

Notfallübung für die Verwaltungs-IT: SharePoint verschlüsselt, Admin-Konto übernommen, Bürgertelefon tot

Es gibt einen Satz, den man in Verwaltungen erstaunlich oft hört, und er ist fast immer falsch: „Wir haben ein Notfallkonzept.“ Was gemeint ist: Es gibt ein Dokument. Es liegt in einer Bibliothek. Es wurde vom Amt für Organisation freigegeben, es hat eine Versionsnummer, und der letzte Mensch, der es gelesen hat, ist inzwischen im Ruhestand. Ob es funktioniert, weiß niemand. Man wird es erfahren.

Notfallpläne teilen ein Schicksal mit Feuerlöschern: Beide sehen an der Wand sehr beruhigend aus, und beide werden erst in dem Moment interessant, in dem niemand mehr Zeit hat, die Bedienungsanleitung zu lesen. Der Unterschied ist, dass die Feuerwehr regelmäßig übt und die IT in der Regel nicht. In den Verwaltungen, die ich begleite, existiert häufig eine sehr solide Dokumentation der Technik und praktisch keine Erfahrung mit dem Ernstfall. Das ist keine Nachlässigkeit, sondern eine Frage der Reihenfolge: Erst wird eingeführt, dann wird betrieben, und irgendwann kommt das Thema Notfall. Nur kommt der Notfall manchmal früher.

Dieser Beitrag beschreibt kein Notfallhandbuch. Er beschreibt ein Format: die moderierte Übung mit drei Szenarien, wie sie sich an einem einzigen Tag mit einem realistischen Teilnehmerkreis durchführen lässt. SharePoint verschlüsselt, Admin-Konto übernommen, Bürgertelefon tot. Drei Lagen, die in Kommunen, Kreisen, Landesbehörden, Zweckverbänden und bei kirchlichen Trägern gleichermaßen weh tun, und die in ihrer Kombination fast alles abdecken, was in einem Microsoft-365-Betrieb schiefgehen kann: Daten, Identitäten, Erreichbarkeit.

Ich beschreibe für jedes Szenario den Ablauf, die Rollen, die Beobachtungspunkte und die Erkenntnisse, die in der Auswertung mit bemerkenswerter Zuverlässigkeit auftauchen. Sie werden feststellen, dass die Befunde selten technischer Natur sind. Die Technik funktioniert meistens. Was fehlt, ist die Vertretung, die Dokumentation und die Ruhe.

Warum die Übung mehr bringt als das nächste Konzept

Der Satz, den Sie mitnehmen sollten

Wenn Sie aus diesem Beitrag nur einen einzigen Gedanken behalten, dann diesen: Große Schäden entstehen nicht, weil jemand, der es nicht kann, hilflos danebensteht. Große Schäden entstehen, weil jemand, der es kann, unter Druck den falschen Knopf drückt.

Das ist kein rhetorischer Effekt, sondern die Erfahrung aus jeder ernsthaften Nachbetrachtung. Der Kollege aus dem Betrieb, der seit vierzehn Jahren die Umgebung kennt, sieht am Freitagnachmittag verschlüsselte Dateien, denkt „das kriege ich hin“, startet die Wiederherstellung über eine Bibliothek, die noch synchronisiert wird, und produziert innerhalb von zwanzig Minuten einen Zustand, den vorher niemand hatte: halb wiederhergestellt, halb verschlüsselt, vollständig undokumentiert. Ein Mensch ohne Berechtigung hätte weniger Schaden angerichtet, weil er nichts hätte tun können.

Kompetenz plus Zeitdruck plus fehlende Absprache ist die gefährlichste Kombination im Notfall. Genau die trainiert eine Übung – nicht das Wissen, sondern die Fähigkeit, kurz innezuhalten, bevor man handelt, und die Frage zu stellen, die im Ernstfall zählt: Wer entscheidet das gerade, und wer schreibt mit?

WICHTIG · Was eine Übung wirklich prüft

Nicht das Können der Belegschaft. Nicht die Qualität der Technik. Sondern drei organisatorische Größen: Wie lange dauert es, bis die richtige Person am Tisch sitzt? Wie lange dauert es, bis jemand entscheidet? Und findet irgendjemand die Unterlagen, die er dafür braucht?

Alle drei Größen lassen sich in Minuten messen. Alle drei sind unabhängig vom Hersteller, vom Betriebsmodell und davon, ob Ihr Tenant beim kommunalen Rechenzentrum, beim Systemhaus oder in Eigenregie betrieben wird.

Was eine Übung ist – und was sie nicht ist

Eine Notfallübung ist kein Penetrationstest, keine Revision und kein Leistungsnachweis. Sie ist ein moderiertes Rollenspiel mit realistischen Einspielungen, in dem bewusst nichts angefasst wird, was produktiv läuft. Niemand meldet sich an, niemand löscht etwas, niemand ruft eine echte Behördennummer an. Es wird geredet, entschieden und protokolliert.

Diese Abgrenzung müssen Sie am Anfang aussprechen, und zwar so deutlich, dass sie im Protokoll steht. Sonst passiert Folgendes: Die IT-Leitung sitzt mit verschränkten Armen da, weil sie befürchtet, dass die Übung ein verstecktes Audit ist. Die Sachbearbeitung antwortet vorsichtig, weil sie nicht weiß, wer die Notizen bekommt. Und der Personalrat hat aus gutem Grund Fragen. Alle drei Reaktionen sind vernünftig – und alle drei ruinieren die Übung, wenn man sie nicht vorher ausräumt.

Der Rahmen, den das Bundesamt für Sicherheit in der Informationstechnik im BSI-Standard 200-4 für das Business Continuity Management beschreibt, ist dabei ein brauchbarer Bezugspunkt. Er unterscheidet Planübungen, Funktionsübungen und Vollübungen und empfiehlt eine rollierende Planung: jährlich mindestens eine Planübung für den Krisenstab plus eine Funktionsübung an einem der kritischen Wiederanlaufpläne, alle zwei bis drei Jahre eine umfassendere Übung. Was hier beschrieben wird, ist eine Planübung mit drei Lagen – das Format mit dem besten Verhältnis von Aufwand zu Erkenntnis.

FAKTEN · Die Lage, nüchtern betrachtet

Das BSI führt Kommunen in seinem Lagebericht 2025 neben kleinen und mittleren Unternehmen und IT-Dienstleistern ausdrücklich als eine der Hauptzielgruppen von Angriffen. Für den Berichtszeitraum wurden rund 950 Ransomware-Vorfälle gemeldet; das Dunkelfeld liegt erfahrungsgemäß deutlich darüber.

Der Angriff auf einen kommunalen IT-Dienstleister in Südwestfalen in der Nacht zum 30. Oktober 2023 betraf 72 Mitgliedskommunen und wirkte darüber hinaus auf mehr als 50 weitere Kommunen und Kreise. Pass- und Zulassungsstellen waren wochenlang eingeschränkt, der Wiederaufbau zog sich über Monate. Lösegeld wurde nicht gezahlt.

Die Lehre daraus ist nicht, dass Dienstleister schlecht arbeiten – die Zusammenarbeit mit einem kommunalen Rechenzentrum oder einem Systemhaus bleibt für die meisten Verwaltungen der

sinnvollste Weg. Die Lehre ist, dass ein Ausfall beim Dienstleister für Ihr Rathaus dieselbe Wirkung hat wie ein Ausfall im eigenen Serverraum: Der Schalter im Bürgerbüro bleibt zu.

Die Übung setzt voraus, dass die Grundentscheidungen getroffen sind: Betriebsmodell, Schutzbedarf, Rollenmodell, Aufbewahrung. Wenn Sie an dieser Stelle stehen und noch weiter vorn im Weg sind, finden Sie die Zusammenhänge im Überblicksbeitrag [Microsoft 365 in der öffentlichen Verwaltung](#), der die einzelnen Bausteine dieser Serie einordnet. Für die Übung selbst brauchen Sie vor allem eines: eine ehrliche Vorstellung davon, welche Fachverfahren wirklich am Tenant hängen. Der Abgleich mit dem IT-Grundschutz in [Schutzbedarf und Microsoft 365: IT-Grundschutz-Abgleich für die Praxis](#) liefert dafür die Vorarbeit.



