

Oversharing im Verwaltungs-Tenant: Warum Copilot die Personalakte findet

Der Moment, in dem eine Verwaltung merkt, dass sie ein Oversharing-Problem hat, dauert ungefähr elf Sekunden. So lange braucht Copilot für die Antwort auf die Frage, die in jedem Pilotbetrieb irgendwann gestellt wird: „Was findest du eigentlich über mich?“ Die Antwort ist meistens höflich, gut gegliedert und mit Quellenangabe versehen. Und sie enthält gelegentlich die Eingruppierung, einen Vermerk aus einem Personalgespräch und den Namen der Sachbearbeitung, die ihn geschrieben hat.

Die erste Reaktion im Raum ist immer dieselbe: Copilot habe da etwas aufgebrochen. Das stimmt nicht. Copilot hat nichts aufgebrochen, nichts umgangen und keine Berechtigung verändert. Es hat gelesen, was das anfragende Konto ohnehin lesen durfte. Der Unterschied ist nur: Bisher hätte jemand wissen müssen, dass es diese Datei gibt, wie sie heißt und wo sie liegt. Jetzt reicht eine Frage in ganzen Sätzen.

Oversharing ist keine Copilot-Eigenschaft. Es ist die Summe aus zehn Jahren pragmatischer Entscheidungen, die einzeln alle vertretbar waren. Ein öffentliches Team, weil es schnell gehen musste. Eine Freigabe an „Jeder außer externen Benutzern“, weil die Vertretung nicht in der Gruppe war. Eine unterbrochene Vererbung, weil das Amt umorganisiert wurde. Copilot ist nicht der Einbrecher. Copilot ist die Taschenlampe im Keller, den seit 2014 niemand mehr betreten hat.

Dieser Beitrag zeigt Ihnen, welche Fundmuster in Verwaltungs-Tenants regelmäßig auftauchen, wie Sie sie mit Bordmitteln und mit Zusatzwerkzeugen finden, und in welcher Reihenfolge Sie sie beheben, ohne dabei den Betrieb Ihrer Fachämter lahmzulegen. Die Reihenfolge ist dabei wichtiger als das Werkzeug.

Copilot bricht nichts auf – es liest nur schneller als Ihre Registratur

Der Unterschied zwischen berechtigt und auffindbar

In der Papierwelt war Sicherheit durch Unauffindbarkeit eine funktionierende Betriebsart. Wer nicht wusste, dass im dritten Regal links hinter den Bauakten ein Ordner mit Abmahnungen steht, kam nicht an ihn heran – selbst wenn der Registraturraum offen stand. Genau diese stillschweigende Sicherungsschicht hat sich in die digitale Ablage mitgeschleppt. Eine SharePoint-Website mit 40.000 Dokumenten, deren Adresse niemand kennt, war praktisch unsichtbar, auch wenn technisch die halbe Verwaltung Leserechte hatte.

Die klassische Suche hat daran wenig geändert. Sie liefert Treffer, wenn man die richtigen Wörter eingibt, und die meisten Beschäftigten geben keine Wörter ein, an die sie nicht denken. Ein Sprachmodell denkt an alles. Es formuliert die Suchanfrage selbst, es kombiniert mehrere Quellen, es fasst zusammen, und es beantwortet auch Fragen, für die es kein Dokument gibt – indem es die Antwort aus fünf Dokumenten zusammensetzt, die jeweils für sich harmlos aussehen.

Damit fällt die letzte informelle Schutzschicht weg. Was übrig bleibt, ist genau das, was in den Berechtigungen steht. Und das ist bei den meisten Verwaltungen deutlich mehr, als die Verwaltungsspitze vermutet.

FAKTENCHECK · Was Copilot technisch tut – und was nicht

Microsoft 365 Copilot arbeitet auf dem bestehenden Berechtigungsmodell. Es liest ausschließlich Inhalte, auf die das anfragende Konto Zugriff hat, und es vergibt selbst keine Rechte.

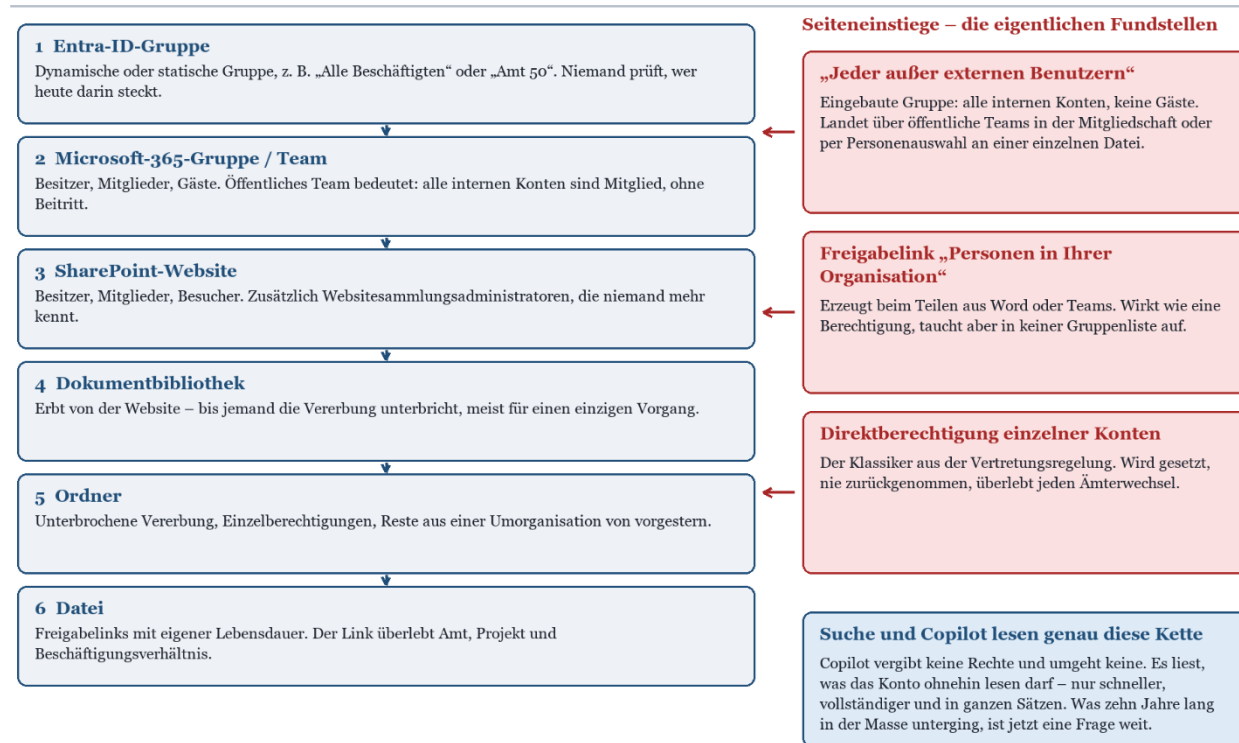
Umgekehrt gilt aber auch: Copilot prüft nicht, ob eine Berechtigung fachlich sinnvoll ist. Eine Datei, die versehentlich für alle internen Konten freigegeben wurde, ist für Copilot eine ganz normale Quelle.

Die Antwort enthält in der Regel Quellenverweise. Das ist der Grund, warum Oversharing-Funde im Pilotbetrieb so schnell auffallen: Die betroffene Person sieht nicht nur die Information, sondern auch den Ablageort.

Die Berechtigungskette – sechs Stufen, an denen Zugriff entsteht

Wer Oversharing beheben will, muss zuerst verstehen, an welchen Stellen Zugriff überhaupt entstehen kann. In SharePoint und Teams sind das sechs Stufen, und jede einzelne kann Rechte hinzufügen. Keine einzige nimmt automatisch welche weg. Dazu kommen drei Seiteneinstiege, die sich der Gruppenlogik vollständig entziehen und deshalb in klassischen Rechteausswertungen gern übersehen werden.

Die Berechtigungskette: sechs Stufen und drei Seiteneinstiege



Skizze 1: Jede Stufe kann Zugriff hinzufügen. Keine Stufe nimmt automatisch welchen weg.

Skizze 1: Die Berechtigungskette und ihre drei Seiteneinstiege. Fundstellen entstehen fast immer rechts, nicht links.

Der praktische Effekt: Eine saubere Gruppenstruktur in Entra ID sagt Ihnen fast nichts über die tatsächliche Sichtbarkeit einer Datei. Sie müssen die unterste Ebene betrachten, und dort liegen Freigabelinks und Einzelberechtigungen, die weder in einer Gruppenmitgliedschaft noch in einer Websiteberechtigung auftauchen.

