben. Wenn du 50 von 100 Konten mit zweitem Faktor geschützt hast, bekommst du fünf von zehn Punkten. Der Wert aktualisiert sich laufend, ein Abgleich der Systemdaten läuft täglich; Empfehlungen zu Entra ID werden wöchentlich, die zu Teams monatlich neu bewertet. Erwarte also nicht, dass sich eine Änderung von gestern Abend heute früh schon in der Zahl zeigt.

Für den Bericht brauchst du drei Dinge: den aktuellen Wert, den Wert des Vorquartals und die Vergleichslinie. Das Defender-Portal liefert unter „Kennzahlen und Trends“ eine Vergleichskurve gegen anonymisierte Häuser mit ähnlicher Anzahl von Lizenzplätzen. Das ist der einzige Benchmark, der etwas taugt – nicht weil er präzise wäre, sondern weil er die Frage „sind wir schlechter als andere?“ vom Bauchgefühl auf eine Kurve verlagert. In der Praxis liegen mittelständische Häuser meist zwischen 40 und 60 Prozent; 70 Prozent sind ein anspruchsvolles, aber erreichbares Ziel.

Warnung: Der Punktestand ist ein Steuerungsinstrument, keine Trophäe

Es gibt Punkte, die du dir mit Einstellungen erkaufst, die deine Belegschaft anschließend umgeht. Und es gibt Maßnahmen mit enormer Wirkung, die kaum Punkte bringen. Wer den Wert zur Zielvorgabe im Bonusgespräch macht, züchtet sich Punktejagd statt Sicherheit.

Formuliere das Ziel deshalb als Korridor („zwischen 68 und 75 Prozent, ohne Ausnahmeregeln für ganze Abteilungen“) und nicht als harte Zahl. Und schreib in den Bericht, welche Punkte du bewusst liegen lässt – Microsoft selbst sagt deutlich, dass der Wert kein Maß für die Wahrscheinlichkeit eines Einbruchs ist.

Wie du den Wert sinnvoll liest, welche Empfehlungen wirklich tragen und wo Punktejagd anfängt, steht im Beitrag [Secure Score: sinnvoll nutzen statt Punktejagd](#).

Zweitens: Abdeckung mit starker Anmeldung

Die wichtigste Einzelzahl im ganzen Bericht, und die einzige, bei der 99 Prozent ein schlechtes Ergebnis ist. Ein Angreifer sucht nicht den Durchschnitt, er sucht das eine Konto ohne zweiten Faktor. Nimm die Zahl aus dem Bericht „Aktivität der Authentifizierungsmethoden“ in Entra ID: Der Reiter „Registrierung“ zeigt dir, wie viele Konten überhaupt zu einer Anmeldung mit zweitem Faktor fähig sind, der Reiter „Verwendung“ zeigt, wie oft sie tatsächlich stattfindet. Für die Auswertungen brauchst du eine Lizenz der Stufe Entra ID P1 oder P2.

Berichte immer beides: Prozentwert und absolute Restzahl. „97 Prozent“ klingt nach Erfolg. „14 Konten ohne zweiten Faktor, davon drei mit Administratorrechten“ klingt nach Handlungsbedarf – und ist dieselbe Information. Nenne außerdem die Notfallkonten separat, denn die sind bewusst anders gebaut und dürfen die Statistik nicht verfälschen.

Drittens: offene kritische Befunde

Hier zählt nicht die Menge, sondern das Alter. Sechs offene kritische Befunde sind kein Drama. Drei kritische Befunde, die seit 94 Tagen offen sind, sind eines – denn sie belegen, dass eure Behebungskette nicht funktioniert. Nimm deshalb zwei Zahlen: die Anzahl offener kritischer Punkte und die Anzahl derer, die älter sind als eure eigene Frist. Die Frist legt ihr einmal fest, schriftlich, und danach diskutiert ihr nicht mehr darüber.

Viertens: Vorfälle und Reaktionszeit

Zwei Zahlen, die zusammengehören: Wie viele Sicherheitsvorfälle gab es, und wie lange hat es vom ersten Alarm bis zur Eindämmung gedauert? Die Reaktionszeit ist die aussagekräftigere von beiden. Eine steigende Anzahl von Vorfällen kann bedeuten, dass ihr mehr angegriffen werdet –

oder schlicht, dass ihr endlich hinschaut. Eine steigende Reaktionszeit bedeutet immer dasselbe: Es wird schlechter.