Die Übung prüft die Organisation, nicht die Belegschaft. Wer das verwechselt, bekommt beim nächsten Mal niemanden mehr an den Tisch.

Skizze 1: Der Aufbau einer moderierten Übung. Links die Einspielungen, in der Mitte der Tisch, rechts die Beobachtung – und unten die Auswertung, ohne die der ganze Tag folgenlos bleibt.

Das Format: Rollen, Regeln, Takt

Wer am Tisch sitzt

Die häufigste Fehlbesetzung einer Notfallübung ist eine reine IT-Runde. Das ist verständlich – die IT organisiert die Übung, also lädt sie die IT ein – und es macht die Übung wertlos. Denn die interessanten Fragen entstehen genau an den Nahtstellen: Darf das Bürgerbüro schließen? Wer sagt der Pressestelle Bescheid? Wann meldet der Datenschutz an die Aufsicht? Und wer entscheidet, ob die Kämmerei die Zahlläufe von Hand macht?

Für eine belastbare Übung brauchen Sie die folgenden Rollen. Nicht alle müssen mit Leitungspersonal besetzt sein, aber jede Rolle braucht einen Menschen, der im Ernstfall tatsächlich dafür zuständig wäre.

Rolle	Aufgabe in der Übung	Typische Besetzung	Fallstrick
Übungsleitung	Gibt Einspielungen, hält Zeit, greift nicht ein	Externe Moderation oder Person ohne operative Rolle	Wer selbst mitspielen will, moderiert nicht
Verwaltungsspitze	Entscheidet über Betriebseinschränkungen	Bürgermeister, Dezernent, Amtsleitung	Erscheint zur Begrüßung und geht wieder
IT-Leitung	Koordiniert Technik, Dienstleister, Prioritäten	Leitung der IT oder des Fachdienstes	Rutscht in die Rolle des Bedieners statt zu führen
Organisationsamt	Kennt Prozesse, Vertretungen, Fristen	Amt für Organisation, Hauptamt	Wird gar nicht erst eingeladen
Datenschutz	Prüft Betroffenheit und Meldewege	Behördlicher Datenschutzbeauftragter	Meldet reflexhaft, bevor die Lage klar ist
Kommunikation	Sprachregelung intern und nach außen	Pressestelle, Büro der Verwaltungsspitze	Fehlt komplett und wird improvisiert
Registratur	Kennt Aktenplan, Aufbewahrung, Aussonderung	Registratur, Archiv	Gilt als nicht betroffen – ist aber Kern des Schadens
Personalrat	Begleitet, prüft die Übungsregeln	Personalrat, in kirchlichen Häusern die Mitarbeitervertretung	Wird erst am Übungstag informiert
Beobachtung	Schreibt mit, bewertet nicht	Zwei Personen ohne Spielrolle	Mischt sich ein und verdirbt den Befund

Ein Wort zur Beobachtung, weil diese Rolle regelmäßig unterschätzt wird: Zwei Personen, die konsequent schweigen, produzieren den gesamten Mehrwert der Veranstaltung. Sie notieren Uhrzeiten, Entscheidungen und wörtliche Zitate. Sie notieren nicht, wer etwas gesagt hat. Ein Beobachtungsprotokoll, in dem Namen stehen, ist keine Übungsdokumentation, sondern ein Personalvorgang – und beim nächsten Mal kommt niemand mehr.

Die Regeln, die vorher feststehen müssen

- **Keine Produktivsysteme.** Es wird nicht angemeldet, nicht gelöscht, nicht gesperrt. Alles läuft am Tisch. Wer wissen will, ob ein Handgriff technisch funktioniert, braucht eine Funktionsübung in einer Testumgebung – das ist ein anderes Format.
- **Keine echten Rufnummern.** Weder die Leitstelle noch die Aufsichtsbehörde noch die Lokalzeitung werden angerufen. Die Übungsleitung spielt sie.
- **Keine Namen im Protokoll.** Befunde werden über Rollen formuliert: „Die Entscheidung über die Abschaltung lag nach 40 Minuten noch bei niemandem“ – nicht: „Herr X hat nicht entschieden.“
- **Kein Abbruch bei Fehlern.** Wenn die Runde eine falsche Entscheidung trifft, greift die Übungsleitung nicht ein. Der Fehler ist das Material.
- **Feste Endzeit.** Neunzig Minuten pro Szenario, Auswertung inklusive. Wer überzieht, verliert die Runde für das zweite Szenario.

WARNUNG · Beteiligung: bitte vorher, nicht nachher

Eine Übung, in der beobachtet wird, wie Menschen unter Druck arbeiten, berührt Beteiligungsrechte

– auch wenn nichts technisch gemessen wird und keine Leistungsdaten erhoben werden. Klären Sie mit dem Personalrat vorab, was protokolliert wird, wer die Protokolle bekommt und wie lange sie aufbewahrt werden. In der Praxis reicht dafür meist eine kurze schriftliche Verabredung; eine eigene Dienstvereinbarung ist selten nötig, kann aber sinnvoll sein, wenn Übungen zur Regel werden sollen.

In kirchlichen Häusern tritt an die Stelle des Personalrats die Mitarbeitervertretung, und der datenschutzrechtliche Rahmen ist ein anderer – die Unterschiede sind in [Microsoft 365 in Kirche, Diakonie und Caritas: DSG-EKD, KDG und Mitarbeitervertretung](#) beschrieben. Bausteine für den Fall, dass Sie ohnehin an einer Dienstvereinbarung arbeiten, finden Sie in [Copilot und Personalrat: Bausteine einer Dienstvereinbarung](#).

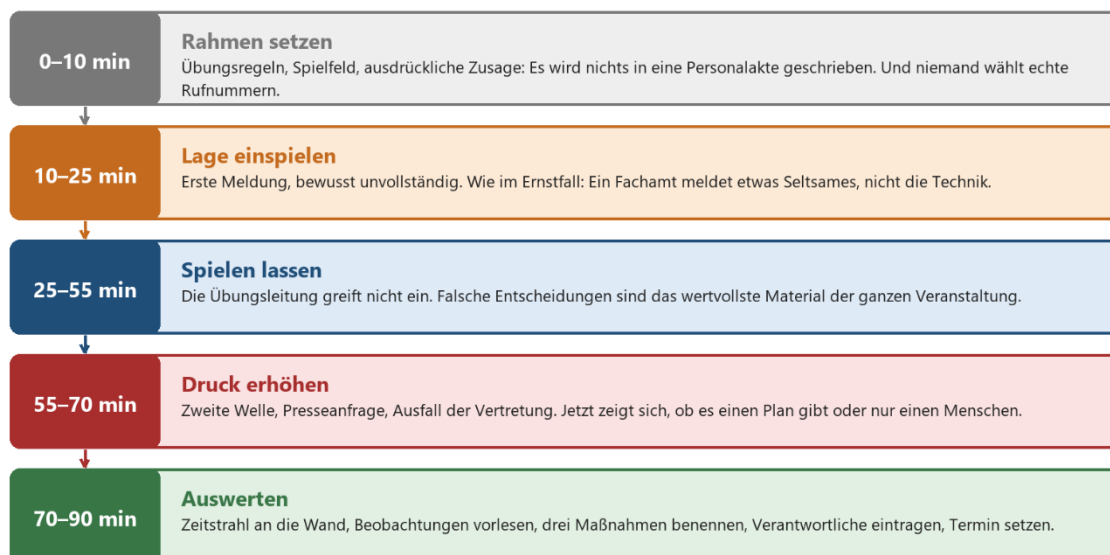
Das ist keine Rechtsberatung. Welche Beteiligungstatbestände im Einzelfall greifen, richtet sich nach dem jeweiligen Landespersonalvertretungsrecht beziehungsweise nach dem kirchlichen Mitarbeitervertretungsrecht.

