Microsoft 365 Audit-Log und Rechnungsprüfung: Nachweise, die Verwaltungen liefern müssen

Es gibt einen Moment, den jede IT-Leitung in der öffentlichen Verwaltung kennt. Das Rechnungsprüfungsamt kündigt eine Prüfung des Bereichs „IT-Beschaffung und IT-Betrieb“ an, und in der Anlage steht ein Satz, der harmlos aussieht: „Bitte legen Sie geeignete Nachweise vor.“ Sieben Wörter. Danach beginnt in vielen Häusern eine Woche, in der drei Personen im Admin Center herumklicken, CSV-Dateien exportieren, die niemand erklären kann, und am Ende ein Dokument entsteht, das mehr Fragen aufwirft als beantwortet.

Das Bittere daran: Die Daten waren fast immer da. Microsoft 365 protokolliert sehr viel – wer eine Datei geteilt hat, wer sich von wo angemeldet hat, wer eine Rolle zugewiesen bekam, wer eine Aufbewahrungsrichtlinie geändert hat. Das Problem ist nicht die Menge. Das Problem ist, dass die Protokolle nach einer technischen Logik aufbewahrt werden und Nachweise nach einer verwaltungsrechtlichen gefordert werden, und dass diese beiden Logiken sich nur zufällig überschneiden. Ein Protokolleintrag verfällt nach 180 Tagen. Eine Prüfung findet zwei Jahre später statt. Sie sehen das Problem.

Und es gibt eine zweite Falle, die deutlich unangenehmer ist als eine Prüffeststellung: Wer anfängt, Protokolldaten auszuwerten, um Nachweise zu erzeugen, bewegt sich mit jedem Klick näher an eine Leistungs- und Verhaltenskontrolle heran. Der Personalrat hat das im Blick, und er hat recht damit. Dieser Beitrag gehört zur Reihe Microsoft 365 in der öffentlichen Verwaltung und beschreibt, wie Sie die Nachweise erzeugen, die Rechnungsprüfungsamt, Datenschutzaufsicht und Personalrat tatsächlich erwarten – und wie Sie dabei die Grenze einhalten, an der die Auswertung aufhören muss.

Vorab eine Klarstellung zum Umfang: Dies ist keine Rechtsberatung. Fristen, Wertgrenzen und Zuständigkeiten unterscheiden sich zwischen den Ländern erheblich, und die kirchlichen Träger arbeiten ohnehin nach eigenem Recht. Alles, was hier zu Fristen und Paragraphen steht, ist Orientierung. Maßgeblich ist Ihr Landesrecht, Ihre Gemeindeordnung, Ihre Prüfungsordnung und im Zweifel die Auskunft Ihres Rechtsamts.

Fakten: Die drei Zahlen, die alles andere bestimmen

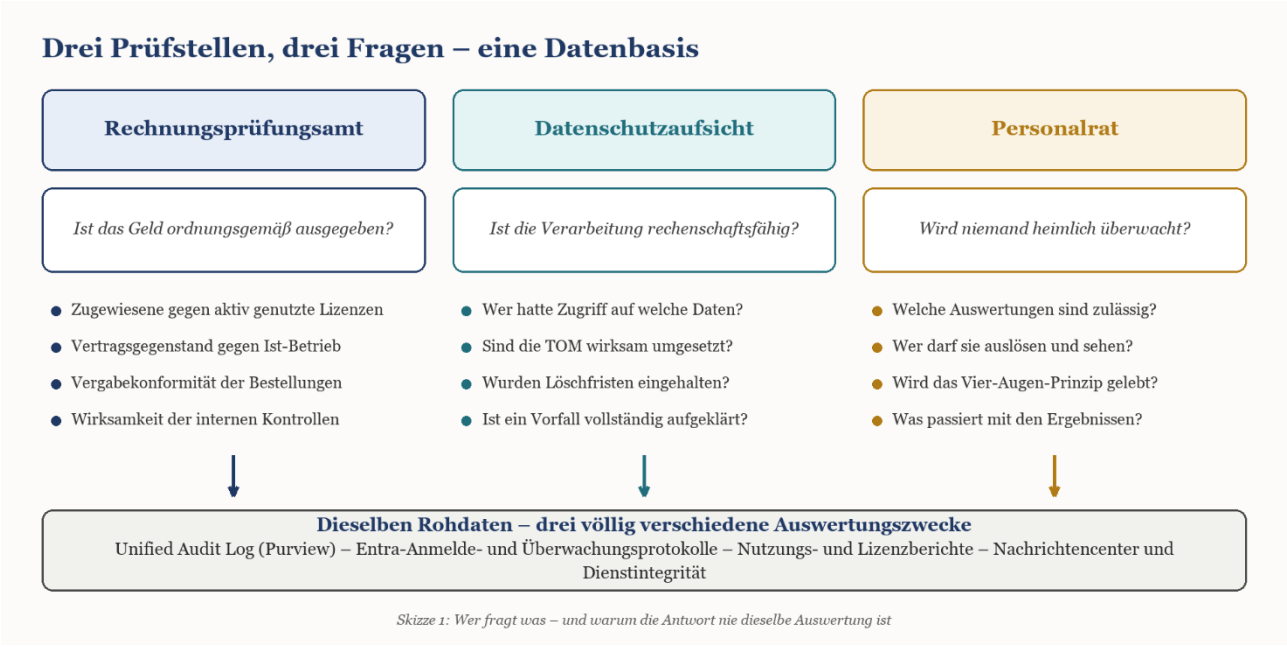
Purview Audit (Standard) hält Auditdatensätze standardmäßig 180 Tage vor. Das ist seit dem 17. Oktober 2023 so; ältere Datensätze wurden nur 90 Tage aufbewahrt.

Die Anmelde- und Überwachungsprotokolle in Microsoft Entra ID sind davon völlig unabhängig: sieben Tage in der kostenlosen Edition, 30 Tage mit Entra ID P1 oder P2.

Keine dieser Aufbewahrungen wirkt rückwirkend. Wer im März eine Lizenz nachkauft oder eine Aufbewahrungsrichtlinie anlegt, bekommt die Daten vom Januar nicht zurück. Nie.

Drei Prüfstellen, drei Fragen – und nur eine Datenbasis

Der häufigste Fehler in der Vorbereitung ist die Annahme, es gebe so etwas wie „den Nachweis“. Den gibt es nicht. Es gibt drei Instanzen, die alle in dieselben Systeme schauen wollen, aber völlig verschiedene Fragen stellen. Wer das nicht sauber trennt, liefert der einen Stelle zu wenig und der anderen zu viel – und die Variante „zu viel“ ist die gefährlichere.