Warum Verwaltungen strukturell stärker betroffen sind

Es gibt drei Gründe, warum Verwaltungs-Tenants im Schnitt mehr Fundstellen enthalten als vergleichbar große Unternehmen. Erstens die Aufgabenvielfalt: Eine Stadtverwaltung führt Personalakten, Sozialdaten, Vergabeunterlagen, Bauakten, Gremienunterlagen und Bürgerdaten im selben Tenant. Ein Maschinenbauer hat Konstruktionsdaten und Personalakten – zwei Kategorien statt zwölf.

Zweitens die Personalfuktuation innerhalb des Hauses. Beschäftigte wechseln zwischen Ämtern, behalten aber ihre alten Zugriffe, weil niemand sie entzieht. Nach fünfzehn Dienstjahren in vier Ämtern hat eine einzelne Person Rechte in Bereichen, in denen sie seit einem Jahrzehnt nicht mehr arbeitet. Das ist keine Nachlässigkeit, sondern das Fehlen eines Prozesses – der Personalwechsel läuft über das Personalamt, die Rechte liegen bei der IT, und dazwischen liegt oft nichts.

Drittens die Pandemie. Zwischen März 2020 und Sommer 2021 wurden in fast jeder Verwaltung Strukturen angelegt, die für zwei Wochen gedacht waren und heute noch stehen. Sie sind der ergiebigste Fundort überhaupt, und sie sind der Grund, warum die Fundliste in der ersten Überprüfung so unangenehm lang wird.

Wenn Sie an dieser Stelle einsteigen und den größeren Zusammenhang suchen: Der Überblicksbeitrag [Microsoft 365 in der öffentlichen Verwaltung](#) ordnet ein, wo dieses Thema zwischen Betriebsmodell, Datenschutz, Vergabe und Schriftgutverwaltung steht. Er ist der rote Faden, in den sich dieser Beitrag einfügt.

WICHTIG · Die unbequeme Vorbemerkung

Oversharing ist kein Grund, Copilot nicht einzuführen. Es ist ein Grund, vorher zu wissen, was im eigenen Tenant liegt. Die Fundstellen existieren nämlich auch ohne Copilot – sie sind heute nur bequemer zu ignorieren.

Umgekehrt ist eine Copilot-Einführung ohne vorherige Bestandsaufnahme eine Wette darauf, dass die Datenschutzbeauftragte nichts erfährt. Diese Wette verliert man in der Regel innerhalb der ersten sechs Wochen.

Drei Fundmuster, die in fast jedem Verwaltungs-Tenant liegen

Die folgenden drei Muster stammen aus Überprüfungen in einer Stadtverwaltung mit rund 1.000 Rufnummern, einem großen Landschaftsverband und einer weiteren Stadtverwaltung mit umfangreicher SharePoint-Nutzung im Sozialbereich. Die Häuser unterscheiden sich in Größe, Aufgabe und Reifegrad erheblich. Die Fundmuster sind trotzdem fast identisch – was ein gutes Zeichen ist, denn es bedeutet, dass sie planbar zu suchen sind.

Fundmuster 1: Die Teams-Gruppe aus der Pandemiezeit

Angelegt an einem Freitagnachmittag im Frühjahr 2020, öffentlich konfiguriert, damit „alle sofort reinkommen“. Inhalt: Dienstpläne, Kontaktlisten mit privaten Rufnummern, Übersichten zu Risikogruppen, in einem Fall eine vollständige Aufstellung der Beschäftigten mit Angaben zu Vorerkrankungen, weil das für die Präsenzplanung gebraucht wurde. Alles fachlich nachvollziehbar. Alles seit Jahren offen.

Der Kern des Problems ist die Einstellung „öffentlich“ bei einer Microsoft-365-Gruppe. Sie bedeutet nicht „für die Allgemeinheit sichtbar“, sondern „jedes interne Konto ist automatisch

berechtigt, ohne Beitritt “ – technisch abgebildet über die eingebaute Gruppe „Jeder außer externen Benutzern“. In der Mitgliederliste des Teams stehen weiterhin nur die zwölf Personen des Krisenstabs. In der Berechtigung steht die gesamte Belegschaft. Genau diese Diskrepanz ist der Grund, warum Fachämter bei der ersten Auswertung reflexhaft widersprechen: Sie sehen die Mitgliederliste, nicht die Berechtigung.

Der Besitzer des Teams ist inzwischen in einem anderen Amt oder im Ruhestand. Damit ist niemand mehr zuständig, und die Frage „Darf das weg?“ hat keinen Adressaten. In der Stadtverwaltung mit den rund 1.000 Rufnummern waren es 63 Teams aus dem Zeitraum 2020 bis 2021, von denen 41 keinen aktiven Besitzer mehr hatten und 17 in den zurückliegenden zwei Jahren keinen einzigen Zugriff verzeichneten.

Fundmuster 2: Die Vergabeakte mit „Jeder außer externen Benutzern“

Das zweite Muster ist heikler, weil es nicht aus Bequemlichkeit entsteht, sondern aus einem echten fachlichen Bedürfnis. Eine Vergabestelle bearbeitet ein Verfahren, die Kämmerei muss die Haushaltsstelle prüfen, das Rechnungsprüfungsamt will begleitend hineinschauen, das Fachamt liefert die Leistungsbeschreibung zu. Vier Bereiche, vier Gruppen, und in der Hektik vor dem Submissionstermin fügt jemand die Berechtigung „Jeder außer externen Benutzern“ hinzu, weil das schneller geht als vier Gruppenanträge.

Nach dem Zuschlag wird die Berechtigung nicht zurückgenommen. Sie steht dann auf einem Ordner, in dem Angebotspreise, Nachweise zur Eignung, interne Wertungsvermerke und der Vergabevorschlag liegen. Bei laufenden Verfahren ist das ein ernsthaftes Problem, denn Copilot beantwortet die Frage nach den Angebotspreisen eines noch nicht abgeschlossenen Verfahrens genauso freundlich wie jede andere. In einem der untersuchten Häuser lag ein Wertungsvermerk zu einem laufenden Verfahren offen, weil die Vorgängerakte als Vorlage kopiert worden war – samt Berechtigung.

Was hier gebraucht wird, ist keine schärfere Regel, sondern eine Struktur, in der der Zugriff für mitprüfende Bereiche vorgesehen ist, ohne dass jemand improvisieren muss. Wie sich das in der Informationsarchitektur abbilden lässt, behandelt der Beitrag zur Teams-Einführung entlang der Ämter.

Weiterführend dazu: [Microsoft Teams in der Verwaltung einführen: Informationsarchitektur entlang der Ämter](#). Für die vergaberechtliche Seite der Beschaffung selbst – Leistungsbeschreibung, Rahmenverträge, Wertgrenzen – siehe [Microsoft 365 rechtssicher beschaffen: Vergabe, Leistungsbeschreibung, Rahmenverträge](#). Wertgrenzen und Fristen sind dort wie hier Orientierung; maßgeblich ist das jeweilige Landesrecht und Ihre Dienstanweisung.

Fundmuster 3: Die vergessene SharePoint-Website mit Sozialdaten

Das dritte Muster ist das gefährlichste, weil es am leisesten ist. Eine Website, die einmal für ein Projekt angelegt wurde – Umstellung eines Fachverfahrens, Einführung eines neuen Antragsprozesses, Vorbereitung einer Organisationsuntersuchung. Für die Migration wurden Echtdaten hochgeladen, weil man mit Testdaten nichts sieht. Das Projekt endete, die Website blieb, die Echtdaten auch.

In der Stadtverwaltung mit der umfangreichen SharePoint-Nutzung im Sozialbereich fand sich eine Website mit knapp 9.000 Dokumenten aus einer Verfahrensumstellung, die vier Jahre zurücklag. Darin: Bewilligungsbescheide, Widersprüche, ärztliche Stellungnahmen. Die Berechtigung stand auf einer Entra-Gruppe, die ursprünglich das Projektteam abbildete und nach der Projektauflösung

mit einer amtsweiten Gruppe verschmolzen worden war. Ergebnis: 180 Konten mit Leserecht auf Sozialdaten, von denen keines je davon erfahren hatte.

Genau hier liegt auch die Grenze zur E-Akte. Diese Dokumente waren nie Teil einer ordnungsgemäßen elektronischen Aktenführung. Sie lagen in einer Projektablage, ohne Aktenzeichen, ohne Aktenplanbezug, ohne Aufbewahrungsbezeichnung, ohne Aussonderungsvorgang. Sie sind damit weder rechtssicher geführt noch geordnet zu vernichten – ein Zustand, den man nicht durch Rechteentzug repariert, sondern nur durch eine Entscheidung darüber, was Akte ist und was Arbeitskopie.

