

Phishing-Vorfall: die ersten 60 Minuten

Es beginnt selten dramatisch. Kein Alarmton, kein rot blinkendes Dashboard, keine dunkle Gestalt mit Kapuze. Es beginnt damit, dass jemand aus der Buchhaltung um 9:47 Uhr im Teams-Chat schreibt: „Du, ich glaub, ich hab da was Falsches angeklickt.“ Und dann folgt diese kleine Pause, in der du merkst, dass dein Vormittag gerade eine andere Richtung genommen hat.

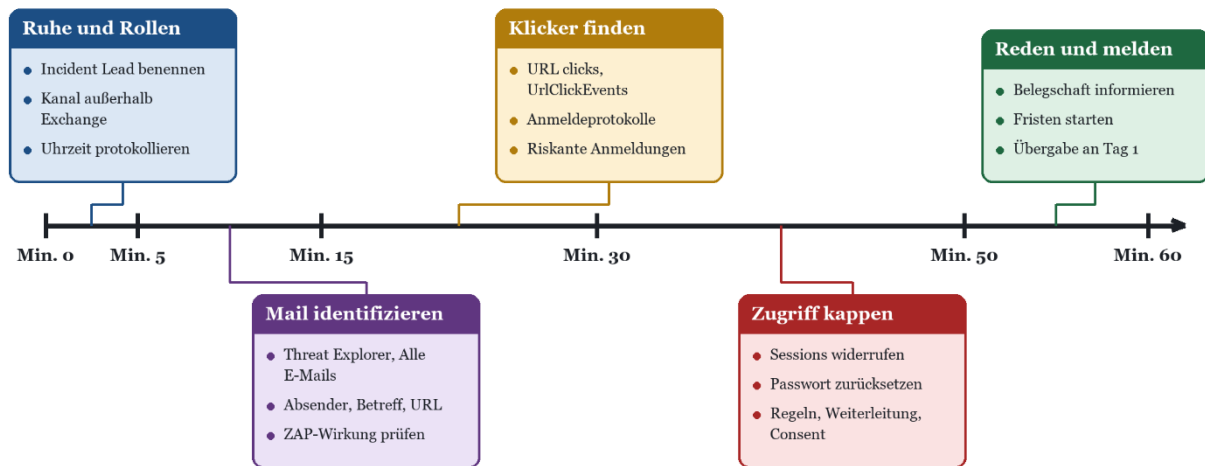
Genau hier entscheidet sich, ob aus einem Klick ein Ärgernis wird oder ein Vorfall mit Meldepflicht, Anwalt und Krisensitzung. Nicht die Technik entscheidet das, sondern die Reihenfolge deiner Handgriffe. Wer in Minute drei das Passwort zurücksetzt und in Minute vierzig merkt, dass die aktive Sitzung des Angreifers seitdem munter weiterlief, hat viel Arbeit investiert und wenig erreicht.

Dieser Beitrag ist deshalb kein Essay über Awareness. Er ist ein Playbook. Minute 0 bis Minute 60, in Schritten, mit den Werkzeugen, die in einem normalen Microsoft-365-Tenant tatsächlich vorhanden sind: Threat Explorer, Zero-hour auto purge, Safe-Links-Klickdaten, Anmeldeprotokolle, Postfachregeln, Consent-Grants. Am Ende weißt du, was du in welcher Minute anfasst — und was du bewusst liegen lässt, weil es in der ersten Stunde nichts verbessert.

Eine Warnung vorweg: Dieses Playbook funktioniert nur, wenn du es liest, bevor du es brauchst. Im Ernstfall liest niemand einen Fachartikel. Im Ernstfall folgt man dem, was man schon einmal geübt hat. Der Rest ist Improvisation mit Publikum.

Die ersten 60 Minuten nach der ersten Meldung

Reihenfolge ist kein Geschmack, sondern Schadensbegrenzung



Parallel laufen die Meldefristen: 24 Stunden Frühwarnung nach BSI, 72 Stunden nach Artikel 33 DSGVO.

Skizze 1: Der 60-Minuten-Zeitstrahl. Fünf Phasen, feste Reihenfolge, klare Übergaben.