Skizze 1: Wer fragt was – und warum die Antwort nie dieselbe Auswertung ist

Was das Rechnungsprüfungsamt wissen will

Das Rechnungsprüfungsamt interessiert sich nicht für Ihre Tenant-Architektur. Es interessiert sich dafür, ob öffentliche Mittel ordnungsgemäß, wirtschaftlich und sparsam eingesetzt wurden und ob die internen Kontrollen funktionieren. Übersetzt in Microsoft-365-Sprache heißt das: Stimmt die Zahl der bezahlten Lizenzen mit der Zahl der tatsächlich genutzten überein? Ist das, was im Vertrag steht, auch das, was betrieben wird? Wurde die Beschaffung vergaberechtlich korrekt abgewickelt? Und gibt es ein nachvollziehbares Verfahren dafür, wer im System was darf?

Die letzte Frage wird gern unterschätzt. Ein Prüfer, der feststellt, dass in einer Stadtverwaltung mit 900 Beschäftigten elf Konten dauerhaft globale Administratorrechte haben, schreibt das auf. Nicht weil das ein Datenschutzproblem wäre – das ist es auch –, sondern weil es ein Problem der internen Kontrolle ist. Wer alles darf, kann auch alles vertuschen, und damit ist die Trennung von Anordnung und Ausführung, die in der Haushaltswirtschaft heilig ist, in der IT nicht abgebildet.

Was die Datenschutzaufsicht wissen will

Die Aufsichtsbehörde fragt nach Rechenschaft. Die Datenschutz-Grundverordnung verlangt nicht nur, dass Sie rechtmäßig verarbeiten, sondern dass Sie es nachweisen können. In der Praxis heißt das: Das Verzeichnis von Verarbeitungstätigkeiten muss zum tatsächlichen Systemzustand passen, die technischen und organisatorischen Maßnahmen müssen belegbar wirksam sein, und wenn etwas schiefgeht, müssen Sie innerhalb von 72 Stunden erklären können, was passiert ist.

Genau an dieser Stelle wird das Auditprotokoll zum Rettungsanker. Ein großer Landschaftsverband hatte den Fall, dass eine Beschäftigte versehentlich eine Freigabe auf eine Bibliothek mit Leistungsakten gesetzt hatte. Die Frage der Aufsicht war nicht „wie konnte das passieren“, sondern „wer hat in den 14 Tagen bis zur Entdeckung tatsächlich zugegriffen“. Ohne Auditprotokoll ist die ehrliche Antwort „das wissen wir nicht“, und diese Antwort führt regelmäßig dazu, dass sicherheitshalber alle Betroffenen benachrichtigt werden müssen. Mit Auditprotokoll war die Antwort: drei Zugriffe, alle aus dem eigenen Fachamt, kein Datenabfluss. Der Unterschied zwischen diesen beiden Antworten beträgt in Personentagen ungefähr das Vierzigfache.

Was der Personalrat wissen will

Der Personalrat stellt die unbequemste Frage, und er stellt sie zu Recht: Was genau kann diese Software über einzelne Beschäftigte herausfinden, und wer darf davon Gebrauch machen? Microsoft 365 ist unstreitig eine technische Einrichtung, die zur Überwachung von Leistung und

Verhalten geeignet ist – nicht weil sie dafür gebaut wäre, sondern weil sie es nebenbei kann. Damit greift in praktisch allen Ländern die Mitbestimmung, und damit brauchen Sie eine Dienstvereinbarung.

Der wichtige Punkt für die Nachweisführung: Eine gute Dienstvereinbarung verbietet nicht die Protokollierung. Sie regelt die Auswertung. Das ist ein großer Unterschied, und er wird in Verhandlungen oft verwischt. Ein Protokoll, das niemand ohne definiertes Verfahren öffnen darf, ist keine Überwachung. Ein Protokoll, in dem die IT jederzeit „mal eben schauen“ kann, ist eine.

Wichtig: Die Reihenfolge entscheidet über den Frieden im Haus

Wer die Dienstvereinbarung erst schreibt, nachdem die erste Auswertung stattgefunden hat, verhandelt aus einer denkbar schlechten Position. Der Personalrat wird dann nicht über Verfahren reden wollen, sondern über Vertrauen. Bausteine für die Vereinbarung stehen im Beitrag zur Dienstvereinbarung in dieser Reihe; die Nachweisregeln aus diesem Artikel gehören als eigener Abschnitt hinein.

Die Nachweisquellen im Tenant – und was sie wirklich hergeben

Microsoft 365 hat nicht ein Protokoll, sondern mindestens vier voneinander unabhängige Datentöpfe mit unterschiedlichen Aufbewahrungsfristen, unterschiedlichen Berechtigungen und unterschiedlicher Aussagekraft. Wer sie verwechselt, produziert Nachweise, die einer Nachfrage nicht standhalten.

Das einheitliche Auditprotokoll in Purview

Das Unified Audit Log ist die zentrale Quelle. Es sammelt Aktivitäten aus Exchange Online, SharePoint, OneDrive, Teams, Entra ID, Power Platform und weiteren Diensten in einem gemeinsamen Datenbestand. Zugriff bekommt nur, wer in Purview der Rollengruppe „Audit Manager“ oder „Audit Reader“ zugeordnet ist – und diese Zuordnung ist selbst einer der Nachweise, die Sie vorlegen werden. Der Unterschied: Audit Reader darf suchen und exportieren, Audit Manager darf zusätzlich die Auditkonfiguration ändern. In einer Verwaltung sollten das getrennte Personen sein.

Bei der Aufbewahrung wird es interessant. Audit (Standard) hält 180 Tage vor. Audit (Premium) hält Datensätze aus Exchange Online, SharePoint, OneDrive und Entra ID ein Jahr lang vor – aber nur für Benutzerkonten, die tatsächlich eine E5-Lizenz oder eine entsprechende Add-on-Lizenz tragen. Für alle anderen, einschließlich Gastkonten, bleibt es bei 180 Tagen. In einem gemischten Verwaltungstenant mit E3 für die Verwaltung, F3 für den Bauhof und E5 nur für die IT bedeutet das: Ihre Aufbewahrung ist nicht einheitlich, sondern personenabhängig. Das erklärt man einem Prüfer besser vorher als hinterher.

Darüber hinaus lassen sich eigene Aufbewahrungsrichtlinien für Auditdaten anlegen: bis zu 50 Stück, mit Dauern von sieben Tagen bis zu zehn Jahren, jeweils mit einer Prioritätszahl zwischen 1 und 10000, wobei jede eigene Richtlinie die Standardrichtlinie übersteuert. Zum Anlegen braucht es die Rolle „Organisationskonfiguration“. Die langen Dauern von drei, fünf, sieben und zehn Jahren setzen die Zehn-Jahres-Add-on-Lizenz zusätzlich zu E5 voraus – ein Kostenfaktor, der in die Lizenzbetrachtung gehört und nicht im Nachgang als Überraschung auftauchen sollte.