Berichte den Mittelwert und den langsamsten Einzelfall. Der langsamste Fall ist der ehrliche: Er zeigt, was passiert, wenn der Alarm freitags um 18:40 Uhr auflief. Und nenne, falls zutreffend, die gesetzlichen Fristen daneben — nach dem BSIG gilt für betroffene Einrichtungen eine Erstmeldung binnen 24 Stunden, eine Folgemeldung binnen 72 Stunden und ein Abschlussbericht binnen eines Monats. Wenn deine durchschnittliche interne Reaktionszeit über der Erstmeldefrist liegt, hast du kein Reporting-Problem, sondern ein Betriebsproblem.

Die Zahlen für die Reaktionszeit sind nur so gut wie euer Ablaufplan. Wie der aussieht, steht im [Incident-Response-Plan für Microsoft 365](#); wie die ersten Minuten konkret ablaufen, zeigt [Phishing-Vorfall: die ersten 60 Minuten](#).

Fünftens: Übungsstand

Die Kennzahl, die am häufigsten fehlt und am schnellsten peinlich wird. Sie beantwortet die Frage: Habt ihr das schon einmal geprobt, oder improvisiert ihr im Ernstfall? Drei Werte reichen: Datum der letzten Notfallübung, Datum der letzten simulierten Phishing-Welle mit Klick- und Meldequote, Datum der letzten Schulung der Geschäftsführung selbst. Der dritte Punkt ist kein Seitenhieb, sondern gesetzliche Pflicht.

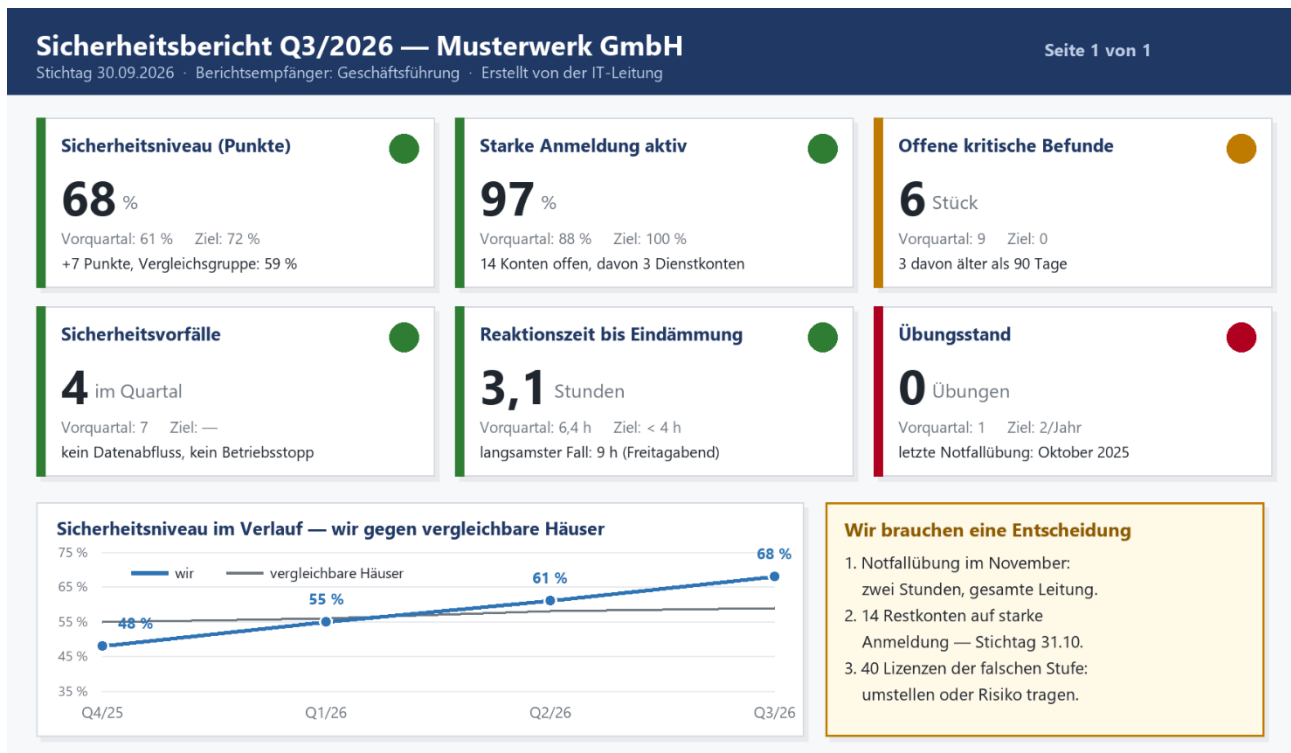
Wenn hier seit zwölf Monaten nichts steht, setz die Zeile trotzdem in den Bericht — rot. Eine leere Zeile schützt niemanden, eine rote Zeile erzeugt einen Termin.