Der Takt einer Einheit

Neunzig Minuten je Szenario klingen knapp und sind es nicht. Die Erfahrung zeigt: Nach einer Stunde ist alles gesagt, was gesagt werden wird, und nach neunzig Minuten ist die Aufmerksamkeit erschöpft. Drei Szenarien plus Pausen plus Schlussrunde ergeben einen vollen Tag. Vier Szenarien ergeben einen verlorenen Tag.

Neunzig Minuten, fünf Phasen

Der Takt einer Übungseinheit – jede Phase hat einen anderen Zweck



Drei Szenarien lassen sich an einem Tag üben. Vier nicht: Nach dem dritten hört niemand mehr zu.

Skizze 2: Der Takt einer Übungseinheit. Die dritte Phase ist die wichtigste – und die, in der die Übungsleitung am meisten Disziplin braucht, weil sie nicht helfen darf.

Die Tabelle unten zeigt die drei Szenarien mit ihrem jeweiligen Übungsziel und der veranschlagten Dauer. Das Übungsziel ist bewusst eng formuliert: Ein Szenario, das alles prüfen soll, prüft nichts.

Szenario	Übungsziel	Dauer
----------	------------	-------

1 · SharePoint verschlüsselt	Entscheidungsfähigkeit bei Datenverlust: Wird gestoppt, bevor wiederhergestellt wird? Ist der Wiederherstellungsweg bekannt und priorisiert? Weiß die Registratur, welches Schriftgut betroffen ist?	90 Minuten
2 · Admin-Konto übernommen	Handlungsfähigkeit bei Identitätsverlust: Kommt die Verwaltung noch in den eigenen Tenant? Wer darf ein privilegiertes Konto sperren? Läuft die Beweissicherung, bevor aufgeräumt wird?	90 Minuten
3 · Bürgertelefon tot	Erreichbarkeit ohne Technik: Existiert eine Rückfallebene, kennt sie jemand, und trägt sie länger als zwei Stunden? Was sagt das Bürgerbüro den Wartenden?	60 bis 90 Minuten
Schlussrunde	Verdichtung: maximal zehn Befunde über alle drei Szenarien, drei davon als Sofortmaßnahme mit Namen und Termin	45 Minuten

Szenario 1: SharePoint verschlüsselt

Ablauf und Einspielungen

Die Lage beginnt nicht mit einem Alarm, sondern mit einer Nachfrage. So ist es im Ernstfall fast immer. Die erste Einspielung lautet sinngemäß: „Aus dem Bauamt meldet eine Kollegin, dass sie ihre Vorlagen nicht mehr öffnen kann. Die Dateien heißen anders als gestern. In dem Ordner liegt außerdem eine Textdatei, die sie nicht kennt.“ Mehr nicht. Kein Umfang, keine Uhrzeit, keine Aussage darüber, ob es andere trifft.

Die zweite Einspielung folgt nach etwa zehn Minuten und erweitert den Radius: „Die Registratur meldet dasselbe für die Bibliothek mit den Vorgängen der Vergabestelle.“ Nach weiteren zehn Minuten kommt die dritte: „Der IT-Dienstleister ist telefonisch nicht erreichbar, die Hotline meldet erhöhtes Aufkommen.“ Und irgendwo bei Minute 55 fragt die Lokalzeitung an, weil jemand aus dem Bauamt in einer öffentlichen Sitzung erwähnt hat, dass „die Computer nicht gehen“.

Diese Reihenfolge ist kein Zufall. Sie bildet nach, was eine Verwaltung im Ernstfall tatsächlich erlebt: Der Schaden wird von den Fachämtern gemeldet, nicht von der Überwachung; die Ausdehnung ist zunächst unbekannt; der Dienstleister ist genau dann beschäftigt, wenn man ihn braucht; und die Öffentlichkeit erfährt es früher, als der Krisenstab denkt.

Beobachtungspunkte

- **Minute bis Stopp.** Wie lange dauert es, bis jemand ausspricht, dass zuerst die Synchronisierung und die betroffenen Konten gestoppt werden müssen – und nicht die Wiederherstellung gestartet?
- **Wer entscheidet die Reihenfolge?** Versionsverlauf, Bibliothek zurücksetzen, Papierkorb, gebuchter Sicherungsdienst: Nennt jemand eine Reihenfolge, oder wird geraten?
- **Wird der Umfang ermittelt, bevor gehandelt wird?** Fragt jemand nach, welche Websites, welche Bibliotheken, welcher Zeitraum? Oder wird die erste gemeldete Bibliothek zum Weltbild?
- **Kommt die Registratur zu Wort?** Der eigentliche Schaden liegt nicht in Dateien, sondern in Vorgängen mit Aufbewahrungsfristen. Fragt jemand, welches Schriftgut betroffen ist?

- **Wann fällt der Begriff Beweissicherung?** Und fällt er, bevor jemand aufräumt?
- **Wer spricht mit dem Dienstleister – und worüber?** Wird eine Störung gemeldet oder ein Sicherheitsvorfall? Das sind zwei verschiedene Prozesse mit zwei verschiedenen Reaktionszeiten.

Verschlüsselte Bibliothek: welcher Weg zuerst?

Die Reihenfolge entscheidet – und sie gehört vor die Übung, nicht in sie



Skizze 3: Die Wiederherstellungswege in SharePoint Online und ihre Reichweite. Die Reihenfolge ist eine Entscheidung, die vorher getroffen und dokumentiert sein muss – in der Übung wird nur geprüft, ob sie jemand kennt.

Die technische Grundlage, damit die Übung nicht im Nebel spielt

Damit die Runde überhaupt sinnvoll diskutieren kann, muss die Übungsleitung die tatsächlichen Möglichkeiten kennen. In SharePoint Online und OneDrive gibt es vier Wiederherstellungswege mit sehr unterschiedlicher Reichweite, und sie greifen nicht ineinander, sondern nebeneinander.

Weg	Reicht wie weit zurück	Wofür geeignet	Voraussetzung
Versionsverlauf	so weit, wie Versionen vorgehalten werden	einzelne Dateien, gezielte Korrektur	Versionierung war aktiv, bevor der Schaden entstand
Bibliothek zurücksetzen	bis zu 30 Tage	Massenänderungen in einer Bibliothek in einem Schritt rückgängig machen	Berechtigung auf der Website, kein laufender Zugriff des Angreifers
Papierkorb	93 Tage über beide Stufen	gelöschte Dateien und Elemente	die Datei wurde gelöscht, nicht nur überschrieben
Microsoft 365 Backup	bis zu 365 Tage	vollständige Websites, Postfächer, OneDrive-Ablagen	der Dienst war gebucht und für die betroffene Website in einer Richtlinie erfasst

FAKTEN · Zahlen, die in der Auswertung gebraucht werden

Der Papierkorb in SharePoint Online hält gelöschte Elemente insgesamt 93 Tage vor, verteilt auf zwei Stufen – den Papierkorb der Website und den der Websitesammlung. Die Funktion zum Zurücksetzen einer Bibliothek reicht 30 Tage zurück und macht sämtliche Aktionen auf Dateien und Ordner in diesem Zeitraum rückgängig.

Microsoft 365 Backup ist ein zubuchbarer, verbrauchsabhängig abgerechneter Dienst. Er erzeugt für OneDrive und SharePoint in den ersten 14 Tagen alle zehn Minuten einen Wiederherstellungspunkt und danach wöchentliche Punkte bis 365 Tage zurück; für Exchange Online liegt die Frequenz über das ganze Jahr bei zehn Minuten. Entscheidend ist die Einschränkung: Wiederherstellungspunkte entstehen erst ab dem Zeitpunkt, zu dem eine Sicherungsrichtlinie für die jeweilige Website eingerichtet wurde. Rückwirkend gibt es nichts.

