

Feuerwehrrübung: Security-Notfälle im Team trainieren

Jedes Unternehmen in Deutschland weiß, wo sich die Belegschaft sammelt, wenn es brennt. Nicht, weil das irgendwo in einem Ordner steht, sondern weil einmal im Jahr eine Sirene losgeht und alle bei Nieselregen auf den Parkplatz laufen, sich zählen lassen und dann Kaffee trinken. Das Ganze dauert zwanzig Minuten, kostet echtes Geld an Arbeitszeit, und niemand käme auf die Idee, es abzuschaffen. Es steht im Arbeitsschutz, und Feuer ist eben ernst.

Und dann gibt es den anderen Notfall. Den, der statistisch deutlich wahrscheinlicher ist als ein Brand, deutlich länger dauert und deutlich mehr kostet: den Security-Vorfall. Für den hat man meistens auch ein Dokument. Das hat sogar jemand gelesen — der Mensch, der es geschrieben hat. Geübt wurde es nie. Wenn es dann so weit ist, stellt sich um 23:40 Uhr heraus, dass niemand weiß, wer ein Adminkonto sperren darf, dass die Telefonnummer der Geschäftsführung in einem Teams-Chat steht, der gerade nicht erreichbar ist, und dass die Frage „Dürfen wir das eigentlich abschalten?“ ungefähr vierzig Minuten Diskussion verschlingt. Vierzig Minuten, in denen ein Verschlüsselungsprozess sehr fleißig weiterarbeitet.

Die Feuerwehrrübung für diesen Fall heißt Tabletop-Übung. Sie kostet 90 Minuten, einen Besprechungsraum und ein bisschen Vorbereitung. Es wird nichts abgeschaltet, nichts geklickt, nichts kaputtgemacht. Es wird geredet — aber unter Zeitdruck, mit Einspielungen, die immer schlechter werden, und mit einem Menschen im Raum, der mitschreibt, wie lange das Team gebraucht hat, bis es die erste Entscheidung getroffen hat. Genau darin liegt der ganze Wert: Eine Tabletop Übung IT-Sicherheit misst nicht deine Technik. Sie misst deine Entscheidungsfähigkeit.

Dieser Beitrag gehört zum Handlungsfeld E der Serie [Microsoft 365 Security](#). Er liefert ein fertiges Format für 90 Minuten: Rollen, Zeitplan, Einspielungen, Beobachtungsbogen, Auswertung, Maßnahmenliste. Dazu drei komplette Szenarien, die du ohne weitere Vorbereitung spielen kannst. Was hier nicht steht, ist der Plan selbst — der steht im Beitrag [Incident-Response-Plan für Microsoft 365](#), und du brauchst ihn, bevor du übst. Eine Übung ohne Plan ist keine Übung, sondern eine Erkenntnisveranstaltung mit sehr niedrigem Ausgangsniveau.

FAKTEN — Warum das Szenario in diesem Beitrag kein Fantasieprodukt ist

Microsoft führt im Digital Defense Report 2025 ClickFix als Ursache von rund 47 Prozent der beobachteten Erstkompromittierungen. Zwischen März und Mai 2025 zählte Microsoft weltweit mehr als 394.000 infizierte Windows-Geräte. ESET maß von Ende 2024 bis Mitte 2025 einen Anstieg der ClickFix-Aktivität um 517 Prozent.

Im August 2026 traf die TerminalFix-Variante zwei Berliner Senatsverwaltungen. Der Zugriff lief vom 7. bis 12. August unbemerkt, entdeckt wurde er am 14. August, öffentlich bestätigt am 28. August. Am 4. September veröffentlichte die Gruppe Rhysida rund 5,8 Terabyte und etwa 1,44 Millionen Dateien. Gefordert waren 30 Bitcoin, umgerechnet etwa zwei Millionen Euro.

Seit der Verkündung des NIS2-Umsetzungsgesetzes am 6. Dezember 2025 gilt für betroffene Einrichtungen die dreistufige Meldepflicht: Frühwarnung binnen 24 Stunden, Folgemeldung binnen 72 Stunden, Abschlussbericht binnen eines Monats. Keine Übergangsfrist. Diese 24 Stunden sind der eigentliche Grund, warum die Geschäftsführung mitüben muss.

Warum am grünen Tisch geübt wird — und nicht am Produktivsystem

Der häufigste Einwand gegen eine Tabletop-Übung lautet: „Das ist doch nur Theorie, wir wollen einen echten Test.“ Der Einwand klingt tatkräftig und ist trotzdem falsch herum gedacht. Ein echter Test prüft, ob deine Technik hält. Eine Tabletop-Übung prüft, ob deine Organisation funktioniert. Und in der überwiegenden Zahl der Vorfälle, die ich gesehen habe, hat nicht die Technik versagt, sondern die Organisation drumherum: Die Erkennung war da, der Alarm ging raus, die Mail landete in einem Postfach, das um 18 Uhr niemand mehr liest.

Das BSI kennt in seinem Standard 200-4 eine ganze Leiter von Übungsformaten, von der reinen Planbesprechung über die Stabsübung bis zur Vollübung mit tatsächlichem Wiederanlauf. Die Planbesprechung — im internationalen Sprachgebrauch die Tabletop-Übung — steht ganz unten auf dieser Leiter, und das ist keine Abwertung, sondern eine Empfehlung: Sie ist der Einstieg, weil sie am wenigsten kostet und am meisten aufdeckt. Wer mit einer Vollübung anfängt, produziert Chaos und lernt daraus vor allem, dass Vollübungen anstrengend sind.

Format	Aufwand	Was es wirklich prüft	Wann sinnvoll
Tabletop-Übung	90 Min., 8 Personen, kein System	Entscheidungswege, Rollen, Kommunikation, ob der Plan im Kopf und nicht nur im Ordner ist	Als Einstieg und danach mindestens jährlich. Immer nach größeren Änderungen an Team oder Plan.
Stabsübung	Halber Tag, mit Protokoll und Lagebild	Zusammenarbeit eines eingespielten Krisenstabs über mehrere Stunden hinweg	Wenn die Tabletop-Übung zweimal sauber gelaufen ist und der Stab formal existiert
Funktionaler Test	Wartungsfenster, echte Systeme	Ob Wiederherstellung, Rückspielung der Sicherung und Notfallzugänge technisch tatsächlich gehen	Ein- bis zweimal jährlich für die kritischsten Wiederanlaufpläne, getrennt von der Tabletop-Übung
Phishing-Simulation	Kampagne über Wochen, ganze Belegschaft	Verhalten einzelner Personen am Posteingang, Meldequote, Wirksamkeit von Schulung	Laufend als Programm — deckt aber nichts über Entscheidungswege auf
Red-Team-Übung	Wochen, externes Team, echtes Geld	Ob deine Abwehr einem geplanten Angriff standhält und ob dein Betrieb ihn überhaupt bemerkt	Wenn die Grundlagen sitzen. Vorher liefert sie nur eine sehr teure Liste bekannter Lücken

Fünf Formate, fünf Zwecke. Sie ersetzen einander nicht — sie bauen aufeinander auf.

Der Vergleich mit der [Red-Team-Übung: der kontrollierte Angriff](#) lohnt sich, weil beide Formate gern verwechselt werden. Ein Red Team greift wirklich an und beantwortet die Frage: Kommen sie rein? Eine Tabletop-Übung greift niemanden an und beantwortet die Frage: Was macht ihr, wenn sie drin sind? Die zweite Frage ist unangenehmer, denn auf sie gibt es keine technische Antwort, die man kaufen könnte. Und sie ist billiger zu beantworten. Wenn dein Budget für genau eine Übung im Jahr reicht, nimm die Tabletop-Übung. Wenn du die Red-Team-Übung zuerst machst, weißt du danach, dass sie reingekommen sind — und stehst immer noch ratlos im Raum.

