

Schutzbedarf und Microsoft 365: IT-Grundschutz-Abgleich für die Praxis

Es gibt in deutschen Verwaltungen ein Dokument, das in erstaunlich vielen Häusern existiert, ordentlich abgeheftet ist, eine Beschlussnummer trägt — und trotzdem keinerlei Wirkung entfaltet: die Schutzbedarfsfeststellung. Sie wurde erstellt, weil der IT-Grundschutz sie verlangt, sie wurde vom Rechnungsprüfungsamt zur Kenntnis genommen, und dann ist sie in den Aktenplan gewandert. Was danach im Tenant passiert, hat mit ihr ungefähr so viel zu tun wie der Brandschutzplan mit der tatsächlich zugestellten Fluchttür.

Das ist keine Bosheit und auch keine Schlamperei. Es liegt daran, dass zwischen der Feststellung „Personalakten haben einen hohen Schutzbedarf hinsichtlich der Vertraulichkeit“ und der Frage „welches Häkchen setze ich in welchem Admin Center“ eine Übersetzungslücke klafft, für die sich niemand zuständig fühlt. Die Informationssicherheitsbeauftragten sprechen Grundschutz. Die Systemadministration spricht Purview, Entra und SharePoint. Beide reden über dieselbe Personalakte und meinen dabei völlig unterschiedliche Objekte.

Dieser Beitrag schließt genau diese Lücke. Er zeigt, wie Sie eine Schutzbedarfsfeststellung so aufsetzen, dass sie sich in Tenant-Einstellungen übersetzen lässt, welche Maßnahme zu welcher Schutzstufe gehört, und wo die ehrlichen Grenzen liegen. Vorweg die wichtigste Botschaft, weil sie in Verwaltungsdiskussionen regelmäßig falsch gedreht wird: Ein hoher Schutzbedarf ist kein Cloud-Verbot. Er ist eine Konfigurationsaufgabe mit Nachweispflicht.

Dieser Beitrag gehört zur Serie [Microsoft 365 in der öffentlichen Verwaltung](#). Dort finden Sie den Gesamtzusammenhang von Betriebsmodell, Beschaffung, Datenschutz und Betrieb. Wenn Sie noch vor der Grundsatzentscheidung stehen, lesen Sie zuerst [Microsoft 365 in der Kommune: Was Sie wirklich entscheiden müssen \(und was nicht\)](#). Die Schutzbedarfsfeststellung kommt danach — aber vor dem ersten produktiven Team.

FAKTEN: Der methodische Rahmen in drei Sätzen

Der BSI-Standard 200-2 beschreibt die IT-Grundschutz-Methodik und kennt für jedes der drei Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit die Kategorien normal, hoch und sehr hoch. Die Einstufung erfolgt über Schadensszenarien, nicht über Bauchgefühl.

Für die Cloud-Nutzung ist der Baustein OPS.2.2 des IT-Grundschutz-Kompendiums einschlägig; hinzu kommen bausteinübergreifend Identitäts- und Berechtigungsverwaltung, Protokollierung und Datensicherung.

Mit IT-Grundschutz++ stellt das BSI das Kompendium seit 2026 auf ein maschinenlesbares, OSCAL-basiertes Format um und konsolidiert die Anforderungslandschaft erheblich. Die Edition 2023 bleibt in einer mehrjährigen Parallelphase maßgeblich — Ihre laufende Feststellung wird davon nicht wertlos, sie sollte aber strukturiert genug sein, um später übernommen zu werden.

Der Perspektivwechsel: Informationsarten statt IT-Systeme

Die häufigste Ursache dafür, dass eine Schutzbedarfsfeststellung im Microsoft-365-Kontext nicht funktioniert, ist ein methodischer Kurzschluss aus der Serverwelt. Dort war die Zuordnung einfach: Es gab den Personalserver, und der Personalserver hatte einen hohen Schutzbedarf. Fertig. Ein Tenant hat aber keinen Personalserver. Er hat einen SharePoint-Dienst, in dem gleichzeitig das Amtsblatt, der Kantinenspeiseplan und Beihilfeunterlagen liegen — und zwar in derselben technischen Plattform, unter derselben Verwaltung, mit derselben Suchmaschine darüber.

Wer in dieser Lage das IT-System einstuft, landet zwangsläufig beim Maximumprinzip und damit bei der Aussage: Der gesamte Tenant hat einen hohen Schutzbedarf. Das ist formal nicht falsch, praktisch aber wertlos. Aus einer solchen Aussage lässt sich keine einzige differenzierte Einstellung ableiten. Sie führt entweder zur Vollbremsung („dann eben keine Cloud“) oder zur Beruhigungspille („wir haben ja Multifaktor“). Beides ist kein Sicherheitskonzept.

Der Aktenplan ist Ihre beste Quelle

Der Ausweg ist unspektakulär und liegt in fast jeder Verwaltung bereits im Regal: Nehmen Sie den Aktenplan. Er ist die einzige Liste im Haus, die Informationen nach fachlicher Bedeutung ordnet statt nach technischem Speicherort. Ein Aktenplan nach kommunalem Schema ist zwar nicht als Sicherheitsinstrument gedacht, aber er beantwortet genau die Frage, die Sie brauchen: Welche Arten von Information entstehen in diesem Haus?

In der Praxis reduzieren Sie den Aktenplan dabei erheblich. Eine mittlere Stadtverwaltung hat in der Feinsystematik mehrere hundert Positionen, aber nur zwölf bis zwanzig unterscheidbare Informationsarten aus Sicherheitssicht. Beihilfeunterlagen, Beurteilungen und Schwerbehindertendaten sind rechtlich verschieden, sicherheitstechnisch aber dieselbe Klasse: personenbezogene Daten Beschäftigter mit hohem Vertraulichkeitsbedarf. Zwölf bis zwanzig Klassen sind handhabbar. Dreihundert sind es nicht.

Wie Sie vom Aktenplan zur Aufbewahrungsbezeichnung kommen und wo die Metadatenstruktur in SharePoint dafür hinreicht, ist Thema von [Schriftgutverwaltung mit Microsoft 365: Vom Aktenplan zur Aufbewahrungsbezeichnung](#). Für die Schutzbedarfsfeststellung reicht die grobe Ebene — Sie klassifizieren Informationsarten, nicht einzelne Vorgänge.

Drei Schutzziele, drei getrennte Antworten

Ein Fehler, der sich hartnäckig hält: Der Schutzbedarf wird als eine einzige Zahl geführt. „Sozialdaten: hoch.“ Das verschenkt die halbe Aussagekraft. Der IT-Grundschutz fragt getrennt nach Vertraulichkeit, Integrität und Verfügbarkeit, und in der Verwaltung fallen die Antworten auffallend oft auseinander.

Eine öffentliche Ratsinformation hat definitionsgemäß keinen Vertraulichkeitsbedarf — sie soll ja gelesen werden. Ihre Integrität ist dagegen erheblich: Wenn jemand die Beschlussvorlage nachträglich verändert, ist der Beschluss angreifbar. Umgekehrt hat eine Sicherheitsüberprüfung eine sehr hohe Vertraulichkeit, aber eine bescheidene Verfügbarkeitsanforderung; wenn die Datei zwei Tage nicht erreichbar ist, geschieht nichts. Das Bürgertelefon hingegen hat überhaupt keinen Vertraulichkeitsbedarf und eine sehr hohe Verfügbarkeitsanforderung.

