

Ransomware-Vorsorge in Microsoft 365

Es gibt zwei Sorten von Organisationen: die einen haben ihre Wiederherstellung getestet, die anderen glauben fest daran, dass sie funktioniert. Der Unterschied zwischen beiden fällt normalerweise an einem Sonntagmorgen um 4:30 Uhr auf, wenn der erste Anruf kommt und jemand mit sehr ruhiger Stimme sagt, dass sich in sämtlichen Dateinamen eine neue Endung eingeschlichen hat.

Die gute Nachricht vorweg: Microsoft 365 bringt für den Verschlüsselungsfall mehr Bordmittel mit, als die meisten Tenants jemals benutzen. Versionsverlauf, zwei Papierkorbstufen, sekundengenaues Zurückrollen ganzer Bibliotheken, Aufbewahrung, dazu ein eigenes Backup-Produkt und ein Ökosystem an Drittanbietern. Die schlechte Nachricht: Diese Bordmittel sind gegen genau eine Hälfte des Erpressungsgeschäfts wirksam. Gegen die andere Hälfte – die Veröffentlichung deiner Daten – hilft kein Backup der Welt, weil eine Kopie, die einmal draußen ist, draußen bleibt.

Dieser Beitrag gehört zum Handlungsfeld Wiederherstellung und behandelt beides: was du mit Bordmitteln, mit Microsoft 365 Backup und mit Drittanbietern tatsächlich zurückholst, und was du vorher tun musst, damit die zweite Erpressungsstufe ins Leere läuft. Dazu kommt die Client-Seite, denn Ransomware verschlüsselt nicht „die Cloud“ – sie verschlüsselt Dateien auf einem Windows-Rechner, und der Sync-Client trägt das Ergebnis danach ausgesprochen zuverlässig nach oben.

Der Beitrag ist Teil der Serie [Microsoft 365 Security](#), in der die einzelnen Handlungsfelder aufeinander aufbauen. Wenn du gerade mitten in einem Vorfall steckst, hör hier auf zu lesen und arbeite zuerst die ersten Schritte ab – der Rest kann warten.

WARNUNG · Wenn es gerade brennt

Dieser Beitrag ist Vorsorge. Wenn bei dir gerade Dateien verschlüsselt werden, sind andere Dinge wichtiger: Sync-Clients stoppen, damit nicht noch mehr verschlüsselte Versionen hochwandern, betroffene Konten sperren, Sitzungen widerrufen, Beweise sichern. Die Reihenfolge dafür steht im Vorfallsteil der Serie.

Und ein Hinweis, der bitter klingt, aber ernst gemeint ist: Fang jetzt nicht an, aufzuräumen. Jede voreilige Löschaktion vernichtet Spuren, die du in vier Wochen für die Meldung an die Aufsicht brauchst.

Was Microsoft 365 von Haus aus schon kann

Bevor du über Budget für ein Backup-Produkt sprichst, lohnt sich ein ehrlicher Blick darauf, was der Tenant heute schon leistet. Die meisten Organisationen unterschätzen das massiv – und überschätzen es gleichzeitig an genau den Stellen, an denen es wehtut. Beides gleichzeitig ist eine Kunst.

Versionierung: dein wichtigster und meistvergessener Schutz

SharePoint und OneDrive führen für Dokumentbibliotheken standardmäßig einen Versionsverlauf, der mindestens 500 Versionen je Datei aufbewahrt. Verschlüsselt Ransomware eine Datei „in place“, also als Änderung der bestehenden Datei, dann ist die saubere Fassung schlicht eine Version tiefer. Das ist der Grund, warum viele Vorfälle in reinen Cloud-Umgebungen wesentlich glimpflicher ausgehen als in klassischen Dateiservern.

Seit Microsoft die Versionslimits überarbeitet hat, gibt es zwei Betriebsarten. Die automatische Einstellung überlässt die Speicheroptimierung dem Dienst: Er behält jüngere Versionen dicht und dünnt ältere aus. Die manuelle Einstellung setzt eine Obergrenze an Hauptversionen, wahlweise kombiniert mit einer Ablauffrist. Die Oberfläche lässt dabei keine Werte unter 100 Versionen oder unter 30 Tagen zu – über die APIs geht weniger, ist aber ausdrücklich nicht empfohlen, weil du dir damit die Wiederherstellung selbst zusammenkürzt.

Zwei Details, die im Ernstfall den Unterschied machen: Löscht ein Anwender eine einzelne Version von Hand, landet sie im Papierkorb der Website und ist eine Weile rettbar. Werden Versionen dagegen automatisch entfernt, weil das Limit der Bibliothek erreicht ist oder ein Bereinigungsauftrag läuft, gehen sie am Papierkorb vorbei und sind endgültig weg. Und: Für Inhalte, die einer Aufbewahrungsrichtlinie oder einem eDiscovery-Hold unterliegen, werden die Versionslimits ignoriert, solange die Aufbewahrung greift.

FAKTEN · Der Versionsverlauf ist endlich

Ein Angreifer, der weiß, was er tut, verschlüsselt eine Datei nicht einmal, sondern hundertfach. Wenn dein Limit bei 100 Hauptversionen liegt, ist die letzte saubere Fassung nach ein paar Durchläufen aus dem Fenster geschoben – und zwar endgültig, weil limitbedingt entfernte Versionen den Papierkorb überspringen.

Genau deshalb ist der Versionsverlauf eine gute erste Verteidigungslinie, aber keine Sicherung. Microsoft schreibt das inzwischen selbst so: Versionen skalieren nicht für einen großflächigen Vorfall, bei dem eine Administratorin oder ein Administrator die Wiederherstellung orchestrieren muss.

Papierkorb: 93 Tage, und zwar zusammen

SharePoint und OneDrive haben zwei Papierkorbstufen. Gelöschte Elemente wandern zuerst in den Papierkorb der Website, von dort in den Papierkorb der Websitesammlung. Der häufigste Irrtum in Wiederherstellungskonzepten: Es sind nicht 93 Tage pro Stufe, sondern 93 Tage insgesamt, gerechnet ab dem Löschen am ursprünglichen Ort. Wer eine Datei am Tag 80 aus der ersten Stufe entfernt, hat in der zweiten Stufe noch 13 Tage – nicht weitere 93.

Nach Ablauf der 93 Tage gibt es noch ein 14-tägiges Zeitfenster, in dem Microsoft die Daten intern wiederherstellen kann; das läuft dann aber über ein Ticket beim Support und nicht über dein Adminportal. Danach ist Schluss. Für die Planung heißt das: Der Papierkorb ist eine Notreserve für Einzelfälle, kein Aufbewahrungskonzept.

