

Incident-Response-Plan für Microsoft 365

Es gibt zwei Sorten von Incident-Response-Plänen. Die erste ist ein Ordner. Achtzig Seiten, Stand irgendwann 2019, mit einem Kapitel über Faxgeräte und einer Telefonliste, auf der drei Leute stehen, die längst woanders arbeiten. Der Ordner steht im Serverraum. Der Serverraum ist verschlossen. Der Schlüssel hängt im Schrank neben dem Ordner. Man ahnt, wie der Abend läuft.

Die zweite Sorte passt auf zwei Seiten. Sie beantwortet vier Fragen, und zwar so, dass sie auch jemand beantworten kann, der um 23:40 Uhr aus dem Bett geklingelt wurde: Wen rufe ich an? Was darf ich sofort tun, ohne zu fragen? Wen muss ich in welcher Frist informieren? Und was mache ich zuerst, damit ich mir die Beweise nicht selbst kaputt trete? Alles andere — die Klickpfade, die Skripte, die Detailabläufe — sind Playbooks. Die liegen woanders, und darauf verweist der Plan. Er enthält sie nicht.

Dieser Beitrag gehört zum Handlungsfeld D der Serie [Microsoft 365 Security](#). In den Handlungsfeldern davor ging es darum, dass es gar nicht erst so weit kommt. Hier geht es um den Tag, an dem es doch so weit gekommen ist. Und um die unangenehme Erkenntnis, dass ein Vorfall nicht nur ein technisches Ereignis ist, sondern vor allem ein Kommunikations- und Entscheidungsproblem mit laufenden gesetzlichen Fristen im Hintergrund.

FAKTEN — Warum das kein theoretisches Thema ist

Im August 2026 traf es zwei Berliner Senatsverwaltungen. Der Zugriff lief unbemerkt vom 7. bis zum 12. August, entdeckt wurde er am 14. August. Die öffentliche Bestätigung kam am 28. August — vierzehn Tage nach der Entdeckung.

Die Ransomware-Gruppe Rhysida veröffentlichte am 4. September rund 5,8 Terabyte und etwa 1,44 Millionen Dateien. Darunter waren knapp 6.000 Dateien mit Zugangsdaten, teils Klartextkennwörter für Datenbanken und Zahlungsdienstleister. Gefordert waren 30 Bitcoin, gezahlt wurde nicht.

Sieben Tage zwischen Zugriff und Entdeckung sind ein Erkennungsproblem. Vierzehn Tage zwischen Entdeckung und öffentlicher Bestätigung sind ein Plan-Problem — und genau darum geht es hier.

Warum zwei Seiten reichen — und achtzig nicht

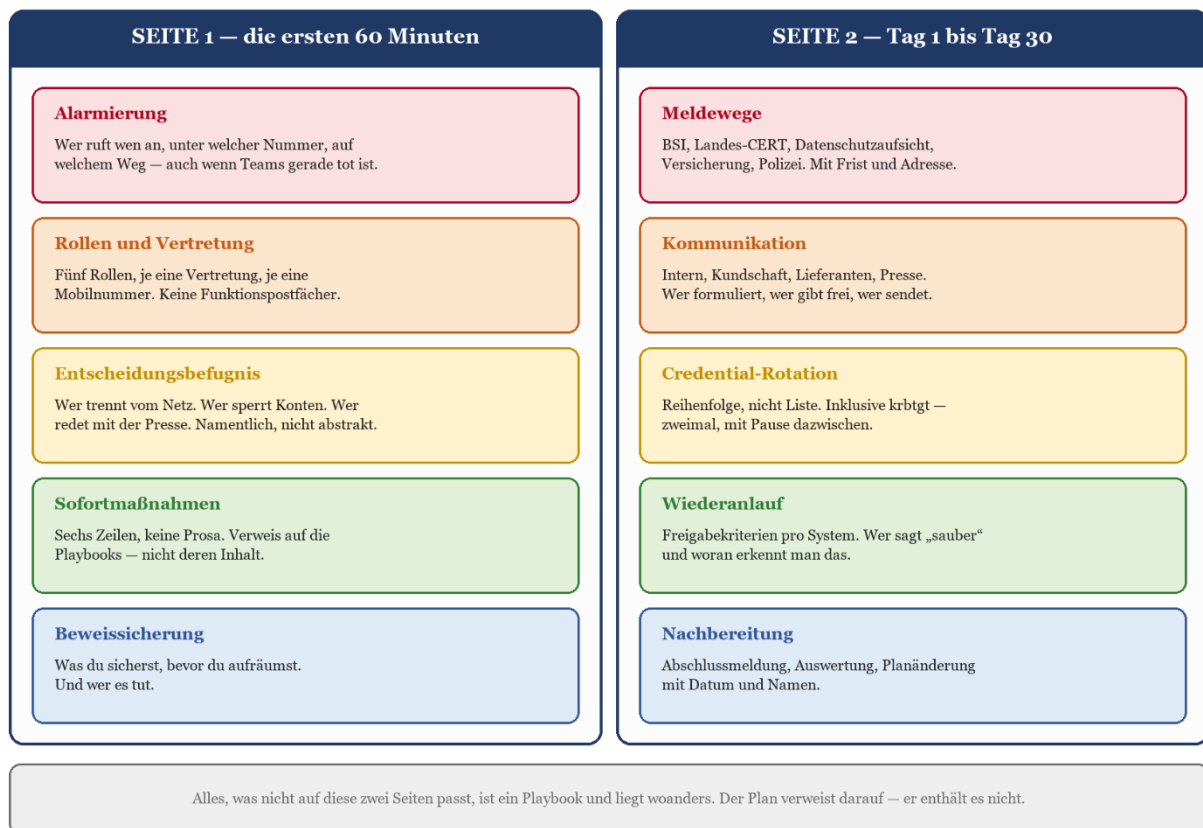
Die Länge eines Notfallplans ist kein Qualitätsmerkmal, sondern ein Risikoindikator. Je dicker das Dokument, desto sicherer kannst du sein, dass es niemand gelesen hat und im Ernstfall auch niemand liest. Ein Vorfall ist kein Leseabend. Er ist eine Situation, in der Menschen unter Zeitdruck, mit unvollständigen Informationen und meistens nachts Entscheidungen treffen, für die sie sich am nächsten Tag rechtfertigen müssen.

Der Plan ist ein Verteiler, kein Handbuch

Ein guter Incident-Response-Plan enthält keine Anleitung. Er enthält Zuständigkeiten, Kontaktdaten, Befugnisse, Fristen und Verweise. Das klingt banal, ist aber der eigentliche Unterschied: Ein Handbuch beantwortet die Frage „wie mache ich das?“. Ein Plan beantwortet die Frage „wer macht das, wann, und wen sage ich Bescheid?“. Die erste Frage kannst du im Ernstfall nachschlagen. Die zweite nicht — für die brauchst du eine Entscheidung, die vorher getroffen wurde.

Praktisch heißt das: Deine Playbooks für Phishing, Ransomware, Kontokompromittierung und Datenabfluss dürfen so lang sein, wie sie eben sind. Der Plan verweist auf sie mit einem Namen und einem Fundort. Mehr nicht.

Der Plan auf zwei Seiten: was wohin gehört



Skizze 1: Die Blattaufteilung. Seite 1 ist die erste Stunde, Seite 2 sind die nächsten dreißig Tage.

Was passiert, wenn der Plan nur im Tenant liegt

Das ist der Klassiker, und er ist so vermeidbar, dass es fast weh tut: Der Notfallplan liegt in SharePoint. Die Telefonliste steht in einem Teams-Wiki. Die Zugangsdaten für die externe Forensik liegen im Kennwortmanager, der über Entra ID angemeldet wird. Und dann ist der Tenant genau das Ding, das gerade brennt.