Entra-Berichte: Anmeldungen, Überwachung, Rollen

Hier lauert der häufigste Irrtum der Praxis: Die Entra-Protokolle sind nicht Teil des einheitlichen Auditprotokolls und werden von den Purview-Aufbewahrungsrichtlinien nicht erfasst. Sie folgen ihrer eigenen Lizenzlogik. Anmelde- und Überwachungsprotokolle: sieben Tage kostenlos, 30 Tage

mit P1 oder P2. Die Nutzungsdaten zur Multifaktor-Authentifizierung: 30 Tage in allen Editionen. Riskante Anmeldungen: sieben, 30 oder 90 Tage je nach Edition, wobei riskante Benutzerkonten ohne festes Limit geführt werden, solange das Risiko nicht bereinigt ist. Microsoft-Graph-Aktivitätsprotokolle gibt es überhaupt nur mit P1 oder P2 und nur dann, wenn Sie sie aktiv exportieren – sonst werden sie schlicht nicht aufbewahrt.

Wer länger aufbewahren will, muss die Protokolle über Diagnoseeinstellungen in ein Speicherkonto oder einen Log-Analytics-Arbeitsbereich ausleiten. Das ist eine bewusste Entscheidung mit Kosten, mit einem eigenen Auftragsverarbeitungsbezug und mit einem eigenen Eintrag im Verarbeitungsverzeichnis. Es ist aber auch die einzige Methode, mit der Sie einem Prüfer im Jahr 2029 zeigen können, wer sich 2026 an einem bestimmten Tag angemeldet hat. Und weil es die einzige ist: Diese Entscheidung gehört in die Einführungskonzeption, nicht in das Krisenmanagement.

Nutzungsberichte im Admin Center – der heikelste Topf

Die Nutzungsberichte im Microsoft 365 Admin Center sind für die Kämmerei attraktiv: Sie zeigen, wie viele Konten Teams, Exchange, SharePoint und OneDrive tatsächlich benutzen. Genau das will das Rechnungsprüfungsamt für die Wirtschaftlichkeitsbetrachtung sehen. Genau das ist aber auch der Bericht, der auf Knopfdruck personenbezogen wird.

Microsoft hat hier vorgesorgt: Seit dem 1. September 2021 sind Benutzer-, Gruppen- und Websitenamen in allen Nutzungsberichten standardmäßig verborgen und werden durch systemgenerierte Werte ersetzt. Die Einstellung findet sich unter Einstellungen, Organisationseinstellungen, Dienste, Berichte und wirkt zugleich auf die Berichte in Microsoft Graph, in Power BI und im Teams Admin Center. Wer die Verschleierung abschaltet, löst damit selbst ein Ereignis aus, das im Auditprotokoll landet. Das ist kein Zufall, sondern Absicht – und es ist genau der Nachweis, den ein Personalrat sehen will.

Warnung: Auswertungsverbote der Dienstvereinbarung

Die folgenden Auswertungen sind in einer typischen Dienstvereinbarung ausdrücklich ausgeschlossen – und sie sind technisch alle in wenigen Minuten machbar. Genau deshalb muss die organisatorische Sperre sitzen:

– Ranglisten oder Auswertungen der Teams-, Chat- oder Anrufaktivität einzelner Personen oder kleiner Organisationseinheiten.

– Auswertung von Anmeldezeiten als Ersatz oder Kontrolle der Zeiterfassung, einschließlich „Wer war am Montag um 7 Uhr online“.

– Standortauswertungen aus IP-Adressen oder Gerätekennungen zur Kontrolle von Homeoffice oder mobilem Arbeiten.

– Auswertung von Lese- und Bearbeitungsvorgängen an Dokumenten zur Bewertung von Arbeitsmenge oder Arbeitstempo.

– Auswertung der Kommunikationsbeziehungen einzelner Personen, insbesondere zu Personalrat, Schwerbehindertenvertretung, Gleichstellungsstelle und Betriebsarzt.

– Deanonymisierung der Nutzungsberichte ohne dokumentierten Anlass und Freigabe.

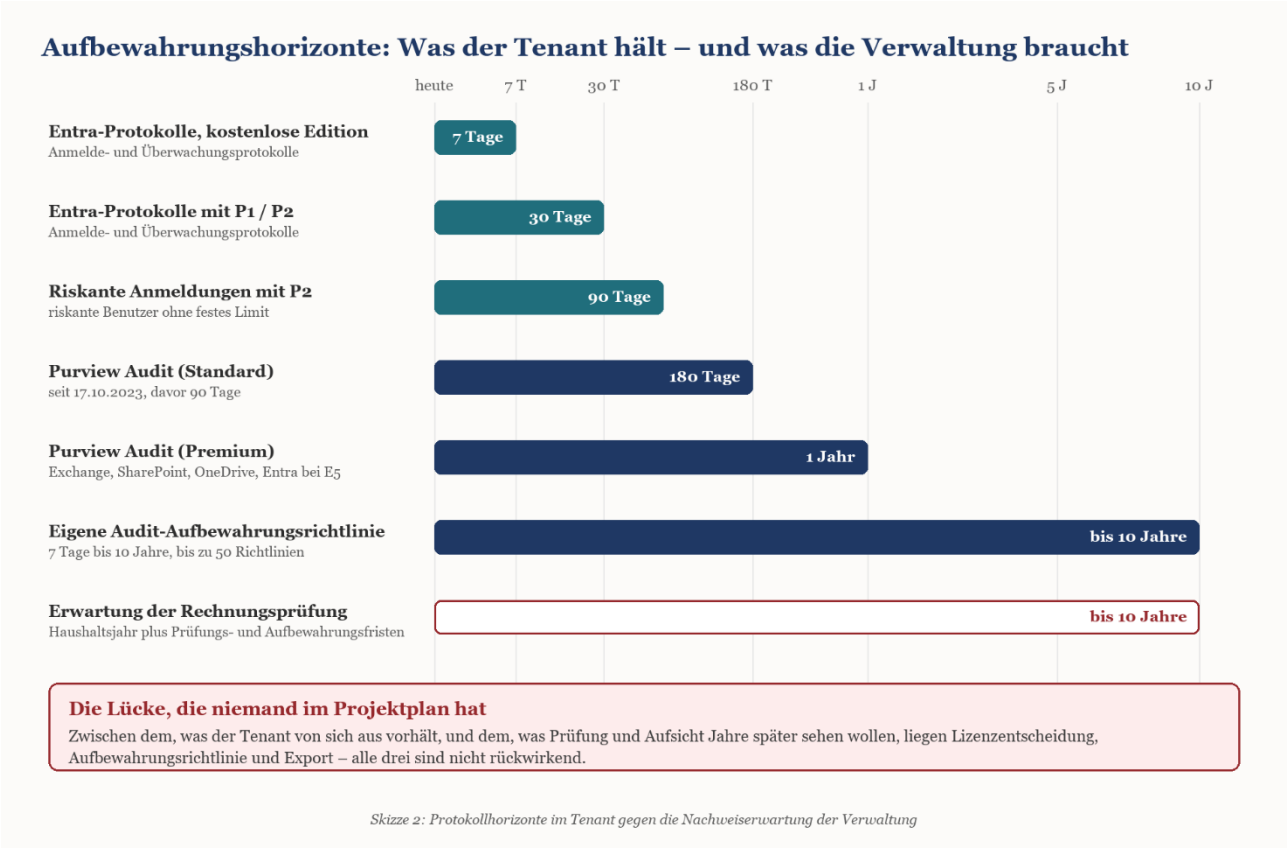
Praktischer Zusatz: Nehmen Sie in die Vereinbarung auf, dass ein Verstoß gegen diese Liste durch die IT selbst ein meldepflichtiger Vorgang ist. Das entlastet die Beschäftigten in der IT-Abteilung, weil sie sich dann auf eine Regel berufen können, statt auf ihr Standing.