Files Restore: der Zeitreiseknopf für Bibliotheken

Die praktischste Bordfunktion trägt einen unauffälligen Namen. Über „Diese Bibliothek wiederherstellen“ beziehungsweise „OneDrive wiederherstellen“ rollst du eine komplette Dokumentbibliothek oder ein ganzes OneDrive auf einen beliebigen Zeitpunkt der letzten 30 Tage zurück – sekundengenau, inklusive aller Umbenennungen, Löschungen und Überschreibungen in diesem Zeitraum. Erkennt OneDrive selbst einen Ransomware-Verdacht, schlägt es beim Wiederherstellen sogar einen passenden Zeitpunkt vor.

Das ist genau das Werkzeug für den typischen Fall „ein Konto war kompromittiert, eine Teamsite ist hin“. Es hat allerdings drei harte Grenzen: 30 Tage, Bibliotheks- statt Tenant-Ebene, und es hilft nicht bei einer komplett gelöschten Bibliothek. Wenn 800 Sites gleichzeitig betroffen sind, klickst du dich mit dieser Funktion durch ein sehr langes Wochenende.

Exchange Online: Wiederherstellbare Elemente

Auf der Postfachseite heißt der Mechanismus „Wiederherstellbare Elemente“. Standardmäßig bleiben endgültig gelöschte Elemente 14 Tage erhalten, konfigurierbar sind bis zu 30 Tage – und das ist eine der wenigen Stellschrauben, die buchstäblich nichts kostet außer zwei Minuten PowerShell. Die Einzelelementwiederherstellung ist in Exchange Online standardmäßig eingeschaltet.

Das Kontingent für diesen Bereich liegt bei 20 Gigabyte weich und 30 Gigabyte hart. Sobald ein Postfach unter Aufbewahrung oder Beweissicherung steht, steigt das auf 90 beziehungsweise 100 Gigabyte. Teams-Chats liegen übrigens in Exchange-Postfächern und Teams-Dateien in SharePoint oder OneDrive – Teams hat also kein eigenes Wiederherstellungskonzept, sondern erbt das der beiden Dienste darunter.

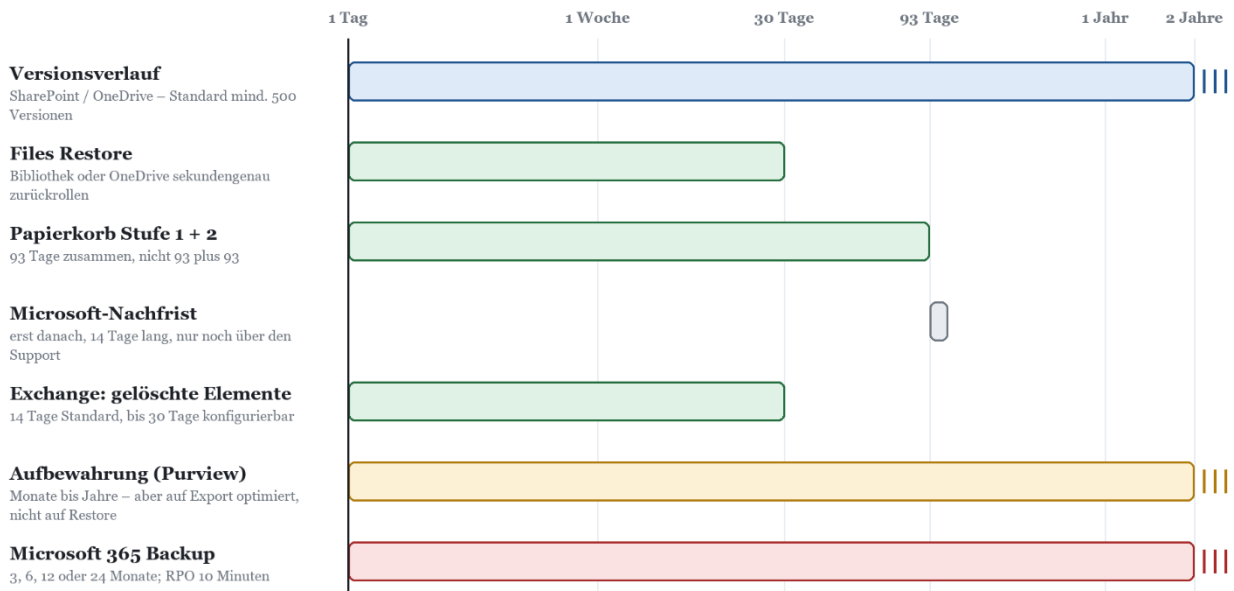
Aufbewahrung ist kein Backup

Aufbewahrungsrichtlinien und -bezeichnungen aus Microsoft Purview verlängern die Haltbarkeit von Inhalten erheblich. Wird ein Dokument unter Aufbewahrung geändert oder gelöscht, landet eine Kopie in der Preservation Hold Library, und die Versionslimits der Bibliothek gelten für dieses Element nicht mehr. Für die Beweisführung nach einem Vorfall ist das Gold wert.

Für die Wiederherstellung ist es das nicht. Aufbewahrung ist auf Export optimiert – auf eDiscovery, auf Recherche, auf einzelne Fundstellen. Sie ist nicht darauf ausgelegt, 400 Websites in einer Nacht auf einen sauberen Stand zurückzusetzen. Wer seine Aufbewahrungsrichtlinie als Backup verkauft, verkauft eine Bibliothekarin als Feuerwehr.

Wie weit zurück kommst du? Die Zeitfenster im Überblick

Balkenlänge = Zeitraum, aus dem du realistisch wiederherstellen kannst



Merke: Der Versionsverlauf hilft nur, solange die Angreifer nicht auch die Versionen aufbrauchen.

Skizze 1: Die Wiederherstellungsfenster der Bordmittel im Vergleich.

Wenn du die Bordmittel nebeneinanderlegst, ergibt sich ein klares Bild davon, wofür sie taugen:

Bordmittel	Zeitfenster	Stark bei	Schwach bei
Versionsverlauf	bis zum Limit,	in-place-Verschlüsselung	vielfacher Überschreibung,

	Standard mind. 500 Versionen	einzelner Dateien	Massenfällen
Papierkorb Stufe 1 und 2	93 Tage insgesamt	versehentlichem und böswilligem Löschen	verschlüsselten Dateien, die nie gelöscht wurden
Files Restore	30 Tage, sekundengenau	einzelnen Bibliotheken und OneDrives	hundertens Sites, gelöschten Bibliotheken
Wiederherstellbare Elemente	14 Tage Standard, bis 30 Tage	gelöschten und manipulierten Mails	allem jenseits von Exchange
Aufbewahrung (Purview)	Monate bis Jahre	Beweissicherung, Nachweisen, eDiscovery	schneller Massenwiederherstellung
Microsoft 365 Backup	3, 6, 12 oder 24 Monate	Massenwiederherstellung mit kurzer RTO	allem außerhalb von SharePoint, OneDrive, Exchange

Microsoft 365 Backup und die Drittanbieter

Irgendwann kippt die Rechnung. Solange du über zehn betroffene Bibliotheken sprichst, sind Bordmittel schnell und kostenlos. Bei tausend Sites reden wir über eine Wiederherstellungsdauer, die dein Geschäft stilllegt als der Angriff selbst. An diesem Punkt kommt ein Backup-Produkt ins Spiel.