Der Plan gehört ausgedruckt an drei Orte: in den Serverraum, in die Schublade der IT-Leitung und in die Aktentasche derjenigen Person, die im Zweifel als Erste am Telefon ist. Zusätzlich als PDF auf einem Datenträger, der nicht im betroffenen Netz hängt. Papier hat einen unschlagbaren Vorteil: Es lässt sich nicht verschlüsseln.

WARNUNG — Der Plan im Tenant ist kein Plan

Wenn dein Notfallplan, deine Telefonliste, dein Kennwortmanager und deine Sicherungen alle über dieselbe Identität erreichbar sind, hast du keinen Notfallplan, sondern eine gemeinsame Ausfallursache. Ein Angreifer mit administrativen Rechten löscht in dieser Reihenfolge: Sicherungen, Protokolle, Notfalldokumentation — und zwar bevor er verschlüsselt.

Prüfe konkret: Kommst du an den Plan heran, wenn du dich nirgends anmelden kannst? Wenn nein, druck ihn aus. Heute, nicht nächsten Monat.

Rollen, Erreichbarkeit und die Frage, wer vom Netz trennt

Die häufigste Verzögerung in der ersten Stunde ist nicht technisch. Sie besteht aus dem Satz „das muss ich erst mit der Geschäftsführung klären“ — gefolgt von einer Mailbox-Ansage. In dieser Zeit

verschlüsselt die Gegenseite weiter. Deshalb ist die Rollen- und Befugnisfrage der wichtigste Abschnitt des ganzen Plans, wichtiger als jeder Klickpfad.

Fünf Rollen reichen — mehr verwirren nur

Große Rahmenwerke kennen ein Dutzend Rollen. Im Mittelstand besetzt du die ohnehin mit fünf Personen, die dann zwölf Hüte tragen und keinen davon richtig. Nimm fünf Rollen, benenne sie namentlich, gib jeder eine Vertretung und mach klar: Wer die Rolle hat, hat auch die Befugnis. Eine Rolle ohne Entscheidungsrecht ist eine Fußnote.

Rolle	Aufgabe im Vorfall	Entscheidet über	Muss erreichbar sein
Vorfalleitung	Führt den Vorfall, hält den Überblick, priorisiert, führt das Protokoll. Arbeitet selbst nicht an der Technik.	Eskalationsstufe, Reihenfolge der Maßnahmen, Hinzuziehen externer Hilfe	rund um die Uhr, Mobilnummer, Vertretung benannt
Technische Leitung	Koordiniert Analyse, Eindämmung, Beweissicherung und Wiederanlauf.	Trennung einzelner Systeme, Isolation von Geräten, Sperrung von Konten	rund um die Uhr, Mobilnummer, Vertretung benannt
Kommunikation	Formuliert intern und extern, hält Sprachregelung und Zeitpunkte fest.	Wortlaut aller Mitteilungen, Zeitpunkt der internen Information	Kernzeit plus Rufbereitschaft
Recht und Datenschutz	Bewertet Meldepflichten, führt die Fristenliste, spricht mit Aufsicht und Versicherung.	Ob und wann gemeldet wird, Umfang der Meldung	Kernzeit, im Vorfall binnen zwei Stunden
Geschäftsführung	Trägt die Entscheidung mit Geschäftsfolgen und die Außenwirkung.	Betriebsstillstand im großen Stil, Lösegeldfrage, Presseauftritt	rund um die Uhr, ohne Vorzimmer dazwischen

Tabelle 1: Fünf Rollen mit klarer Befugnis schlagen zwölf Rollen mit Rückfragepflicht.

Erreichbarkeit ist eine Zahl, keine Absicht

„Ist im Notfall erreichbar“ steht in vielen Plänen und bedeutet nichts. Was du brauchst: eine Mobilnummer, eine Zweitnummer, und die Aussage, über welchen Weg diese Person erreicht wird, wenn das Firmennetz und Teams ausgefallen sind. Signalisiert wird über privat erreichbare Kanäle, und das musst du vorher besprechen, nicht in der Nacht.

Ein zweiter Punkt, den fast alle vergessen: die Gegenrichtung. Wie erreicht dich der Bereitschaftsdienst deines Dienstleisters, wenn dein Postfach nicht erreichbar ist? Trag eine externe Alternativadresse ein, die nicht auf deiner eigenen Domäne liegt. Und teste einmal im Jahr, ob sie noch jemand liest.

TIPP — Die Telefonkarte im Scheckkartenformat

Der praktischste Teil eines Notfallplans ist eine laminierte Karte im Format einer Bankkarte: fünf Rollen, fünf Namen, fünf Mobilnummern, die Nummer des Bereitschaftsdiensts und die Nummer der externen Forensik. Auf der Rückseite die vier Sofortmaßnahmen und der Satz, dass Trennen erlaubt ist.

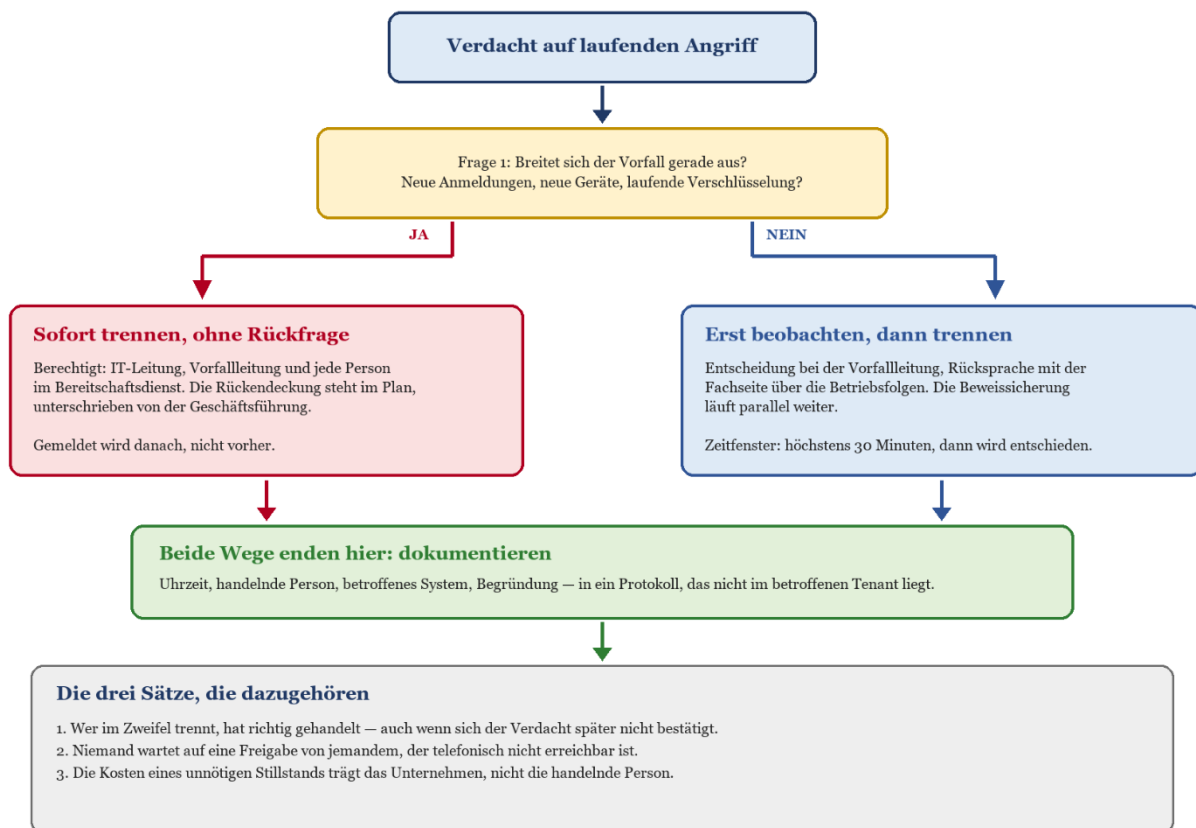
Kostet zwölf Euro für die ganze Mannschaft und ist im Ernstfall wertvoller als jedes Konzeptpapier.