Was eine Tabletop-Übung leistet — und was nicht

Ehrlichkeit über die Grenzen des Formats erspart dir hinterher Enttäuschung. Eine Tabletop-Übung leistet zuverlässig vier Dinge: Sie deckt fehlende Zuständigkeiten auf, sie deckt fehlende Informationen auf, sie deckt fehlende Erreichbarkeit auf, und sie macht der Geschäftsführung körperlich spürbar, wie eng 24 Stunden sind. Der letzte Punkt ist der wertvollste und lässt sich durch kein Dokument der Welt ersetzen.

Sie leistet ausdrücklich nicht: den Nachweis, dass deine Sicherungen zurückspielbar sind. Den Nachweis, dass Defender den Angriff erkennt. Den Nachweis, dass dein Break-Glass-Konto funktioniert — das prüfst du separat, siehe [Break-Glass-Konten anlegen und überwachen](#). Und sie ersetzt keine Härtung. Ein Team, das perfekt kommuniziert, während der Tenant offensteht wie ein Scheunentor, kommuniziert eben sehr gut über den eigenen Untergang. Die Reihenfolge ist: erst die [Tenant-Härtung: die 20 wichtigsten Schrauben](#), dann üben, wie man mit dem Rest umgeht.

Warum die Geschäftsführung nicht „später informiert“ wird

Der reflexhafte Vorschlag lautet meistens: „Wir üben erst mal in der IT, und wenn das klappt, holen wir die Geschäftsführung dazu.“ Das ist gut gemeint und garantiert, dass die entscheidenden Fragen nie geübt werden. Denn drei der vier härtesten Entscheidungen eines Ransomware-Vorfalles trifft die IT gar nicht: Zahlen wir? Schalten wir das Werk ab, obwohl heute ausgeliefert werden muss? Was sagen wir der Presse, bevor es jemand anders sagt? Und wer unterschreibt die Meldung ans BSI?

Diese Entscheidungen sind unter Zeitdruck emotional, nicht analytisch. Wer sie zum ersten Mal im echten Vorfall trifft, trifft sie schlecht — nicht aus Inkompetenz, sondern weil ihm die Erfahrung fehlt, wie sich diese Art von Druck anfühlt. Die Übung liefert genau diese Erfahrung zum Preis von 90 Minuten Kalenderzeit. Wie du das Thema so aufbereitest, dass diese 90 Minuten überhaupt genehmigt werden, steht im Beitrag [Security-Reporting für die Geschäftsführung](#).

WARNUNG — Der Satz, der die Übung schon vorher zerstört

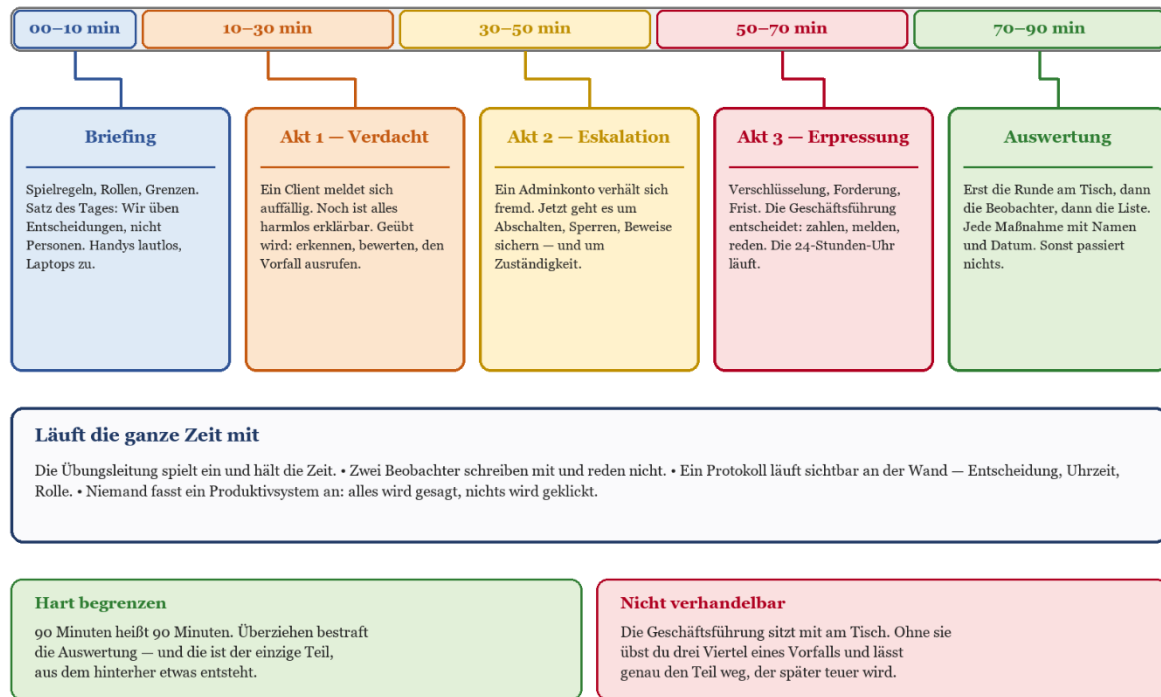
„Wir laden die Geschäftsführung ein, damit sie mal sieht, was wir hier leisten.“ Sobald die Übung als Leistungsschau geplant wird, wird sie eine. Dann werden die Einspielungen weichgespült, die Antworten vorher abgesprochen, und am Ende steht ein Ergebnis, das niemandem nützt.

Die Ansage vor der Übung lautet stattdessen: Wir üben, damit die Fehler heute passieren und nicht im August. Wer heute keinen Fehler macht, hat nichts gelernt. Und wer den Fehler eines anderen später im Flur erwähnt, fliegt bei der nächsten Übung raus.

Das Drehbuch: 90 Minuten in fünf Blöcken

Neunzig Minuten sind kein Zufallswert. Sie passen in einen normalen Kalender, sie überstehen einen Nachmittag ohne Verpflegung, und sie sind kurz genug, dass die Geschäftsführung zusagt. Wichtig ist die Aufteilung: Drei Akte zu je zwanzig Minuten, davor zehn Minuten Briefing, danach zwanzig Minuten Auswertung. Die Auswertung ist nicht der Rest, der übrig bleibt — sie ist der einzige Teil, aus dem hinterher etwas entsteht. Wer die Akte überzieht und die Auswertung streicht, hat eine unterhaltsame Diskussionsrunde veranstaltet und sonst nichts.

90 Minuten Feuerwehrübung – der Ablauf am Stück



Skizze 1: Der 90-Minuten-Ablauf. Die Zeitanteile sind die Botschaft – die Auswertung ist genauso lang wie ein ganzer Akt.

Zwei Wochen vorher: die Vorbereitung

Die Übung selbst dauert 90 Minuten. Die Vorbereitung dauert etwa vier bis sechs Stunden, verteilt über zwei Wochen, und die investiert im Wesentlichen eine Person: die Übungsleitung. Das ist ehrlicher, als so zu tun, als sei das Format aufwandsfrei. Es ist trotzdem das günstigste Format, das du bekommen kannst.