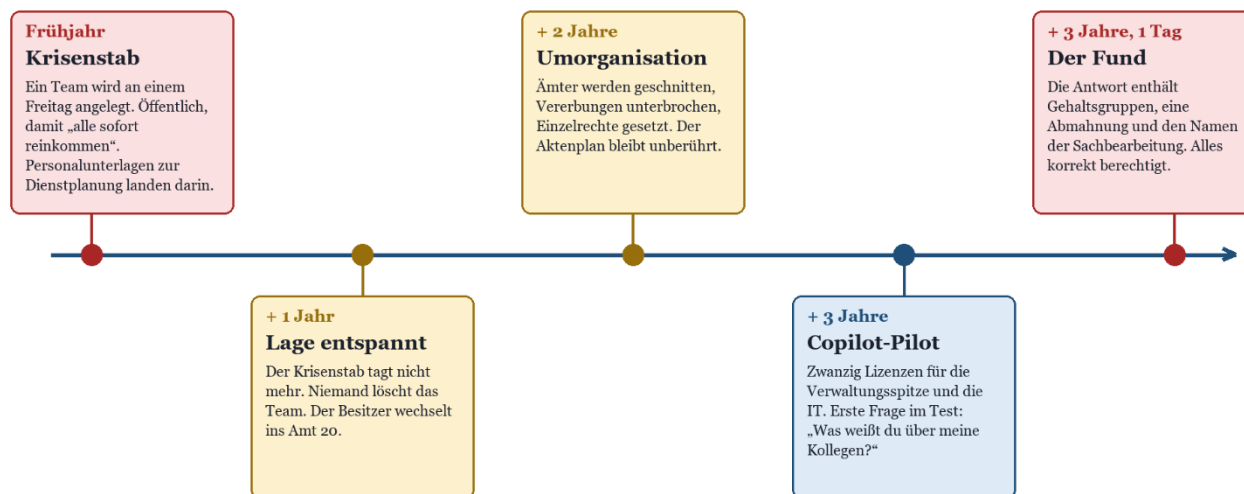
Wo diese Grenze nach den Landes-E-Government-Gesetzen genau verläuft und was SharePoint dabei leisten kann und was nicht, behandelt [SharePoint als E-Akte? Was geht, was nicht und wo die Grenze nach Landesrecht liegt](#). Die Zuordnung von Aktenplan und Aufbewahrungsbezeichnung beschreibt [Schriftgutverwaltung mit Microsoft 365: Vom Aktenplan zur Aufbewahrungsbezeichnung](#).

WARNUNG · Echtdaten in Projektablagen

Der Satz „Wir brauchen für den Test einmal echte Fälle“ ist der Ursprung eines erheblichen Teils aller Sozialdaten-Fundstellen. Er ist fachlich verständlich und trotzdem der Punkt, an dem eine Verarbeitung beginnt, für die es meist keine dokumentierte Grundlage gibt.

Nehmen Sie Migrations- und Testablagen deshalb ausdrücklich in Ihre Fundsuche auf, auch wenn sie nicht nach Fachverfahren aussehen. Webseitenamen wie „Projekt“, „Migration“, „Test“, „Alt“ oder eine Jahreszahl im Titel sind gute Filter für den ersten Durchgang.

Wie eine Fundstelle entsteht: die typische Karriere eines Oversharing-Falls



Skizze 2: Kein einziger Schritt war ein Fehler im Sinne der Dienstanweisung. Das Ergebnis ist trotzdem ein Meldefall.

Skizze 2: Die typische Entstehungsgeschichte. Jeder Schritt für sich war vertretbar.

Die drei Muster unterscheiden sich in Ursache, Datenart und Dringlichkeit. Sie brauchen deshalb auch unterschiedliche Sofortmaßnahmen. Die folgende Übersicht ordnet sie ein.

Fundmuster	Woran Sie es erkennen	Datenart	Sofortmaßnahmen	Dauerhafte Lösungen
Pandemie-Team	Öffentliche Gruppe,	Personaldaten, Gesundheitsangaben	Sichtbarkeit für Suche und Copilot	Besitzerpflicht, Richtlinie für inaktive

	angelegt 2020/2021, kein aktiver Besitzer, kein Zugriff seit über 12 Monaten	, private Kontaktdaten	abschalten, Besitzersuche starten	Websites, geordnete Auflösung
Vergabeakte offen	Berechtigung „Jeder außer externen Benutzern“ auf Ordner- oder Websiteebene, oft nach Kopie einer Vorgängerakte	Angebotspreise, Wertungsvermerke, Eignungsnachweise	Breite Berechtigung entfernen, laufende Verfahren zuerst	Vorlagenstruktur mit vorgesehenen Prüfpunkten für Kämmererei und Rechnungsprüfungsamt
Vergessene Projektwebsite	Kein Zugriff seit Jahren, Name mit Projekt-, Jahres- oder Migrationsbezug, Berechtigung über eine gewachsene Gruppe	Sozialdaten, Bescheide, ärztliche Unterlagen	Zugriff auf einen benannten Kreis reduzieren, Datenschutz einbinden	Entscheidung Akte oder Arbeitskopie, danach Aufbewahrung oder geordnete Vernichtung
Alte Freigabelinks	Links vom Typ „Personen in Ihrer Organisation“ auf Einzeldateien, teils Jahre alt	quer durch alle Bereiche	Links mit Ablaufdatum versehen, Altbestand berichten lassen	Standardtyp für Freigabelinks einschränken, Ablaufdatum verpflichtend
Rechte-Erbe nach Amtswechsel	Einzelne Konten mit Zugriff auf Bereiche, in denen sie nicht mehr arbeiten	abhängig vom früheren Amt	Bericht über die Zugriffe je Person, Abgleich mit dem Personalamt	Prozessverzahnung zwischen Personalamt und Rechtevergabe beim internen Wechsel

Wie Sie das finden: Bordmittel, Zusatzwerkzeuge, Read-only-Überprüfung

Die gute Nachricht: Sie müssen nicht raten. Es gibt Berichte, die genau diese Muster sichtbar machen. Die weniger gute: Sie verteilen sich auf drei Oberflächen mit unterschiedlichen Lizenzvoraussetzungen, und keine davon liefert Ihnen eine fertige Priorisierung. Die Arbeit, aus Zeilen eine Rangfolge zu machen, bleibt bei Ihnen.

Was die Bordmittel hergeben

Ohne jede Zusatzlizenz kommen Sie weiter, als viele annehmen. Das SharePoint Admin Center zeigt Ihnen aktive Websites mit Speicherbelegung, letzter Aktivität und Websitesammlungsadministratoren. Über die SharePoint-Online-PowerShell holen Sie sich mit Get-SPOSite, Get-SPOUser und Get-SPOSiteGroup eine vollständige Liste aller Websites samt

Gruppenmitgliedschaften – inklusive der Frage, wo die Gruppe „Jeder außer externen Benutzern“ auf Websiteebene steht. Das ist mühsam, aber es ist belastbar.

Das Audit-Log in Microsoft Purview beantwortet die Frage, die im Ernstfall wirklich zählt: Hat jemand zugegriffen, und wenn ja, wer und wann. Diese Auswertung sollten Sie beherrschen, bevor Sie sie brauchen. Für die Praxis der Nachweisführung gegenüber der Rechnungsprüfung lohnt der Blick in den entsprechenden Beitrag dieser Reihe.

Details zur Auswertung und zu den Aufbewahrungszeiträumen des Protokolls finden Sie in [Microsoft 365 Audit-Log und Rechnungsprüfung: Nachweise, die Verwaltungen liefern müssen](#).

Die Grenzen der Bordmittel sind allerdings klar. Sie sehen die Websiteebene gut, die Ordner- und Dateiebene schlecht und Freigabelinks praktisch gar nicht in aggregierter Form. Genau dort liegen aber die Fundstellen, die im Pilotbetrieb auffallen. Und Sie bekommen keine Angabe darüber, wie viele Konten auf einen bestimmten Ordner tatsächlich Zugriff haben – die Zahl, die eine Verwaltungsspitze hören will.

Was SharePoint Advanced Management ergänzt

SharePoint Advanced Management, kurz SAM, füllt genau diese Lücke. Die Berichte zur Datenzugriffs-Governance liefern einen Momentaufnahme-Bericht über den Berechtigungsstand aller Websites, einen Bericht über Inhalte, die in den zurückliegenden 28 Tagen mit „Jeder außer externen Benutzern“ geteilt wurden, eine Auswertung der Freigabelink-Aktivität im selben Zeitraum sowie einen Bericht, der für eine einzelne Person auflistet, auf welche Websites sie zugreifen kann und wie dieser Zugriff zustande kommt. Der letzte Bericht ist der, den Personalräte am schnellsten verstehen.