Wer trennt vom Netz — die eine Frage, die vorher geklärt sein muss

Das ist die Frage, an der die meisten Vorfälle Zeit verlieren. Die Antwort im Plan muss lauten: Bei laufender Ausbreitung trennt jede Person aus dem Bereitschaftsdienst sofort, ohne Rückfrage. Und dieser Satz braucht eine Unterschrift der Geschäftsführung, weil sonst niemand ihn glaubt.

Der Grund ist psychologisch, nicht technisch. Wer nachts um zwei einen Produktionsserver vom Netz nimmt und am nächsten Morgen erklären muss, warum die Schicht stand, denkt zweimal nach. Wenn im Plan schwarz auf weiß steht, dass eine Trennung im Zweifel richtig war und die Kosten das Unternehmen trägt, entfällt dieses Zögern. Genau das ist der Zweck der Regelung.

Wer trennt vom Netz — der Entscheidungsbaum ohne Rückfrage



Skizze 2: Der Entscheidungsbaum für die Trennung. Zwei Wege, ein gemeinsames Ende: dokumentieren.

WARNUNG — Trennen heißt nicht ausschalten

Ein hartes Herunterfahren vernichtet den Arbeitsspeicher — und damit oft die einzigen Spuren des Angriffs, die nicht auf der Platte liegen. Trenne die Netzverbindung, isoliere das Gerät über Defender for Endpoint, zieh im Zweifel das Kabel. Aber schalte nicht aus, solange die Beweissicherung nicht entschieden hat.

Die Ausnahme: laufende Verschlüsselung auf einem Dateiserver. Da geht Schadensbegrenzung vor Beweiserhaltung — und diese Ausnahme steht im Plan, damit niemand sie in der Nacht neu erfinden muss.

Playbook-Verweise: der Plan zeigt, wo es steht

Der Plan enthält eine kurze Tabelle mit Szenarien. Pro Szenario: die erste Maßnahme in einer Zeile, der Name des Playbooks und wo es liegt. Wer die erste Maßnahme kennt, gewinnt Zeit; wer das Playbook findet, gewinnt Qualität.

Szenario	Erste Maßnahme in einer Zeile	Playbook
Phishing mit Klick	Sitzungen des Kontos widerrufen, Kennwort zurücksetzen, Posteingangsregeln prüfen	Playbook P-01, Ordner Notfall, Seite 1 bis 4
Kompromittiertes Konto	Anmeldung sperren, Sitzungen widerrufen, MFA-Methoden prüfen, Weiterleitungen aufheben	Playbook P-02, Ordner Notfall, Seite 5 bis 11
Ransomware auf Endgeräten	Geräte isolieren, Sicherungen vom Netz trennen, Verschlüsselungsumfang feststellen	Playbook P-03, Ordner Notfall, Seite 12 bis 22
Verdacht auf Tier-0-Kompromittierung	Bereitschaft der Forensik alarmieren, keine Rotation starten, Protokolle sichern	Playbook P-04, Ordner Notfall, Seite 23 bis 31
Datenabfluss ohne Verschlüsselung	Ausgehende Verbindungen prüfen, Freigaben und Gastzugriffe einfrieren	Playbook P-05, Ordner Notfall, Seite 32 bis 38
Ausfall ohne Angriffsverdacht	Vorfalleitung informiert, Betriebshandbuch statt Notfallplan	kein Playbook, regulärer Betriebsprozess

Tabelle 2: Playbook-Verweise im Plan. Eine Zeile Sofortmaßnahme, ein Fundort — mehr gehört nicht auf die zwei Seiten.

Die Playbooks selbst sind eigene Beiträge dieser Serie: [Phishing-Vorfall: die ersten 60 Minuten](#), [Kompromittiertes Konto erkennen und aufräumen](#) und [Ransomware-Vorsorge in Microsoft 365](#) decken die drei häufigsten Fälle ab. Wenn du gerade erst anfängst, bau diese drei zuerst und lass den Rest offen. Drei geübte Playbooks sind besser als neun ungelesene.

Meldewege: BSI, Landes-CERT, Datenschutz, Versicherung

Hier wird es unangenehm, weil hier Fristen laufen, die niemand anhält, während du analysierst. Und weil mehrere Uhren gleichzeitig ticken, die unterschiedliche Auslöser, unterschiedliche Adressaten und unterschiedliche Inhalte haben. Der häufigste Fehler: Man wartet, bis man weiß, was passiert ist. Dann ist die erste Frist längst weg.

Die Kette 24 Stunden, 72 Stunden, ein Monat

Das NIS2-Umsetzungsgesetz wurde am 6. Dezember 2025 verkündet und gilt seitdem. Für besonders wichtige und wichtige Einrichtungen sieht § 32 BSIG eine dreistufige Meldekette vor: eine Frühwarnung binnen 24 Stunden nach Kenntnis eines erheblichen Sicherheitsvorfalls, eine Folgemeldung mit erster Bewertung binnen 72 Stunden und eine Abschlussmeldung binnen eines Monats. Dauert der Vorfall länger an, kommt eine Fortschrittmeldung dazu. Das Meldeportal des BSI ist seit dem 6. Januar 2026 in Betrieb, die gesetzliche Registrierungsfrist lief am 6. März 2026 ab.

Wichtig ist das Prinzip dahinter: Schnelligkeit vor Vollständigkeit. Die Frühwarnung nach 24 Stunden verlangt keine Ursachenanalyse. Sie verlangt die Aussage, dass etwas passiert ist, welcher Art es vermutlich ist und ob ein grenzüberschreitender Bezug denkbar erscheint. Wer darauf wartet, dass die Forensik fertig ist, hat das Verfahren missverstanden. Welche technischen Maßnahmen in Microsoft 365 dabei regulatorisch zählen, behandelt [NIS2 aus Security-Sicht: technische Maßnahmen in M365](#) ausführlicher.

Artikel 33 und 34 DSGVO: die andere Uhr

Parallel läuft der Datenschutz, und der hat eine eigene Logik. Artikel 33 DSGVO verlangt die Meldung einer Verletzung des Schutzes personenbezogener Daten an die zuständige Aufsichtsbehörde binnen 72 Stunden ab Kenntnis. Später ist möglich, aber begründungspflichtig — und die Begründung wird geprüft. Artikel 34 verlangt zusätzlich die Benachrichtigung der betroffenen Personen, wenn voraussichtlich ein hohes Risiko besteht. Dafür gibt es keinen Stundenwert, sondern das schöne Wort „unverzüglich“, das im Zweifel schneller bedeutet als 72 Stunden.