WICHTIG — Was dieses Playbook voraussetzt

Es geht von einem Microsoft-365-Tenant mit Exchange Online und Defender for Office 365 aus. Ohne Defender for Office 365 fehlen dir die Klickdaten aus Safe Links und der Threat Explorer; du bleibst dann auf Nachrichtenverfolgung und Anmeldeprotokolle beschränkt und arbeitest spürbar langsamer. Die Schritte zu Konten, Sessions, Postfachregeln und Consent funktionieren auch dann.

Minute 0 bis 5: Ruhe, Rollen, Rahmen

Die ersten fünf Minuten gehören nicht der Technik. Sie gehören der Organisation. Das klingt nach Beraterprosa, ist aber der häufigste Grund, warum eine Stunde später niemand mehr weiß, wer eigentlich was gemacht hat und ob das Postfach der Geschäftsführung schon geprüft wurde oder nur zweimal angeschaut.

Eine Person führt, alle anderen liefern zu

Benenne sofort einen Incident Lead. Das ist nicht zwingend die technisch stärkste Person im Raum, sondern die, die den Überblick behält und nicht selbst im Portal verschwindet. Wer führt, klickt nicht. Wer klickt, führt nicht. Diese Trennung fühlt sich in einem Zehn-Personen-IT-Team albern an und rettet trotzdem regelmäßig den Vormittag.

Danach: ein Protokoll. Kein Ticketsystem-Epos, sondern eine simple Liste mit Uhrzeit und Handlung. „09:52 — Mail in Threat Explorer identifiziert, 41 Empfänger.“ „09:58 — Soft Delete ausgelöst.“ Diese Liste ist später die Grundlage für jede Meldung, jede Nachfrage der Aufsichtsbehörde und jede unangenehme Frage aus der Geschäftsführung. Nachträglich rekonstruierte Zeitstempel sind wertlos.

Kommunikationskanal außerhalb des kompromittierten Systems

Wenn du vermutest, dass ein Konto übernommen wurde, ist E-Mail als Abstimmungskanal für das Reaktionsteam eine schlechte Idee. Der Angreifer liest möglicherweise mit. Ein separater Teams-Kanal ist besser als nichts, aber auch nur, solange der Tenant nicht insgesamt in Frage steht. Für den ernststen Fall gehört eine Telefonliste in den Ordner, den du auch ohne Netzwerk erreichst.

WARNUNG — Der teuerste Fehler der ersten Minuten

Die Mail an alle: „Achtung, Phishing-Welle, bitte nichts anklicken!“ — geschrieben in Minute vier, bevor irgendjemand weiß, welche Mail eigentlich gemeint ist. Das Ergebnis ist berechenbar: Dreißig Rückfragen, zwölf weitergeleitete Verdachtsfälle, ein blockiertes Postfach beim Helpdesk und niemand, der noch ruhig analysieren kann. Die Warnung kommt in Minute 50, nicht in Minute 4 — mit Betreff, Absender und einer klaren Handlungsanweisung.

Wer macht was, wenn die Uhr läuft

Vier Rollen, vier Zeitfenster, keine Doppelarbeit

	Minute 0 bis 15	Minute 15 bis 30	Minute 30 bis 50	Minute 50 bis 60
Incident Lead	Lage aufnehmen, Rollen setzen, Protokoll starten	Entscheidet Umfang: Einzelfall oder Kampagne	Priorisiert Konten, gibt harte Maßnahmen frei	Entscheidet über Meldung und Übergabe
Administration	Threat Explorer, Mail suchen, ZAP-Wirkung prüfen	URL clicks auswerten, Klicker-Liste erstellen	Sessions widerrufen, Passwörter, Regeln, Consent	Nachweise sichern, Exportdateien ablegen
Kommunikation	Kanal außerhalb Exchange aufsetzen	Kurztext vorbereiten, noch nicht senden	Warnung an die Belegschaft ohne Schuldzuweisung	Nachfassen, Rückmeldekanal betreuen
Recht und Leitung	Wird informiert, nicht beschäftigt	Bewertet Datenkategorien und Betroffene	Prüft Fristen nach DSGVO und BSIg	Zeichnet Frühwarnung ab, informiert Gremien

Regel: Wer meldet, entscheidet nicht. Wer entscheidet, klickt nicht selbst im Portal herum.

Skizze 2: Rollen und Zeitfenster. Vier Spuren, die parallel laufen, ohne sich zu behindern.