Was Microsoft 365 Backup zusätzlich leistet

Microsoft 365 Backup ist ein eigenes, verbrauchsabhängig abgerechnetes Produkt. Es sichert SharePoint-Websites, OneDrive-Konten und Exchange-Postfächer – wahlweise alle oder ausgewählte – und wird im Microsoft 365 Admin Center konfiguriert. Der entscheidende architektonische Punkt: Die Sicherungen entstehen innerhalb der Datengrenzen der geschützten Dienste. Deine Daten verlassen die Vertrauensgrenze von Microsoft 365 nicht und bleiben in der Region, die deine Datenresidenz vorgibt. Nach Azure gehen ausschließlich Metadaten wie Tenant- und Site-Kennungen, und die nur zur Abrechnung.

Der Wiederherstellungszeitraum ist je Richtlinie auf 3 Monate, 6 Monate, 1 Jahr oder 2 Jahre einstellbar; Bestandsrichtlinien stehen auf einem Jahr. Für SharePoint und OneDrive gibt es Wiederherstellungspunkte im 10-Minuten-Raster für die zurückliegenden zwei Wochen und danach wöchentlich bis 52 Wochen zurück; Exchange Online liefert das 10-Minuten-Raster über die vollen 52 Wochen. Die Speicherung erfolgt „append only“ – der Dienst kann bestehende Sicherungskopien technisch gar nicht überschreiben, was Manipulationen an alten Ständen ausschließt.

Beim Tempo liegt der eigentliche Mehrwert. Eine einzelne Website oder ein einzelnes OneDrive ist über einen sogenannten Express-Wiederherstellungspunkt typischerweise in unter 20 Minuten zurück; bei Massenwiederherstellungen nennt Microsoft bis zu 250 Schutzeinheiten pro Stunde und Größenordnungen von ein bis drei Terabyte pro Stunde. Einzelne Dateien und Ordner lassen sich inzwischen granular suchen und zurückholen, ohne die ganze Website zurückzurollen.

FAKTEN · Zahlen, die du für die Budgetdiskussion brauchst

Abrechnung: 0,15 US-Dollar pro Gigabyte geschützter Daten und Monat. Wiederherstellungen selbst sind kostenfrei.

Voraussetzungen: ein gültiges Azure-Abonnement mit eingerichteter Pay-as-you-go-Abrechnung sowie die Rolle SharePoint-Administrator oder Globaler Administrator. Für den laufenden Betrieb gibt es die dedizierte Rolle „Microsoft 365 Backup Administrator“.

Anlauf: Eine neue Schutzrichtlinie braucht rund 60 Minuten zur Verarbeitung und weitere 60

Minuten bis zu den ersten Wiederherstellungspunkten. Ein Backup, das du am Tag des Vorfalls einschaltetest, ist also genau so wertvoll wie ein Feuerlöscher, den du beim Brand bestellst.

Ausstieg: Nach dem Offboarding bleiben die Sicherungen 90 Tage in einer Art Papierkorb erhalten. Aufbewahrungs- und Löschrichtlinien aus Purview berühren das Wiederherstellungsfenster des Backups nicht.

WICHTIG · Was Microsoft 365 Backup nicht abdeckt

Der Umfang ist präzise: SharePoint, OneDrive, Exchange Online. Teams-Inhalte sind nur insoweit dabei, wie sie in diesen drei Diensten liegen. Was nicht gesichert wird: Konfiguration in Entra ID, Conditional-Access-Regeln, Intune-Richtlinien, Power-Platform-Umgebungen, Planner-Pläne und einige ältere Websitevorlagen. Auch SharePoint-Embedded-Container, in denen unter anderem Loop-Arbeitsbereiche liegen, gehören zu den nicht unterstützten Vorlagen.

Ebenfalls nicht abgedeckt: Änderungen an Entwürfen, gesetzte Kennzeichnungen und ähnliche Kleinigkeiten in Postfächern. Gesichert werden Änderungen und Löschungen an abgeschlossenen Elementen – wobei Löschungen immer erfasst werden, unabhängig vom 10-Minuten-Raster.

Kurz: Deine Daten sind geschützt, deine Tenant-Konfiguration nicht. Für die brauchst du einen dokumentierten Wiederaufbau – oder Infrastruktur als Code.

Wann ein Drittanbieter trotzdem sinnvoll ist

Die ehrliche Antwort lautet: häufiger, als Microsoft es gern hätte, und seltener, als der Vertrieb der Backup-Hersteller behauptet. Drei Argumente tragen wirklich.

Erstens die Kopie außerhalb des Mandanten. Wer regulatorisch oder aus Prinzip eine Sicherung braucht, die einen kompletten Tenant-Verlust überlebt – Kontoschließung, vollständige Kompromittierung der Administration, Anbieterwechsel –, kommt an einer externen Kopie nicht vorbei. Microsoft 365 Backup liegt konstruktionsbedingt innerhalb der Microsoft-365-Vertrauensgrenze; das ist für Geschwindigkeit ein Vorteil und für dieses eine Szenario ein Nachteil.

Zweitens der Umfang. Gute Drittlösungen sichern Teams-Strukturen samt Kanälen und Registerkarten, Planner, Entra-Objekte oder Verzeichnisrollen mit. Drittens die Aufbewahrung jenseits von zwei Jahren und die Wiederherstellung in einen anderen Mandanten – Standardanforderung bei Ausgründungen und Zukäufen.

Ein Hinweis, den Microsoft selbst gibt und der zu selten ankommt: Drittanbieterlösungen, die auf der Microsoft 365 Backup Storage Plattform aufsetzen, erben deren Wiederherstellungsgeschwindigkeit. Lösungen, die die Daten stattdessen klassisch über die Graph-API abziehen und woanders ablegen, tun das nicht – und genau das merkst du erst, wenn du 40 Terabyte zurückspielen willst.

WARNUNG · Dein Backup ist selbst ein Angriffsziel

Jede Drittlösung braucht eine App-Registrierung mit weitreichenden Leserechten auf sämtliche Postfächer und Websites. Das ist per Definition das mächtigste Konto in deinem Tenant, und es hat kein Gesicht, keine MFA-Aufforderung und meistens auch keine Ablaufüberwachung für das Geheimnis.