Lizenzseitig ist die Lage angenehmer, als sie klingt: SAM steht zur Unterstützung der Copilot-Einführung bereits dann zur Verfügung, wenn im Tenant mindestens eine Copilot-Lizenz einem Konto zugewiesen ist – diese Person muss nicht die SharePoint-Administration sein. Voraussetzung ist eine passende Basislizenz aus den Office-365- oder Microsoft-365-Enterprise-beziehungsweise Education-Reihen. Ohne Copilot-Lizenz gibt es SAM als eigenständiges Add-on. Einzelne Funktionen bleiben dem Add-on vorbehalten.

Was das für Ihre Lizenzplanung insgesamt bedeutet – E3, E5, F3 und die Behördenkonditionen – ordnet [Microsoft 365 Lizenzen für Verwaltungen: E3, E5, F3 und die Behördenkonditionen](#) ein.

FAKTENCHECK · Zahlen, die Sie für die Planung brauchen

Der Bericht zu „Jeder außer externen Benutzern“ betrachtet die zurückliegenden 28 Tage, zeigt in der Oberfläche die 100 Websites mit der höchsten Aktivität und lässt sich als CSV mit bis zu einer Million Websitezeilen herunterladen. Sie können bis zu zehn solcher Berichte vorhalten; ein Lauf kann bis zu 24 Stunden dauern und lässt sich alle 24 Stunden wiederholen.

Zugriffsüberprüfungen können Sie für bis zu 100 Websites direkt aus der Berichtsansicht anstoßen, für größere Mengen per PowerShell. Aus dem organisationsweiten Berechtigungsbericht sind bis zu 1.000 Überprüfungen je Kalendermonat möglich.

Wichtig für die Interpretation: Die Spalte mit der Zahl der berechtigten Konten dedupliziert nicht. Wer über eine Gruppe und zusätzlich über einen Freigabelink Zugriff hat, wird doppelt gezählt. Die Zahl ist ein Maß für Exponiertheit, keine Kopfzahl.

Der eigentliche Hebel von SAM liegt weniger in den Berichten als in der Delegation. Sie als IT-Administration dürfen aus Compliance-Gründen ohnehin nicht in die Inhalte schauen, und Sie können fachlich nicht beurteilen, ob eine Vergabeakte offen sein darf. Die Zugriffsüberprüfung

schickt genau diese Frage an die Websitebesitzer – mit einer Oberfläche, in der sie die breite Berechtigung mit wenigen Klicks entfernen und die Prüfung abschließen können. Der Rücklauf kommt bei Ihnen an, mit Namen, Zeitstempel und Kommentar. Das ist der Nachweis, den das Rechnungsprüfungsamt sehen will.

TIPP · Die Benachrichtigungs-E-Mail vorher anpassen

Die automatische E-Mail an die Websitebesitzer lässt sich in Absenderkennung, Titel, Text und ergänzendem Verweis anpassen. Nutzen Sie das. Eine unangepasste englischsprachige Systemmail mit der Aufforderung, Berechtigungen zu prüfen, landet in einer Verwaltung mit Sicherheit als Phishing-Verdacht beim IT-Sicherheitsbeauftragten – und Ihre Überprüfung startet mit einem Sicherheitsvorfall, den Sie selbst ausgelöst haben.

Kündigen Sie den Versand zusätzlich über den regulären Dienstweg an: kurze Information an die Amtsleitungen, ein Absatz im Intranet, ein Hinweis in der Dienstberatung. Der Rücklauf steigt dadurch spürbar.

Was Microsoft Purview beisteuert

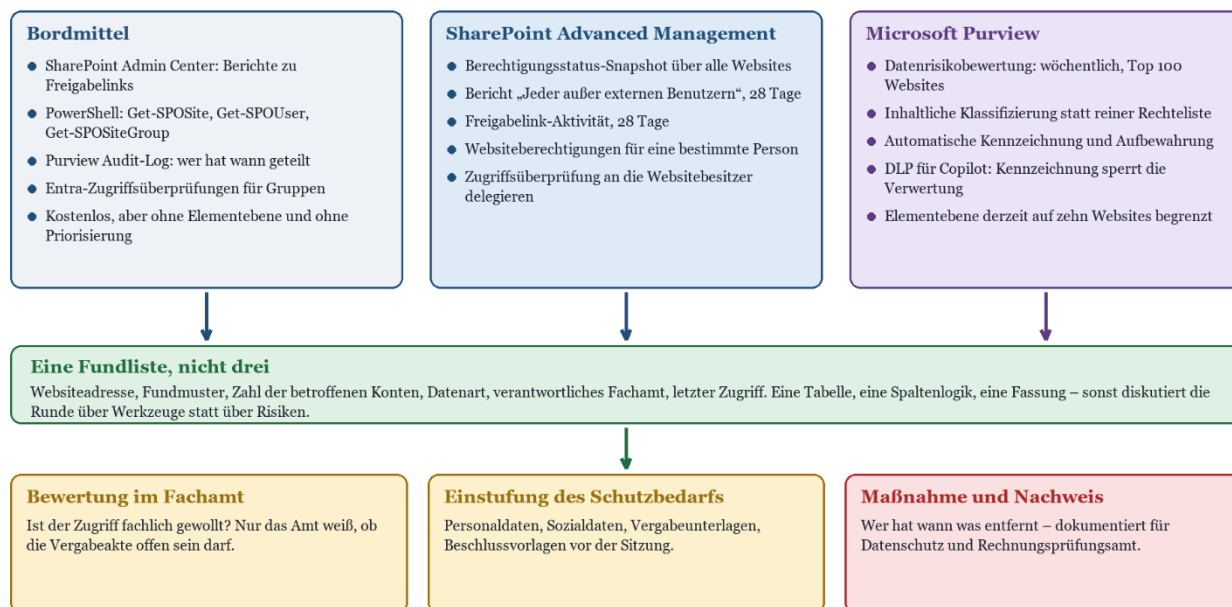
SAM sieht Berechtigungen. Purview sieht Inhalte. Das ist der Unterschied, der über die Priorisierung entscheidet: Eine Website mit 4.000 offenen Dokumenten aus dem Bereich Öffentlichkeitsarbeit ist harmlos, eine Website mit 40 offenen Dokumenten aus dem Bereich Beihilfe ist es nicht. Ohne inhaltliche Klassifizierung sortieren Sie nach der falschen Spalte.

Die Datenrisikobewertungen in der Datensicherheits-Statusverwaltung laufen standardmäßig wöchentlich über die 100 meistgenutzten SharePoint-Websites und zeigen, wie viele Elemente sensible Informationen enthalten und wie breit diese freigegeben sind. Beim ersten Lauf vergehen einige Tage, bis Ergebnisse erscheinen. Eigene Bewertungen können Sie auf ausgewählte Websites oder Personengruppen zuschneiden; die Auswertung auf Elementebene ist derzeit auf zehn SharePoint-Websites begrenzt, mit einer Obergrenze von 200.000 Elementen je Speicherort. OneDrive ist auf Elementebene nicht dabei.

Aus derselben Oberfläche heraus lassen sich direkt Maßnahmen anstoßen: eine automatische Kennzeichnung für unklassifizierte Dokumente mit sensiblen Inhalten, eine Aufbewahrungsrichtlinie für Inhalte, auf die seit Jahren niemand mehr zugegriffen hat, oder eine Regel, die Copilot die Verwertung von Dokumenten mit bestimmten Vertraulichkeitsbezeichnungen untersagt. Die letzte Variante ist bemerkenswert, weil sie den Zugriff unberührt lässt: Die Beschäftigten kommen weiterhin an die Datei, Copilot verwendet sie aber nicht mehr für Antworten.

Für die Aufbewahrungs- und Aussonderungsseite – Fristen, Disposition, Vernichtungsnachweis – siehe [Aufbewahrung und Aussonderung mit Purview: Fristen, Disposition, Vernichtungsnachweis](#). Wenn Aufbewahrungsrichtlinien in Ihrem Tenant nicht so greifen, wie sie sollen, hilft [Wenn die Aufbewahrungsrichtlinie einfach aufhört: SharePoint-Störungsanalyse in der Verwaltung](#) bei der Eingrenzung.

Vom Werkzeug zur Entscheidung: der Trichter einer Oversharing-Überprüfung



Skizze 3: Werkzeuge liefern Zeilen. Entscheidungen liefern die Fachämter – die IT liefert die Grundlage dafür.