Diese Differenzierung ist kein akademischer Luxus. Sie entscheidet darüber, welche Maßnahme Sie ergreifen. Vertraulichkeit übersetzt sich in Verschlüsselung und Zugriffsbeschränkung. Integrität übersetzt sich in Versionierung, Aufbewahrungsrichtlinien und Protokollierung. Verfügbarkeit übersetzt sich in Betriebsmodell, Ausweichverfahren und Wiederherstellungskonzept. Wer alles in einen Topf wirft, verschlüsselt am Ende das Amtsblatt und sichert die Personalakte nicht.

Informationsart	Vertraulichkeit	Integrität	Verfügbarkeit	Kritischer Punkt
Amtsblatt, öffentliche Ratsinformation	normal	hoch	normal	Nachträgliche Veränderung von Beschlussunterlagen
Interne Dienstanweisungen, Organigramme	normal	normal	normal	Unproblematisch, gehört in den offenen Bereich
Sitzungsvorlagen nicht öffentlicher Teil	hoch	hoch	normal	Vorzeitiges Bekanntwerden vor der Beschlussfassung
Vergabeunterlagen vor	hoch	hoch	hoch	Wettbewerbsverzerrung, Rügen,

Zuschlag				Nachprüfungsverfahren
Personalvorgänge und Beurteilungen	hoch	hoch	normal	Mitbestimmung, Fürsorgepflicht, Persönlichkeitsrecht
Sozialdaten aus Jugend- und Sozialamt	hoch	hoch	hoch	Besondere Kategorien, teils lebensrelevante Vorgänge
Melde- und Ausweisdaten	hoch	sehr hoch	hoch	Auskunftssperren, Manipulation an Identitätsdaten
Bauakten mit Betriebsgeheimnissen	hoch	normal	normal	Geschäftsgeheimnisse Dritter im eigenen Haus
Kassen- und Zahlungsverkehrsdaten	hoch	sehr hoch	hoch	Zahlungsmanipulation, Chefmasche, Vier-Augen-Prinzip
Vorgänge mit Verschlusssachen-Charakter	sehr hoch	sehr hoch	normal	Gehört in der Regel nicht in den Standard-Tenant
Leitsysteme Wasser, Abwasser, Verkehr	hoch	sehr hoch	sehr hoch	Kritische Dienstleistung, eigene Regulierung

Beispielhafte Einstufung typischer Informationsarten. Die Werte sind ein Diskussionsangebot, keine Vorgabe — die Bewertung müssen Sie mit Ihren Fachämtern und der Datenschutzbeauftragung selbst vornehmen.

Maximum, Kumulation, Verteilung — die drei Effekte

Die Methodik kennt drei Effekte bei der Vererbung des Schutzbedarfs, und alle drei haben im Tenant eine sehr konkrete Entsprechung.

- **Maximumprinzip:** Der Schutzbedarf einer Site richtet sich nach der schutzbedürftigsten Information darin. Eine Team-Site, in der neben Protokollen auch ein einziger Personalvorgang liegt, ist eine Personalvorgangs-Site. In der Praxis ist genau das der Normalfall — und der Grund, warum saubere Informationsarchitektur mehr Sicherheit bringt als jedes zusätzliche Werkzeug.
- **Kumulationseffekt:** Viele Einzelinformationen mit normalem Bedarf ergeben in Summe einen hohen Bedarf. Ein Verzeichnis mit dreißig Anschriften ist harmlos. Das vollständige Melderegister als Auszug in einer Excel-Datei auf einer offenen Site ist es nicht. Cloud-Plattformen begünstigen Kumulation, weil Zusammenführen technisch trivial ist.
- **Verteilungseffekt:** Wird eine Information so aufgeteilt, dass die Teile für sich unkritisch sind, sinkt der Bedarf. Das klingt elegant, funktioniert im Dokumentenkontext aber selten. Verlassen Sie sich nicht darauf, außer Sie können die Trennung technisch erzwingen.

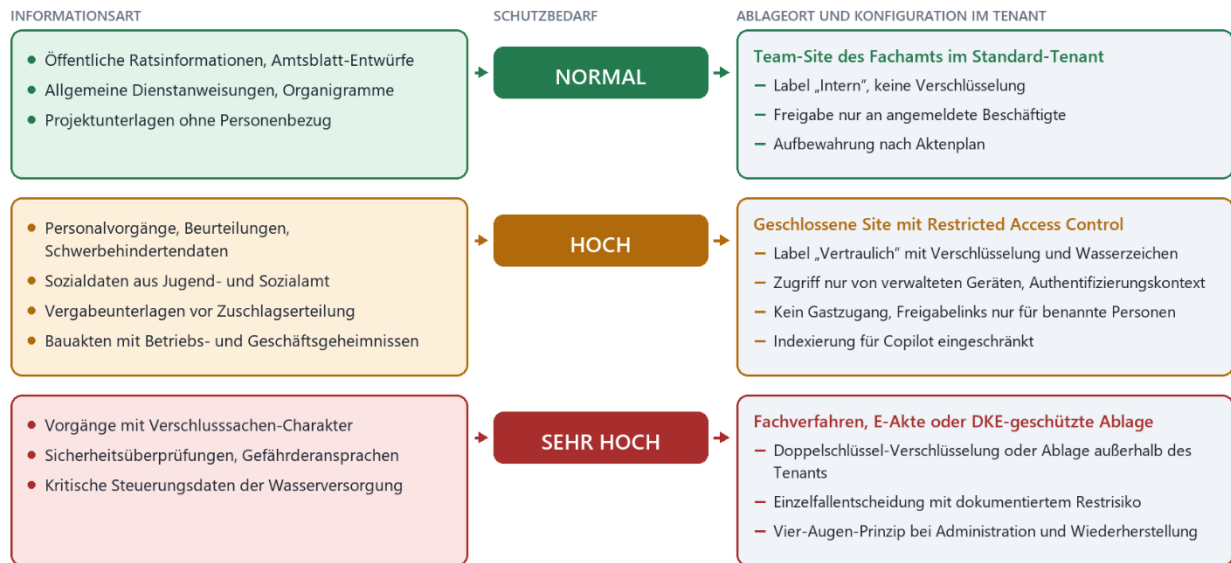
WARNUNG: Der Kumulationseffekt ist der eigentliche Cloud-Effekt

In einem Aktenschrank kumuliert nichts, weil niemand vierhundert Ordner gleichzeitig aufschlägt. In einem Tenant mit organisationsweiter Suche und einem Assistenzsystem darüber kumuliert alles, was ein Konto lesen darf, in dem Moment, in dem jemand eine Frage stellt.

Das ist kein Argument gegen die Cloud. Es ist ein Argument dafür, den Kumulationseffekt in der Feststellung ausdrücklich zu bewerten und daraus Sichtbarkeitsregeln abzuleiten — nicht erst dann, wenn die Assistenzfunktion bereits ausgerollt ist.

Informationsarten und Ablageorte

Nicht das IT-System bestimmt den Schutzbedarf, sondern die Information, die darin liegt



Der Ablageort folgt der Informationsart. Wo Landesrecht die führende Akte im E-Akte-System verlangt, bleibt SharePoint Arbeitsraum und wird nicht zum Aktensystem.

Skizze 1: Informationsarten, Schutzbedarf und die daraus folgenden Ablageorte im Tenant.

Die Übersetzung: von der Schutzstufe zur Tenant-Einstellung

Jetzt kommt der Teil, den die meisten Sicherheitskonzepte auslassen. Sie haben zwölf Informationsarten mit je drei Schutzzielen bewertet. Was folgt daraus technisch? Die Antwort besteht aus drei Bausteinen, die zusammen wirken müssen: einem Label, das die Stufe transportiert, einer Zugriffsregel, die sie durchsetzt, und einem Speicherort, der zu ihr passt. Fehlt einer der drei, ist die Wirkung gleich null.