Behandle diese Registrierung entsprechend: eigene Überwachung, kurzlebige Anmeldeinfos, dokumentierte Berechtigungen, Alarm bei jeder Änderung. Und schalte bei Microsoft 365 Backup die Benachrichtigungen für potenziell schädliche Ereignisse ein – bis zu 20 Empfänger werden informiert, wenn jemand Schutzeinheiten entfernt, Richtlinien pausiert oder das Produkt abschaltet.

Wie du App-Registrierungen und erteilte Berechtigungen dauerhaft im Griff behältst, steht in [App-Registrierungen und Consent-Governance](#). Für die grundsätzliche Frage, welche Schrauben im Tenant zuerst angezogen gehören, ist [Tenant-Härtung: die 20 wichtigsten Schrauben](#) der richtige Einstieg.

Kriterium	Bordmittel	Microsoft 365 Backup	Drittanbieter
Kosten	im Abo enthalten	0,15 USD pro GB und Monat	Lizenz je Postfach oder Nutzer plus Speicher
Zeitfenster	30 bis 93 Tage, Versionen je nach Limit	3 bis 24 Monate	frei, oft unbegrenzt
RPO	abhängig von Version und Sync	10 Minuten	typisch 4 bis 24 Stunden
Massenwiederherstellung	unpraktikabel	sehr schnell, bis 250 Einheiten pro Stunde	stark abhängig von der Architektur
Speicherort	im Dienst	innerhalb der Microsoft-365-Datengrenze	beim Anbieter, in Azure oder bei dir
Tenant-Verlust überlebt?	nein	nein	ja, bei externer Ablage
Abdeckung über SPO/ODB/EXO hinaus	nein	nein	je nach Produkt Teams, Planner, Entra
Zusätzliche Angriffsfläche	keine	gering, Rollen im Tenant	App-Registrierung mit Vollzugriff

Double Extortion: warum ein perfektes Backup nicht reicht

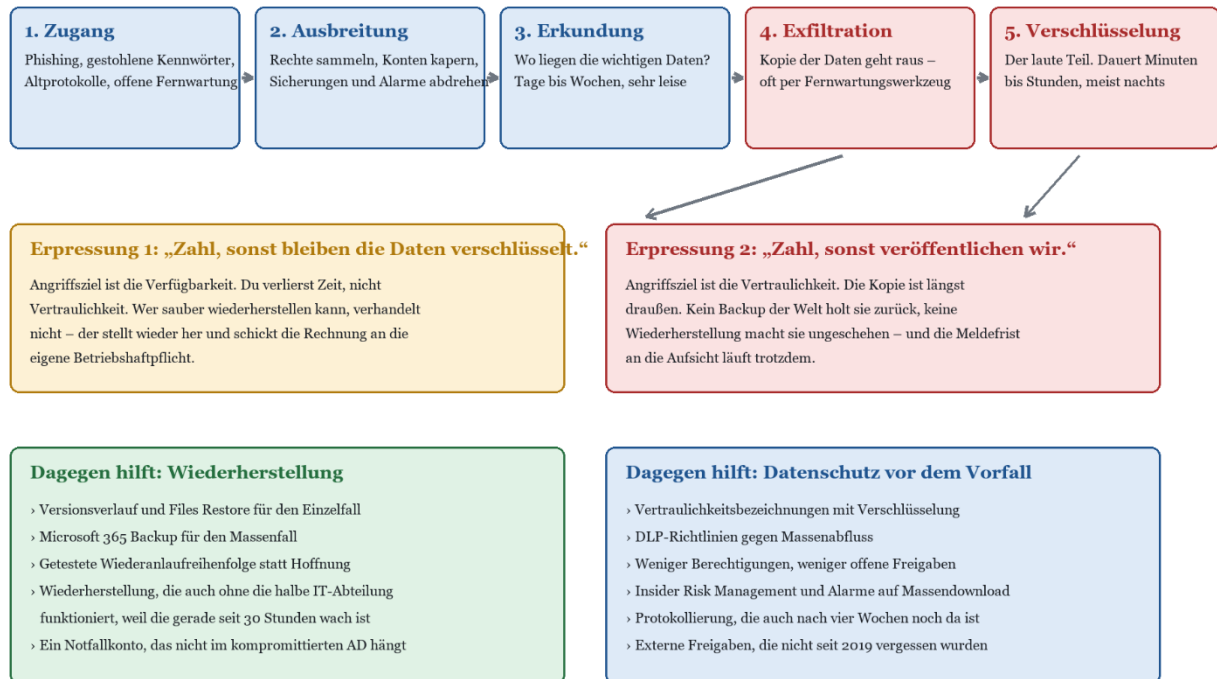
Bis hierher ging es um Verfügbarkeit. Jetzt kommt der Teil, den Backup-Präsentationen gern überspringen, weil er die schöne Geschichte kaputt macht.

Moderne Erpressungsgruppen verschlüsseln nicht mehr einfach. Sie brechen ein, bewegen sich tage- bis wochenlang unauffällig durch die Umgebung, suchen gezielt nach interessanten Daten – Verträge, Personalakten, Konstruktionsunterlagen, Patientendaten, Kalkulationen – und kopieren die heraus. Erst danach wird verschlüsselt. Das Verschlüsseln ist der laute Teil, der Datendiebstahl war der leise. Anschließend gibt es zwei Forderungen: eine für den Schlüssel, eine dafür, dass die Daten nicht auf einer Leak-Seite landen.

In Microsofts Digital Defense Report 2025 zielten 80 Prozent der von der Incident-Response-Einheit untersuchten Vorfälle auf Datendiebstahl ab. Über die Hälfte aller Angriffe mit bekanntem Motiv war durch Erpressung und Ransomware getrieben; reine Spionage machte nur einen kleinen einstelligen Anteil aus. In 79 Prozent der Ransomware-Fälle war mindestens ein Fernwartungswerkzeug im Spiel – also legitime Software, die in keiner Blockliste steht und die deine Administration selbst betreibt.

Double Extortion: zwei Erpressungen, ein Vorfall

Das Backup rettet dich vor der linken Hälfte. Vor der rechten rettet es dich nicht.



Wer nur sichert, ist gegen die Hälfte des Geschäftsmodells geschützt. Die Angreifer wissen das.

Skizze 2: Der Ablauf einer Double-Extortion-Kampagne – und wo Sicherung hilft und wo nicht.

Die Konsequenz ist unbequem, aber logisch: Ein Backup verkürzt die Ausfallzeit und nimmt der ersten Forderung die Grundlage. An der zweiten ändert es exakt nichts. Wenn die Kopie draußen ist, hast du keinen Verfügbarkeitsvorfall mehr, sondern eine Datenschutzverletzung mit Meldepflicht, Betroffeneninformation und einer Presseanfrage, die schneller kommt als dein erstes Lagebild.