Wenn dein Haus einen ausgearbeiteten Ablauf hat, ist jetzt der Moment, ihn zu öffnen. Was in so einen Ablauf gehört und wie du ihn schlank hältst, steht im Beitrag [Incident-Response-Plan für Microsoft 365](#). Und wenn du beim Lesen merkst, dass es diesen Plan bei dir noch nicht gibt: Das ist kein Grund, diesen Artikel wegzulegen, sondern einer, ihn zu Ende zu lesen und danach eine [Feuerwehrrübung: Security-Notfälle im Team trainieren](#) anzusetzen.

Minute 5 bis 15: Die Mail identifizieren und ausrollen

Jetzt wird es technisch. Ziel dieser zehn Minuten: Du weißt, welche Nachricht der Auslöser ist, wie viele Postfächer sie erreicht hat, wo sie aktuell liegt — und sie ist auf dem Weg aus den Postfächern heraus.

Threat Explorer: von einer Meldung zur Kampagne

Der Einstieg ist im Defender-Portal unter Explorer beziehungsweise Threat Explorer. Nimm das, was du hast: Absenderadresse, Betreffzeile, Zeitpunkt. Die Ansicht „Alle E-Mails“ ist dein Arbeitsbereich, weil sie eben nicht nur das zeigt, was Defender bereits als bösartig eingestuft hat. Genau darum geht es ja: Die Mail ist durchgekommen.

Filtere zuerst breit, dann eng. Ein sehr häufiger Anfängerfehler ist, sofort nach der exakten Betreffzeile zu suchen. Angreifer variieren Betreffzeilen pro Empfänger. Suche stattdessen nach der Absenderdomäne, nach der Absender-IP oder nach der URL im Nachrichtentext. Erst diese Suche zeigt dir, ob du es mit einer Einzelmail oder mit einer Welle über 300 Postfächer zu tun hast.

Ein Detail, das im Ernstfall gern übersehen wird: Der Threat Explorer zählt jeden Empfänger als eigene Nachricht. Eine Mail an fünf Adressen erscheint als fünf Nachrichten. Das ist für die Bewertung der Lage wichtig — und gleich noch wichtiger, wenn du über Grenzwerte bei der Bereinigung stolperst.

Die Datumsauswahl im Explorer reicht bis 30 Tage zurück. Das klingt komfortabel, ist es aber nur bedingt: Wenn du eine Kampagne aufarbeitest, die schon drei Wochen läuft, arbeitest du am Rand des Fensters, und die Zahlen fangen an zu wackeln. In den ersten 60 Minuten spielt das keine Rolle. Merk es dir für Tag zwei.

Zero-hour auto purge: was ohne dein Zutun passiert

Bevor du selbst zur Tat schreitest, lohnt ein Blick darauf, was der Dienst bereits erledigt hat. Zero-hour auto purge — kurz ZAP — greift nachträglich in Postfächer ein, wenn sich die Bewertung einer bereits zugestellten Nachricht ändert. Genau der Fall also, den du gerade vor dir hast: Die Mail war beim Empfang unauffällig, die Signatur kam später.

FAKTEN — Was Zero-hour auto purge kann und was nicht

ZAP arbeitet in allen Organisationen mit Postfächern in Exchange Online und braucht dafür keine besondere Lizenz. Für ZAP in Microsoft Teams ist Defender for Office 365 Plan 1 oder Plan 2 erforderlich.

- Rückwirkendes Suchfenster: die letzten 48 Stunden zugestellter Nachrichten. Was älter ist, fasst ZAP nicht mehr an.
- Bei Schadsoftware und bei Phishing mit hoher Konfidenz landet die Nachricht in der Quarantäne — unabhängig davon, ob sie schon gelesen wurde.
- Bei einfachem Phishing hängt das Ergebnis von der Aktion ab, die in der Antispam-Richtlinie für dieses Verdikt eingestellt ist: Verschieben in den Junk-E-Mail-Ordner oder Quarantäne. Bei „X-Header hinzufügen“ oder „Betreff ergänzen“ tut ZAP schlicht nichts.
- Bei Spam greift ZAP nur bei ungelesenen Nachrichten. Bei Phishing und Schadsoftware dagegen auch bei gelesenen.