Vom Schutzbedarf zur Tenant-Einstellung

Fünf Schritte, die eine Schutzbedarfsfeststellung in konfigurierte Wirklichkeit übersetzen



Jährliche Fortschreibung: neue Fachverfahren, neue Ämter, neue Funktionen

Die Schritte drei und vier sind der eigentliche Grundschutz-Abgleich. Wer bei Schritt zwei aufhört, hat ein Dokument, aber keinen konfigurierten Tenant.

Skizze 2: Der Übersetzungspfad von der Informationsart bis zum prüffähigen Nachweis.

Labels: der Träger der Schutzstufe

Vertraulichkeitsbezeichnungen aus Microsoft Purview sind das naheliegende Vehikel, weil sie das Einzige sind, das gleichzeitig am Dokument, an der E-Mail, am Team und an der Site hängen kann. Für die Verwaltung heißt das: Sie bilden Ihre Schutzstufen eins zu eins auf Labels ab und widerstehen der Versuchung, für jedes Amt ein eigenes zu bauen.

Vier bis fünf Labels sind das Maximum, das eine Sachbearbeitung im Alltag korrekt auseinanderhält. Bewährt hat sich: „Öffentlich“, „Intern“, „Vertraulich“ und „Streng vertraulich“, wobei die letzten beiden Unterbezeichnungen für Sonderfälle tragen können. Wichtig ist die Reihenfolge, denn die Priorität der Bezeichnungen entscheidet, was passiert, wenn ein höher eingestuftes Dokument in einer niedriger eingestuften Site landet. Microsoft 365 blockiert das nicht, sondern erzeugt ein Prüfereignis mit dem Namen „Detected document sensitivity mismatch“ und benachrichtigt die Person, die hochgeladen hat, sowie die Site-Verantwortlichen. Genau dieses Ereignis ist Ihr späterer Nachweis, dass Fehlalagen erkannt werden — heben Sie es auf, statt die Benachrichtigung abzuschalten.

Ein Detail, das in Projekten regelmäßig Ärger macht: Bezeichnungen für Container müssen zunächst in Entra ID freigeschaltet und synchronisiert werden, und die Wirkung tritt zeitversetzt ein. Rechnen Sie bei neuen Bezeichnungen mit rund einer Stunde, bei Änderungen an bestehenden mit vierundzwanzig Stunden, und bei Einstellungen zu geteilten Kanälen ebenfalls mit vierundzwanzig Stunden. Wer während eines Workshops eine Bezeichnung anlegt und sie sofort vorführen will, steht dumm da. Planen Sie das ein.

Zugriffsregeln: Container-Label und Conditional Access

Ein Label am Dokument allein schützt wenig, wenn der Raum darum offen steht. Der stärkere Hebel liegt beim Container. Eine Vertraulichkeitsbezeichnung, die auf ein Team, eine Microsoft-365-Gruppe oder eine SharePoint-Site angewendet wird, kann eine ganze Reihe von Einstellungen setzen und festnageln: ob die Gruppe öffentlich oder privat ist, ob Gäste hinzugefügt werden dürfen, ob und an wen aus der Site heraus extern freigegeben werden darf, ob der Zugriff von nicht verwalteten Geräten blockiert oder auf die Browseransicht beschränkt wird, welcher Authentifizierungskontext gilt, ob ein privates Team überhaupt auffindbar ist und ob andere Teams in geteilte Kanäle eingeladen werden dürfen. Per PowerShell kommen der Standardtyp des Freigabelinks und die Einstellung hinzu, ob Mitglieder überhaupt teilen dürfen.

Damit haben Sie fast alles, was eine Verwaltung braucht — mit einem einzigen Objekt, das die Site-Verantwortlichen selbst setzen können. Und genau das ist auch die Gefahr: Sobald Sie Freigabe- und Kontexteinstellungen an das Label hängen, können Site-Verantwortliche diese Einstellungen durch einen Labelwechsel ändern. Das ist gewollte Delegation, muss aber in der Dienstanweisung stehen und geschult werden.

Der Authentifizierungskontext ist der Punkt, an dem Purview und Entra ineinandergreifen: Sie definieren im Regelwerk der bedingten Zugriffe, was für diesen Kontext gilt — mehrstufige Anmeldung, konformes Gerät, Nutzungsbedingungen — und hängen ihn dann an das Label. Wie ein solches Regelwerk für Rathaus, Bauhof und Homeoffice aussieht, ohne die Außendienstkräfte auszusperrern, beschreibt [Conditional Access für Verwaltungen: Regelwerk für Rathaus, Bauhof und Homeoffice](#).

Zwei Einschränkungen gehören in jedes Konzept, weil sie sonst im Betrieb hochkommen. Erstens greift die Einstellung für nicht verwaltete Geräte nur, wenn die zugehörige Richtlinie für app-erzwungene Beschränkungen tatsächlich existiert; ohne sie ist das Häkchen im Label wirkungslos. Und sie greift nur, wenn sie mindestens so restriktiv ist wie die mandantenweite Einstellung. Zweitens unterstützen nicht alle Anwendungen Authentifizierungskontexte: Die Teams-Anwendung für Windows und macOS tut es, der Teams-Webclient nicht; der OneDrive-

Synchronisierungsclient unterstützt sie nur für OneDrive und unter Android gar nicht; Abläufe mit Power Apps und Power Automate können ebenso stolpern wie Anwendungen von Drittanbietern. Wer den Kontext an eine Site hängt, auf die eine Fachanwendung zugreift, sollte das vorher testen.

Speicherorte: die dritte Zutat

Die dritte Frage ist die unbequemste: Gehört diese Informationsart überhaupt hierhin? Für den Großteil des Verwaltungsschriftguts lautet die Antwort ja, und zwar mit den beschriebenen Einstellungen. Für einen kleinen Rest lautet sie nein — und zwar nicht, weil die Cloud unsicher wäre, sondern weil ein Fachverfahren die fachlich richtige Ablage ist.

Hier verläuft auch die Grenze, die in Schriftgut-Projekten am häufigsten verwischt wird: SharePoint ist ein hervorragender Arbeitsraum und ein brauchbares Ablagesystem, aber die führende Akte im Sinne der E-Government-Gesetze der Länder ist es in aller Regel nicht. Wo Ihr Landesrecht ein Aktensystem mit bestimmten Eigenschaften verlangt, bleibt SharePoint davor — nicht dahinter. Die Abgrenzung im Detail behandelt [SharePoint als E-Akte? Was geht, was nicht und wo die Grenze nach Landesrecht liegt](#). Prüfen Sie das jeweils gegen die Regelungen Ihres Landes; die Unterschiede zwischen den Bundesländern sind erheblich, und dieser Beitrag ersetzt keine rechtliche Prüfung.

Bei einer Stadtverwaltung, die SharePoint im Sozialbereich einsetzen wollte, hat genau diese Unterscheidung das Projekt gerettet. Die ursprüngliche Idee war, die Hilfeplanung vollständig in SharePoint zu führen. Nach der Schutzbedarfsbetrachtung blieb ein deutlich kleinerer, dafür tragfähiger Zuschnitt: Zusammenarbeit, Terminabstimmung, Entwürfe und Protokolle in einer geschlossenen Site mit eingeschränkter Zugriffssteuerung; die Falldokumentation weiterhin im Fachverfahren. Das war unspektakulär, aber es hat funktioniert — und es war gegenüber der Aufsicht erklärbar.

Die Übersetzungstabelle

Die folgende Tabelle ist der Kern dieses Beitrags. Sie ordnet jedem Maßnahmenfeld eine Ausprägung je Schutzstufe zu. Nehmen Sie sie als Vorlage, streichen Sie, was nicht passt, und ergänzen Sie, was Ihr Haus zusätzlich braucht. Wichtig ist nicht, dass Sie meine Zuordnung übernehmen — wichtig ist, dass Ihre Feststellung am Ende eine solche Tabelle enthält.