Zeitpunkt	Was passiert	Wer macht es	Ergebnis
T minus 14 Tage	Termin setzen, Teilnehmerkreis festlegen, Zusage der Geschäftsführung einholen	Übungsleitung	Kalendereintrag mit Raum, 90 Minuten, kein Videocall nebenher
T minus 10 Tage	Szenario auswählen und auf das eigene Haus anpassen: echte Systemnamen, echte Abteilungen	Übungsleitung mit IT-Betrieb	Szenariotext, eine halbe Seite
T minus 7 Tage	Sechs Einspielungen ausformulieren, Kanäle festlegen, Beobachtungspunkte definieren	Übungsleitung	Sechs Karten, ausgedruckt
T minus 5 Tage	Zwei Beobachter briefen, Beobachtungsbogen aushändigen	Übungsleitung	Zwei Personen, die wissen, dass sie schweigen sollen
T minus 2 Tage	Aktuellen Stand des Notfallplans ausdrucken und in den Raum legen – ohne Ankündigung	Übungsleitung	Der Plan liegt da. Ob ihn jemand nimmt, ist ein Befund
Tag der Übung	90 Minuten spielen, Protokoll sichtbar an der Wand mitschreiben lassen	Alle	Rohbeobachtungen, Protokoll, erste Maßnahmenideen
T plus 3 Tage	Beobachtungen verdichten, Maßnahmenliste finalisieren, an alle verteilen	Übungsleitung	Fünf bis sieben Maßnahmen mit Namen und Termin

T plus 42 Tage	Nachverfolgungstermin, 30 Minuten, dieselbe Runde	Übungsleitung	Erledigt oder nicht erledigt. Nichts dazwischen
-----------------------	---	---------------	---

Der Vorbereitungsplan. Die letzte Zeile ist die, die am häufigsten fehlt — und die einzige, die aus einer Übung eine Verbesserung macht.

Der Minutenplan

Der folgende Plan ist erprobt und lässt sich unverändert übernehmen. Die Angaben sind Minuten ab Übungsbeginn. Halte sie ein — notfalls schneidest du eine Diskussion mitten im Satz ab. Genau das passiert im Ernstfall auch, nur dass dort niemand höflich fragt.

Minute	Block	Was geschieht	Worauf die Beobachter achten
00–10	Briefing	Spielregeln, Rollen verteilen, Grenzen ansagen: Es wird nichts geklickt, niemand wird bewertet, alles wird ausgesprochen. Szenariolage in vier Sätzen vorlesen.	Fragt jemand nach dem Notfallplan? Weiß jeder, welche Rolle er hat?
10–30	Akt 1: Verdacht	Einspielung 1 und 2. Ein Client verhält sich seltsam, ein Ticket kommt herein. Nichts ist eindeutig. Das Team muss bewerten und entscheiden, ob es einen Vorfall ausruft.	Wie lange bis zur Einstufung? Wer darf einstufen? Wird jemand alarmiert?
30–50	Akt 2: Eskalation	Einspielung 3 und 4. Ein Adminkonto ist auffällig, ein Tunnel läuft seit Stunden. Jetzt geht es um Sperren, Trennen, Beweise sichern — und um die Frage, wer das darf.	Wird gesperrt oder erst diskutiert? Sichert jemand Protokolle, bevor aufgeräumt wird?
50–70	Akt 3: Erpressung	Einspielung 5 und 6. Verschlüsselung läuft, die Forderung kommt per Mail an die Geschäftsführung, eine Redaktion ruft an. Die 24-Stunden-Frist beginnt.	Wer entscheidet über Zahlung? Wer meldet? Wer redet? Läuft eine Uhr mit?
70–90	Auswertung	Erst die Runde: drei Fragen an jede Person. Dann die Beobachter. Dann die Maßnahmenliste, live an der Wand, mit Namen und Datum.	Die Beobachter reden jetzt zum ersten Mal — und zwar zu Sachverhalten, nicht zu Personen.

Der Minutenplan. Ausdrucken, auf den Tisch legen, sichtbar mitlaufen lassen.

TIPP — Die Uhr an der Wand

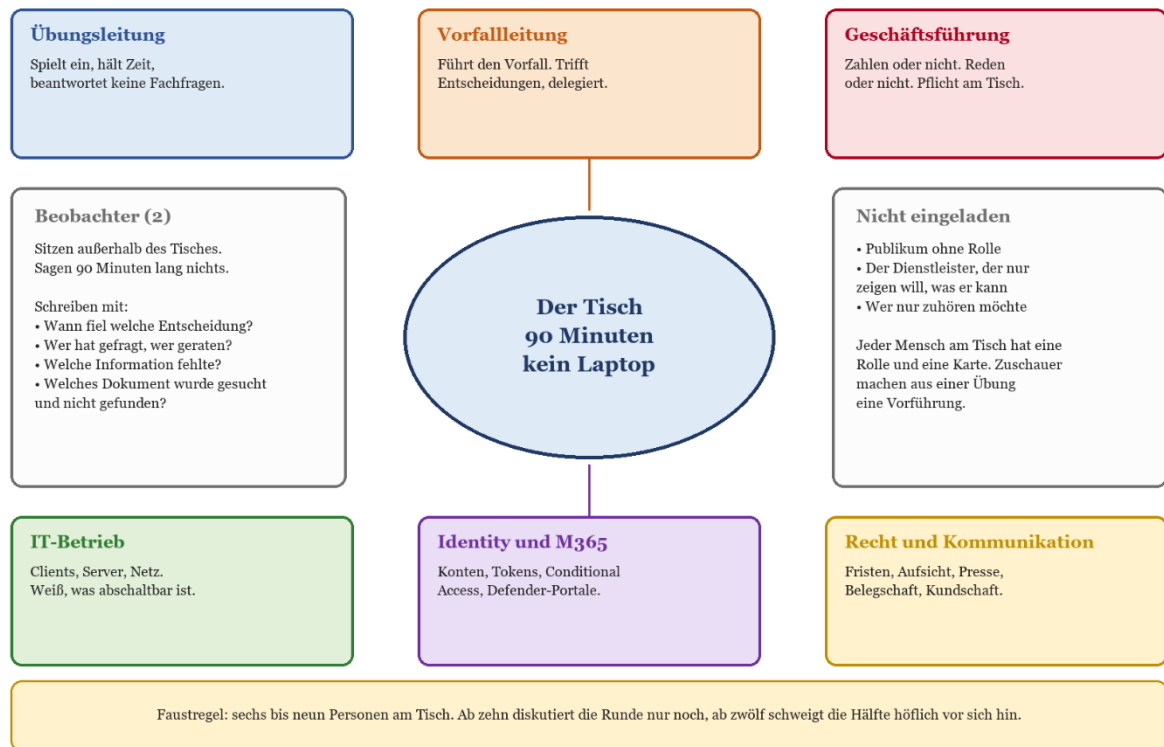
Projiziere eine große Uhr oder einen laufenden Zähler an die Wand — nicht die Uhrzeit, sondern die Zeit seit dem ersten Alarm im Szenario. Nichts erzeugt so zuverlässig echtes Vorfallgefühl wie eine Zahl, die hochläuft, während die Runde noch über Zuständigkeiten diskutiert.

In Akt 3 stellst du die Uhr auf die 24-Stunden-Frist der Frühwarnung um und lässt sie rückwärts laufen. Der Effekt auf die Diskussionsdisziplin ist erstaunlich.

Rollen am Tisch: sechs bis neun Personen, keine Zuschauer

Die Besetzung entscheidet über den Wert der Übung. Zu klein, und es fehlen die Perspektiven, an denen es im Ernstfall hakt. Zu groß, und die Runde wird zur Podiumsdiskussion. Sechs bis neun Personen am Tisch, zwei Beobachter daneben, eine Übungsleitung davor — das ist die Konfiguration, die in mittelständischen Häusern funktioniert.