Skizze 3: Drei Werkzeugbahnen, eine Fundliste, drei Bewertungsschritte.

Frage	Bordmittel	SharePoint Advanced Management	Microsoft Purview
Welche Websites gibt es und wer verwaltet sie?	Ja, vollständig	Ja, mit Besitzerpflicht und Attestierung	Nicht der Schwerpunkt
Wo steht „Jeder außer externen Benutzern“?	Websiteebene ja, Elementebene nein	Ja, Website- und Elementebene, 28-Tage-Fenster	Indirekt über die Freigabeauswertung
Welche Freigabelinks bestehen?	Nur einzeln, nicht aggregiert	Ja, Aktivitätsbericht über 28 Tage	Ja, in der Risikobewertung
Auf was kann eine bestimmte Person zugreifen?	Aufwendig per Skript	Ja, als eigener Bericht	Ja, in einer eigenen Bewertung
Welche Inhalte sind fachlich schutzbedürftig?	Nein	Nur über gesetzte Vertraulichkeitsbezeichnungen	Ja, das ist der Kern
Sichtbarkeit sofort einschränken	Nur grob über die Sucheinstellung der Website	Ja, gezielt je Website	Ja, über die Kennzeichnungsregel
Prüfung an das Fachamt delegieren	Nein	Ja, mit Rücklauf und Zeitstempel	Eingeschränkt, per Benachrichtigung
Nachweis für die Rechnungsprüfung	Audit-Log, roh	Berichte plus Rücklauf der Überprüfungen	Bewertungsberichte, exportierbar

Read-only-Überprüfung: warum Finden und Beheben getrennt gehören

Es gibt einen guten Grund, die Bestandsaufnahme organisatorisch von der Bereinigung zu trennen. Wer sucht und gleichzeitig aufräumt, produziert eine Fundliste, die am Ende nicht mehr prüfbar ist, weil unterwegs Zustände verändert wurden. Für das Rechnungsprüfungsamt und für die Datenschutzbeauftragte ist das ein Problem: Sie können nicht mehr rekonstruieren, wie breit ein Zugriff zum Zeitpunkt der Feststellung war.

Eine Überprüfung mit ausschließlich lesenden Rechten beantwortet vier Fragen und verändert dabei nichts: Welche Websites und Teams gibt es, wer ist zuständig, wo stehen breite Berechtigungen, und welche davon liegen auf Inhalten mit erhöhtem Schutzbedarf. Das Ergebnis ist eine datierte Fundliste mit Risikoeinstufung – und damit die Grundlage für eine Beschlussvorlage, die den Aufwand für die Bereinigung begründen kann. Der Zugriff dafür lässt sich sauber begrenzen; wie man solche erhöhten Rechte zeitlich befristet und protokolliert vergibt, beschreibt der Beitrag zu privilegierten Konten.

Konkret: [Privilegierte Konten in der Verwaltungs-IT: Rollen, PIM und der Fall des einen Admins](#). Für die Absicherung der Zugänge selbst – Standorte, Geräte, Homeoffice – siehe [Conditional Access für Verwaltungen: Regelwerk für Rathaus, Bauhof und Homeoffice](#).

TIPP · Copilot- und Oversharing-Überprüfung zum Festpreis

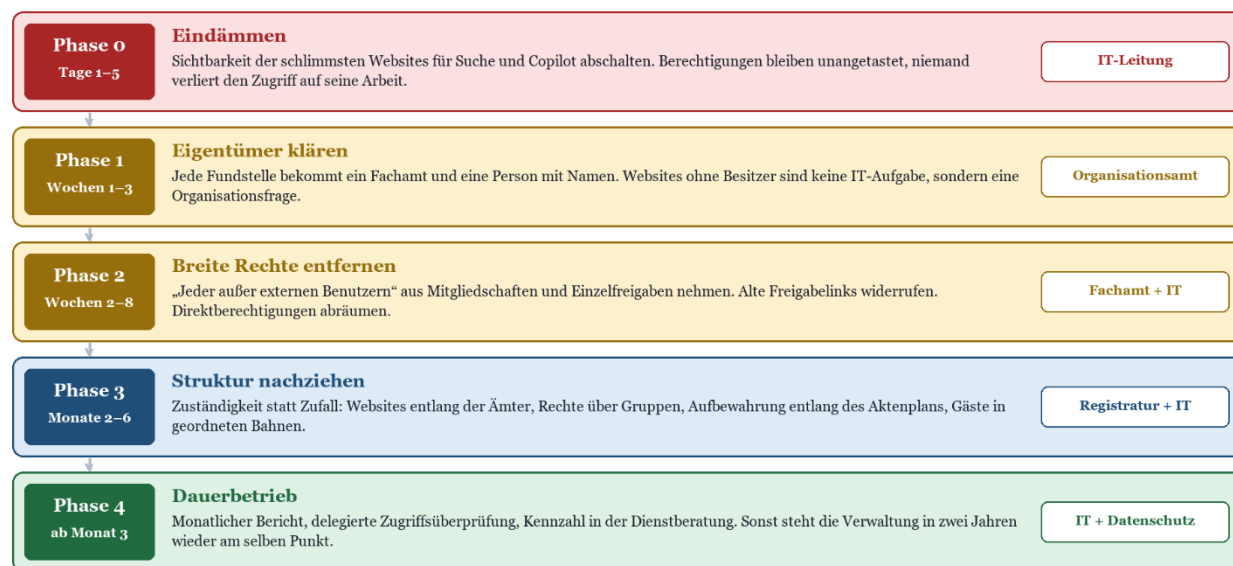
Wenn Sie die Bestandsaufnahme nicht aus dem laufenden Betrieb heraus stemmen wollen oder eine unabhängige Zweitmeinung neben Ihrem Systemhaus oder Ihrem kommunalen Rechenzentrum brauchen: Diese Überprüfung gibt es als abgegrenztes Paket mit lesendem Zugriff, festem Umfang und festem Preis – Ergebnis ist die datierte Fundliste samt Risikoeinstufung und Maßnahmenreihenfolge, in einer Form, die sich einer Beschlussvorlage beilegen lässt.

Umfang und Ablauf: [Microsoft-365-Beratung für Verwaltungen](#).

Beheben in der richtigen Reihenfolge

Die häufigste Fehlentscheidung nach der ersten Fundliste ist der Versuch, gleich richtig aufzuräumen: Berechtigungskonzept schreiben, Websitestruktur neu schneiden, Gruppenlogik vereinheitlichen. Das ist fachlich alles korrekt und dauert anderthalb Jahre. In diesen anderthalb Jahren steht die Vergabeakte weiter offen. Drehen Sie die Reihenfolge um: erst eindämmen, dann verstehen, dann strukturell lösen.

Reihenfolge der Behebung: erst eindämmen, dann verstehen, dann aufräumen



Skizze 4: Wer mit Phase 3 anfängt, ist in zwei Jahren fertig – und hat zwei Jahre lang das Risiko getragen.

Skizze 4: Fünf Phasen mit Zeitrahmen und Zuständigkeit.

Phase 0: Eindämmen, ohne jemandem die Arbeit wegzunehmen

Für die schwersten Fundstellen brauchen Sie eine Maßnahme, die sofort wirkt und niemanden bei der Arbeit behindert. Genau dafür gibt es die eingeschränkte Inhaltssuche auf Websiteebene: Sie schaltet die Auffindbarkeit einer Website in der organisationsweiten Suche und in den Copilot-Erlebnissen ab und entfernt gleichzeitig die KI-Einstiegspunkte auf der Website selbst – die Copilot-Schaltfläche, die KI-Aktionen und das Erstellen von Agenten. Die Berechtigungen bleiben dabei vollständig unverändert. Wer heute mit der Website arbeitet, arbeitet morgen genauso weiter.

Technisch ist das eine Eigenschaft der Website, gesetzt über die Websiteeinstellungen im Admin Center oder per PowerShell mit Set-SPOSite und dem Schalter RestrictContentOrgWideSearch. Die Verwaltung dieser Einstellung lässt sich an die Websiteadministration delegieren; wer sie dann ändert, muss eine Begründung hinterlegen, und die Vorgänge landen im Prüfprotokoll. Für eine Verwaltung ist das eine brauchbare Kombination aus Handlungsfähigkeit vor Ort und Nachvollziehbarkeit.

WARNUNG · Zwei Einschränkungen, die Sie einplanen müssen

Erstens die Laufzeit: Die Einstellung muss durch die Indexsysteme propagieren. Bei großen Websites dauert das; jenseits von 500.000 Elementen kann die vollständige Wirkung mehr als eine Woche in Anspruch nehmen. Wer am Montag abschaltet und am Dienstag testet, hält die Maßnahme fälschlich für wirkungslos.