- ZAP wirkt auch im Ordner „Gelöschte Elemente“ und in anderen Ordnern, in die eine Regel die Nachricht verschoben hat — solange sie nicht gelöscht wurde.
- ZAP funktioniert nicht bei Postfächern, die on premises liegen und nur über Microsoft 365 geschützt werden.
- Die Belegschaft bekommt nichts mit: Es gibt keine Benachrichtigung, wenn ZAP eine Nachricht verschiebt.
- Zulassungslisten, Nachrichtenflussregeln, SecOps-Postfächer und Simulations-URLs in der Richtlinie für erweiterte Zustellung können ZAP aushebeln.
- Im Postfachüberwachungsprotokoll von Exchange taucht ZAP nicht als Systemaktion auf. Sichtbar wird es im Threat Explorer über die Spalte für zusätzliche Aktionen und im Bericht zum Nachrichtenfluss.

Die praktische Konsequenz: Verlass dich nicht darauf, dass ZAP schon aufgeräumt hat. Prüfe es. Und rechne damit, dass eine sauber gemachte Phishing-Mail ohne Anhang und mit einer erst nach Zustellung scharf geschalteten Landing Page genau die Art von Nachricht ist, bei der die Signatur eben nicht rechtzeitig kommt.

Take action: aufräumen mit Ansage

Im Threat Explorer markierst du die betroffenen Nachrichten und startest über „Aktion ausführen“ die Bereinigung. Welche Aktion die richtige ist, hängt davon ab, ob du Beweise brauchst oder Ruhe.

Aktion	Was passiert	Wiederherstellbar	Wann sinnvoll
In den Junk-Ordner	Nachricht landet im Junk-E-Mail-Ordner	Ja, durch den Nutzer	Verdacht, aber noch keine Klarheit
In gelöschte Elemente	Nachricht landet im Papierkorb des Postfachs	Ja, durch den Nutzer	Schnelle Sichtbarkeitsreduktion
Vorläufig löschen	Verschieben nach Wiederherstellbare Elemente	Ja, durch Nutzer und Administration	Standardfall im laufenden Vorfall
Endgültig löschen	Nachricht wird endgültig entfernt	Nur über Einzelelementwiederherstellung	Bestätigte Schadsoftware, klare Lage
In den Posteingang	Rückgängigmachen einer Aktion	Entfällt	Fehlalarm, Korrektur

Tabelle 1: Bereinigungsaktionen im Threat Explorer. Im Zweifel vorläufig löschen — das ist reversibel und beendet trotzdem die Gefahr weiterer Klicks.

WARNUNG — Grenzen, die du im Ernstfall triffst

Für die Freigabe der Bereinigung brauchst du die Rolle „Search and Purge“. Standardmäßig hängt sie an den Rollengruppen Organisationsverwaltung und Datenermittler. Wenn dein Bereitschaftsdienst diese Rolle nicht hat, kann er die Aktion nur zur Genehmigung einreichen — und dann wartet ihr nachts um drei auf jemanden mit den richtigen Rechten.

Außerdem drosselt der Dienst großflächige Bereinigungen: Maximal 50 gleichzeitig aktive E-Mail-Bereinigungen pro Organisation, und wenn eine laufende Bereinigung mehr als eine Million Nachrichten umfasst, werden keine neuen mehr angenommen. Aus der Handauswahl im Explorer kannst du bis zu 100 Nachrichten übernehmen, über eine Abfrageauswahl bis zu 200.000. Microsoft empfiehlt Stapel von höchstens 50.000.

Nicht bereinigen kannst du Nachrichten, die endgültig gelöscht wurden, die on premises oder extern liegen, die verworfen wurden oder deren Ablageort unbekannt ist. Für die on-premises-Fälle

bleibt nur der Weg über die eigenen Werkzeuge oder ein Telefonat mit den betroffenen Personen. Auch das gehört ins Protokoll.

Wie Safe Links und Safe Attachments überhaupt konfiguriert sein müssen, damit dir diese Daten im Vorfall zur Verfügung stehen, ist ein eigenes Thema — nachzulesen unter [Defender for Office 365: Safe Links und Safe Attachments](#). Wenn du nach diesem Vorfall feststellst, dass die Richtlinien nie sauber ausgerollt wurden, ist das die erste Aufgabe für Tag zwei.