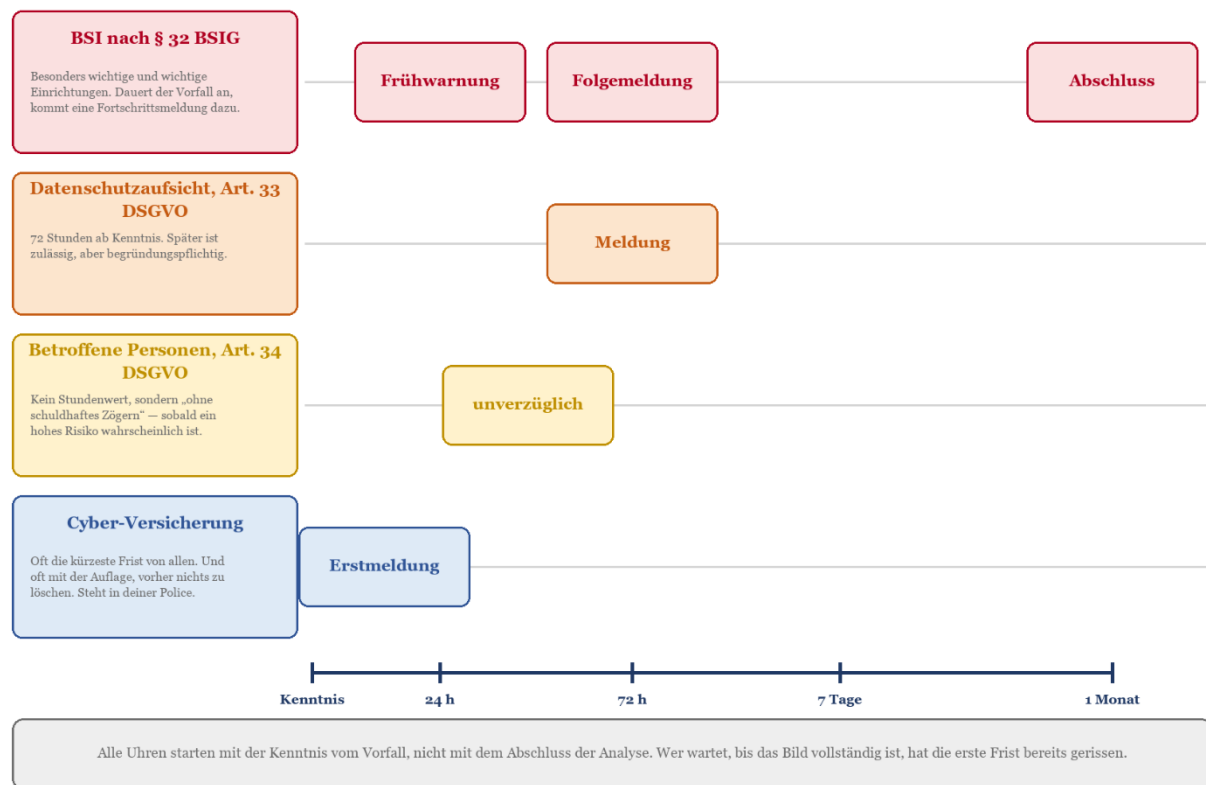
Der Denkfehler, den ich regelmäßig sehe: „Wir wissen ja noch nicht, ob Daten abgeflossen sind.“ Die Meldepflicht knüpft nicht an den Nachweis des Abflusses an, sondern an die Verletzung des Schutzes. Eine Verschlüsselung von Daten ist bereits eine Verletzung der Verfügbarkeit. Wer bei einem Ransomware-Vorfall meint, die DSGVO gehe ihn nichts an, weil nichts abgeflossen sei, wird von der Aufsichtsbehörde eines Besseren belehrt.

Landes-CERT, Polizei und die Versicherung

Neben den Pflichtmeldungen gibt es zwei sinnvolle freiwillige Wege und einen vertraglichen. Das CERT deines Bundeslands oder das zuständige Verwaltungs-CERT ist für Behörden und kommunale Einrichtungen häufig der schnellere und praktischere Ansprechpartner als der formale Meldeweg. Die Zentralen Ansprechstellen Cybercrime der Landeskriminalämter nehmen Anzeigen entgegen und arbeiten in der Regel deutlich unaufgeregter, als die meisten befürchten.

Und dann ist da die Cyber-Versicherung, die in der Praxis die kürzeste Frist von allen hat. Viele Policen verlangen eine Erstmeldung innerhalb weniger Stunden und verbieten gleichzeitig, vorher Systeme zu bereinigen oder Daten zu löschen. Wer den Dienstleister der Versicherung nicht einbindet, riskiert den Deckungsschutz. Diese Frist gehört in den Plan, mit der Policennummer und der Schadenmeldenummer daneben.

Vier Uhren, ein Startschuss: die Meldefristen



Skizze 3: Vier Uhren, ein Startschuss. Alle Fristen beginnen mit der Kenntnis, nicht mit dem Analyseergebnis.

Adressat	Frist	Auslöser	Wer meldet
BSI, Frühwarnung	24 Stunden ab Kenntnis	erheblicher Sicherheitsvorfall bei einer besonders wichtigen oder wichtigen Einrichtung	Recht und Datenschutz, Freigabe Vorfallleitung
BSI, Folgemeldung	72 Stunden ab Kenntnis	derselbe Vorfall, nun mit erster Bewertung und Erkenntnisstand	Recht und Datenschutz
BSI, Abschluss	ein Monat nach der Folgemeldung	Abschluss mit Ursachenanalyse und getroffenen Maßnahmen	Recht und Datenschutz, Freigabe Geschäftsführung
Datenschutzbehörde	72 Stunden ab Kenntnis	Verletzung des Schutzes personenbezogener Daten, auch bei bloßem Verfügbarkeitsverlust	Datenschutzbeauftragung
Betroffene Personen	unverzüglich	voraussichtlich hohes Risiko für die Rechte und Freiheiten der Betroffenen	Kommunikation, Freigabe Datenschutz
Cyber-Versicherung	laut Police, oft wenige Stunden	Verdacht auf einen versicherten Schadenfall	Geschäftsführung oder Vorfallleitung
Landes-CERT	freiwillig, so früh wie möglich	Vorfall mit möglicher Relevanz für andere Einrichtungen	Technische Leitung
Polizei, Zentrale Ansprechstelle Cybercrime	freiwillig, nach Beweissicherung	Straftat, insbesondere Erpressung oder Datenabfluss	Geschäftsführung

Tabelle 3: Die Meldematrix. Trag die tatsächlichen Adressen, Portale und Nummern direkt in deine Fassung ein.

FAKTEN — Was bei Verstößen droht

Das NIS2-Umsetzungsgesetz sieht Bußgelder von bis zu 10 Millionen Euro für besonders wichtige Einrichtungen und bis zu 7 Millionen Euro für wichtige Einrichtungen vor. Sanktioniert wird dabei

nicht nur der Vorfall, sondern auch das Versäumen der Meldung.

Hinzu kommt die persönliche Verantwortung der Leitungsebene für die Umsetzung und Überwachung der Risikomanagementmaßnahmen. Das ist der Grund, warum die Geschäftsführung in der Rollentabelle steht — nicht aus Höflichkeit.

Kommunikation unter Druck: was Berlin lehrt

Der Fall der beiden Berliner Senatsverwaltungen im August 2026 ist deshalb so lehrreich, weil er technisch nichts Ungewöhnliches zeigt, kommunikativ aber alles, was schiefgehen kann. Die Zeitachse: unbemerkter Zugriff vom 7. bis 12. August, Entdeckung am 14. August, öffentliche Bestätigung am 28. August, Veröffentlichung von 5,8 Terabyte durch die Tätergruppe am 4. September. Vierzehn Tage zwischen Entdeckung und Bestätigung — und in diesen vierzehn Tagen bestimmt nicht mehr die betroffene Organisation die Erzählung, sondern jeder andere.

Das ist keine Kritik an den Beteiligten, die in einer sehr unangenehmen Lage sehr viel zu tun hatten. Es ist eine Beobachtung über Pläne: Wenn im Plan nicht steht, wer wann was sagt, sagt erst mal niemand etwas. Und Schweigen ist unter Druck keine neutrale Option, sondern eine aktive Entscheidung mit Wirkung. Wie der Fall im Detail verlief und welche Härtungslücken er sichtbar gemacht hat, steht im [Dossier TerminalFix und der Berlin-Hack](#).

Intern zuerst — immer

Die Belegschaft erfährt vom Vorfall entweder von dir oder aus der Zeitung. Es gibt keine dritte Möglichkeit, und die zweite kostet Vertrauen, das du im Wiederanlauf dringend brauchst. Die interne Erstinformation muss nicht vollständig sein. Sie muss existieren, und sie muss drei Dinge enthalten: was bekannt ist, was die Leute jetzt tun sollen, und wann die nächste Information kommt.