Sechstens: Lizenz-Lücken

Die Kennzahl, die dein Budgetgespräch trägt. Sie sagt: Für welche Schutzfunktionen habt ihr bezahlt, ohne sie zu nutzen — und welche Funktionen fehlen euch, weil die Lizenzstufe sie nicht enthält? Beide Richtungen sind interessant. Ungenutzte Funktionen sind verbranntes Geld, das du mit einer Konfiguration zurückholst. Fehlende Funktionen sind eine bewusste Risikoentscheidung, und die trifft nicht die IT, sondern die Geschäftsführung.

Ein Detail, das gern für Verwirrung sorgt: Der Punktestand zeigt dir alle Empfehlungen eines Produkts, unabhängig davon, welche Lizenzstufe du tatsächlich gebucht hast. Du siehst also Vorschläge, die du gar nicht umsetzen kannst. Das ist beabsichtigt — und genau deshalb gehört die Lizenz-Lücke als eigene Zeile in den Bericht, statt als Fußnote im Punktestand unterzugehen.

Kennzahl	Beantwortet die Frage	Woher die Zahl kommt	Ampel
Sicherheitsniveau (Punktestand)	Wird unsere Grundkonfiguration besser?	Defender-Portal, Bereich Secure Score, Reiter Kennzahlen und Trends	Korridor, Vergleich zur Gruppe
Starke Anmeldung	Kann sich jemand allein mit einem Passwort anmelden?	Entra ID, Bericht Aktivität der Authentifizierungsmethoden (P1/P2)	100 % oder rot
Offene kritische Befunde	Bleiben ernste Dinge bei uns liegen?	Defender-Portal und euer Ticketsystem, gefiltert auf kritisch	Alter, nicht Anzahl
Vorfälle und Reaktionszeit	Merken wir es, und wie schnell reagieren wir?	Vorfallsliste im Defender-Portal, Zeitstempel aus dem Ticket	Mittelwert und langsamster Fall
Übungsstand	Können wir im Ernstfall handeln?	Eigener Kalender, Ergebnisse der Phishing-Simulation	Datum, nicht Note
Lizenz-Lücken	Zahlen wir für Schutz, den wir nicht nutzen?	Lizenzbericht im Admin Center, Abgleich mit aktiven Funktionen	Anteil ungenutzter Funktionen



Skizze 2: Beispiel-Dashboard. Sechs Kacheln, eine Verlaufskurve mit Vergleichslinie, ein Kasten mit drei Entscheidungen. Mehr passt nicht auf eine Seite — und mehr braucht es auch nicht.

Die Vorlage: dein Quartalsreport zum Abtippen

Die folgende Tabelle ist der ganze Bericht. Kopiere sie, ersetze die Beispielwerte, und du bist fertig. Die Spalte „Deutung“ ist die einzige, die dich Denkarbeit kostet — genau ein Satz, keine Prosa, kein Konjunktiv. Wenn du dort mehr als eine Zeile brauchst, hast du die Kennzahl nicht verstanden.

Kennzahl	Vorquartal	Aktuell	Ziel	Ampel	Deutung in einem Satz
Sicherheitsniveau (Punktestand)	61 %	68 %	72 %	grün	Sieben Punkte gewonnen, vergleichbare Häuser liegen bei 59 Prozent.
Konten mit starker Anmeldung	88 %	97 %	100 %	grün	14 Konten offen, davon drei Dienstkonten mit erhöhten Rechten.
Offene kritische Befunde	9	6	0	gelb	Drei Befunde sind älter als 90 Tage und blockieren sich gegenseitig.
Sicherheitsvorfälle im Quartal	7	4	—	grün	Kein Datenabfluss, kein Betriebsstillstand, alle Fälle geschlossen.
Reaktionszeit bis Eindämmung	6,4 h	3,1 h	unter 4 h	grün	Langsamster Fall neun Stunden, Alarm lief am Freitagabend auf.
Übungen im laufenden Jahr	1	0	2	rot	Seit Oktober 2025 keine Notfallübung, Termin steht bis heute nicht.
Lizenz-Lücken	12 %	8 %	0 %	gelb	40 Konten auf einer Stufe ohne den Schutz, den wir eingeplant hatten.