Wer am Tisch sitzt — und wer bewusst danebensitzt



Skizze 2: Die Sitzordnung. Die Beobachter sitzen bewusst außerhalb des Tisches — sichtbar, aber nicht beteiligt.

Rolle	Auftrag in der Übung	Typischer Fehler, den die Übung sichtbar macht
Vorfalleitung	Führt den Vorfall, trifft und dokumentiert Entscheidungen, delegiert, hält die Lage zusammen	Löst selbst technische Probleme statt zu führen — und niemand hat mehr den Überblick
Geschäftsführung	Entscheidet über Zahlung, Abschaltung, externe Kommunikation, Einbindung von Behörden und Versicherung	Fragt nach technischen Details statt nach Auswirkungen und Optionen und bremst damit die Runde aus
IT-Betrieb	Kennt Clients, Server, Netze und Abhängigkeiten. Sagt, was abschaltbar ist und was daran hängt	Sagt „das geht nicht“, ohne zu sagen, was stattdessen geht
Identity und Microsoft 365	Konten, Rollen, Tokens, Conditional Access, Defender- und Purview-Portale	Weiß nicht auswendig, wo Sitzungen widerrufen werden — und sucht dann live in der Dokumentation
Recht und Datenschutz	Meldefristen, Aufsichtsbehörden, Betroffenenrechte, Beweissicherung, Versicherung	Ist gar nicht eingeladen. Und die 72-Stunden-Frist fällt erst in der Auswertung jemandem ein
Kommunikation	Interne und externe Sprachregelung, Presse, Kundschaft, Lieferanten, Belegschaft	Wartet auf vollständige Informationen, die es in den ersten Stunden grundsätzlich nicht gibt
Betriebsrat (optional)	Beobachtet, wo Beschäftigtendaten berührt werden, und bringt diese Sicht früh ein	Wird erst im echten Vorfall dazugeholt — und blockiert dann zu Recht die naheliegende Auswertung
Übungsleitung	Spielt ein, hält die Zeit, beantwortet Rückfragen zur Lage, aber nie zur Fachfrage	Hilft aus Mitleid, wenn die Runde feststeckt — und macht damit den Befund unsichtbar

Rollenkarten. Eine Zeile pro Person, ausgedruckt, vor den Platz gelegt.

Die Übungsleitung: unbeliebt und unverzichtbar

Die Übungsleitung spielt nicht mit. Das ist die schwerste Disziplin, besonders wenn sie ohnehin die Person ist, die den Notfallplan geschrieben hat. Sie kennt jede Antwort, sieht jeden Fehler und darf keinen einzigen korrigieren. Sie sagt Sätze wie „Das entscheidet ihr“ und „Ich weiß es nicht, was macht ihr jetzt?“ und hält Pausen aus, in denen niemand redet. Die peinliche Stille nach einer Einspielung, auf die keiner reagiert, ist der wertvollste Befund des ganzen Nachmittags.

Wenn du diese Disziplin intern nicht aufbringen kannst — weil die einzige Person mit dem nötigen Überblick zwingend fachlich mitspielen muss —, hol die Übungsleitung von außen. Genau dafür gibt es die [Microsoft 365 Security Beratung](#): Ein externer Kopf schreibt die Einspielungen, hält die Zeit und spricht die unangenehmen Befunde aus, ohne am Montag danach wieder neben den Beteiligten zu sitzen.

Beobachter: die eigentliche Messtechnik

Zwei Personen, die 90 Minuten lang nichts sagen und alles mitschreiben. Sie sind keine Prüfer und vergeben keine Noten. Sie protokollieren Beobachtungen mit Zeitstempel, und zwar entlang von vier festen Fragen, die auf ihrem Bogen stehen:

- Wann fiel welche Entscheidung — und wer hat sie getroffen? Wenn niemand sie getroffen hat, sondern sie sich irgendwie ergeben hat, ist genau das die Beobachtung.
- Welche Information wurde gesucht und nicht gefunden? Telefonnummern, Vertragsnummern, Ansprechpartner beim Dienstleister, Lizenzstand, Netzpläne.
- Welches Dokument wurde geöffnet — und welches lag da, ohne dass es jemand anfasste?
- Wo hat die Runde eine Annahme getroffen, statt nachzufragen? Annahmen unter Druck sind die häufigste Fehlerquelle und in der Auswertung besonders lehrreich.

Verteile die beiden Beobachter thematisch: Eine Person beobachtet Technik und Ablauf, die andere Kommunikation und Entscheidung. Sonst schreiben beide dasselbe mit und übersehen dasselbe.

WICHTIG — Beobachten heißt nicht bewerten

Der Beobachtungsbogen enthält keine Namen. Er enthält Rollen. „Die Vorfallleitung fragte um Minute 41 zum ersten Mal nach dem Notfallplan“ ist ein Befund. „Frau M. hat den Plan nicht gekannt“ ist eine Personalangelegenheit — und die zerstört dir jede weitere Übung im Haus.

Diese Regel sagst du im Briefing laut an. Und du hältst dich in der Auswertung sichtbar daran, auch wenn alle wissen, wer gemeint ist.

Einspielungen: der Motor der ganzen Veranstaltung

Ohne Einspielungen ist eine Tabletop-Übung ein Meeting. Die Einspielung — international Inject — ist die Nachricht, die von außen in die Runde platzt und die Lage verändert. Sechs Stück reichen für 90 Minuten, zwei pro Akt. Mehr wird hektisch, weniger wird zäh.

Anatomie einer Einspielung

Jede Einspielung wird vorher ausgeschrieben. Improvisieren wirkt souverän und ist unfair: Eine spontan erfundene Wendung, die die Runde nicht auflösen kann, produziert Frust statt Erkenntnis. Fünf Felder pro Karte, mehr braucht es nicht.

Anatomie einer Einspielung — die Karte, die du vorher schreibst

Zeitpunkt Minute 34 — nicht „irgendwann in Akt 2“. Sonst schiebt die Übungsleitung im Eifer. Kanal Wie kommt es rein? Ticket, Telefon, Mail, Alarm, Nachricht der Geschäftsführung. Wortlaut Ausformuliert, vorgelesen oder ausgedruckt. Improvisierte Einspielungen sind unfair. Erwartete Reaktion Was ein gut aufgestelltes Team jetzt täte. Nur für die Übungsleitung sichtbar. Beobachtungspunkt Die eine Frage, die die Beobachter hier beantworten sollen.	Ausgefüllt: Einspielung 3 von 6 Zeitpunkt Minute 52, Akt 2 Kanal Telefon — Übungsleitung ruft die Vorfälleleitung direkt an Wortlaut „Hier ist der Bereitschaftsdienst. Unser Adminkonto adm-mfischer hat heute Nacht um 3:14 Uhr von einem Gerät angemeldet, das nicht im Bestand steht. MFA hat bestätigt. Danach wurde ein Postfach exportiert. Was machen wir?“ Erwartete Reaktion Konto sperren, Sitzungen widerrufen, Refresh-Tokens zurückziehen, Exportauftrag prüfen, Audit-Log sichern — und die Geschäftsführung informieren, nicht erst nachher. Beobachtungspunkt Wie lange dauert es vom Anruf bis zur Entscheidung? Und wer trifft sie?
--	---

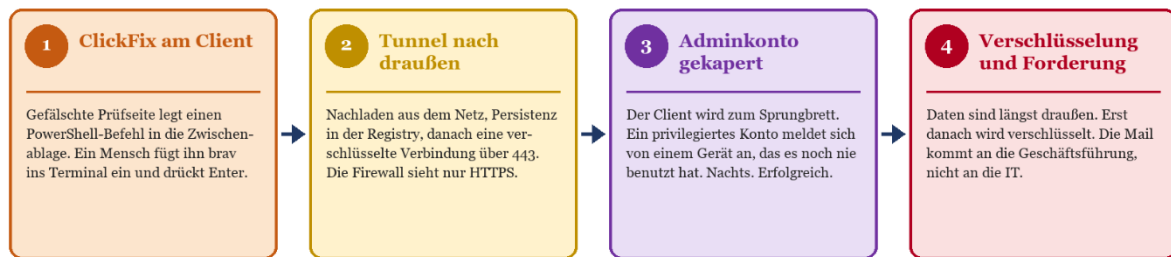
Skizze 3: Der Aufbau einer Einspielungskarte — links das Schema, rechts eine vollständig ausgefüllte Karte aus dem Leitszenario.