Maßnahmenfeld	Schutzbedarf normal	Schutzbedarf hoch	Schutzbedarf sehr hoch
Vertraulichkeitsbezeichnung	„Intern“, ohne Verschlüsselung, Kennzeichnung optional	„Vertraulich“ mit Verschlüsselung, Kopf- oder Fußzeile, Wasserzeichen	Eigene Unterbezeichnung, Doppelschlüssel oder Ablage außerhalb des Tenants
Container-Einstellung	Team öffentlich möglich, Gäste nach Regelwerk	Team zwingend privat, Gastzugang gesperrt, private Teams nicht auffindbar	Eingeschränkte Zugriffssteuerung auf eine benannte Sicherheitsgruppe
Externe Freigabe	Für angemeldete externe Personen nach Freigabeprozess	Nur bestehende Gäste, keine anonymen Links, Standardlink „bestimmte Personen“	Keine externe Freigabe, Mitglieder dürfen nicht teilen
Gerätezugriff	Zugriff von privaten Geräten browserbasiert zulässig	Nur verwaltete und konforme Geräte, Download blockiert oder begrenzt	Nur verwaltete Geräte im definierten Netz, kein Synchronisierungsclient
Anmeldung	Phishing-resistente	Zusätzlicher	Kontext mit

	Mehrfaktoranmeldung als Grundlinie	Authentifizierungskontext, kürzere Sitzungsdauer	Nutzungsbedingungen, Anmeldung nur aus benannten Netzen
Speicherort	SharePoint, Teams, OneDrive im Standard-Tenant	Dedizierte Site mit eigener Berechtigungslogik, keine OneDrive-Ablage	Fachverfahren, E-Akte oder gesonderte Umgebung nach Einzelfallprüfung
Sichtbarkeit für Suche und Assistenz	Volle Indexierung, organisationsweite Suche	Eingeschränkte Auffindbarkeit für die Site, Prüfung vor Assistenzeinsatz	Von Index und Assistenzfunktionen ausgenommen
Aufbewahrung und Aussonderung	Aufbewahrungsbezeichnung nach Aktenplan, automatische Zuweisung	Bezeichnung mit Prüfschritt vor Löschung, Vier-Augen-Prinzip	Manuelle Disposition mit dokumentiertem Vernichtungsnachweis
Protokollierung	Standardprotokollierung des Prüfprotokolls	Verlängerte Aufbewahrung, Auswertung von Zugriffs- und Freigabeereignissen	Zusätzliche Ausleitung in ein eigenes Auswertungssystem
Administration	Rollenbasiert, getrennte Verwaltungskonten	Zeitlich begrenzte Rechteerhöhung mit Genehmigung und Begründung	Vier-Augen-Prinzip, Genehmigung durch eine zweite Person, enge Zeitfenster
Wiederherstellung	Plattformmechanismen und Versionierung genügen	Zusätzliche Sicherung mit definierter Wiederherstellungszeit	Getestete Wiederherstellung mit Nachweis, jährliche Übung
Verschlüsselungsschlüssel	Microsoft-verwaltet	Microsoft-verwaltet, Kundenschlüssel bei begründetem Ausstiegsszenario	Doppelschlüssel oder Verzicht auf die Plattform für diese Informationsart

Übersetzungstabelle Schutzbedarf zu Maßnahme in Microsoft 365. Die Spalte „sehr hoch“ ist bewusst die kürzeste — dort geht es weniger um Konfiguration als um die Frage, ob die Informationsart überhaupt in den Tenant gehört.

WARNUNG: Schutzbedarf „hoch“ ist kein Cloud-Verbot

In Verwaltungsdiskussionen wird die Einstufung „hoch“ regelmäßig als Ausschlusskriterium behandelt: hoher Schutzbedarf, also keine Cloud, Diskussion beendet. Diese Schlussfolgerung steht so weder im BSI-Standard 200-2 noch im Baustein zur Cloud-Nutzung. Der Grundschutz sagt: Bei hohem Schutzbedarf reichen die Basis-Anforderungen nicht aus, es sind zusätzliche Maßnahmen erforderlich, und die Restrisiken sind von der Leitung zu tragen und zu dokumentieren.

Das ist ein Arbeitsauftrag, kein Verbot. Er lautet: zusätzliche Maßnahmen festlegen, umsetzen, wirksam halten und nachweisen. Genau dafür ist die Übersetzungstabelle oben da. Wer die Einstufung „hoch“ als Cloud-Verbot liest, spart sich die Arbeit — und handelt sich dafür ein anderes Problem ein, nämlich Schattenlösungen. Der Personalvorgang, der nicht in die geschützte Site darf, landet dann als Anhang im privaten Postfach.

Umgekehrt gilt genauso: „hoch“ ist auch kein Freibrief. Wenn Sie die zusätzlichen Maßnahmen nicht umsetzen können oder wollen, dann ist die Antwort tatsächlich nein — aber dann sagen Sie das begründet und nicht mit Verweis auf eine Regel, die es so nicht gibt.

TIPP: Zwei Spalten, die Ihre Tabelle zusätzlich braucht

Ergänzen Sie die Übersetzungstabelle um eine Spalte „umgesetzt am“ und eine Spalte „geprüft am, durch wen“. Damit wird aus dem Konzept ein Nachweis. Das Rechnungsprüfungsamt fragt nicht, was Sie sich vorgenommen haben, sondern was gilt und woher Sie das wissen.

Ergänzen Sie außerdem eine Spalte „Lizenzvoraussetzung“. Ein erheblicher Teil der Maßnahmen in der Spalte „hoch“ setzt Funktionen voraus, die nicht in jedem Plan enthalten sind. Diese Prüfung gehört in die Feststellung und nicht erst in die Rechnung.

„Sehr hoch“: die ehrliche Grenzbetrachtung

Über den Schutzbedarf „normal“ streitet niemand, über „hoch“ lässt sich sachlich arbeiten. Interessant und unangenehm wird es bei „sehr hoch“. Hier gilt eine einfache Wahrheit, die man in Verwaltungspräsentationen selten so klar formuliert sieht: Sie können in Microsoft 365 sehr weitgehende Vertraulichkeit herstellen, aber Sie bezahlen dafür mit Funktion. Die Frage ist nicht, ob es geht, sondern was danach noch geht.

