

Security-Monitoring und Betriebsrat: was mitbestimmungspflichtig ist

Es gibt zwei Arten, ein Sicherheitsprojekt in Deutschland gegen die Wand zu fahren. Die erste ist technisch und dauert ein paar Wochen. Die zweite beginnt mit einem freundlichen Brief des Betriebsrats, in dem das Wort „Unterlassung“ vorkommt, und dauert ein Jahr. Die zweite Variante ist die teurere, und sie trifft fast immer Häuser, die alles richtig machen wollten: Defender ausgerollt, Protokolle eingeschaltet, Alarmer scharf. Nur eben ohne die Menschen zu fragen, deren Verhalten dabei nebenbei mitprotokolliert wird.

Der Reflex im Betrieb ist dabei immer derselbe: „Wir überwachen doch keine Leute, wir schützen die Firma.“ Das stimmt sogar — und ist juristisch trotzdem irrelevant. Das Gesetz fragt nicht nach deiner Absicht. Es fragt, ob die Technik geeignet ist, Verhalten oder Leistung zu erfassen. Und ein Endpoint-Sensor, der jeden gestarteten Prozess, jede Netzwerkverbindung und jede geöffnete Datei meldet, beantwortet diese Frage sehr eindeutig mit Ja. Ob du das je auswerten willst, interessiert an dieser Stelle niemanden.

Die gute Nachricht: Mitbestimmung ist kein Verhinderungsinstrument, sondern eine Betriebsgenehmigung. Eine saubere Betriebsvereinbarung verschafft dir Rechtssicherheit, die du sonst nirgends bekommst — und sie beantwortet ganz nebenbei genau die Fragen, die dir dein Datenschutzbeauftragter ohnehin gestellt hätte. Häuser mit einer guten Vereinbarung rollen schneller aus als Häuser ohne, weil niemand mehr auf halber Strecke die Notbremse zieht.

Dieser Beitrag sortiert das Feld: welche Rechtsgrundlage greift, welche Microsoft-365-Funktion tatsächlich welches Verhalten protokolliert, aus welchen Bausteinen eine Betriebsvereinbarung besteht, die im Ernstfall trägt — und wie du das Verfahren aufsetzt, ohne dass der Rollout ein Jahr im Wartezimmer sitzt.

WICHTIG · Das hier ist keine Rechtsberatung

Dieser Text beschreibt die Praxis aus IT-Sicht: welche Systeme welche Daten erzeugen und welche Regelungspunkte sich daraus ergeben. Er ersetzt weder die arbeitsrechtliche Prüfung durch eine Anwaltskanzlei noch die Bewertung durch euren Datenschutzbeauftragten. Rechtsprechung ändert sich, Landespersonalvertretungsrecht unterscheidet sich von Land zu Land, und der konkrete Wortlaut einer Vereinbarung entscheidet im Zweifel über alles. Lass den Entwurf juristisch prüfen, bevor er unterschrieben wird.

Warum dein Sicherheitswerkzeug juristisch ein Überwachungsgerät ist

Der Ausgangspunkt ist ein einziger Satz aus dem Betriebsverfassungsgesetz, und er ist kurz genug, dass du ihn dir merken kannst. Paragraph 87 Absatz 1 Nummer 6 gibt dem Betriebsrat ein Mitbestimmungsrecht bei der Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen. Über dieses Wörtchen „bestimmt“ ist jahrzehntelang gestritten worden, und der Streit ist entschieden:

Es kommt nicht darauf an, was du vorhast. Es kommt darauf an, ob die Einrichtung objektiv geeignet ist, Informationen über Verhalten oder Leistung zu erheben und aufzuzeichnen.

Damit fällt praktisch jedes Sicherheitswerkzeug in Microsoft 365 unter die Mitbestimmung. Nicht, weil Microsoft besonders neugierig wäre, sondern weil moderne Angriffserkennung ohne Verhaltensdaten gar nicht funktioniert. Ein System, das erkennen soll, dass sich ein Konto ungewöhnlich verhält, muss zwangsläufig wissen, wie sich dieses Konto normalerweise verhält. Das ist kein Konstruktionsfehler, das ist der Konstruktionszweck.

Die Entscheidung, die jeder kennt

FAKTEN · Microsoft 365 vor dem Bundesarbeitsgericht

Das Bundesarbeitsgericht hat am 8. März 2022 im Verfahren 1 ABR 20/21 entschieden, dass die unternehmenseinheitliche Einführung und Anwendung von Microsoft Office 365 der Mitbestimmung nach Paragraph 87 Absatz 1 Nummer 6 BetrVG unterliegt und dass dafür der Gesamtbetriebsrat zuständig ist. Begründung im Kern: Die Software erfasst Nutzungsverhalten und ermöglicht Auswertungen — mehr braucht es nicht.

- › Für dich heißt das: Die Grundsatzfrage ist nicht mehr verhandelbar. Verhandelbar sind nur noch die Bedingungen.
- › In Konzernstrukturen entscheidet die Reichweite der Technik über die Zuständigkeit: Ein zentral betriebener Tenant ist selten eine Angelegenheit des einzelnen Standorts.

Interessant ist die Gegenprobe. Das Arbeitsgericht Hamburg hat im Januar 2024 im Verfahren 24 BVGa 1/24 entschieden, dass die bloße Erlaubnis, ChatGPT über den Browser mit privaten Konten zu nutzen, kein Mitbestimmungsrecht auslöst — unter anderem, weil der Arbeitgeber in dieser Konstellation gar keine Daten erhält. Das ist die Trennlinie: Entscheidend ist nicht, wie modern oder beunruhigend eine Technik wirkt, sondern ob bei dir im Haus Daten über Menschen anfallen, auf die du zugreifen kannst. Bei einem Tenant, der dir gehört, ist diese Frage schnell beantwortet.

Personalrat: gleiche Musik, andere Nummer

Im öffentlichen Dienst läuft dasselbe Verfahren unter anderem Namen. Für Bundesbehörden steht die Regelung in Paragraph 80 Absatz 1 Nummer 21 des Bundespersonalvertretungsgesetzes und ist inhaltlich deckungsgleich formuliert: Mitbestimmung bei Einführung und Anwendung technischer Einrichtungen, die dazu geeignet sind, das Verhalten oder die Leistung der Beschäftigten zu überwachen. Das Ergebnis heißt dann Dienstvereinbarung statt Betriebsvereinbarung, und der Personalrat sitzt am Tisch statt des Betriebsrats.

Die Länder haben eigene Personalvertretungsgesetze mit eigener Nummerierung und teilweise abweichenden Verfahren. Wer für eine Stadtverwaltung, eine Hochschule oder eine Landesbehörde plant, sollte deshalb nicht mit dem Bundesrecht argumentieren, sondern mit dem einschlägigen Landesgesetz — inhaltlich landest du am selben Punkt, formal blamierst du dich sonst in der ersten Sitzung. Und beim Konfliktverfahren gibt es echte Unterschiede: Während in der Privatwirtschaft die Einigungsstelle verbindlich entscheidet, endet das Stufenverfahren im öffentlichen Dienst je nach Gegenstand und Gesetz auch mal bei einer Empfehlung.

