

Alert Policies und Benachrichtigungen richtig aufsetzen

Es gibt eine Sorte Sicherheitsvorfall, die im Nachhinein besonders weh tut: die, bei der alles funktioniert hat. Die Erkennung hat angeschlagen. Die Richtlinie hat ausgelöst. Der Alarm wurde erzeugt, sauber kategorisiert, mit einem Schweregrad versehen und per E-Mail verschickt. Nur eben an ein Sammelpostfach, in das seit der Migration vor zwei Jahren niemand mehr hineingesehen hat. Der Angreifer hatte neun Tage Ruhe. Die Technik hatte recht. Beides gleichzeitig.

Alarmierung ist der unspektakulärste Teil von Microsoft 365 Security und gleichzeitig der, an dem am häufigsten die ganze Kette reißt. Lizenzen kann man kaufen. Richtlinien kann man klicken. Aber die Frage, wer freitags um 22:40 Uhr tatsächlich auf einen Alarm schaut und was diese Person dann darf, beantwortet kein Produktdatenblatt. Genau darum geht es hier: wie du die eingebauten Microsoft 365 Alert Policies schärfst, welche eigenen Richtlinien du zusätzlich brauchst und wie du den Weg vom Ereignis bis zu einer handelnden Person so baust, dass er nicht in einem Outlook-Ordner endet.

Der Beitrag gehört zur Serie [Microsoft 365 Security](#), die die Handlungsfelder von der Anmeldung bis zum Notfall durchgeht. Die Alarmierung ist darin das Bindeglied: Sie macht aus Konfiguration Betrieb.

WARNUNG · Ein Alarm im ungelesenen Postfach ist Dekoration

Du kannst zwanzig Richtlinien aktivieren, Schwellwerte feinschleifen und Schweregrade vergeben. Wenn die Benachrichtigung in einem Postfach landet, das keine feste Zuständigkeit hat, hast du kein Sicherheitsmonitoring gebaut, sondern ein Archiv für spätere Schuldzuweisungen.

Der Test dazu ist brutal einfach und dauert fünf Minuten: Schick eine Nachricht an dein Alarmpostfach und warte. Wenn nicht innerhalb der vereinbarten Reaktionszeit jemand antwortet, ist die Kette offen. Nicht schwach, nicht verbesserungswürdig — offen. Und zwar seit dem Tag, an dem du sie eingerichtet hast.

Warum die meisten Alarme im Nichts verpuffen

Die Standardsituation im Mittelstand sieht ungefähr so aus. Irgendwann hat jemand im Defender-Portal gesehen, dass es Alarmrichtlinien gibt. Weil man auf Nummer sicher gehen wollte, wurden bei einer Handvoll Richtlinien E-Mail-Benachrichtigungen aktiviert und als Empfänger eine Verteilerliste eingetragen, in der die halbe IT steht und aus historischen Gründen auch noch der ehemalige Dienstleister. Nach drei Wochen hat der Erste eine Outlook-Regel gebaut, die alles mit diesem Betreff in einen Unterordner schiebt. Nach acht Wochen haben es alle anderen auch getan. Damit war das Thema erledigt — im schlechten Sinne.

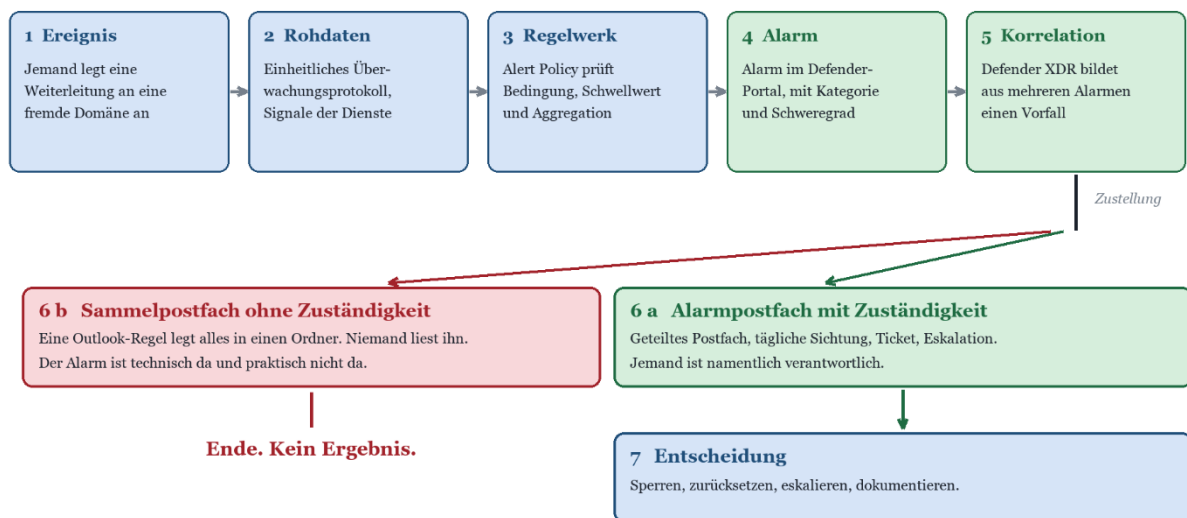
Das Problem ist nicht Faulheit, sondern Mathematik. Ein durchschnittlicher Tenant mit ein paar hundert Postfächern erzeugt in der Grundkonfiguration eine erhebliche Menge informativer Alarme, die zu neunundneunzig Prozent nichts bedeuten: als Junk gemeldete Nachrichten,

abgeschlossene Prüfungen eingereicherter Mails, ablaufende Einträge in der Tenant Allow/Block List, gestartete eDiscovery-Suchen. Diese Alarme sind fachlich korrekt und in der Summe tödlich, weil sie die wenigen wirklich wichtigen Meldungen unter sich begraben.

Wer Alarmierung ernst nimmt, arbeitet deshalb an zwei Enden gleichzeitig: Er reduziert das Rauschen aggressiv und baut für den kleinen Rest einen Kanal, der wirklich Aufmerksamkeit erzeugt. Nur zu reduzieren führt zu einem stillen Tenant, in dem nichts mehr auffällt. Nur zu benachrichtigen führt zu dem Ordner, den niemand öffnet.

Der Alarmweg

Vom Ereignis bis zu der Person, die etwas entscheidet



Skizze 1: Der Alarmweg vom Ereignis bis zu der Person, die entscheidet. Die Abzweigung nach unten links ist der Normalfall in Tenants ohne festgelegte Zuständigkeit.

Die drei Bruchstellen der Kette

Wenn du in einem Kundenprojekt die Alarmierung auseinandernimmst, findest du fast immer dieselben drei Stellen, an denen der Weg endet.