Doppelschlüssel-Verschlüsselung und ihr Preis

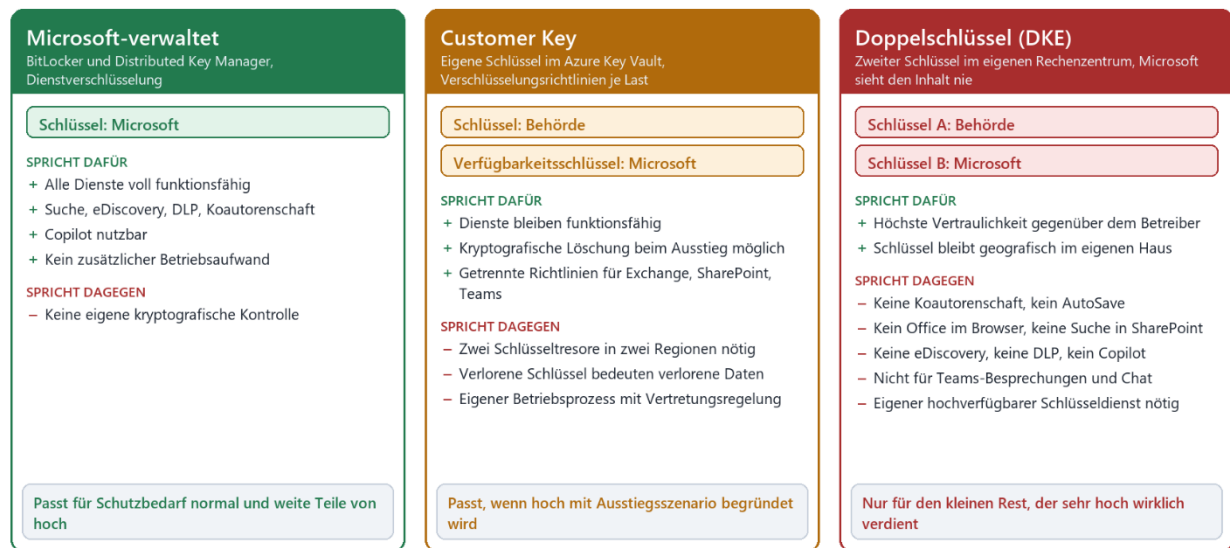
Die Doppelschlüssel-Verschlüsselung schützt Inhalte mit zwei Schlüsseln: einem, den Microsoft in Azure verwahrt, und einem zweiten, den Sie in einem eigenen Dienst betreiben — im eigenen Rechenzentrum oder bei einem Betreiber Ihrer Wahl. Ohne beide Schlüssel ist der Inhalt nicht lesbar. Für Microsoft ist er damit faktisch nicht zugänglich. Das ist genau die Eigenschaft, die viele Informationssicherheitsbeauftragte suchen.

Die Kehrseite ist konsequent, und Microsoft benennt sie in der eigenen Dokumentation ungewöhnlich offen. Was mit doppelt verschlüsselten Inhalten nicht mehr funktioniert: gemeinsames Bearbeiten und automatisches Speichern, das Öffnen im Browser, Suche und Indexierung in SharePoint und OneDrive, elektronische Beweissicherung, Verlustvermeidungsrichtlinien, die Verwendung als Standardbezeichnung einer Dokumentbibliothek, Loop-Komponenten sowie Teams-Besprechungen und Chats. Und die Assistenzfunktionen sehen den Inhalt ebenfalls nicht — weder im Ruhezustand noch während der Bearbeitung in den aktuellen Office-Versionen. Ablegen können Sie solche Dateien in SharePoint und OneDrive, ansehen müssen Sie sie in der Anwendung auf dem Arbeitsplatzrechner.

Damit ist klar, wofür das Verfahren taugt und wofür nicht. Es taugt für einen kleinen, klar abgegrenzten Bestand, an dem nicht kollaborativ gearbeitet wird. Es taugt nicht als Grundeinstellung für ein ganzes Amt. Microsoft selbst beschreibt die typische Verteilung so: rund 80 Prozent unkritische Daten, rund 15 Prozent schützenswerte Daten, für die Klassifizierung und Zugriffssteuerung der richtige Weg sind, und rund 5 Prozent Kronjuwelen. Diese Verteilung deckt sich gut mit dem, was Verwaltungen finden, wenn sie ihren Aktenplan ehrlich durchgehen.

Wer hält welchen Schlüssel — und was das kostet

Drei Stufen der Schlüsselhoheit in Microsoft 365 und ihre Funktionsfolgen



Faustregel aus der Praxis: rund 80 Prozent der Verwaltungsdaten sind unkritisch, rund 15 Prozent brauchen Label und Zugriffsregeln, rund 5 Prozent verdienen eine Sonderbehandlung.

Skizze 3: Drei Stufen der Schlüsselhoheit und die Funktionen, die dabei auf der Strecke bleiben.

Kundenschlüssel: der mittlere Weg

Zwischen der Microsoft-verwalteten Grundverschlüsselung und der Doppelschlüssel-Variante liegt der Kundenschlüssel. Ihre Daten werden ohnehin immer ruhend verschlüsselt, über Datenträgerverschlüsselung und einen verteilten Schlüsselverwalter. Der Kundenschlüssel legt eine zusätzliche Ebene darüber, bei der die Wurzelschlüssel in Ihren eigenen Schlüsseltresoren liegen. Sie autorisieren Microsoft ausdrücklich, diese Schlüssel für Suche, Beweissicherung und Schadsoftwareprüfung zu verwenden — deshalb bleiben die Dienste funktionsfähig.

Verschlüsselungsrichtlinien gibt es in drei Ausprägungen: eine für mehrere Arbeitslasten gemeinsam, die unter anderem Teams-Chats, Aufzeichnungen im Teams-Speicher, Interaktionen mit Assistenzfunktionen und die Konfiguration der Vertraulichkeitsbezeichnungen abdeckt; eine für Exchange-Postfächer, von denen bis zu fünfzig gleichzeitig aktiv sein können; und eine für SharePoint und OneDrive. Wichtig für die Konzeption: Dateien und Aufzeichnungen, die aus Teams heraus in SharePoint landen, fallen unter die SharePoint-Richtlinie, nicht unter die für mehrere Arbeitslasten.

Der eigentliche Wert liegt aus Verwaltungssicht weniger in der Verschlüsselung selbst als im Ausstiegsszenario. Wenn Sie den Zugriff auf Ihre Schlüssel widerrufen, wird auch der von Microsoft gehaltene Verfügbarkeitsschlüssel gelöscht, und die Daten sind kryptografisch vernichtet. Das ist eine Antwort auf die Frage, die in jeder zweiten Beschlussvorlage steht: Was passiert, wenn wir aussteigen wollen oder müssen? Der Preis dafür ist Betriebsdisziplin. Verlorene Schlüssel bedeuten verlorene Daten — es gibt keine Kulanzwiederherstellung. Wer diesen Weg geht, braucht eine dokumentierte Vertretungsregelung, getrennte Tresore in getrennten Regionen und eine geübte Wiederherstellung.

Kriterium	Microsoft-verwaltet	Kundenschlüssel	Doppelschlüssel
Schlüsselhoheit	vollständig beim Betreiber	Wurzelschlüssel bei der Behörde	ein Schlüssel dauerhaft im eigenen Haus
Suche und Indexierung	voll	voll	nicht in SharePoint und OneDrive

Gemeinsames Bearbeiten	voll	voll	nicht möglich
Office im Browser	voll	voll	nicht möglich
Beweissicherung und Verlustvermeidung	voll	voll	nicht möglich
Assistenzfunktionen	nutzbar	nutzbar	kein Zugriff auf die Inhalte
Teams-Besprechungen und Chat	voll	voll	nicht unterstützt
Betriebsaufwand	gering	mittel bis hoch	hoch, eigener Dienst nötig
Ausstiegsszenario	vertraglich geregelt	kryptografische Löschung möglich	Schlüssel bleibt ohnehin im Haus
Typischer Anteil am Bestand	rund 80 Prozent	je nach Begründung	wenige Prozent

Vergleich der drei Schlüsselmodelle. Die Spalte „Doppelschlüssel“ ist keine Warnung vor dem Verfahren, sondern eine Anforderung an dessen Zuschnitt.

Datenverarbeitungsraum und souveräne Angebote

Ein Teil der Schutzbedarfsdiskussion in Verwaltungen dreht sich nicht um Verschlüsselung, sondern um Orte. Dazu gehört der europäische Datenverarbeitungsraum, den Microsoft in drei Stufen aufgebaut hat: seit Januar 2023 werden Kundendaten der Kerndienste in der EU und der EFTA gespeichert und verarbeitet, seit Januar 2024 gilt das auch für pseudonymisierte personenbezogene Daten, und seit Februar 2025 bleiben auch die im Rahmen technischer Unterstützung übermittelten Daten wie Protokolle in dieser Region. Für Ihre Feststellung heißt das: Der Standortfrage können Sie mit einer belegbaren Aussage begegnen, statt sie als offenes Risiko stehen zu lassen.

