ULRICH B. BODDENBERG

IT-CONSULTING · SOFTWARE ENGINEERING · TECHNOLOGIESEMINARE

Insider Risk Management in Microsoft 365 – Sicherheit, Datenschutz und Compliance

Inhaltsverzeichnis

Ulrich B. Boddenberg · Robert-Götz-Str. 20 · D-44319 Dortmund
E-Mail: ulrich@boddenberg.de · www.boddenberg.de · Telefon: +49 231 222458 121 ·
IBAN: DE56 4405 0199 0001 3191 91 · Stadtsparkasse Dortmund (DORTDE33XXX)
Steuer-Nr.: 316/5026/1511 · USt.Id: DE232577137

Einführung: Schutz vor internen Bedrohungen in Microsoft 365

Bei der IT-Sicherheit denken viele zunächst an externe Angreifer – doch ebenso kritisch sind Risiken aus dem Inneren einer Organisation. **Insider Risk Management in Microsoft 365** (Teil von Microsoft Purview) zielt darauf ab, **unternehmensinterne Sicherheitsrisiken frühzeitig zu erkennen und zu verhindern**. Diese Lösung korreliert verschiedenste Signale aus Microsoft 365, um **potenzielle böswillige oder unbeabsichtigte Aktivitäten von Insidern** zu identifizieren (etwa Diebstahl geistigen Eigentums, Datenlecks oder andere Compliance-Verstöße). Durch **datenbasierte Analysen und Machine Learning** werden verdächtige Muster aufgedeckt, sodass Sicherheits- und Compliance-Teams **proaktiv eingreifen** können, bevor Schaden entsteht. Gleichzeitig ist das System *„Privacy by Design"* konzipiert – Benutzer werden standardmäßig **pseudonymisiert dargestellt**, und erst berechtigte Ermittler können bei Bedarf die Identität einsehen. So werden **Datenschutz** und Unternehmenswerte gewahrt, während die **Sicherheitsziele** – Schutz sensibler Daten und Einhaltung von Compliance-Vorgaben – erreicht werden.

Datenkontrolle und Compliance stehen im Mittelpunkt: Insider Risk Management ermöglicht es, **Richtlinien für den Umgang mit sensiblen Informationen** zu definieren und durchzusetzen. Unternehmen können genau festlegen, welche riskanten Handlungen überwacht werden – etwa das Herunterladen großer Datenmengen, das Versenden vertraulicher Dokumente nach extern oder ungewöhnliche Zugriffe außerhalb der Arbeitszeiten. Wird gegen solche Richtlinien verstoßen, erzeugt das System **automatisch einen Alarm**. Fälle können zur Untersuchung eskaliert werden, und notwendige Maßnahmen wie **Zugriffsentzug oder Benutzerverwarnungen** lassen sich einleiten. All dies geschieht im Rahmen der Microsoft 365-Compliance-Umgebung (Microsoft Purview), die sicherstellt, dass **Audit-Protokolle, Nachvollziehbarkeit und rollenbasierte Zugriffskontrolle** vorhanden sind. Kurz: Insider Risk Management verbindet **Sicherheitsstrategie und Datenschutz** – interne Bedrohungen werden effektiv eingedämmt, ohne die **Compliance** oder die Rechte der Mitarbeiter aus den Augen zu verlieren.

In dieser Abhandlung erhalten Sie einen umfassenden Überblick über *Insider Risk Management in Microsoft 365*. Zunächst betrachten wir praktische **Anwendungsbeispiele** aus dem Unternehmensalltag, in denen Insider-Risiken aufgedeckt oder verhindert wurden. Anschließend erläutern wir die **technischen Funktionen** und Integrationen der Lösung – von Microsoft Purview und Defender über

Sentinel bis zu Information Protection. Wir beleuchten neue, **kürzlich eingeführte Funktionen** (z. B. KI-gestützte Risikobewertungen, adaptive Richtlinien, erweiterte Signale aus Teams, SharePoint und Exchange) und diskutieren, wie Unternehmen **jeder Größenordnung** Insider Risk Management für Governance, Transparenz und Skalierbarkeit nutzen können. Zudem führen wir Sie **Schritt für Schritt** durch die Einführung eines Insider-Risk-Management-Programms – von der Vorbereitung über Pilotierung und Rollout bis zum kontinuierlichen Monitoring. Ein besonderes Kapitel widmet sich dem **Spannungsfeld zwischen Überwachung und Mitbestimmung**, insbesondere im deutschen Kontext von Datenschutz und Betriebsrat. Abschließend ziehen wir ein differenziertes **Fazit**, geben **Handlungsempfehlungen** und werfen einen strategischen Ausblick auf die Weiterentwicklung von Insider-Risiko-Management und **Microsoft 365-Sicherheit**.

Praxisbeispiele: Insider-Risiken erkennen und verhindern

Um die Vorteile von Insider Risk Management greifbar zu machen, betrachten wir fünf realistische Szenarien aus der Praxis. Diese Beispiele zeigen, wie verschiedene **Funktionen von Microsoft 365** – von Data Loss Prevention (DLP) über Benutzer- und Aktivitätenanalysen bis zu Kommunikationsrichtlinien – zusammenwirken, um **Insider-Risiken aufzudecken oder zu vereiteln**. Jedes Szenario beleuchtet einen anderen Aspekt interner Risiken und demonstriert, wie **automatisierte Untersuchungen und Eskalationen in Microsoft Purview** dazu beitragen, Bedrohungen einzudämmen.

Beispiel 1: Datendiebstahl durch kündigenden Mitarbeiter

Ein langjähriger Mitarbeiter hat gekündigt und befindet sich in seinen letzten Tagen im Unternehmen. In der Vergangenheit kam es häufig vor, dass scheidende Mitarbeiter noch schnell Firmendaten mitnahmen – ein klassisches Insider-Risiko. In unserem Szenario versucht der Mitarbeiter, kurz vor seinem Austritt **eine große Menge vertraulicher Dokumente** von SharePoint auf einen USB-Stick zu kopieren und zusätzlich einige Berichte an seine **private E-Mail-Adresse** zu senden.

Microsoft 365 **Data Loss Prevention (DLP)** schlägt sofort Alarm, als sensible Dateien das Unternehmen verlassen sollen. **Insider Risk Management** greift diese Warnungen auf und **korreliert sie mit weiteren Aktivitäten** des Mitarbeiters: Es fällt auf, dass er in den letzten 24 Stunden ungewöhnlich viele Dateien aus einem vertraulichen Projektordner heruntergeladen hat. Zudem zeigen **Geräte-Signale** (integriert via

Microsoft Defender for Endpoint), dass er Dateien auf ein Wechsellaufwerk kopiert hat. Aufgrund der Kombination dieser Indikatoren und der Information aus HR, dass der Mitarbeiter kündigt, erreicht sein **Risikolevel** den vordefinierten Schwellenwert – das Insider-Risk-Management-Tool erstellt **automatisch einen Insider Risk Case**.

In der Microsoft Purview-Complianceportal wird dieser Fall dem Sicherheitsbeauftragten anonymisiert zur Prüfung bereitgestellt. Über eine **automatisierte Untersuchung** (Auto-Investigation) sammelt das System weitere Details: Es protokolliert die exakten Dateinamen, Zeiten und Zielpfade der verdächtigen Aktionen. Der zuständige **Insider-Risk-Analyst** erhält eine Benachrichtigung und kann im Dashboard sehen, dass hier möglicherweise ein **Datenabfluss durch einen austretenden Mitarbeiter** stattfindet. Dank integrierter **Richtlinien für austretende Mitarbeiter** (ein vordefiniertes Policy-Template von Microsoft Purview) wurde dieses Muster erkannt. Der Analyst dekonymisiert den Nutzer (mit Zustimmung eines zweiten Prüfers, gemäß Vier-Augen-Prinzip) und bestätigt die Identität. Anschließend wird sofort eine **Eskalation** eingeleitet: Die IT-Abteilung sperrt den Zugriff des Mitarbeiters auf OneDrive und Exchange, und das Compliance-Team informiert die Rechtsabteilung. Durch die enge Verzahnung von **DLP** und **Insider Risk Management** konnte in diesem Fall ein vermutlich *böswilliger Datenabzug* im letzten Moment gestoppt werden, bevor wertvolles Firmen-Know-how das Unternehmen verlassen konnte.

Beispiel 2: Schleichende Datenexfiltration über längere Zeit

Nicht jeder Insider-Vorfall passiert auf einmal – manche internen Täter versuchen, **Daten in kleinen Portionen** unbemerkt zu stehlen. Im zweiten Beispiel fällt eine Mitarbeiterin dadurch auf, dass sie über mehrere Wochen verteilt immer wieder einzelne Dateien mit sensiblen Inhalten nach außen sendet. An einem Tag druckt sie ein vertrauliches Dokument aus, am nächsten Tag versendet sie eine Excel-Liste an ihren privaten Account, einige Tage später lädt sie eine PDF-Datei in eine persönliche Cloud hoch. Jede dieser Aktionen für sich genommen bleibt unter dem Radar der klassischen Sicherheitslösungen. Eine **herkömmliche DLP-Lösung** würde vielleicht jeden Vorfall einzeln betrachten und als geringfügig einstufen, **ohne das Muster zu erkennen**.

Hier kommt die **ML-gestützte Analyse** von Insider Risk Management ins Spiel. Microsoft 365 beobachtet aggregiert die Aktivitäten der Mitarbeiterin über einen längeren Zeitraum (z. B. 30 Tage) und vergleicht die Muster mit dem normalen Verhalten in ihrer Abteilung. Dank des Modells zur *kumulativen Exfiltrationserkennung* (Cumulative Exfiltration Activities Detection, CEAD) erkennt das System, dass die Mitarbeiterin **außergewöhnlich viele Vorgänge im Zusammenhang mit sensiblen**

Daten durchführt – verteilt über Tage und Wochen. Gegenüber dem Referenzwert ähnlicher Benutzer im Unternehmen überschreitet ihr Verhalten die üblichen Schwankungen deutlich.