Bruchstelle	Symptom	Woran es liegt	Gegenmittel
Erkennung fehlt	Es gibt gar keinen Alarm für den Vorgang, der später zum Vorfall wird.	Nur die Standardrichtlinien sind aktiv. Externe Weiterleitung, erteilte Einwilligungen oder Rollenzuweisungen werden nicht überwacht.	Eigene Richtlinien für die vier klassischen Lücken anlegen.
Zustellung verpufft	Der Alarm existiert im Portal, aber niemand erfährt davon.	Benachrichtigung nicht aktiviert, Empfänger ein toter Verteiler, Nachricht im Junk-Ordner gelandet.	Ein geteiltes Postfach mit Zuständigkeit, Zustellung testen, Absender freigeben.
Reaktion ist undefiniert	Die Meldung wird gelesen, aber niemand weiß, was jetzt passieren	Kein Ablauf, keine Eskalationsstufen, keine Befugnis zum Sperren eines	Eskalationstreppe mit Namen und Zeiten, verankert im Notfallplan.

	soll.	Kontos.	
--	-------	---------	--

Auffällig ist, dass nur die erste Bruchstelle technisch ist. Die anderen beiden sind Organisation. Genau deshalb scheitert Alarmierung so zuverlässig in Projekten, die ausschließlich in der Portaloberfläche stattfinden.

Wie Alert Policies technisch funktionieren

Bevor du an Schwellwerten drehst, lohnt sich ein sauberes Modell davon, was eine Alarmrichtlinie eigentlich ist. Du findest die Richtlinien im Microsoft Defender Portal unter **E-Mail und Zusammenarbeit > Richtlinien und Regeln > Warnungsrichtlinie**, direkt erreichbar unter <https://security.microsoft.com/alertpoliciesv2>. Die erzeugten Alarme landen anschließend unter **Incidents und Warnungen > Warnungen**.

Der Aufbau einer Richtlinie

Jede Alarmrichtlinie besteht aus denselben Bausteinen, egal ob sie von Microsoft mitgeliefert wird oder von dir stammt:

- **Aktivität.** Der überwachte Vorgang, in der Regel eine Operation aus dem einheitlichen Überwachungsprotokoll — etwa das Anlegen einer Posteingangsregel oder eine Rollenzuweisung.
- **Bedingungen.** Zusätzliche Filter: bestimmte Konten, IP-Adressen oder Adressbereiche, Dateinamen, Ziel-URLs. Auch Benutzertags lassen sich als Bedingung nutzen, was den Alarm gleich mit Kontext zur betroffenen Person versieht.
- **Auslösebedingung.** Jedes Mal, ab einem Schwellwert innerhalb eines Zeitfensters, oder wenn die Häufigkeit für deine Organisation ungewöhnlich wird.
- **Kategorie.** Datenverlustprävention, Informationsgovernance, Nachrichtenfluss, Berechtigungen, Bedrohungsverwaltung oder Sonstige. Die Kategorie entscheidet mit darüber, wer den Alarm überhaupt sehen darf.
- **Schweregrad.** Niedrig, Mittel, Hoch oder Informativ. Klingt nach Kosmetik, ist aber der wichtigste Filter für alles, was danach kommt.
- **Benachrichtigung.** Empfängerliste und ein Tageslimit für Nachrichten. Ist das Limit erreicht, verstummt die Richtlinie für diesen Tag — im Portal erscheinen die Alarme trotzdem weiter.

FAKTEN • Verhalten, das im Betrieb regelmäßig überrascht

Diese Randbedingungen erklären die meisten Rückfragen nach dem ersten Konfigurationstag:

- Nach dem Anlegen oder Ändern einer Richtlinie dauert es **bis zu 24 Stunden**, bis Alarme ausgelöst werden können. Die Richtlinie muss erst zur Erkennungsmaschine synchronisiert werden. Wer unmittelbar nach dem Speichern testet, testet nichts.
- Bei Erkennung auf Basis ungewöhnlicher Aktivität baut Microsoft zunächst eine Grundlinie auf. Das dauert **bis zu sieben Tage**, in denen keine Alarme entstehen.
- Beim Schwellwertverfahren muss der Wert mindestens **3** betragen, das Zeitfenster mehr als **60 Minuten**.
- Einige Standardrichtlinien enthalten Filter, die in der Portaloberfläche gar nicht sichtbar sind.

Wenn du wissen willst, warum eine Richtlinie nicht auslöst, hilft nur die PowerShell.

Der letzte Punkt ist im Alltag der ärgerlichste. Die vollständigen Eigenschaften einer Standardrichtlinie bekommst du nur über die Security-und-Compliance-PowerShell:

```
Connect-IPPSSession

Get-ProtectionAlert -Identity "Suspicious email forwarding activity" | Format-List

# Zusätzlich die zugrunde liegende Regeldefinition anzeigen:
Get-ProtectionAlert -Identity "Suspicious email forwarding activity" -IncludeRuleXml
```

Die drei Aggregationsarten

Der praktisch wichtigste Hebel gegen Rauschen ist die Aggregation. Sie entscheidet, ob du eine Mail pro Ereignis bekommst oder eine pro Welle. In der PowerShell heißt der Parameter `AggregationType`, im Portal steht er hinter der Frage, wann ein Alarm ausgelöst werden soll.

Aggregationsart	Verhalten	Sinnvoll für	Fallstrick
None	Jedes einzelne Vorkommnis erzeugt einen Alarm.	Seltene, eindeutige Ereignisse: neue Rollenzuweisung, Anmeldung eines Break-Glass-Kontos, Änderung an Verbindern.	Bei häufigen Aktivitäten produziert diese Einstellung Massenpost.
SimpleAggregation	Alarm, wenn der Schwellwert innerhalb des Zeitfensters überschritten wird. Voreinstellung im Portal.	Mengenphänomene mit bekanntem Normalmaß: Downloads, Löschungen, externe Freigaben.	Schwellwert mindestens 3, Zeitfenster über 60 Minuten. Zu hohe Werte machen die Richtlinie stumm.
AnomalousAggregation	Alarm, wenn die Häufigkeit die gelernte Grundlinie deutlich übersteigt.	Alles, wo du das Normalmaß nicht kennst und auch nicht schätzen willst.	Sieben Tage Anlaufzeit, benötigt die höhere Lizenzstufe, und die Grundlinie lernt schlechte Gewohnheiten mit.

Ein unterschätzter vierter Hebel steckt im Parameter `NotifyUserOnFilterMatch`. Damit bekommst du bei einer aggregierten Richtlinie trotzdem eine Frühwarnung beim ersten Treffer, während der eigentliche Alarm weiterhin erst beim Überschreiten des Schwellwerts entsteht. Für Massen-Download-Szenarien ist das genau die richtige Mischung aus Ruhe und Reaktionsfähigkeit. Ebenso nützlich ist `AlertBy`: Der Parameter sorgt dafür, dass im Alarm überhaupt die betroffene Entität auftaucht. Ohne ihn bekommst du eine Meldung ohne Angabe, wer eigentlich gemeint ist — ein Klassiker unter den selbstgebauten Enttäuschungen.