Zweitens der Charakter: Das ist eine Sichtbarkeitsbremse, keine Sicherheitsgrenze. Wer die Adresse kennt und berechtigt ist, kommt weiterhin an die Inhalte, und Inhalte, die eine Person ohnehin geöffnet hat, bleiben in ihren persönlichen Kontexten verwertbar. Setzen Sie das Mittel also gezielt ein und nicht großflächig – sonst sinkt die Qualität der Copilot-Antworten in der gesamten Verwaltung, ohne dass Ihr eigentliches Problem gelöst wäre.

Ein Hinweis zur älteren Variante, der eingeschränkten SharePoint-Suche mit einer Positivliste von bis zu 100 Websites: Dieses Verfahren läuft aus, seit dem 31. Juli 2026 ist eine Neuaktivierung

nicht mehr möglich. Wenn Sie es im Einsatz haben, behandeln Sie es als Übergangslösung und planen Sie den Umstieg auf die websitebezogene Einschränkung ein. Wer noch nicht damit gestartet ist, überspringt es.

Phase 1: Eigentümerschaft klären, bevor Sie fachlich entscheiden

Jede Fundstelle braucht ein Fachamt und eine Person mit Namen. Das klingt banal und ist in der Praxis der zeitraubendste Teil des gesamten Vorhabens. Eine Website ohne Besitzer ist keine IT-Frage, sondern eine Organisationsfrage: Wer ist heute für den Vorgang zuständig, den es damals gab? Diese Zuordnung kann nur das Organisationsamt leisten, und sie sollte formell erfolgen, nicht per Zuruf.

Setzen Sie dabei eine Mindestregel durch: zwei Besitzer je Website, davon einer aus der Amtsleitung oder Sachgebietsleitung. Ein einzelner Besitzer ist im Ergebnis dasselbe wie kein Besitzer, sobald diese Person länger krank ist, wechselt oder in den Ruhestand geht. In den untersuchten Häusern lag der Anteil der Websites mit genau einem oder gar keinem aktiven Besitzer regelmäßig zwischen 30 und 60 Prozent.

Phase 2: Breite Berechtigungen entfernen – und zwar in dieser Rangfolge

Jetzt wird tatsächlich aufgeräumt. Die Rangfolge ergibt sich aus Schutzbedarf mal Breite mal Aktualität – nicht aus der Anzahl der Dokumente. Vier Kategorien in dieser Reihenfolge:

- Laufende Verfahren mit Vertraulichkeitsanforderung: offene Vergabeakten, laufende Personalverfahren, Beschlussvorlagen vor der Gremiensitzung. Hier zählt jeder Tag.
- Besondere Kategorien personenbezogener Daten: Gesundheitsangaben, Sozialdaten, Angaben aus dem Betreuungs- und Jugendhilfebereich, Beihilfeunterlagen.
- Reguläre Personaldaten: Beurteilungen, Eingruppierungen, Vermerke aus Personalgesprächen, Abmahnungen, Bewerbungsunterlagen.
- Alles Übrige mit breiter Freigabe: Vorlagen, Protokolle, Auswertungen. Wichtig für die Hygiene, aber nicht dringlich.

Praktisch bedeutet Entfernen dreierlei: die Gruppe „Jeder außer externen Benutzern“ aus SharePoint-Gruppen und aus Einzelfreigaben von Dateien, Ordnern und Listen herausnehmen; bestehende Freigabelinks widerrufen statt sie nur zu ignorieren; und Direktberechtigungen einzelner Konten durch Gruppen ersetzen. Der dritte Punkt ist der unbeliebteste, weil er kurzfristig Arbeit macht und langfristig als einziger verhindert, dass das Problem zurückkehrt.

WICHTIG · Nicht löschen, solange die Aussonderung nicht geklärt ist

Der Reflex, eine vergessene Website mit alten Sozialdaten einfach zu löschen, ist verständlich und in der Sache oft falsch. Solange nicht geklärt ist, ob es sich um Schriftgut mit Aufbewahrungspflicht handelt, ist das Löschen selbst der Rechtsverstoß – und in Häusern mit Archivpflicht steht dem Archiv ein Anhebungsverfahren zu.

Trennen Sie deshalb sauber: Rechte entziehen ist eine Sofortmaßnahme und jederzeit zulässig. Vernichten ist ein eigener Vorgang mit eigener Entscheidung, eigener Dokumentation und – je nach Landesrecht und Archivsatzung – eigener Beteiligung. Die konkreten Fristen und Zuständigkeiten regelt Ihr Landesrecht; verstehen Sie die Angaben hier als Orientierung, nicht als Rechtsauskunft.

Phase 3: Struktur nachziehen, damit es nicht zurückkommt

Erst jetzt lohnt die strukturelle Arbeit, und jetzt lohnt sie wirklich. Websites entlang der Ämter und Aufgaben statt entlang von Projekten. Rechte ausschließlich über Gruppen, deren Pflege an einem definierten Prozess hängt. Ein Standardtyp für Freigabelinks, der nicht „Personen in Ihrer Organisation“ lautet, und ein verpflichtendes Ablaufdatum. Gastzugänge in geordneten Bahnen, damit Planungsbüros, freie Träger und Gremienmitglieder nicht über Umwege eingebunden werden.

Für die Gästeseite: [Gäste in Teams und SharePoint: Planungsbüros, Träger und Gremienmitglieder sicher einbinden](#). Und weil an dieser Stelle immer die Frage nach der Aktenführung kommt: Eine SharePoint-Struktur ist kein Ersatz für eine E-Akte nach den Landes-E-Government-Gesetzen. Sie kann Ablage, Zusammenarbeit und Aufbewahrung sehr gut abbilden; die Anforderungen an eine ordnungsgemäße elektronische Aktenführung – Vollständigkeit, Nachvollziehbarkeit, Unveränderbarkeit im Sinne des Fachrechts – deckt sie ohne zusätzliche Festlegungen nicht ab. Wo genau die Grenze liegt, hängt vom Landesrecht ab und ist in [SharePoint als E-Akte? Was geht, was nicht und wo die Grenze nach Landesrecht liegt](#) ausgeführt.

Zur Struktur gehört auch die Schulung. Der weitaus größte Teil aller Fundstellen entsteht nicht durch Böswilligkeit oder Unkenntnis der Regeln, sondern dadurch, dass die Beschäftigten den Unterschied zwischen einem Freigabelink, einer Gruppenmitgliedschaft und einer Websiteberechtigung nicht kennen. Diese drei Begriffe in einer halben Stunde zu erklären, ist die günstigste Präventionsmaßnahme, die Sie haben.

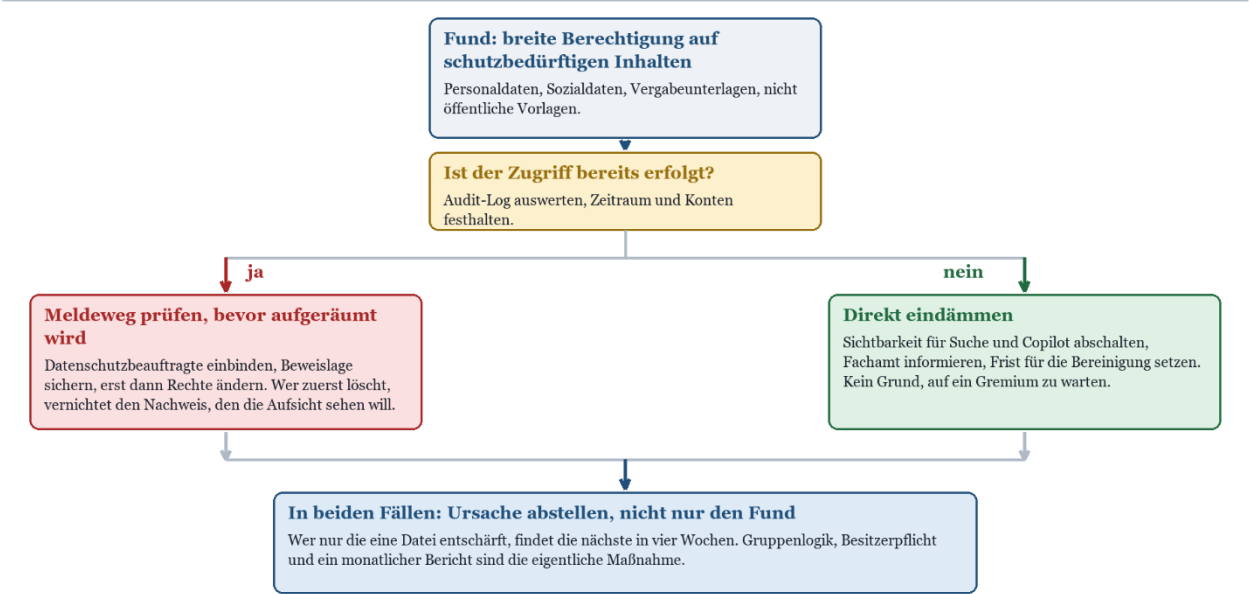
Passende Formate dafür: [Microsoft-365-Schulung für Verwaltungen](#).