Die Nachweistabelle: Was Sie liefern, woher es kommt, wie lange es lebt

Die folgende Tabelle ist der Kern dieses Beitrags. Sie ist bewusst so gehalten, dass Sie sie als Anlage zu einer Beschlussvorlage oder als Anhang zur Dienstvereinbarung verwenden können. Die Spalte

„Aufbewahrung“ nennt jeweils den Standardfall; die letzte Spalte sagt, was Sie tun müssen, wenn Sie länger brauchen.

Nachweis	Quelle im Tenant	Aufbewahrung im Standard	Wenn Sie länger brauchen
Wer hat auf eine Datei oder Bibliothek zugegriffen	Unified Audit Log, SharePoint- und OneDrive-Datensätze	180 Tage; 1 Jahr mit Audit (Premium) bei E5-lizenziertem Konto	Eigene Audit-Aufbewahrungsrichtlinie, für mehr als 1 Jahr Add-on nötig
Wer hat ein Postfach geöffnet oder E-Mails gelesen	Unified Audit Log, Aktion MailItemsAccessed	Standardmäßig aktiv bei E3 und E5; Aufbewahrung wie oben	Nur über Audit-Aufbewahrungsrichtlinie oder Export
Wer hat sich wann von wo angemeldet	Entra-Anmeldeprotokolle	7 Tage kostenlos, 30 Tage mit P1 oder P2	Diagnoseeinstellung in Speicherkonto oder Log Analytics
Wer hat Rollen, Gruppen oder Richtlinien geändert	Entra-Überwachungsprotokolle und Unified Audit Log	30 Tage in Entra; im Auditprotokoll 180 Tage	Export beider Quellen, sonst entstehen Lücken
Wer hatte zum Stichtag welche privilegierte Rolle	Entra-Rollenzuweisungen, PIM-Aktivierungsverlauf	Zuweisung ist Momentaufnahme, Verlauf zeitlich begrenzt	Stichtagsexport als eigenes Dokument zur Akte
Berechtigungen wurden regelmäßig überprüft	Zugriffsüberprüfungen in Entra ID Governance	Ergebnisverlauf in der Governance-Lösung	Ergebnis als PDF zur Akte, Lizenz Governance oder Entra Suite nötig
Aufbewahrungs- und Löschfristen wurden umgesetzt	Purview-Aufbewahrungsrichtlinien und -bezeichnungen	Konfiguration dauerhaft, Auswertung punktuell	Regelmäßiger Konfigurationsexport mit Datum
Unterlagen wurden ordnungsgemäß ausgesondert	Dispositionsverfahren in Purview, Vernichtungsnachweis	Nachweis dauerhaft, sofern erzeugt und abgelegt	Nachweis gehört in die Akte, nicht in den Tenant
Daten waren wiederherstellbar	Protokoll des Wiederherstellungstests, Sicherungslösung	Nur so lange, wie Sie das Protokoll aufbewahren	Testprotokoll als Verwaltungsvorgang führen
Der Dienst war verfügbar	Dienstintegrität und Nachrichtencenter im Admin Center	Historie im Portal zeitlich begrenzt	Monatlicher Export oder eigene Verfügbarkeitsdokumentation
Lizenzen wurden wirtschaftlich eingesetzt	Lizenzübersicht und Nutzungsberichte im Admin Center	Nutzungsberichte je nach Bericht 7 bis 180 Tage	Quartalsweiser anonymisierter Export als Anlage
Beschäftigte wurden geschult und unterwiesen	Schulungsdokumentation, nicht der Tenant	Nach Ihren eigenen Regelungen	Teilnahmelisten und Unterweisungsnachweise zur Personalakte



Skizze 2: Protokollhorizonte im Tenant gegen die Nachweiserwartung der Verwaltung

Tipp: Der Test, der zehn Minuten dauert und viel Peinlichkeit erspart

Nehmen Sie sich einen beliebigen Tag vor, der 200 Tage zurückliegt, und versuchen Sie, für diesen Tag drei Dinge zu belegen: eine Dateifreigabe nach außen, eine Anmeldung eines bestimmten Kontos und eine Änderung an einer Berechtigungsgruppe. Wenn Sie nach zehn Minuten nichts in der Hand haben, wissen Sie jetzt, wie Ihre Nachweislage aussieht – und zwar zu einem Zeitpunkt, an dem Sie noch etwas daran ändern können.

Technische Vertiefung zu den hier genannten Quellen

- Aufbewahrung und Aussonderung mit Purview: Fristen, Disposition, Vernichtungsnachweis
- Privilegierte Konten in der Verwaltungs-IT: Rollen, PIM und der Fall des einen Admins
- Microsoft 365 Lizenzen für Verwaltungen: E3, E5, F3 und die Behördenkonditionen

Die Dienstvereinbarung als Auswertungsgrenze

Technisch können Sie fast alles. Genau deshalb muss organisatorisch fast alles verboten sein. Eine Dienstvereinbarung, die nur festhält, dass „eine Leistungs- und Verhaltenskontrolle nicht stattfindet“, ist eine Absichtserklärung, kein Verfahren. Sie hilft weder dem Personalrat noch der IT, und im Konfliktfall hilft sie überhaupt niemandem.

Was tatsächlich in die Vereinbarung gehört

Brauchbar wird eine Vereinbarung, wenn sie vier Dinge abschließend regelt. Erstens: eine Positivliste zulässiger Auswertungszwecke. Zweitens: wer eine Auswertung beantragen darf und wer sie freigibt. Drittens: wie ausgewertet wird, also das Vier-Augen-Prinzip mit namentlicher Dokumentation. Viertens: was mit dem Ergebnis und mit den Rohdaten geschieht, einschließlich einer eigenen Löschfrist für den Auswertungsdatensatz.

Die Positivliste ist der Teil, um den am längsten gerungen wird, und sie ist kürzer, als die IT anfangs glaubt. Realistisch tragen: die Aufklärung eines konkreten Sicherheitsvorfalls, die Erfüllung einer gesetzlichen Auskunfts- oder Meldepflicht, die Störungsbeseitigung im technischen Sinn, die Erfüllung eines Auskunftsanspruchs nach Artikel 15 der Datenschutz-Grundverordnung und die Vorlage von Nachweisen gegenüber Rechnungsprüfung und Aufsicht in aggregierter, nicht personenbezogener Form. Alles andere braucht einen sehr guten Grund und den ausdrücklichen Beschluss des Gremiums.