Sobald diese **Anomalie** erkannt wird, generiert Insider Risk Management einen Alarm. Eine automatische **Sequenzanalyse** stellt zudem fest, dass die Mitarbeiterin häufig direkt nach dem Herunterladen von Dateien ungewöhnliche Folgeaktionen vornimmt – z. B. Dateiumbenennungen gefolgt von Datei-Uploads auf externe Speicher. Dieses zusammengesetzte Muster deutet auf einen Versuch hin, Spuren zu verwischen und eine **schrittweise Datenexfiltration** zu verschleiern. Im Purview-Portal entsteht ein Fall mit hoher Priorität, da hier ein möglicher gezielter Datendiebstahl vermutet wird. Das Sicherheitsteam erhält detaillierte Einsichten: etwa welche **sensitiven Informationstypen** betroffen waren und ob die Dokumente klassifizierte (gelabelte) Informationen enthielten. Mit diesen Informationen konfrontiert, gesteht die Mitarbeiterin schließlich, dass sie in Aussicht auf einen neuen Job bei einem Mitbewerber Firmenunterlagen sammeln wollte. Durch die Kombination von **Benutzer- und Aktivitätenanalyse über längere Zeiträume** sowie intelligenten ML-Modellen konnte dieser schwer erkennbare Vorfall aufgedeckt werden – ein gutes Beispiel dafür, wie moderne Insider-Risikomanagement-Tools auch *schleichende Gefahren* sichtbar machen.

Beispiel 3: Auffällige Kommunikation als Frühwarnsignal

Insider-Risiken zeigen sich nicht nur in direkten Datenaktionen, sondern oft auch im **Kommunikationsverhalten**. Im dritten Szenario beobachtet das Unternehmen einen Mitarbeiter, der in Microsoft Teams und E-Mails durch **ungewöhnlich negative oder regelwidrige Kommunikation** auffällt. Er verwendet etwa eine aggressive, beleidigende Sprache gegenüber Kollegen in Teams-Chats und erwähnt wiederholt Frustration über das Unternehmen. Solche Kommunikationsmuster können auf einen **unzufriedenen oder potenziell illoyalen Mitarbeiter** hindeuten – ein mögliches Frühwarnsignal für kommende Regelverstöße oder Sabotage.

Microsoft Purview verfügt über **Communication Compliance**-Richtlinien, die genau solche Inhalte erkennen. In unserem Fall schlagen die Kommunikationsrichtlinien Alarm wegen Verstößen gegen den Verhaltenskodex (beleidigende Nachrichten) und möglicher Andeutungen, vertrauliche Informationen weiterzugeben. Diese Informationen fließen nun als Signal in das **Insider Risk Management** ein. Tatsächlich hat der betreffende Mitarbeiter kurz nach einer Abmahnung durch seinen Vorgesetzten begonnen, sich auffällig zu verhalten. Insider Risk Management kombiniert die Hinweise aus Teams-Chats mit weiteren Indikatoren: Der Mitarbeiter hat etwa zur

gleichen Zeit begonnen, **vermehrt Dateien aus einem sensiblen Projektordner** auf SharePoint aufzurufen, ohne dass es dafür eine berufliche Notwendigkeit gab. Außerdem wurden **E-Mails mit sensiblen Schlagwörtern** (z. B. „Gehaltsliste“, „Projektofferte“) an externe Empfänger erkannt.

Auf Basis dieser **vielfältigen Signale** (Kommunikationsverhalten + Datenzugriffe) bewertet das System den Mitarbeiter als *erhöhtes Insider-Risiko*. Ein Fall wird eröffnet, und das interdisziplinäre Insider-Risk-Management-Team – bestehend aus IT-Sicherheit, Compliance, HR und ggf. Rechtsabteilung – tritt zusammen. Zunächst bleibt die Identität des Mitarbeiters anonymisiert, um Vorurteilen vorzubeugen. Die Analysten sichten die Chatverläufe (soweit zulässig), Protokolle der Datenzugriffe und die DLP-Events. Durch diese ganzheitliche Betrachtung ergibt sich ein Bild: Der Mitarbeiter ist unzufrieden und könnte in Kürze versuchen, sensible Daten zu exfiltrieren. Als präventive Maßnahme wird beschlossen, ihn vertraulich auf die Situation anzusprechen. Gleichzeitig verschärft das Unternehmen die **Überwachung seiner Aktivitäten adaptiv**: Sämtliche Interaktionen mit sensiblen Daten werden nun in Echtzeit geprüft, und bestimmte Aktionen (z. B. das Teilen von Dateien nach extern) werden für ihn temporär blockiert. Tatsächlich zeigt sich, dass der Mitarbeiter kurz darauf versucht, doch noch Daten zu kopieren – was durch die neuen Beschränkungen verhindert wird. Dieses Beispiel verdeutlicht, wie **Kommunikationsrichtlinien** als **Frühwarnsystem** dienen können. **Insider Risk Management** nutzt solche weichen Signale, um proaktiv ein mögliches Sicherheitsproblem zu erkennen, bevor konkreter Schaden entsteht.

Beispiel 4: Umgehung von Sicherheitsmaßnahmen mit sequenziellen Aktionen

Erfahrene Insider mit bösen Absichten versuchen oft, **Sicherheitsmaßnahmen gezielt zu umgehen**. Im vierten Szenario entdeckt Insider Risk Management einen Mitarbeiter der F&E-Abteilung, der scheinbar **clever vorgeht**, um Daten zu stehlen. Er hat Zugang zu einer streng vertraulichen technischen Dokumentation. Anstatt die Datei direkt herunterzuladen und weiterzuleiten (was DLP leicht erkennen würde), wendet er einen Trick an: Zunächst kopiert er den Inhalt der Datei und fügt ihn in ein neues Word-Dokument ein. Dieses neue Dokument **entfernt er von allen vertraulichen Kennzeichnungen** – er ändert z. B. den Titel und entfernt die Microsoft Information Protection Labels, die automatisch auf die Originaldatei angewendet waren. Anschließend druckt er das Dokument als PDF aus und gibt der PDF einen unverfänglichen Namen. Danach versucht er, diese PDF an einen externen Partner zu mailen.

Ein derartiger Vorgang ist darauf ausgelegt, **inhaltliche Schutzmechanismen zu unterlaufen** – die vertrauliche Information verlässt das Unternehmen in vermeintlich harmloser Form. Allerdings greifen hier die **fortschrittlichen Sequenz-Detektionsfunktionen** von Microsoft 365. Insider Risk Management erkennt die **Abfolge verdächtiger Aktivitäten**: Datei kopiert → Datei umbenannt/umetikettiert → sensitives Dokument gedruckt/exportiert → Datei gelöscht oder versandt. Jede Aktion für sich könnte legitim erscheinen, doch die **Sequenz als Ganzes** deutet auf eine Absicht hin, Daten an der DLP-Prüfung vorbeizuschleusen. Das System generiert einen hochpriorisierten Alarm, da eine definierte **Sequenz-Richtlinie** ausgelöst wurde.

Im Purview-Portal sieht der Ermittler dank der Forensikdaten genau diese Schritte zeitlich aufgefädelt: Wann wurde welches Label entfernt, wann wurde gedruckt, wann gelöscht usw. – inklusive Dateinamen und Gerätenutzung. Diese **Visualisierung der Ereigniskette** (Sequence Analysis) macht die mutmaßliche Absicht klar erkennbar. Das Sicherheitsteam handelt umgehend: Der Mitarbeiter wird noch während der Untersuchung vom Netzwerk getrennt, alle Zugriffe auf sensible Bereiche werden entzogen. Später bestätigt sich, dass er versuchte, **geistiges Eigentum** für einen privaten Zweck abzuziehen. Durch die **automatisierte Erkennung komplexer Sequenzen** konnte dieser gezielte Angriff von innen erfolgreich vereitelt werden – ein eindrucksvolles Beispiel dafür, wie **kombinierte Signale** (z. B. Label-Änderungen, Druckvorgänge, Dateiaktionen) in Microsoft 365 zu **hochwertigen Alarmen** führen.

Beispiel 5: Versehentliche Datenweitergabe und gezielte Schulung

Nicht alle Insider-Vorfälle basieren auf böser Absicht – häufig sind es **Versehen oder Unachtsamkeiten** von Mitarbeitern, die zu Datenschutzvorfällen führen. Im letzten Beispiel nutzt ein Mitarbeiter einer Fachabteilung einen Cloud-Speicherdienst außerhalb von Microsoft 365, um an einem Dokument zu arbeiten. Er lädt vertrauliche Kundendaten auf seine persönliche Dropbox hoch, weil ihm nicht bewusst ist, dass dies gegen die Richtlinien verstößt. Ebenso schickt er einer externen Beratung einige interne Unterlagen per E-Mail, da er die **Unternehmensrichtlinie zur Dateifreigabe** missverstanden hat. Solche Aktionen sind *gut gemeint, aber riskant* – sie können zu Datenverlust oder Compliance-Problemen (z. B. Verstoß gegen DSGVO) führen, wenn sensible Inhalte in unkontrollierte Umgebungen gelangen.

Microsoft 365 DLP erkennt die E-Mail mit den internen Unterlagen und markiert sie als Verstoß (die Dokumente enthielten z. B. den Vermerk "Vertraulich"). Gleichzeitig registriert Defender for Cloud Apps (Cloud App Security) die Nutzung eines **nicht**

genehmigten Cloud-Dienstes und meldet eine Warnung. Diese Signale werden vom **Insider Risk Management** aggregiert. Das System stuft den Vorfall zunächst als **mittelmäßig riskant** ein, da keine Anzeichen für Vorsatz vorliegen, jedoch ein **Schulungsbedarf** offensichtlich ist. Im Purview-Portal wird ein Fall erstellt, jedoch mit dem Hinweis auf **möglicherweise unbeabsichtigtes Verhalten**. Der Insider-Risk-Analyst prüft die Aktivitäten und stellt fest, dass der Mitarbeiter bislang unauffällig war und vermutlich aus Unwissen gehandelt hat.