Was gegen die zweite Erpressung wirkt

Gegen Veröffentlichung hilft nur, dass die abgeflossenen Daten für die Angreifer wertlos oder gar nicht erst zugänglich sind. Das ist Arbeit, die vor dem Vorfall passiert:

- Vertraulichkeitsbezeichnungen mit Verschlüsselung: Eine Datei, die auch außerhalb des Tenants nur mit gültiger Berechtigung lesbar ist, hat auf einer Leak-Seite wenig Unterhaltungswert.
- DLP-Richtlinien: Sie erkennen und blockieren Massenabflüsse über die Wege, die Angreifer bevorzugen – Weiterleitung nach außen, Kopieren auf Wechseldatenträger, Freigabe an fremde Konten.
- Berechtigungshygiene: Der häufigste Verstärker eines Vorfalls ist ein Konto, das auf alles zugreifen durfte. Wer aufräumt, verkleinert den Radius eines einzelnen kompromittierten Kontos erheblich.
- Alarmer auf Massenzugriffe: Tausend Dateidownloads in zehn Minuten sind kein normales Arbeitsverhalten, auch nicht im Controlling zum Quartalsende.

Bezeichnungen, DLP und Insider-Risiken sind ein eigenes Handlungsfeld – der Einstieg dazu steht im [Kompetenzbereich Microsoft Purview](#). Ergänzend lohnt sich ein Blick darauf, wie du [Gastzugriff](#)

[und externe Freigaben härten](#) – vergessene Freigabelinks sind ein beliebter Abflussweg, der ganz ohne Schadsoftware auskommt.

TIPP · Die Frage, die du der Geschäftsführung stellen solltest

Nicht: „Haben wir ein Backup?“ Sondern: „Welche zehn Datenbestände würden uns wirklich wehtun, wenn sie morgen öffentlich wären – und was schützt genau diese zehn heute?“

Die Antwort auf die erste Frage ist meistens ja und beruhigt niemanden, der schon einmal einen echten Vorfall erlebt hat. Die Antwort auf die zweite Frage ist unangenehm und produziert Budget.

Der Referenzfall vor der Haustür

Wer in Deutschland über Vorsorge diskutiert, braucht kein hypothetisches Szenario. Es gibt genug dokumentierte Fälle, in denen Verwaltungen und Unternehmen wochenlang handlungsunfähig waren, weil Wiederanlauf und Wiederherstellung nicht durchdacht waren – und in denen zusätzlich Daten abgeflossen sind.

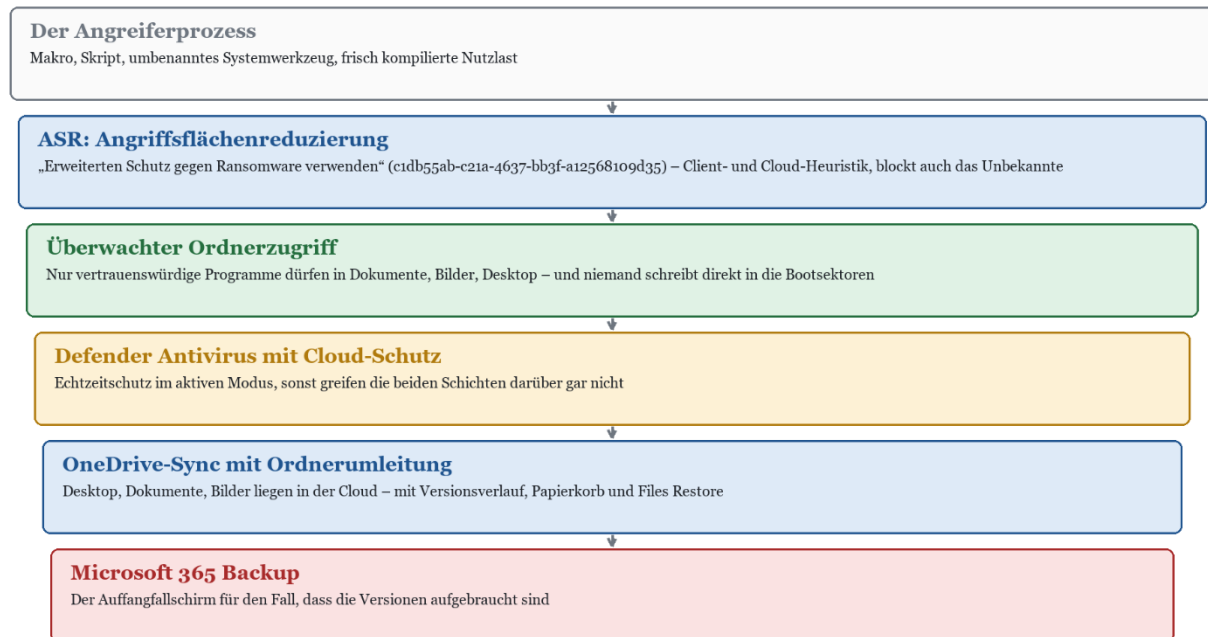
Für die Serie haben wir einen solchen Fall aufgearbeitet: [Dossier TerminalFix und der Berlin-Hack](#). Der Wert liegt weniger in der Frage, wer wie hereingekommen ist – das ist im Nachhinein immer klar –, sondern darin, welche Entscheidungen in den ersten Stunden getroffen wurden und wie lange die Wiederherstellung tatsächlich gedauert hat. Genau diese Zahlen fehlen in den meisten internen Notfallkonzepten, und genau sie brauchst du, wenn du dein eigenes Wiederherstellungsziel begründen willst.

Die Client-Seite: dort, wo verschlüsselt wird

Es gibt eine hartnäckige Vorstellung, dass Ransomware „die Cloud angreift“. Tut sie nicht. Sie läuft auf einem Windows-Rechner, verschlüsselt dort lokale Dateien und alles, was über Netzlaufwerke oder Sync-Clients erreichbar ist, und der OneDrive-Client lädt die verschlüsselten Fassungen anschließend zuverlässig hoch. Der beste Ransomware-Schutz für deinen Tenant ist deshalb ein Endgerät, auf dem der Verschlüsselungsprozess gar nicht erst zum Zug kommt.

Wo die Verschlüsselung wirklich passiert: die Schichten am Endgerät

Ransomware verschlüsselt nicht „die Cloud“. Sie verschlüsselt Dateien auf einem Windows-Rechner – der Sync-Client trägt das Ergebnis dann brav hoch.



Reihenfolge des Rollouts: erst Überwachungsmodus, dann blockieren. Wer umgekehrt vorgeht, lernt das Helpdesk-Team sehr schnell besser kennen.

Skizze 3: Die Schutzschichten am Endgerät – jede Schicht fängt ab, was die darüber durchgelassen hat.