Darunter kommt der Teil, den die Geschäftsführung tatsächlich braucht — und er besteht aus höchstens drei Punkten:

- Notfallübung im November ansetzen, zwei Stunden, gesamte Leitung anwesend. Entscheidung: Termin.

- Die 14 verbliebenen Konten bis zum 31.10. auf starke Anmeldung umstellen, drei davon erfordern eine Umstellung im Fachverfahren. Entscheidung: Budget für den Dienstleister.
- 40 Lizenzen der falschen Stufe: umstellen für rund X Euro im Jahr — oder die Lücke bewusst tragen. Entscheidung: mit Namen und Datum.

Die Ampelregeln legst du vorher fest

Der häufigste Streit in Berichtssitzungen dreht sich nicht um Zahlen, sondern um Farben. „Ist 68 Prozent wirklich grün?“ Diese Diskussion gewinnst du nur, indem du sie ein einziges Mal führst — vorher, im Beisein der Geschäftsführung, mit Protokoll. Danach ist die Farbe eine Rechenoperation und keine Meinung.

Ampelregeln vorher festlegen — sonst diskutiert ihr über Farben statt über Risiken

Sicherheits-niveau (Punkte)	Starke Anmeldung	Kritische Befunde offen	Reaktionszeit bis Eindämmung	Übungen im Jahr	Lizenz-Lücken
 unter 55 %	 unter 90 %	 mehr als 5	 über 24 h	 keine	 über 10 %
 55 bis 69 %	 90 bis 99 %	 1 bis 5	 4 bis 24 h	 eine	 1 bis 10 %
 ab 70 %	 100 %	 keine	 unter 4 h	 zwei	 keine

Die Schwellen stehen im Protokoll der Sitzung, in der sie beschlossen wurden. Wer sie ändern will, ändert sie vor dem Stichtag — nicht danach.

Skizze 3: Beispiel für einen Ampelrahmen. Die Zahlen sind Vorschläge, keine Naturgesetze — entscheidend ist, dass sie schriftlich feststehen, bevor der Stichtag kommt.

Der Deutungssatz: eine Zeile, kein Aufsatz

Ein guter Deutungssatz enthält eine Bewegungsrichtung und eine Ursache. „Sieben Punkte gewonnen, im Wesentlichen durch das Abschalten der alten Anmeldeverfahren.“ Fertig. Kein „aufgrund der im Rahmen der Maßnahmenumsetzung erzielten Fortschritte“. Niemand hat das je zu Ende gelesen, auch nicht der, der es geschrieben hat.

Tipp: Der Satz, der deinen Bericht rettet

Schreib jede Zeile so, als müsstest du sie einem klugen Menschen erklären, der gerade aus einem Flugzeug steigt und drei Minuten Zeit hat. Wenn du dabei ein Wort verwendest, das du im gleichen Atemzug erklären müsstest, ersetze es.

Praktischer Test: Lies deinen Bericht jemandem aus dem Vertrieb vor. Wenn diese Person danach sagen kann, was besser und was schlechter geworden ist, taugt der Bericht. Wenn sie höflich nickt, taugt er nicht.

Sprache: übersetzen statt weglassen

Fachbegriffe wegzulassen ist genauso falsch wie sie ungefiltert hinzuschreiben. Die Geschäftsführung soll ja verstehen, worüber sie entscheidet. Der Trick ist die Übersetzung: der deutsche Begriff im Bericht, der Fachbegriff höchstens in Klammern dahinter, damit deine Leute im Anschluss wissen, wonach sie im Portal suchen müssen.