Lizenzen und Rollen, ohne Schönfärberei

Alarmrichtlinien gibt es in allen gängigen Enterprise-Plänen. Die interessanten Funktionen nicht. Schwellwertbasierte und anomaliebasierte Auslösung setzen E5 beziehungsweise G5 voraus — oder

E1, F1, G1, E3, F3 oder G3 mit einem passenden Zusatzabonnement wie Defender for Office 365 Plan 2, Microsoft 365 E5 Compliance oder dem Zusatz für eDiscovery und Audit. Wer nur E3 hat, kann eigene Richtlinien ausschließlich mit -AggregationType None bauen, also mit einem Alarm pro Ereignis. Das ist kein Beinbruch, verlangt aber eine deutlich sorgfältigere Auswahl der überwachten Vorgänge.

Bei den Berechtigungen gilt: Zum Ansehen der Richtlinien brauchst du die Rolle **Nur-Anzeigen-Warnungen verwalten**, zum Anlegen und Ändern die Rolle **Warnungen verwalten** oder Organisationskonfiguration. In Tenants mit einheitlicher rollenbasierter Zugriffssteuerung von Defender XDR entspricht das lesend den Sicherheitsdaten-Grundlagen und schreibend der Berechtigung für Erkennungsoptimierung. Was du ausdrücklich nicht brauchst, ist die Rolle des globalen Administrators. Microsoft weist inzwischen in der eigenen Dokumentation darauf hin, dass diese Rolle Notfällen vorbehalten bleiben sollte. Wie du die passenden Konten dafür baust und überwachst, steht in [Break-Glass-Konten anlegen und überwachen](#).

Standard-Richtlinien: welche du schärfst, welche du abschaltest

Microsoft liefert eine ganze Reihe von Systemrichtlinien mit. Sie stehen in der Übersicht fett gedruckt und tragen den Typ **System**. Bei ihnen kannst du genau drei Dinge ändern: an- und ausschalten, Empfänger setzen, Tageslimit konfigurieren. Alles andere ist festgenagelt. Das ist weniger schlimm, als es klingt — die eigentliche Arbeit besteht ohnehin darin, zu entscheiden, welche Richtlinie es wert ist, jemanden aus dem Feierabend zu holen.

Triage-Matrix für Alarme

Was du sofort meldest, was du sammelst und was du abschaltest



Skizze 2: Nicht jeder Alarm verdient eine Benachrichtigung. Die Einordnung nach Häufigkeit und Schadenspotenzial entscheidet über den Kanal.

Die Kandidaten für eine sofortige Benachrichtigung

Die folgenden Systemrichtlinien gehören in jedem Tenant an einen Kanal, den jemand zeitnah liest. Sie sind selten genug, um nicht zu nerven, und teuer genug, um Aufmerksamkeit zu rechtfertigen.

Standardrichtlinie	Grad	Warum sie zählt	Empfehlung
Suspicious email forwarding activity	Hoch	Automatische Weiterleitung an ein verdächtiges externes Konto — das klassische Frühwarnsignal für ein übernommenes Postfach.	Benachrichtigung an das Alarmpostfach, Sichtung binnen einer Stunde.
User restricted from sending email	Hoch	Ein Konto wurde vom Postausgang ausgesperrt. Das passiert nicht aus Versehen.	Sofort. Das Konto gilt bis zum Beweis des Gegenteils als kompromittiert.
Suspicious connector activity	Hoch	Verdächtige Aktivität auf einem eingehenden Verbinder, Mail wird blockiert.	Sofort. Verbinder sind ein beliebter Weg, den Mailfluss zu manipulieren.
Tenant restricted from sending email	Hoch	Der gesamte Tenant darf nicht mehr senden. Der Betriebsstillstand ist bereits da.	Sofort, zusätzlich Eskalation an die IT-Leitung.
Potential nation-state activity	Hoch	Microsoft meldet einen Übernahmever such auf Konten deines Tenants.	Sofort. Diese Meldung kommt selten und nie ohne Grund.
Elevation of Exchange admin privilege	Niedrig	Jemand wurde in eine administrative Rollengruppe in Exchange Online aufgenommen.	Der Schweregrad ist niedrig, die Relevanz nicht. Benachrichtigung aktivieren.
Email sending limit exceeded	Mittel	Ein Konto hat mehr Mail versendet, als die Richtlinie für ausgehenden Spam erlaubt.	Benachrichtigung, kombiniert mit einem Blick auf die Anmeldeorte.
Messages containing malicious entity not removed after delivery	Mittel	Die automatische Bereinigung ist fehlgeschlagen, die Nachricht liegt noch im Postfach.	Benachrichtigung, weil hier tatsächlich Handarbeit nötig wird.

Die Kandidaten für den Papierkorb

Genauso wichtig ist die Gegenrichtung. Diese Richtlinien laufen in vielen Tenants aktiv mit und erzeugen den Großteil des Rauschens, ohne je zu einer Entscheidung zu führen.

Richtlinie oder Gruppe	Problem	Maßnahme
Email reported by user as junk / not junk	Reine Mengenmeldung. Der Wert steckt im Bericht, nicht in einer Mail an die IT.	Benachrichtigung aus, Richtlinie an. Auswertung über die Berichte.
Admin submission result completed	Eine Erinnerung an die eigene Arbeit vom Vortag.	Benachrichtigung aus.
eDiscovery search started or exported	In Organisationen mit regelmäßiger Recherche schlicht Alltag.	Benachrichtigung aus, sofern die Personalvertretung nichts anderes

		vereinbart hat.
Email messages containing malware removed after delivery	Wurde durch die Richtlinie für schädliche Dateien abgelöst und läuft doppelt.	Alte Richtlinie deaktivieren, Nachfolgerichtlinie nutzen.
Email messages containing phish URLs removed after delivery	Ebenfalls abgelöst, diesmal durch die Richtlinie für schädliche URLs.	Alte Richtlinie deaktivieren.
Unusual volume of external file sharing	Wird von Microsoft wegen hoher Fehlalarmquote schrittweise außer Betrieb genommen.	Durch eine eigene Richtlinie mit passendem Schwellwert ersetzen.

TIPP · Erst messen, dann abschalten

Bevor du eine Richtlinie deaktivierst, sieh dir eine Woche lang an, wie viele Alarme sie erzeugt und wie viele davon zu einer Handlung geführt haben. Die Quote aus beidem ist die einzige Kennzahl, die im Alarmbetrieb wirklich zählt.