Aspekt	Betriebsrat	Personalrat
Norm	Paragraph 87 Absatz 1 Nummer 6 BetrVG	Paragraph 80 Absatz 1 Nummer 21

		BPersVG, Landesrecht abweichend nummeriert
Auslöser	Technik objektiv zur Verhaltens- oder Leistungserfassung geeignet	wortgleich formuliert, gleiche Auslegung
Ergebnis	Betriebsvereinbarung	Dienstvereinbarung
Zuständigkeit	Betriebsrat, bei unternehmensweiter Technik Gesamt- oder Konzernbetriebsrat	örtlicher Personalrat, Stufenvertretung bei zentraler Einführung
Konflikt	Einigungsstelle, Spruch ersetzt die Einigung	Stufenverfahren, je nach Gegenstand Einigungsstelle oder Letztentscheidung der Dienststellenleitung
Sanktion bei Alleingang	Unterlassungsanspruch, einstweilige Verfügung	vergleichbar, zusätzlich dienstrechtliche Folgen

Tabelle 1: Derselbe Sachverhalt, zwei Rechtskreise — die praktischen Unterschiede.

Was passiert, wenn du es einfach machst

Die unangenehme Antwort lautet: erst einmal nichts. Du rollst aus, es läuft, niemand merkt etwas. Bis der erste Fall kommt, in dem jemand aus einer Protokollzeile eine arbeitsrechtliche Konsequenz ableiten möchte. Dann steht die Frage im Raum, auf welcher Grundlage das System überhaupt betrieben wird, und die Antwort „steht halt im Projektauftrag“ hilft niemandem.

Praktisch drohen drei Dinge. Erstens der Unterlassungsanspruch: Der Betriebsrat kann verlangen, dass du die mitbestimmungswidrige Anwendung einstellst, notfalls per einstweiliger Verfügung. Ein abgeschalteter Endpoint-Sensor ist ein schlechtes Ergebnis für alle Beteiligten, aber es ist ein realistisches. Zweitens der Verlust jeder Verhandlungsposition: Wer erst nachträglich an den Tisch kommt, verhandelt nicht mehr über Zweck und Fristen, sondern über Vertrauen. Drittens die Einigungsstelle, die den Streit zwar löst, aber nach ihrem Zeitplan und ihren Vorstellungen, nicht nach deinen.

TIPP · Rahmen plus Anlagen schlägt Einzelvereinbarung

Verhandle nicht für jedes Produkt eine eigene Vereinbarung. Setz einen Rahmen auf, der Zweck, Rollen, Auswertungsverfahren und Vier-Augen-Prinzip einmal regelt, und häng die einzelnen Werkzeuge als Anlagen daran. Wenn Microsoft im nächsten Halbjahr eine neue Erkennungsfunktion ausrollt, brauchst du dann eine neue Anlage statt einer neuen Verhandlung.

- › Im Rahmen steht, wie ausgewertet wird.
- › In der Anlage steht, was ein konkretes Produkt erhebt und wie lange es das speichert.
- › Ein kurzes Änderungsverfahren für neue Anlagen gehört in den Rahmen — sonst verhandelst du doch wieder jedes Mal neu.

Was welches Produkt tatsächlich sieht

Die meisten Konflikte entstehen nicht, weil jemand böse Absichten hätte, sondern weil niemand im Raum genau sagen kann, welche Daten eigentlich anfallen. Der Betriebsrat vermutet ein Rundum-Überwachungssystem, die IT beteuert, es gehe nur um Schadsoftware, und beide haben unrecht. Deshalb lohnt sich der nüchterne Blick auf die fünf Bausteine, die in fast jedem Haus im Einsatz sind.

Was welches Produkt tatsächlich sieht

Fünf Bausteine des Microsoft-365-Monitorings und die Datenarten, die sie über Menschen erzeugen

	Anmeldung, IP, Standort	Gerät, Prozesse, Dateien	AD- und Netzwerkverkehr	Zugriff auf Postfach und Dateien	Inhalte und Dateinamen	Risikobewertung je Person
Defender for Endpoint						—
Defender for Identity		—		—	—	
Insider Risk Management			—			
Purview Audit-Log		—	—			—
Entra Anmeldeprotokolle			—	—	—	

erfasst regelmäßig
 teilweise, hängt an der Konfiguration
 — erfasst das Produkt nicht

Alle fünf erzeugen personenbeziehbare Daten. Genau das macht sie zur technischen Einrichtung im Sinne des Paragraphen 87 Absatz 1 Nummer 6 BetrVG.

Skizze 1: Welche Datenarten die fünf zentralen Bausteine über Menschen erzeugen — die Grundlage für jedes ehrliche Gespräch mit der Arbeitnehmervertretung.

Entra Anmeldeprotokolle: das Bewegungsprofil, das keiner so nennt

Die Anmeldeprotokolle in Microsoft Entra ID sind der harmloseste und zugleich aussagekräftigste Datenbestand im Tenant. Jede Anmeldung erzeugt einen Eintrag mit Zeitstempel, Konto, Anwendung, IP-Adresse, abgeleitetem Standort, Gerät und Ergebnis. Wer daraus eine Woche lang eine Zeitreihe baut, hat ein ordentliches Bild davon, wann jemand arbeitet, von wo aus, und mit welchem Gerät. Das ist keine Unterstellung, das ist einfach die Datenlage.

Die Aufbewahrung hängt an der Lizenz: Mit Entra ID Free stehen Anmelde- und Überwachungsprotokolle sieben Tage zur Verfügung, mit P1 und P2 sind es 30 Tage. Riskante Anmeldungen aus Identity Protection halten mit P2 90 Tage. Wer länger aufbewahren will, muss die Protokolle aktiv ausleiten — und genau diese Ausleitung ist der Punkt, an dem viele Vereinbarungen stillschweigend ihre eigene Löschfrist aushebeln. Wie diese Protokolle im Alltag genutzt werden, steht bei den [Conditional-Access-Baselines](#) und bei der [Einführung von MFA in Microsoft 365](#).

Purview Audit-Log: das stille Gedächtnis des Tenants

Das einheitliche Überwachungsprotokoll ist der Datenbestand mit der größten Reichweite und dem geringsten Aufsehen. Es zeichnet tausende Aktivitäten quer über Exchange, SharePoint, OneDrive, Teams und Entra ID auf: welche Datei jemand geöffnet, geteilt, umbenannt oder gelöscht hat, wer welche Postfachelemente gelesen hat, wer sich an einer Besprechung beteiligt hat. Mit Audit (Premium) kommen Ereignisse hinzu, die man sich einmal auf der Zunge zergehen lassen sollte — etwa die Suchbegriffe, die jemand in Exchange Online oder SharePoint eingegeben hat. Mehr zu diesem Werkzeugkasten im [Kompetenzbereich Microsoft Purview](#).