Statt einer harten Maßnahme wird entschieden, den Mitarbeiter und sein Team gezielt nachzuschulen. Über eine vorbereitete **Notice-Vorlage** in Insider Risk Management erhält der Mitarbeiter eine E-Mail, die ihn auf den Richtlinienverstoß hinweist und die korrekten Vorgehensweisen erläutert (z. B. Nutzung von **OneDrive for Business** statt privater Clouds, geschütztes Teilen via SharePoint, etc.). Der Mitarbeiter reagiert einsichtig, entfernt die Daten aus der Dropbox und nutzt fortan die bereitgestellten sicheren Methoden. Dieser Fall wird im System als **geschlossen** markiert, ohne dass disziplinarische Schritte nötig waren. Für das Compliance-Team dient er aber als Hinweis, die interne Kommunikation zu **Sicherheitsrichtlinien** zu verbessern.

Dieses Beispiel zeigt, dass Insider Risk Management nicht nur zur **Bestrafung** dient, sondern vor allem zur **Risikominimierung durch Aufklärung**. Durch das Zusammenspiel verschiedener Funktionen – Cloud-App-Überwachung, DLP und das Fall-Management in Purview – konnten **versehentliche Verstöße** erkannt und behoben werden, bevor ein echter Schaden entstand. Zudem hilft die Dokumentation solcher Vorfälle dem Unternehmen, **Trends zu analysieren** und präventive Maßnahmen (wie Trainings oder angepasstere Richtlinien) abzuleiten. So fördert die Lösung letztlich eine Kultur der Aufmerksamkeit und Compliance, indem sie aus Fehlern **Lernchancen** macht.

Technische Funktionsweise des Insider Risk Management in Microsoft 365

Nach den Praxisbeispielen werfen wir einen Blick auf die **technischen Grundlagen** und die Architektur des Insider Risk Management in Microsoft 365. Die Lösung ist eng in die Microsoft-Purview-Compliance-Suite integriert und schöpft aus einer Vielzahl von Datenquellen innerhalb und außerhalb von Microsoft 365, um ein umfassendes Bild von Nutzeraktivitäten zu erhalten.

Abb. 1: Vereinfachter Workflow von Microsoft Purview Insider Risk Management – von Richtlinien über Alerts bis zur Untersuchung und Maßnahmen (Schema eines Insider-

Risikomanagement-Workflows).

Signalquellen und Indikatoren: Insider Risk Management korreliert Ereignisse aus praktisch allen relevanten Services von Microsoft 365. **Exchange Online** und **Teams** liefern Hinweise auf verdächtige Nachrichten oder Dateifreigaben, **SharePoint Online** und **OneDrive** melden Massen-Downloads, Freigaben oder das Zugreifen auf sensible Dateien, **Windows 10/11**-Clients liefern via **Microsoft Defender for Endpoint** Informationen zu Dateioperationen auf Geräten (z. B. Kopieren auf USB, lokale Dateiverschiebungen, Drucken). Auch **Azure Active Directory (Entra)** kann einbezogen werden – zum Beispiel via **Conditional Access Signale**, die ungewöhnliche Anmeldeorte oder -zeiten eines Benutzers markieren. Alle diese Signale werden im Hintergrund gesammelt und ausgewertet. Microsoft hat eine Vielzahl **vordefinierter Risiko-Indikatoren** bereitgestellt (Stand 2023/2024 sind es über 15 neue Indikatoren zusätzlich zu den ursprünglichen). Beispiele solcher Indikatoren sind:

- **Massendownloads oder -löschungen** von Dateien in kurzer Zeit
- **Externes Teilen** von als vertraulich klassifizierten Dokumenten
- **Versand sensibler Informationen** per E-Mail an Empfänger außerhalb der Organisation
- **Verstöße gegen DLP-Policies** (z. B. Versuch, Kreditkartendaten oder personenbezogene Daten zu übertragen)
- **Geräte-Aktivitäten** wie das Kopieren sensibler Dateien auf Wechseldatenträger, ungewöhnliches Drucken oder Screenshot-Erstellung
- **Label-Änderungen** bei Dokumenten (Herabstufen oder Entfernen von Sensitivity Labels)
- **Auffällige Kommunikationsinhalte** (z. B. beleidigende Sprache oder das Preisgeben vertraulicher Infos in Chats, erkannt durch Communication Compliance)

Diese Indikatoren können je nach Geschäftsrisiko priorisiert werden. Unternehmen haben die Möglichkeit, **eigene Schwellenwerte und Kombinationen** festzulegen. Beispielsweise könnte eine Policy definieren: *„Wenn ein Benutzer innerhalb von 7 Tagen mehr als 100 vertrauliche Dateien herunterlädt **und** in derselben Zeit mindestens 1 Datei an eine externe Adresse sendet, triggere Alarm.“* Durch solche kombinierten Kriterien werden **Fehlalarme reduziert**, und wirklich riskante Muster stechen hervor.

Risikobewertung und -Scoring: Hinter den Kulissen arbeitet Insider Risk Management mit einem **Scoring-Modell**. Jede erkannte Aktion, die auf eine Richtlinie passt, erhöht (oder in manchen Fällen senkt) den Risiko-Score eines Benutzers. Faktoren wie **Wiederholungsrate, Schweregrad der Daten** (z. B. top-geheime Infos vs. intern), und

Kontext (etwa ob der Benutzer kürzlich eine Kündigung angekündigt hat) beeinflussen die Gewichtung. Microsoft setzt hierbei auch **Machine-Learning-Modelle** ein, um Anomalien zu entdecken, die mit statischen Regeln schwer zu fassen wären. Ein Beispiel ist das zuvor erwähnte Modell zur schleichenden Exfiltration (CEAD) oder die Sequenzanalyse von Kombinationshandlungen. Diese ML-Modelle vergleichen das Benutzerverhalten mit **historischen Daten und Peer-Gruppen** – so können sie erkennen, wenn jemand deutlich vom üblichen Verhalten abweicht. Wird ein vordefinierter **Risikowert** überschritten, erzeugt das System automatisch einen **Alert** und – je nach Konfiguration – direkt einen **Case (Fall)** zur Untersuchung.

Dashboard und Fallmanagement: Im Microsoft Purview Compliance-Portal steht eine spezielle **Insider-Risk-Management-Dashboard** zur Verfügung. Hier sehen berechtigte Analytiker auf einen Blick alle **aktiven Warnungen**, laufenden Fälle, Statistiken zu Richtlinientreffern sowie gelistete **Risikobenutzer** (pseudonymisiert) mit ihrem aktuellen Score. Aus diesem Dashboard heraus kann man in einzelne Fälle eintauchen. Jeder **Case** enthält eine **Timeline der relevanten Aktivitäten** des Betroffenen, verbunden mit den getriggerten Indikatoren. Dazu können Ermittler zusätzliche Daten einsehen: z. B. Vorschaubilder von Dokumenten (wenn Forensik aktiviert ist), Kommunikationsausschnitte oder **Kartenansichten der Dateiaktionen**. Dieses Fallmanagement ist darauf ausgelegt, **teamübergreifend** zu arbeiten – so können Notizen hinzugefügt, Zuständigkeiten (z. B. Zuweisung an einen zweiten Ermittler) vergeben und sogar ein dedizierter **Microsoft Teams-Kanal** für den Fall erstellt werden, in dem sich Sicherheitsteam, HR und Rechtsabteilung abstimmen können (diese Option existiert seit einer neueren Version). Falls ein Vorfall juristisch relevant wird, lässt sich der Fall auch an **Microsoft Purview eDiscovery (Premium)** übergeben, um Beweismaterial für rechtliche Schritte zu sichern.

Integration mit Microsoft Defender und Sentinel: Ein großer Vorteil von Microsofts Ökosystem ist die Verzahnung zwischen Sicherheitslösungen. So können Organisationen **Microsoft Defender for Endpoint (MDE)** einsetzen, um Endgeräteaktivitäten als Signale bereitzustellen – etwa das Blockieren von USB-Geräten oder das Erkennen von riskanten Aktionen auf Clients fließen direkt in das Insider Risk Management ein. MDE ermöglicht auch, *gezielte Gerätedaten* (wie die genaue Datei, die kopiert wurde) an Purview zu liefern, um die Untersuchungen zu untermauern. **Microsoft Defender for Cloud Apps** (früher MCAS) wiederum meldet riskante Cloud-Nutzungen, wie im Beispiel 5 gesehen (Shadow IT). Diese Informationen erhöhen die Abdeckung auf Aktivitäten, die außerhalb von M365-Kernservices stattfinden, aber trotzdem sicherheitsrelevant sind.

Darüber hinaus lassen sich die Insider-Risk-Alerts auch ins **SIEM** integrieren. Microsoft

bietet einen **Connector für Microsoft Sentinel** (Azure Sentinel) an, der die Insider Risk Management Vorfälle und Warnungen in Sentinel einspeist. So können SOC-Analysten alle Sicherheitsalarme – ob extern oder intern – in einem zentralen Monitoring sammeln. Ein Anwendungsfall: Korrelation mit anderen Ereignissen. Wenn z. B. zeitgleich ein externer Angriff und ein Insider-Alarm erfolgen, könnte Sentinel dies erkennen und verbandelte Vorfälle vermuten. Ebenso können in Sentinel eigene Playbooks (über Azure Logic Apps) definiert werden, die bei einem Insider-Alert **automatisch Maßnahmen** auslösen – etwa das Erstellen eines Tickets im ITSM-System oder das sofortige Verschärfen von Zugriffsrichtlinien. Diese SIEM-Integration erhöht die **Skalierbarkeit** der Überwachung, insbesondere in großen Organisationen mit einem 24/7-Security Operations Center.