Phase 4: Dauerbetrieb – der Teil, den alle unterschätzen

Ein einmaliges Aufräumen hält etwa achtzehn Monate. Danach ist der Zustand wieder da, weil die Ursachen weiterlaufen: neue Projekte, neue Teams, Amtswechsel, Vertretungsregelungen. Der Dauerbetrieb braucht deshalb drei Bausteine, die alle wenig Aufwand kosten, wenn sie einmal stehen.

- Ein monatlicher Bericht über neu entstandene breite Freigaben, ausgewertet in einer festen Runde aus IT, Datenschutz und Organisationsamt. Zwanzig Minuten, feste Tagesordnung.
- Turnusmäßige Zugriffsüberprüfungen, delegiert an die Websitebesitzer, mit Rücklaufquote als Kennzahl. Wer nicht antwortet, bekommt die Einschränkung der Auffindbarkeit – das erhöht die Rücklaufquote erfahrungsgemäß deutlich.
- Eine Bestätigungspflicht für Websitebesitzer: einmal im Jahr bestätigen, dass die Website noch gebraucht wird, die Angaben stimmen und die Berechtigungen passen. Ohne Bestätigung startet ein definierter Auflösungsprozess.

Fundstelle auf dem Tisch – und jetzt?



Skizze 5: Die Reihenfolge entscheidet, ob am Ende ein Nachweis oder eine Erinnerungslücke steht.

Skizze 5: Der Entscheidungsweg für die einzelne Fundstelle.

Phase	Zeiträumen	Wer führt	Ergebnis	Woran Sie den Abschluss erkennen
0 – Eindämmen	Tage 1 bis 5	IT-Leitung	Schwerste Fundstellen sind für Suche und Copilot unsichtbar	Liste der eingeschränkten Websites, dokumentiert und begründet
1 – Eigentümer	Wochen 1 bis 3	Organisationsamt	Jede Fundstelle hat ein Amt und zwei benannte Besitzer	Keine Website mehr ohne aktive Besitzer in der Auswertung
2 – Bereinigen	Wochen 2 bis 8	Fachamt mit IT	Breite Berechtigungen und Altlinks sind entfernt	Rücklauf der Zugriffsüberprüfungen vollständig, Nachlauf dokumentiert
3 – Struktur	Monate 2 bis 6	Registratur mit IT	Gruppenlogik, Freigaberegeln, Aufbewahrung, Schulung stehen	Neue Websites entstehen im vorgesehenen Muster, nicht daneben
4 – Dauerbetrieb	ab Monat 3, laufend	IT mit Datenschutz	Monatsbericht, Überprüfungen, Bestätigungspflicht laufen	Zahl der neuen breiten Freigaben je Monat sinkt und bleibt niedrig

Was Sie parallel mit Personalrat, Datenschutz und Prüfung klären

Personalrat: Der Bericht über eine einzelne Person ist der heikle Punkt

Für den Personalrat ist Oversharing zunächst eine gute Nachricht – es geht schließlich darum, dass Personal­daten der Beschäftigten besser geschützt werden. Der Konflikt entsteht an einer anderen

Stelle: Der Bericht, der auflistet, auf welche Websites eine bestimmte Person zugreifen kann, ist personenbezogen. Er lässt sich für eine Bereinigung nutzen und ebenso für eine Verhaltenskontrolle.

Regeln Sie das vorab und schriftlich: zu welchem Zweck dieser Bericht erzeugt wird, wer ihn erzeugen darf, wie lange er aufbewahrt wird, und dass eine Auswertung zur Leistungs- oder Verhaltenskontrolle ausgeschlossen ist. Dasselbe gilt für die Auswertung des Prüfprotokolls. Wenn Sie ohnehin an einer Dienstvereinbarung zu Copilot arbeiten, gehört dieser Punkt hinein – er ist konkreter und leichter zu verhandeln als die abstrakte Frage nach der KI-Nutzung.

Bausteine und Formulierungsansätze dafür: [Copilot und Personalrat: Bausteine einer Dienstvereinbarung](#). Für kirchliche Träger mit Mitarbeitervertretung und den Datenschutzregelungen nach DSGVO oder KDG gilt das sinngemäß, siehe [Microsoft 365 in Kirche, Diakonie und Caritas: DSGVO, KDG und Mitarbeitervertretung](#).

Datenschutz: Fund ist nicht gleich Meldefall – aber die Prüfung ist Pflicht

Eine breite interne Berechtigung ist noch keine Datenschutzverletzung. Sie wird zu einer, wenn ein unbefugter Zugriff tatsächlich stattgefunden hat. Genau deshalb ist die Auswertung des Prüfprotokolls kein optionaler Nachgang, sondern Teil der Feststellung: Ohne sie können Sie die Frage nach dem tatsächlichen Zugriff nicht beantworten, und ohne diese Antwort lässt sich weder eine Meldung begründen noch eine unterbliebene Meldung.

Binden Sie die Datenschutzbeauftragte deshalb vor dem Aufräumen ein, nicht danach. Und halten Sie die Reihenfolge ein: dokumentieren, bewerten, dann bereinigen. Wer zuerst die Rechte entzieht, verändert den Zustand, den er hätte belegen müssen.

Die Rechtsgrundlagen für den Copilot-Einsatz selbst und die Frage nach der Datenschutz-Folgenabschätzung behandelt [Microsoft 365 Copilot in der Verwaltung: Datenschutz, Rechtsgrundlage, DSFA](#). Für die Einordnung des Schutzbedarfs nach IT-Grundschutz siehe [Schutzbedarf und Microsoft 365: IT-Grundschutz-Abgleich für die Praxis](#).

Rechnungsprüfungsamt: Was am Ende vorgelegt werden muss

Das Rechnungsprüfungsamt interessiert sich weniger für die Fundstellen als für den Prozess. Vier Nachweise sollten Sie erzeugen können: die datierte Fundliste zum Zeitpunkt der Feststellung, die Entscheidung über jede Fundstelle mit Begründung und Verantwortlichkeit, die Durchführung mit Zeitstempel, und den Nachweis, dass ein wiederkehrendes Verfahren eingerichtet wurde. Ein Bereinigungsprojekt ohne den vierten Punkt wird in der übernächsten Prüfung erneut aufschlagen.

Betriebsmodell und Delos Cloud: eine getrennte Frage

In der Diskussion taucht regelmäßig der Einwand auf, man müsse das Thema ohnehin nicht klären, weil man perspektivisch in eine souveräne Umgebung wechsele. Das trägt nicht. Oversharing ist ein Problem der Berechtigungspflege und der Ablagestruktur, nicht des Rechenzentrumsstandorts. Eine Fundliste, die heute 180 Konten mit Zugriff auf Sozialdaten ausweist, weist morgen in jeder anderen Umgebung dieselben 180 Konten aus – die Daten wandern schließlich mit, samt Berechtigungen.

Zur Delos Cloud nüchtern: Das Angebot richtet sich an die öffentliche Verwaltung in Deutschland und betreibt Microsoft-Technologie in einer eigenständig verantworteten Umgebung. Welche Dienste in welchem Umfang und Zeitrahmen verfügbar sind, entwickelt sich fortlaufend; belastbare Terminaussagen gehören nicht in einen Fachartikel, sondern in eine aktuelle Auskunft des Anbieters. Für Ihre Planung heißt das: Behandeln Sie die Betriebsmodellfrage und die

Oversharing-Bereinigung als zwei unabhängige Vorgänge. Die Bereinigung zahlt auf jede denkbare Zielarchitektur ein.

Zur Einordnung des Angebots: [Delos Cloud für Kommunen: Was das Angebot ist, wen es betrifft und was fehlt](#). Zur grundsätzlichen Betriebsmodellentscheidung und was daran wirklich zu entscheiden ist: [Microsoft 365 in der Kommune: Was Sie wirklich entscheiden müssen \(und was nicht\)](#).

Häufige Fragen

Können wir Copilot einfach abschalten, bis wir aufgeräumt haben?