Die mildere Alternative zum Abschalten ist die Alarmoptimierung unter **Einstellungen** > **Microsoft Defender XDR** > **Warnungsoptimierung**. Damit unterdrückst du gezielt einzelne Ausprägungen statt der ganzen Erkennung. Achtung: Auf Alarme aus eigenen Erkennungsregeln wirken diese Regeln nicht.

Eigene Richtlinien: die vier, die fast immer fehlen

Die Standardrichtlinien decken vor allem den Mailfluss und die Bedrohungsabwehr ab. Vier Vorgänge, die in echten Vorfällen regelmäßig eine Rolle spielen, sind darin gar nicht oder nur unzureichend abgebildet. Wenn du an einem einzigen Nachmittag genau eine Sache ändern willst: diese vier.

Externe Weiterleitung von E-Mail

Der Klassiker. Wer ein Postfach übernimmt, will als Erstes still mitlesen, ohne sich ständig neu anmelden zu müssen. Eine Posteingangsregel, die Kopien an eine externe Adresse schickt, ist dafür perfekt: unauffällig, dauerhaft und aus Sicht des Postfachs völlig regulär. Die mitgelieferte Richtlinie **Creation of forwarding/redirect rule** erfasst allerdings nur Regeln, die über Outlook im Web oder über die Exchange-Online-PowerShell angelegt werden, und trägt den Schweregrad **Informativ**. Beides ist zu wenig.

```
Connect-IPPSSession
```

```
New-ProtectionAlert -Name "ORG-Weiterleitungsregel angelegt" `
-Category ThreatManagement -ThreatType Activity `
-Operation "New-InboxRule" -AggregationType None `
-Severity High -AlertBy User `
-NotifyUser "alarm@contoso.de" -NotificationEnabled $true `
-Description "Meldet jede neu angelegte Posteingangsregel."
```

```
# Zweite Richtlinie für die Weiterleitung auf Postfachebene:
New-ProtectionAlert -Name "ORG-Postfach-Weiterleitung gesetzt" `
-Category ThreatManagement -ThreatType Activity `
```

```
-Operation "Set-Mailbox" -AggregationType None `
-Severity High -AlertBy User -NotifyUser "alarm@contoso.de"
```

Technisch sauberer bleibt es, externe automatische Weiterleitung in der Richtlinie für ausgehenden Spam gleich ganz zu unterbinden. Der Alarm bleibt trotzdem sinnvoll: Der Versuch ist die Information, nicht der Erfolg. Wie das in eine Gesamthärtung passt, steht in [Tenant-Härtung: die 20 wichtigsten Schrauben](#).

Massen-Download aus SharePoint und OneDrive

Zwei Szenarien, ein Signal: Entweder jemand schafft Daten aus dem Haus, oder eine Person verabschiedet sich mit dem gesamten Projektlaufwerk in ein neues Arbeitsverhältnis. In beiden Fällen sieht die Telemetrie gleich aus — sehr viele Downloads in kurzer Zeit durch ein einzelnes Konto.

Hier ist Aggregation Pflicht. Ein Alarm pro heruntergeladener Datei wäre selbst für geduldige Menschen zu viel. Setz einen Schwellwert, der zu deinem Betrieb passt, und begrenze zusätzlich die Zahl der Benachrichtigungen pro Tag.

```
New-ProtectionAlert -Name "ORG-Massen-Download durch ein Konto" `
-Category ThreatManagement -ThreatType Activity `
-Operation "FileDownloaded" -AggregationType SimpleAggregation `
-Threshold 300 -TimeWindow 120 -AlertBy User `
-Severity Medium -NotifyUser "alarm@contoso.de" `
-NotifyUserOnFilterMatch $false `
-NotifyUserThrottleThreshold 5 -NotifyUserThrottleWindow 1440
```

Wer Defender for Cloud Apps im Einsatz hat, bekommt für dieses Muster zusätzlich die Anomalieerkennung und die Möglichkeit, Aktivitätsrichtlinien mit Governance-Aktionen zu verbinden — also nicht nur zu melden, sondern die Sitzung gleich zu beenden. Wann sich das im Mittelstand rechnet, behandelt [Defender for Cloud Apps im Mittelstand](#).

WICHTIG · Massen-Download ist mitbestimmungsrelevant

Eine Richtlinie, die das Downloadverhalten einzelner Konten auswertet, ist eine technische Einrichtung zur Verhaltens- und Leistungskontrolle im Sinne des Betriebsverfassungsgesetzes. Das heißt nicht, dass du sie nicht bauen darfst — es heißt, dass du sie vorher mit der Personalvertretung besprichst und Zweck, Empfängerkreis, Aufbewahrung und Auswertungsverfahren schriftlich festhältst.

Der pragmatische Weg: Zweckbindung auf Sicherheitsvorfälle, Vier-Augen-Prinzip bei der Auswertung, klare Löschfristen. Die Details stehen in [Security-Monitoring und Betriebsrat: was mitbestimmungspflichtig ist](#).

Neuer Administrator mit hohen Rechten

Ein frisch angelegter globaler Administrator ist entweder ein geplanter Vorgang, von dem du weißt, oder das Ende deiner Zuständigkeit für diesen Tenant. Einen dritten Fall gibt es nicht. Trotzdem ist genau dieses Ereignis in der Standardausstattung nicht mit einer Benachrichtigung hinterlegt: Die mitgelieferte Richtlinie deckt die Exchange-Rollengruppen ab, nicht die Verzeichnisrollen von Microsoft Entra ID.

```
New-ProtectionAlert -Name "ORG-Privilegierte Rolle zugewiesen" `
-Category AccessGovernance -ThreatType Activity `
-Operation "Add member to role." -AggregationType None `
-Severity High -AlertBy User `
-NotifyUser "alarm@contoso.de","it-leitung@contoso.de" `
-NotificationEnabled $true `
-Description "Meldet jede Zuweisung einer Verzeichnisrolle."
```

Wer Privileged Identity Management einsetzt, bekommt zusätzlich die dortigen Sicherheitswarnungen — insbesondere die Meldung über Rollen, die am Verfahren vorbei direkt zugewiesen wurden. Diese Meldungen gehen in der Voreinstellung an die Inhaber privilegierter Rollen, was praktisch klingt und in der Praxis bedeutet, dass sie in denselben Postfächern landen wie alles andere. Trag dein Alarmpostfach mit ein.