Das Vier-Augen-Verfahren technisch abbilden

Ein Vier-Augen-Prinzip, das nur auf dem Papier steht, ist ein Ehrenwort. Abbilden lässt es sich mit Bordmitteln: Die Berechtigung zur Auditsuche wird nicht dauerhaft vergeben, sondern über Privileged Identity Management zeitlich befristet und mit Genehmigung aktiviert. Die Aktivierung erzeugt einen eigenen Protokolleintrag mit Begründung. Damit haben Sie dokumentiert, wer wann warum in das Protokoll schauen durfte – und das ist der Nachweis, mit dem Sie vor den Personalrat treten können, ohne ins Schwitzen zu kommen.

Der zweite Baustein ist die Trennung der Rollen: Die Person, die die Auditkonfiguration ändern darf, ist nicht dieselbe, die auswertet. In kleinen Häusern mit drei IT-Kräften ist das eine echte Zumutung, und sie lässt sich nur lösen, indem eine Rolle nach außen gegeben wird – an das kommunale Rechenzentrum, an das Systemhaus oder an eine benachbarte Verwaltung im Rahmen einer Amtshilfe. Das ist kein Makel, sondern die einzige ehrliche Antwort auf eine Personaldecke, die eine vollständige Funktionstrennung nicht hergibt. Wichtig ist nur, dass die Konstruktion dokumentiert und vertraglich abgesichert ist.

Skizze 3: Auswertungsverfahren mit Rollentrennung, wie es in eine Dienstvereinbarung gehört

Wenn Auswertung zulässig ist – und wenn nicht

Die folgende Tabelle beantwortet die Frage, die in der Praxis am häufigsten gestellt wird: „Dürfen wir jetzt reinschauen oder nicht?“ Sie ersetzt keine Vereinbarung, aber sie sortiert die typischen Anlässe so, dass die Diskussion im Arbeitskreis nicht bei null beginnt.

Anlass	Auswertung zulässig?	Verfahren

Verdacht auf kompromittiertes Konto	Ja, personenbezogen und sofort	Sicherheitsvorfall, Dokumentation nachziehen, Personalrat informieren
Aufsichtsanfrage nach einem Datenschutzvorfall	Ja, im Umfang der Anfrage	Antrag, Freigabe durch Datenschutzbeauftragte Person, Vier-Augen-Auswertung
Auskunftsanspruch einer betroffenen Person	Ja, beschränkt auf diese Person	Standardverfahren des Datenschutzes, Auswertung protokollieren
Rechnungsprüfung fragt nach Lizenzauslastung	Ja, aber nur aggregiert	Anonymisierte Nutzungsberichte, keine Deanonymisierung
Amtsleitung fragt nach Teams-Nutzung eines Amtes	Nur oberhalb einer Mindestgruppengröße	Schwellenwert in der Vereinbarung festlegen, üblich sind fünf bis zehn Personen
Verdacht auf Arbeitszeitverstoß	Nein	Anmeldedaten sind kein Zeiterfassungsersatz, Weg über das Personalamt
Vorgesetzte Person will Aktivität eines Kontos sehen	Nein	Kein zulässiger Zweck ohne konkreten dokumentierten Verdacht
Störungsanalyse, etwa Synchronisierungsfehler	Ja, technisch begrenzt	Nur technische Felder, kein Inhaltsbezug, Ticketnummer als Anlass
Ermittlungsersuchen einer Strafverfolgungsbehörde	Nur auf Rechtsgrundlage	Über Rechtsamt, niemals direkt aus der IT heraus beantworten

Warnung: Die Auswertung, die selbst zum Vorfall wird

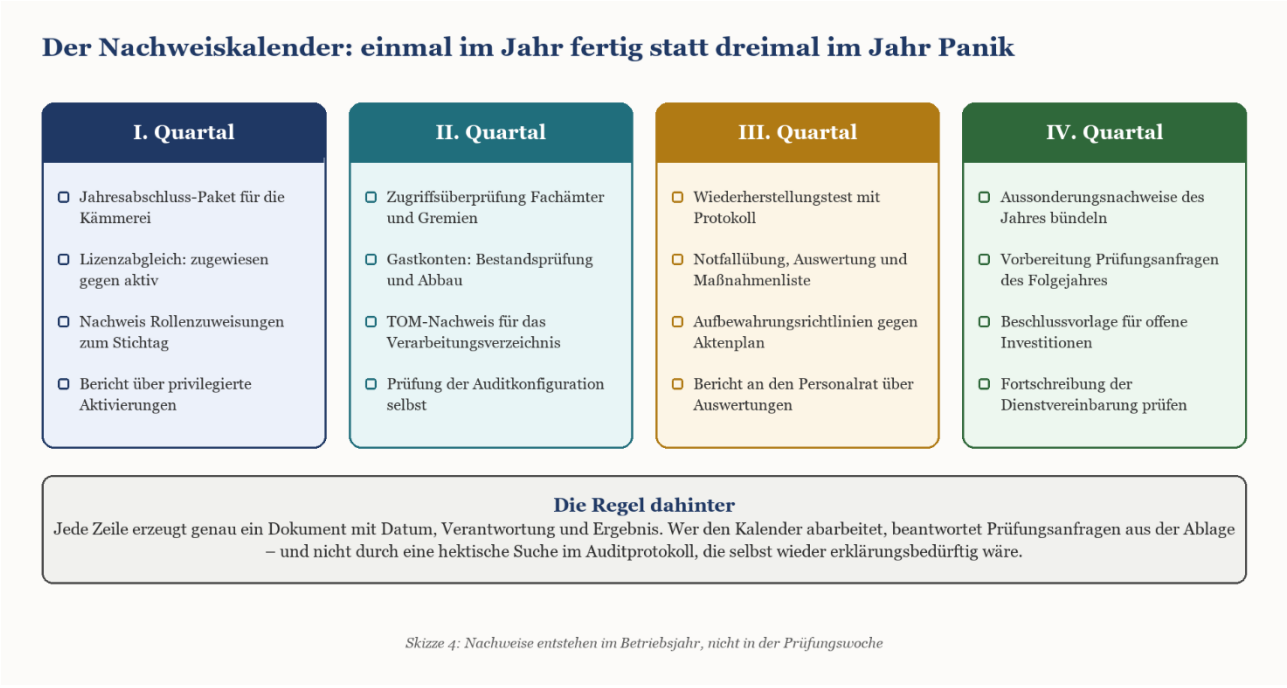
Eine Suche im Auditprotokoll ist eine Verarbeitung personenbezogener Daten. Wenn sie ohne zulässigen Zweck erfolgt, ist sie ein Datenschutzverstoß – und zwar einer, der bestens dokumentiert ist, weil das System die Suche selbst protokolliert. Der Satz „ich habe nur kurz nachgesehen“ ist damit forensisch nachweisbar und im Zweifel dienstrechtlich relevant. Sagen Sie das Ihrem Team lieber einmal zu deutlich als einmal zu wenig.

Nachweise erzeugen, ohne in Panik zu geraten

Der eigentliche Trick liegt nicht in der Auditsuche. Er liegt darin, Nachweise als Nebenprodukt des normalen Betriebs entstehen zu lassen. Wer einmal im Jahr einen definierten Satz von Dokumenten erzeugt, ablegt und mit Datum versieht, muss im Prüfungsfall nichts suchen. Er muss nur die Akte aufschlagen.