Das wichtigste Feld ist der Kanal. Im echten Vorfall kommt Information nie über einen einzigen Weg herein, sondern über fünf gleichzeitig, von denen drei sich widersprechen. Ein Team, das nur geübt hat, auf ein Dashboard zu schauen, ist blind für den Anruf aus der Produktion und die Mail an die Geschäftsführung. Verteile deine sechs Einspielungen deshalb bewusst: Ticket, Alarm, Telefon, Mail, Nachricht aus dem Fachbereich, Anruf von außen.

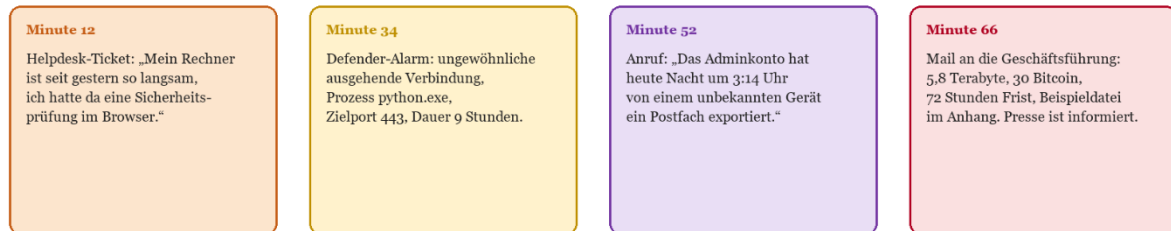
Das Leitszenario in vier Akten

Das Leitszenario dieses Beitrags folgt einer Kette, die 2026 in genau dieser Form gelaufen ist: ClickFix am Client, verschlüsselter Tunnel nach draußen, gekapertes Adminkonto, Verschlüsselung und Erpressung. Der Reiz dieser Kette liegt darin, dass jeder Schritt für sich harmlos aussieht und erst die Verkettung den Schaden ergibt — genau das ist die Erfahrung, die dein Team machen soll.

Das Leitszenario: vom Terminal-Tipp zur Erpressungsmail



Was du daraus als Einspielung machst



Der didaktische Trick

Jede Einspielung kommt über einen anderen Kanal: Ticket, Alarm, Anruf, Mail. Genau so passiert es im Ernstfall auch — und genau daran scheitern Teams, die nur den einen Kanal geübt haben, auf den sie ohnehin schauen.

Skizze 4: Die Angriffskette des Leitszenarios und die Einspielungen, die daraus entstehen. Jede kommt über einen anderen Kanal.

Die technischen Details dieser Kette — die gefälschte Prüfseite, das Nachladen über PowerShell, die signierte Programmdatei, die eine fremde Bibliothek aus demselben Verzeichnis lädt, der Tunnel über Port 443 — sind im [Dossier TerminalFix und der Berlin-Hack](#) nachgezeichnet. Dieses Dossier ist gleichzeitig die beste Szenario-Vorlage, die du in die Hand nehmen kannst: Es enthält eine echte Zeitleiste mit echten Datumsangaben, echte Zahlen und ein Ende, das nicht ausgedacht ist. Nimm die dortige Abfolge, ersetze die Berliner Systemnamen durch deine eigenen, und du hast in einer Stunde ein Szenario, dem niemand am Tisch vorwerfen kann, es sei übertrieben.

Min.	Kanal	Einspielung (Wortlaut, gekürzt)	Beobachtungspunkt
12	Ticket	„Mein Rechner ist seit gestern extrem langsam. Ich hatte eine Sicherheitsprüfung im Browser, da musste ich etwas ins Terminal einfügen, damit die Seite lädt.“	Erkennt jemand das Muster? Oder wird das Ticket als Leistungsproblem eingeordnet und weitergereicht?
24	Alarm	Defender for Endpoint meldet: ungewöhnlicher übergeordneter Prozess, Skriptausführung aus C:\ProgramData, mittlerer Schweregrad, seit 19 Stunden offen.	Wird der Alarm mit dem Ticket verknüpft? Wer schaut überhaupt in das Portal?
34	Telefon	Der Netzbetrieb ruft an: Ein Client baut seit neun Stunden eine dauerhafte verschlüsselte Verbindung zu einer unbekannten Adresse auf. Port 443, unauffälliges Protokoll.	Wird jetzt der Vorfall ausgerufen? Wird der Client getrennt — und wer entscheidet das?
52	Telefon	Die Bereitschaft meldet: Das Adminkonto adm-mfischer hat nachts um 3:14 Uhr von einem unbekannten Gerät angemeldet, MFA bestätigt, danach ein Postfach exportiert.	Sperren oder beobachten? Werden Sitzungen und Tokens widerrufen? Wird das Audit-Log gesichert?

62	Mail an die Geschäftsführung	„Wir haben 5,8 Terabyte Ihrer Daten. 30 Bitcoin binnen 72 Stunden, sonst Veröffentlichung. Anbei drei Beispieldateien aus Ihrer Personalabteilung.“	Wer liest die Mail zuerst? Wird sie an die IT weitergeleitet — und wird sie vorher gesichert?
70	Anruf von außen	Eine Redaktion fragt an: „Uns liegen Daten aus Ihrem Haus vor. Nehmen Sie dazu Stellung? Wir gehen in zwei Stunden online.“	Gibt es eine Sprachregelung? Wer darf reden? Läuft parallel die 24-Stunden-Frist mit?

Die sechs Einspielungen des Leitszenarios. Vollständige Wortlaute passen auf sechs Karten im Format DIN A6.

Die Reaktion auf die Einspielung aus Minute 52 ist der fachliche Kern des Ganzen. Was mit einem verdächtigen privilegierten Konto konkret zu tun ist — sperren, Sitzungen widerrufen, Refresh-Tokens zurückziehen, Postfachregeln prüfen, App-Zustimmungen kontrollieren —, steht Schritt für Schritt im Beitrag [Kompromittiertes Konto erkennen und aufräumen](#). Wenn dein Team an dieser Stelle ins Stocken gerät, hast du bereits die erste Maßnahme deiner Liste gefunden.

WARNUNG — Vier Einspielungen, die deine Übung ruinieren

Die unlösbare: „Das gesamte Rechenzentrum steht in Flammen.“ Beeindruckend, aber es gibt keine Entscheidung zu treffen — also lernt niemand etwas.

Die technische Detailfrage: „Welchen Befehl gibst du jetzt in der PowerShell ein?“ Das ist ein Wissenstest, keine Übung. Prüfe Wissen in einer Schulung, nicht am Tisch.

Die unfaire Wendung: eine Information, die es im Haus schlicht nicht gibt und die die Übungsleitung sich ausgedacht hat, um clever zu wirken.