Das steht im Portal	Das schreibst du in den Bericht
Secure Score	Sicherheitsniveau als Punktestand: wie viele der empfohlenen Einstellungen wir tatsächlich nutzen
MFA / Multi-Faktor-Authentifizierung	Starke Anmeldung: zusätzlich zum Passwort ein zweiter Nachweis, etwa per App oder Sicherheitsschlüssel
Conditional Access	Zugriffsregeln: wer sich von wo und mit welchem Gerät anmelden darf
Incident / Alert	Sicherheitsvorfall (bestätigt) und Warnmeldung (noch ungeprüft) — nicht dasselbe, nie vermischen
MTTR / Mean Time to Respond	Reaktionszeit: Stunden vom ersten Alarm bis zur Eindämmung
Legacy Authentication	Alte Anmeldeverfahren, die keinen zweiten Faktor können und deshalb abgeschaltet gehören
SIEM / Microsoft Sentinel	Zentrale Auswertung: sammelt Protokolle aus mehreren Systemen und erkennt Muster über deren Grenzen hinweg
Attack Simulation Training	Geplante Phishing-Übung mit Auswertung, wie viele geklickt und wie viele gemeldet haben
Risk accepted	Bewusst getragene Restgefahr — mit Namen, Begründung und Datum
Tenant	Unser Mandant: der abgegrenzte Bereich, in dem all unsere Konten und Daten liegen

Warnung: Was im Bericht nichts zu suchen hat

Keine Abfragesprache. Keine Zeile KQL, keine Regelnamen, keine Bildschirmfotos aus dem Analysewerkzeug. Sie beweisen nur, dass du ein Werkzeug bedienen kannst — die Frage stand nie im Raum.

Keine Produktnamen als Selbstzweck. „Wir haben Defender for Cloud Apps ausgerollt“ ist keine Kennzahl, sondern eine Tätigkeitsbeschreibung. Interessant wäre: Was siehst du jetzt, was du vorher nicht gesehen hast?

Keine personenbezogenen Einzelfälle. Wer geklickt hat, geht die Geschäftsführung nichts an — Quoten ja, Namen nein. Das ist nicht nur Anstand, sondern in mitbestimmten Häusern auch eine Frage der Betriebsvereinbarung.

Wo genau die Grenze zwischen zulässiger Auswertung und Verhaltenskontrolle verläuft und was der Betriebsrat mitzureden hat, klärt der Beitrag [Security-Monitoring und Betriebsrat: was mitbestimmungspflichtig ist](#).

Der Quartalsrhythmus: acht Stunden, viermal im Jahr

Der Bericht kostet dich pro Quartal ungefähr einen Arbeitstag, wenn du ihn nicht am Vorabend zusammenschusterst. Verteilt auf vier Termine wird daraus eine Nebenbeschäftigung.

Zusammengedrängt auf einen Abend wird daraus eine Zahlensammlung ohne Deutung — und die Deutung ist der einzige Teil, für den dich niemand ersetzen kann.

Der Quartalsrhythmus: acht Arbeitsstunden, verteilt auf vier Termine



Wer den Report erst am Vorabend der Sitzung baut, liefert eine Zahlensammlung ohne Deutung.

Die Deutung ist der einzige Teil, für den dich niemand ersetzen kann.

Skizze 4: Der Quartalsrhythmus. Zahlen ziehen, deuten, Vorlage füllen, vortragen — vier Termine, zusammen rund viereinhalb Stunden reine Arbeit plus Vorlauf.

Woher du die Zahlen holst

Alle sechs Kennzahlen stammen aus Werkzeugen, die du bereits bezahlst. Den Punktestand samt Verlauf und Vergleichskurve findest du im Defender-Portal unter „Secure Score“; das Portal führt außerdem eine Gesamtübersicht unter „Berichte“, die standardmäßig die letzten 90 Tage abdeckt und sich als Rohmaterial gut eignet. Die Anmeldeabdeckung liefert Entra ID, die Vorfallsliste das Defender-Portal, die Lizenzsicht das Admin Center. Für den Zugriff genügen lesende Rollen — Sicherheitsleseberechtigter oder globaler Leser reichen, du musst dafür niemandem Administratorrechte geben. Falls ihr die feinere Rechtevergabe im Defender-Portal nutzt, gibt es dort eine eigene Leseberechtigung für die Sicherheitsbewertung.

Wichtig: Wer den Bericht zieht, braucht keine Vollrechte

Ein wiederkehrender Fehler: Für das Reporting bekommt jemand Administratorrechte, weil es „schneller geht“. Damit erzeugst du genau die Art von Dauerkonto mit hohen Rechten, deren Abschaffung du auf derselben Seite empfiehlst.