Der Nachweiskalender

Die folgende Aufteilung hat sich in mehreren Häusern bewährt. Sie ist bewusst so gelegt, dass die aufwendigen Punkte nicht mit dem Jahresabschluss kollidieren und dass der Wiederherstellungstest in die ruhigere Sommerphase fällt.



Skizze 4: Nachweise entstehen im Betriebsjahr, nicht in der Prüfungswoche

Der Aufwand dafür ist überschaubar. In einer Stadtverwaltung mit rund 1.000 Rufnummern und entsprechend großem Tenant liegt der Jahresaufwand für den kompletten Kalender bei geschätzt zwölf bis achtzehn Personentagen, verteilt über vier Quartale und mehrere Schultern. Zum Vergleich: Eine unvorbereitete Prüfung mit anschließender Stellungnahme zu Prüffeststellungen kostet erfahrungsgemäß mehr – und sie kostet es unter Zeitdruck, was den unangenehmeren Teil ausmacht.

Was die Kämmerei wirklich braucht

Für die Kämmerei und das Rechnungsprüfungsamt reduziert sich das Ganze meist auf drei Fragen. Erstens: Wie viele Lizenzen sind beschafft, wie viele zugewiesen, wie viele aktiv genutzt? Die Differenz zwischen zugewiesen und aktiv ist die Kennzahl, um die es geht. Zweitens: Passt der Lizenzmix zur tatsächlichen Aufgabenstruktur, oder trägt der Bauhof E3-Lizenzen, weil das bei der Beschaffung einfacher war? Drittens: Sind die Vertragsverlängerungen rechtzeitig und vergabekonform vorbereitet?

Eine Anmerkung zur Aussagekraft der Nutzungszahlen, die man einem Prüfer besser mitgibt: „Aktiv“ heißt in den Berichten, dass innerhalb des Betrachtungszeitraums mindestens eine Aktivität stattgefunden hat. Ein Konto, das einmal im Monat eine E-Mail liest, ist genauso „aktiv“ wie eines, das täglich acht Stunden in Teams verbringt. Wer aus diesen Zahlen eine Wirtschaftlichkeitsaussage ableitet, muss diesen Vorbehalt dazuschreiben. Tut er es nicht, wird ihn der nächste Prüfbericht daran erinnern.

Fakten: Was Sie über Ihre eigenen Auditeinstellungen wissen sollten

Nicht jede Aktivität wird ohne Zutun protokolliert. Die Postfachaktion MailItemsAccessed ist bei E3- und E5-lizenzierten Konten standardmäßig aktiv, die Protokollierung von Suchvorgängen in Exchange Online über SearchQueryInitiatedExchange dagegen muss ausdrücklich eingeschaltet werden.

Beim Export gilt: Aus einer einzelnen Auditsuche lassen sich maximal 50.000 Einträge als CSV-Datei herunterladen, und je Konto können bis zu zehn Suchaufträge gleichzeitig laufen, davon einer ohne Filter. Wer größere Mengen braucht, arbeitet über die Audit-Search-API in Microsoft Graph, die gegenüber dem klassischen PowerShell-Cmdlet die verlässlichere Vollständigkeit liefert.

Der Status Ihrer Auditkonfiguration ist selbst ein Nachweis. Exportieren Sie ihn einmal im Jahr mit Datum – das ist billiger als die Diskussion darüber, ab wann eine Einstellung aktiv war.

Die Grenze zur E-Akte sauber ziehen

Ein Punkt, der in Prüfungen regelmäßig für Verwirrung sorgt: Protokolldaten sind kein Schriftgut im Sinne des Aktenplans. Ein Auditeintrag ist ein technischer Datensatz, kein Vorgangsbestandteil. Das Ergebnis einer Auswertung dagegen – also der Prüfvermerk, der Bericht, die Stellungnahme – ist sehr wohl Schriftgut und gehört nach Aktenplan abgelegt, mit Aufbewahrungsfrist und späterer Aussonderung.

Und noch klarer: Nichts davon macht SharePoint zu einer E-Akte. Ob und in welcher Form eine elektronische Akte geführt werden muss, richtet sich nach dem E-Government-Gesetz Ihres Landes und den dazu ergangenen Regelungen, nicht nach den Funktionen eines Kollaborationswerkzeugs. Ein sauber geführtes Auditprotokoll ist ein Beleg für Ordnungsmäßigkeit im IT-Betrieb; es ist kein Beleg für eine ordnungsgemäße Aktenführung und ersetzt keine Vorgangsbearbeitung.

Wo die Nachweisführung an andere Themen anschließt

› SharePoint als E-Akte? Was geht, was nicht und wo die Grenze nach Landesrecht liegt
› Schriftgutverwaltung mit Microsoft 365: Vom Aktenplan zur Aufbewahrungsbezeichnung
› Backup und Wiederherstellung in Microsoft 365: Die Risikoentscheidung fürs Rechnungsprüfungsamt
› Notfallübung für die Verwaltungs-IT: SharePoint verschlüsselt, Admin-Konto übernommen, Bürgertelefon tot

Typische Prüffeststellungen – und wie Sie ihnen zuvorkommen

Prüffeststellungen wiederholen sich erstaunlich zuverlässig. Das liegt nicht daran, dass Verwaltungen besonders nachlässig wären, sondern daran, dass dieselben strukturellen Engpässe überall wirken: zu wenig Personal für eine saubere Funktionstrennung, ein Cloud-Dienst, der sich schneller ändert als die Dokumentation, und ein Beschaffungsvorgang, der die laufende Bewirtschaftung nicht mitgedacht hat.

Feststellung	Wovon sie meist kommt	Was hilft
Zu viele dauerhaft privilegierte Konten	Notfallzugriff wurde nie zurückgebaut, Vertretungsregelung über Rechte gelöst	PIM mit Genehmigung, zwei dokumentierte Notfallkonten, Stichtagsnachweis
Keine Nachweise über den Prüfzeitraum	Standardaufbewahrung von 180 beziehungsweise 30 Tagen abgelaufen	Aufbewahrungsrichtlinie und Export frühzeitig entscheiden
Lizenzen ohne erkennbare Nutzung	Austritte nicht zurückgemeldet, kein Prozess zwischen Personalamt und IT	Quartalsabgleich als fester Termin, Off-Boarding schriftlich regeln
Externe Zugriffe ohne Dokumentation	Planungsbüros und Gremienmitglieder als Gäste eingeladen, nie überprüft	Zugriffsüberprüfung mit Ablaufdatum, Verantwortliche je Gastgruppe
Aufbewahrungsrichtlinie greift nicht wie dokumentiert	Konfiguration geändert, Dokumentation nicht nachgezogen	Jährlicher Konfigurationsexport, Abgleich gegen Aktenplan
Keine Dienstvereinbarung oder veraltete Fassung	Vereinbarung vor Einführung neuer Dienste geschlossen	Öffnungsklausel mit jährlicher Fortschreibung im Gremium
Kein Nachweis über Wiederherstellbarkeit	Sicherung existiert, wurde aber nie ernsthaft zurückgespielt	Wiederherstellungstest mit Protokoll, Datum und Ergebnis