Einwilligung für eine Anwendung erteilt

Der leiseste der vier Vorgänge und derjenige, der am längsten unentdeckt bleibt. Eine Person klickt in einem gut gemachten Dialog auf Zustimmung, und eine fremde Anwendung hat dauerhaften Zugriff auf Postfach, Dateien und Kalender — ohne Kennwort, ohne zweiten Faktor, und ohne dass ein Zurücksetzen der Anmeldedaten daran etwas ändert. Genau deshalb ist die erteilte Einwilligung inzwischen ein Standardschritt in ernstzunehmenden Angriffsketten.

```
New-ProtectionAlert -Name "ORG-Einwilligung für Anwendung erteilt" `
-Category AccessGovernance -ThreatType Activity `
-Operation "Consent to application." -AggregationType None `
-Severity High -AlertBy User `
-NotifyUser "alarm@contoso.de" -NotificationEnabled $true
```

Der Alarm ist die Rückfallebene, nicht die Lösung. Die Lösung heißt: Einwilligung durch Endanwender einschränken und einen Genehmigungsablauf einrichten. Beides beschreibt [App-Registrierungen und Consent-Governance](#) im Detail. Der Alarm bleibt trotzdem stehen, denn Genehmigungsabläufe haben die unangenehme Eigenschaft, unter Zeitdruck umgangen zu werden.

TIPP · Namenskonvention und Sicherungskopie

Gib eigenen Richtlinien einen Präfix, etwa ORG-, und schreib in die Beschreibung, wer sie warum angelegt hat und wann sie zuletzt geprüft wurde. In einem Tenant mit siebzig Richtlinien ist das der Unterschied zwischen Pflege und Archäologie.

Exportiere die Konfiguration regelmäßig mit `Get-ProtectionAlert | Export-Clixml` und leg den Export dorthin, wo auch der Rest deiner Betriebsdokumentation liegt. Nach einem Tenant-Umbau willst du nachsehen können, was vorher galt.

Der Empfängerkanal: ein Postfach, das jemand liest

Jetzt der Teil, an dem die meisten Projekte scheitern. Du hast saubere Richtlinien mit vernünftigen Schwellwerten. Wohin gehen die Meldungen?

Das Alarmpostfach

Die Antwort ist nicht der Verteiler der IT-Abteilung und schon gar nicht die persönliche Adresse der Person, die zufällig das Projekt gemacht hat. Die Antwort ist ein geteiltes Postfach mit einem sprechenden Namen, auf das ein fest benannter Personenkreis Zugriff hat. Die Anforderungen daran sind unspektakulär und werden trotzdem selten alle erfüllt.

Anforderung	Warum	Prüffrage
Geteiltes Postfach, keine Verteilergruppe	Ein Postfach hat einen Bearbeitungsstand. Ein Verteiler hat nur Kopien.	Sind Gelesen-Status und Kategorien für alle sichtbar?
Mindestens zwei, höchstens fünf Personen mit Zugriff	Unter zwei ist es ein Einzelfallrisiko, über fünf fühlt sich niemand mehr zuständig.	Gibt es eine aktuelle Namensliste?
Absenderadressen als vertrauenswürdig eingestuft	Die Alarmmail im Junk-Ordner ist der häufigste stille Ausfall überhaupt.	Landet eine Testnachricht wirklich im Posteingang?
Weiterleitung in ein Ticketsystem	Sichtung, Zuweisung und Nachweis in einem Werkzeug statt in Outlook-Kategorien.	Erzeugt jede Alarmmail ein Ticket?
Zweiter Kanal für hohe Schweregrade	E-Mail ist außerhalb der Arbeitszeit kein Alarmierungsmittel.	Kommt die Meldung auf einem Telefon an, das klingelt?
Vierteljährlicher Zustelltest	Postfächer, Regeln und Personen ändern sich. Die Kette altert leise.	Ist der letzte Test dokumentiert?

Der zweite Kanal ist der Punkt, an dem viele stützen. E-Mail ist ein hervorragendes Medium für Arbeitsvorrat und ein miserables für Dringlichkeit. Alles, was einen hohen Schweregrad hat und außerhalb der Bürozeiten passieren kann, braucht einen Weg auf ein Gerät, das klingelt. Ob das ein Teams-Kanal mit Push-Meldung, eine Rufbereitschaftslösung oder eine schlichte SMS aus einem Playbook ist, ist zweitrangig — dass es ihn gibt, nicht.

Eskalation mit Namen und Uhrzeiten

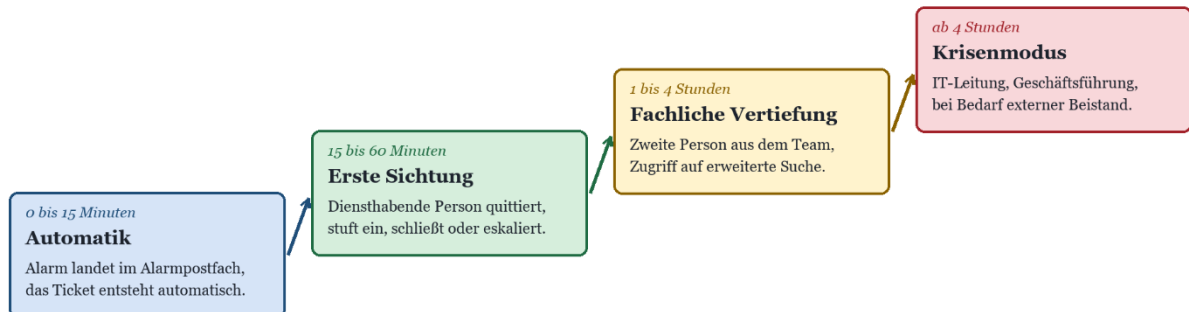
Eskalation ist kein Organigramm, sondern eine Uhr. Die entscheidende Eigenschaft: Sie läuft von selbst weiter, wenn niemand reagiert. Ein Ablauf, der voraussetzt, dass die richtige Person die Lage von sich aus als schwerwiegend erkennt, ist genau in dem Moment nutzlos, in dem er gebraucht wird.

Die Eskalationstreppe

Wer wann übernimmt, wenn niemand reagiert

Regel: Jede Stufe hat einen Namen, keine Rolle im Konjunktiv.

Ohne quittierte Übernahme läuft der Alarm automatisch eine Stufe höher.



Skizze 3: Vier Stufen, feste Zeiten, automatische Weitergabe. Ohne quittierte Übernahme geht der Alarm eine Stufe höher.

Die Zeiten in der Skizze sind ein Vorschlag für einen mittelständischen Betrieb ohne eigenes Sicherheitsteam. Wer rund um die Uhr produziert, wird enger takten müssen; wer im Zwei-Personen-Betrieb arbeitet, wird die dritte Stufe an einen Dienstleister vergeben. Wichtig ist nicht die konkrete Zahl, sondern dass es eine gibt und dass sie irgendwo steht, wo man sie nachts findet. Der richtige Ort dafür ist der [Incident-Response-Plan für Microsoft 365](#) — die Alarmierung ist dessen Eingangstür, nicht sein Ersatz.

WARNUNG · Die Befugnis muss vor dem Vorfall geklärt sein

Der häufigste Grund, warum ein erkannter Vorfall trotzdem stundenlang weiterläuft, ist nicht fehlende Technik, sondern fehlende Erlaubnis. Die diensthabende Person sieht den Alarm, sieht das übernommene Konto der Vertriebsleitung und traut sich nicht, es zu sperren. Das ist kein Charakterfehler, sondern ein Führungsver säumnis.