Bei den Fristen wird es interessant: Audit (Standard) hält die Aufzeichnungen seit Oktober 2023 für 180 Tage vor, vorher waren es 90. Audit (Premium) bewahrt Datensätze aus Exchange, SharePoint, OneDrive und Entra ID standardmäßig ein Jahr auf, für alles andere gelten weiterhin 180 Tage, sofern du keine eigene Aufbewahrungsrichtlinie definierst. Und mit einer Zusatzlizenz sind zehn Jahre möglich. Ein Betriebsrat, der das zum ersten Mal hört, stellt danach genau eine Frage — und die ist berechtigt.

Defender for Endpoint: der Sensor, der wirklich alles sieht

Der Endpunktsensor ist das Werkzeug mit der größten Tiefe. Er erhebt laut Herstellerdokumentation Dateidaten mit Namen, Größen und Hashwerten, Prozessdaten, Registrierungsdaten, Netzwerkverbindungen mit Zieladressen und Ports sowie Gerätedaten. Die Daten liegen 180 Tage im Portal sichtbar vor, in der erweiterten Suche sind sie 30 Tage lang abfragbar. Wie du den Sensor ohne Kollateralschäden in Betrieb nimmst, steht im Beitrag [Defender for Endpoint: Onboarding ohne Drama](#).

Zwei Funktionen erzeugen in der Verhandlung erfahrungsgemäß den meisten Gesprächsbedarf. Die erste ist die Gerätezeitachse: eine chronologische Liste dessen, was auf einem Rechner passiert ist. Fachlich unverzichtbar, für Uneingeweihte sieht sie aus wie ein Tagebuch. Die zweite ist Live Response — der interaktive Fernzugriff auf ein Gerät, inklusive Möglichkeit, Dateien herunterzuladen. Das ist unter Sicherheitsleuten eine Selbstverständlichkeit und aus Sicht der Belegschaft ein Zugriff auf den Arbeitsplatz. Regele es explizit, dann ist es kein Problem mehr.

Defender for Identity: unauffällig, aber nicht harmlos

Der Sensor auf dem Domänencontroller wertet Authentifizierungs- und Verzeichnisverkehr aus: Kerberos- und NTLM-Anmeldungen, LDAP-Abfragen, DNS-Anfragen, dazu passende Windows-Sicherheitsereignisse. Daraus entstehen Entitätsprofile, Pfade für mögliche seitliche Bewegungen und eine Bewertung, welche Konten besondere Aufmerksamkeit verdienen. Die Aufbewahrung liegt ebenfalls bei 180 Tagen. Was hinter den Protokollmechanismen steckt, ist im [Kompetenzbereich Kerberos](#) ausführlich beschrieben; die Betriebssicht liefert der Beitrag [Defender for Identity: das Active Directory im Blick](#).

In der Praxis ist das der am leichtesten zu verhandelnde Baustein, weil die Daten maschinennah sind: Ein Ticketaustausch zwischen zwei Servern sagt wenig über Arbeitsverhalten aus. Verschweigen solltest du trotzdem nichts. Die Untersuchungspriorität, die das Produkt einzelnen Konten zuweist, ist der Sache nach eine Bewertung einer Person — auch wenn sie ausschließlich aus technischen Auffälligkeiten berechnet wird.

Insider Risk Management: hier wird es unangenehm

Alle bisherigen Werkzeuge erzeugen Verhaltensdaten als Nebenprodukt der Angriffserkennung. Insider Risk Management ist anders: Es ist das einzige Produkt im Portfolio, dessen ausdrücklicher Zweck darin besteht, das Verhalten einzelner Menschen zu bewerten und mit einer Risikoeinstufung zu versehen. Wer das in der Verhandlung als „auch nur eine Sicherheitsfunktion“ verkauft, verspielt jede Glaubwürdigkeit, die er sich vorher erarbeitet hat.

Microsoft hat das Datenschutzproblem konstruktiv adressiert. Benutzernamen sind per Voreinstellung pseudonymisiert: Aus einer realen Person wird in der Oberfläche ein Kürzel in der

Art von „AnonIS8-988“. Die Einstellung gilt für alle Richtlinien und rückwirkend für alle bestehenden Treffer. Dazu kommen rollenbasierte Zugriffsrechte, die Analyse von Ermittlungs- und Prüfungshandlungen im Protokoll und ein Analysemodus, der zunächst nur aggregierte Aussagen darüber liefert, ob es überhaupt Anlass zu einer Richtlinie gibt.

WARNUNG · Der Auslöser, der jede Verhandlung kippen kann

Insider-Risk-Richtlinien lassen sich an Ereignisse aus dem Personalsystem koppeln — etwa an ein hinterlegtes Austrittsdatum oder an eine erfasste Leistungsbewertung. Fachlich ist das nachvollziehbar, weil Datenabflüsse statistisch rund um Kündigungen auftreten. In der Sitzung klingt es allerdings nach genau dem Szenario, vor dem der Paragraph 87 schützen soll: Wer kündigt, wird beobachtet.

- › Sprich diesen Punkt von dir aus an, bevor jemand ihn findet.
- › Wenn du den Personalkonnektor nicht zwingend brauchst, lass ihn weg — der Vertrauensgewinn ist mehr wert als die zusätzliche Trefferquote.
- › Wenn du ihn brauchst, regele Anlass, Dauer und Kreis der betroffenen Konten schriftlich und eng.

Baustein	Erhebt im Kern	Aufbewahrung ab Werk	Typischer Streitpunkt
Entra Anmeldeprotokolle	Konto, Zeit, IP, Standort, Gerät, Anwendung, Ergebnis	7 Tage (Free), 30 Tage (P1/P2), 90 Tage riskante Anmeldungen (P2)	Standort- und Zeitdaten ergeben ein Anwesenheitsbild
Purview Audit-Log	Datei- und Postfachzugriffe, Freigaben, Teams-Aktivitäten, in Premium auch Suchbegriffe	180 Tage, Premium 1 Jahr für Exchange, SharePoint, OneDrive und Entra, mit Zusatzlizenz 10 Jahre	Reichweite und Langzeitaufbewahrung
Defender for Endpoint	Dateien, Prozesse, Registrierung, Netzwerkverbindungen, Geräteangaben	180 Tage im Portal, 30 Tage in der erweiterten Suche	Gerätezeitachse und Live Response
Defender for Identity	Kerberos, NTLM, LDAP, DNS, Sicherheitsereignisse der Domänencontroller	180 Tage	Untersuchungspriorität als Kontobewertung
Insider Risk Management	Datenbewegungen, Downloads, Weiterleitungen, Richtlinienverstöße, Risikobewertung je Person	abhängig von Richtlinie und Fallakte	Personenbezug ist der Zweck, nicht die Nebenwirkung

Tabelle 2: Die fünf Bausteine im Überblick — Datenarten, voreingestellte Aufbewahrung und der Punkt, an dem es in der Verhandlung erfahrungsgemäß hakt.