Lesende Rollen genügen für sämtliche sechs Kennzahlen. Wenn deine Berichtsperson trotzdem mehr braucht, ist das ein eigener Befund für den Bericht — kein Grund, die Rechte zu vergeben.

Wenn eine zentrale Auswertung im Spiel ist

Sobald ihr Microsoft Sentinel einsetzt, ändert sich am Bericht selbst erstaunlich wenig — und das ist das Ziel. Die zentrale Auswertung liefert dir bessere Zahlen zur Reaktionszeit und einen vollständigeren Blick über Systemgrenzen hinweg, aber sie gehört nicht als eigenes Kapitel in den Report. Was hineingehört, sind zwei Zeilen im Anhang: was die Auswertung im Quartal gekostet hat und welche Fälle ohne sie unentdeckt geblieben wären.

Die Kostenfrage ist inzwischen etwas beweglicher geworden. Seit 2026 unterscheidet Microsoft zwei Ebenen: eine Analyse-Ebene für die laufende Erkennung und eine kostengünstigere Ebene für die Langzeitablage selten benötigter Daten. Dazu kommen mengenabhängige Zusatzerate, die deutlich unter dem Verbrauchspreis liegen; die Einstiegsstufe beginnt bei 100 Gigabyte pro Tag, eine kleinere Stufe von 50 Gigabyte pro Tag gab es befristet zu Aktionskonditionen. Für den Mittelstand heißt das praktisch: Rechne die Datenmenge, bevor du anschließt, und zieh die selten gebrauchten Protokolle auf die günstigere Ebene.

Wann sich der Aufwand rechnet und wann er es nicht tut, rechnet der Beitrag [Microsoft Sentinel anbinden: wann es sich lohnt](#) durch. Wenn du stattdessen mit Bordmitteln auskommen willst, ist [Alert Policies und Benachrichtigungen richtig aufsetzen](#) der günstigere Einstieg.

Der Anhang, den niemand liest — und der trotzdem sein muss

Hinter die eine Seite gehören zwei bis vier Seiten Anhang: die Liste der offenen kritischen Befunde mit Datum, die Vorfallsübersicht mit Zeitstempeln, die Lizenzaufstellung. Nicht, weil sie jemand liest, sondern weil sie im Prüfungsfall vorhanden sein muss. Der Anhang ist die Rückversicherung, die eine Seite ist die Kommunikation. Verwechsle die beiden nicht, und misch sie erst recht nicht.

Häufige Fragen

Reicht wirklich eine Seite, oder wirkt das nicht zu dünn?

Eine Seite mit sechs bewerteten Kennzahlen und drei Entscheidungsvorlagen ist erheblich dichter als zwanzig Seiten Tätigkeitsbericht. Und sie hat einen unschätzbaren Vorteil: Sie wird gelesen. Wenn dir jemand vorwirft, das sei zu wenig, leg den Anhang daneben — der ist dick genug für jedes Bedürfnis nach Gründlichkeit.

Wie oft sollte ich berichten — reicht einmal im Jahr?

Nein. Die gesetzliche Pflicht lautet nicht „billigen“, sondern „billigen und überwachen“. Überwachung ist ein Vorgang, kein Ereignis. Vier datierte Berichte im Jahr belegen sie; einer belegt sie nicht. Bei akuten Lagen kommt ein Sonderbericht dazu, aber der ersetzt den Rhythmus nicht.

Was mache ich, wenn eine Kennzahl schlecht aussieht — schönen oder nicht?

Nicht schönen. Eine rote Zeile ist der einzige Grund, warum dir jemand Budget gibt. Und sie ist deine persönliche Absicherung: Wer eine Lücke dokumentiert gemeldet hat, steht nach einem Vorfall in einer völlig anderen Position als der, der sie beruhigend formuliert hat. Der Bericht schützt nicht nur das Unternehmen, sondern auch dich.

Meine Geschäftsführung fragt nach dem Vergleich zu Wettbewerbern. Was kann ich liefern?

Die Vergleichslinie im Defender-Portal, mehr nicht — und die zeigt anonymisierte Häuser mit ähnlicher Anzahl von Lizenzplätzen, keine Branchenkonkurrenz. Sag das offen dazu. Ein Vergleich mit falscher Präzision ist gefährlicher als gar keiner, weil er Entscheidungen trägt, die er nicht tragen kann.

Wer sollte den Bericht vortragen: die IT-Leitung oder ein externer Dienstleister?