Minute 15 bis 30: Klicker finden und Konten prüfen

Die Mail ist raus. Die Frage, die jetzt zählt, lautet nicht mehr „Wer hat sie bekommen?“, sondern „Wer hat sie ernst genommen?“. Und das ist eine völlig andere Zahl. In einer typischen Welle bekommen vierzig Personen die Mail, sechs klicken, zwei geben etwas ein, und eine bestätigt anschließend auch noch die Push-Benachrichtigung, weil sie dachte, das gehöre dazu. Dieser eine Fall ist dein Vorfall.

URL clicks: die Ansicht, die du zuerst brauchst

Der Threat Explorer hat eine eigene Ansicht für URL-Klicks. Sie zeigt Klicks auf Links in E-Mails, in Teams-Nachrichten sowie in Dateien aus SharePoint und OneDrive. Du kannst die Auswertung nach URL-Domäne, nach Klick-Verdikt, nach vollständiger URL oder nach Domäne und Pfad gruppieren. Für den Vorfall willst du die vollständige URL, weil Angreifer gern eindeutige Pfade pro Empfänger vergeben.

Entscheidend ist die Spalte mit dem Verdikt. Sie sagt dir, ob Safe Links den Klick abgefangen hat oder ob die Person auf der Seite des Angreifers gelandet ist. Und sie hat mehr Werte als die zwei, die man erwartet.

Verdikt	Bedeutung	Deine Bewertung
Blockiert	Safe Links hat das Öffnen verhindert	Entwarnung für diesen Klick, Konto trotzdem kurz prüfen
Blockierung überschrieben	Warnseite kam, Person klickte weiter	Behandeln wie „zugelassen“, plus Gespräch
Zugelassen	Person konnte die URL öffnen	Vollständige Kontoprüfung, hohe Priorität
Verdikt ausstehend	Detonationsseite wurde angezeigt	Prüfen, ob danach ein weiterer Klick folgte
Ausstehendes Verdikt umgangen	Person hat die Detonationsseite überklickt	Wie „zugelassen“ behandeln
Fehler / Fehlerseite	Verdikt konnte nicht erfasst werden	Konservativ als Klick werten
Keines	Kein Verdikt erfassbar, Öffnen möglich	Konservativ als Klick werten

Tabelle 2: Klick-Verdikte aus Safe Links und ihre Konsequenz im Vorfall. „Blockierung überschrieben“ ist der Wert, den man beim schnellen Lesen übersieht.

UrlClickEvents: dieselbe Frage, präziser gestellt

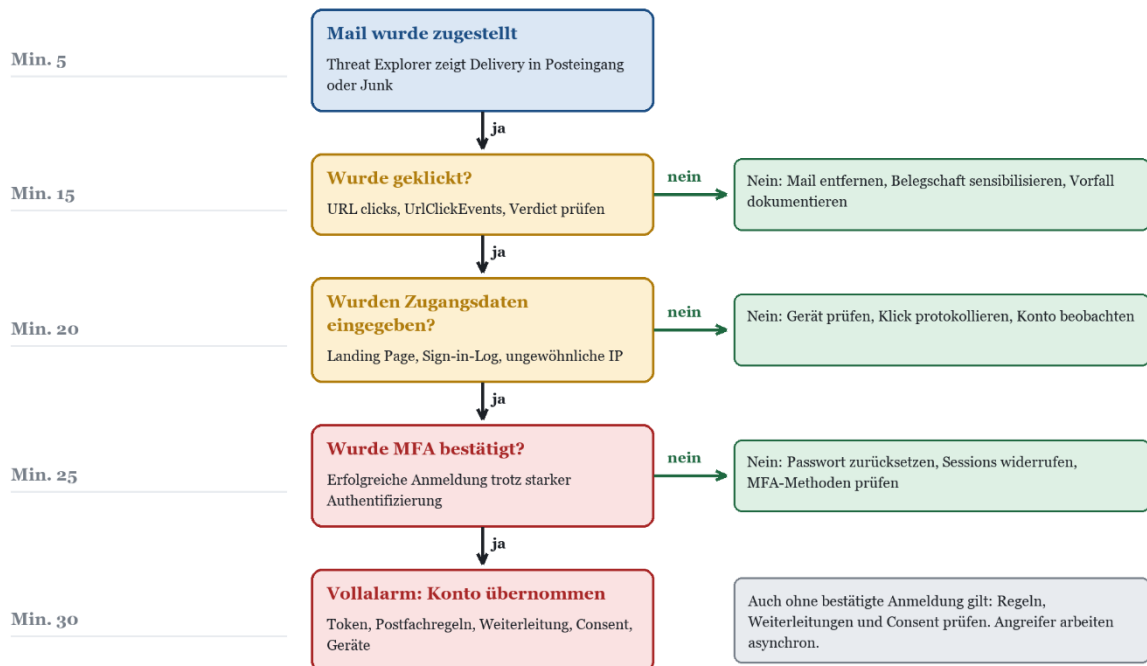
Wenn du die erweiterte Suche im Defender-Portal nutzt, steht dir die Tabelle UrlClickEvents zur Verfügung. Sie enthält die Rohdaten zu jedem zugelassenen oder blockierten Klick — mit Zeitstempel, Konto, URL, Bedrohungstyp und der Information, ob die Warnseite überschrieben wurde. Die interessanten Aktionstypen sind ClickAllowed, ClickBlocked, UrlScanInProgress und UrlErrorPage.