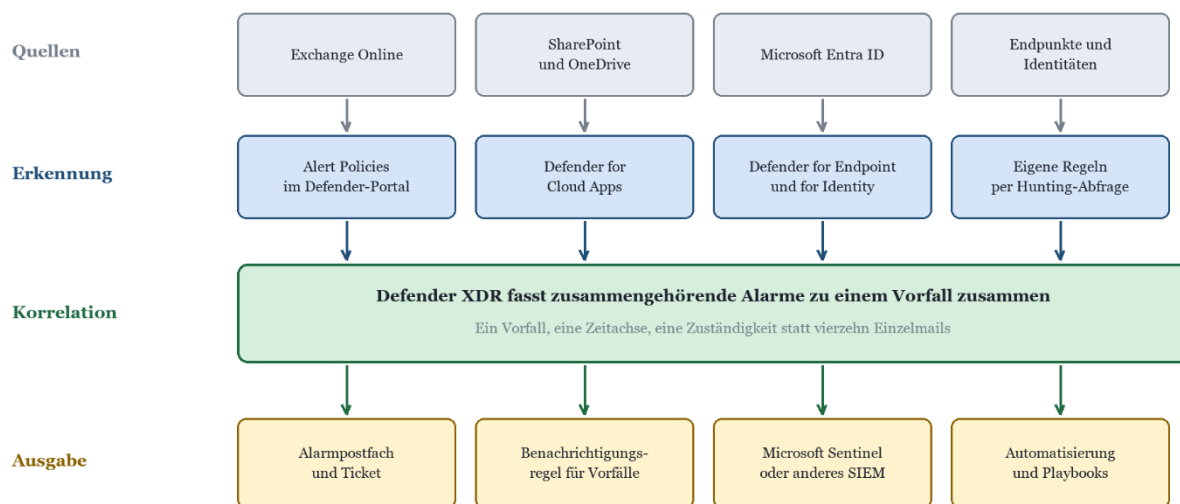
Halte deshalb schriftlich fest, wer welche Sofortmaßnahme ohne Rücksprache durchführen darf: Konto sperren, Sitzungen widerrufen, Anmeldedaten zurücksetzen, Weiterleitung entfernen, Anwendung deaktivieren. Mit Rückendeckung der Geschäftsführung, auf einer Seite, unterschrieben. Ohne dieses Blatt ist deine Eskalationstreppe eine Empfehlung.

Verbindung zu Defender XDR und zum SIEM

Alarmrichtlinien sind nur eine von mehreren Quellen. Parallel dazu erzeugen Defender for Office 365, Defender for Endpoint, Defender for Identity, Defender for Cloud Apps und der Identitätsschutz von Entra ID eigene Signale. Wenn all das ungefiltert in dein Alarmpostfach läuft, hast du das Rauschproblem nur verlagert.

Vom Signal zum Vorfall

Wie Alert Policies, Defender XDR und ein SIEM zusammenspielen



Erst wenn der letzte Kasten eine Person mit Namen enthält, ist die Kette geschlossen.

Skizze 4: Quellen, Erkennung, Korrelation, Ausgabe. Die Korrelationsebene ist der Grund, warum du nicht jede Einzelmeldung zustellen musst.

Warum Vorfälle die bessere Einheit sind

Defender XDR fasst zusammengehörende Alarme aus allen angebundenen Quellen zu einem Vorfall zusammen und führt Vorfälle bei Bedarf weiter zusammen, wenn die Korrelationslogik gemeinsame Elemente erkennt. Aus vierzehn Einzelmeldungen — verdächtige Anmeldung, neue Posteingangsregel, ungewöhnlicher Download, Massenversand — wird ein Vorfall mit einer Zeitachse. Das ist nicht nur bequemer, es ist auch die einzige Darstellung, in der man den Angriff als Ablauf erkennt statt als Sammlung von Zufällen. Wie gut das funktioniert, hängt übrigens daran, wie viele Entitäten deine Alarme mitbringen — noch ein Argument für den Parameter AlertBy.

Praktische Konsequenz: Der Hauptkanal deiner Benachrichtigung sollte auf Vorfällen aufsetzen, nicht auf Einzelalarmen. Die Regeln dafür legst du unter **Einstellungen** > **Microsoft Defender XDR** > **E-Mail-Benachrichtigungen** an. Dort kannst du nach Schweregrad filtern, nach Dienstquelle und Erkennungsquelle unterscheiden, den Gerätegruppenbereich einschränken und festlegen, dass pro Vorfall genau eine Nachricht verschickt wird. Diese letzte Einstellung ist der Unterschied zwischen Information und Belästigung. Zum Anlegen brauchst du die Berechtigung zum Verwalten von Sicherheitseinstellungen; nutze die Testfunktion für den Versand gleich mit.

Eine tragfähige Aufteilung sieht in der Praxis so aus:

Kanal	Inhalt	Empfänger	Erwartete Reaktion
Benachrichtigungsregel für Vorfälle, Schweregrad Hoch	Korrelierte Vorfälle aus allen Defender-Diensten.	Alarmpostfach und zweiter Kanal mit Push-Meldung.	Sichtung binnen 60 Minuten, auch abends.
Alarmrichtlinien mit hohem Schweregrad	Die vier eigenen Richtlinien plus die kritischen Systemrichtlinien.	Alarmpostfach.	Sichtung binnen 60 Minuten während der Arbeitszeit.

Portal, ohne Benachrichtigung	Alles Übrige, inklusive der informativen Systemrichtlinien.	Niemand per Mail.	Tägliche Sichtung als Arbeitsvorrat.
SIEM oder Microsoft Sentinel	Vollständiger Alarm- und Vorfallstrom plus Rohprotokolle.	Maschine, nicht Mensch.	Automatische Auswertung, Aufbewahrung, Korrelation mit anderen Quellen.

Wann ein SIEM dazukommt

Die Grenze der Bordmittel ist erreicht, wenn du eines von drei Dingen brauchst: längere Aufbewahrung, als die Portale bieten; Korrelation mit Quellen außerhalb von Microsoft 365 — Firewall, Verzeichnisdienst vor Ort, Fachanwendungen; oder Automatisierung, die über die eingebauten Reaktionen hinausgeht. Dann lohnt sich die Anbindung an Microsoft Sentinel. Vorher ist sie ein teurer Weg, dieselben Alarme in einer zweiten Oberfläche nicht zu lesen. Die Abwägung im Detail steht in [Microsoft Sentinel anbinden: wann es sich lohnt](#).

