

Backup und Wiederherstellung in Microsoft 365: Die Risikoentscheidung fürs Rechnungsprüfungsamt

Es gibt in der Verwaltungs-IT zwei Sorten von Gesprächen über Backup. Die erste Sorte findet in einer Dienstberatung statt, dauert elf Minuten und endet mit dem Satz: „Das macht doch Microsoft.“ Die zweite Sorte findet an einem Freitagnachmittag statt, dauert bis Sonntagabend und beginnt mit dem Satz: „Wir haben da ein Problem im Sozialamt.“ Die zweite Sorte ist deutlich lehrreicher. Sie ist nur schlecht planbar.

Der Satz „Das macht doch Microsoft“ ist übrigens nicht komplett falsch. Microsoft betreibt für SharePoint, OneDrive und Exchange Online eine Infrastruktur mit mehrfach redundanten Kopien Ihrer Daten, die einen Rechenzentrumsausfall abfedert, ohne dass irgendjemand in Ihrem Haus etwas davon merkt. Was Microsoft damit ausdrücklich nicht verspricht, ist der Schutz vor Ihnen selbst. Vor dem gelöschten Ordner, dem kompromittierten Administratorkonto, dem Verschlüsselungstrojaner, der über die Synchronisierung in die Bibliothek des Bauamts läuft, und vor dem Fachverfahrensexport, der seit vierzehn Monaten in einer Bibliothek liegt, die vorletzte Woche jemand aufgeräumt hat.

Dieser Beitrag beantwortet nicht die Frage, ob Sie ein Backup brauchen. Diese Frage ist in der Verwaltung nämlich falsch gestellt. Die richtige Frage lautet: Für welche Datenbestände reichen die Bordmittel, für welche nicht — und wo steht das aufgeschrieben, wenn in zwei Jahren jemand vom Rechnungsprüfungsamt danach fragt? Backup in Microsoft 365 ist keine Glaubensfrage. Es ist eine dokumentierte Risikoentscheidung. Und eine dokumentierte Risikoentscheidung darf durchaus lauten: Wir verzichten. Sie darf nur nicht lauten: Wir haben nicht darüber nachgedacht.

FAKTENKASTEN — WORUM ES HIER GEHT

Microsoft 365 kennt drei Schichten der Wiederherstellung: die Bordmittel im Tenant (Papierkörbe, Versionierung, Selbstbedienung), die Aufbewahrung über Microsoft Purview und ein separat zu beauftragendes Backup-Produkt. Die drei Schichten lösen unterschiedliche Probleme und lassen sich nicht gegeneinander tauschen.

Die Bordmittel enden nach spätestens 93 Tagen, in Exchange Online nach 14 bis 30 Tagen. Ein Rückgriff darüber hinaus ist ohne Backup-Produkt nicht möglich — auch nicht über den Support.

Der Betrag, um den es geht, liegt in vielen Häusern im niedrigen vierstelligen Bereich pro Jahr. Der Aufwand, um die Entscheidung sauber zu begründen, liegt bei etwa zwei Arbeitstagen. Beides ist überschaubar. Peinlich wird nur, wenn keines von beidem stattgefunden hat.

Dieser Beitrag ist Teil der Serie [Microsoft 365 in der öffentlichen Verwaltung](#). Er setzt voraus, dass die grundsätzlichen Weichen — Betriebsmodell, Schutzbedarf, Lizenzen — bereits gestellt sind oder zumindest bearbeitet werden. Wenn Sie noch am Anfang stehen, sortiert [Microsoft 365 in der Kommune: Was Sie wirklich entscheiden müssen \(und was nicht\)](#) die Reihenfolge der Entscheidungen; die Einordnung des Schutzbedarfs finden Sie in [Schutzbedarf und Microsoft 365: IT-Grundschutz-Abgleich für die Praxis](#).

Was Microsoft 365 von Haus aus kann — und was das wirklich heißt

Bevor Sie über ein Produkt reden, sollten Sie wissen, was Sie ohnehin schon haben. Die Bordmittel sind besser als ihr Ruf und schlechter als ihre Legende. Beides hilft nicht weiter, wenn Sie nicht die Zahlen kennen. Also: die Zahlen.

Der Papierkorb ist ein Sicherheitsnetz, kein Fallschirm

SharePoint und OneDrive haben einen zweistufigen Papierkorb. Löscht jemand eine Datei, landet sie im Papierkorb der Website. Wird sie dort gelöscht oder der Papierkorb geleert, wandert sie in den Papierkorb der Websitesammlung, oft „zweite Stufe“ genannt. Entscheidend ist die Gesamtfrist: 93 Tage ab dem Löschen am ursprünglichen Ort. Nicht 93 Tage je Stufe. Die zweite Stufe erbt schlicht die Restlaufzeit. Wer aus dem Papierkorb der Websitesammlung löscht, löscht sofort und endgültig.

Zwei Feinheiten, die in Verwaltungen regelmäßig für Überraschungen sorgen. Erstens: Der Papierkorb der Websitesammlung hat ein Kontingent. Läuft er über, werden die ältesten Einträge entfernt, damit die neuesten hineinpassen. Bei einer Massenzöschung kann das Netz also reißen, obwohl die 93 Tage noch nicht abgelaufen sind. Zweitens: Wer über Schnittstellen arbeitet — also über CSOM oder REST, wie es Migrationswerkzeuge, Fachverfahrensanbindungen und selbstgebaute Skripte tun —, kann Elemente entweder in den Papierkorb verschieben oder direkt löschen. Direkt gelöschte Elemente sind aus beiden Papierkorbstufen nicht mehr wiederherstellbar. Sofort. Ohne Rückfrage.

Auch gelöschte Websitesammlungen bleiben 93 Tage erhalten und können von der SharePoint-Administration im Admin Center zurückgeholt werden. Danach sind sie samt Listen, Bibliotheken, Seiten, Untersites und Berechtigungen fort. Für die 14 Tage nach der endgültigen Zöschung hält Microsoft noch eigene Sicherungen vor, aus denen der Support in engen Grenzen eine Wiederherstellung anstoßen kann. Danach ist Schluss — Microsoft formuliert das ungewöhnlich klar: Nach Ablauf dieser Frist werden die Daten nicht mehr aufbewahrt und können nicht wiederhergestellt werden.

Versionierung rettet Dateien, keine Organisationen

Die Versionshistorie ist das mit Abstand nützlichste Bordmittel, weil sie das häufigste Problem löst: Jemand hat etwas überschrieben. Standardmäßig bewahrt SharePoint bis zu 500 Versionen einer Datei auf. Mit der intelligenten Versionierung, die Microsoft seit 2025 in die Fläche gebracht hat, ändert sich die Logik: Statt stumpf 500 Versionen zu horten, behält der Dienst in den ersten 30 Tagen dicht, danach ausgedünnt und nach 180 Tagen nur noch wöchentliche Stände — innerhalb derselben Obergrenze. Für die Speicherrechnung ist das eine gute Nachricht. Für die Wiederherstellung heißt es: Je älter der Schaden, desto grobmaschiger das Netz.

Und hier liegt die eigentliche Schwäche. Versionierung ist ein Werkzeug für Einzelfälle. Wenn in einer Bibliothek des Sozialamts 180.000 Dateien in einer Nacht überschrieben wurden, ist die Aussage „die alte Version ist ja noch da“ formal richtig und praktisch wertlos. Sie können 180.000 Dateien nicht einzeln zurückholen, und Sie wollen es auch nicht per Skript um drei Uhr morgens versuchen, während der Personalrat wissen möchte, ob am Montag jemand arbeiten kann. Eine

Stadtverwaltung mit SharePoint im Sozialbereich hat genau diesen Unterschied auf die harte Tour gelernt: Die Daten waren nie weg. Die Wiederherstellung dauerte trotzdem elf Tage.