FAKTEN · Drei Zahlen, die du auswendig können solltest

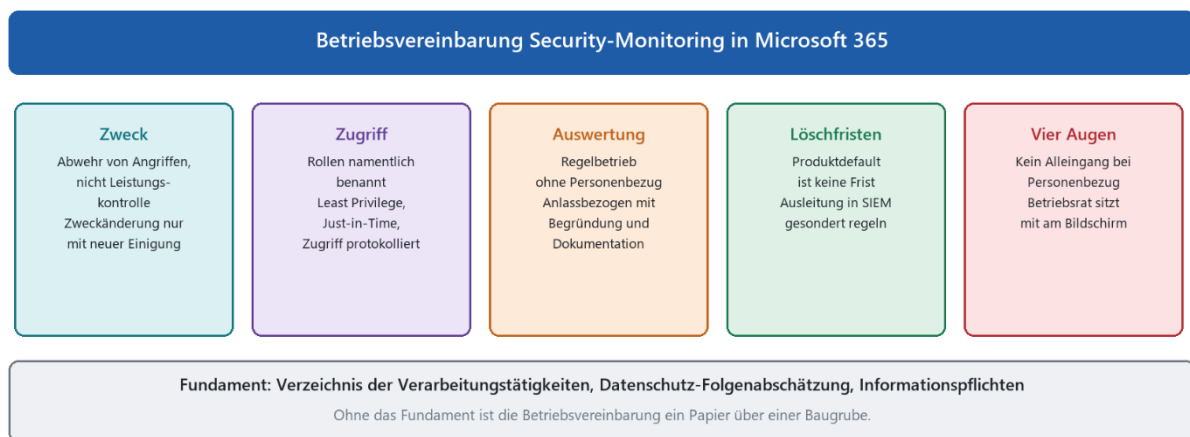
180 Tage ist der Standardwert, der dir überall begegnet: bei Defender for Endpoint, bei Defender for Identity und bei Purview Audit (Standard). 30 Tage ist die Frist, mit der du in der erweiterten Suche und bei den Entra-Anmeldeprotokollen arbeitest. Und 10 Jahre ist der Maximalwert, den Purview Audit mit Zusatzlizenz erreicht — technisch möglich, praktisch fast immer erklärungsbedürftig.

Die fünf Bausteine einer belastbaren Betriebsvereinbarung

Eine gute Betriebsvereinbarung ist kein Rechtsaufsatz, sondern eine Betriebsanleitung. Sie beantwortet fünf Fragen so konkret, dass zwei Jahre später jemand, der bei der Verhandlung nicht dabei war, damit arbeiten kann. Wozu wird erhoben, wer darf hineinschauen, wie wird ausgewertet, wann wird gelöscht, und wer kontrolliert die Kontrolleure.

Die fünf tragenden Säulen

Fehlt eine davon, wackelt die ganze Vereinbarung — und zwar meist genau dann, wenn es ernst wird



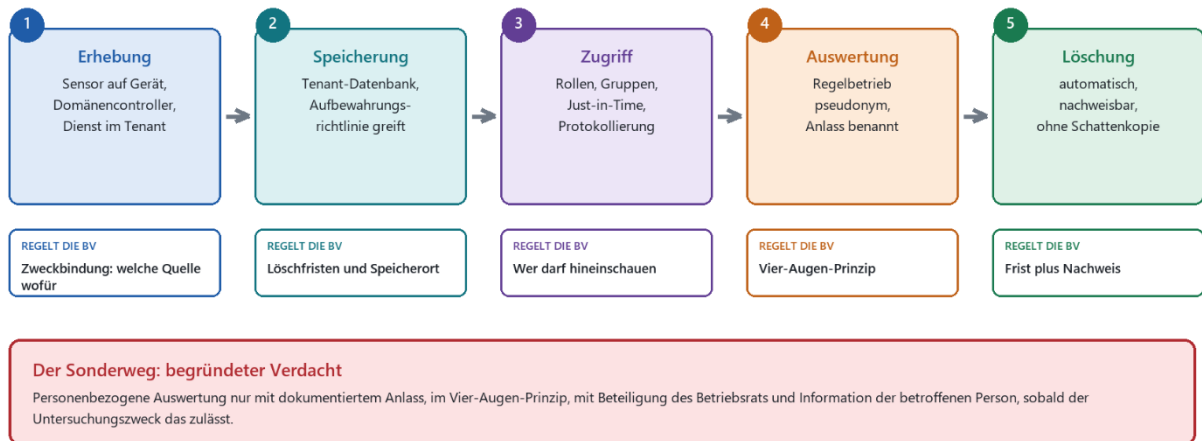
Die Reihenfolge ist kein Zufall: Ohne definierten Zweck lässt sich keine der anderen vier Säulen sinnvoll bemaßen.

Skizze 2: Die fünf Säulen einer Vereinbarung — und das Fundament aus Verzeichnis der Verarbeitungstätigkeiten, Datenschutz-Folgenabschätzung und Informationspflichten.

Der zweite Blick lohnt sich auf den Lebensweg eines einzelnen Ereignisses. Vom Sensor bis zur Löschung durchläuft jede Protokollzeile fünf Stationen, und an jeder greift eine Regel — oder eben keine. Genau an den Stellen ohne Regel entstehen später die Diskussionen.

Der Weg eines Ereignisses

An jeder Station greift eine Regel der Betriebsvereinbarung — oder eben keine



Wer diese fünf Stationen sauber regelt, hat den größten Teil einer Betriebsvereinbarung bereits geschrieben.

Skizze 3: Fünf Stationen vom Sensor bis zur Löschung. Wer für jede eine Regel formuliert hat, hat den Hauptteil der Vereinbarung geschrieben.

Zweck: die Negativabgrenzung ist wichtiger als die Positivliste

Jede Vereinbarung beginnt mit dem Zweck, und fast jede formuliert ihn zu schwach. „Zur Gewährleistung der Informationssicherheit“ ist kein Zweck, das ist eine Überschrift. Belastbar wird es erst, wenn du dazuschreibst, was ausdrücklich nicht Zweck ist: keine Leistungskontrolle, keine Anwesenheitsüberwachung, keine Auswertung zur Bewertung der Arbeitsqualität, keine automatisierte Erstellung von Ranglisten oder Profilen zu Personalzwecken.

Der zweite unverzichtbare Satz ist das Zweckänderungsverbot: Daten, die zur Angriffserkennung erhoben wurden, dürfen nicht stillschweigend zu etwas anderem verwendet werden. Wenn ein neuer Zweck entsteht — und das kommt vor —, braucht es eine neue Einigung. Dieser Satz kostet dich nichts und beruhigt die Gegenseite mehr als drei Seiten technische Erläuterung.