Eigene Erkennungsregeln als Ergänzung

Für Muster, die sich mit den vorgegebenen Operationen nicht abbilden lassen, gibt es benutzerdefinierte Erkennungsregeln auf Basis von Hunting-Abfragen. Sie laufen in festen Intervallen, erzeugen Alarme, können Reaktionen auslösen und fließen in die Korrelation ein. Der Preis dafür ist Pflege: Eine Abfrage, die niemand mehr versteht, ist nach der nächsten Schemaänderung stumm. Merk dir außerdem, dass die eingebauten Optimierungsregeln auf Alarme aus eigenen Erkennungsregeln nicht wirken — selbstgebautes Rauschen musst du selbst dämpfen.

Betrieb: tunen, messen, aufräumen

Alarmierung ist kein Projekt mit Abnahme, sondern ein Zustand, der gepflegt werden will. Der Aufwand dafür ist überschaubar, wenn er regelmäßig stattfindet, und unbezahlbar, wenn er zwei Jahre liegen bleibt.

Ein Rhythmus, der sich durchhalten lässt

Takt	Was zu tun ist	Dauer
Täglich	Sichtung des Alarmpostfachs und der offenen Vorfälle: quittieren, zuweisen, schließen.	10 bis 20 Minuten
Wöchentlich	Blick auf die Alarme ohne Benachrichtigung. Gibt es Muster, die eine Benachrichtigung verdienen?	20 Minuten
Monatlich	Kennzahlen erheben: Alarme je Richtlinie, Anteil mit Handlung, mittlere Zeit bis zur Quittierung.	30 Minuten
Quartalsweise	Zustelltest, Empfängerliste gegen die Personalliste prüfen, neue Standardrichtlinien sichten.	1 Stunde

Jährlich	Vollständige Durchsicht aller Richtlinien, Abgleich mit dem Notfallplan, Übung.	1 Tag
----------	---	-------

Die Kennzahlen, die etwas aussagen

- **Handlungsquote je Richtlinie.** Anteil der Alarme, die zu einer Maßnahme geführt haben. Unter fünf Prozent über mehrere Monate bedeutet: Benachrichtigung abschalten oder Schwellwert anheben.
- **Mittlere Zeit bis zur Quittierung.** Wie lange dauert es, bis ein Alarm einen Bearbeitungsstand bekommt? Diese Zahl misst deine Organisation, nicht deine Technik.
- **Anteil außerhalb der Arbeitszeit.** Wenn ein relevanter Teil der Alarme nachts und am Wochenende entsteht, brauchst du eine Rufbereitschaft und keine weitere Richtlinie.
- **Alarme ohne Empfänger.** Richtlinien mit aktiver Benachrichtigung, deren Empfängeradresse nicht mehr existiert. Diese Zahl sollte null sein und ist es fast nie.

Für die Berichterstattung nach oben taugen diese Zahlen übrigens deutlich besser als jede Punktzahl aus einer Bewertungsoberfläche. Sie beschreiben, ob dein Betrieb funktioniert, nicht ob deine Konfiguration einem Idealbild entspricht. Wie du daraus eine Vorlage machst, die in einer Sitzung der Geschäftsführung besteht, zeigt [Security-Reporting für die Geschäftsführung](#). Wie du die Bewertungsoberfläche trotzdem sinnvoll nutzt, statt Punkte zu jagen, steht in [Secure Score: sinnvoll nutzen statt Punktejagd](#).

FAKTEN · Ein realistischer Zielzustand

Für einen Tenant mit 300 bis 800 Postfächern und ohne eigenes Sicherheitsteam sind diese Größenordnungen erreichbar und ausreichend:

- Zwischen 3 und 8 Alarmmails pro Woche im Alarmpostfach, nicht mehr.
- Zwischen 4 und 10 aktive Richtlinien mit Benachrichtigung, davon 4 selbst gebaut.
- Sichtung an jedem Arbeitstag, quittiert von einer namentlich benannten Person.
- Reaktionszeit von einer Stunde innerhalb der Arbeitszeit, vier Stunden außerhalb.
- Ein dokumentierter Zustelltest pro Quartal, eine Übung pro Jahr.

Umsetzung in einer Woche

Wenn du das Thema von null aufsetzt, ist der folgende Ablauf realistisch. Er kommt ohne Projektstrukturplan aus und liefert nach fünf Arbeitstagen einen Zustand, der besser ist als der in den meisten Tenants.

1. **Tag 1 — Bestandsaufnahme.** Alle Richtlinien exportieren, Empfänger prüfen, tote Adressen notieren. Eine Woche Alarmvolumen je Richtlinie erheben.
2. **Tag 2 — Kanal bauen.** Alarmpostfach anlegen, Zugriff vergeben, Ticketanbindung einrichten, Zustellung testen. Zweiten Kanal für hohe Schweregrade festlegen.
3. **Tag 3 — Standard schärfen.** Empfänger auf das Alarmpostfach umstellen, informative Richtlinien von der Benachrichtigung befreien, abgelöste Richtlinien deaktivieren.

4. **Tag 4 — Eigene Richtlinien.** Die vier Richtlinien für Weiterleitung, Massen-Download, Rollenzuweisung und Einwilligung anlegen. Die Personalvertretung vorher einbinden, nicht hinterher.
5. **Tag 5 — Ablauf festschreiben.** Eskalationstreppe mit Namen und Zeiten aufschreiben, Befugnisse unterschreiben lassen, Termin für den ersten Test im nächsten Quartal setzen.

Am Tag danach passiert genau nichts, weil die Synchronisierung der neuen Richtlinien bis zu 24 Stunden dauert und anomaliebasierte Erkennung noch eine Woche lernt. Plane den ersten echten Funktionstest also nicht für den Freitagnachmittag ein.

Wenn du das nicht allein machen möchtest: Genau diese Woche ist ein typisches Format in der [Microsoft 365 Security Beratung](#) — einmal gemeinsam durchziehen, danach läuft es im eigenen Betrieb. Wer lieber das eigene Team befähigt, findet den Stoff in der [Schulung Microsoft 365 Security](#). Und wer sehen will, wie eine solche Kette in einem realen Vorfall aussieht, wenn sie an der falschen Stelle reißt, findet die Aufarbeitung im Dossier [TerminalFix und der Berlin-Hack](#).

Häufige Fragen

Warum löst meine neue Alarmrichtlinie nicht aus?

In neun von zehn Fällen ist es die Wartezeit: Nach dem Anlegen oder Ändern dauert es bis zu 24 Stunden, bis die Richtlinie zur Erkennungsmaschine synchronisiert ist. Bei anomaliebasierter Auslösung kommen bis zu sieben Tage Lernzeit dazu. Bleibt es danach still, prüf die Aggregation — ein Schwellwert von 50 in einem Zeitfenster von 60 Minuten wird in einem kleinen Tenant nie erreicht. Und wenn es eine Standardrichtlinie ist: Die enthält möglicherweise Filter, die im Portal nicht angezeigt werden und die du nur über `Get-ProtectionAlert -IncludeRuleXml` zu sehen bekommst.