Die ASR-Regel gegen Ransomware

Unter den Regeln zur Reduzierung der Angriffsfläche gibt es eine, die genau für diesen Zweck gebaut wurde: „Erweiterten Schutz gegen Ransomware verwenden“, intern die Kennung c1db55ab-c21a-4637-bb3f-a12568109d35. Sie kombiniert Heuristik auf dem Client mit Cloud-Bewertung und entscheidet, ob eine Datei sich wie Ransomware verhält.

Der entscheidende und zugleich unbequeme Teil steht in Microsofts eigener Beschreibung: Diese Regel blockiert nicht nur Dateien mit schlechter Reputation, sondern ausdrücklich auch solche, die noch keine positive Reputation haben. Nicht blockiert wird, was in der Microsoft-Cloud als unschädlich bekannt ist, was gültig signiert ist oder was verbreitet genug ist, um nicht als Ransomware zu gelten.

Übersetzt heißt das: Deine frisch kompilierte Branchenanwendung, die einmal im Jahr aktualisiert wird und die niemand außerhalb deines Hauses kennt, ist ein Kandidat für einen Fehlalarm. Solche Blockaden lösen sich in der Regel von selbst auf, sobald die Reputation der Datei steigt. Wenn nicht, konfigurierst du einen regelspezifischen Ausschluss – wobei diese Regel nur begrenzte Ausschlussmöglichkeiten bietet.

WICHTIG · Ohne Cloud-Schutz keine Wirkung

Die Regel setzt Microsoft Defender Antivirus und aktivierten Cloud-Schutz voraus. Ist der Cloud-Schutz aus – aus Datenschutzgründen, aus Gewohnheit, weil es vor Jahren einmal jemand deaktiviert hat –, läuft die Regel ins Leere.

Ebenfalls prüfen: Defender Antivirus muss im aktiven Modus laufen. Passivmodus neben einem Drittprodukt reicht für die Regel und für den überwachten Ordnerzugriff nicht.

Die Regel wirft Meldungen an die Anwender und erzeugt EDR-Warnungen, das heißt: Du siehst die Treffer auch zentral im Defender-Portal, statt sie aus lokalen Ereignisprotokollen

zusammenzusuchen.

Überwacher Ordnerzugriff

Der überwachte Ordnerzugriff dreht das Prinzip um: Statt zu erkennen, was böse ist, erlaubt er Schreibzugriffe auf geschützte Ordner nur vertrauenswürdigen Programmen. Geschützt sind standardmäßig Dokumente, Bilder, Musik, Videos und Favoriten der Benutzer- und Systemkonten sowie die öffentlichen Entsprechungen – und die Bootsektoren der Festplatte. Die Standardliste kannst du nicht ändern, aber erweitern; Netzwerkfreigaben und verbundene Laufwerke werden unterstützt.

Ein Detail, das den Zusammenhang zur Cloud herstellt: Wenn die Ordnerumleitung (Known Folder Move) Dokumente, Bilder und Desktop nach OneDrive verschiebt, schützt der überwachte Ordnerzugriff den Ordner an seinem umgeleiteten Ort. Ordnerumleitung und Client-Schutz greifen also ineinander – und du bekommst gleichzeitig Versionsverlauf und Files Restore für die Benutzerdaten obendrauf.

Vertrauenswürdige Programme bestimmt Defender überwiegend selbst anhand von Verbreitung und Reputation. Was blockiert wird, kannst du gezielt zulassen, dabei sind Umgebungsvariablen und Platzhalter im Pfad erlaubt. Eine wichtige Ausnahme: Skript-Interpreter wie PowerShell gelten grundsätzlich als nicht vertrauenswürdig, und daran ändert auch ein Zulassungsindikator nichts – die einzige Möglichkeit ist, sie explizit als zugelassene Anwendung einzutragen. Was man, mit Verlaub, sehr gut überlegen sollte.

Modus	Wert	Wirkung	Wofür geeignet
Deaktiviert	0	kein Schutz	Ausgangszustand
Aktiviert (Blockieren)	1	nicht vertrauenswürdige Programme dürfen nicht schreiben	Zielzustand nach der Auswertung
Überwachungsmodus	2	Zugriffe werden protokolliert, nicht blockiert	Pflichtübung vor dem Scharfschalten
Nur Datenträgeränderung blockieren	3	schützt nur die Bootsektoren	pragmatischer Einstieg, kaum Fehlalarme
Nur Datenträgeränderung überwachen	4	protokolliert Schreibzugriffe auf Bootsektoren	Vorstufe zu Modus 3

TIPP · Der pragmatische Einstieg

Wenn dir der volle Ordnerschutz zu viel Feinarbeit ist, fang mit Modus 3 an: Nur Schreibzugriffe auf die Bootsektoren werden blockiert. Legitime Software schreibt dort praktisch nie, Fehlalarme sind entsprechend selten – und du bist gegen Bootkits und Wiper geschützt, während der Ordnerschutz parallel im Überwachungsmodus seine Ausnahmeliste aufbaut.

Zwei Wermutstropfen für die Planung: Der überwachte Ordnerzugriff ist eine Windows-Funktion und steht auf Linux und macOS auch dann nicht zur Verfügung, wenn die Geräte in Defender for Endpoint eingebunden sind. Und bei Netzwerkfreigaben kann der Schutz spürbar Leistung kosten, weil jeder Zugriff eines nicht vertrauenswürdigen Prozesses den Dateiserver befragt.

Beide Funktionen brauchen sauber eingebundene Geräte. Wie das ohne wochenlanges Ringen mit dem Clientmanagement gelingt, steht in [Defender for Endpoint: Onboarding ohne Drama](#). Und

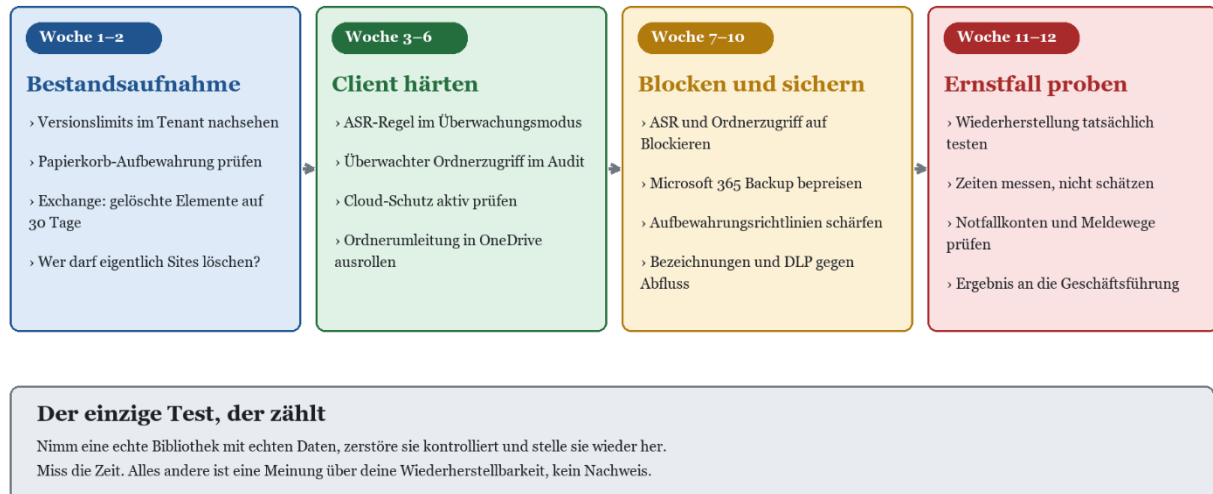
weil der häufigste Einstiegsweg immer noch eine Mail ist, gehören [Defender for Office 365: Safe Links und Safe Attachments](#) sowie das Abschalten von [Legacy Authentication](#) in dasselbe Paket.