Exchange Online: 14 Tage sind schneller vorbei, als eine Krankmeldung dauert

In Exchange Online liegen gelöschte Elemente nach dem Leeren des Ordners „Gelöschte Elemente“ im Ordner für wiederherstellbare Elemente. Die Standardaufbewahrung dort beträgt 14 Tage; sie lässt sich je Postfach auf maximal 30 Tage anheben. Dreißig Tage ist das Maximum, nicht der Anfang einer Verhandlung. Wer sechs Wochen krank war und danach feststellt, dass ein Ordner fehlt, hat Pech gehabt — es sei denn, ein Hold oder eine Aufbewahrungsrichtlinie greift. Und Holds sind, wie gleich zu sehen, etwas anderes als ein Backup.

Gelöschte Postfächer, etwa nach dem Ausscheiden aus dem Dienst, folgen wieder eigenen Fristen. Das ist einer der Gründe, warum die Frage „Wie lange behalten wir Postfächer nach dem Ausscheiden?“ in die Dienstvereinbarung und in das Verarbeitungsverzeichnis gehört und nicht in die spontane Entscheidung der Benutzerverwaltung.

Aufbewahrung mit Purview: die Schicht, die am häufigsten missverstanden wird

Aufbewahrungsrichtlinien und Aufbewahrungsbezeichnungen aus Microsoft Purview sorgen dafür, dass Inhalte für eine definierte Zeit erhalten bleiben, auch wenn jemand sie löscht oder überschreibt. In SharePoint und OneDrive geschieht das über die Preservation Hold Library, eine versteckte Systembibliothek, die im Hintergrund Kopien der Originale einsammelt. Das ist ein starkes Werkzeug für Fristen und für die Aussonderung — und es ist eine Schicht, die Sie ohnehin brauchen, wenn Ihr Haus Fristen aus dem Aktenplan in Microsoft 365 abbilden will.

Nur ist es eben kein Wiederherstellungswerkzeug. Für die Praxis der Fristenverwaltung ist [Aufbewahrung und Aussonderung mit Purview: Fristen, Disposition, Vernichtungsnachweis](#) der passende Einstieg; die Anbindung an den Aktenplan behandelt [Schriftgutverwaltung mit Microsoft 365: Vom Aktenplan zur Aufbewahrungsbezeichnung](#). Und weil beide Schichten getrennt arbeiten, gilt umgekehrt: Aufbewahrungs- und Löschrichtlinien aus Purview greifen nicht in das Wiederherstellungsfenster eines Backups ein. Was Sie dort löschen lassen, bleibt in der Sicherung, bis deren Fenster abläuft.

WARNUNG — EINE AUFBEWAHRUNGSBEZEICHNUNG IST KEIN BACKUP

Das ist der teuerste Denkfehler in diesem Themenfeld, und er ist erstaunlich verbreitet — bis in Beschlussvorlagen hinein. Aufbewahrung hält Inhalte fest. Backup stellt Zustände wieder her. Das ist nicht dasselbe.

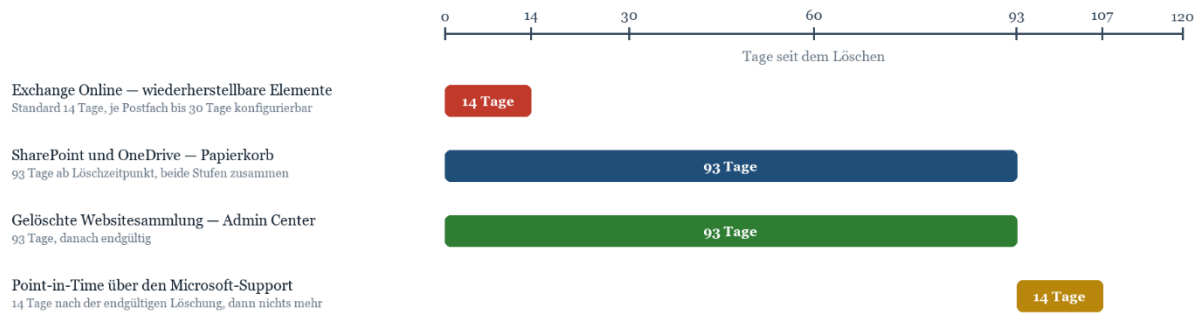
Eine Aufbewahrungsrichtlinie verhindert, dass Inhalte verschwinden. Sie verhindert nicht, dass die produktive Bibliothek unbrauchbar ist. Nach einem Verschlüsselungsvorfall liegen die sauberen Originale womöglich in der Preservation Hold Library — in einer versteckten Bibliothek, ohne Ordnerstruktur, ohne Metadaten der Fachverfahren, nicht für den interaktiven Zugriff gebaut und ohne Werkzeug, das 180.000 Dateien an ihren Platz zurücksortiert. Sie haben die Daten. Sie haben keinen Arbeitsstand.

Umgekehrt gilt dasselbe: Ein Backup ist kein Aufbewahrungskonzept. Es kennt Ihren Aktenplan nicht, es dokumentiert keine Aussonderung und es liefert keinen Vernichtungsnachweis. Wer Aufbewahrung durch Backup ersetzt, hat sein Schriftgutproblem nur verschoben.

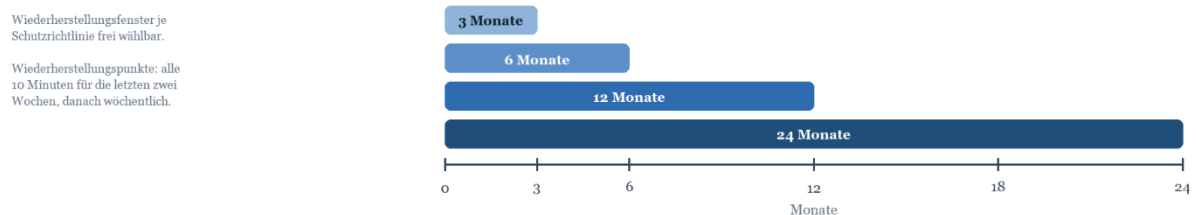
Und wenn die Aufbewahrung nicht so wirkt, wie sie soll, ist das eine eigene Fehlersuche: [Wenn die Aufbewahrungsrichtlinie einfach aufhört: SharePoint-Störungsanalyse in der Verwaltung.](#)

Wie weit reicht der Rückgriff? Bordmittel gegen Backup-Fenster

Bordmittel im Tenant — Skala in Tagen



Microsoft 365 Backup — Skala in Monaten



Bordmittel enden nach spätestens 107 Tagen. Alles, was danach auffällt, ist ohne Backup verloren.

Skizze 1: Die Bordmittel haben harte Enden. Ein Backup-Fenster wird gewählt, nicht geerbt.

Drei Szenarien, die Sie durchspielen müssen

Eine Risikoentscheidung entsteht nicht aus Produktvergleichen, sondern aus Szenarien. Drei davon reichen für den Anfang. Sie decken zusammen fast alles ab, was in Verwaltungen tatsächlich passiert — und sie fallen unterschiedlich aus, was den ganzen Reiz der Sache ausmacht.

Szenario 1: Ransomware über die synchronisierte Bibliothek

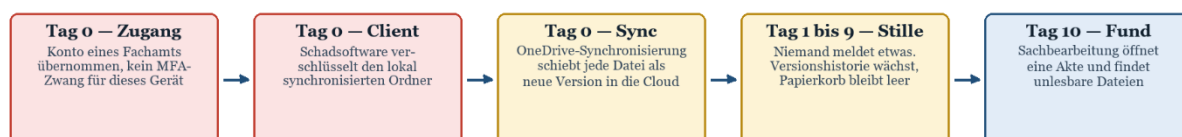
Der Klassiker läuft nicht über den Server, sondern über den Arbeitsplatz. Ein Konto wird übernommen, die Schadsoftware verschlüsselt lokal, und die Synchronisierung erledigt den Rest: Jede verschlüsselte Datei landet als neue Version in der Bibliothek. Nichts wird gelöscht. Der Papierkorb bleibt leer und meldet freundlich, dass alles in Ordnung ist.