Die Rettung von außen: „Der Dienstleister meldet, er habe das Problem schon behoben.“ Nichts beendet eine Diskussion so gründlich und so nutzlos.

Drei fertige Szenarien zum sofortigen Spielen

Die folgenden drei Szenarien sind vollständig und einsatzfähig. Ersetze die Platzhalter durch deine eigenen System- und Abteilungsnamen — das dauert eine Viertelstunde und verdoppelt die Wirkung, weil niemand mehr sagen kann, das sei ja alles theoretisch. Spiele eines pro Halbjahr. Nach drei Durchläufen kennt dein Team das Format gut genug, dass du zur Stabsübung hochschalten kannst.

SZENARIO A — Der freundliche Terminal-Tipp (Einstiegsniveau, 90 Minuten)

Lage: Eine Person aus dem Vertrieb hat gestern eine Website besucht, auf der eine Prüfseite erschien. Um fortzufahren, sollte sie eine Tastenkombination drücken und einen Befehl einfügen. Sie hat es getan, die Seite lud, und der Termin war wichtig. Heute ist der Rechner langsam.

Verlauf: Ticket beim Helpdesk (Min. 12) — Endpoint-Alarm mittleren Schweregrads (Min. 24) — Dauerverbindung nach außen (Min. 34) — der Client hat nachts auf drei Dateiserver zugegriffen (Min. 48) — ein zweiter Rechner in derselben Abteilung zeigt dasselbe Muster (Min. 58) — die Geschäftsführung fragt, ob man die Abteilung heute noch arbeiten lassen kann (Min. 66).

Lernziele: Erkennen eines Musters aus zwei für sich harmlosen Meldungen. Wer ruft den Vorfall aus? Wer darf einen Client trennen? Wie viel Ausfall darf eine Vorsichtsmaßnahme kosten?

Fallstrick für die Übungsleitung: Die Runde will sofort alles abschalten. Frage dann ruhig nach, was das für die Auslieferung morgen bedeutet — und wer diese Entscheidung trägt.

SZENARIO B — Der Admin, der nicht mehr dir gehört (mittleres Niveau, 90 Minuten)

Lage: Ein privilegiertes Konto hat sich nachts um 3:14 Uhr erfolgreich angemeldet. Die Multifaktor-Anmeldung wurde bestätigt. Das Gerät steht nicht im Bestand. Die Person, der das Konto gehört, hat

Urlaub und ist nicht erreichbar.

Verlauf: Anruf der Bereitschaft (Min. 10) — ein Postfach der Geschäftsführung wurde exportiert (Min. 20) — eine neue Anwendung mit weitreichender Zustimmung wurde im Tenant registriert (Min. 32) — eine Weiterleitungsregel schickt Rechnungsmails an eine externe Adresse (Min. 44) — die Buchhaltung meldet eine geänderte Bankverbindung bei einem Lieferanten (Min. 56) — ein zweites Adminkonto zeigt dasselbe Verhalten (Min. 68).

Lernziele: Reihenfolge beim Aufräumen. Sperren zerstört Spuren, Beobachten kostet Zeit — wer entscheidet? Wann wird das Break-Glass-Konto gezogen? Wie erkennt man, ob weitere Konten betroffen sind, bevor man alles zurücksetzt?

Fallstrick für die Übungsleitung: Wenn jemand vorschlägt, einfach alle Kennwörter zurückzusetzen, frage nach, wie viele Konten das sind, wer das nachts macht und was mit den Dienstkonten passiert.

SZENARIO C — Freitag, 16:40 Uhr — die Erpressung (Vollniveau, 90 Minuten)

Lage: Freitagnachmittag. Zwei Dateiserver antworten nicht mehr. Der Rest des Hauses arbeitet normal. Die Geschäftsführung wollte um 17 Uhr los.

Verlauf: Server nicht erreichbar (Min. 08) — Dateien tragen eine unbekannte Endung, ein Textdokument liegt in jedem Ordner (Min. 16) — Erpressungsmail an die Geschäftsführung mit Beispieldateien aus der Personalabteilung (Min. 28) — die Sicherungslösung meldet, dass die letzten drei Sicherungsläufe fehlgeschlagen sind (Min. 40) — eine Redaktion ruft an (Min. 52) — die Versicherung fragt nach dem Vorfallprotokoll, das es bislang nicht gibt (Min. 62) — ein Großkunde fragt, ob seine Daten betroffen sind (Min. 72).

Lernziele: Zahlen oder nicht. Meldung binnen 24 Stunden an das BSI, Datenschutzmeldung binnen 72 Stunden, beides parallel zur technischen Arbeit. Wer schreibt das Protokoll, während alle arbeiten? Und wer sagt der Belegschaft am Montag früh, was Sache ist?

Fallstrick für die Übungsleitung: Lass die Frage nach der Zahlung nicht abstrakt bleiben. Nenne eine konkrete Summe, eine konkrete Frist und frage die Geschäftsführung direkt: „Sie haben jetzt zwei Minuten. Wie lautet Ihre Entscheidung?“

Zwei Hinweise zu den Szenarien. Erstens: Sie bauen aufeinander auf. Szenario A endet dort, wo Szenario B beginnt, und Szenario B endet dort, wo Szenario C beginnt. Wenn du sie in dieser Reihenfolge über drei Halbjahre spielst, hat dein Team am Ende eine vollständige Angriffskette durchlebt, ohne je mehr als 90 Minuten am Stück investiert zu haben.

Zweitens: Sie setzen unterschiedliche Vorarbeit voraus. Szenario A funktioniert ohne alles. Szenario B wird deutlich ergiebiger, wenn ihr wisst, wie eure Anmeldeprotokolle aussehen — siehe [Alert Policies und Benachrichtigungen richtig aufsetzen](#) und [Defender for Identity: das Active Directory im Blick](#). Szenario C braucht ehrliche Antworten zur Sicherung, und die findest du im Beitrag [Ransomware-Vorsorge in Microsoft 365](#), bevor du übst. Sonst besteht die halbe Übung aus der Feststellung, dass es niemand genau weiß — was zwar auch ein Ergebnis ist, aber eines, das du deutlich billiger haben kannst.

TIPP — Das Berlin-Dossier als Szenario-Vorlage

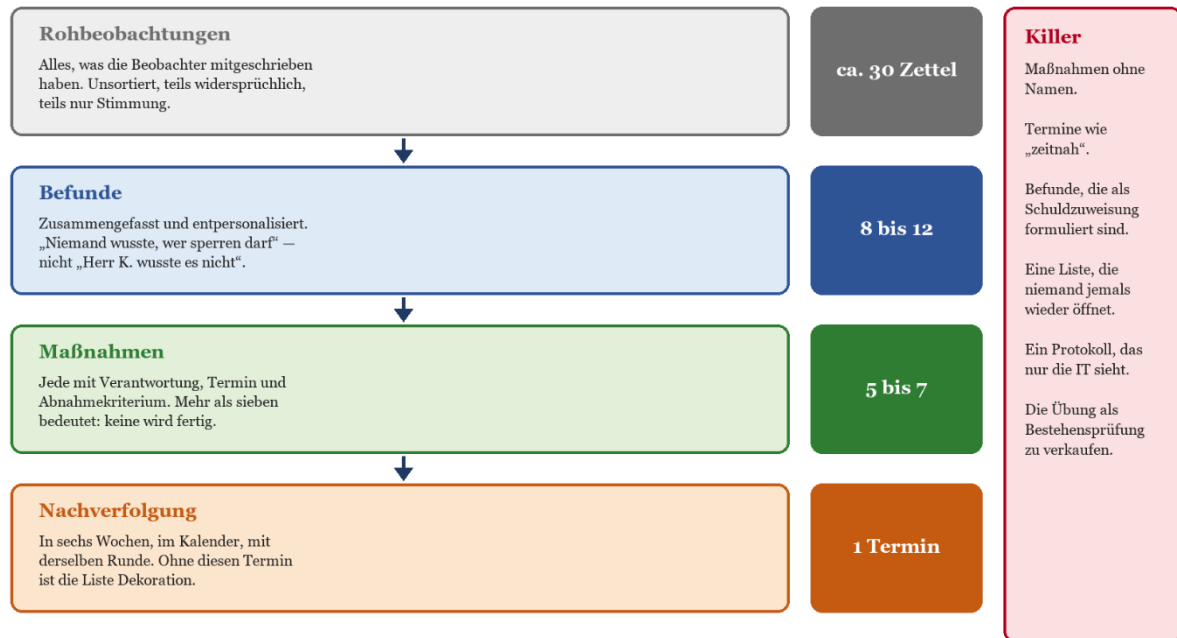
Wenn du ein viertes Szenario brauchst oder eines mit maximaler Glaubwürdigkeit: Nimm das [Dossier TerminalFix und der Berlin-Hack](#). Dort steht eine dokumentierte Zeitleiste — Zugriff ab dem 7. August, Entdeckung am 14. August, öffentliche Bestätigung am 28. August, Veröffentlichung der Daten am 4. September.