Vom Konzept zum Fahrplan

Ransomware-Vorsorge scheitert selten an fehlendem Wissen. Sie scheitert daran, dass sie als Großprojekt gedacht wird, für das nie der richtige Moment ist. Also machen wir sie klein.

Ein Fahrplan, den du auch neben dem Tagesgeschäft schaffst

Vier Etappen. Keine davon braucht ein Projekt mit Lenkungsausschuss.



Skizze 4: Ein Fahrplan über zwölf Wochen, der neben dem Tagesgeschäft funktioniert.

Die Bestandsaufnahme, die niemand macht

Bevor du irgendetwas einschaltest, beantworte fünf Fragen schriftlich. Erstens: Welche Versionslimits gelten in deinem Tenant – automatisch oder manuell, und mit welchen Werten? Zweitens: Wie lange bleiben gelöschte Elemente in Exchange erhalten, 14 Tage oder 30? Drittens: Wer darf Websites und Postfächer löschen? Viertens: Welche Daten wären bei einer Veröffentlichung existenzbedrohend? Fünftens: Wie lange darf die Wiederherstellung dauern, bevor der Betrieb ernsthaft Schaden nimmt?

Die fünfte Frage ist die einzige, die nicht die IT beantwortet. Sie kommt aus dem Geschäft, und ohne eine Zahl daraus lässt sich weder ein Backup-Produkt begründen noch ein Verzicht darauf.

Reihenfolge beim Ausrollen

Für die Client-Schutzfunktionen gilt ausnahmslos: erst Überwachungsmodus, dann blockieren. Zwei bis vier Wochen Beobachtung reichen in den meisten Umgebungen, um die Ausnahmen zu finden. Wer die Regeln direkt scharf stellt, lernt am ersten Montagmorgen sein Helpdesk-Team von einer neuen Seite kennen – und die Wahrscheinlichkeit, dass die Regel danach dauerhaft ausgeschaltet bleibt, liegt erfahrungsgemäß nahe bei eins.

Für die Cloud-Seite gilt das Gegenteil: Die Verlängerung der Aufbewahrung wiederherstellbarer Elemente auf 30 Tage, das Nachziehen der Versionslimits und das Einschalten der Benachrichtigungen kannst du sofort machen. Diese Änderungen haben kein Störpotenzial und wirken ab der ersten Minute.

Der Test, der zählt

Eine Wiederherstellung, die nie durchgeführt wurde, ist keine Wiederherstellung, sondern eine Absichtserklärung. Nimm eine echte Bibliothek mit echten Daten, zerstöre sie kontrolliert – Massenumbenennung, Massenüberschreibung, Löschung – und stelle sie wieder her. Miss die Zeit. Miss auch, wie lange es dauert, bis jemand den Schaden überhaupt bemerkt.

Diese zweite Zahl ist meistens die unangenehmere. In vielen Organisationen fällt eine großflächige Verschlüsselung erst auf, wenn morgens die ersten Anrufe kommen. Alarmrichtlinien auf Massenlöschung, Massendownload und ungewöhnliche Dateiumbenennungen kürzen dieses Fenster von Stunden auf Minuten.

Wie du solche Alarme aufsetzt, ohne im Rauschen zu ertrinken, steht in [Alert Policies und Benachrichtigungen richtig aufsetzen](#). Den Ablauf für den Ernstfall selbst hältst du im [Incident-Response-Plan für Microsoft 365](#) fest – und probst ihn in einer [Feuerwehrübung](#), bevor es ernst wird.

TIPP · Drei Dinge für den Montagmorgen

1. Prüfe in der Exchange-Verwaltung, ob die Aufbewahrung gelöschter Elemente auf 30 Tage steht. Wenn nicht, änderst du das heute. Es kostet nichts.
2. Schalte die ASR-Regel gegen Ransomware in den Überwachungsmodus. Auch das kostet nichts und liefert dir in zwei Wochen belastbare Daten darüber, was bei dir überhaupt auffallen würde.
3. Schreib auf, wie lange eine vollständige Wiederherstellung deiner drei wichtigsten SharePoint-Websites dauern würde. Wenn du es nicht weißt, hast du dein erstes Testszenario gefunden.

Häufige Fragen

Brauche ich überhaupt ein Backup, wenn Microsoft doch alles repliziert?

Replikation und Sicherung lösen unterschiedliche Probleme. Die Replikation sorgt dafür, dass deine Daten einen Rechenzentrumsausfall überstehen – sie bildet aber immer den aktuellen Stand ab, auch wenn der aktuelle Stand verschlüsselt ist. Ein Backup gibt dir einen früheren, gesunden Zustand zurück. Microsoft formuliert das selbst so und hat an der geteilten Verantwortung für Datensicherung nichts geändert: Der Dienst hält die Plattform verfügbar, für die Wiederherstellbarkeit deiner Inhalte sorgst du.

Reicht der Versionsverlauf nicht aus?

Für den Einzelfall oft ja. Für den Ernstfall nein. Versionen sind ein Selbstbedienungswerkzeug für einzelne Dateien und Bibliotheken; sie skalieren nicht für einen Vorfall, bei dem hunderte Websites gleichzeitig betroffen sind, und sie können aufgebraucht werden, wenn ein Angreifer oft genug überschreibt. Dazu kommt: Versionen, die wegen eines Limits entfernt werden, gehen am Papierkorb vorbei und sind endgültig weg.

Verlassen die Daten bei Microsoft 365 Backup den Tenant?

Nein. Die Sicherungen entstehen innerhalb der Datengrenzen der geschützten Dienste und respektieren deine Datenresidenz. Nach Azure gehen nur Metadaten wie Tenant- und Site-Kennungen, ausschließlich zur Abrechnung. Das ist für Geschwindigkeit und Datenschutz ein Vorteil – und gleichzeitig der Grund, warum das Produkt einen vollständigen Verlust des Mandanten nicht abdeckt.