Der dritte Punkt ist der wichtigste und wird fast immer vergessen. „Wir informieren wieder heute um 17 Uhr“ verhindert mehr Flurfunk als jede inhaltliche Aussage. Und daran musst du dich halten, auch wenn es nichts Neues gibt. „Es gibt keinen neuen Stand“ ist eine vollwertige Information.

Extern: drei Textbausteine, die schon fertig sind

Wenn du unter Druck formulierst, formulierst du schlecht. Deshalb gehören drei Rohtexte in den Anhang des Plans, vorab abgestimmt mit Recht und Geschäftsführung: eine interne Erstinformation, eine Kundeninformation und eine Pressemitteilung. Alle drei mit Lücken für das Konkrete, alle drei so formuliert, dass sie ohne juristische Nachbearbeitung raus können.

Was in keinen dieser Texte gehört: Spekulationen über die Ursache, Schuldzuweisungen an Dienstleister, Zusagen über Zeitpunkte, die du nicht halten kannst, und die Formulierung „nach aktuellem Kenntnisstand sind keine Daten abgeflossen“, solange du das nicht wirklich weißt. Dieser Satz ist der zuverlässigste Weg, zwei Wochen später dementieren zu müssen.

Zielgruppe	Wann	Kanal	Wer formuliert	Wer gibt frei
Belegschaft	innen 4 Stunden nach Feststellung	Aushang, SMS-Verteiler, Telefonkette — nicht per Mail im betroffenen Tenant	Kommunikation	Vorfallleitung
Betriebsrat	unverzüglich, vor allen Maßnahmen mit	persönlich, dann schriftlich	Kommunikation	Geschäftsführung

	Personenbezug			
Kundschaft mit Betroffenheit	innen 24 Stunden	direkte Ansprache durch die Betreuung, kein Serienbrief	Kommunikation und Vertrieb	Geschäftsführung
Lieferanten und Dienstleister	innen 24 Stunden, wenn Schnittstellen betroffen sind	Telefon, dann schriftlich	Technische Leitung	Vorfälleleitung
Presse	sobald ein belastbarer Kernsachverhalt steht	Mitteilung plus benannte Ansprechperson	Kommunikation	Geschäftsführung
Betroffene Personen nach Art. 34	unverzüglich bei hohem Risiko	individuell, in klarer und einfacher Sprache	Datenschutz und Kommunikation	Geschäftsführung

Tabelle 4: Die Kommunikationsmatrix. Wer formuliert und wer freigibt, sind zwei verschiedene Zeilen — das spart im Ernstfall eine Diskussion.

TIPP — Die Sprachregelung, die immer funktioniert

Drei Sätze, die du in fast jeder Lage sagen kannst, ohne dich festzulegen: Was bekannt ist, wird gesagt. Was nicht bekannt ist, wird als unbekannt bezeichnet. Was vermutet wird, bleibt drin.

Konkret: „Wir haben am Datum X einen Sicherheitsvorfall festgestellt und sofort Maßnahmen eingeleitet. Ob und in welchem Umfang Daten betroffen sind, wird derzeit geprüft; wir informieren dazu, sobald belastbare Ergebnisse vorliegen. Die zuständigen Behörden sind informiert.“

Das ist unspektakulär, ehrlich und muss später nicht zurückgenommen werden. Genau darum geht es.

Beweissicherung, Credential-Rotation, Wiederanlauf

Jetzt zum technischen Teil, den der Plan nur anreißt, dessen Reihenfolge er aber festlegt. Denn die Reihenfolge ist es, die im Ernstfall verloren geht: Es wird aufgeräumt, bevor gesichert wurde. Es wird rotiert, bevor der Angreifer draußen ist. Es wird wieder angefahren, bevor jemand weiß, wie er hereinkam.

Erst sichern, dann aufräumen

Beweissicherung klingt nach Staatsanwaltschaft, ist aber vor allem Selbstschutz. Ohne Protokolle kannst du weder die Frage der Aufsichtsbehörde beantworten, welche Daten betroffen waren, noch die Frage der Versicherung, wie der Angriff verlief, noch deine eigene Frage, ob der Angreifer wirklich weg ist. Und Protokolle sind endlich.

FAKTEN — Wie lange deine Spuren überhaupt existieren

Im Microsoft-Purview-Auditprotokoll gilt für Einträge seit dem 17. Oktober 2023 eine Standardaufbewahrung von 180 Tagen. Mit E5 beziehungsweise passendem Zusatz werden Vorgänge aus Microsoft Entra ID, Exchange, SharePoint und OneDrive standardmäßig ein Jahr aufbewahrt; alle übrigen Aktivitäten bleiben bei 180 Tagen, sofern du keine eigene Aufbewahrungsrichtlinie anlegst.

Praktische Folge: Wer einen Angriff entdeckt, der vor sieben Monaten begann, findet im Standardfall nichts mehr über dessen Anfang. Die Aufbewahrung ist damit keine Compliance-Frage, sondern eine Ermittlungsfrage. Mehr zu den Auswertungsmöglichkeiten im [Kompetenzbereich Microsoft Purview](#).

Was du in der ersten Stunde exportierst und außerhalb des betroffenen Tenants ablegst: das Auditprotokoll für den relevanten Zeitraum, die Anmeldeprotokolle aus Entra ID, die Nachrichten- und Weiterleitungsspuren aus Exchange Online, die Warnungen aus dem Defender-Portal und die

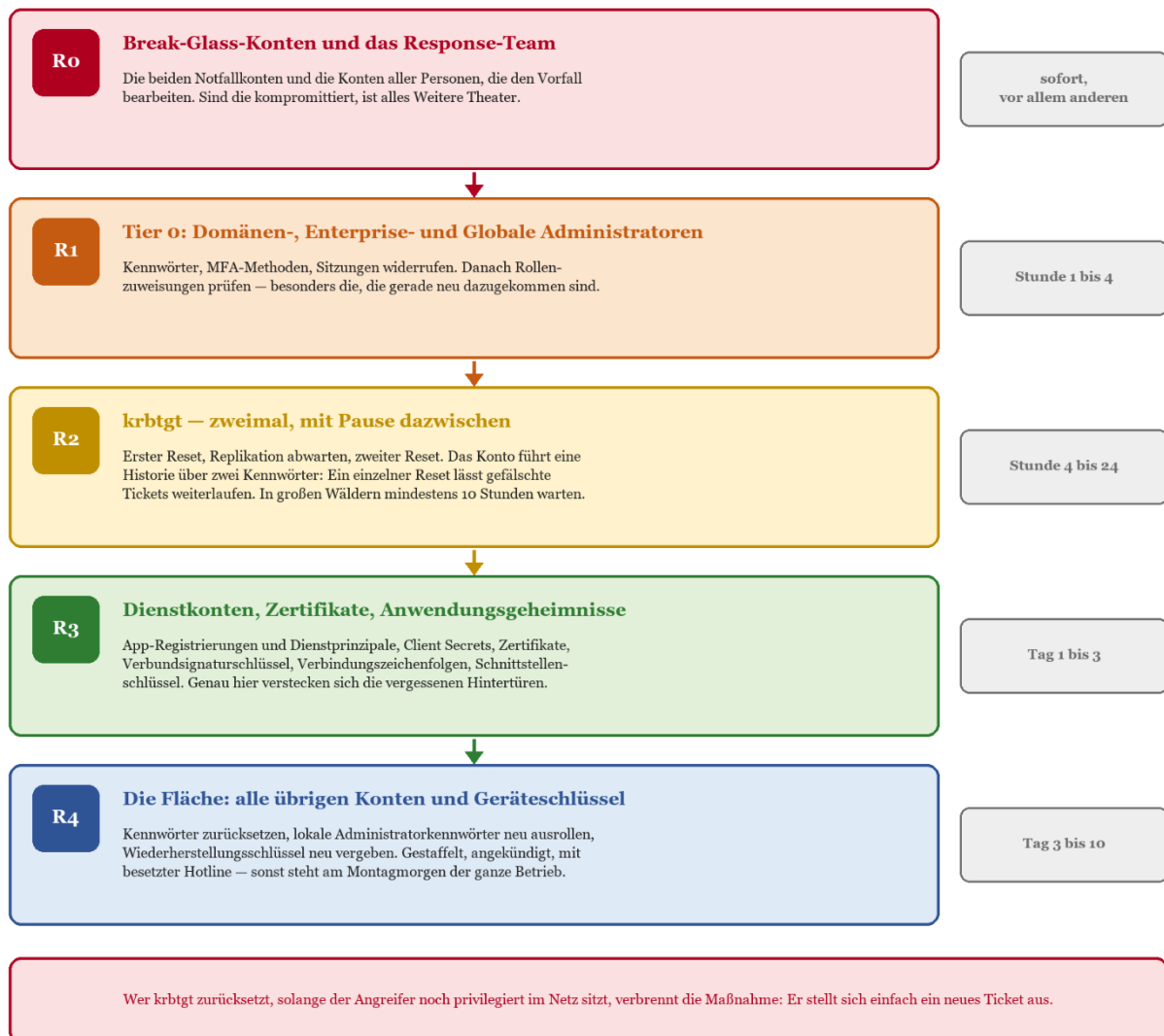
Konfigurationsstände der betroffenen Konten. Speicherabbilder betroffener Systeme macht die Forensik, aber nur, wenn die Systeme bis dahin nicht ausgeschaltet wurden.