Setze diese Zeitleiste in dein Haus. Frage an jeder Station: Hätten wir das hier bemerkt? Womit? Wer hätte es gesehen? Und was hätten wir in den sieben Tagen dazwischen getan? Diese Variante braucht keine erfundenen Einspielungen — die Realität hat sie geliefert.

Auswertung: aus 30 Zetteln werden fünf Maßnahmen

Hier entscheidet sich, ob die Übung etwas wert war. Zwanzig Minuten heiße Auswertung direkt im Anschluss, solange alle noch im Raum und noch aufgedreht sind. Danach zwei Stunden stille Arbeit der Übungsleitung. Und dann eine Liste, die kurz genug ist, um abgearbeitet zu werden.

Die Auswertung: vom Zettel zur Maßnahme mit Namen



Skizze 5: Der Trichter von der Rohbeobachtung zur nachverfolgten Maßnahme. Die Zahlen rechts sind Erfahrungswerte, keine Zielvorgaben — aber sie stimmen erstaunlich oft.

Die heiße Auswertung: drei Fragen, eine Runde

Reihum, jede Person am Tisch, maximal zwei Minuten. Drei Fragen, immer dieselben, immer in dieser Reihenfolge:

- Was hat funktioniert? Zuerst, und nicht als Höflichkeitsfloskel. Was gut lief, willst du wissen und behalten — und es senkt die Abwehrhaltung für die nächste Frage.
- Wo hast du dich unsicher gefühlt? Nicht „wo war ein Fehler“, sondern „wo warst du unsicher“. Unsicherheit lässt sich zugeben, ein Fehler nicht.
- Was hätte dir in diesem Moment geholfen? Das ist die Frage, aus der die Maßnahmen entstehen. Die Antworten sind meistens erschreckend banal: eine aktuelle Telefonliste, ein Blatt mit Zuständigkeiten, ein Klickpfad, eine Freigabe im Voraus.

Erst danach reden die Beobachter. Sie tragen Beobachtungen vor, keine Bewertungen, und sie beginnen mit Zeitangaben: „Um Minute 34 lag der Alarm vor, die Entscheidung fiel um Minute 51.“ Die Runde interpretiert selbst. Sie tut das erfahrungsgemäß härter und ehrlicher, als jeder Beobachter es dürfte.

Die Maßnahmenliste, die überlebt

Fünf bis sieben Maßnahmen. Mehr sind eine Wunschliste. Jede bekommt vier Angaben, sonst zählt sie nicht: eine Person, einen Termin, ein Abnahmekriterium und einen Aufwand. Die Liste entsteht live an der Wand, damit niemand hinterher überrascht ist, seinen Namen darauf zu finden.

Befund aus der Übung	Maßnahme	Abnahmekriterium	Frist
Niemand wusste, wer ein Adminkonto sperren darf	Ein Blatt „Wer darf was sofort“, unterschrieben von der Geschäftsführung, im Notfallplan	Blatt liegt vor, unterschrieben, im Plan verlinkt	2 Wochen
Die Erpressungsmail wurde vor der Sicherung weitergeleitet	Kurzanweisung zur Beweissicherung bei verdächtigen Mails, auf einer Seite	Anweisung liegt vor und wurde in einer Teamrunde vorgestellt	3 Wochen
Die Telefonliste war zwei Jahre alt und lag nur digital vor	Alarmierungsliste aktualisieren, ausdrucken, an drei Orten hinterlegen	Drei Ausdrücke vorhanden, Stichprobe zeigt korrekte Nummern	1 Woche
Sitzungen und Tokens widerrufen fand niemand auf Anhieb	Klickpfad als Playbook mit Bildern, verlinkt aus dem Notfallplan	Zwei Personen führen den Pfad im Testtenant ohne Hilfe aus	4 Wochen
Die 24-Stunden-Frist war der Runde nicht präsent	Fristenübersicht auf eine Seite, Bestandteil des Notfallplans, mit Zuständigkeit je Frist	Übersicht vorhanden, in der nächsten Übung zieht sie jemand heran	3 Wochen
Kein Protokoll während der Übung, alles aus dem Gedächtnis	Protokollvorlage anlegen, Rolle „Protokoll“ fest im Plan verankern	Vorlage existiert, Rolle ist benannt und vertreten	2 Wochen

Eine echte Maßnahmenliste nach einer ersten Übung. Auffällig: keine einzige Maßnahme kostet Lizenzgeld. Das ist der Normalfall.

Fällt dir etwas auf? Keine dieser Maßnahmen ist ein Produkt. Es sind Blätter, Listen, Klickpfade und Unterschriften. Genau das ist das typische Ergebnis einer ersten Tabletop-Übung, und es ist auch die beste Nachricht für dein Budget: Der Großteil dessen, was im Ernstfall Zeit kostet, lässt sich mit Papier und Klarheit beheben. Erst die zweite oder dritte Übung fördert Befunde zutage, für die du wirklich Technik brauchst — dann meist in Richtung Erkennung, siehe [Microsoft Sentinel anbinden: wann es sich lohnt](#).

WICHTIG — Der Termin in sechs Wochen ist Teil der Übung

Setze den Nachverfolgungstermin, bevor alle den Raum verlassen. Dreißig Minuten, dieselbe Runde, sechs Wochen später. Pro Maßnahme genau zwei Zustände: erledigt oder nicht erledigt. Kein „in Arbeit“, kein „zu 80 Prozent“.

Ohne diesen Termin liegt die Erledigungsquote nach meiner Erfahrung bei etwa einem Drittel. Mit ihm bei über achtzig Prozent. Der Unterschied besteht aus dreißig Minuten Kalenderzeit — das ist das beste Verhältnis von Aufwand zu Wirkung in diesem gesamten Beitrag.

Häufige Fragen zur Tabletop-Übung

Wie oft sollten wir üben?

Mindestens einmal im Jahr, besser halbjährlich. Zusätzlich immer dann, wenn sich etwas Wesentliches ändert: neue Vorfallleitung, neue Geschäftsführung, größere Umstellung in der IT, neuer Dienstleister. Das erste Jahr würde ich mit drei Übungen planen — die erste deckt so viel auf, dass eine Wiederholung nach vier Monaten sich lohnt, allein um zu sehen, ob die Maßnahmen tatsächlich gewirkt haben.