Reicht E3 für sinnvolle Alarmierung?

Für die Grundausstattung ja, für Komfort nein. Mit E3 ohne Zusatzabonnement kannst du eigene Richtlinien nur mit einem Alarm pro Ereignis bauen. Für drei der vier empfohlenen Eigenbau-Richtlinien reicht das völlig, weil Rollenzuweisung, Einwilligung und Weiterleitungsregel ohnehin selten vorkommen. Beim Massen-Download stößt du an die Grenze: Ohne Aggregation bekommst du eine Meldung pro Datei. Dort hilft nur, die Bedingungen sehr scharf zu ziehen oder auf Defender for Cloud Apps auszuweichen.

Wie viele Empfänger gehören in eine Benachrichtigung?

Genau einer: das Alarmpostfach. Alles Weitere regelst du hinter dem Postfach — Zugriffsrechte, Ticketanbindung, Weiterleitung an den zweiten Kanal. Wenn du fünf Adressen in die Richtlinie einträgst, hast du fünf Personen, von denen jede annimmt, dass sich eine der anderen kümmert. Die einzige sinnvolle Ausnahme sind die wenigen Meldungen mit unmittelbarer Geschäftsrelevanz, etwa die Sperrung des gesamten Tenants für den Mailversand — da darf die IT-Leitung mit auf die Liste.

Was mache ich gegen zu viele Alarme?

Der Reihe nach: erstens Benachrichtigung abschalten und Alarme nur noch im Portal sammeln, zweitens Schwellwert und Zeitfenster nachziehen, drittens gezielte Optimierungsregeln für wiederkehrende gutartige Muster anlegen, viertens — und erst dann — die Richtlinie deaktivieren. Wer mit Schritt vier anfängt, schaltet irgendwann genau die Erkennung ab, die er beim nächsten Vorfall gebraucht hätte.

Brauche ich für Alarmrichtlinien den Betriebsrat?

Sobald eine Richtlinie das Verhalten einzelner Personen auswertet — Downloadmengen, Sendeverhalten, Anmeldeorte — ist sie mitbestimmungsrelevant. Reine Systemmeldungen wie eine Sperrung des Tenants durch Microsoft sind es nicht. In der Praxis löst man das mit einer Vereinbarung, die Zweckbindung, Empfängerkreis, Aufbewahrung und Auswertungsverfahren regelt, statt jede Richtlinie einzeln zu verhandeln. Das ist auch für die IT der bequemere Weg, weil neue Richtlinien dann keine Neuverhandlung auslösen.

Wie teste ich, ob die Kette funktioniert?

Nicht mit einer Testmail an das Postfach — das prüft nur die Zustellung. Lös einen echten Vorgang aus: Leg auf einem Testkonto eine Posteingangsregel mit Weiterleitung an eine externe Adresse an und stopp die Zeit, bis jemand reagiert. Das ist unangenehm und deshalb der einzige Test, der etwas aussagt. Als Format eignet sich eine [Feuerwehrübung](#), bei der du gleich mehrere Abläufe gemeinsam durchspielst.

Was ist mit Alarmen aus Defender for Endpoint und Identity?

Die laufen nicht über Alarmrichtlinien, sondern kommen als eigenständige Alarme in die Korrelation. Steuern kannst du sie über die Benachrichtigungsregeln für Vorfälle. Das ist auch der Grund, warum der Hauptkanal auf Vorfällen aufsetzen sollte: Nur dort laufen die Signale aus [Defender for Endpoint](#), [Defender for Identity](#) und [Defender for Office 365: Safe Links und Safe Attachments](#) zusammen.

Was passiert, wenn das Tageslimit erreicht ist?

Dann verstummt die E-Mail-Benachrichtigung für diesen Tag, die Alarme entstehen im Portal aber weiter. Das ist ein Schutz gegen Massenpost und gleichzeitig eine Falle: Ausgerechnet an dem Tag, an dem eine Richtlinie ihr Limit reißt, ist meistens etwas los. Setz das Limit deshalb nicht zu niedrig und behandle das Erreichen des Limits selbst als Signal — wenn eine Richtlinie regelmäßig anschlägt, stimmt entweder der Schwellwert nicht oder in deinem Tenant passiert gerade etwas.

Fazit

Alarmierung ist der Teil von Microsoft 365 Security, der am wenigsten nach Technik aussieht und am meisten über den Reifegrad eines Betriebs verrät. Die Richtlinien selbst sind in einem halben Tag konfiguriert. Zeit kostet die Entscheidung, welche Meldung eine Unterbrechung wert ist, und die Verabredung, wer sie bekommt.

Wenn du drei Dinge mitnimmst, dann diese. Erstens: Weniger Benachrichtigungen sind besser — vier bis zehn Richtlinien mit E-Mail-Versand reichen, alles andere gehört in den Arbeitsvorrat. Zweitens: Die vier selbst gebauten Richtlinien für externe Weiterleitung, Massen-Download, Rollenzuweisung und erteilte Einwilligung schließen die Lücken, die die Standardausstattung offen lässt. Drittens: Der Kanal am Ende der Kette braucht einen Namen, eine Zeit und eine Befugnis. Ohne diese drei Angaben ist alles davor Zierrat.

Und dann kommt der unangenehme Teil, den keine Konfiguration ersetzt: einmal im Quartal ausprobieren, ob die Kette hält. Es dauert eine Stunde. Der Alternativtermin wird von jemand anderem gesetzt, zu einem deutlich ungünstigeren Zeitpunkt, und dauert erfahrungsgemäß länger.

TIPP · Weiterlesen

Themen, die unmittelbar an der Alarmierung hängen:

- > [Incident-Response-Plan für Microsoft 365](#) — was passiert, nachdem der Alarm gelesen wurde.
- > [Microsoft Sentinel anbinden: wann es sich lohnt](#) — die Ausbaustufe, wenn Bordmittel nicht mehr reichen.
- > [Kompromittiertes Konto erkennen und aufräumen](#) — die häufigste Ursache hinter einem echten Alarm.
- > [Phishing-Vorfall: die ersten 60 Minuten](#) — der Ablauf, den deine Eskalationstreppe auslöst.
- > [App-Registrierungen und Consent-Governance](#) — damit der Einwilligungsalarm die Ausnahme bleibt.
- > [Gastzugriff und externe Freigaben härten](#) — weniger externe Freigaben bedeuten weniger Fehlalarme.
- > [Ransomware-Vorsorge in Microsoft 365](#) — der Fall, in dem Minuten wirklich zählen.
- > [NIS2 aus Security-Sicht: technische Maßnahmen in M365](#) — warum dokumentierte Meldewege inzwischen Pflicht sein können.