Eine Aufbewahrungsrichtlinie aus Microsoft Purview ist kein Backup, wirkt in diesem Szenario aber wie eine zusätzliche Schicht: Wo sie greift, wird die Originalfassung eines geänderten oder gelöschten Dokuments in der Bibliothek für Aufbewahrung gehalten – auch dann, wenn die sichtbare Fassung unbrauchbar ist.

Ob und wie diese Wege in Ihrem Haus tatsächlich zur Verfügung stehen, ist eine Risikoentscheidung mit Kostenfolge, die das Rechnungsprüfungsamt nachvollziehen können muss – die Abwägung ist in [Backup und Wiederherstellung in Microsoft 365: Die Risikoentscheidung fürs Rechnungsprüfungsamt](#) ausführlich beschrieben. Wie Aufbewahrungsrichtlinien in der Verwaltung aufgesetzt werden und was die Bibliothek für Aufbewahrung praktisch bedeutet, steht in [Aufbewahrung und Aussonderung mit Purview: Fristen, Disposition, Vernichtungsnachweis](#). Und falls Sie beim Nachstellen des Szenarios feststellen, dass die Richtlinien gar nicht greifen wie gedacht, hilft [Wenn die Aufbewahrungsrichtlinie einfach aufhört: SharePoint-Störungsanalyse in der Verwaltung](#) bei der Eingrenzung.

Was regelmäßig herauskommt

Drei Befunde tauchen in diesem Szenario mit ermüdender Regelmäßigkeit auf.

Erstens: Die Wiederherstellung wird zu früh gestartet. In der Mehrzahl der Übungen sagt jemand innerhalb der ersten zehn Minuten den Satz „Das stelle ich eben wieder her“ – bevor geklärt ist, ob die Verschlüsselung noch läuft. Wenn das synchronisierende Endgerät weiter aktiv ist, wird die wiederhergestellte Fassung erneut überschrieben, und der 30-Tage-Rückblick der Bibliothek füllt sich mit einer zweiten Schadensschicht. Das ist der falsche Knopf, gedrückt von jemandem, der es eigentlich kann.

Zweitens: Es gibt keine Vertretung für die Entscheidung. In einer Stadtverwaltung mit SharePoint im Sozialbereich stellte sich in der Auswertung heraus, dass genau eine Person berechtigt war, eine Bibliothek zurückzusetzen – und dass diese Person am Übungstag turnusmäßig frei hatte. Die Runde hat vierzig Minuten lang sehr kompetent über Wiederherstellungswege gesprochen, ohne dass jemand die Frage gestellt hätte, wer den Vorgang tatsächlich auslösen darf.

Drittens: Die Registratur wird vergessen. Die Diskussion dreht sich um Dateien, obwohl der Schaden in Vorgängen entsteht. Erst in der Auswertung fällt auf, dass niemand geklärt hat, ob es sich bei den betroffenen Ablagen um Schriftgut mit Aufbewahrungsfrist handelt und wer beurteilt, ob eine Rekonstruktion erforderlich ist. Die Runde hat einen IT-Vorfall behandelt. Es war auch ein Vorfall der Schriftgutverwaltung.

WICHTIG · Die Grenze zur E-Akte gehört in die Übung

Wenn in Ihrem Haus Schriftgut in SharePoint liegt, muss vor der Übung klar sein, welcher Teil davon aktenrelevant ist und welcher nicht. SharePoint kann Ablage, Zusammenarbeit und Aufbewahrung – ob es in Ihrem Land als E-Akte im Sinne des jeweiligen E-Government-Gesetzes gilt, ist eine ganz andere Frage und in aller Regel zu verneinen, solange kein Verfahren mit entsprechender Funktionalität dahintersteht. Die Abgrenzung ist in [SharePoint als E-Akte? Was geht, was nicht und wo die Grenze nach Landesrecht liegt](#) ausgeführt, die Systematik vom Aktenplan zur Aufbewahrungsbezeichnung in [Schriftgutverwaltung mit Microsoft 365: Vom Aktenplan zur Aufbewahrungsbezeichnung](#).

Für die Übung genügt eine Ansage der Registratur: Diese drei Bibliotheken enthalten aktenrelevantes Schriftgut, jene nicht. Ohne diese Ansage diskutiert die Runde über Dateiverluste und übersieht den Verwaltungsschaden.

Szenario 2: Admin-Konto übernommen

Ablauf und Einspielungen

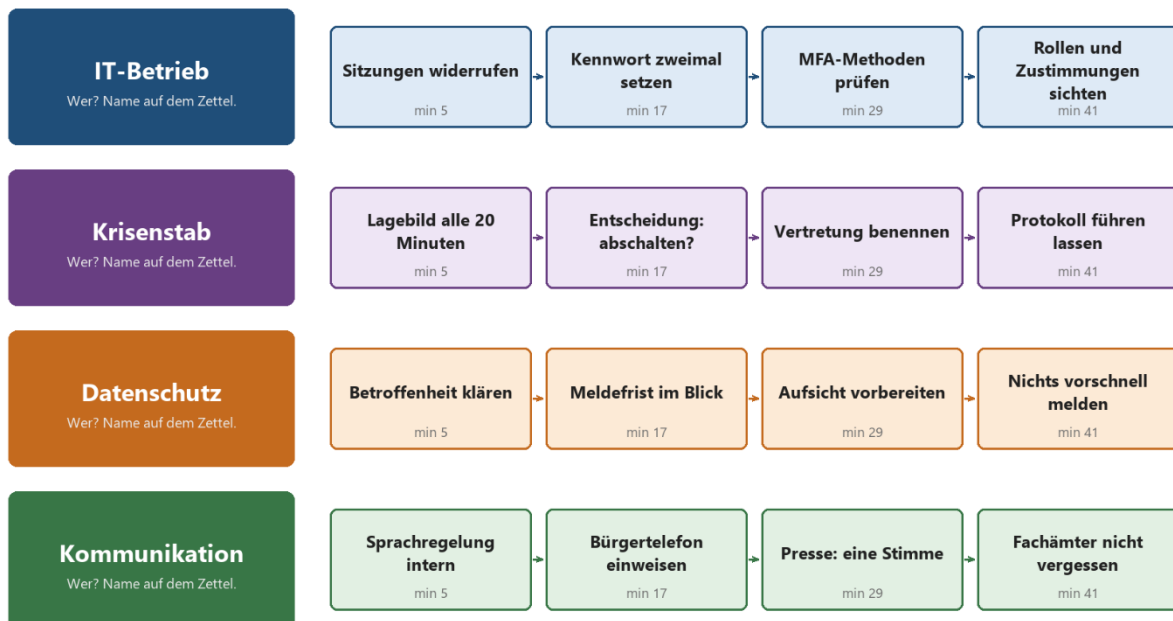
Das zweite Szenario ist das unangenehmste, weil es an die Grundlage geht: Wenn die Identität kompromittiert ist, sind alle anderen Schutzmaßnahmen Verhandlungsmasse. Die Einstiegseinspielung: „Im Aktivitätsprotokoll steht eine erfolgreiche Anmeldung eines Kontos mit erhöhten Rechten aus einem Land, in dem diese Verwaltung keine Außenstelle betreibt. Zeitpunkt: heute Nacht, 03:14 Uhr. Danach wurden mehrere Rollenzuweisungen geändert.“

Nach zehn Minuten die zweite Welle: „Ein weiteres Konto hat eine neue Authentifizierungsmethode registriert – eine Telefonnummer, die niemand zuordnen kann.“ Nach zwanzig Minuten die dritte: „Mehrere Postfächer im Fachbereich Soziales haben seit heute Morgen Weiterleitungsregeln, die vorher nicht da waren.“ Und in Minute 55, wenn die Runde sich gerade sortiert hat: „Der Kollege, der die Rollen im Tenant verwaltet, ist im Urlaub und nicht erreichbar.“

Diese letzte Einspielung ist der eigentliche Kern des Szenarios. In den meisten Verwaltungen ist die Zahl der Menschen, die im Notfall eine Rollenzuweisung ändern oder ein privilegiertes Konto sperren dürfen, erschreckend nahe an eins. Das ist kein Vorwurf – es ist die logische Folge knapper Stellenpläne und des berechtigten Wunsches, privilegierte Rechte eng zu halten. Nur muss man wissen, dass man diesen Zustand hat, bevor er akut wird.