Verbindung mit Microsoft Information Protection: Microsoft 365 besitzt mit **Information Protection** ein umfassendes Klassifizierungs- und Labeling-System für Daten. Diese Klassifizierungen (Sensitivity Labels, z. B. "Öffentlich", "Vertraulich", "Streng Vertraulich") und auch automatisiert erkannte **Sensitive Information Types** (wie Kreditkartennummern, personenbezogene Daten usw.) spielen im Insider Risk Management eine wichtige Rolle. Viele Richtlinien lassen sich so einstellen, dass **nur Aktionen mit bestimmten Klassifizierungen** betrachtet werden – zum Beispiel ausschließlich Vorfälle, die **geheime** Daten betreffen. Umgekehrt kann das Entfernen oder Herabstufen eines Labels selbst als verdächtige Aktion gewertet werden (wie in Beispiel 4 gezeigt). Die Kombination aus **MIP** und Insider Risk Management stellt sicher, dass die **Inhaltssensitivität** in die Risikoanalyse einfließt. Somit wird etwa ein Download von 50 Dokumenten, die alle als "öffentlich" klassifiziert sind, anders bewertet als ein Download von 5 Dokumenten, die "vertraulich" sind. Unternehmen profitieren hier von einem ganzheitlichen **Data Governance-Ansatz**: von der **Erkennung und Klassifizierung** wichtiger Daten über **Schutzmaßnahmen** (Verschlüsselung, DLP) bis hin zu **Überwachung und Reaktion** bei Verstößen – alles nahtlos integriert in Microsoft 365.

Zusammengefasst funktioniert Insider Risk Management in Microsoft 365 als **Konzert verschiedener Tools**: Purview als Orchestrator im Compliance-Bereich, Defender und DLP als Sensoren und Enforcer, Information Protection als Kontextlieferant und Sentinel als übergeordnete Monitoring- und Response-Plattform. Diese technische Verzahnung ermöglicht es, Insider-Risiken **früh und zuverlässig** zu erkennen und mit abgestimmten Mitteln darauf zu reagieren – und das unter Wahrung von **Transparenz und Datenschutz** durch Funktionen wie Pseudonymisierung, rollenbasierte Zugriffe und umfassende Protokollierung.

Neue Funktionen und aktuelle Entwicklungen im Insider Risk Management

Die Landschaft der Insider-Risikoabwehr entwickelt sich stetig weiter – Microsoft erweitert kontinuierlich die Fähigkeiten von Purview Insider Risk Management, um neuen Bedrohungen und Anforderungen gerecht zu werden. Im Folgenden betrachten wir einige **neue oder kürzlich eingeführte Funktionen**, die besonders hervorstechen. Dazu zählen der **Einsatz von KI (Künstlicher Intelligenz)** und Machine Learning zur Risikobewertung, **adaptive Richtlinien** für dynamischen Schutz sowie **erweiterte Signalquellen** und Integrationen (etwa aus Teams, SharePoint, Exchange und sogar aus der Nutzung von KI-Anwendungen).

- **ML-gestützte Anomalie- und Sequenz-Erkennung:** Moderne Insider-Risikoerkennung geht über starre Regeln hinaus. Microsoft hat etwa das **Cumulative Exfiltration Detection (CEAD)** eingeführt, ein ML-Modell, das *kumulative Datenabflüsse* erkennt, wie im Beispiel 2 beschrieben. Dieses Modell lernt das übliche Level an Datei-Exporten in der Organisation oder Peer-Gruppe und schlägt Alarm, wenn ein Nutzer über einen Zeitraum hinweg signifikant mehr Daten exfiltriert als normal. Ebenso wurden **Sequenzindikatoren** stark ausgebaut: Früher dienten Sequenzen (z. B. "Datei umbenennen -> Datei exfiltrieren -> Datei löschen") nur als Kontext, jetzt können sie **direkt als Auslöser** für Richtlinienalarme fungieren. D. h. Administratoren können definieren, dass genau solch eine Sequenz einen Alarm erzeugt, auch wenn Einzelaktionen unkritisch wären. Dies erhöht die **Qualität der Alerts**, weil zielgerichtete, komplexe Insider-Handlungen erkannt werden, die herkömmliche DLP übersehen würde. Insgesamt sorgen diese ML-Verbesserungen dafür, dass **weniger Fehlalarme** auftreten und echte Risiken besser hervorgehoben werden.
- **Adaptive Schutzmaßnahmen (Adaptive Protection):** Eine der spannendsten Weiterentwicklungen ist die Einführung **adaptiver Richtlinien** im Insider Risk Management. Dabei handelt es sich um einen Ansatz, der **dynamisch die Sicherheitskontrollen verschärft**, sobald das System einen erhöhten Risikolevel für einen Benutzer feststellt. Konkret bedeutet das: Microsoft 365 kann z. B. DLP-Restriktionen *situationsabhängig* anpassen. Hat ein Mitarbeiter einen hohen Insider-Risikowert, so könnten automatisch strengere Regeln für ihn gelten – etwa Blockieren aller Dateidownloads aus bestimmten sensiblen SharePoint-Sites oder das Erzwingen von Verschlüsselung bei E-Mail-Anhängen. Gleichzeitig dürfen für niedrig riskante Benutzer die Richtlinien großzügiger

bleiben, um ihre Produktivität nicht unnötig einzuschränken. Diese Adaptive Protection wird durch die Verknüpfung von Insider Risk Management mit **Microsoft Entra (Azure AD) Conditional Access** ermöglicht. So kann beispielsweise ein Conditional-Access-Policy aktiviert werden, die einem "High Risk User" (Einstufung kommt aus IRM) den Zugriff auf bestimmte Cloud-Apps verwehrt oder zusätzliche MFA-Anforderungen stellt. Ein praktisches Beispiel: Ein Mitarbeiter mit niedrigem Risiko darf weiterhin Teams benutzen wie gewohnt, ein Mitarbeiter mit hohem Risiko hingegen bekommt beim Versuch, in Teams eine Datei mit sensiblen Inhalten zu teilen, einen Block oder zumindest einen zusätzlichen Bestätigungsschritt. Adaptive Richtlinien helfen, den **Spagat zwischen Sicherheit und Produktivität** zu meistern – Schutz wird dort verstärkt, wo er nötig ist, und bleibt flexibel, wo kein akutes Risiko besteht.

- **Erweiterte Signalsammlung aus M365-Diensten:** Microsoft hat in den letzten Releases die Bandbreite der überwachten Aktivitäten deutlich vergrößert. Insbesondere **Microsoft Teams** ist nun eine reichhaltige Signalquelle. So können Insider-Richtlinien jetzt auch auslösen, wenn etwa **Teams-Nachrichten sensible Informationstypen** enthalten (z. B. jemand postet Kundendaten in einen öffentlichen Kanal). Ebenfalls neu ist die enge **Integration mit Communication Compliance**, wie zuvor dargestellt: Nicht regelkonformes Verhalten in Kommunikation (Belästigung, Drohungen, Andeutungen von Datenweitergabe) kann direkt als **Signal für Insider Risk** herangezogen werden. **SharePoint und OneDrive** liefern inzwischen detailliertere Signale – etwa wird das *Herabstufen von Dokumentenklassifikationen* (Label-Downgrade) oder der Zugriff auf **Prioritätsdateien/-standorte** (die als besonders sensibel markiert sind) erfasst. In **Exchange Online** wiederum können jetzt auch bestimmte Muster im Mailverkehr als Signal dienen, z. B. wenn ein Benutzer in kurzer Zeit an viele externe Empfänger sendet oder manuell E-Mail-Regeln erstellt, um Kopien von Mails an externe Postfächer weiterzuleiten. Diese Verbesserungen stellen sicher, dass **keine blinden Flecken** entstehen – alle relevanten Kanäle, über die Daten fließen könnten, werden abgedeckt.
- **Integration von KI-/Copilot-Signalen:** Mit dem Aufkommen von **Generativer KI** in Unternehmen (Stichwort: Benutzer nutzen Tools wie ChatGPT, Copilots etc.) hat Microsoft begonnen, auch hierfür Lösungen zu bieten. Neu angekündigt (Stand 2024/2025) sind **Risky AI Usage**-Erkennungen in Insider Risk Management. Diese zielen darauf ab zu erkennen, wenn Mitarbeiter sensible Daten in KI-Systeme einspeisen oder riskante Prompts verwenden. Beispielsweise würde ein Alarm erzeugt, wenn ein Nutzer große Textmengen mit vertraulichen Inhalten in **ChatGPT Enterprise** oder den **Microsoft 365 Copilot** eingibt. Ebenso soll erkannt werden, wenn ein KI-Service Antworten gibt,

die mit internen sensiblen Informationen erstellt wurden. Solche Signale fließen in den Insider-Risikolevel ein und ermöglichen es, **frühzeitig gegenzusteuern**, bevor Daten über externe KI-APIs abfließen. Ergänzend dazu wird **Microsoft Edge for Business** mit neuen Schutzfunktionen ausgestattet, die abhängig vom IRM-Risikolevel des Nutzers bestimmte KI-Aktionen im Browser blockieren oder erlauben. Adaptive Protection kann so etwa verhindern, dass ein als risikoreich eingestufter Benutzer *überhaupt* sensible Inhalte an ein KI-System sendet. Diese Entwicklungen zeigen den **zukunftsorientierten Ansatz**: Insider Risk Management passt sich neuen Technologien an, um auch dort Datenabfluss und Missbrauch zu verhindern, wo klassische DLP nicht ohne Weiteres greifen kann.

- **Automatisierte Alarm-Triage mittels KI:** Angesichts der wachsenden Flut an Sicherheitsmeldungen arbeitet Microsoft daran, **KI-Assistenz in die Fallbearbeitung** zu integrieren. Ein Beispiel ist der *Alert Triage Agent* auf Basis von **Microsoft Security Copilot**, der 2025 in Insider Risk Management eingeführt wurde. Dieses KI-Modul analysiert eingehende Insider Alerts und hilft den Sicherheitsanalysten, die **wichtigsten Fälle zuerst** anzugehen. Es bewertet die Alarme anhand von Kontext und potentiellem Schadensausmaß und liefert Erklärungen, warum ein bestimmter Fall dringlich ist. In ersten Tests zeigte sich, dass solche KI-Unterstützung die Effizienz deutlich steigern kann – gerade bei Unternehmen, die täglich dutzende von Warnungen überprüfen müssen. Der Triage Agent, der im April 2025 zunächst als Public Preview startete, nutzt *Generative AI*, um Muster zu erkennen, die menschliche Analysten möglicherweise übersehen, und um **empfohlene Prioritäten** auszusprechen. Während der endgültige Einfluss solcher Tools noch in der Praxis evaluiert wird, deutet der Trend darauf hin, dass **AI künftig vermehrt Routineaufgaben** im Insider Risk Management übernimmt – von der Priorisierung bis möglicherweise hin zur automatischen Fallbearbeitung in einfachen Szenarien. Für Unternehmen bedeutet das eine Chance, trotz knapper Security-Ressourcen (Stichwort Fachkräftemangel) die wachsende Anzahl an Sicherheitsvorfällen im Griff zu behalten.