TIPP • Der Satz, der Phishing-Simulationen rettet

Simulierte Phishing-Kampagnen sind ein Musterbeispiel für notwendige Zweckabgrenzung: Sie erzeugen zwangsläufig eine Liste von Personen, die geklickt haben. Schreib in die Vereinbarung, dass Ergebnisse ausschließlich aggregiert berichtet werden, dass individuelle Klickdaten nur für die automatische Zuweisung von Schulungsinhalten genutzt werden und dass keine arbeitsrechtlichen Konsequenzen daran hängen. Dann bekommst du die Kampagne genehmigt — sonst nicht.

Zugriff: Rollen mit Namen, nicht mit Wunschdenken

„Zugriff haben nur berechtigte Personen“ ist die zweite typische Leerformel. Was hineingehört, sind benannte Rollen mit benannten Berechtigungen: Wer darf Warnungen sehen, wer darf Fallakten anlegen, wer darf pseudonymisierte Namen aufdecken, wer darf Live Response

ausführen, wer darf Aufbewahrungsrichtlinien ändern. Und wer darf nichts davon, obwohl er global administrieren könnte.

Technisch ist das gut lösbar. Rollenbasierte Zugriffssteuerung im Defender-Portal und in Purview, zeitlich befristete Rechtevergabe über Privileged Identity Management und eine saubere Trennung zwischen Betrieb und Auswertung reichen weit. Der Punkt, den Betriebsräte zu Recht nachfragen: Auch die Prüfer werden geprüft. Jeder Zugriff auf personenbezogene Auswertungen landet selbst im Protokoll, und dieses Protokoll darf nicht von denselben Personen verwaltet werden, deren Handeln es aufzeichnet.

Rolle	Darf	Darf nicht	Kontrolle
Betrieb Sicherheitssysteme	konfigurieren, Sensoren verwalten, Systemzustand prüfen	personenbezogene Auswertungen durchführen	Konfigurationsänderungen protokolliert
Auswertung Regelbetrieb	Warnungen bearbeiten, technische Analyse, aggregierte Berichte	Pseudonyme aufdecken, Fallakten zu Personen anlegen	Zugriffe im Protokoll, Stichproben
Anlassbezogene Untersuchung	nach dokumentiertem Anlass personenbezogen auswerten	ohne Anlass und ohne zweite Person tätig werden	Vier-Augen-Prinzip, Betriebsrat informiert
Arbeitnehmervertretung	Einsicht in Protokolle über Auswertungen, Teilnahme an Stufe 3	eigenständige Auswertung von Beschäftigtendaten	Regelung im Rahmen der Vereinbarung
Externer Dienstleister	vertraglich definierte Leistungen, dokumentierte Zugriffe	unbegrenzter Dauerzugriff auf Rohdaten	Auftragsverarbeitung, Zugriff auf Antrag

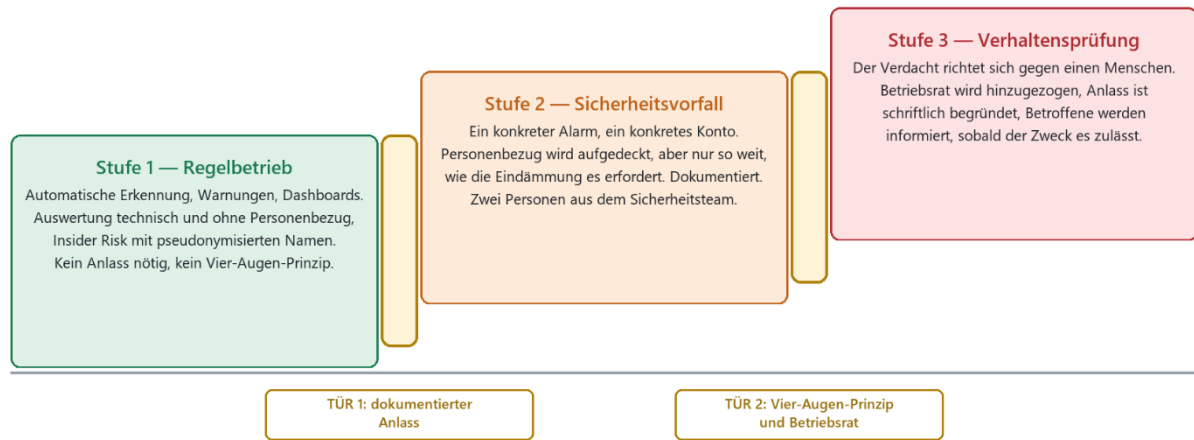
Tabelle 3: Ein Rollenmodell, das in Verhandlungen erfahrungsgemäß trägt. Die Zuordnung zu konkreten Personen gehört namentlich in die Anlage.

Auswertung: drei Stufen, zwei Türen

Der Kern jeder Vereinbarung ist das Auswertungsverfahren, und der praktikabelste Aufbau ist ein Stufenmodell. Im Regelbetrieb arbeitet das Sicherheitsteam technisch und ohne Personenbezug: Warnungen, Dashboards, Trends. Sobald ein konkreter Sicherheitsvorfall vorliegt, wird der Personenbezug so weit aufgedeckt, wie die Eindämmung es erfordert — mit Dokumentation und im Vier-Augen-Prinzip. Und erst wenn sich ein Verdacht gegen einen Menschen richtet, kommt die dritte Stufe mit Beteiligung der Arbeitnehmervertretung.

Drei Stufen, zwei Türen

Je näher die Auswertung an den einzelnen Menschen rückt, desto mehr Augen gehören an den Bildschirm



Die Türen sind der eigentliche Verhandlungsgegenstand. Wer sie offen lässt, verhandelt später vor der Einigungsstelle.

Skizze 4: Das Stufenmodell mit den beiden Türen — dokumentierter Anlass und Vier-Augen-Prinzip. Die Türen sind der eigentliche Verhandlungsgegenstand.