Daneben steht die Delos Cloud, eine Plattform der SAP-Tochter Delos Cloud, die Microsoft-Technologie unter deutschem Betrieb bereitstellt. Erste Azure-Dienste und Office 365 wurden im Verlauf des Jahres 2025 für Evaluierungen verfügbar gemacht; die Prüfung, ob die Plattform die Anforderungen des Bundes an Informationssicherheit und Vertraulichkeit erfüllt, läuft unter Beteiligung des BSI. Was das Angebot heute ist, für wen es überhaupt in Betracht kommt und was daran noch offen ist, ordnet [Delos Cloud für Kommunen: Was das Angebot ist, wen es betrifft und was fehlt](#) ein. Für Ihre Schutzbedarfsfeststellung gilt: Planen Sie nicht auf ein künftiges Angebot hin. Stufen Sie ein, was Sie heute betreiben, und halten Sie die Feststellung so, dass ein Umzug später kein neues Konzept erfordert.

FAKTEN: Nachweise, die Sie ohne eigenen Aufwand verwenden können

Der Kriterienkatalog C5 des BSI umfasst in der Fassung von 2020 einhunderteinundzwanzig Anforderungen in siebzehn Themenbereichen und wird derzeit überarbeitet. Er unterscheidet Testate vom Typ 1, die das Konzept prüfen, und vom Typ 2, die die Wirksamkeit über einen Zeitraum betrachten.

Microsoft weist für definierte Dienstbereiche C5-Testate aus. Diese Testate können Sie als Nachweis für die Anbieterebene verwenden — für alles, was Sie selbst darauf aufbauen und konfigurieren, brauchen Sie jedoch weiterhin Ihren eigenen Nachweis. Genau diese Trennlinie sollte in Ihrer Feststellung ausdrücklich stehen, weil sie in Prüfungen sonst zu Missverständnissen führt.

Für die Bundesverwaltung existiert zusätzlich der Mindeststandard des BSI zur Nutzung externer Cloud-Dienste. Für Länder, Kommunen und Zweckverbände ist er nicht unmittelbar bindend, taugt

aber als gut strukturierte Prüfliste — und wird von Aufsichtsbehörden gelegentlich als Maßstab herangezogen.

Der Abgleich im Betrieb: Bausteine, Nachweise, Restrisiken

Eine Schutzbedarfsfeststellung ist kein Dokument, sondern ein Zustand. Sie ist dann richtig, wenn sie beschreibt, was tatsächlich eingestellt ist, und wenn sie das belegen kann. Dieser Abschnitt behandelt die drei Dinge, die dafür nötig sind: die Zuordnung zu den Bausteinen, den Nachweis und den offen benannten Rest.

Welche Bausteine ein Tenant tatsächlich trifft

Die Modellierung ist der Punkt, an dem viele Häuser zu viel Zeit verlieren. Ein Microsoft-365-Tenant ist kein einzelnes Zielobjekt, sondern eine Ansammlung von Diensten, die mehrere Bausteine gleichzeitig berühren. Die folgende Tabelle ordnet die wichtigsten Themenfelder ihrer Entsprechung im Tenant und dem zugehörigen Nachweis zu. Sie ersetzt die Modellierung nicht, verkürzt aber die Diskussion darüber, wo man anfängt.

Themenfeld im Grundschutz	Entsprechung im Tenant	Nachweis, der sich erzeugen lässt
Cloud-Nutzung, Anbietersteuerung	Vertragslage, Dienstauswahl, Regionsfestlegung, Testate des Anbieters	Leistungsbeschreibung, Auftragsverarbeitung, Testat, eigene Prüfliste
Identitäts- und Berechtigungsverwaltung	Entra ID, Gruppenmodell, Berechtigungsvergabe, Gastkonten	Zugriffsüberprüfungen, Bericht über Gruppenmitgliedschaften
Privilegierte Konten	Rollenmodell, zeitlich begrenzte Rechteerhöhung, Notfallkonten	Genehmigungsprotokoll, Bericht über Rollenaktivierungen
Zugriffsschutz und Authentisierung	Regelwerk bedingter Zugriffe, Authentifizierungskontexte, Gerätekonformität	Richtlinienauswertung, Anmeldeprotokolle, Ausnahmeliste
Informationsklassifizierung	Vertraulichkeitsbezeichnungen für Elemente und Container	Bezeichnungsbericht, Ereignisse zu Fehlalagen
Datenschutz und Auskunftsfähigkeit	Inhaltssuche, Beweissicherung, Verlustvermeidung	Suchergebnisse, dokumentierte Auskunftsvorgänge
Aufbewahrung und Aussonderung	Aufbewahrungsbezeichnungen, Disposition, Vernichtungsnachweis	Bezeichnungszuweisung, Dispositionsprotokoll
Protokollierung und Auswertung	Einheitliches Prüfprotokoll, Ausleitung in eigene Auswertung	Protokollauszug mit Zeitraum und Suchbedingung
Datensicherung	Plattformmechanismen, Versionierung, ergänzende Sicherung	Wiederherstellungstest mit Zeitmessung und Protokoll
Notfallvorsorge	Ausweichverfahren, Kommunikationswege, Rollen im Ereignisfall	Übungsprotokoll, Auswertung, Maßnahmenliste
Schulung und Sensibilisierung	Rollenbezogene Qualifizierung, Umgang mit Bezeichnungen und Freigaben	Teilnahmenachweis, Lernstandserhebung

Themenfelder und ihre Entsprechung im Tenant. Der Nachweis in der dritten Spalte ist der eigentliche Zweck der Übung.

Zu mehreren dieser Zeilen gibt es eigene Beiträge in dieser Serie: Wie Sie Rollen und zeitlich begrenzte Rechteerhöhung so einrichten, dass nicht am Ende eine einzige Person alles darf, steht in [Privilegierte Konten in der Verwaltungs-IT: Rollen, PIM und der Fall des einen Admins](#). Welche

Nachweise das Rechnungsprüfungsamt aus dem Prüfprotokoll tatsächlich erwarten kann, behandelt [Microsoft 365 Audit-Log und Rechnungsprüfung: Nachweise, die Verwaltungen liefern müssen](#). Und warum die Verfügbarkeitsspalte Ihrer Feststellung eine bewusste Risikoentscheidung zur Datensicherung verlangt, statt sich auf den Papierkorb zu verlassen, steht in [Backup und Wiederherstellung in Microsoft 365: Die Risikoentscheidung fürs Rechnungsprüfungsamt](#).

Oversharing ist der Regelfall, nicht der Sonderfall

Wenn Sie in einem gewachsenen Tenant messen, wie viele Dokumente für „alle in der Organisation“ freigegeben sind, ist das Ergebnis regelmäßig unangenehm. Das ist keine Nachlässigkeit einzelner Personen, sondern eine Folge davon, dass Teilen in Microsoft 365 der bequemste Weg ist und über Jahre niemand hingesehen hat. Solange nur Menschen suchen, fällt es kaum auf. Sobald eine Assistenzfunktion dazukommt, fällt es sofort auf.

Für die Schutzbedarfsfeststellung bedeutet das: Die Spalte „Sichtbarkeit für Suche und Assistenz“ ist keine Zusatzzeile für später, sondern gehört zum Vertraulichkeitsteil. Technisch stehen dafür in der erweiterten SharePoint-Verwaltung mehrere Werkzeuge bereit — Berichte über zu weit geteilte Inhalte, die eingeschränkte Zugriffssteuerung, die den Zugriff auf eine benannte Gruppe begrenzt, und die eingeschränkte Auffindbarkeit, die verhindert, dass Inhalte einer Site in der organisationsweiten Suche und in Assistenzantworten auftauchen, ohne die Berechtigungen selbst zu ändern. Seit 2026 lässt sich die Steuerung der Auffindbarkeit auch an Site-Verantwortliche delegieren, die sie dann mit Begründung setzen — was in Verwaltungen mit vielen Fachämtern deutlich besser skaliert als eine zentrale Liste.