Diese Beispiele neuer Funktionen zeigen, dass Microsoft Purview Insider Risk Management ständig **weiterentwickelt und verbessert** wird. Gerade **Machine Learning und KI** stehen im Mittelpunkt, um sowohl die Erkennung *smarter* zu machen als auch die **Bearbeitung** der Fälle effizienter zu gestalten. Gleichzeitig wird das **Spektrum der überwachten Aktivitäten** laufend erweitert – von klassischen Office-Daten bis hin zu modernen Kollaborations- und KI-Tools. Unternehmen, die auf Microsoft 365 setzen, können somit sicher sein, dass ihre Insider-Risk-Strategie mit den neuesten Bedrohungen Schritt hält. Dennoch ist es wichtig zu betonen: Technik allein löst nicht alle Probleme. Die besten Ergebnisse erzielt man, wenn diese Innovationen in

ein durchdachtes Gesamtkonzept eingebettet sind – mit klaren Richtlinien, geschulten Mitarbeitern und abgestimmten Prozessen, wie wir im Folgenden sehen werden.

Einsatz in Unternehmen: Governance, Transparenz und Skalierbarkeit

Insider Risk Management ist nicht nur etwas für Großkonzerne – die Thematik betrifft **Unternehmen jeder Größenordnung**, vom Mittelständler bis zum globalen Konzern. Allerdings unterscheiden sich die Umsetzung und Schwerpunkte je nach Unternehmensgröße und -kultur. In diesem Abschnitt betrachten wir, wie man ein Insider-Risiko-Programm **skalierbar und transparent** gestaltet und welche **Governance-Aspekte** wichtig sind, damit die Lösung effektiv und akzeptiert ist.

Governance und Richtlinienrahmen: Unabhängig von der Größe des Unternehmens sollte Insider Risk Management in einen klaren **Governance-Rahmen** eingebettet sein. Das bedeutet: Es gibt definierte **Rollen und Verantwortlichkeiten** (z. B. Insider Risk Analyst, Ermittler, Datenschutzbeauftragter, etc.) und es existieren Richtlinien, *wann* und *wie* welche Datenüberwachung stattfinden darf. Besonders in großen Organisationen empfiehlt es sich, ein **querschnittliches Gremium** oder Komitee zu etablieren, das das Insider-Risk-Programm steuert – mit Vertretern aus IT-Security, Compliance, Datenschutz, Personal (HR) und Recht. Dieses Gremium setzt die Prioritäten (welche Risiken sind kritisch?), genehmigt neue Insider-Richtlinien und überprüft regelmäßig die Effektivität der Maßnahmen. In kleineren Unternehmen mag ein einziger IT-Leiter zusammen mit dem Datenschutzbeauftragten diese Rolle übernehmen. Wichtig ist in jedem Fall, dass Insider Risk Management **nicht isoliert von der restlichen Compliance- und Sicherheitsstrategie** betrieben wird, sondern als integraler Bestandteil davon. Es sollte an bestehende Policies (z. B. Acceptable Use Policy, Datenschutzrichtlinien) anknüpfen und durch entsprechende **Dienstanweisungen oder Betriebsvereinbarungen** formal verankert sein.

Transparenz und Vertrauenskultur: Gerade im deutschen Umfeld spielt **Transparenz** gegenüber den Mitarbeitern eine zentrale Rolle für die Akzeptanz solcher Überwachungsmaßnahmen. Unternehmen sollten frühzeitig und offen kommunizieren, **welche Art von Monitoring** eingeführt wird und warum. Eine Kultur, die *Sicherheit als gemeinsames Ziel* versteht, wird Insider-Risk-Maßnahmen eher unterstützen. Beispielsweise kann man Schulungen und Info-Sessions anbieten, in denen erklärt wird, dass das System vor allem dazu dient, **Firmen-Know-how zu schützen und Compliance-Verstöße zu verhindern**, nicht um Mitarbeiter auszuspionieren. Oft wird

empfohlen – und von Betriebsräten gefordert – dass Mitarbeiter zumindest in Kenntnis gesetzt werden, **welche Daten erfasst** und wie sie ausgewertet werden. Microsoft Purview IRM bietet hier den Vorteil der eingebauten **Pseudonymisierung** und strikten Rechtevergabe: Einfache Administratoren sehen keine Klarnamen, und nur speziell befugte Personen (im Rahmen definierter Verfahren) dürfen Verdachtsfälle einsehen. Dieses Prinzip sollte den Mitarbeitern erklärt werden, um Vertrauen zu schaffen, dass **Datenschutz und Persönlichkeitsschutz** trotz der Überwachung gewahrt bleiben. Zudem kann Transparenz bedeuten, dass regelmäßige **Berichte** über die Nutzung des Tools anonymisiert veröffentlicht werden (z. B. „Im letzten Quartal gab es X Alarme, in Y Fällen erfolgten Schulungsmaßnahmen, keine ungerechtfertigten Überwachungen fanden statt“). Solche Schritte fördern eine **Vertrauenskultur**, in der Sicherheit und Datenschutz Hand in Hand gehen.

Skalierbarkeit und Automatisierung: Für große Unternehmen mit tausenden Mitarbeitern muss ein Insider-Risk-Programm **skaliert** werden können. Hier zeigen sich die Stärken von Microsoft 365: Da IRM cloudbasiert ist, lässt es sich in derselben Umgebung auf 50 oder 50.000 Nutzer anwenden. Die **Machine-Learning-Modelle** und intelligenten Filter helfen, auch bei hohem Aufkommen den Überblick zu behalten, indem sie wie erwähnt **die wichtigsten Alarme priorisieren** und Duplikate reduzieren. Außerdem ermöglichen Integrationen wie mit Microsoft Sentinel, dass bestehende Security Operation Center die Insider-Überwachung in ihre Workflows integrieren, ohne separate Infrastruktur. Für kleinere Firmen ist hingegen attraktiv, dass man mit **vorkonfigurierten Richtlinien** (Microsoft liefert einige Templates etwa für „Datendiebstahl durch kündigende Mitarbeiter“ oder „Vertrauliche Daten in Kommunikation“) schnell starten kann, ohne ein großes Expertenteam aufzubauen. Auch bietet Microsoft die Möglichkeit, via **FastTrack**-Programme oder Partnerunterstützung die Einführung zu begleiten, was gerade KMU nutzen können, um Fachwissen einzukaufen.

Einsatzperspektiven für kleine und große Unternehmen: Ein **kleines Unternehmen** mit z. B. 100 Mitarbeitern und hohem Schutzbedarf (etwa in der Technologieentwicklung) kann mit IRM gezielt seine Kronjuwelen schützen: Es könnte sich auf 2–3 kritische Insider-Risiko-Szenarien konzentrieren, die sehr **maßgeschneidert** eingestellt werden. Zum Beispiel Überwachung von Quellcode-Repo-Zugriffen oder CAD-Zeichnungen bei den paar Entwicklern, die diese haben – während man den Rest der Organisation relativ unbehelligt lässt. Durch die geringe Belegschaft ist auch der Abstimmungsaufwand mit dem Betriebsrat überschaubar; oft kennt man sich persönlich und kann die Vorteile direkt vermitteln.

Ein **Großkonzern** hingegen, verteilt über verschiedene Länder, wird IRM breit ausrollen

und in seine bestehende Governance integrieren. Hier kommen Features wie **Priority User Groups** zum Tragen – man definiert etwa, dass die Führungsebene oder R&D-Leitung **als Prioritätsnutzer** besonders überwacht werden (weil dort die kritischsten Daten abfließen könnten). Gleichzeitig muss man in großen Organisationen stärker auf **regionale Unterschiede** achten: In manchen Ländern gelten strengere Regeln für Mitarbeiterüberwachung als in anderen. Die Lösung muss also flexibel in einzelnen Jurisdiktionen angepasst werden (z. B. gewisse Signaltypen in der EU deaktivieren, falls nötig, oder unterschiedlich lange Aufbewahrungszeiten von Protokollen je Land einhalten). Microsoft Purview erlaubt die **Segmentierung** nach Organisationseinheiten – Policies können z. B. nur für Mitarbeiter in bestimmten Ländern gelten, während andere ausgeschlossen sind. Das erhöht die Komplexität, ist aber für die globale Skalierung essentiell.

Nicht zuletzt spielt bei der Skalierbarkeit auch der **Lizenzaspekt** eine Rolle: Insider Risk Management erfordert in der Regel Microsoft 365 E5 oder einen zusätzlichen Compliance-Add-on SKU. Größere Firmen mit E5-Lizenzen haben es daher oft „inklusive“, während Mittelständler ohne E5 erst die Wirtschaftlichkeit prüfen. Microsoft adressiert das, indem es Trials anbietet und den Nutzen – wie wir gesehen haben – durch potentielle Vermeidung teurer Datenlecks rechtfertigt. Dennoch sollten Unternehmen jeder Größe einen **Business Case** rechnen: Ab welcher Schadenshöhe lohnt sich das Investment in diese Technologie? Meist lautet die Antwort: *Ein einziger verhinderter Insider-Vorfall kann die Kosten bereits wettmachen*, wenn man an mögliche Datenschutzstrafen oder Umsatzeinbußen durch Know-how-Abfluss denkt.

Zusammenfassend lässt sich sagen: Mit dem richtigen **Governance-Modell**, einer **transparente Kommunikation** und der **passenden Skalierungsstrategie** kann Insider Risk Management in Microsoft 365 in jeder Unternehmensgröße erfolgreich eingesetzt werden. Es bietet großen Unternehmen die nötige Tiefe und Automatisierung, um millionenfache Events zu stemmen, und kleineren Organisationen die Benutzerfreundlichkeit und Fokussierung, um ohne riesiges Security-Team gezielt ihre Werte zu schützen.