Technisch überleben die alten Versionen. Organisatorisch ist das nur dann eine gute Nachricht, wenn Sie ein Werkzeug haben, das ganze Websites auf einen Zeitpunkt zurückrollt. Für persönliche Ablagen gibt es „Dateien wiederherstellen“ in OneDrive, eine Selbstbedienungsfunktion mit einem Zeitfenster von 30 Tagen. Für Bibliotheken der Fachämter, in denen die eigentliche Arbeit liegt, gibt es diese Funktion nicht in vergleichbarer Form. Das ist der Punkt, an dem viele Häuser zum

ersten Mal merken, dass die Frage nicht „sind die Daten weg?“ lautet, sondern „wie viele Personentage kostet es, sie zurückzuholen?“.

Vorbeugend hilft hier weniger das Backup als der Zugang: [Conditional Access für Verwaltungen: Regelwerk für Rathaus, Bauhof und Homeoffice](#) beschreibt das Regelwerk, das den Erstzugriff erschwert. Und weil der Angriff über ein Konto läuft, das jemand geöffnet hat, gehört auch [Microsoft-365-Schulung für Verwaltungen](#) in die Rechnung — die günstigste Wiederherstellung ist die, die nicht stattfinden muss.

Ransomware im Tenant: Der Weg vom Client in die Bibliothek



Was die Bordmittel an Tag 10 leisten

- Versionshistorie: Die letzte saubere Version liegt noch da — pro Datei, einzeln, per Hand oder Skript.
- Papierkorb: hilft nicht, denn nichts wurde gelöscht. Es wurde überschrieben.
- OneDrive „Dateien wiederherstellen“: rollt ein Laufwerk auf einen Zeitpunkt zurück. Für Bibliotheken der Fachämter greift das nicht.
- Aufbewahrungsrichtlinie: bewahrt die Originale in der Preservation Hold Library — als Compliance-Kopie, nicht als Wiederherstellungswerkzeug.

Was ein Backup an Tag 10 leistet

- Rücksetzen ganzer Websites auf einen Zeitpunkt vor Tag 0 — in einem Vorgang, nicht Datei für Datei.
- Wiederherstellungspunkte im 10-Minuten-Raster für die zurückliegenden zwei Wochen.
- Wiederherstellung an denselben oder an einen neuen Ort, damit die Fachämter vergleichen können, was gilt.

Die eigentliche Frage lautet nicht, ob die Daten noch da sind. Sie lautet, wie lange die Wiederherstellung dauert.

Skizze 2: Der Ablauf ist unspektakulär. Der Wiederanlauf ist es nicht.

Szenario 2: Böswillige Löschung mit Adminrechten

Das unangenehmste Szenario ist nicht der externe Angreifer, sondern das legitime Konto mit hohen Rechten. Eine Kündigung, ein Konflikt, ein Dienstleisterwechsel — die Motive sind vielfältig, die Wirkung ist dieselbe. Wer SharePoint-Administrationsrechte hat, kann Websitesammlungen löschen, Papierkörbe leeren und mit einem PowerShell-Befehl endgültig entfernen, was vorher noch 93 Tage Restlaufzeit hatte. Wer Exchange-Administrationsrechte hat, kann Postfächer entfernen. Und wer beides hat, kann einen Tenant in einer Stunde erheblich beschädigen.

Bordmittel helfen hier nur begrenzt, weil sie mit denselben Rechten bedienbar sind, die der Schaden nutzt. Ein Backup-Produkt ist an dieser Stelle strukturell im Vorteil: Microsoft 365 Backup speichert Sicherungen in Append-only-Speicher, das heißt, vorhandene Sicherungsstände lassen sich nicht verändern oder überschreiben. Löschen lassen sie sich — sonst wäre eine Abmeldung vom Dienst nicht möglich —, aber danach gibt es eine feste Nachfrist von 90 Tagen, in der sich die Sicherungen zurückholen lassen. Zusätzlich lässt sich eine Benachrichtigungsliste mit bis zu 20 Empfängern hinterlegen, die bei potenziell schädlichen Aktionen automatisch informiert wird: beim Abschalten des Dienstes, beim Entfernen von Schutzeinheiten, beim Pausieren von Richtlinien.

Die eigentliche Gegenmaßnahme bleibt trotzdem organisatorisch. Wenn in Ihrem Haus genau eine Person dauerhaft Globaler Administrator ist — der viel zitierte „Fall des einen Admins“ —, dann ist das Backup ein Pflaster auf einer Konstruktion, die man besser ändert. Wie das geht, steht in [Privilegierte Konten in der Verwaltungs-IT: Rollen, PIM und der Fall des einen Admins](#). Und wer nachvollziehen will, wer wann was gelöscht hat, braucht die Protokolle, die [Microsoft 365 Audit-Log und Rechnungsprüfung: Nachweise, die Verwaltungen liefern müssen](#) behandelt.

Szenario 3: Der Fachverfahrensexport, den niemand vermisst hat

Das dritte Szenario ist unspektakulär und deshalb gefährlich. Ein Fachverfahren legt Exporte in einer SharePoint-Bibliothek ab — Auswertungen der Kämmerei, Listen aus dem Einwohnerwesen, Bescheidkopien, Protokolle einer Schnittstelle. Niemand liest sie regelmäßig. Ein technisches Konto räumt auf, ein Ordner wird umstrukturiert, eine Migration läuft, und die Dateien sind weg. Auffallen tut es, wenn zehn Monate später eine Anfrage kommt und jemand den Stand von damals braucht.

Alle Bordmittel haben zu diesem Zeitpunkt längst zugeschlagen: 93 Tage sind vorbei, die 14 Tage Nachlauf beim Support ebenfalls. Ohne Backup mit einem Fenster von zwölf oder 24 Monaten ist der Stand nicht wiederherstellbar. Punkt. Ein großer Landschaftsverband hat aus genau dieser Erfahrung eine schlichte Regel gemacht: Jede Bibliothek, in die ein technisches Konto schreibt, ist Backup-pflichtig — unabhängig davon, wie wichtig ihr Inhalt beim Anlegen schien.

Hier liegt zugleich die Grenze zur E-Akte. Was aktenrelevant ist, gehört in ein System, das das E-Government-Recht Ihres Landes für die Aktenführung vorsieht — mit den dortigen Anforderungen an Ordnung, Nachvollziehbarkeit und Aussonderung. SharePoint ist Ablage und Zusammenarbeit, nicht automatisch Aktenführung. Wo genau die Linie verläuft, hängt vom Landesrecht ab und ist in [SharePoint als E-Akte? Was geht, was nicht und wo die Grenze nach Landesrecht liegt](#) ausführlich beschrieben. Ein Backup ersetzt diese Abgrenzung nicht — es sichert nur, was auch immer Sie dort abgelegt haben.

Szenario	Reichen die Bordmittel?	Backup nötig?	Der entscheidende Punkt
Versehentlich gelöschte Einzeldatei, Meldung binnen Tagen	Ja	Nein	Papierkorb Stufe 1, in Sekunden erledigt. Dafür ist er gebaut.
Überschriebene Datei, alter Stand gesucht	Ja, innerhalb der Versionsgrenzen	Nein	Versionshistorie greift; nach 180 Tagen nur noch grob gestufte Stände.
Gelöschte Websitesammlung, Meldung binnen 93 Tagen	Ja	Nein	Wiederherstellung im SharePoint Admin Center, ein Vorgang.
Ransomware verschlüsselt eine Bibliothek über die Synchronisierung	Formal ja, praktisch nein	Ja	Die Daten sind da. Die Rückführung von Hand kostet Wochen statt Stunden.
Ransomware trifft mehrere Ämter gleichzeitig	Nein	Ja, dringend	Ohne Rücksetzen ganzer Websites gibt es keinen planbaren Wiederanlauf.