Die erste Stunde nach der Kontoübernahme

Vier Bahnen, die gleichzeitig laufen müssen – und in der Übung nacheinander laufen



In der Übung stellt sich fast immer heraus: Drei der vier Bahnen warten auf dieselbe Person.

Das ist der Befund, wegen dem sich der ganze Tag lohnt.

Skizze 4: Vier Bahnen, die parallel laufen müssen. In der Übung laufen sie fast immer nacheinander – weil sie auf dieselbe Person warten.

Beobachtungspunkte

- **Kommt jemand überhaupt noch hinein?** Wird nach Notfallzugängen gefragt? Weiß jemand, wo die Zugangsdaten liegen, wer sie holen darf und wie das Vier-Augen-Prinzip dabei aussieht?
- **Sperren oder beobachten?** Sofortiges Sperren beendet den Zugriff und vernichtet unter Umständen die Spur. Wer trifft diese Abwägung, und mit welcher Begründung?
- **Wird die Beweissicherung angesprochen?** Bevor Weiterleitungsregeln gelöscht werden: Hat jemand die Protokolle gesichert? Und weiß jemand, wie lange sie überhaupt vorgehalten werden?
- **Wer informiert wen?** Der Datenschutz braucht früh eine Einschätzung zur Betroffenheit. Die Verwaltungsspitze braucht eine Entscheidungsvorlage. Der Dienstleister braucht eine klare Einstufung. Passiert das parallel oder nacheinander?
- **Wird über die Fachverfahren gesprochen?** Wenn Anmeldung und Fachverfahren zusammenhängen, hat die Sperrung eines Kontos Folgen weit über Microsoft 365 hinaus.

Die technische Grundlage

Handgriff	Wirkung	Wer darf das	Fallstrick in der Übung
Anmeldung blockieren	verhindert neue Anmeldungen des Kontos	Rolle mit Benutzerverwaltung	beendet bestehende Sitzungen nicht
Sitzungen widerrufen	entwertet ausgestellte Token, erzwingt	Benutzer- oder Sicherheitsadministration	wird oft vergessen – das Konto bleibt

	Neuanmeldung		trotz neuem Kennwort aktiv
Kennwort zurücksetzen	sperrt den Zugang über die bekannten Zugangsdaten	Benutzerverwaltung, bei Hybrid auch lokal	bei synchronisierten Konten hängt die Wirkung an der Replikation
Authentifizierungsmethoden prüfen	entfernt vom Angreifer hinterlegte Methoden	Authentifizierungsadministration	eine übersehene Methode macht alles andere wirkungslos
Rollen und Zustimmungen sichten	findet nachträglich vergebene Rechte und Anwendungsfreigaben	Rollenverwaltung, Anwendungsadministration	wird als letzter Punkt behandelt, gehört aber nach vorn
Notfallzugang verwenden	stellt Handlungsfähigkeit her, wenn regulär niemand hineinkommt	nach dokumentiertem Verfahren, mit Vier-Augen-Prinzip	die Zugangsdaten liegen im Tresor – und der Tresorschlüssel im Büro des Erkrankten

FAKTEN · Was der Tenant für Sie festhält – und wie lange

Microsoft empfiehlt zwei reine Cloud-Konten für den Notfallzugang, dauerhaft mit der Rolle des globalen Administrators belegt, nicht einzelnen Personen zugeordnet, mit starker Anmeldung über einen Sicherheitsschlüssel oder zertifikatsbasiert, und mindestens eines davon von allen Richtlinien für bedingten Zugriff ausgenommen. Ausdrücklich Teil der Empfehlung: Das Verfahren zur Nutzung muss dokumentiert und die Beteiligten müssen darin geübt sein.

Das einheitliche Überwachungsprotokoll hält Aktivitäten in der Standardausführung 180 Tage vor; für Protokolle, die vor dem 17. Oktober 2023 entstanden sind, galten 90 Tage. Längere Vorhaltezeiten setzen entsprechende Lizenzierung voraus. Wer nach einem halben Jahr forensisch nachvollziehen will, was passiert ist, findet unter Umständen nichts mehr.

Gelöschte Benutzerkonten und Gruppen bleiben in Microsoft Entra ID 30 Tage wiederherstellbar. Danach ist die Löschung endgültig – auch der Support kann sie nicht rückgängig machen. In der Übung ist das die Antwort auf die Frage, was passiert, wenn ein übernommenes Konto Objekte entfernt.

Wie ein belastbares Rollenmodell mit zeitlich begrenzter Rechteerhöhung aussieht und warum der Fall des einen Administrators so verbreitet ist, ist Thema von [Privilegierte Konten in der Verwaltungs-IT: Rollen, PIM und der Fall des einen Admins](#). Welche Nachweise Sie aus dem Überwachungsprotokoll ziehen können und wie man sie prüffest aufbereitet, steht in [Microsoft 365 Audit-Log und Rechnungsprüfung: Nachweise, die Verwaltungen liefern müssen](#). Und weil ein großer Teil der Übernahmen an einer Lücke im Regelwerk für bedingten Zugriff hängt, lohnt der Abgleich mit [Conditional Access für Verwaltungen: Regelwerk für Rathaus, Bauhof und Homeoffice](#).

Was regelmäßig herauskommt

Der erste Befund ist fast immer derselbe: Der Notfallzugang existiert auf dem Papier, aber niemand am Tisch weiß, wo die Zugangsdaten liegen. Oder er existiert, und in der Auswertung stellt sich

heraus, dass er als einziges Konto von den Richtlinien für bedingten Zugriff ausgenommen ist, seit vier Jahren nicht angefasst wurde und mit einer Anmeldemethode geschützt ist, die seither abgekündigt wurde. Ein Notfallzugang, der nie erprobt wurde, ist kein Notfallzugang, sondern eine Hoffnung.

Der zweite Befund betrifft die Reihenfolge. Fast alle Runden sperren zuerst und sichern danach – oder sichern gar nicht. Das ist menschlich völlig verständlich, kostet aber genau die Informationen, die man später gegenüber der Aufsicht, der Versicherung und dem Rechnungsprüfungsamt braucht. Die Sofortmaßnahme aus diesem Befund ist banal und wirksam: eine einseitige Handlungsanweisung, in der die Reihenfolge steht, laminiert, im Serverraum und im Büro der IT-Leitung.

Der dritte Befund ist die Panik. Sie äußert sich in Verwaltungen selten laut, sondern als Beschleunigung: Sätze werden kürzer, Fragen werden nicht mehr beantwortet, mehrere Personen arbeiten parallel an derselben Sache, ohne es voneinander zu wissen. In einem großen Landschaftsverband hat die Beobachtung protokolliert, dass zwischen Minute 34 und Minute 41 drei verschiedene Personen unabhängig voneinander beschlossen hatten, denselben Dienstleister anzurufen – und dass niemand davon im Protokoll stand. Der Befund lautete nicht „Panik“, sondern: Es fehlt eine Person, die ausschließlich schreibt.

TIPP · Der Schreiber ist die billigste Maßnahme überhaupt

Benennen Sie im Notfallplan eine Rolle, die nichts anderes tut als protokollieren: Uhrzeit, Meldung, Entscheidung, wer informiert wurde. Kein Werkzeug nötig, ein Blatt Papier genügt und funktioniert auch dann noch, wenn der Tenant nicht erreichbar ist.