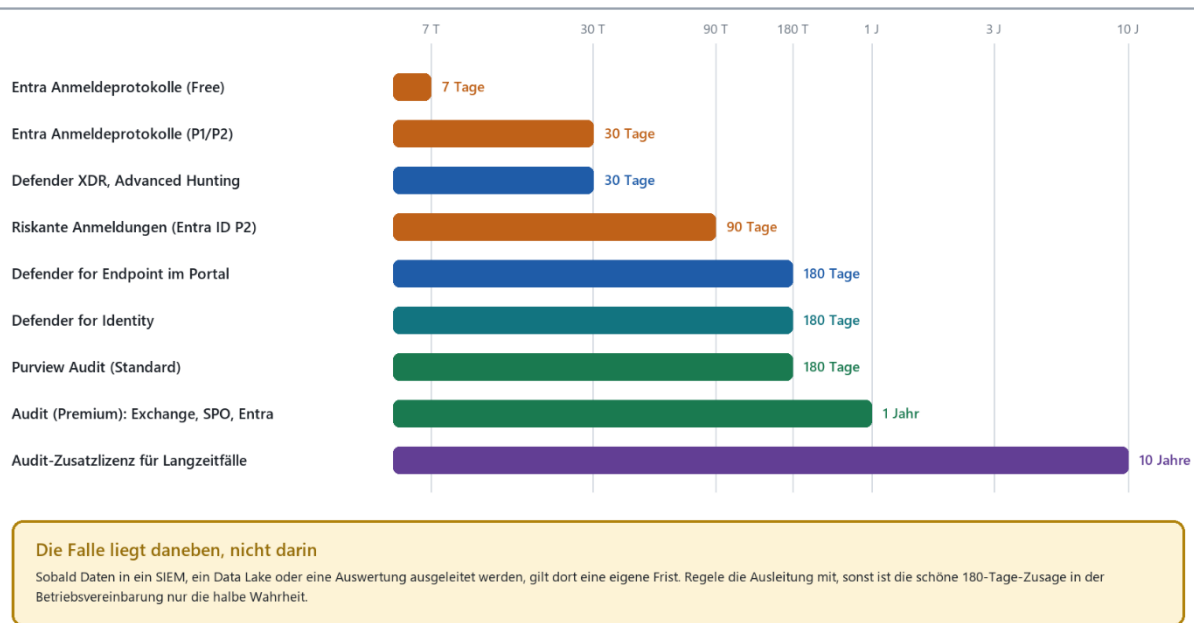
Der Charme des Modells liegt darin, dass es der Realität entspricht. Ein Sicherheitsteam will überhaupt nicht wissen, wer wann welche Datei geöffnet hat — bis zu dem Moment, in dem genau diese Information darüber entscheidet, ob ein Angreifer noch im Netz ist. Wie dieser Moment im Ernstfall abläuft, steht im [Incident-Response-Plan für Microsoft 365](#) und beim Vorgehen für ein [kompromittiertes Konto](#). Wer die Stufen einmal in einer [Feuerwehrrübung](#) durchgespielt hat, verhandelt sie anschließend deutlich entspannter.

Löschfristen: der Produktdefault ist keine Frist

Die voreingestellte Aufbewahrung eines Produkts ist eine technische Eigenschaft, keine Zusage. Sie kann sich mit einer Lizenzänderung verschieben, und sie sagt nichts darüber aus, was mit Kopien passiert. Genau deshalb gehört in die Vereinbarung nicht nur eine Zahl, sondern auch die Aussage, wo überall diese Zahl gilt.

Wie lange die Systeme sich erinnern

Voreingestellte Aufbewahrung, logarithmisch aufgetragen — die Spanne reicht von einer Woche bis zu einem Jahrzehnt



Voreinstellungen laut Herstellerdokumentation, Stand 2026. Abweichende Aufbewahrungsrichtlinien gehören in die Anlage der Vereinbarung.

Skizze 5: Voreingestellte Aufbewahrung im Vergleich. Die Bandbreite von sieben Tagen bis zu zehn Jahren ist der Grund, warum pauschale Zusagen in Vereinbarungen selten halten.

Die häufigste Lücke ist die Ausleitung. Sobald Protokolle in ein SIEM, ein Data Lake oder eine Auswertungsplattform fließen, gilt dort eine eigene Aufbewahrung — und die ist gerne länger. Wenn du eine [Anbindung an Microsoft Sentinel](#) planst oder schon betreibst, regele die Fristen dort mit, einschließlich Archivstufen und Langzeitspeicher. Sonst steht in der Vereinbarung eine beruhigende Zahl, während die Daten an anderer Stelle drei Jahre überdauern.

Zwei weitere Punkte gehören dazu. Erstens Fallakten: Daten in einer laufenden Untersuchung dürfen nicht mitten im Verfahren verschwinden, deshalb braucht es eine ausdrückliche Regel für Aufbewahrung während und nach einem Fall. Zweitens der Nachweis: Eine Löschfrist, deren Einhaltung niemand prüfen kann, ist eine Absichtserklärung. Ein jährlicher Bericht über Bestände und Löschungen an die Arbeitnehmervertretung kostet wenig und ersetzt viel Misstrauen.

Vier-Augen-Prinzip: die Regel, die alle anderen absichert

Das Vier-Augen-Prinzip ist der Baustein, an dem sich entscheidet, ob eine Vereinbarung im Betrieb ernst genommen wird. Es bedeutet nicht, dass zwei Personen gemeinsam auf einen Bildschirm starren müssen. Es bedeutet, dass eine personenbezogene Auswertung erst beginnt, wenn eine zweite, benannte Person den Anlass geprüft und gegengezeichnet hat — und dass beides dokumentiert wird.

Vier Details entscheiden über die Praxistauglichkeit. Erstens: Wer sind die zweiten Augen? Eine Person aus dem Sicherheitsteam, der Datenschutzbeauftragte oder ein benanntes Mitglied der Arbeitnehmervertretung — alles ist regelbar, aber es muss benannt sein. Zweitens: Was passiert nachts um drei? Ohne Vertretungsregelung steht dein Vorfall bis Montag. Drittens: Wie wird dokumentiert? Ein kurzes Formular mit Anlass, Umfang, Zeitraum und Beteiligten reicht völlig,

aber es muss existieren. Viertens: Wer sieht das Protokoll? Wenn die Arbeitnehmervertretung regelmäßig Einsicht in die Liste der durchgeführten Auswertungen erhält, erledigen sich die meisten Grundsatzdebatten von selbst.

WARNUNG · Die Notfallklausel, die fast immer fehlt

Ein Angriff hält sich nicht an Sitzungstermine. Ohne ausdrückliche Notfallregelung steht dein Sicherheitsteam bei einem laufenden Vorfall vor der Wahl zwischen Vereinbarungsbruch und Kontrollverlust. Regele deshalb: Bei akuter Gefahr darf sofort personenbezogen ausgewertet werden, die Arbeitnehmervertretung wird unverzüglich informiert, und die Maßnahme wird innerhalb einer festen Frist nachträglich dokumentiert und gemeinsam bewertet.

- › Ohne diese Klausel wird die Vereinbarung im ersten echten Vorfall gebrochen — und danach glaubt niemand mehr an sie.
- › Mit dieser Klausel hast du eine Rechtsgrundlage für den schlechtesten Tag des Jahres.

So bringst du das Verfahren durch, ohne ein Jahr zu verlieren

Die meisten Verzögerungen entstehen nicht am Verhandlungstisch, sondern davor: Niemand kann sagen, welche Daten anfallen, also wird gefragt, also wird recherchiert, also vergehen Wochen. Wer mit einer belastbaren Datenübersicht in das erste Gespräch geht, spart sich zwei Runden.