Szenario	Reichen die Bordmittel?	Backup nötig?	Der entscheidende Punkt
Böswillige Löschung mit Administrationsrechten, Papierkorb geleert	Nein	Ja	Endgültiges Löschen per PowerShell umgeht beide Papierkorbstufen.
Löschung über Schnittstelle statt Papierkorb (CSOM oder REST)	Nein	Ja	Direkt gelöschte Elemente erreichen den Papierkorb nie.
Fachverfahrensexport, Fehlen fällt nach zehn Monaten auf	Nein	Ja, mit langem Fenster	Alle Bordmittelfristen sind abgelaufen. Der Support kann nicht helfen.
Postfach einer ausgeschiedenen Person, Anfrage nach acht Monaten	Nein	Ja oder Aufbewahrung	14 bis 30 Tage im Ordner für wiederherstellbare Elemente, dann nichts mehr.
Aufbewahrungsfrist für Schriftgut über Jahre	Nein — falsches Werkzeug	Nein — falsches Werkzeug	Das ist ein Fall für Aufbewahrung und Aussonderung, nicht für Backup.

Tabelle 1: Szenarienraster. Die letzte Zeile ist die wichtigste — nicht jedes Datenproblem ist ein Backup-Problem.

TIPP — DER SZENARIENTEST IN DER DIENSTBERATUNG

Nehmen Sie die Tabelle mit in die nächste Runde mit den Amtsleitungen und stellen Sie genau eine Frage je Fachamt: „Welche Ihrer Ablagen dürfen für zwei Arbeitstage nicht verfügbar sein, und welche dürfen für zwei Wochen nicht verfügbar sein?“

Sie bekommen erstaunlich präzise Antworten, sobald es konkret wird. Und Sie bekommen nebenbei die Priorisierung, die Sie für die Schutzrichtlinien Ihrer Backup-Richtlinien brauchen — plus ein Protokoll, das später Teil der Beschlussvorlage wird.

Microsoft 365 Backup, Drittprodukte und die ehrliche Rechnung

Wenn die Szenarien zeigen, dass Bordmittel nicht reichen, stellt sich die Frage nach dem Werkzeug. Es gibt drei Wege, und alle drei sind vertretbar. Sie unterscheiden sich in Betriebsaufwand, Vergabeaufwand und in der Frage, wo die Kopie liegt.

Was Microsoft 365 Backup leistet

Microsoft 365 Backup ist ein eigenständiges, verbrauchsabhängig abgerechnetes Angebot für SharePoint-Websites, OneDrive-Konten und Exchange-Online-Postfächer. Das Wiederherstellungsfenster wird je Schutzrichtlinie gewählt: drei Monate, sechs Monate, ein Jahr oder zwei Jahre. Wiederherstellungspunkte liegen für SharePoint und OneDrive in den ersten zwei Wochen im 10-Minuten-Raster, danach wöchentlich; für Exchange Online durchgehend im 10-Minuten-Raster über 52 Wochen. Abgerechnet wird mit 0,15 US-Dollar je Gigabyte und Monat für die geschützten Daten. Wiederherstellungen selbst kosten nichts.

Der eigentliche Verkaufspunkt ist nicht die Sicherung, sondern die Geschwindigkeit der Wiederherstellung. Weil die Sicherungen innerhalb der Dienstgrenzen liegen und die Daten den Microsoft-Datenraum nie verlassen, entfällt das Zurückkopieren über eine Internetleitung. Microsoft nennt für eine einzelne Website mit einem sogenannten Express-Wiederherstellungspunkt typischerweise etwa 30 Minuten, für 250 Schutzseinheiten rund vier Stunden und bei großen Wiederherstellungen bis zu 250 Schutzseinheiten je Stunde. Das sind Medianwerte aus Microsoft-Messungen, keine zugesicherten Werte für Ihren Tenant — aber sie liegen in einer anderen Größenordnung als jede Rückspielung über das Netz.

FAKTENKASTEN — MICROSOFT 365 BACKUP IN ZAHLEN

- Abrechnung: 0,15 US-Dollar je Gigabyte und Monat, verbrauchsabhängig über eine Azure-Abonnement-Verknüpfung. Wiederherstellungen sind kostenfrei.
- Wiederherstellungsfenster je Richtlinie: 3, 6, 12 oder 24 Monate. Bestehende Richtlinien laufen standardmäßig auf 12 Monate.
- Wiederherstellungspunkte: alle 10 Minuten für die letzten zwei Wochen, danach wöchentlich (SharePoint, OneDrive). Exchange Online: 10 Minuten über 52 Wochen.
- Granularität der Sicherung: SharePoint-Website, OneDrive-Konto, Postfach. Wiederherstellung von Postfachelementen einzeln, von Websites als Rücksetzung auf einen Zeitpunkt.
- Speicherung als Append-only: vorhandene Sicherungsstände sind nicht überschreibbar. Nach einer Abmeldung vom Dienst gilt eine Nachfrist von 90 Tagen.
- Aufbewahrungs- und Löschrichtlinien aus Purview wirken nicht auf das Wiederherstellungsfenster — die beiden Schichten sind voneinander getrennt.
- Berechtigungen zur Einrichtung: SharePoint-Administration oder Globale Administration; für den laufenden Betrieb gibt es die eigene Rolle „Microsoft 365 Backup Administrator“.
- Für Government-Community-Cloud-Umgebungen ist der Dienst verfügbar. Die Datenhaltung folgt der Datenresidenz des Tenants.

Was Microsoft 365 Backup nicht abdeckt

Die Abdeckung endet bei drei Diensten. Alles andere im Tenant ist nicht enthalten, und das ist in Verwaltungen relevanter, als es klingt. Nicht abgedeckt sind insbesondere Einzel- und Gruppenchats in Teams, Aufgaben und Pläne, Loop-Komponenten, die Konfiguration von Microsoft Entra ID mit Rollen, Gruppen, Richtlinien für bedingten Zugriff und Anwendungsregistrierungen sowie alles, was in der Power Platform liegt.

Für Verwaltungen mit Fachanwendungen auf SharePoint-Listen oder Dataverse ist der letzte Punkt ein eigenes Thema — [Power Platform in der Verwaltung: SharePoint-Listen oder Dataverse für Fachanwendungen?](#) geht darauf ein. Kanalunterhaltungen in Teams liegen in der Gruppenpostfach- und SharePoint-Struktur dahinter und sind damit teilweise mit abgedeckt; die persönlichen Chats sind es nicht. Wie die Informationsarchitektur diesen Unterschied beeinflusst, behandelt [Microsoft Teams in der Verwaltung einführen: Informationsarchitektur entlang der Ämter](#).

Und ein Punkt, der in Datenschutzprüfungen zuverlässig aufkommt: Die Sicherungen verlassen den Microsoft-Datenraum nicht. Das ist je nach Blickwinkel das stärkste Argument für oder gegen das Produkt. Wer eine Kopie außerhalb der Plattform will — weil das Schutzkonzept eine Trennung

von Produktiv- und Sicherungssystem verlangt oder weil eine Aufsicht das so sieht —, findet sie hier nicht.

Drittprodukte, kommunale Rechenzentren und der Weg über den Vertrag

Drittanbieter sichern nach außen, decken mehr Dienste ab und bringen eigene Berichtsfunktionen mit. Sie kosten dafür Betriebsaufwand, brauchen Speicherplatz, erfordern eine eigene Auftragsverarbeitungsvereinbarung und laufen häufig als eigene Vergabe. Ein wesentlicher Teil dieser Produkte setzt inzwischen ohnehin auf der Microsoft-Backup-Plattform auf und ergänzt sie um Oberfläche und Berichtswesen — die Grenze zwischen „Microsoft-Produkt“ und „Drittprodukt“ ist also weniger scharf, als die Präsentationen vermuten lassen.