Schritt-für-Schritt: Einführung eines Insider Risk Management Programms in Microsoft 365

Die erfolgreiche Implementierung von Insider Risk Management ist weniger ein einmaliges Projekt als vielmehr der Aufbau eines **kontinuierlichen Programms**. Im Folgenden skizzieren wir die empfohlene **Vorgehensweise in sieben Schritten** – von

den ersten Vorbereitungen bis zum dauerhaften Betrieb. Diese Schritte helfen, technische, organisatorische und kulturelle Aspekte zu berücksichtigen, sodass das Programm sowohl **wirkungsvoll** als auch **rechtssicher** eingeführt wird.

1. **Vorbereitungsphase:** Zunächst gilt es, die **Grundlagen zu legen**. Bilden Sie ein Kernteam aus relevanten Stakeholdern – typischerweise **IT-Sicherheit, Compliance/Datenschutz, HR und Rechtsabteilung**. Führen Sie eine **Risikoanalyse** durch: Welche Insider-Risiken sind für Ihr Unternehmen am gravierendsten? (z. B. Abwanderung von Forschungsdaten, unerlaubter Zugang zu Patientendaten, Verstöße gegen Exportkontrollrichtlinien etc.) Basierend darauf definieren Sie klare **Schutzziele**. Ebenfalls in dieser Phase: Prüfen Sie die **rechtlichen Rahmenbedingungen**. In Deutschland ist das z. B. die Abstimmung mit dem Betriebsrat (siehe nächstes Kapitel) und die Durchführung einer **Datenschutz-Folgenabschätzung** (Data Protection Impact Assessment), falls nötig. Identifizieren Sie außerdem, welche **Microsoft 365-Lizenzen** und -Module benötigt werden (E5, E5 Compliance Add-on oder spezielle Add-ons für Insider Risk). Legen Sie fest, wer die Rollen „Insider Risk Analyst“ und „Investigator“ erhält, und sorgen Sie für entsprechende Schulungen dieser Personen.
2. **Pilotphase:** Starten Sie mit einem **begrenzten Pilot**. Wählen Sie eine kontrollierte Umgebung oder Abteilung für den Testlauf – idealerweise einen Bereich mit erhöhtem Schutzbedarf, aber überschaubarer Größe (z. B. die IT-Administratoren selbst oder die Forschungsabteilung). Konfigurieren Sie zunächst **einige wenige Richtlinien** mit eher *konservativen Schwellenwerten*, um ein Gefühl für das System zu bekommen, ohne eine Flut von Alerts auszulösen. Viele Unternehmen nutzen anfangs die **„Insider Risk Analytics“**-Funktion: Diese kann, bevor man überhaupt Policies aktiviert, eine Analyse fahren, welche potenziell riskanten Aktivitäten in den letzten Monaten vorgekommen wären. So bekommen Sie einen Eindruck, wo Handlungsbedarf besteht. Im Pilot sollte das Team die gesamte Prozesskette üben: Vom Eingang eines Alerts, über die Untersuchung im Purview-Portal, bis hin zur Eskalation/Kommunikation. Holen Sie in dieser Phase aktiv **Feedback** ein – von den Analysten (Benutzerfreundlichkeit? Fehlalarme?) ebenso wie von eventuell betroffenen Nutzern oder dem Betriebsrat. Ziel der Pilotphase ist es, die **Richtlinien zu kalibrieren** (Schwellen ggf. anpassen, überflüssige Signale ausschließen) und zu prüfen, ob alle organisatorischen Abläufe funktionieren.
3. **Implementierung der Lösung:** Nach einem erfolgreichen Pilot können Sie Insider Risk Management **unternehmensweit einführen**. Importieren oder erstellen Sie nun die vollständigen **Policy-Sets** entsprechend Ihrer identifizierten Risiken. Nutzen Sie gerne die **vorhandenen Templates** von Microsoft als Ausgangspunkt (z. B. für Datendiebstahl, Datenschutzverletzungen,

Kommunikationsverstöße) und passen Sie diese an Ihre Bedürfnisse an. Richten Sie die **globalen Einstellungen** ein: Aktivieren Sie die Benutzer-Pseudonymisierung (standardmäßig an), konfigurieren Sie eventuelle **Ausnahmen** (z. B. bestimmte SharePoint-Pfade oder Dateitypen von der Überwachung ausnehmen, um Rauschen zu reduzieren), definieren Sie „Priority Users“ und verknüpfen Sie bei Bedarf externe Konnektoren (z. B. **physische Badge-Systeme** für Zutrittsdaten, falls relevant). Stellen Sie sicher, dass **alle erforderlichen Datenquellen** angebunden sind: z. B. Onboarden der Endpunkte in Defender for Endpoint, Verbinden von Cloud App Security, etc., wie im technischen Teil beschrieben. Ein wichtiger Aspekt ist auch die **Automatisierung**: Überlegen Sie, welche Reaktionen automatisiert ablaufen sollen. Beispielsweise könnten Sie Microsoft Power Automate nutzen, um bei einem hohen Insider-Score automatisch einen vordefinierten Workflow zu triggern (Benachrichtigung an Vorgesetzte, Sperrung des Accounts, etc.). Testen Sie die Konfiguration ausführlich, indem Sie bekannte Szenarien bewusst provozieren (sofern erlaubt), um zu sehen, ob die Alarme wie gewünscht anschlagen.

4. **Rollout und Kommunikation:** Aktivieren Sie die Richtlinien *stufenweise*, z. B. zuerst für kritischste Abteilungen, dann sukzessive für alle. Parallel dazu ist die **Mitarbeiterkommunikation** zentral. Informieren Sie die Belegschaft über die Einführung von Insider Risk Management, idealerweise bevor es aktiv überwacht. Erklären Sie in verständlichen Worten das „Warum“ – nämlich Schutz der Firma und letztlich der Arbeitsplätze, sowie Sicherstellung von Compliance (z. B. keine DSGVO-Strafen). Betonen Sie den **Datenschutz**: dass keine Dauerüberwachung jeder E-Mail erfolgt, sondern gezielt bei definierten Risiken geschaut wird, und dass es Sicherheitsvorkehrungen gibt (Anonymisierung, Protokollierung). Gehen Sie ggf. auf die Mitbestimmungsvereinbarung mit dem Betriebsrat ein, damit Mitarbeiter wissen, es ist alles **in geordneten Bahnen**. Neben allgemeinen Ankündigungen kann es sinnvoll sein, **zielgruppenspezifische Trainings** anzubieten – z. B. für Vorgesetzte, wie sie mit Meldungen umgehen sollen, oder für Mitarbeiter in sensiblen Positionen, was von ihnen besonders erwartet wird. Im Rollout sollte auch eine **Anlaufstelle für Fragen** bereitstehen (etwa der Datenschutzbeauftragte oder CISO), um Unsicherheiten abzubauen. Technisch bedeutet Rollout auch, fortlaufend zu beobachten, ob die Systemperformance und das Alert-Volumen mit dem Hochlauf skaliert. Gegebenenfalls justieren Sie in den ersten Wochen nochmals die Schwellenwerte, falls zu viele oder zu wenige Alarme kommen.
5. **Kontinuierliches Monitoring und Verbesserung:** Ist das System im Wirkbetrieb, beginnt die eigentliche Daueraufgabe. **Monitoring** bedeutet hier

zweierlei: Zum einen natürlich das tägliche Überwachen und Bearbeiten der Insider-Alerts durch die Analysten – hierzu sollten klare **SLAs** definiert sein, wie schnell ein High-Severity-Alarm untersucht werden muss usw. Zum anderen aber auch das Meta-Monitoring des Programms selbst. Führen Sie regelmäßige **Review-Meetings** durch (z. B. monatlich oder quartalsweise), in denen Kennzahlen betrachtet werden: Wie viele Incidents gab es? Welche Kategorien traten häufig auf? Waren es eher echte Funde oder False Positives? Dieses Reporting hilft, das Programm gegenüber dem Management zu **rechtfertigen** und ggf. zusätzliche Ressourcen zu beantragen. Zudem können Änderungen im Unternehmen Anpassungen erfordern: Neue Geschäftsbereiche oder Technologien (z. B. die Einführung von Microsoft 365 Copilot im Unternehmen) erfordern eventuell neue Richtlinien oder Ausnahmen. Halten Sie sich über die **Weiterentwicklungen von Microsoft Purview** auf dem Laufenden (wie im vorherigen Abschnitt beschrieben). Es kommen jährlich neue Funktionen hinzu, die Sie per Update aktivieren oder in Anspruch nehmen können, um Ihre Abdeckung zu verbessern. Nicht zuletzt: Schulen Sie Ihr Incident Response Team regelmäßig weiter, tauschen Sie sich mit anderen Unternehmen aus (z. B. in Fachverbänden oder Microsoft User Groups), um **Best Practices** zu lernen. Insider Risk Management ist ein fortlaufender Lernprozess – was heute als sicher gilt, kann morgen ein Risiko darstellen und umgekehrt. Durch ein lebendiges Programm, das sich kontinuierlich **anpasst und verbessert**, stellen Sie sicher, dass Sie immer einen Schritt voraus sind.

Durch die Befolgung dieser Schritte nähert sich die Einführung strukturiert und unter Einbindung aller notwendigen Stellen. Besonders die **Pilotierung** und der fortlaufende **Dialog mit Stakeholdern** (Mitarbeitervertretung, Datenschutz etc.) sorgen dafür, dass das Programm nicht am „grünen Tisch“ vorbeientwickelt wird, sondern **praktikabel und akzeptiert** ist. Im nächsten Abschnitt gehen wir noch detaillierter auf die Balance mit dem Betriebsrat und Datenschutz ein – ein Aspekt, der während aller obigen Phasen mitbedacht werden sollte.