Wenn du [Microsoft Sentinel anbinden: wann es sich lohnt](#) angebunden hast, ist dieser Teil deutlich entspannter, weil die Daten ohnehin außerhalb liegen und länger vorgehalten werden. Wenn nicht, brauchst du einen geübten Exportweg. Ein Exportweg, den niemand je ausprobiert hat, ist im Ernstfall kein Exportweg.

Credential-Rotation in Ringen — inklusive krbtgt

Der klassische Fehler bei der Rotation ist die alphabetische Liste. Man setzt Kennwörter zurück, irgendwo fängt man an, und weil es viel Arbeit ist, dauert es Tage. In dieser Zeit hat der Angreifer die noch nicht rotierten Zugänge und baut sich in aller Ruhe einen neuen Weg hinein. Rotiere in Ringen, von innen nach außen, und rotiere erst, wenn du hinreichend sicher bist, dass die Gegenseite keinen aktiven Zugang mehr hat.

Credential-Rotation: Reihenfolge schlägt Vollständigkeit



Skizze 4: Die Rotation läuft in Ringen. Ring R2 ist der, den fast alle Pläne vergessen.

Ring R2 verdient eine eigene Erklärung. Das Konto krbtgt ist das Dienstkonto der Kerberos-Schlüsselverteilung im Active Directory. Wer den Kennworthash dieses Kontos besitzt, kann sich

beliebige gültige Kerberos-Tickets ausstellen — für jedes Konto, mit jeder Berechtigung, ohne dass ein Domänencontroller Verdacht schöpft. Das ist der Grund, warum bei einer bestätigten Kompromittierung von Domänenadministratoren kein Weg an der Rotation dieses Kontos vorbeiführt.

Und sie muss zweimal erfolgen. Das Konto führt eine Historie über die letzten beiden Kennwörter, damit bei einem regulären Wechsel bereits ausgestellte Tickets nicht schlagartig ungültig werden. Genau diese Kulanz nutzt ein gefälschtes Ticket auch: Nach einem einzelnen Zurücksetzen ist der alte Hash noch gültig. Zwischen den beiden Zurücksetzungen muss die Replikation vollständig durchgelaufen sein — in großen Wäldern rechnet man mit mindestens zehn Stunden, sonst arbeitet ein Domänencontroller weiter mit einem Kennwort, das die anderen schon nicht mehr kennen. Die Hintergründe zu Tickets, Hashes und Verschlüsselungstypen stehen im [Kompetenzbereich Kerberos](#).

WARNUNG — krbtgt-Rotation zum falschen Zeitpunkt ist verschwendete Munition

Setzt du krbtgt zurück, während der Angreifer noch privilegierten Zugang hat, stellt er sich anschließend einfach ein neues Ticket aus — und du hast deine wirkungsvollste Maßnahme verbrannt und ihn gleichzeitig gewarnt, dass du ihn siehst.

Reihenfolge: erst Eindämmung und Rausdrängen, dann Rotation. Und wenn du nicht sicher bist, ob der Zugang wirklich beendet ist, holst du an dieser Stelle externe Forensik dazu. Das ist kein Eingeständnis von Schwäche, sondern die günstigere Variante.

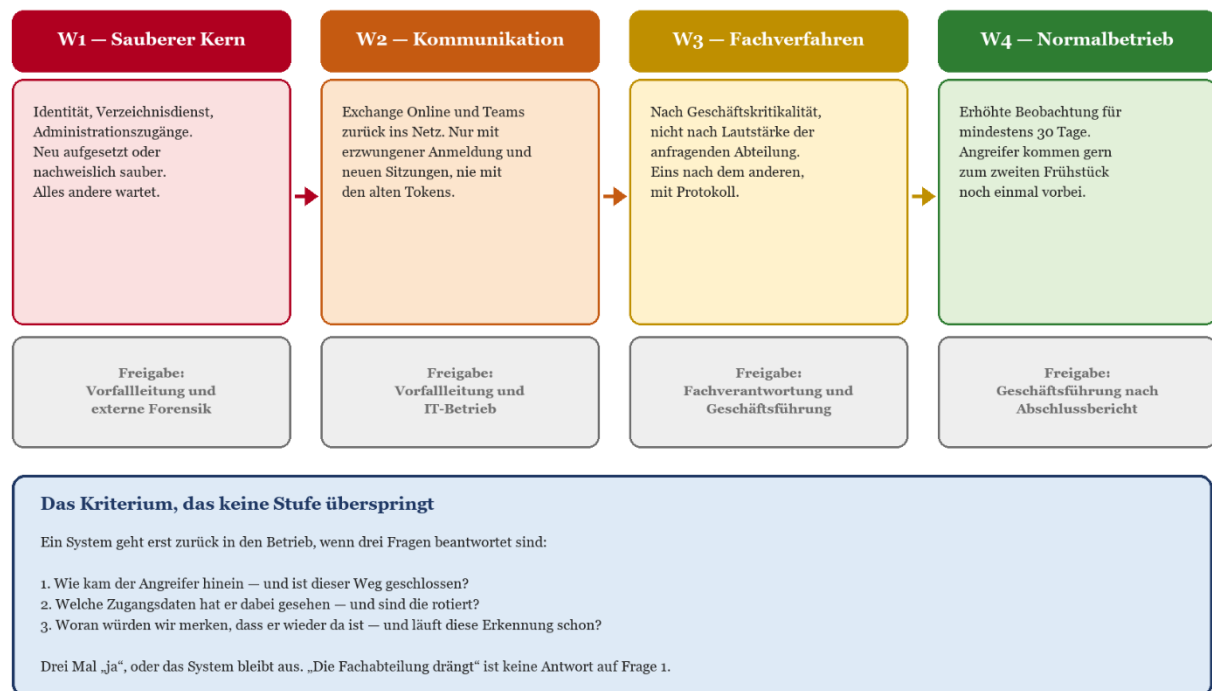
Zweiter Klassiker: die Rotation wird einmal durchgeführt und im Protokoll als erledigt vermerkt. Ein einzelner Reset reicht nicht. Zwei Durchgänge, mit dokumentierter Pause dazwischen.