Müssen wir dafür einen Notfallplan haben?

Streng genommen nein — du kannst auch ohne Plan üben und wirst dann sehr schnell feststellen, dass du einen brauchst. Das ist eine teure Art, zu dieser Erkenntnis zu kommen. Sinnvoller ist die Reihenfolge: erst einen schlanken Plan schreiben, wie im Beitrag [Incident-Response-Plan für](#)

[Microsoft 365](#) beschrieben, dann üben, dann den Plan anhand der Befunde korrigieren. Die Übung ist das Prüfverfahren für den Plan, nicht sein Ersatz.

Was, wenn die Geschäftsführung keine Zeit hat?

Dann verschiebe die Übung, statt sie ohne Geschäftsführung durchzuziehen. Das klingt kompromisslos und ist es auch. Eine Übung ohne die Ebene, die über Zahlung, Abschaltung und Kommunikation entscheidet, übt genau die Fragen nicht, die im Ernstfall den größten Schaden anrichten. Wenn das Terminproblem chronisch ist, ist es kein Terminproblem, sondern ein Bewusstseinsproblem — und das löst du über die Aufbereitung, siehe [Security-Reporting für die Geschäftsführung](#).

Braucht es dafür externe Unterstützung?

Nicht zwingend. Der Aufwand liegt bei vier bis sechs Stunden Vorbereitung, und das Material in diesem Beitrag ist bewusst so geschrieben, dass du es allein umsetzen kannst. Extern lohnt sich in zwei Fällen: wenn niemand im Haus die Rolle der Übungsleitung glaubwürdig ausfüllen kann, ohne fachlich mitzuspielen, und wenn die Befunde politisch heikel sind. Ein externer Mund sagt manche Sätze folgenloser. Beides deckt die [Microsoft 365 Security Beratung](#) ab.

Wie verhindern wir, dass die Übung in Schuldzuweisungen kippt?

Durch drei Regeln, die du im Briefing ansagst und dann konsequent durchhältst: Beobachtungen werden auf Rollen bezogen, nicht auf Namen. Was im Raum passiert, bleibt im Raum. Und die Auswertung beginnt mit dem, was funktioniert hat. Wenn du diese Regeln beim ersten Verstoß nicht durchsetzt — auch und gerade, wenn die Geschäftsführung den Verstoß begeht —, war es die letzte Übung, bei der jemand ehrlich geantwortet hat.

Ist das dasselbe wie eine Phishing-Simulation?

Nein, und die beiden ergänzen sich. Eine Phishing-Simulation misst das Verhalten vieler einzelner Personen am Posteingang und läuft als Dauerprogramm — wie du sie sauber aufsetzt, steht im Beitrag [Attack Simulation Training: Phishing-Übungen richtig aufsetzen](#). Eine Tabletop-Übung misst das Verhalten einer kleinen Gruppe unter Entscheidungsdruck und läuft als Einzeltermin. Die eine senkt die Wahrscheinlichkeit, dass es passiert. Die andere senkt den Schaden, wenn es doch passiert.

Müssen wir den Betriebsrat einbeziehen?

Für die Übung selbst in aller Regel nicht — es werden keine Beschäftigtendaten ausgewertet, es wird geredet. Interessant wird es, wenn aus der Übung Maßnahmen zur Überwachung entstehen, etwa eine bessere Auswertung von Anmeldeprotokollen. Dann greift die Mitbestimmung, und zwar früher, als viele denken. Die Abgrenzung erklärt der Beitrag [Security-Monitoring und Betriebsrat: was mitbestimmungspflichtig ist](#). Ein pragmatischer Weg: den Betriebsrat als Beobachter einladen. Er sieht, warum die Auswertung gebraucht wird, und die spätere Verhandlung wird deutlich kürzer.

Was dokumentieren wir für einen Prüfer?

Vier Dinge, und die entstehen ohnehin: die Einladung mit Teilnehmerkreis und Rollen, das Szenariodokument mit den Einspielungen, den Auswertungsbericht mit den Befunden und die Maßnahmenliste mit Verantwortung, Terminen und dokumentiertem Abschluss. Das genügt für ISO 27001, für den IT-Grundschutz und für die Nachweispflichten aus NIS2, deren technische

Seite der Beitrag [NIS2 aus Security-Sicht: technische Maßnahmen in M365](#) behandelt. Wichtig ist die letzte Spalte: Ein Prüfer interessiert sich weniger dafür, dass du geübt hast, als dafür, was du danach geändert hast.

Können wir das auch aus dem Homeoffice machen?

Es geht, aber es kostet etwa ein Drittel der Wirkung. Am Bildschirm fehlt die Körpersprache, die der Beobachtung ihre halbe Substanz gibt, und niemand spürt die Stille im Raum, wenn eine Einspielung unbeantwortet bleibt. Wenn es verteilt sein muss: Kameras an, keine Nebentätigkeiten, ein separater Kanal für die Einspielungen, und ein dritter Beobachter, weil zwei am Bildschirm weniger mitbekommen. Und plane 105 statt 90 Minuten ein.

Fazit

Die Feuerwehrübung funktioniert seit Jahrzehnten, weil sie drei Dinge richtig macht: Sie ist kurz, sie ist verpflichtend, und sie wird wiederholt, obwohl beim letzten Mal alles geklappt hat. Dieselben drei Eigenschaften machen eine Tabletop-Übung wertvoll. Neunzig Minuten, ein Termin im Kalender, ein festes Format, das dein Team beim dritten Mal so gut kennt, dass es sich auf den Inhalt konzentrieren kann statt auf die Methode.

Der Gewinn liegt nicht in der Übung selbst, sondern in ihren Nebenprodukten: einer aktuellen Telefonliste, einem unterschriebenen Blatt mit Befugnissen, einer Fristenübersicht, einem Klickpfad, den zwei Personen ohne Hilfe abarbeiten können. Lauter unspektakuläre Dinge, die im Ernstfall zwischen zwanzig Minuten und vier Stunden Unterschied machen. Und vier Stunden sind bei einer laufenden Verschlüsselung ein anderes Unternehmen.

Fang klein an. Nimm Szenario A, nimm sechs Personen, nimm einen Nachmittag im nächsten Monat. Setze den Nachverfolgungstermin gleich mit dazu. Und wenn dir jemand sagt, dafür sei gerade keine Zeit, dann rechne ihm die Alternative vor: In Berlin lagen zwischen dem ersten Zugriff und der Entdeckung sieben Tage und zwischen der Entdeckung und der öffentlichen Bestätigung vierzehn. Diese vierzehn Tage sind kein technisches Problem. Sie sind ein Übungsproblem — und Übungsprobleme kannst du an einem Nachmittag angehen.

WEITER — So geht es weiter in der Serie

- › Vorher lesen und schreiben: [Incident-Response-Plan für Microsoft 365](#)
- › Die Stufe darüber, wenn die Grundlagen sitzen: [Red-Team-Übung: der kontrollierte Angriff](#)
- › Fachliches Fundament für Szenario B: [Kompromittiertes Konto erkennen und aufräumen](#)
- › Fachliches Fundament für Szenario C: [Ransomware-Vorsorge in Microsoft 365](#)
- › Die ersten 60 Minuten im Detail: [Phishing-Vorfall: die ersten 60 Minuten](#)
- › Realer Fall als Szenario-Vorlage: [Dossier TerminalFix und der Berlin-Hack](#)
- › Wissen im Team aufbauen: [Schulung Microsoft 365 Security](#)
- › Begleitung bei Plan und Übung: [Microsoft 365 Security Beratung](#)