Auftragsverarbeitung unvollständig dokumentiert	Zusatzdienste und Exportziele nachträglich hinzugekommen	Verarbeitungsverzeichnis bei jeder Diensterweiterung fortschreiben

Der Fall, der immer wieder auftaucht

Eine Stadtverwaltung hatte SharePoint im Sozialbereich eingeführt, sorgfältig geplant, mit Berechtigungskonzept und Schulung. Zwei Jahre später fragte die Prüfung nach der Wirksamkeit des Berechtigungskonzepts. Die Antwort hätte lauten müssen: „Hier sind die Ergebnisse der jährlichen Zugriffsüberprüfung." Sie lautete stattdessen: „Wir haben das Konzept, hier ist das PDF von damals." Zwischen dem Konzept und der Wirklichkeit lagen zwei Jahre Personalfluktuation, drei Umorganisationen und eine unbekannte Zahl von Berechtigungen, die aus „nur ganz kurz" dauerhaft geworden waren.

Die Feststellung war unvermeidlich. Behoben wurde sie mit einer jährlichen Zugriffsüberprüfung, deren Ergebnis als PDF zur Akte geht, und mit der schlichten Regel, dass jede Berechtigungsgruppe eine verantwortliche Person aus dem Fachamt hat – nicht aus der IT. Die IT verwaltet Rechte, sie entscheidet nicht über sie. Dieser eine Satz hat in der Nachprüfung mehr bewirkt als das gesamte ursprüngliche Konzept.

Tipp: Wenn die eigene Kapazität nicht reicht

Die Funktionstrennung, die Prüfung und Aufsicht erwarten, ist in Häusern unter etwa 300 Beschäftigten mit eigenem Personal kaum darstellbar. Das ist kein Argument gegen die Anforderung, sondern eines für eine bewusste Aufteilung: kommunales Rechenzentrum, Systemhaus, interkommunale Zusammenarbeit oder eine externe Zweitmeinung für die Auswertungsfreigabe. Wichtig ist, dass die Konstruktion vor der Prüfung existiert und vertraglich sauber ist. Wenn Sie an dieser Stelle eine unabhängige Einordnung brauchen, finden Sie sie in der Microsoft-365-Beratung für Verwaltungen.

Zwei Anschlüsse dazu: Die organisatorische Rollenverteilung zwischen Haus und Dienstleister ist Thema des Beitrags Microsoft 365 und das kommunale Rechenzentrum: Rollen, Schnittstellen, Zweitmeinung, und wenn es um die Frage geht, wer die Auswertungsbefugnis überhaupt bekommt, hilft die unabhängige Einordnung in der Microsoft-365-Beratung für Verwaltungen. Dass die Beschäftigten wissen, was protokolliert wird und was nicht, ist übrigens ebenfalls ein Nachweis – die entsprechende Unterweisung gehört in die Microsoft-365-Schulung für Verwaltungen und wird mit Teilnahmeliste dokumentiert.

Ein Wort zu souveränen Umgebungen

Die Frage nach Delos Cloud kommt in diesem Zusammenhang zuverlässig. Nüchtern betrachtet ändert eine souveräne Betriebsumgebung an der Nachweislogik dieses Beitrags wenig: Protokolle entstehen, Aufbewahrungsfristen gelten, eine Dienstvereinbarung wird trotzdem gebraucht, und die Rechnungsprüfung fragt dieselben Dinge. Was sich ändern kann, sind Betreiberkonstellation, Auftragsverarbeitung und der jeweils verfügbare Funktionsumfang. Welche Dienste zu welchem Zeitpunkt in welchem Umfang bereitstehen, ist eine Frage der jeweils aktuellen Ankündigungslage – planen Sie Ihre Nachweisführung nicht auf einen Termin, sondern auf den Bestand. Eine Einordnung des Angebots steht im Beitrag Delos Cloud für Kommunen: Was das Angebot ist, wen es betrifft und was fehlt.

Häufige Fragen

Wie lange werden Microsoft-365-Auditdaten aufbewahrt?

Purview Audit (Standard) bewahrt Auditdatensätze standardmäßig 180 Tage auf. Mit Audit (Premium) werden Datensätze aus Exchange Online, SharePoint, OneDrive und Entra ID ein Jahr lang aufbewahrt, allerdings nur für Konten mit E5-Lizenz oder passender Add-on-Lizenz; alle übrigen Datensätze bleiben bei 180 Tagen. Eigene Aufbewahrungsrichtlinien erlauben Dauern von sieben Tagen bis zehn Jahren, wobei die langen Zeiträume ab drei Jahren eine Zusatzlizenz voraussetzen. Die Anmelde- und Überwachungsprotokolle in Entra ID sind davon getrennt und liegen bei sieben Tagen ohne und 30 Tagen mit P1 oder P2.

Reicht das Auditprotokoll als Nachweis für die Rechnungsprüfung aus?

In der Regel nicht allein. Das Rechnungsprüfungsamt fragt nach Wirtschaftlichkeit und interner Kontrolle, und dafür sind Lizenzübersichten, Vertragsunterlagen, Rollenzuweisungen zum Stichtag und die Ergebnisse von Zugriffsüberprüfungen aussagekräftiger als einzelne Protokolleinträge. Das Auditprotokoll belegt Vorgänge, nicht Ordnungsmäßigkeit. Nehmen Sie es als eine von mehreren Quellen und legen Sie die aggregierten Auswertungen als eigene, datierte Dokumente vor.

Darf ich als IT-Leitung einfach ins Auditprotokoll schauen?

Technisch ja, wenn Sie die Rolle haben. Rechtlich und dienstrechtlich kommt es auf den Zweck an. Sobald ein Bezug zu einzelnen Beschäftigten entsteht, brauchen Sie einen in der Dienstvereinbarung vorgesehenen Anlass und das dort geregelte Verfahren. Und bedenken Sie: Ihre Suche wird selbst protokolliert. Die Vorstellung, ein Blick ins Protokoll bliebe unbemerkt, ist ein Irrtum mit potenziell dienstrechtlichen Folgen.

Was passiert, wenn wir die Aufbewahrung erst jetzt verlängern?

Dann gilt die neue Aufbewahrung ab dem Zeitpunkt der Änderung für neu entstehende Datensätze. Bereits eingelaufene Einträge behalten ihre ursprünglich zugewiesene Lebensdauer. Rechnen Sie also nicht damit, dass eine Umstellung im Herbst Ihnen die Daten des Frühjahrs rettet. Dasselbe gilt für Lizenzupgrades in Entra ID: Nach dem Wechsel von der kostenlosen auf eine Premium-Edition sehen Sie zunächst nur die Daten, die noch innerhalb der alten Sieben-Tage-Frist lagen.

Wie beteiligen wir den Personalrat richtig?