Was kostet Microsoft 365 Backup?

0,15 US-Dollar pro Gigabyte geschützter Daten und Monat, Wiederherstellungen sind kostenfrei. Abgerechnet wird verbrauchsabhängig über ein verknüpftes Azure-Abonnement mit eingerichteter Pay-as-you-go-Abrechnung. Rechne vorher aus, wie viel dein SharePoint- und Postfachbestand tatsächlich umfasst – die Zahl überrascht die meisten in beide Richtungen.

Schützt ein Backup vor der Veröffentlichung meiner Daten?

Nein, und das ist der wichtigste Satz dieses Beitrags. Ein Backup stellt Verfügbarkeit wieder her. Gegen die Drohung, die abgeflossene Kopie zu veröffentlichen, wirken nur Maßnahmen, die vor dem Abfluss greifen: Vertraulichkeitsbezeichnungen mit Verschlüsselung, DLP, weniger Berechtigungen, Alarmer auf Massenzugriffe. Wer nur sichert, ist gegen die Hälfte des Geschäftsmodells geschützt.

Blockiert die ASR-Regel meine Fachanwendungen?

Möglicherweise – vor allem selten genutzte, frisch kompilierte oder nicht signierte Software. Die Regel blockiert bewusst auch Dateien ohne positive Reputation. In der Regel lösen sich solche Blockaden mit steigender Verbreitung von selbst auf; andernfalls kannst du regelspezifische Ausschlüsse setzen oder mit einem Zulassungsindikator arbeiten. Deshalb: erst Überwachungsmodus, dann blockieren.

Wie lange darf ich mir für die Wiederherstellung Zeit lassen?

Das entscheidet nicht die IT, sondern das Geschäft. Als Orientierung: Microsoft gibt für Microsoft 365 Backup bei einer einzelnen Website unter 20 Minuten an und bei großen Wiederherstellungen bis zu 250 Schutzeinheiten pro Stunde. Wer mit Bordmitteln arbeitet, sollte für jede betroffene Bibliothek einige Minuten Handarbeit einplanen – bei 500 Bibliotheken ist das ein sehr langes Wochenende.

Sind Teams-Daten mitgesichert?

Teilweise. Teams-Chats liegen in Exchange-Postfächern, Teams-Dateien in SharePoint und OneDrive – diese Inhalte sind über die jeweiligen Mechanismen abgedeckt. Die Teams-Struktur selbst, also Kanäle, Registerkarten und Einstellungen, gehört nicht zum Umfang von Microsoft 365 Backup. Dafür brauchst du entweder eine Drittlösung oder einen dokumentierten Wiederaufbau.

Was ist mit unseren Servern und Dateifreigaben vor Ort?

Für die gilt nichts von alledem. Dieser Beitrag deckt Microsoft 365 ab; klassische Dateiserver, Hypervisoren und Datenbanken brauchen ein eigenes Sicherungskonzept mit unveränderlichen Kopien und einem Stand außerhalb der Domäne. Der Zusammenhang ist trotzdem eng: Wer sein Active Directory verliert, verliert in der Regel auch den Zugang zum Tenant – weshalb Notfallkonten dorthin gehören, wo die Domäne sie nicht mit in den Abgrund zieht.

Wie solche Konten aussehen, steht in [Break-Glass-Konten anlegen und überwachen](#).

Zählt Ransomware-Vorsorge auf NIS2 ein?

Ja, und zwar mehrfach. Sicherheitsmanagement, Wiederherstellung und Krisenmanagement gehören zu den ausdrücklich genannten Risikomanagementmaßnahmen. Wer die Wiederherstellung testet und dokumentiert, erledigt Vorsorge und Nachweispflicht in einem Aufwasch – was die Diskussion über das Budget deutlich vereinfacht.

Die technische Seite dazu steht in [NIS2 aus Security-Sicht: technische Maßnahmen in M365](#).

Fazit

Microsoft 365 gibt dir eine erstaunlich gute Ausgangslage: Versionsverlauf, zwei Papierkorbstufen, 30 Tage sekundengenaues Zurückrollen, wiederherstellbare Elemente in Exchange und eine Aufbewahrung, die im Zweifel Jahre trägt. Für den Einzelfall reicht das oft. Für den Massenfall reicht es nicht, und dafür gibt es mit Microsoft 365 Backup ein Produkt, das genau diese Lücke schließt – schnell, innerhalb der Datengrenze und mit einem Preismodell, das man ausrechnen kann. Wer eine Kopie außerhalb des Mandanten braucht oder mehr als SharePoint, OneDrive und Exchange sichern will, greift zusätzlich zu einem Drittanbieter und behandelt dessen App-Registrierung dann wie das mächtige Konto, das sie ist.

Der Teil, der am häufigsten fehlt, ist aber weder das eine noch das andere. Es ist die Erkenntnis, dass Wiederherstellung nur gegen die erste Erpressung hilft. Die zweite – Veröffentlichung – gewinnst du nur mit Arbeit, die lange vor dem Vorfall passiert: Bezeichnungen, DLP, aufgeräumte Berechtigungen, Alarme auf Massenzugriffe. Und am Endgerät mit zwei Schaltern, die kein Geld kosten und in fast keinem Tenant aktiv sind: der ASR-Regel gegen Ransomware und dem überwachten Ordnerzugriff.

Wenn du nach diesem Beitrag genau eine Sache machst, dann diese: Stelle eine echte Bibliothek wieder her und stoppe die Zeit. Alles andere ist eine Meinung über deine Wiederherstellbarkeit. Das Ergebnis ist ein Nachweis – und, ganz nebenbei, die beste Folie, die du der Geschäftsführung je gezeigt hast.

WEITER IM THEMA

- › [Microsoft 365 Security](#) — die Serie mit allen Handlungsfeldern im Überblick
- › [Phishing-Vorfall: die ersten 60 Minuten](#) — der Einstiegsweg, der die meisten Vorfälle eröffnet
- › [Kompromittiertes Konto erkennen und aufräumen](#) — bevor aus einem Konto ein Vorfall wird
- › [Incident-Response-Plan für Microsoft 365](#) — der Ablauf für den Ernstfall
- › [Kompetenzbereich Microsoft Purview](#) — Bezeichnungen und DLP gegen die zweite Erpressung
- › [Dossier TerminalFix und der Berlin-Hack](#) — der Referenzfall mit echten Zahlen
- › [MFA in Microsoft 365 richtig einführen](#) — die wirksamste Einzelmaßnahme gegen den Erstzugang
- › [Security-Reporting für die Geschäftsführung](#) — damit aus dem Test ein Budget wird
- › [Microsoft 365 Security Beratung](#) — wenn du den Fahrplan lieber begleitet aufsetzt
- › [Schulung Microsoft 365 Security](#) — für Teams, die es selbst können wollen