Diese Rolle löst gleich drei Probleme: Sie erzeugt den Nachweis für die spätere Prüfung, sie verhindert Doppelarbeit, und sie zwingt den Krisenstab dazu, Entscheidungen laut auszusprechen – weil sonst nichts aufgeschrieben werden kann. In der Übung ist das der Befund mit dem besten Verhältnis von Aufwand zu Wirkung.

Szenario 3: Bürgertelefon tot

Ablauf und Einspielungen

Das dritte Szenario wird gern belächelt und ist das mit der unmittelbarsten Außenwirkung. Wenn SharePoint verschlüsselt ist, merkt es die Öffentlichkeit am dritten Tag. Wenn das Bürgertelefon tot ist, merkt sie es in der ersten Minute – und zwar diejenigen Bürgerinnen und Bürger, die keine Alternative haben.

Die Einstiegseinspielung: „Seit 8:40 Uhr kommen keine externen Anrufe mehr an. Interne Gespräche funktionieren. Die Vermittlung meldet, dass das Display nichts Auffälliges zeigt.“ Nach zehn Minuten: „Das Bürgerbüro meldet Wartende, die berichten, sie hätten seit einer Stunde vergeblich angerufen.“ Nach zwanzig Minuten: „Die Leitstelle fragt, ob Ihre Rufumleitung für den Bereitschaftsdienst funktioniert.“ Und gegen Ende: „Der Anbieter meldet eine Störung ohne Zeitangabe für die Behebung.“

Der Reiz dieses Szenarios liegt darin, dass es keine Schuldfrage gibt. Niemand hat etwas falsch gemacht, es gibt keinen Angreifer, keinen Datenschutzvorfall und niemanden, dem man Vorwürfe

machen könnte. Genau deshalb spielt die Runde es entspannter – und genau deshalb kommen hier die ehrlichsten Antworten.

Beobachtungspunkte

- **Wie lange bis zur Feststellung?** Wann merkt die Verwaltung selbst, dass sie nicht erreichbar ist? In der Praxis meldet das fast immer eine Person von außen.
- **Gibt es eine Rückfallebene, und kennt sie jemand?** Mobilfunk, Ansage beim Anbieter, Hinweis auf der Website, Schild an der Tür – was davon ist vorbereitet und wer darf es auslösen?
- **Sind die Sonderfälle bedacht?** Bereitschaftsdienste, Rufumleitungen zur Leitstelle, Aufzugsnotruf, Faxeingang der Vergabestelle, Sammelnummern von Fachämtern mit Fristen.
- **Was sagt das Bürgerbüro?** Gibt es einen Satz, den die Kolleginnen und Kollegen am Schalter sagen können? Oder erfinden sechs Menschen sechs Varianten?
- **Wer spricht mit dem Anbieter?** Und liegt die Vertragsnummer griffbereit, oder liegt sie in dem Ablagesystem, das gerade nicht erreichbar ist?

Rückfallebene	Trägt wie lange	Voraussetzung	In der Übung geprüft
Ansage beim Anbieter	unbegrenzt	vorbereiteter Text, benannte Person mit Zugang zum Portal	Kennt jemand die Zugangsdaten?
Umleitung auf Mobilfunk	Stunden bis Tage	Liste dienstlicher Mobilnummern, Zuordnung zu Fachämtern	Ist die Liste aktuell und außerhalb des Tenants verfügbar?
Hinweis auf der Website	unbegrenzt	Redaktionsrechte, unabhängig von der Büro-IT erreichbar	Wer kann veröffentlichen, wenn die Anmeldung hakt?
Aushang und Schalterbetrieb	Öffnungszeiten	vorbereitete Vorlage, Abstimmung mit dem Bürgerbüro	Existiert die Vorlage – auf Papier?
Rückrufliste	so lange, wie jemand zurückruft	Erfassung der Anliegen, definierte Priorisierung nach Fristen	Wer entscheidet, welches Anliegen zuerst zurückgerufen wird?

Was regelmäßig herauskommt

In einer Stadtverwaltung mit rund 1.000 Rufnummern ergab die Übung einen Befund, der sich mit Technik nicht beheben lässt: Es gab eine ausgezeichnete Rückfallebene für die zentrale Vermittlung und keine einzige für die Durchwahlen der Fachämter. Die Vermittlung hätte also weiterhin sagen können, dass die Verwaltung erreichbar ist – ohne jemanden verbinden zu können. In der Auswertung wurde daraus eine sehr konkrete Maßnahme: eine Liste der zwölf Rufnummern, die zuerst wieder erreichbar sein müssen, abgestimmt mit dem Amt für Organisation und ausdrücklich nicht mit der IT.

Der zweite regelmäßige Befund betrifft die Sonderanschlüsse. Aufzugsnotruf, Brandmeldeanlage, Bereitschaftsdienste, das Faxgerät der Vergabestelle, an dem immer noch fristwahrende Erklärungen eingehen: Diese Anschlüsse gehören selten der IT und tauchen deshalb in keiner IT-Dokumentation auf. In der Übung fällt das innerhalb von zwanzig Minuten auf, weil jemand aus dem Gebäudemanagement danach fragt. Ohne Übung fällt es beim Ausfall auf.

Welche dieser Fälle die Telefonie technisch abbilden muss und wie sie in eine Vergabeunterlage kommen, ist Gegenstand von [Notruf, Fax und Sonderanschlüsse: Die Verwaltungsfälle, die Teams](#)

Phone lösen muss sowie von Teams-Telefonie für Kommunen: Direct Routing, Operator Connect und die Vergabeunterlage. Für Häuser mit Krankenhausbetrieb in kommunaler Trägerschaft kommt eine eigene Ebene dazu, die in Microsoft 365 im Krankenhaus in kommunaler Trägerschaft: Büro-IT, Zusammenarbeit, Telefonie beschrieben ist.

WARNUNG · Der Denkfehler bei der Notrufführung

In Übungen taucht regelmäßig die Annahme auf, ein Ausfall der Büro-IT betreffe den Notruf nicht, weil „der ja über eine eigene Leitung geht“. Das stimmt in manchen Häusern und in vielen nicht. In modernen Telefonielösungen hängt die Notrufführung an der Standortermittlung des Endgeräts und an einer Richtlinie, die dem Konto oder dem Netzwerkstandort zugeordnet ist – ist keine Richtlinie ermittelbar, ist der Nutzer für Notrufe nicht freigeschaltet.

Das ist kein Grund zur Panik und auch kein Argument gegen eine Migration. Es ist ein Grund, den Fall einmal aufzuschreiben, mit dem Anbieter zu klären und in die Übung aufzunehmen – bevor jemand im Ernstfall aus einer falschen Annahme heraus entscheidet.

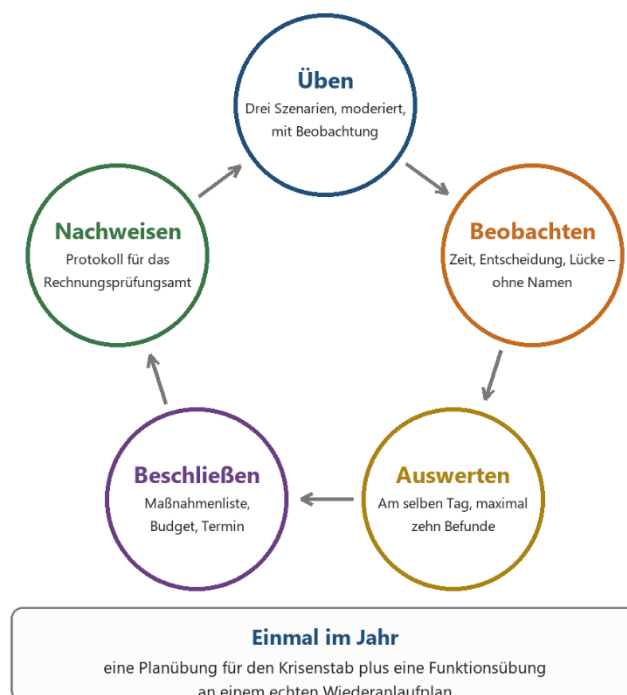
Nach der Übung: aus Befunden werden Beschlüsse

Der gefährlichste Moment einer Notfallübung ist nicht das Szenario, sondern die Woche danach. Alle waren beeindruckt, alle haben etwas gelernt, alle haben wieder Termine. Vier Wochen später erinnert sich niemand mehr an den zweiten Befund, und im Jahresbericht steht ein Satz über die durchgeführte Übung, der niemandem hilft.