Vergiss neben den Konten die Geheimnisse nicht. App-Registrierungen mit lang laufenden Client Secrets, Dienstprinzipale mit weitreichenden Berechtigungen, Zertifikate für Verbunddienste, Verbindungszeichenfolgen in Automatisierungen: Das ist der Ring R3, und er ist der, in dem die vergessenen Hintertüren stecken. Ein Angreifer, der einen Dienstprinzipal mit Anwendungsberechtigungen anlegt, überlebt jede Kennwortrotation der Welt. Wer die Erkennung dafür im Vorfeld aufsetzen will, findet die Grundlagen in [Defender for Identity: das Active Directory im Blick](#) und [Alert Policies und Benachrichtigungen richtig aufsetzen](#).

Wiederanlauf: die Freigabe ist eine Entscheidung, keine Erleichterung

Der Wiederanlauf ist die Phase, in der der Druck am größten und die Disziplin am kleinsten ist. Alle wollen zurück in den Betrieb, die Fachabteilungen rufen an, die Geschäftsführung fragt nach dem Zeitpunkt, und irgendwann sagt jemand „das läuft doch wieder“. Genau dann wird der zweite Vorfall vorbereitet.

Wiederanlauf: vier Stufen, vier Freigaben



Skizze 5: Vier Stufen, vier Freigaben. Keine Stufe überspringt die drei Fragen unten rechts.

Der Plan legt die Stufen und die Freigebenden fest, nicht die Termine. Termine ergeben sich aus dem Befund. Was der Plan aber festlegt: dass ein System erst zurückkommt, wenn der Eintrittsweg geschlossen, die betroffenen Zugangsdaten rotiert und eine Erkennung für einen Rückfall aktiv ist. Diese drei Fragen sind nicht verhandelbar, und die Vorfalleitung darf sie nicht allein aufweichen.

Zur Wiederherstellung selbst: Wiederherstellen aus einer Sicherung, die aus dem Zeitraum des unbemerkten Zugriffs stammt, holt den Angreifer zurück ins Haus. Deshalb brauchst du den Erstzugriffszeitpunkt, bevor du den Wiederherstellungspunkt wählst — und deshalb ist die Beweissicherung keine akademische Übung. Wie die Sicherungsseite vorab aussehen muss, damit du an dieser Stelle überhaupt eine Wahl hast, steht in [Ransomware-Vorsorge in Microsoft 365](#).

Die Vorlage: dein Plan auf zwei Seiten

Hier ist das Gerüst. Nimm es, kürze es dort, wo es für dich nicht passt, und füll die rechte Spalte mit echten Namen und echten Nummern. Ein Plan mit Platzhaltern ist schlimmer als keiner, weil er das Gefühl von Vorbereitung erzeugt, ohne sie zu liefern.

Feld	Was hineingehört	Beispieleintrag
Geltung und Auslöser	Ab wann gilt dieser Plan statt des normalen Störungsprozesses	Bei jedem begründeten Verdacht auf unbefugten Zugriff, Datenabfluss oder Verschlüsselung
Alarmierungsweg	Nummer, Reihenfolge, Alternativkanal ohne Firmennetz	Bereitschaft 0170-..., danach Vorfalleitung 0171-..., Ausweichkanal: SMS-Verteiler „Notfall“
Rolle Vorfalleitung	Name, Vertretung, Mobilnummer, Befugnis	M. Kern, Vertretung A. Roth, 0171-..., entscheidet über Eskalation und externe Hilfe
Rolle Technische Leitung	Name, Vertretung, Mobilnummer, Befugnis	T. Weiss, Vertretung J. Barth, 0172-..., entscheidet über Trennung und Isolation
Rolle Kommunikation	Name, Vertretung, Mobilnummer, Befugnis	S. Adler, Vertretung P. Lang, 0173-..., formuliert alle Mitteilungen

Rolle Recht und Datenschutz	Name, Vertretung, Mobilnummer, Befugnis	Kanzlei ..., DSB Frau ..., 0174-..., führt die Fristenliste
Trennbefugnis	Wer darf ohne Rückfrage trennen, mit Rückendeckungssatz	Bereitschaft, Technische Leitung, Vorfalleitung. Rückendeckung unterschrieben am ...
Sofortmaßnahmen	Höchstens sechs Zeilen, keine Klickpfade	Isolieren, Sitzungen widerrufen, Sicherungen trennen, Protokolle exportieren, Uhrzeit notieren
Playbook-Verweise	Szenario, Playbook-Nummer, Fundort	P-01 Phishing, P-02 Konto, P-03 Ransomware, P-04 Tier 0, P-05 Datenabfluss, Ordner Notfall
Beweissicherung	Was, durch wen, wohin, in welcher Reihenfolge	Auditprotokoll, Anmeldeprotokolle, Nachrichtenspuren — Export auf externen Datenträger, durch Technische Leitung
Meldefristen	Adressat, Frist, Kontakt, wer meldet	BSI 24/72/1 Monat über das Meldeportal, Aufsicht 72 Stunden, Versicherung Police Nr. ...
Kommunikationsmatrix	Zielgruppe, Zeitpunkt, Kanal, Freigabe	Belegschaft binnen 4 Stunden, Kundschaft binnen 24 Stunden, Presse nach Kernsachverhalt
Textbausteine	Fundort der drei vorbereiteten Rohtexte	Anhang A bis C des Plans, abgestimmt am ...
Credential-Rotation	Ringe R0 bis R4 mit Zuständigkeit, krbtgt ausdrücklich benannt	R0 Break-Glass, R1 Tier 0, R2 krbtgt zweimal mit 10 Stunden Pause, R3 Geheimnisse, R4 Fläche
Wiederanlauf	Stufen W1 bis W4 mit Freigebenden und den drei Pflichtfragen	W1 Kern, W2 Kommunikation, W3 Fachverfahren, W4 Normalbetrieb
Externe Hilfe	Forensik, Dienstleister, Versicherung mit Nummer und Vertragsstand	Forensik ... Rufbereitschaft 24/7, Rahmenvertrag vom ..., Kundennummer ...
Nachbereitung	Auswertungstermin, Verantwortung, Fristen für Planänderungen	Auswertung binnen 14 Tagen nach Abschluss, Planfortschreibung binnen 30 Tagen
Stand und Prüfung	Versionsdatum, nächste Prüfung, letzte Übung	Fassung 3.1 vom ..., nächste Prüfung ..., letzte Übung ...

Tabelle 5: Die Vorlage. Achtzehn Felder, zwei Seiten, keine Platzhalter mehr, wenn du fertig bist.

WICHTIG — Ein ungeübter Plan ist eine Vermutung

Ein Plan, der nie durchgespielt wurde, beschreibt nicht, was passieren wird, sondern was sich jemand am Schreibtisch vorgestellt hat. Der erste Trockenlauf deckt regelmäßig auf: Zwei der Nummern sind veraltet, niemand weiß, wo der Exportweg für die Protokolle liegt, und die Person mit der Trennbefugnis wusste gar nicht, dass sie sie hat.

Plane mindestens einmal im Jahr eine Übung am Tisch, zwei Stunden, alle fünf Rollen im Raum. Wie das ohne Aufwandsexplosion geht, steht in [Feuerwehrübung: Security-Notfälle im Team trainieren](#). Wenn du weitergehen willst, ist [Red-Team-Übung: der kontrollierte Angriff](#) die nächste Stufe.

Und nach jeder echten Störung, auch nach einer harmlosen: Plan aufschlagen, eine Seite anpassen, Datum ändern. Zwanzig Minuten. Das ist der Unterschied zwischen einem lebenden Dokument und einem Ordner im Regal.

Häufige Fragen

Wir sind sechzig Leute. Brauchen wir wirklich fünf Rollen?