Mitbestimmung und Datenschutz: Erfolgsfaktor Betriebsrat

Die Einführung eines Überwachungssystems wie Insider Risk Management berührt in Deutschland unweigerlich Fragen des **Datenschutzes und der Mitbestimmung**. IT-Leiter und Datenschutzbeauftragte müssen eng mit dem **Betriebsrat** zusammenarbeiten, um das Vorhaben rechtskonform und transparent zu gestalten.

Dieser Abschnitt diskutiert typische Spannungsfelder und gibt Empfehlungen, wie man diese meistern kann, sodass am Ende sowohl die **Sicherheit** als auch die **Vertrauenswürdigkeit** der Lösung gewährleistet sind.

Betriebsrat und Zustimmungspflicht: Nach §87 Abs. 1 Nr. 6 BetrVG hat der Betriebsrat ein Mitbestimmungsrecht, wenn technische Einrichtungen eingeführt werden, die dazu bestimmt sind, das Verhalten oder die Leistung von Arbeitnehmern zu überwachen. Ein Tool wie Insider Risk Management fällt in der Regel unter diese Kategorie. Das bedeutet: Ohne **Zustimmung des Betriebsrats** (oder einer Einigungsstelle) darf das System nicht in Betrieb gehen. In der Praxis wird daher fast immer eine **Betriebsvereinbarung** abgeschlossen, die genau regelt, *welche Daten erfasst* und *wie sie verwendet* werden. IT-Entscheider sollten den Betriebsrat so früh wie möglich ins Boot holen – idealerweise schon in der Planungsphase, bevor Fakten geschaffen werden. Ein Ansatz kann sein, gemeinsam mit dem Betriebsrat eine Art **Richtlinienkatalog** auszuarbeiten: z. B. Festzulegen, dass nur bestimmte besonders schützenswerte Daten überwacht werden (Prinzip der Datensparsamkeit), dass private Nutzungen von z. B. E-Mail nach Möglichkeit ausgefiltert werden, etc. Oftmals besteht die Sorge des Betriebsrats, dass ein umfassendes Monitoring zu einem Klima der Bespitzelung führt. Hier kann man entgegenwirken, indem man in der Vereinbarung **Kontrollmechanismen** einbaut – etwa, dass die Identität eines Mitarbeiters nur bei konkretem Verdacht durch einen definierten Prozess aufgedeckt werden darf (was dem Standard in Purview entspricht, Stichwort Pseudonymisierung und Vier-Augen-Prinzip). Auch kann vereinbart werden, dass der Betriebsrat bei schwerwiegenden Fällen informiert wird oder im jährlichen Turnus Berichte über den Einsatz der Software erhält. Je nach Unternehmen kann auch eine **gemeinsame Kommission** (HR, Datenschutz, Betriebsrat) eingerichtet werden, die zweifelshafte Fälle prüft, um Willkür auszuschließen.

Datenschutz und rechtliche Rahmenbedingungen: Neben dem Betriebsverfassungsrecht sind die Vorgaben der DSGVO und des Bundesdatenschutzgesetzes (BDSG) zu beachten, insbesondere §26 BDSG, der den Umgang mit Beschäftigtendaten regelt. Wichtig ist eine **Rechtsgrundlage** für die Verarbeitung der Mitarbeiterdaten zu haben. Im Regelfall wird man sich auf *berechtigte Interessen des Arbeitgebers* (Art. 6 Abs. 1 lit. f DSGVO) in Verbindung mit §26 BDSG stützen, oder – falls eine Betriebsvereinbarung vorliegt – auf diese als normenkonkretisierende Maßnahme (Art. 88 DSGVO). Die berechtigten Interessen müssen sorgfältig abgewogen werden gegen die Persönlichkeitsrechte der Beschäftigten. Dokumentieren Sie diese Abwägung, idealerweise im Rahmen einer **Datenschutz-Folgenabschätzung (DSFA)**, da bei umfangreicher Verhaltensüberwachung i. d. R. ein hohes Risiko für Persönlichkeitsrechte

angenommen werden kann. In der DSFA sollte beschrieben werden, welche Risiken für die Rechte der Mitarbeiter bestehen (etwa Fehlalarme, Profilbildung) und welche **Maßnahmen zu deren Minderung** ergriffen werden (Pseudonymisierung, Zugriffsbeschränkungen, Transparenz, etc.).

Ein weiteres rechtliches Thema ist die **Zweckbindung**: Die erhobenen Daten (Protokolle, Alerts) dürfen nur für den vorgesehenen Zweck *Insider-Risikomanagement* genutzt werden. Es wäre unzulässig, mit denselben Überwachungsdaten z. B. Leistungskontrollen durchzuführen oder sie für völlig andere Disziplinarmaßnahmen zu verwenden, die nichts mit den definierten Sicherheits- und Compliance-Zielen zu tun haben. Eine klare Zweckbindung in der Betriebsvereinbarung schafft hier Sicherheit. Ebenso sollte geregelt sein, wie lange die Daten aufbewahrt werden (Stichwort Löschkonzept) – z. B. automatische Löschung von geschlossenen Fällen nach X Monaten, sofern keine weiteren Schritte (etwa gerichtliche Verfahren) anhängig sind.

Transparenzpflichten gegenüber Mitarbeitern: Auch ohne gesetzliche Pflicht empfiehlt es sich aus Compliance-Sicht, die Mitarbeiter **umfassend zu informieren**. Dies kann über die bereits erwähnte Mitarbeiterkommunikation im Rollout geschehen, sollte aber idealerweise auch schriftlich (im Intranet oder Mitarbeiterhandbuch) niedergelegt sein. Inhalte sollten sein: *Was* wird überwacht (z. B. "Dienstliche E-Mails auf bestimmte Schlagworte, Dateiaktionen auf Firmengeräten, etc.), *Wer* wertet es aus (nur speziell befugte Personen unter Wahrung der Anonymität bis zur Eskalation), *Warum* wird es gemacht (Schutz vor Datenabfluss, Erfüllung rechtlicher Pflichten wie z. B. Schutz personenbezogener Daten) und *Wie* die Mitarbeiterrechte gewahrt bleiben (z. B. Möglichkeit zur Stellungnahme im Verdachtsfall, Einbindung der Mitbestimmung). In manchen Fällen kann auch ein **Opt-out oder Opt-in** diskutiert werden – etwa, dass bestimmte private Verwendungen explizit ausgeschlossen sind. Allerdings ist dies bei Sicherheitsüberwachungen tricky; meist geht man den Weg, private Nutzung von Arbeitsmitteln generell zu untersagen oder klar abzugrenzen, damit das Monitoring datenschutzkonform bleibt.

Spannungsfeld Praxisbeispiele: Die zuvor geschilderten Beispiele zeigen bereits, wo Konflikte liegen können. Beispiel 3 mit der Kommunikationsüberwachung berührt direkt die **Grenze zur Persönlichkeitskontrolle**. Hier wäre in Deutschland besonders sensibel zu prüfen, ob und wie solche Kommunikation gescannt werden darf. In vielen Fällen werden Unternehmen vielleicht darauf verzichten oder nur sehr eingeschränkt (z. B. nur auf geschäftsbezogene Chats, nicht aber auf persönliche 1:1 Chats, und auch dort vielleicht nur auf bestimmte Keywords, nicht auf kompletten Inhalt). Der Betriebsrat wird hier sicher Mitspracherecht einfordern, um Mitarbeiter vor Überwachung ihrer persönlichen Kommunikation zu schützen. Ein guter Kompromiss

kann sein, **stufenweise Verfahren** zu vereinbaren: Erst bei konkreten Anhaltspunkten wird tiefer in Inhalte geschaut, ansonsten bleiben Verstöße auf einer abstrakten Ebene (z. B. "Verstoßtyp X wurde festgestellt" ohne sofort Namen und Wortlaut preiszugeben).

Rechtssichere Einführung – Handlungsempfehlungen: Aus den obigen Punkten lassen sich einige Best Practices ableiten:

- **Frühzeitige Einbindung des Betriebsrats:** Nicht erst präsentieren, wenn alles fertig ist, sondern möglichst gemeinsam gestalten. Transparenz und Kooperationsbereitschaft schaffen Vertrauen.
- **Klare Regelungen in einer Betriebsvereinbarung:** Hier alle wichtigen Punkte festhalten – Zweck, Umfang der Überwachung, Verfahren bei Alerts, Rechte der Arbeitnehmer, Datenschutzmaßnahmen, Beteiligung des BR, etc. Diese Vereinbarung von beiden Seiten unterschreiben lassen. Sie bietet Rechtssicherheit für beide Parteien.
- **Datenschutz-Prinzipien strikt einhalten:** Minimierung (nur notwendige Daten erfassen), Zweckbindung, Zugriffsbeschränkung, Transparenz, zeitnahe Löschung. Microsofts Tool-Unterstützung (Privacy by Design) kann man hier als Vorteil hervorheben – z. B. dass standardmäßig anonymisiert wird.
- **Schulungen und Awareness mit dem Betriebsrat zusammen:** Evtl. kann man gemeinsame Infoveranstaltungen von IT-Security und Betriebsrat anbieten, was signalisiert, dass hier kein Geheimbereich entsteht, sondern eine gemeinsame Initiative zum Wohle des Unternehmens und der Belegschaft.
- **Kontinuierliche Überprüfung:** Rechtliche Rahmenbedingungen ändern sich (Stichwort ePrivacy oder neue Gerichtsurteile zur Mitarbeiterüberwachung). Halten Sie daher Ihr Programm auch juristisch aktuell. Ziehen Sie den Datenschutzbeauftragten regelmäßig hinzu für Audits.

Letztlich sollte Insider Risk Management **nicht als Instrument der Misstrauenskultur** verstanden werden, sondern als notwendige Maßnahme in einer digitalen Arbeitswelt voller Risiken. Wenn Mitarbeiter verstehen, dass ihr Arbeitgeber sie nicht *persönlich* ausforscht, sondern alle gemeinsam vor Schaden schützen will – und dass ihre privaten Rechte respektiert bleiben – dann lässt sich das Spannungsfeld gut auflösen. In vielen Unternehmen hat sich gezeigt, dass nach anfänglicher Skepsis eine gewisse **Normalität** einkehrt: Die Belegschaft akzeptiert die Überwachung als „Hintergrundrauschen“ wie eine Alarmanlage – sie ist da, aber man spürt sie nicht im Alltag, solange man nichts falsch macht. Aufgabe der Führung ist es, dieses Gleichgewicht zu halten: maximale Sicherheit bei maximaler Achtung der Mitarbeiterrechte.