Deshalb gehört die Auswertung an denselben Tag und die Maßnahmenliste in dieselbe Sitzung. Maximal zehn Befunde über alle drei Szenarien, davon drei mit Namen und Termin. Nicht fünfzehn. Eine Liste, die abgearbeitet wird, ist mehr wert als ein Katalog, der vollständig ist.

Vom Rollenspiel zum Nachweis

Eine Übung ohne Folgeeintrag ist ein netter Nachmittag



Skizze 5: Der Regelkreis. Ohne den Schritt nach unten rechts bleibt die Übung eine Erzählung; mit ihm wird sie ein Nachweis.

Typischer Befund	Maßnahme	Verantwortlich	Nachweis
Reihenfolge der Wiederherstellung unbekannt	Einseitige Handlungsanweisung, laminiert, an zwei Orten	IT-Leitung	Dokument mit Datum, Kenntnisnahme im Team
Nur eine Person darf entscheiden	Zweite Person benennen und berechtigen, Verfahren dokumentieren	IT-Leitung mit Amt für Organisation	Rollenübersicht, Vertretungsregelung
Notfallzugang nicht erprobt	Jährliche Erprobung im Vier-Augen-Prinzip, protokolliert	IT-Leitung	Erprobungsprotokoll mit zwei Unterschriften
Kein Protokollführer im Krisenstab	Rolle im Notfallplan verankern, Vordruck bereitstellen	Amt für Organisation	Aktualisierter Notfallplan
Registratur nicht eingebunden	Zuordnung aktenrelevanter Ablagen erstellen und pflegen	Registratur	Übersicht je Website, Stand und Fortschreibung
Sonderanschlüsse nicht erfasst	Bestandsaufnahme über Gebäudemanagement und Fachämter	Gebäudemanagement	Liste mit Anschluss, Zweck, Anbieter, Ansprechpartner
Rückfallebene nur für die Vermittlung	Priorisierte Liste der zuerst wiederherzustellenden Rufnummern	Amt für Organisation	Abgestimmte Liste, Bestandteil des Notfallplans

Die Beschlussvorlage, die daraus wird

Drei der Befunde kosten Geld: ein zubuchbarer Sicherungsdienst, zusätzliche Lizenzen für privilegierte Rollen, eine Rückfallebene für die Telefonie. Diese drei gehören in eine Beschlussvorlage, und zwar mit dem Übungsprotokoll als Anlage. Das ist der eigentliche politische Wert einer Notfallübung: Sie verwandelt ein abstraktes Risiko in einen dokumentierten Befund, den die Verwaltungsspitze und der Hauptausschuss nachvollziehen können.

Für die Rechnungsprüfung ist die Kombination aus Übungsprotokoll, Maßnahmenliste und Erledigungsvermerk der sauberste denkbare Nachweis, dass das Haus sich mit seinen Risiken befasst hat. Wie eine Konzeptionsphase samt Beschlussvorlage aufgebaut wird, ohne dass daraus ein Zweijahresprojekt wird, ist in [Microsoft-365-Einführung in der Verwaltung: Konzeptionsphase in 4,5 Tagen und die Beschlussvorlage](#) beschrieben.

TIPP • Wenn es eine Stufe härter sein soll

Die hier beschriebene Planübung ist der Einstieg. Wer danach wissen will, ob die Handgriffe auch technisch sitzen, braucht ein Format mit realer Erprobung in einer Testumgebung und mit simuliertem Angreiferverhalten. Das Notfall- und Red-Team-Übungsformat ist Teil des Angebots unter [Microsoft-365-Schulung für Verwaltungen](#) und lässt sich auf den Teilnehmerkreis Ihres Hauses zuschneiden.

Wenn zuerst die Grundlagen fehlen – Rollenmodell, Aufbewahrung, Betriebsmodell – ist die Übung der falsche zweite Schritt. Dann lohnt der Blick auf [Microsoft-365-Beratung für Verwaltungen](#), bevor Sie einen Übungstag ansetzen, der vor allem Lücken in der Konzeption zutage fördert.

Und wenn der Betrieb beim Dienstleister liegt?

Dann üben Sie mit. Das ist keine Zumutung, sondern gute fachliche Praxis: Ein kommunales Rechenzentrum oder ein Systemhaus, das den Tenant betreibt, hat eigene Notfallprozesse, und die sind in aller Regel besser dokumentiert als die der Verwaltung. Was regelmäßig fehlt, ist die Nahtstelle: Wer meldet was an wen, in welcher Einstufung, mit welcher Reaktionszeit, und wer entscheidet, wenn beide Seiten auf die andere warten?

Laden Sie die Verantwortlichen des Dienstleisters für das zweite Szenario ein. Nicht als Prüfling, sondern als Rolle am Tisch. Der häufigste Befund aus dieser Konstellation ist erfreulich unspektakulär: Beide Seiten haben einen Plan, und die Pläne kennen einander nicht.

Wie sich Rollen, Schnittstellen und Verantwortlichkeiten zwischen Verwaltung und Betreiber sauber schneiden lassen, steht in [Microsoft 365 und das kommunale Rechenzentrum: Rollen, Schnittstellen, Zweitmeinung](#). Für Häuser, die einen Teil ihrer Anmeldung noch lokal betreiben, kommt eine zusätzliche Abhängigkeit hinzu, die in [ADFS oder Entra ID in der Verwaltung: Die Entscheidung entlang der Fachverfahren](#) behandelt wird – und die im Notfall darüber entscheidet, ob die Sperrung eines Kontos in Sekunden oder in einem Replikationsintervall wirkt.

FAKTEN · Ein Wort zur souveränen Plattform

In vielen Häusern taucht in der Diskussion um Notfallvorsorge der Hinweis auf die Delos Cloud auf, also auf eine in Deutschland betriebene, auf Microsoft-Technologie aufsetzende Plattform für den öffentlichen Sektor. Für die Übung ist das aus einem einfachen Grund unerheblich: Kein Betriebsmodell und kein Betreiber ersetzt die Frage, wer bei Ihnen im Haus im Ernstfall entscheidet und wer mitschreibt.

Verfügbarkeit, Funktionsumfang und Zeitpläne sind Gegenstand laufender Entwicklung; Aussagen dazu gehören in eine eigene Betrachtung und nicht in eine Notfallplanung. Der Sachstand ist in [Delos Cloud für Kommunen: Was das Angebot ist, wen es betrifft und was fehlt](#) zusammengefasst, die Modellfrage in [Standard-Tenant oder Hybrid: Die Betriebsmodell-Entscheidung für Verwaltungen](#).

Häufige Fragen

Wie viel Vorbereitung braucht so ein Übungstag?

Rechnen Sie mit zwei bis drei Personentagen für die Vorbereitung, verteilt auf zwei bis drei Wochen. Der größte Anteil entfällt nicht auf die Szenarien, sondern auf zwei Dinge: die Abstimmung mit dem Personalrat und die Klärung, welche Ablagen und welche Rufnummern in Ihrem Haus überhaupt kritisch sind. Die Einspielungen selbst sind in einem halben Tag geschrieben, wenn die Vorarbeit steht.

Können wir das intern moderieren?