Fünf Rollen heißt nicht fünf Vollzeitstellen. In einem Unternehmen dieser Größe sind das typischerweise drei Personen, die sich die Rollen teilen, plus die externe Kanzlei und die Geschäftsführung. Was zählt, ist nicht die Anzahl der Köpfe, sondern dass für jede der fünf Aufgaben jemand namentlich zuständig ist. Die Kombination aus Vorfallleitung und Technischer Leitung in einer Person funktioniert allerdings selten: Wer selbst an der Konsole sitzt, führt keinen Vorfall.

Ab wann ist ein Vorfall meldepflichtig?

Bei NIS2 knüpft die Pflicht an den erheblichen Sicherheitsvorfall an — schwerwiegende Betriebsstörung, finanzieller Verlust oder erhebliche Auswirkungen auf andere. Beim Datenschutz genügt bereits die Verletzung des Schutzes personenbezogener Daten, wozu auch reiner Verfügbarkeitsverlust durch Verschlüsselung zählt. Die praktische Antwort: Kläre die Frage früh mit Recht und Datenschutz, nicht in Stunde zwanzig. Und melde im Zweifel — eine unnötige Frühwarnung ist folgenlos, eine versäumte nicht.

Wer darf entscheiden, dass wir zahlen?

Ausschließlich die Geschäftsführung, und diese Entscheidung gehört nicht in die Nacht des Vorfalls. Was in den Plan gehört, ist der Satz, dass die Frage nur auf Ebene der Geschäftsführung und nur mit rechtlicher Begleitung behandelt wird, und dass niemand aus dem Response-Team eigenständig mit der Gegenseite kommuniziert. Berlin hat 30 Bitcoin nicht gezahlt und die Daten trotzdem verloren — Zahlen ist keine Garantie, sondern eine Wette.

Reicht Microsoft Defender, oder brauchen wir externe Forensik?

Für Erkennung, Isolation und einen Großteil der Analyse kommst du mit dem Defender-Portal und der erweiterten Suche sehr weit — vorausgesetzt, das Onboarding ist sauber gelaufen, siehe [Defender for Endpoint: Onboarding ohne Drama](#). Externe Forensik brauchst du in zwei Fällen: bei begründetem Verdacht auf Tier-O-Kompromittierung und immer dann, wenn die Ergebnisse gegenüber Aufsicht, Versicherung oder Gericht belastbar sein müssen. Die Rahmenvereinbarung dafür schließt du vorher ab, nicht am Vorfallabend um 23 Uhr.

Wie oft muss der Plan aktualisiert werden?

Fest terminiert einmal im Jahr, anlassbezogen nach jeder Personalveränderung in einer der fünf Rollen, nach jeder Übung und nach jeder echten Störung. Die Kontaktdaten sind der Teil, der am schnellsten verrottet: Prüfe sie halbjährlich, indem du die Nummern tatsächlich anrufst. Ein Abgleich mit dem Telefonverzeichnis ist kein Test.

Was ist mit dem Betriebsrat?

Der Betriebsrat wird im Vorfall informiert, sobald Maßnahmen mit Personenbezug anstehen — und das sind sie fast immer, sobald du Anmeldeprotokolle auswertest oder Konten sperrst. Die Grundlagen dafür regelst du besser vorher in einer Betriebsvereinbarung als hinterher in einer Krisensitzung. Was mitbestimmungspflichtig ist und was nicht, behandelt [Security-Monitoring und Betriebsrat: was mitbestimmungspflichtig ist](#) im Detail. Ein Satz gehört trotzdem in den Plan: die Nummer der oder des Vorsitzenden.

Sollen wir eine Break-Glass-Anmeldung in den Plan schreiben?

Ja — aber nicht die Zugangsdaten selbst. In den Plan gehört, dass es zwei Notfallkonten gibt, wo die Anmeldedaten physisch liegen, wer sie entnehmen darf und dass jede Entnahme protokolliert und gemeldet wird. Die Kennwörter kommen versiegelt in den Tresor, nicht in das Dokument. Wie die Konten aufgebaut und überwacht werden, steht in [Break-Glass-Konten anlegen und überwachen](#).

Wir haben keinen Plan und wenig Zeit. Womit fangen wir an?

Mit einer Seite: fünf Rollen, fünf Nummern, der Trennbefugnis-Satz mit Unterschrift und den vier Meldefristen. Das schaffst du an einem Nachmittag. Die zweite Seite und die Playbooks kommen danach. Diese eine Seite ist bereits mehr wert als das achtzigseitige Werk, das in sechs Monaten fertig sein soll — denn der Vorfall richtet sich nicht nach deiner Projektplanung.

Fazit

Ein Incident-Response-Plan ist kein Sicherheitsprodukt, sondern eine Sammlung von Entscheidungen, die du in Ruhe triffst, damit sie unter Druck nicht getroffen werden müssen. Wer trennt. Wer spricht. Wer meldet. Wann kommt was zurück. Diese vier Antworten sind der eigentliche Inhalt. Alles andere ist Anhang.

Die drei Punkte, an denen Pläne in der Praxis reißen, sind bemerkenswert konstant: Die Trennbefugnis ist nicht geklärt, deshalb wartet nachts jemand auf einen Rückruf. Die Fristen sind nicht bekannt, deshalb wird gemeldet, wenn das Ergebnis vorliegt — also zu spät. Und die Rotation wird als Liste statt als Reihenfolge abgearbeitet, wobei krrtgt entweder vergessen oder nur einmal zurückgesetzt wird. Alle drei kosten nichts in der Vorbereitung und viel im Ernstfall.

Berlin hat gezeigt, was vierzehn Tage Schweigen kosten. Nicht weil dort schlecht gearbeitet worden wäre, sondern weil unter Druck nur das funktioniert, was vorher entschieden war. Schreib die zwei Seiten. Druck sie aus. Spiel sie einmal durch. Und dann hoffe, dass du sie nie brauchst — mit dem angenehmen Gefühl, dass es nicht schlimm wäre, wenn doch.

Wenn du den Plan nicht allein aufsetzen willst oder eine Zweitmeinung zur Belastbarkeit deiner Fassung suchst, ist die [Microsoft 365 Security Beratung](#) der passende Einstieg. Soll das Team die Abläufe selbst beherrschen, führt der Weg über die [Schulung Microsoft 365 Security](#).

WEITER — Passende Beiträge aus dieser Reihe

- › [Microsoft 365 Security](#) — die Übersicht über alle Handlungsfelder
- › [Feuerwehrrübung: Security-Notfälle im Team trainieren](#) — den Plan im Team durchspielen, bevor es ernst wird
- › [Kompromittiertes Konto erkennen und aufräumen](#) — das Playbook für den häufigsten Einzelfall
- › [Ransomware-Vorsorge in Microsoft 365](#) — die Vorsorge, die den Wiederanlauf überhaupt erst ermöglicht
- › [Phishing-Vorfall: die ersten 60 Minuten](#) — die ersten 60 Minuten nach dem Klick
- › [Dossier TerminalFix und der Berlin-Hack](#) — Kommunikation unter Druck, an einem realen Fall
- › [NIS2 aus Security-Sicht: technische Maßnahmen in M365](#) — welche Maßnahmen regulatorisch zählen
- › [Break-Glass-Konten anlegen und überwachen](#) — die Konten, die im Notfall noch funktionieren
- › [Kompetenzbereich Kerberos](#) — Hintergründe zu Tickets, Hashes und krrtgt
- › [Kompetenzbereich Microsoft Purview](#) — Auditprotokolle als Grundlage der Beweissicherung
- › [Tenant-Härtung: die 20 wichtigsten Schrauben](#) — die Schrauben, die den Vorfall

unwahrscheinlicher machen

- › [Security-Reporting für die Geschäftsführung](#) — wie du das Thema in der Geschäftsführung platzierst
- › [Microsoft 365 Security Beratung](#) — Unterstützung beim Aufsetzen und Prüfen des Plans
- › [Schulung Microsoft 365 Security](#) — wenn das Team es selbst können soll