Der Fahrplan

1. Produktinventur: Welche Sicherheitswerkzeuge sind aktiv, welche geplant, welche längst eingeschaltet, ohne dass jemand es entschieden hätte. Ehrlichkeit an dieser Stelle spart später Vertrauen.
2. Datensteckbrief je Produkt: Welche Datenarten, welche Aufbewahrung, welche Auswertungsmöglichkeiten, welche Rollen. Eine Seite pro Werkzeug, in verständlicher Sprache.
3. Frühes Erstgespräch ohne Verhandlungsdruck: Erklären, zeigen, Fragen sammeln. Nicht der Moment für einen fertigen Entwurf.
4. Entwurf des Rahmens mit Zweck, Rollen, Stufenmodell, Fristen und Vier-Augen-Prinzip, juristisch vorgeprüft.
5. Pilotbetrieb mit ausdrücklicher Duldungsregelung und begrenzter Nutzergruppe, damit die Technik läuft, während der Text reift.
6. Anlagen je Produkt, Verabschiedung, Information der Belegschaft in einer Sprache, die niemand nachschlagen muss.
7. Schulung der auswertenden Personen auf das Verfahren, nicht nur auf die Werkzeuge.
8. Jährlicher Review mit Bericht über Auswertungen, Löschungen und neue Produktfunktionen.

Phase	Dauer	Ergebnis	Häufigste Bremse
Inventur und Steckbriefe	2 bis 4 Wochen	belastbare Datenübersicht	niemand weiß, was alles aktiv ist
Erstgespräch und Fragenrunde	2 bis 6 Wochen	gemeinsames Problemverständnis	Sitzungsrhythmus des Gremiums
Entwurf und Abstimmung	4 bis 12 Wochen	verhandlungsreifer Rahmen	juristische Schleifen, fehlende Notfallklausel

Pilotbetrieb	parallel, 4 bis 8 Wochen	Technik läuft, Erfahrungswerte liegen vor	fehlende Duldungsregelung
Verabschiedung und Rollout	2 bis 6 Wochen	unterschiedene Vereinbarung, Ausrollung	Anlagen unvollständig

Tabelle 4: Realistischer Zeitrahmen für ein mittelständisches Haus mit funktionierender Arbeitnehmervertretung. Die Spanne wächst mit der Zahl der Standorte.

Was Arbeitnehmervertretungen wirklich überzeugt

Nicht die Folien. Was funktioniert, ist die Demonstration am lebenden Objekt: Portal aufmachen, eine Suche starten, zeigen, was man sieht — und vor allem zeigen, was man nicht sieht. Der Moment, in dem ein Betriebsrat feststellt, dass in der erweiterten Suche keine E-Mail-Inhalte stehen, sondern Metadaten, ist mehr wert als jede Zusicherung im Text.

Zweitens hilft Transparenz über die Motivation. Wer erklären kann, warum ein Haus Angriffserkennung braucht, argumentiert leichter als jemand, der auf abstrakte Bedrohungslagen verweist. Das [Dossier TerminalFix und der Berlin-Hack](#) zeigt an einem realen Fall, wie ein Angriff abläuft und an welchen Stellen Protokolldaten den Unterschied machen. Und wenn regulatorischer Druck dazukommt, hilft der Blick auf die [technischen Maßnahmen aus NIS2-Sicht](#): Nachweispflichten sind ein Argument, das auch Gremien überzeugt, die technischen Argumenten skeptisch gegenüberstehen.

Drittens: Gib der Gegenseite eigene Kompetenz. Der Betriebsrat darf nach Paragraph 80 Absatz 2 BetrVG Auskunft verlangen und unter bestimmten Voraussetzungen einen Sachverständigen hinzuziehen. Wer das aktiv anbietet, statt es abzuwehren, verkürzt das Verfahren. Eine gemeinsame [Schulung zu Microsoft 365 Security](#) für IT und Gremium ist erstaunlich oft die günstigste Abkürzung im ganzen Projekt.

Die vier Fehler, die du sonst garantiert machst

- Nachrüsten statt vorbereiten: Das System läuft seit acht Monaten, und die Vereinbarung soll das nachträglich legitimieren. Das funktioniert manchmal, kostet aber immer Vertrauen und meist zusätzliche Zugeständnisse.
- Berichte mit Namen: Ein Sicherheitsbericht an die Geschäftsführung, in dem Personen auftauchen, ist ein Verstoß gegen den vereinbarten Zweck. Aggregiert berichten, Personenbezug nur im Einzelfall und nur nach Verfahren.
- Neue Funktionen still aktivieren: Cloud-Dienste bekommen laufend neue Erkennungsfunktionen. Ohne Änderungsverfahren in der Vereinbarung wächst dein Monitoring an der Abstimmung vorbei — und irgendwann fällt es jemandem auf.
- Den Datenschutzbeauftragten erst am Ende einbinden: Datenschutz-Folgenabschätzung, Verzeichnis der Verarbeitungstätigkeiten und Betriebsvereinbarung gehören zusammen. Wer sie nacheinander abarbeitet, macht dieselbe Arbeit dreimal.

Wenn du das Verfahren zum ersten Mal aufsetzt, lohnt sich externe Begleitung vor allem für die Datensteckbriefe und das Stufenmodell — das sind die Teile, an denen sich Verhandlungen erfahrungsgemäß festbeißen. Wie das im Rahmen einer [Beratung zu Microsoft 365 Security](#) abläuft, ist an anderer Stelle beschrieben. Den Gesamtüberblick über die Serie und die technischen Bausteine findest du im Themenbereich [Microsoft 365 Security](#).

Passend dazu aus derselben Reihe

- › [Defender for Endpoint: Onboarding ohne Drama](#) — was der Sensor erhebt und wie du ihn einführst
- › [Attack Simulation Training: Phishing-Übungen richtig aufsetzen](#) — der Klassiker unter den mitbestimmungspflichtigen Auswertungen
- › [Security-Reporting für die Geschäftsführung](#) — aggregiert berichten, ohne den Zweck zu verlassen
- › [Alert Policies und Benachrichtigungen richtig aufsetzen](#) — wer wann worüber informiert wird
- › [Defender for Cloud Apps im Mittelstand](#) — der Baustein mit dem größten Erklärungsbedarf nach Insider Risk
- › [Zero Trust im Mittelstand: pragmatisch statt dogmatisch](#) — warum mehr Kontrolle nicht automatisch mehr Überwachung heißt

Häufige Fragen

Brauche ich wirklich eine Vereinbarung, bevor ich Defender for Endpoint einschalte?

Wenn es in deinem Haus eine Arbeitnehmervertretung gibt: ja, jedenfalls eine Verständigung. Das Mitbestimmungsrecht greift bei Einführung und Anwendung, nicht erst bei der ersten Auswertung. In der Praxis reicht für den Start häufig eine schriftliche Duldungsregelung für einen begrenzten Pilotbetrieb, während der Text der eigentlichen Vereinbarung entsteht. Ohne Gremium bleibt die datenschutzrechtliche Seite — Rechtsgrundlage, Folgenabschätzung, Information der Belegschaft — trotzdem vollständig bestehen.