Früh und schriftlich. Microsoft 365 ist eine technische Einrichtung, die zur Überwachung geeignet ist, damit greift die Mitbestimmung nach dem jeweiligen Landespersonalvertretungsrecht. Praktisch bewährt hat sich, dem Gremium nicht die Technik zu erklären, sondern die Auswertungsmöglichkeiten – also konkret zu zeigen, was mit welchen Klicks sichtbar wäre. Daraus entsteht die Positivliste der zulässigen Zwecke, und daraus wiederum die Dienstvereinbarung. Ein jährlicher Bericht über tatsächlich durchgeführte Auswertungen schafft mehr Vertrauen als jede Zusicherung.

Was ist der Unterschied zwischen Entra-Protokollen und dem Auditprotokoll?

Es sind zwei getrennte Systeme mit getrennter Aufbewahrung. Die Entra-Protokolle dokumentieren Anmeldungen und Verzeichnisänderungen und werden nach Lizenzstufe sieben oder 30 Tage vorgehalten. Das einheitliche Auditprotokoll in Purview dokumentiert Aktivitäten in den Diensten und folgt der Purview-Aufbewahrung. Manche Ereignisse tauchen in beiden auf, viele nur in einem. Wer nur eine Quelle exportiert, hat Lücken, die im Prüfungsfall unangenehm auffallen.

Dürfen wir Nutzungsberichte mit Klarnamen an die Kämmerei geben?

Grundsätzlich nicht. Die Berichte sind seit September 2021 standardmäßig anonymisiert, und das ist für diesen Zweck auch völlig ausreichend: Für eine Wirtschaftlichkeitsbetrachtung brauchen Sie Summen, keine Namen. Die Deanonymisierung ist eine bewusste Einstellungsänderung, sie wirkt auf alle Berichte einschließlich der Auswertungen über Microsoft Graph und das Teams Admin Center, und sie wird selbst als Ereignis protokolliert. Wer sie ohne Anlass vornimmt, hat ein Problem mit der Dienstvereinbarung.

Wie gehen wir mit Auskunftsersuchen nach Artikel 15 um?

Das ist einer der wenigen Fälle, in denen eine personenbezogene Auswertung nicht nur zulässig, sondern geboten ist – allerdings beschränkt auf die anfragende Person. Legen Sie dafür ein festes Verfahren fest, mit Zuständigkeit bei der datenschutzbeauftragten Person, definierten Suchräumen und einer Frist. Und dokumentieren Sie die Auswertung, denn sie ist selbst eine Verarbeitung, über die Sie Rechenschaft ablegen müssen.

Brauchen wir Audit (Premium), also faktisch E5?

Das hängt vom Schutzbedarf ab, nicht vom Wunsch nach Vollständigkeit. Ein Haus, das Sozialdaten, Personaldaten oder Ordnungsdaten in der Cloud verarbeitet, wird eine Aufbewahrung von 180 Tagen im Vorfallfall als knapp empfinden – Kompromittierungen bleiben oft Monate unbemerkt. Ein Weg ist E5 für die Konten mit erhöhtem Schutzbedarf und Export der übrigen Protokolle. Die Entscheidung gehört in die Schutzbedarfsfeststellung und in die Beschlussvorlage, mit Kosten und Alternativen, nicht in eine Bauchentscheidung der IT.

Was ist mit Copilot – entstehen dadurch neue Nachweispflichten?

Ja, und zwar an zwei Stellen. Erstens werden Copilot-Interaktionen protokolliert, was die Frage nach zulässigen Auswertungen neu stellt und in die Dienstvereinbarung gehört. Zweitens macht Copilot bestehende Berechtigungsfehler sichtbar: Was eine Person lesen darf, kann Copilot für sie finden und zusammenfassen. Damit wird der Nachweis über ein wirksames Berechtigungskonzept vom theoretischen zum sehr praktischen Thema.

Weiterführend in dieser Reihe

› Copilot und Personalrat: Bausteine einer Dienstvereinbarung
› Oversharing im Verwaltungs-Tenant: Warum Copilot die Personalakte findet
› Schutzbedarf und Microsoft 365: IT-Grundschutz-Abgleich für die Praxis
› Conditional Access für Verwaltungen: Regelwerk für Rathaus, Bauhof und Homeoffice
› Gäste in Teams und SharePoint: Planungsbüros, Träger und Gremienmitglieder sicher einbinden
› Microsoft-365-Einführung in der Verwaltung: Konzeptionsphase in 4,5 Tagen und die Beschlussvorlage

Fazit

Nachweisfähigkeit in Microsoft 365 ist kein Werkzeugproblem. Die Werkzeuge sind da, sie sind gut dokumentiert, und sie protokollieren mehr, als den meisten Häusern lieb ist. Das Problem ist der Zeitversatz: Protokolle verfallen nach Monaten, Prüfungen kommen nach Jahren. Wer diese Lücke nicht bewusst schließt – durch Lizenzentscheidung, Aufbewahrungsrichtlinie oder Export –, schließt sie gar nicht, denn rückwirkend geht hier nichts.

Die zweite Erkenntnis ist unbequemer: Die meisten Nachweise, die Prüfung und Aufsicht wirklich überzeugen, stammen gar nicht aus dem Protokoll. Sie stammen aus dem Betrieb. Ein dokumentierter Wiederherstellungstest, eine durchgeführte Zugriffsüberprüfung, ein

Stichtagsexport der privilegierten Rollen, eine gelebte Dienstvereinbarung – das sind die Unterlagen, die eine Prüfung trägt. Das Auditprotokoll ist der Notnagel für den Fall, dass etwas schiefgegangen ist, nicht der Regelnachweis dafür, dass alles gut läuft.

Und die dritte, die man in Verwaltungen ungern ausspricht: Die Grenze zur Leistungs- und Verhaltenskontrolle verläuft nicht dort, wo die Technik aufhört, sondern dort, wo Ihre Organisation sie zieht. Technisch können Sie fast alles über fast jeden herausfinden. Dass Sie es nicht tun, ist kein Systemzustand, sondern eine Entscheidung – und diese Entscheidung muss geschrieben, beschlossen, technisch abgesichert und regelmäßig überprüft sein. Wer das hat, kann jeder der drei Prüfstellen entspannt gegenübertreten. Wer es nicht hat, kann nur hoffen, dass niemand nachfragt. Erfahrungsgemäß fragt immer irgendwann jemand nach.

Wichtig: Die drei Dinge, die Sie diese Woche anstoßen können

1. Prüfen Sie, wie lange Ihr Tenant heute tatsächlich aufbewahrt – getrennt für Purview und für Entra, und getrennt nach Lizenzklassen Ihrer Konten.
2. Legen Sie fest, wer im Haus überhaupt eine Auditsuche auslösen darf, und befristen Sie diese Berechtigung. Unbefristete Auswertungsrechte sind in jeder Prüfung eine Feststellung.
3. Setzen Sie vier Termine in den Jahreskalender, einen pro Quartal, und hängen Sie an jeden genau ein Dokument, das dabei entstehen muss. Mehr braucht es für den Anfang nicht.