Warum ein Assistenzsystem die Personalakte findet, obwohl niemand sie ihm gezeigt hat, und wie eine Aufräumaktion praktisch abläuft, beschreibt [Oversharing im Verwaltungs-Tenant: Warum Copilot die Personalakte findet](#). Die datenschutzrechtliche Seite einschließlich der Frage nach Rechtsgrundlage und Folgenabschätzung behandelt [Microsoft 365 Copilot in der Verwaltung: Datenschutz, Rechtsgrundlage, DSFA](#).

Restrisiken benennen statt verschweigen

Der unbeliebteste Teil jeder Feststellung ist der Abschnitt über die Risiken, die bleiben. Er ist trotzdem der wichtigste, denn er ist der einzige, der die Leitung wirklich betrifft. Der IT-Grundschutz ist an dieser Stelle unmissverständlich: Risiken, die nicht behandelt werden, muss die Leitung ausdrücklich übernehmen. Nicht die IT-Leitung, nicht die Informationssicherheitsbeauftragte — die Leitung.

In der Praxis bedeutet das, dass drei bis fünf Restrisiken sauber formuliert in die Beschlussvorlage gehören, mit Beschreibung, Begründung und dem, was Sie zur Minderung tun. Typische Kandidaten in Verwaltungen: der Zugriff des Betreibers auf Metadaten, die Abhängigkeit von einem Anbieter bei Dienstaussfällen, die Reichweite der eigenen Sicherung im Verhältnis zur Wiederherstellungserwartung, und die Tatsache, dass eine Fehlkonfiguration im Tenant schneller wirkt als jede Freigabekette es korrigieren kann.

Ein großer Landschaftsverband hat das gut gelöst, indem die Restrisiken nicht als Anlage, sondern als eigener Beschlusspunkt in die Vorlage kamen. Vier Sätze pro Risiko, eine Seite insgesamt. Das hat die Diskussion im Gremium nicht verlängert, sondern verkürzt — weil klar war, worüber abgestimmt wird. Der Umkehrschluss gilt auch: Eine Vorlage ohne benannte Restrisiken erzeugt in Gremien Misstrauen, weil erfahrene Mitglieder wissen, dass es sie gibt.

WICHTIG: Der Personalrat gehört an den Tisch, bevor die Tabelle fertig ist

Ein erheblicher Teil der Maßnahmen in der Spalte „hoch“ berührt die Mitbestimmung: Protokollierung von Zugriffen, Auswertung von Freigabeereignissen, Gerätekonformität, Sitzungsdauern. Wer die Übersetzungstabelle zuerst fertig baut und sie dann vorlegt, verhandelt über

ein fertiges Bauwerk. Das dauert länger als eine frühe Beteiligung.

In kirchlichen Einrichtungen tritt an diese Stelle die Mitarbeitervertretung, und es gelten mit dem kirchlichen Datenschutzrecht eigene Regelwerke. Die Übersetzungslogik dieses Beitrags bleibt dieselbe, die Beteiligungsschritte unterscheiden sich.

Welche Bausteine eine Dienstvereinbarung braucht und wie sich Protokollierung regeln lässt, ohne dass daraus eine Verhaltenskontrolle wird, steht in [Copilot und Personalrat: Bausteine einer Dienstvereinbarung](#). Für kirchliche Träger ordnet [Microsoft 365 in Kirche, Diakonie und Caritas: DSG-EKD, KDG und Mitarbeitervertretung](#) die Besonderheiten ein.

Der Fahrplan und die Rollen darin

Die Frage, wie lange das dauert, kommt in jedem Vorgespräch. Die ehrliche Antwort: Die Feststellung selbst ist in wenigen Wochen machbar, wenn die richtigen Personen gleichzeitig im Raum sitzen. Was lange dauert, ist die Umsetzung — und zwar nicht aus technischen Gründen, sondern weil jedes Amt seine eigenen Sonderfälle hat.

Fahrplan: von der Feststellung zur nachweisbaren Configuration

Realistische Abfolge für eine mittlere Kommunalverwaltung



Die Beschlussvorlage entsteht nach Woche 4. Wer sie vorher schreibt, beschließt eine Absicht statt einer Maßnahme.

Skizze 4: Ein realistischer Fahrplan von der Feststellung bis zum laufenden Nachweis.

Zwei Punkte aus der Praxis dazu. Erstens: Die Beschlussvorlage entsteht nach der Übersetzungsmatrix, nicht davor. Eine Vorlage, die nur eine Absicht beschreibt, muss später nachgebessert werden, und Nachbesserungen kosten in Gremien mehr Vertrauen als sie an Zeit sparen. Zweitens: Der Pilot gehört in zwei Ämter mit unterschiedlichem Charakter. Kämmererei und Bauamt sind eine gute Kombination, weil das eine mit stark strukturierten, integritätskritischen Vorgängen arbeitet und das andere mit vielen externen Beteiligten.

Wie sich eine solche Konzeptionsphase mit Fachämtern, Personalrat und IT-Leitung in wenigen Tagen durchführen lässt und was am Ende in die Beschlussvorlage gehört, beschreibt [Microsoft-365-Einführung in der Verwaltung: Konzeptionsphase in 4,5 Tagen und die Beschlussvorlage](#). Wenn Sie für den Abgleich eine unabhängige Zweitmeinung neben Ihrem Systemhaus oder Ihrem kommunalen Rechenzentrum suchen — beide sind für den Betrieb wertvoll, haben aber naturgemäß eine eigene Perspektive auf die Architektur —, finden Sie den Rahmen dafür auf der Seite zur [Microsoft-365-Beratung für Verwaltungen](#). Wie sich Rollen und Schnittstellen zum Rechenzentrum sauber schneiden lassen, behandelt [Microsoft 365 und das kommunale Rechenzentrum: Rollen, Schnittstellen, Zweitmeinung](#).

TIPP: Der Test, der jede Feststellung ehrlich macht

Nehmen Sie nach Abschluss der Feststellung eine beliebige Zeile aus Ihrer Informationsartentabelle und fragen Sie die Systemadministration: Zeig mir am Bildschirm, wo das eingestellt ist. Wenn die Antwort ein Verweis auf ein Dokument ist, ist die Feststellung nicht fertig. Wenn die Antwort ein Admin Center ist, ist sie es.

Machen Sie diesen Test bei drei Zeilen. Er dauert zwanzig Minuten und ersetzt ein halbes Audit.

Häufige Fragen

Müssen wir jede Informationsart einzeln einstufen oder reicht eine Sammelaussage?

Eine Sammelaussage für den ganzen Tenant ist methodisch zulässig, praktisch aber nutzlos, weil sich daraus keine differenzierten Einstellungen ableiten lassen. Sinnvoll sind zwölf bis zwanzig Informationsarten. Fassen Sie zusammen, was sicherheitstechnisch gleich behandelt wird, auch wenn es rechtlich verschieden ist. Beihilfeunterlagen und Beurteilungen bekommen dieselbe Zeile.

Dürfen Sozialdaten überhaupt in Microsoft 365?