Technisch ja, über die Lizenzzuweisung. Fachlich löst es nichts. Die Fundstellen bestehen unabhängig von Copilot, und die klassische Suche findet sie ebenfalls – nur langsamer. Sinnvoller ist die umgekehrte Reihenfolge: eindämmen, was schwer wiegt, und die Einführung in dem Bereich beginnen, den Sie bereits überprüft haben. Ein schrittweiser Rollout entlang der bereinigten Bereiche ist ohnehin das robustere Vorgehen.

Sieht Copilot auch Inhalte, auf die nur der Administrator Zugriff hat?

Nein. Copilot antwortet im Kontext des anfragenden Kontos und nutzt ausschließlich Inhalte, für die dieses Konto berechtigt ist. Der relevante Sonderfall ist ein anderer: Wenn Administrationskonten gleichzeitig als Arbeitskonten mit Copilot-Lizenz genutzt werden, kann deren sehr weiter Zugriff in Antworten einfließen. Trennen Sie diese Konten – das ist ohnehin eine Grundregel und in diesem Fall besonders sichtbar.

Unsere Beschäftigten haben doch Verschwiegenheitspflicht. Reicht das nicht?

Die Verschwiegenheitspflicht regelt, was jemand weitergeben darf. Sie regelt nicht, was jemand sehen darf. Der datenschutzrechtliche Maßstab ist die Erforderlichkeit für die jeweilige Aufgabe, und die ist bei 180 Konten mit Lesezugriff auf Bewilligungsbescheide schwer zu begründen. Zudem: Die Pflicht schützt nicht davor, dass eine Information in einer generierten Zusammenfassung auftaucht, die jemand ohne jede Absicht angefordert hat.

Wie lange dauert so eine Bestandsaufnahme?

Die technische Auswertung ist eine Frage von Tagen – die Berichte laufen weitgehend automatisiert, größere Läufe brauchen bis zu 24 Stunden. Der zeitkritische Teil ist die Zuordnung der Zuständigkeiten und die fachliche Bewertung. Für eine mittlere Stadtverwaltung sollten Sie für die Bestandsaufnahme inklusive Bewertung zwei bis vier Wochen ansetzen, für die Bereinigung der schwerwiegenden Fälle weitere sechs bis zehn Wochen. Häuser mit vielen inaktiven Websites liegen darüber.

Können wir die Bereinigung unserem Systemhaus oder dem kommunalen Rechenzentrum übertragen?

Die technische Umsetzung ja, und dort sitzt oft genau das Umgebungswissen, das eine externe Unterstützung erst mühsam aufbauen müsste. Was nicht delegierbar ist, sind zwei Dinge: die fachliche Entscheidung, ob ein Zugriff gewollt ist – das können nur Ihre Fachämter –, und die Verantwortung für die Verarbeitung, die bei Ihnen als verantwortlicher Stelle bleibt. Sinnvoll ist eine klare Rollenteilung, und je nach Konstellation eine unabhängige Zweitmeinung auf die Ergebnisse.

Zur Rollenteilung mit dem kommunalen Rechenzentrum: [Microsoft 365 und das kommunale Rechenzentrum: Rollen, Schnittstellen, Zweitmeinung.](#)

Was ist mit OneDrive? Da liegt doch auch alles Mögliche.

Zu Recht gefragt. OneDrive ist in mehreren Auswertungen nur eingeschränkt abgedeckt: Der Bericht zu breiten Freigaben in der Admin-Oberfläche betrachtet SharePoint-Websites, für OneDrive brauchen Sie den Weg über PowerShell. Die Auswertung auf Elementebene in der Risikobewertung unterstützt OneDrive derzeit nicht. Praktisch heißt das: OneDrive gehört in den Überprüfungsumfang, aber mit anderen Werkzeugen und meist im zweiten Durchgang.

Hilft es, die Website einfach aus der Suche zu nehmen?

Die Einstellung „Diese Website in Suchergebnissen anzeigen“ auf Nein zu setzen, ist ein Bordmittel und wirkt breiter als gedacht: Sie entfernt die Inhalte auch aus der websiteeigenen Suche, was die Beschäftigten, die dort arbeiten, unmittelbar behindert. Für eine gezielte Eindämmung ist die websitebezogene Einschränkung der Auffindbarkeit das passendere Mittel, weil sie die Arbeit vor Ort unberührt lässt. Beides bleibt eine Sichtbarkeitsmaßnahme, keine Berechtigung.

Wir haben keine Copilot-Lizenzen. Bekommen wir die Berichte trotzdem?

Die erweiterten Berichte hängen an der Copilot-Lizenzierung oder am eigenständigen Zusatzprodukt. Eine einzige zugewiesene Copilot-Lizenz im Tenant genügt, um die Governance-Funktionen zur Vorbereitung der Einführung freizuschalten – das ist für eine Bestandsaufnahme oft der pragmatische Weg. Ohne beides bleiben Ihnen die Bordmittel; damit kommen Sie an die Websiteebene heran, aber nicht an eine belastbare Auswertung auf Datei- und Linkebene.

Sollen wir vor der Bereinigung überhaupt schon eine Beschlussvorlage schreiben?

Ja, und zwar eine, die die Fundliste in aggregierter Form enthält – Anzahl der Fundstellen je Kategorie, Anzahl betroffener Konten, geschätzter Aufwand, Reihenfolge. Ohne Zahlen wird die Bereinigung als IT-Fleißarbeit wahrgenommen und bekommt keine Ressourcen. Mit Zahlen ist sie eine Risikoentscheidung der Verwaltungsspitze, und das ist sie auch.

Wie sich eine solche Vorlage zusammen mit dem Gesamtkonzept aufsetzen lässt, zeigt [Microsoft-365-Einführung in der Verwaltung: Konzeptionsphase in 4,5 Tagen und die Beschlussvorlage.](#)

Fazit

Copilot findet die Personalakte, weil sie auffindbar ist. Das ist keine Eigenschaft der Technik, sondern das Ergebnis von zehn Jahren pragmatischer Einzelentscheidungen, die in der Papierwelt folgenlos geblieben wären. Der Umgang damit ist unangenehm, aber er ist beherrschbar – und er ist unabhängig davon notwendig, ob Sie Copilot einführen, verschieben oder ganz sein lassen.

Drei Punkte, die den Unterschied machen. Erstens die Reihenfolge: eindämmen, verstehen, bereinigen, strukturieren, dauerhaft überwachen. Wer mit dem Berechtigungskonzept beginnt, trägt das Risiko anderthalb Jahre länger als nötig. Zweitens die Arbeitsteilung: Die IT liefert Fundlisten, die Fachämter liefern Entscheidungen. Jeder Versuch, das zu vertauschen, endet in einer Warteschleife. Drittens der Dauerbetrieb: Ein einmaliges Aufräumen hält knapp anderthalb Jahre, ein monatlicher Bericht hält dauerhaft.

Und ein letzter Gedanke für die Verwaltungsspitze: Die unangenehmste Variante ist nicht, dass die Fundstellen existieren. Die unangenehmste Variante ist, dass sie existieren und im Pilotbetrieb von

einer beliebigen Person entdeckt werden, statt vorher von Ihnen. Der Unterschied zwischen beidem ist ein Vorlauf von wenigen Wochen.

TIPP · Weiter im Thema

- › Rechtsgrundlage, Verarbeitungsverzeichnis und Folgenabschätzung für den Copilot-Einsatz
- › Bausteine für die Dienstvereinbarung mit dem Personalrat
- › Die Grenze zwischen SharePoint-Ablage und E-Akte nach Landesrecht
- › Informationsarchitektur entlang der Ämter als dauerhafte Lösung
- › Nachweise für Rechnungsprüfung und Aufsicht aus dem Prüfprotokoll

[Microsoft 365 Copilot in der Verwaltung: Datenschutz, Rechtsgrundlage, DSFA](#) · [Copilot und Personalrat: Bausteine einer Dienstvereinbarung](#) · [SharePoint als E-Akte? Was geht, was nicht und wo die Grenze nach Landesrecht liegt](#) · [Microsoft Teams in der Verwaltung einführen: Informationsarchitektur entlang der Ämter](#) · [Microsoft 365 Audit-Log und Rechnungsprüfung: Nachweise, die Verwaltungen liefern müssen](#)

Ergänzend zur Absicherung des Betriebs: [Backup und Wiederherstellung in Microsoft 365: Die Risikoentscheidung fürs Rechnungsprüfungsamt](#) und [Notfallübung für die Verwaltungs-IT: SharePoint verschlüsselt, Admin-Konto übernommen, Bürgertelefon tot.](#)