Wir haben eine IT-Rahmenvereinbarung von 2015. Reicht die?

Fast nie. Vereinbarungen aus dieser Zeit beschreiben Systeme, die im Rechenzentrum standen und deren Funktionsumfang sich nur mit einem Projekt änderte. Eine Cloud-Plattform, die quartalsweise neue Erkennungsfunktionen bekommt, passt in diesen Rahmen nicht hinein. Prüfe den Text auf drei Punkte: Nennt er die Datenarten, nennt er Fristen, und enthält er ein Verfahren für neue Funktionen. Fehlt einer davon, ist die Vereinbarung Geschichte und kein Schutzschild.

Gilt das alles auch für den Personalrat in einer Behörde?

Inhaltlich ja, formal mit anderen Vorschriften. Für Bundesbehörden steht die Mitbestimmung in Paragraf 80 Absatz 1 Nummer 21 BPersVG, die Länder haben eigene Personalvertretungsgesetze mit eigener Systematik. Das Ergebnis heißt Dienstvereinbarung. Unterschiede gibt es vor allem beim Konfliktverfahren und bei der Frage, welche Stufenvertretung zuständig ist, wenn eine Plattform zentral betrieben wird. Der fachliche Teil — Datenarten, Rollen, Fristen, Stufenmodell — ist identisch.

Muss ich bei einem laufenden Angriff erst den Betriebsrat fragen?

Nein, wenn eure Vereinbarung eine Notfallklausel enthält. Genau dafür ist sie da: Bei akuter Gefahr wird gehandelt, die Arbeitnehmervertretung wird unverzüglich informiert, und die Maßnahme wird nachträglich dokumentiert und gemeinsam bewertet. Ohne diese Klausel gerätst du in eine unangenehme Lage, in der die richtige technische Entscheidung formal angreifbar ist. Deshalb gehört der Punkt in jeden Entwurf, und zwar von Anfang an.

Darf ich Sicherheitsberichte an die Geschäftsführung geben?

Aggregiert ja, personenbezogen nur im geregelten Einzelfall. Ein monatlicher Bericht über blockierte Angriffe, Konfigurationsabweichungen und offene Risiken ist unproblematisch, solange keine Person identifizierbar wird. Vorsicht ist bei kleinen Gruppen geboten: Wenn eine Abteilung aus drei Personen besteht, ist auch eine Statistik über diese Abteilung faktisch personenbezogen. Setz eine Mindestgruppengröße für aggregierte Auswertungen fest, dann ist die Frage ein für alle Mal erledigt.

Ist Insider Risk Management überhaupt durchsetzbar?

Durchsetzbar ist es, aber nicht im Vorbeigehen. Es ist das einzige Werkzeug im Portfolio, dessen Zweck die Bewertung von Personen ist, und entsprechend genau wird hingeschaut. Was hilft: mit der Analysefunktion starten, die zunächst nur aggregiert zeigt, ob es überhaupt ein Problem gibt; Pseudonymisierung eingeschaltet lassen; auf den Personalkonnektor verzichten, wenn er nicht zwingend gebraucht wird; und den Kreis der Auswertenden klein und namentlich halten. Wer stattdessen mit dem vollen Funktionsumfang in die Sitzung geht, bekommt gar nichts.

Was passiert, wenn wir uns nicht einigen?

Dann entscheidet in der Privatwirtschaft die Einigungsstelle, und ihr Spruch ersetzt die Einigung zwischen den Parteien. Das ist kein Weltuntergang, aber es dauert, es kostet, und das Ergebnis kennt niemand vorher. Erfahrungsgemäß ist eine Einigungsstelle immer dann wahrscheinlich, wenn zu Beginn zu wenig erklärt und zu früh verhandelt wurde. Im öffentlichen Dienst hängt der Ausgang vom jeweiligen Personalvertretungsgesetz ab.

Bekommt der Betriebsrat Zugriff auf das Defender-Portal?

Vollzugriff eher nicht, und er will ihn meist auch nicht — damit würde das Gremium selbst zur auswertenden Stelle. Bewährt hat sich ein anderes Modell: regelmäßige Einsicht in das Protokoll der durchgeführten personenbezogenen Auswertungen, Teilnahme an Auswertungen der dritten Stufe und das Recht, sich Funktionen im System zeigen zu lassen. Das schafft Kontrolle, ohne neue Zugriffswege auf Beschäftigtendaten zu öffnen.

Wie lange darf ich Protokolle aufbewahren?

Das Gesetz nennt keine Zahl, es verlangt Erforderlichkeit. In der Praxis sind die Voreinstellungen der Produkte ein guter Ausgangspunkt: 180 Tage bei Defender for Endpoint, Defender for Identity und Purview Audit (Standard), 30 Tage bei den Anmeldeprotokollen mit Entra ID P1 oder P2. Wer längere Fristen will, braucht eine Begründung — forensische Nachvollziehbarkeit und

regulatorische Nachweispflichten sind gängige und akzeptierte Argumente. Wer kürzere Fristen zusagt, sollte vorher prüfen, ob das Produkt sie technisch überhaupt umsetzen kann.

Fazit

Security-Monitoring in Microsoft 365 ist mitbestimmungspflichtig. Nicht ein bisschen, nicht vielleicht, sondern praktisch durchgehend — weil jede ernstzunehmende Angriffserkennung Verhaltensdaten braucht und weil das Gesetz auf die objektive Eignung schaut, nicht auf deine Absicht. Diese Erkenntnis ist unbequem, aber sie ist auch die Grundlage für ein Verfahren, das funktioniert.

Der Weg dorthin ist erstaunlich geradlinig. Erst ehrlich aufschreiben, welches Produkt welche Daten erzeugt und wie lange sie liegen bleiben. Dann fünf Fragen beantworten: Zweck, Zugriff, Auswertung, Löschfristen, Vier-Augen-Prinzip. Dann das Stufenmodell so bauen, dass es einem echten Vorfall standhält, inklusive Notfallklausel für den Tag, an dem niemand Zeit für eine Sitzung hat. Und dann jährlich nachziehen, weil Cloud-Dienste sich weiterentwickeln, auch wenn deine Vereinbarung das nicht tut.

Was du dabei gewinnst, ist mehr als juristische Ruhe. Ein Haus, in dem die Belegschaft weiß, was protokolliert wird und wer unter welchen Bedingungen hineinschaut, meldet Vorfälle schneller. Und schnelle Meldungen sind, bei allem Respekt vor der Technik, immer noch die wirksamste Erkennungsmethode, die dein Haus zu bieten hat. Die Betriebsvereinbarung ist damit kein Preis, den du für die Sicherheit zahlst — sie ist ein Teil davon.