Fazit: Nutzenabwägung, Empfehlungen und strategischer Ausblick

Insider Risk Management in Microsoft 365 erweist sich als mächtiges Werkzeug, um der wachsenden Gefahr durch interne Sicherheitsvorfälle zu begegnen. Für **IT-Entscheider** und **Datenschutzbeauftragte** liegt der Reiz darin, eine *ganzheitliche Lösung* zu haben, die nahtlos in die vorhandene Microsoft 365-Umgebung integriert ist und sowohl **technische Schutzmaßnahmen** als auch **Compliance-Anforderungen** bedient. Die vorangegangenen Kapitel haben gezeigt, dass die Einführung zwar sorgfältige Planung und Abstimmung erfordert, aber einen hohen **Mehrwert** bietet:

Auf der **Nutzen**-Seite steht vor allem die **präventive Wirkung**. Viele Zwischenfälle können vereitelt werden, bevor ein tatsächlicher Schaden entsteht – sei es finanzieller Natur (etwa durch Abfluss von Geschäftsgeheimnissen an Konkurrenten) oder in Form von **Compliance-Verstößen**, die zu Strafen führen könnten. Die Möglichkeit, sowohl **vorsätzliche** als auch **fahrlässige** Handlungen zu erkennen, hilft dem Unternehmen, angemessen zu reagieren – vom disziplinarischen Durchgreifen in gravierenden Fällen bis zur Schulung und Sensibilisierung bei versehentlichen Fehlern. Darüber hinaus schafft das Programm eine **abschreckende Wirkung**: Mitarbeiter, die wissen, dass bestimmte Aktionen bemerkt werden könnten, lassen potenziell eher von einem Fehlverhalten ab. Dies trägt zu einer insgesamt höheren **Sicherheitskultur** im Unternehmen bei.

Natürlich gibt es auch **Herausforderungen** und eventuelle Nachteile. Die **Implementierungskosten** (Lizenzkosten für Microsoft 365 E5 Compliance, Zeitaufwand für Einrichtung und Betrieb, ggf. Personalstellen für Analysten) sind ein Faktor – doch diese müssen ins Verhältnis gesetzt werden zu den Kosten eines einzigen schweren Insider-Vorfalls, der leicht in die Millionen gehen kann. Ein kritischer Punkt ist zweifelsohne das Thema **Vertrauen und Privatsphäre**: Wenn das Programm schlecht kommuniziert oder überzogen eingesetzt wird, kann es die Moral der Mitarbeiter beeinträchtigen. Hier haben wir betont, dass *Transparenz und klare Grenzen* die Lösung sind, damit der Nutzen nicht von negativen kulturellen Folgen überschattet wird. Ein weiterer potenzieller Nachteil ist die Abhängigkeit von der Technologie: Ein *"False Negative"* (also ein übersehenes Risiko) könnte falsche Sicherheit wiegen. Daher sollte man nie allein auf das Tool vertrauen, sondern immer auch einen wachsamen Blick und **weitere Kontrollen** (wie ein Hinweisgebersystem oder manuelle Audits) im Mix behalten.

Handlungsempfehlungen: Für Organisationen, die Insider Risk Management in

Microsoft 365 einführen wollen, ergeben sich folgende konkrete Ratschläge:

- **1. Strategische Verankerung:** Stellen Sie sicher, dass das Vorhaben vom oberen Management unterstützt wird und in die übergeordnete **Security- und Compliance-Strategie** passt. Definieren Sie messbare Ziele (z. B. Reduktion von Datenlecks, Einhaltung bestimmter Standards wie ISO 27001 oder CMMC), an denen Sie den Erfolg des Programms später bewerten können.
- **2. Lizenz- und Kostenplanung:** Prüfen Sie frühzeitig die Lizenzoptionen. Gegebenenfalls kann ein **Microsoft 365 E5-Test** genutzt werden, um das Feature-Set zu evaluieren. Planen Sie auch die personellen Ressourcen – wer soll die Alerts bearbeiten, wer schult die Mitarbeiter etc. Hier lohnt es sich, vielleicht einen **Stufenplan** aufzustellen: Anfangs mit Teilzeitkräften im Team starten und je nach Alert-Volumen aufstocken.
- **3. Pilot und iteratives Vorgehen:** Beginnen Sie klein und iterativ. Nutzen Sie die Pilotphase, um **lernend** an die für Ihr Unternehmen optimalen Einstellungen zu kommen. Was in anderen Firmen ein Risiko ist, muss es bei Ihnen nicht sein und umgekehrt. Lassen Sie Raum, um Policies anzupassen und Prozesse zu optimieren, bevor Sie voll ausrollen.
- **4. Kommunikation & Training:** Investieren Sie in die **Bewusstseinsbildung** Ihrer Belegschaft. Machen Sie klar, dass Insider Risk Management kein "Überwachungsmonster", sondern eine zeitgemäße Schutzmaßnahme ist. Bieten Sie Schulungen an – z. B. „Do's and Don'ts" im Umgang mit sensiblen Daten – um proaktiv Fehlverhalten zu reduzieren. Je mehr Mitarbeiter die Sinnhaftigkeit verstehen, desto weniger werden Sie das Tool überhaupt „brauchen", weil gute Sicherheitsgewohnheiten gefördert werden.
- **5. Zusammenarbeit mit dem Datenschutz/Betriebsrat:** Pflegen Sie eine enge Partnerschaft mit dem Datenschutzbeauftragten und dem Betriebsrat. Sie sind nicht Gegner dieses Projekts, sondern wichtige **Partner, um die Balance** zu halten. Holen Sie regelmäßiges Feedback ein, auch nachdem das System live ist. Das schafft Akzeptanz und hilft, früh Gegensteuer zu geben, falls irgendwo der Schuh drückt (z. B. wenn Mitarbeiter Beschwerden äußern).
- **6. Technische Feineinstellungen:** Nutzen Sie die technischen Möglichkeiten voll aus: Aktivieren Sie **Signalreduzierung** (z. B. Duplikaterkennung, die Microsoft anbietet, um Wiederholungsalarme zu filtern), nutzen Sie *Ausnahmen* wo sinnvoll (um bekannte unkritische Vorgänge vom Alarm auszunehmen), und probieren Sie neue Features (wie Adaptive Protection) ruhig in kontrolliertem Rahmen aus, um einen Mehrwert zu erzielen. Bleiben Sie am Ball, was Updates betrifft – Microsoft veröffentlicht regelmäßige Verbesserungen, die oft auf Kundenfeedback basieren.

Ulrich B. Boddenberg · Robert-Götz-Str. 20 · D-44319 Dortmund
E-Mail: ulrich@boddenberg.de · www.boddenberg.de · Telefon: +49 231 222458 121 ·
IBAN: DE56 4405 0199 0001 3191 91 · Stadtsparkasse Dortmund (DORTDE33XXX)
Steuer-Nr.: 316/5026/1511 · USt.Id: DE232577137

Zum **strategischen Ausblick**: Insider Risk Management wird voraussichtlich an Bedeutung *weiter zunehmen*. In einer Arbeitswelt, die durch **Cloud, Remote Work und nun auch KI-Tools** immer dezentraler und dynamischer wird, steigen zwangsläufig die **Angriffs- und Risikoflächen im Inneren**. Unternehmen werden sich vermehrt fragen (müssen), wie sie ihre Daten nicht nur vor Hackern, sondern auch vor internen Schwachstellen schützen. Regulatorisch könnte mehr Druck entstehen – man denke an Sektoren wie das Finanzwesen, wo heute schon strenge Anforderungen an die Überwachung von Mitarbeiterkommunikation bestehen, oder an neue Regularien, die den Schutz von Geschäftsgeheimnissen forcieren. Microsoft Purview Insider Risk Management ist in diesem Umfeld gut positioniert, zumal Microsoft die Integration von **künstlicher Intelligenz** aggressiv vorantreibt. In Zukunft könnten wir noch **intelligentere Systeme** sehen, die kontextbasiert Entscheidungen treffen, wann ein Vorfall eskaliert oder sogar automatisch verhindert wird (etwa indem verdächtige Aktionen in Echtzeit blockiert werden, bevor Schaden entsteht). Auch eine engere Verzahnung mit **präventiven Schulungsmaßnahmen** ist denkbar – beispielsweise, dass das System Nutzern bei kleineren Verstößen interaktiv Hinweise gibt (eine Art „Coach“ für datenbewusstes Verhalten).

Alles in allem bietet Insider Risk Management in Microsoft 365 Unternehmen die Chance, **Unsichtbares sichtbar** zu machen – nämlich Risiken, die im Verborgenen lauern. Richtig eingesetzt, lassen sich damit nicht nur Datenverluste und Compliance-Verstöße reduzieren, sondern auch eine Unternehmenskultur fördern, die auf **Sicherheit und Vertrauen** basiert. Die Nutzenabwägung fällt in den meisten Fällen positiv aus, solange man die Technik **verantwortungsvoll und mit Augenmaß** einsetzt. Mit klaren Spielregeln, Kooperation aller Beteiligten und Offenheit für neue Technologien können IT-Leiter und Datenschutzbeauftragte so eine robuste *letzte Verteidigungslinie* im Sicherheitskonzept ihres Unternehmens einziehen – zum Schutz von Unternehmenswerten **und** Mitarbeiterinteressen gleichermaßen.

Ulrich B. Boddenberg · Robert-Götz-Str. 20 · D-44319 Dortmund
E-Mail: ulrich@boddenberg.de · www.boddenberg.de · Telefon: +49 231 222458 121 ·
IBAN: DE56 4405 0199 0001 3191 91 · Stadtsparkasse Dortmund (DORTDE33XXX)
Steuer-Nr.: 316/5026/1511 · USt.Id: DE232577137