Für viele Häuser ist der pragmatischste Weg ohnehin ein anderer: Das kommunale Rechenzentrum oder das Systemhaus, das den Tenant betreut, hat für diesen Fall meist ein Angebot im Portfolio, das gebündelt beschafft und betrieben wird. Das ist häufig eine gute Lösung — vorausgesetzt, Sie wissen, welches Wiederherstellungsfenster darin enthalten ist, wer die Wiederherstellung auslöst und wie lange sie dauert. Die Rollenverteilung zwischen Haus und Dienstleister sortiert [Microsoft 365 und das kommunale Rechenzentrum: Rollen, Schnittstellen, Zweitmeinung](#).

Der Beschaffungsweg selbst richtet sich nach dem Vergaberecht Ihres Landes und nach den dort geltenden Wertgrenzen. Bei den Größenordnungen, um die es hier geht, liegen viele Fälle unterhalb der Schwelle für ein förmliches Verfahren — aber das ist eine Frage, die die Vergabestelle beantwortet, nicht die IT und nicht dieser Beitrag. Orientierung zu Leistungsbeschreibung und Rahmenverträgen gibt [Microsoft 365 rechtssicher beschaffen: Vergabe, Leistungsbeschreibung, Rahmenverträge](#); die Einordnung in die Lizenzlandschaft leistet [Microsoft 365 Lizenzen für Verwaltungen: E3, E5, F3 und die Behördenkonditionen](#).

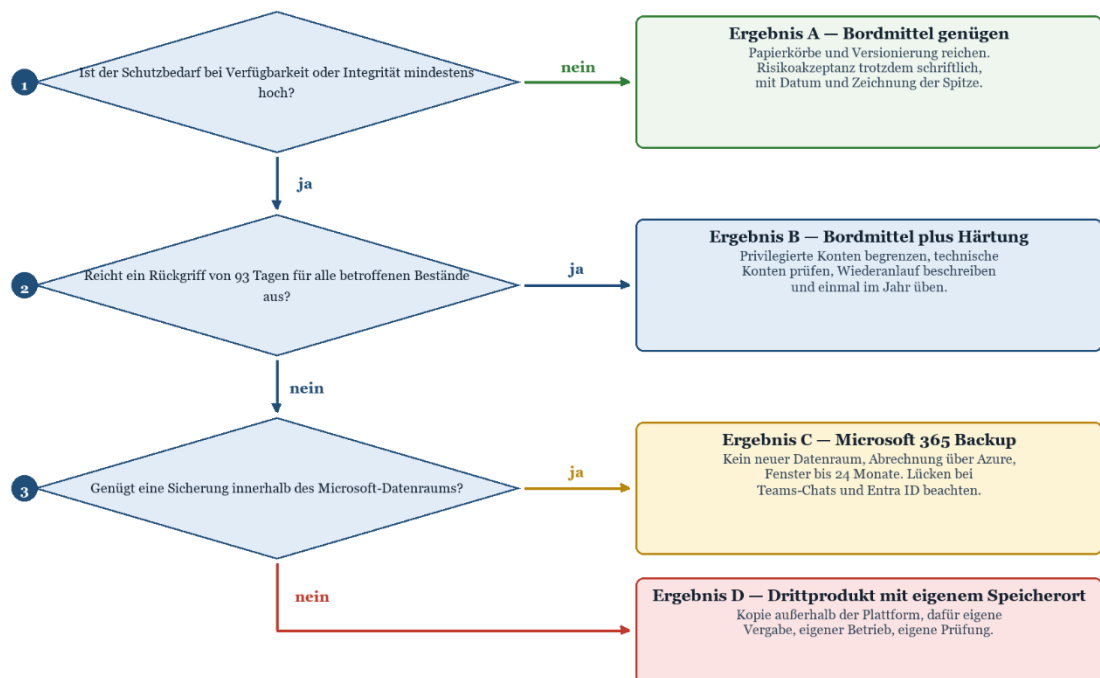
Wenn Ihr Haus einen souveränen Betrieb prüft, verschiebt sich die Frage, aber sie verschwindet nicht: Auch dort ist zu klären, welche Wiederherstellungsfunktionen in welchem Umfang zur Verfügung stehen und ob sie dem Funktionsumfang des öffentlichen Angebots entsprechen. Belastbare Aussagen dazu gehören in die Leistungsbeschreibung und nicht in eine Roadmap-Folie; der Sachstand ist in [Delos Cloud für Kommunen: Was das Angebot ist, wen es betrifft und was fehlt](#) nüchtern beschrieben. Wer Teile der Daten im eigenen Haus behält, bekommt zusätzlich zwei Sicherungswelten, die zusammenpassen müssen — siehe [Standard-Tenant oder Hybrid: Die Betriebsmodell-Entscheidung für Verwaltungen](#).

Kriterium	Bordmittel im Tenant	Microsoft 365 Backup	Drittprodukt mit eigenem Speicher
Rückgriff maximal	93 Tage (SharePoint, OneDrive), 14 bis 30 Tage (Exchange)	3, 6, 12 oder 24 Monate je Richtlinie	Frei wählbar, je nach Vertrag und Speicher
Rücksetzen ganzer Websites	Nur bei gelöschter Websitesammlung	Ja, auf einen Zeitpunkt, an denselben oder einen neuen Ort	Ja, Umfang je Produkt
Wiederherstellung großer Mengen	Unrealistisch von Hand	Bis zu 250 Schutzeinheiten je Stunde (Medianangabe)	Abhängig von Leitung und Zielsystem, meist deutlich langsamer

Kriterium	Bordmittel im Tenant	Microsoft 365 Backup	Drittprodukt mit eigenem Speicher
Schutz vor Adminrechten	Gering — dieselben Rechte greifen	Append-only, 90 Tage Nachfrist, Benachrichtigung mehrerer Personen	Hoch bei getrennter Rechteverwaltung und unveränderlichem Speicher
Ort der Kopie	Im Dienst	Im Microsoft-Datenraum, Datenresidenz des Tenants	Nach Vertrag wählbar, auch außerhalb der Plattform
Abgedeckte Dienste	SharePoint, OneDrive, Exchange, Teams-Kanäle	SharePoint, OneDrive, Exchange Online	Je Produkt, oft zusätzlich Teams-Chats und Verzeichniskonfiguration
Kosten	Enthalten	0,15 US-Dollar je Gigabyte und Monat, verbrauchsabhängig	Meist je Postfach und Monat zuzüglich Speicher
Vergabeaufwand	Keiner	Gering — Verbrauchsabrechnung über Azure	Eigenes Verfahren, Wertgrenzen nach Landesrecht prüfen
Betriebsaufwand	Keiner	Gering — Richtlinien pflegen, Meldungen auswerten	Mittel bis hoch — eigenes System, eigene Überwachung
Nachweis fürs Rechnungsprüfungsamt	Risikoakzeptanz muss schriftlich vorliegen	Richtlinien, Protokolle, Übungsprotokoll	Berichte des Produkts, Übungsprotokoll

Tabelle 2: Der Vergleich ist keine Rangliste. Er ist eine Liste von Fragen, die Sie beantworten müssen.

Entscheidungspfad: Bordmittel, Microsoft 365 Backup oder Drittprodukt



Kein Pfad ist an sich richtig. Falsch ist nur der Pfad, den niemand aufgeschrieben hat.

Skizze 3: Vier Fragen führen zu vier vertretbaren Ergebnissen.

TIPP — RECHNEN SIE DEN BETRAG AUS, BEVOR SIE DISKUTIEREN

Die Debatte über Backup dauert in Verwaltungen typischerweise länger als die Erhebung der Zahl, um die es geht. Nehmen Sie den belegten Speicher aus dem Berichtsbereich des Admin Centers — SharePoint, OneDrive und Exchange zusammen, einschließlich Papierkörben und Onlinearchiven —, multiplizieren Sie mit 0,15 US-Dollar und mit zwölf. Das ist die Größenordnung für ein Jahr.