Grundsätzlich ja, mit einer Einschränkung: Die Übungsleitung darf nicht mitspielen. Wenn die IT-Leitung moderiert, fehlt sie am Tisch – und genau ihre Entscheidungen wollen Sie beobachten. Praktikabel ist eine Moderation aus einem anderen Amt, etwa dem Amt für Organisation, das mit dem Format vertraut gemacht wird. Die Beobachtung sollte in jedem Fall aus zwei Personen bestehen, die sonst nichts zu tun haben.

Müssen wir dafür produktive Systeme anfassen?

Nein, und Sie sollten es ausdrücklich nicht tun. Eine Planübung findet vollständig am Tisch statt. Wenn Sie technische Handgriffe erproben wollen – Notfallzugang, Sitzungswiderruf, Zurücksetzen einer Bibliothek –, ist das eine Funktionsübung in einer Testumgebung und ein eigener Termin mit eigener Vorbereitung. Beides zu vermischen führt dazu, dass eine der beiden Übungen schlecht wird.

Wie oft sollten wir üben?

Ein realistischer Takt für eine Kommune mittlerer Größe ist: einmal jährlich eine Planübung mit zwei bis drei Szenarien, dazu eine Funktionsübung an einem der Wiederanlaufpläne. Der BSI-Standard 200-4 beschreibt für das Übungsprogramm eine ähnliche Größenordnung und ergänzt sie um umfassendere Übungen in längeren Abständen. Wichtiger als die Frequenz ist die Nachverfolgung: Zwei gut ausgewertete Übungen in drei Jahren wirken mehr als vier folgenlose.

Was, wenn die Übung peinlich wird?

Dann hat sie funktioniert. Eine Übung, in der alles glattgeht, war entweder zu einfach oder wurde vorher durchgesprochen. Entscheidend ist, wie das Ergebnis kommuniziert wird: Befunde über Rollen, nicht über Personen; Maßnahmen statt Bewertungen; und eine klare Ansage der Verwaltungsspitze am Ende des Tages, dass die Erkenntnisse ausschließlich in die Verbesserung fließen. Wenn diese Ansage fehlt, ist die zweite Übung wertlos, weil alle vorsichtig antworten.

Dürfen wir Beobachtungsprotokolle aufbewahren?

Aufbewahren ja, aber in der Form, in der sie geschrieben werden sollten: ohne Namen, ohne Zuordnung zu Personen, als Beschreibung von Abläufen und Zeitpunkten. In dieser Form sind sie ein Nachweis über die Organisation und kein Personaldatum. Die konkrete Ausgestaltung – Aufbewahrungsdauer, Zugriffsberechtigte, Beteiligung – klären Sie mit dem Datenschutz und dem Personalrat vorab; die Anforderungen ergeben sich aus dem jeweiligen Landesrecht beziehungsweise, bei kirchlichen Trägern, aus dem kirchlichen Datenschutzrecht.

Wie binden wir externe Beteiligte ein?

Planungsbüros, freie Träger und Gremienmitglieder sind im Ernstfall betroffen, gehören aber nicht an den Übungstisch. Nehmen Sie sie als Einspielung auf: „Ein Planungsbüro meldet, dass es seit heute Morgen nicht mehr auf den gemeinsamen Bereich zugreifen kann.“ Damit prüfen Sie, ob jemand an die externen Beteiligten denkt – ein Punkt, der ohne Einspielung zuverlässig untergeht.

Wie Gastzugänge sauber aufgesetzt werden, damit diese Frage im Notfall überhaupt beantwortbar ist, steht in [Gäste in Teams und SharePoint: Planungsbüros, Träger und Gremienmitglieder sicher einbinden](#).

Was hat das mit Berechtigungen zu tun?

Mehr, als es zunächst aussieht. Der Umfang eines Schadens hängt unmittelbar davon ab, wie weit die Berechtigungen eines übernommenen Kontos reichen. Ein Konto, das auf drei Bibliotheken zugreifen kann, verschlüsselt drei Bibliotheken. Ein Konto, das über eine großzügig geteilte

Struktur an halbe Fachbereiche kommt, verschlüsselt halbe Fachbereiche. Deshalb ist die Aufräumarbeit an übermäßig geteilten Inhalten keine Fleißaufgabe, sondern Schadensbegrenzung im Voraus.

Warum diese Strukturen entstehen und wie man sie in den Griff bekommt, ist Thema von [Oversharing im Verwaltungs-Tenant: Warum Copilot die Personalakte findet.](#)

Wer trägt die Kosten einer Übung?

Der Übungstag selbst kostet vor allem Arbeitszeit: acht bis zehn Personen für einen Tag, dazu die Vorbereitung. Was Geld kostet, sind die Maßnahmen, die aus der Übung folgen. Genau deshalb ist die Reihenfolge richtig herum: Erst der dokumentierte Befund, dann die Beschlussvorlage. Ein Antrag auf ein zusätzliches Sicherungsbudget, dem ein Übungsprotokoll beiliegt, hat im Hauptausschuss eine andere Qualität als ein Antrag, dem ein Herstellerprospekt beiliegt.

Und wenn wir noch gar kein Microsoft 365 haben?

Dann üben Sie trotzdem – die drei Szenarien funktionieren mit jeder Plattform. Die Fragen nach Vertretung, Entscheidungsbefugnis, Protokollführung und Rückfallebene sind produktunabhängig. Ändern werden sich nur die technischen Details der Wiederherstellungswege. Es spricht sogar einiges dafür, die erste Übung vor einer Einführung anzusetzen: Die Befunde sind dann Eingangsgröße für die Konzeption und nicht Reparatur hinterher.

Fazit

Notfallvorsorge in der Verwaltungs-IT scheitert selten an fehlendem Wissen und fast nie an fehlender Technik. Sie scheitert an drei sehr menschlichen Dingen: Es gibt keine Vertretung für die Person, die entscheiden darf. Es gibt keine Aufzeichnung dessen, was gerade passiert. Und es gibt unter Druck den Reflex, sofort zu handeln, statt kurz zu fragen, ob Handeln gerade die richtige Idee ist.

Alle drei lassen sich an einem einzigen Tag sichtbar machen. Drei moderierte Szenarien, ein Tisch mit den Rollen, die im Ernstfall wirklich zusammenkommen, zwei Menschen, die schweigen und mitschreiben, und eine Auswertung, die noch am selben Tag stattfindet. Das ist kein großes Projekt. Es ist ein Termin im Kalender.

Und wenn Sie danach nur eine einzige Maßnahme umsetzen, dann diese: Schreiben Sie die Reihenfolge auf. Erst stoppen, dann bewerten, dann sichern, dann wiederherstellen. Ein laminiertes Blatt an der Wand des Serverraums verhindert mehr Schaden als die meisten Sicherheitsprodukte, weil es genau in dem Moment wirkt, in dem jemand, der es eigentlich kann, gerade dabei ist, unter Druck den falschen Knopf zu drücken.

TIPP • Weiter im Thema

- › [Microsoft 365 in der öffentlichen Verwaltung](#)
- › [Backup und Wiederherstellung in Microsoft 365: Die Risikoentscheidung fürs Rechnungsprüfungsamt](#)
- › [Privilegierte Konten in der Verwaltungs-IT: Rollen, PIM und der Fall des einen Admins](#)
- › [Microsoft 365 Audit-Log und Rechnungsprüfung: Nachweise, die Verwaltungen liefern müssen](#)

- › [Aufbewahrung und Aussonderung mit Purview: Fristen, Disposition, Vernichtungsnachweis](#)
- › [Microsoft 365 und das kommunale Rechenzentrum: Rollen, Schnittstellen, Zweitmeinung](#)
- › [Notruf, Fax und Sonderanschlüsse: Die Verwaltungsfälle, die Teams Phone lösen muss](#)
- › [Microsoft 365 in der Kommune: Was Sie wirklich entscheiden müssen \(und was nicht\)](#)