Diese Frage lässt sich nicht pauschal beantworten, und dieser Beitrag ist keine Rechtsberatung. Was sich sagen lässt: Der Schutzbedarf für Sozialdaten ist hoch, und daraus folgt eine Reihe zusätzlicher Maßnahmen, keine automatische Ablehnung. Ob Ihr Landesrecht, die Sozialgesetzgebung und Ihre Aufsicht das für den konkreten Anwendungsfall mittragen, müssen Sie mit Ihrer Datenschutzbeauftragung und gegebenenfalls der Aufsichtsbehörde klären. In der Praxis führt die Prüfung häufig zu einer Aufteilung: Zusammenarbeit und Entwürfe in einer geschützten Site, Falldokumentation im Fachverfahren.

Wie viele Vertraulichkeitsbezeichnungen sollten wir anlegen?

Vier bis fünf auf der obersten Ebene, mit wenigen Unterbezeichnungen für Sonderfälle. Mehr behält niemand auseinander, und falsch angewendete Bezeichnungen sind schlechter als gar keine, weil sie eine Sicherheit vortäuschen, die nicht besteht. Trennen Sie außerdem sauber zwischen Bezeichnungen für Elemente und solchen für Container — das reduziert die Verwirrung erheblich, verlangt aber Sorgfalt bei der Priorisierungsreihenfolge.

Was ist mit Daten, die schon jahrelang falsch abgelegt sind?

Die räumen Sie nicht von Hand auf. Beginnen Sie mit Berichten über zu weit geteilte Inhalte, sperren Sie die schlimmsten Fälle über eingeschränkte Zugriffssteuerung, und nehmen Sie die betroffenen Sites vorübergehend aus der organisationsweiten Auffindbarkeit heraus. Erst danach räumen Sie fachlich auf, Amt für Amt. Die Reihenfolge ist wichtig: Zuerst die Blutung stoppen, dann behandeln.

Reicht das C5-Testat von Microsoft als Nachweis für unsere Aufsicht?

Für die Anbieterebene ja, für Ihre eigene Konfiguration nein. Das Testat sagt etwas über den Betrieb der Plattform aus, nicht über Ihre Berechtigungen, Ihre Bezeichnungen und Ihre Freigabeeinstellungen. Diese Trennlinie sollten Sie in der Feststellung ausdrücklich ziehen, sonst entsteht in Prüfungen der Eindruck, Sie hätten sich auf fremde Nachweise verlassen.

Sollen wir auf die Delos Cloud warten?

Planen Sie nicht auf einen Termin hin, den Sie nicht selbst kontrollieren. Stufen Sie ein, was Sie heute betreiben oder betreiben wollen, und halten Sie die Feststellung so allgemein formuliert, dass ein späterer Wechsel der Plattform keine vollständige Neubewertung erzwingt. Die Informationsarten und ihre Schutzstufen ändern sich dadurch nicht — nur die Maßnahmenspalte.

Wer schreibt die Feststellung eigentlich?

Verantwortlich ist die Informationssicherheitsbeauftragte, inhaltlich liefern müssen aber die Fachämter, weil nur sie wissen, was ihre Informationen wert sind. Die IT liefert die Maßnahmenspalte. Die Datenschutzbeauftragte prüft die personenbezogene Seite. Die Leitung übernimmt die Restrisiken. Wenn eine dieser vier Rollen fehlt, entsteht ein Dokument statt eines Zustands.

Wie oft muss die Feststellung fortgeschrieben werden?

Einmal jährlich als Routine, zusätzlich anlassbezogen bei neuen Fachverfahren, neuen Diensten im Tenant und größeren organisatorischen Änderungen. Cloud-Dienste verändern sich laufend; eine Feststellung, die drei Jahre unverändert im Aktenplan liegt, beschreibt einen Tenant, den es so nicht mehr gibt.

Was kostet uns die Umsetzung der Spalte „hoch“?

Der größere Posten ist selten die Lizenz, sondern die Zeit für Informationsarchitektur, Beteiligung und Schulung. Prüfen Sie trotzdem früh, welche Maßnahmen an Planvoraussetzungen hängen — Kundenschlüssel und Doppelschlüssel setzen gehobene Pläne voraus, ebenso mehrere der Werkzeuge zur Sichtbarkeitssteuerung. Diese Prüfung gehört in die Feststellung, damit die Kämmerei nicht überrascht wird.

Fazit

Eine Schutzbedarfsfeststellung, die im Aktenplan liegt und keine Entsprechung im Tenant hat, ist kein Sicherheitsinstrument, sondern eine Ablage. Der Unterschied zwischen beiden liegt in einer einzigen Tabelle: der Zuordnung von Schutzstufe zu konkreter Einstellung. Diese Tabelle zu bauen, ist unspektakuläre Arbeit von vielleicht vier Wochen. Sie nicht zu bauen, kostet Sie später deutlich mehr — spätestens dann, wenn ein Assistenzsystem eine Frage beantwortet, die niemand gestellt haben wollte.

Drei Punkte sollten Sie aus diesem Beitrag mitnehmen. Erstens: Stufen Sie Informationsarten ein, nicht IT-Systeme, und bewerten Sie Vertraulichkeit, Integrität und Verfügbarkeit getrennt. Zweitens: Übersetzen Sie jede Stufe in drei Dinge — ein Label, eine Zugriffsregel, einen Speicherort. Fehlt eines davon, ist die Maßnahme unwirksam. Drittens: Behandeln Sie „hoch“ als Konfigurationsauftrag und „sehr hoch“ als Grundsatzfrage. Die Verwechslung dieser beiden Stufen ist die häufigste Ursache dafür, dass Verwaltungsprojekte entweder zu früh abbrechen oder zu spät merken, dass sie etwas übersehen haben.

Und der praktischste Rat zum Schluss: Der Aufwand liegt nicht in der Technik. Die Einstellungen selbst sind in wenigen Tagen gesetzt. Der Aufwand liegt darin, zwölf Fachämter dazu zu bringen, ihre Informationen ehrlich zu bewerten, und danach die Belegschaft dazu, die richtige Bezeichnung zu wählen. Beides ist Kommunikationsarbeit, keine Administrationsarbeit — und beides entscheidet darüber, ob Ihre Feststellung nach zwei Jahren noch stimmt.

Weil der letzte Punkt so oft unterschätzt wird: Eine Vertraulichkeitsbezeichnung wirkt nur, wenn sie angewendet wird, und angewendet wird sie nur, wenn die Sachbearbeitung versteht, warum. Rollenbezogene Qualifizierung für Fachämter, Registratur und Führungskräfte ist deshalb Teil der Maßnahme und nicht Beiwerk — Zuschnitte dafür finden Sie auf der Seite zur [Microsoft-365-Schulung für Verwaltungen](#).

Weiterlesen in dieser Serie

- › [Microsoft 365 in der öffentlichen Verwaltung](#) — der Gesamtüberblick zur Serie
- › [Standard-Tenant oder Hybrid: Die Betriebsmodell-Entscheidung für Verwaltungen](#) — wenn die Verfügbarkeitsspalte das Betriebsmodell berührt

- › [Aufbewahrung und Aussonderung mit Purview: Fristen, Disposition, Vernichtungsnachweis](#) — die Integritätsseite der Feststellung
- › [Gäste in Teams und SharePoint: Planungsbüros, Träger und Gremienmitglieder sicher einbinden](#) — Freigaberegeln für externe Beteiligte
- › [Microsoft Teams in der Verwaltung einführen: Informationsarchitektur entlang der Ämter](#) — die Architektur, die das Maximumprinzip entschärft
- › [Notfallübung für die Verwaltungs-IT: SharePoint verschlüsselt, Admin-Konto übernommen, Bürgertelefon tot](#) — der Praxistest für die Verfügbarkeitsannahmen
- › [Microsoft 365 Lizenzen für Verwaltungen: E3, E5, F3 und die Behördenkonditionen](#) — welche Maßnahme an welchem Plan hängt