Bei 8 Terabyte belegtem Speicher, was für eine mittlere Stadtverwaltung ein realistischer Wert ist, landen Sie bei rund 14.400 US-Dollar im Jahr. Bei 2 Terabyte sind es rund 3.600. Das ist eine Zahl, mit der die Kämmerei arbeiten kann — und eine Zahl, die die Diskussion oft in fünf Minuten beendet, in die eine oder in die andere Richtung.

Wichtig für die Haushaltsplanung: Der Betrag wächst mit dem Datenbestand. Planen Sie eine jährliche Steigerung ein und prüfen Sie, ob eine Bereinigung alter Versionen und Papierkörbe vor der Aktivierung sinnvoll ist.

Die Entscheidung dokumentieren: Was das Rechnungsprüfungsamt sehen will

Jetzt kommt der Teil, den IT-Abteilungen gerne überspringen und den das Rechnungsprüfungsamt zuerst aufschlägt. Das Amt prüft nicht, ob Sie das beste Produkt gekauft haben. Es prüft, ob eine Entscheidung getroffen, begründet, von der richtigen Stelle verantwortet und anschließend auch umgesetzt wurde. Eine gut begründete Entscheidung für die Bordmittel besteht diese Prüfung. Ein teures Produkt ohne Entscheidungsgrundlage besteht sie nicht.

Drei Zahlen, die Sie festlegen müssen

Vor jedem Produktvergleich stehen drei Festlegungen, und sie gehören der Verwaltungsspitze, nicht der IT. Erstens der Schutzbedarf je Datenbestand, insbesondere für Verfügbarkeit und Integrität. Zweitens die tolerierbare Ausfallzeit — wie lange darf ein Fachamt ohne seine Ablage arbeiten, bevor es ernst wird? Drittens der tolerierbare Datenverlust — auf welchen Stand darf zurückgesetzt werden, ohne dass Arbeit unwiederbringlich verloren geht? In der Fachsprache heißen die letzten beiden RTO und RPO. In der Beschlussvorlage heißen sie besser „tolerierbare Ausfallzeit“ und „tolerierbarer Datenverlust“, weil das jeder im Hauptausschuss versteht.

Diese drei Festlegungen leiten Sie aus dem Schutzbedarf ab, den Sie im IT-Grundschutz-Abgleich ohnehin erheben. Wenn dieser Schritt bei Ihnen noch aussteht, ist er die eigentliche Vorarbeit: [Schutzbedarf und Microsoft 365: IT-Grundschutz-Abgleich für die Praxis](#). Ohne Schutzbedarfsfeststellung ist jede Backup-Entscheidung eine Meinung.

Die Beschlussvorlage und ihre Zulieferer

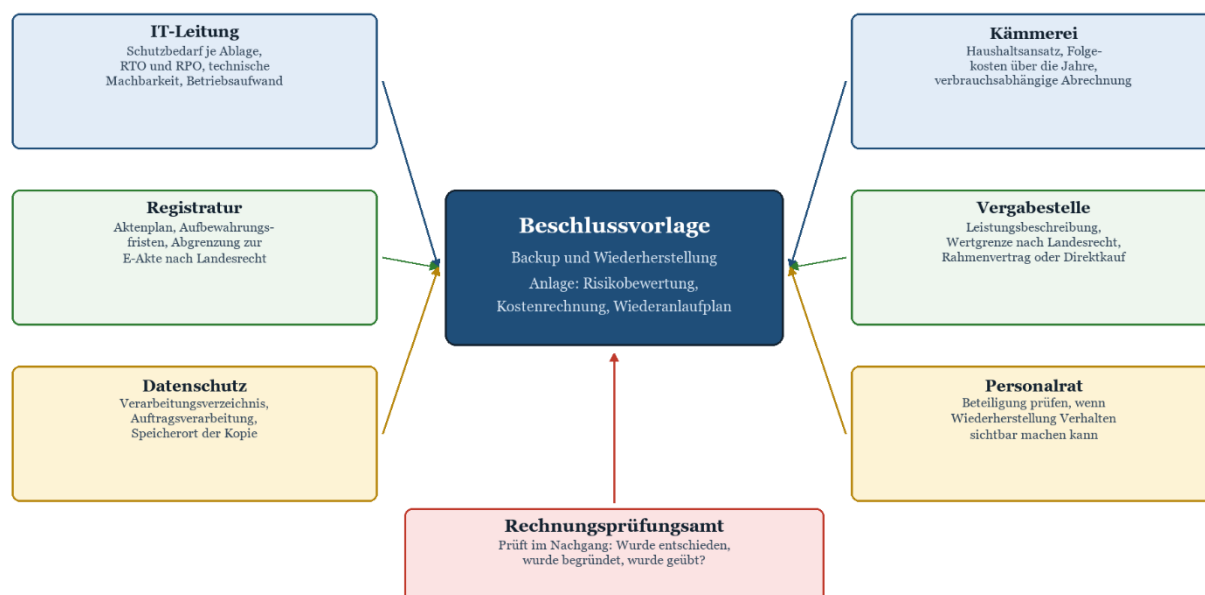
Eine tragfähige Beschlussvorlage für dieses Thema hat sechs Zulieferer und passt trotzdem auf drei Seiten. Die IT-Leitung liefert Schutzbedarf, Zeitvorgaben und technische Machbarkeit. Die Registratur klärt, welche Bestände aktenrelevant sind und deshalb ohnehin einer anderen Logik folgen. Die Datenschutzbeauftragten prüfen Verarbeitungsverzeichnis, Auftragsverarbeitung und den Ort der Kopie. Die Kämmerei bringt Haushaltsansatz und Folgekosten ein. Die Vergabestelle

klärt den Beschaffungsweg. Der Personalrat wird beteiligt, soweit die Beteiligungstatbestände Ihres Landes das vorsehen.

Beim Personalrat lohnt eine Präzisierung, weil sie oft für unnötige Reibung sorgt: Ein Backup ist keine Verhaltens- oder Leistungskontrolle. Es ist eine Sicherungskopie. Beteiligungsrelevant wird es dort, wo Wiederherstellungsvorgänge personenbezogene Daten sichtbar machen könnten — etwa wenn ein Postfach in ein anderes Konto zurückgespielt wird — oder wo Protokolle über Wiederherstellungen ausgewertet werden. Diese Punkte gehören in eine Dienstvereinbarung oder in eine Ergänzung zu einer bestehenden.

Welche Bausteine sich dafür bewährt haben, zeigt exemplarisch [Copilot und Personalrat: Bausteine einer Dienstvereinbarung](#) — die Systematik ist auf dieses Thema übertragbar, auch wenn der Anlass ein anderer ist.

Wer liefert was: Die Aktenlage hinter der Risikoentscheidung



Skizze 4: Sechs Zulieferer, eine Vorlage, ein Prüfvermerk zwei Jahre später.

Der Wiederanlaufplan und die Übung

Ein Backup, dessen Wiederherstellung nie erprobt wurde, ist eine Ausgabe, keine Sicherheit. Das ist keine Beratergeschwätzigkeit, sondern die häufigste Feststellung in Prüfberichten: Das Produkt war beschafft, die Richtlinie war aktiv, und im Ernstfall wusste niemand, wer sie bedienen darf und in welcher Reihenfolge welche Ämter zurückgeholt werden. Eine Stadtverwaltung mit rund 1.000 Rufnummern hat in ihrer ersten Übung festgestellt, dass die Wiederherstellung technisch in gut zwei Stunden lief — und die Abstimmung darüber, welcher Zeitpunkt der richtige ist, zweieinhalb Tage brauchte. Das Werkzeug war nicht das Problem.