Die IT-Leitung. Ein externer Dienstleister kann die Vorlage bauen, die Zahlen prüfen und beim ersten Durchlauf danebensitzen — vortragen sollte, wer im Haus verantwortlich ist. Sonst entsteht der Eindruck, Sicherheit sei eingekauft und damit erledigt. Ist sie nicht.

Wir sind gar nicht von NIS2 betroffen. Brauchen wir das trotzdem?

Ja, aus zwei Gründen. Erstens ändert sich der Betroffenenkreis schneller, als man Verträge umschreibt — über Lieferketten, Umsatzschwellen oder Zukäufe. Zweitens haben

Cyberversicherungen, Auftraggeber und Wirtschaftsprüfung längst eigene Nachweispflichten entwickelt, die praktisch dasselbe verlangen. Der Aufwand ist derselbe, der Anlass ist ein anderer.

Sollen einzelne Namen im Bericht auftauchen?

Bei Entscheidungen ja, bei Fehlern nein. „Verantwortlich für die Umstellung: Bereichsleitung Fertigung, Termin 31.10.“ ist eine saubere Zuordnung. „Drei Klicks kamen aus dem Einkauf“ ist eine Schuldzuweisung mit Ansage — und je nach Betriebsvereinbarung auch noch unzulässig.

Fazit

Ein Sicherheitsbericht für die Geschäftsführung ist kein Technikdokument mit weniger Details, sondern ein Entscheidungsdokument mit ein paar Zahlen. Sechs Kennzahlen genügen: Punktestand mit Trend und Vergleich, Abdeckung mit starker Anmeldung, offene kritische Befunde nach Alter, Vorfälle und Reaktionszeit, Übungsstand, Lizenz-Lücken. Jede Zeile bekommt eine Ampel nach vorher festgelegten Regeln und einen Satz Deutung. Darunter stehen drei Punkte, die eine Entscheidung brauchen — mit Termin und Namen.

Der eigentliche Gewinn liegt nicht im Dokument, sondern im Rhythmus. Vier datierte Seiten im Jahr verwandeln eine gesetzliche Pflicht aus § 38 BSIG in eine Routine, die nebenbei mitläuft. Sie verhindern den Zustand, in dem ihr nach einem Vorfall gemeinsam im Raum sitzt und niemand mehr weiß, wer wovon wann Kenntnis hatte. Und sie kosten dich ungefähr einen Arbeitstag pro Quartal — deutlich weniger als die Rekonstruktion derselben Informationen unter Zeitdruck, mit einem Anwalt im Nebenzimmer.

Fang beim nächsten Quartalswechsel an. Nimm die Vorlage aus diesem Beitrag, trag ein, was du in zwei Stunden zusammenbekommst, und lass bewusst Lücken stehen. Ein Bericht mit drei roten Zeilen und vier ehrlichen Fragezeichen ist beim ersten Mal genau richtig. Beim vierten Mal sind die Fragezeichen weg — und dann hast du etwas, das trägt.

Weiter lesen: Passende Beiträge aus dieser Serie

- › [Microsoft 365 Security — Überblick über alle Handlungsfelder](#)
- › [Secure Score: sinnvoll nutzen statt Punktejagd](#)
- › [NIS2 aus Security-Sicht: technische Maßnahmen in M365](#)
- › [Microsoft Sentinel anbinden: wann es sich lohnt](#)
- › [MFA in Microsoft 365 richtig einführen](#)
- › [Tenant-Härtung: die 20 wichtigsten Schrauben](#)
- › [Feuerwehrübung: Security-Notfälle im Team trainieren](#)
- › [Attack Simulation Training: Phishing-Übungen richtig aufsetzen](#)
- › [Zero Trust im Mittelstand: pragmatisch statt dogmatisch](#)

Wenn du den ersten Quartalsreport nicht allein bauen willst — einmal gemeinsam aufsetzen, Ampelregeln festlegen, Vorlage übergeben —, führt der Weg über die [Beratung zu Microsoft 365 Security](#). Wenn stattdessen dein Team den Rhythmus selbst übernehmen soll, ist die [Schulung Microsoft 365 Security](#) der direktere Weg. Und wer wissen will, wie schnell aus einem gut gemeinten Bericht ein Aktenzeichen wird, findet im Dossier [TerminalFix und der Berlin-Hack](#) den ausführlichen Fall.