Legen Sie eine Reihenfolge fest: Welches Amt zuerst, welche Websites gehören zusammen, wer entscheidet über den Wiederherstellungszeitpunkt, wer informiert die Fachämter, wer die Bürgerschaft. Und dann üben Sie es einmal im Jahr, vorzugsweise mit einem Szenario, das weh tut. Wie eine solche Übung aufgebaut wird, beschreibt [Notfallübung für die Verwaltungs-IT:](#)

SharePoint verschlüsselt, Admin-Konto übernommen, Bürgertelefon tot – mit einem Ablauf, der ohne externe Begleitung funktioniert.

Und dokumentieren Sie die Übung. Ein zweiseitiges Protokoll mit Datum, Beteiligten, gewähltem Szenario, gemessenen Zeiten und drei Feststellungen reicht vollkommen aus. Dieses Protokoll ist im Prüffall mehr wert als jede Produktbeschreibung, weil es das Einzige ist, was belegt, dass die Lösung nicht nur gekauft, sondern auch bedienbar ist.

WICHTIG – DIE VIER UNTERLAGEN, DIE IM PRÜFFALL REICHEN

Sie brauchen keine 60-seitige Konzeption. Sie brauchen vier Dokumente, die zueinander passen und ein Datum tragen:

- Die Schutzbedarfsfeststellung je Datenbestand, mit Angabe der tolerierbaren Ausfallzeit und des tolerierbaren Datenverlusts.
- Die Risikoentscheidung selbst – als Beschlussvorlage oder als Vermerk mit Zeichnung der Verwaltungsspitze. Auch ein begründeter Verzicht ist eine Entscheidung und gehört genau hierhin.
- Den Wiederanlaufplan: Wer entscheidet, wer bedient, in welcher Reihenfolge, wer informiert wen.
- Das Protokoll der letzten Übung, mit Datum, Beteiligten, gemessenen Zeiten und Feststellungen.

Was das Rechnungsprüfungsamt fragt	Was Sie vorlegen	Wo es entsteht
Ist der Schutzbedarf der Daten festgestellt?	Schutzbedarfsfeststellung je Ablage oder Fachamt	IT-Leitung mit den Fachämtern, im Rahmen des IT-Grundschutz-Abgleichs
Wurde über Backup entschieden – und von wem?	Beschlussvorlage oder gezeichneter Vermerk mit Datum	Verwaltungsspitze, auf Zuarbeit der IT-Leitung
Warum diese Lösung und nicht eine andere?	Kurzer Variantenvergleich mit Kosten und Begründung	IT-Leitung, gegebenenfalls mit Vergabestelle
War der Beschaffungsweg vergaberechtlich zulässig?	Vergabevermerk, Wertgrenzenprüfung nach Landesrecht	Vergabestelle
Wie hoch sind die Folgekosten und sind sie veranschlagt?	Haushaltsansatz mit Fortschreibung über drei Jahre	Kämmerei
Ist die Verarbeitung datenschutzrechtlich abgebildet?	Eintrag im Verarbeitungsverzeichnis, Auftragsverarbeitung, Ort der Kopie	Datenschutzbeauftragte
Wurde der Personalrat beteiligt, soweit erforderlich?	Beteiligungsvermerk oder Dienstvereinbarung	Personalamt mit Personalrat
Kollidiert das mit der Aufbewahrung und Aussonderung?	Abgrenzungsvermerk Backup gegen Aufbewahrung, Bezug zum Aktenplan	Registratur mit Datenschutzbeauftragten

Was das Rechnungsprüfungsamt fragt	Was Sie vorlegen	Wo es entsteht
Funktioniert die Wiederherstellung tatsächlich?	Übungsprotokoll mit gemessenen Zeiten	IT-Leitung, jährliche Notfallübung
Wer darf Wiederherstellungen auslösen?	Rollenkonzept mit dokumentierter Rechtevergabe	IT-Leitung, Rollen- und Rechteverwaltung

Tabelle 3: Prüffragen und ihre Antworten. Zehn Zeilen, die einen Prüfvermerk sehr viel kürzer machen.

Aufbewahrung, Aussonderung und die Grenze zur E-Akte

Ein letzter Punkt, der in der Vorlage nicht fehlen darf, weil er sonst später als Widerspruch auffällt. Ein Backup mit einem Fenster von 24 Monaten hält Daten vor, die nach Ihrem Aktenplan möglicherweise schon hätten ausgesondert werden müssen. Das ist kein Skandal, aber es ist erklärungsbedürftig, und es gehört ins Verarbeitungsverzeichnis: Sicherungskopien mit begrenzter, technisch bedingter Vorhaltefrist und ohne fachliche Nutzung sind etwas anderes als eine fortgesetzte Verarbeitung. Formulieren Sie das einmal sauber, stimmen Sie es mit den Datenschutzbeauftragten ab, und die Frage ist erledigt.

Und ziehen Sie die Linie zur Aktenführung ausdrücklich. Was nach dem E-Government-Recht Ihres Landes aktenrelevant ist, folgt den dortigen Anforderungen — ein Backup ersetzt weder ein Aktenführungssystem noch die Aussonderung mit Vernichtungsnachweis. Die Abgrenzung im Detail leisten [SharePoint als E-Akte? Was geht, was nicht und wo die Grenze nach Landesrecht liegt](#) und [Aufbewahrung und Aussonderung mit Purview: Fristen, Disposition, Vernichtungsnachweis](#). Für kirchliche Träger gilt dasselbe Muster unter anderem Recht: DSG-EKD beziehungsweise KDG und die Mitarbeitervertretung statt Personalrat, siehe [Microsoft 365 in Kirche, Diakonie und Caritas: DSG-EKD, KDG und Mitarbeitervertretung](#).

Wenn Sie das Thema nicht isoliert, sondern im Rahmen einer geordneten Konzeptionsphase bearbeiten wollen, ist Backup üblicherweise ein Baustein von mehreren — der Ablauf dazu steht in [Microsoft-365-Einführung in der Verwaltung: Konzeptionsphase in 4,5 Tagen und die Beschlussvorlage](#). Und wenn Sie für die Bewertung eine Zweitmeinung suchen, die weder ein Produkt verkauft noch den Betrieb übernimmt: [Microsoft-365-Beratung für Verwaltungen](#).

Häufige Fragen

Macht Microsoft nicht ohnehin ein Backup unserer Daten?

Microsoft betreibt Redundanz, keine Sicherung für Ihre Zwecke. SharePoint, OneDrive und Exchange Online halten mehrfach replizierte Kopien vor, um Ausfälle in der Infrastruktur abzufangen. Diese Kopien schützen vor Hardware- und Rechenzentrumsproblemen, nicht vor Löschungen, Überschreibungen oder Verschlüsselung durch Schadsoftware. Für diese Fälle stehen Ihnen die Bordmittel mit ihren Fristen zur Verfügung — und darüber hinaus nur ein separat beauftragtes Backup.

Kann der Microsoft-Support etwas wiederherstellen, wenn alle Fristen abgelaufen sind?

Nach der endgültigen Löschung hält SharePoint Sicherungen für weitere 14 Tage vor, aus denen der Support in bestimmten Fällen eine Wiederherstellung einer Websitesammlung oder eines Zeitpunkts anstoßen kann. Nach Ablauf dieser 14 Tage werden die Daten nicht mehr aufbewahrt. Kalkulieren Sie diese Nachfrist nicht ein: Sie ist keine zugesicherte Leistung, sondern ein enges Zeitfenster für Ausnahmefälle, und sie setzt voraus, dass der Verlust überhaupt schon aufgefallen ist.

Reicht eine Aufbewahrungsrichtlinie nicht aus, wenn wir sie großzügig setzen?

Nein, weil sie ein anderes Problem löst. Eine Aufbewahrungsrichtlinie stellt sicher, dass Inhalte nicht verschwinden — sie legt Kopien in der Preservation Hold Library ab. Sie stellt keinen Arbeitsstand wieder her. Nach einem größeren Vorfall haben Sie mit einer Aufbewahrungsrichtlinie eine Menge Dateien in einer versteckten Systembibliothek und kein Werkzeug, das sie mit Struktur und Metadaten zurückbringt. Großzügig gesetzte Aufbewahrung erzeugt zudem Speicherkosten und kollidiert mit Ihrem Aussonderungskonzept.

Was kostet Microsoft 365 Backup für eine mittlere Kommunalverwaltung?

Die Abrechnung erfolgt verbrauchsabhängig mit 0,15 US-Dollar je Gigabyte und Monat auf die geschützten Daten; Wiederherstellungen sind kostenfrei. Für die Schätzung nehmen Sie den belegten Speicher in SharePoint, OneDrive und Exchange einschließlich Papierkörben und Onlinearchiven. Bei 2 Terabyte liegen Sie bei rund 3.600 US-Dollar im Jahr, bei 8 Terabyte bei rund 14.400. Sie können auch nur ausgewählte Websites und Postfächer schützen — was in Verwaltungen oft die sinnvollere Variante ist, weil nicht jede Projektablage denselben Schutzbedarf hat.

Sichert Microsoft 365 Backup auch Teams-Chats und unsere Entra-Konfiguration?

Nein. Das Produkt deckt SharePoint-Websites, OneDrive-Konten und Exchange-Online-Postfächer ab. Persönliche Chats und Gruppenchats in Teams sind nicht enthalten, ebenso wenig Aufgaben, Loop-Komponenten, die Konfiguration von Microsoft Entra ID — Rollen, Gruppen, Richtlinien für bedingten Zugriff, Anwendungsregistrierungen — und die Power Platform. Kanalunterhaltungen liegen technisch in den dahinterliegenden Strukturen und sind dadurch teilweise mit erfasst. Wenn Ihr Schutzkonzept diese Lücken adressieren muss, brauchen Sie ergänzende Maßnahmen oder ein Drittprodukt.

Wo liegen die Sicherungen und ist das datenschutzrechtlich unproblematisch?

Die Sicherungen bleiben innerhalb der Dienstgrenzen von Microsoft 365 und folgen der Datenresidenz Ihres Tenants; nach Microsoft-Angaben verlassen nur begrenzte Metadaten wie

Tenant- und Website-Kennungen den Bereich, und zwar ausschließlich zur Abrechnung. Rechtlich ist das eine Verarbeitung im Rahmen Ihrer bestehenden Auftragsverarbeitungsvereinbarung, die im Verarbeitungsverzeichnis abgebildet werden muss. Ob Ihr Schutzkonzept zusätzlich eine Kopie außerhalb der Plattform verlangt, ist eine Frage, die Ihre Datenschutzbeauftragten und gegebenenfalls die Aufsicht beantworten — nicht der Produktvergleich.

Wie schnell ist eine Wiederherstellung wirklich?

Microsoft nennt als Medianwerte für eine einzelne Website mit Express-Wiederherstellungspunkt etwa 30 Minuten, für 50 Schutzeinheiten rund drei Stunden, für 250 rund vier Stunden und für größere Mengen bis zu 250 Schutzeinheiten je Stunde. Für Postfächer liegen die Werte typischerweise bei 100 bis 500 Elementen je Minute. Das sind Erwartungswerte aus Microsoft-Messungen, keine Zusagen. Planen Sie in Ihrem Wiederanlaufplan mit Puffer — und rechnen Sie die Abstimmungszeit ein, die in der Praxis regelmäßig länger dauert als der technische Vorgang.

Wir wollen kein Backup beschaffen. Reicht das?

Das kann vollkommen ausreichen — wenn es eine Entscheidung ist und kein Versäumnis. Halten Sie schriftlich fest, welche Datenbestände betroffen sind, welche Szenarien Sie geprüft haben, welches Restrisiko Sie akzeptieren und wer diese Akzeptanz verantwortet. Ergänzen Sie flankierende Maßnahmen: verschärfter Umgang mit privilegierten Konten, engere Regeln für technische Konten, Aufbewahrung für die wirklich kritischen Bestände, Benachrichtigungen bei Massenlöschungen. Ein begründeter Verzicht mit Datum und Unterschrift ist prüfungsfest. Ein ungeklärter Zustand ist es nie.

Brauchen wir das auch, wenn ein kommunales Rechenzentrum unseren Tenant betreut?

Die Frage bleibt dieselbe, sie wird nur an anderer Stelle beantwortet. Klären Sie konkret: Ist ein Backup Bestandteil des Vertrags? Welches Wiederherstellungsfenster gilt? Wer darf eine Wiederherstellung auslösen und in welcher Reaktionszeit? Gibt es ein Übungsprotokoll? Diese vier Antworten gehören in Ihre Akte, unabhängig davon, wer den Betrieb führt. Die Verantwortung für die Daten bleibt bei Ihrem Haus.

Fazit

Backup in Microsoft 365 ist kein Bekenntnis, sondern ein Vorgang. Er beginnt mit dem Schutzbedarf, führt über drei Szenarien und endet mit einer gezeichneten Entscheidung, einem Wiederanlaufplan und einem Übungsprotokoll. Ob am Ende ein Produkt beschafft wird oder nicht, ist dabei nicht die entscheidende Frage — es ist die Frage, die sich aus den vorherigen Antworten ergibt.

Was Sie mitnehmen sollten: Die Bordmittel sind gut für den Alltag und enden hart. 93 Tage in SharePoint und OneDrive, 14 bis 30 Tage in Exchange Online, danach 14 Tage Nachlauf beim Support und dann nichts mehr. Versionierung rettet Dateien, keine Ämter. Aufbewahrung ist kein Backup, und Backup ist kein Aufbewahrungskonzept. Microsoft 365 Backup ist die betriebsarme Variante mit Fenstern bis 24 Monaten und ohne neuen Datenraum, aber mit klaren Lücken bei

Teams-Chats, Verzeichniskonfiguration und Power Platform. Ein Drittprodukt schließt diese Lücken und kostet dafür Vergabe- und Betriebsaufwand.

Und der Satz, den Sie im Prüftermin brauchen, lautet nicht „wir haben ein Backup“. Er lautet: „Wir haben den Schutzbedarf festgestellt, drei Szenarien geprüft, die Entscheidung am 10. September dokumentiert, den Wiederanlauf beschrieben und im Mai geübt. Hier sind die vier Unterlagen.“ Danach wird das Gespräch erfahrungsgemäß kurz — und das ist bei Rechnungsprüfung die höchste erreichbare Form von Lob.

WEITER IM THEMA

Diese Beiträge greifen die hier angesprochenen Punkte auf und vertiefen sie:

- › [Notfallübung für die Verwaltungs-IT: SharePoint verschlüsselt, Admin-Konto übernommen, Bürgertelefon tot](#)
- › [Microsoft 365 Audit-Log und Rechnungsprüfung: Nachweise, die Verwaltungen liefern müssen](#)
- › [Schutzbedarf und Microsoft 365: IT-Grundschutz-Abgleich für die Praxis](#)
- › [Aufbewahrung und Aussonderung mit Purview: Fristen, Disposition, Vernichtungsnachweis](#)
- › [SharePoint als E-Akte? Was geht, was nicht und wo die Grenze nach Landesrecht liegt](#)
- › [Wenn die Aufbewahrungsrichtlinie einfach aufhört: SharePoint-Störungsanalyse in der Verwaltung](#)
- › [Privilegierte Konten in der Verwaltungs-IT: Rollen, PIM und der Fall des einen Admins](#)
- › [Microsoft 365 rechtssicher beschaffen: Vergabe, Leistungsbeschreibung, Rahmenverträge](#)
- › [Microsoft 365 und das kommunale Rechenzentrum: Rollen, Schnittstellen, Zweitmeinung](#)
- › [Microsoft-365-Einführung in der Verwaltung: Konzeptionsphase in 4,5 Tagen und die Beschlussvorlage](#)