Der eigentliche Wert liegt in der Verknüpfung: Du kannst die Klickdaten mit den E-Mail-Ereignissen und mit den Endpunktdaten zusammenführen und siehst dann in einer Zeitleiste, was nach dem Klick auf dem Gerät passiert ist. Für die ersten 60 Minuten reicht meist eine simple

Liste: Welches Konto, welche Zeit, welches Verdikt. Speichere die Abfrage. Beim nächsten Mal brauchst du sie in dreißig Sekunden statt in acht Minuten.

Wie tief steckt der Vorfall wirklich?

Jede Ja-Antwort kostet dich eine weitere Eskalationsstufe



Skizze 3: Der Eskalationsbaum. Jede Ja-Antwort erweitert den Kreis der Maßnahmen.

Anmeldeprotokolle und riskante Anmeldungen

Parallel zu den Klickdaten öffnest du die Anmeldeprotokolle in Entra ID, gefiltert auf die Konten aus deiner Klicker-Liste und auf das Zeitfenster ab der Zustellung. Du suchst nach drei Dingen: erfolgreiche Anmeldungen aus ungewöhnlichen Ländern, Anmeldungen mit auffälligen Clients und Anmeldungen, die trotz Mehrfaktor-Authentifizierung erfolgreich waren, obwohl der eigentliche Nutzer gerade in einer Besprechung saß.

Hast du Entra ID Protection lizenziert, sind die Berichte zu riskanten Anmeldungen und riskanten Benutzern der schnellere Weg. Eine Anmeldung wird als riskant geführt, sobald für sie mindestens eine Risikoerkennung vorliegt; das Benutzerrisiko aggregiert dagegen Erkennungen über die Zeit, etwa geleakte Anmeldedaten, die auch ohne konkrete Anmeldung gemeldet werden. Für die Bewertung im Vorfall ist beides interessant, denn ein hohes Benutzerrisiko ohne auffällige Anmeldung heißt oft: Der Angreifer hat die Zugangsdaten, nutzt sie aber noch nicht.

Signal	Wo du es findest	Was es dir sagt
Zustellung und Ablageort	Threat Explorer, Ansicht Alle E-Mails	Umfang der Welle, aktueller Ort der Nachricht
ZAP-Wirkung	Threat Explorer, Spalte zusätzliche Aktion; Bericht Nachrichtenfluss	Ob der Dienst bereits eingegriffen hat
Klick auf den Link	Ansicht URL clicks; Tabelle UrlClickEvents	Wer die Seite des Angreifers gesehen hat
Erfolgreiche Anmeldung	Anmeldeprotokolle in Entra ID	Ob die Zugangsdaten funktioniert haben
Risikobewertung	Berichte zu riskanten Anmeldungen und	Priorisierung ohne manuelle Korrelation

	riskanten Benutzern	
Postfachaktivität	Überwachungsprotokoll, Ereignisse zu Postfachregeln	Ob bereits Persistenz aufgebaut wurde
App-Berechtigungen	Unternehmensanwendungen, Berechtigungen und Zustimmungen	Ob ein Zugriff unabhängig vom Passwort besteht

Tabelle 3: Die sieben Quellen, aus denen sich die Lage in der ersten Stunde zusammensetzt. Mehr brauchst du nicht, weniger reicht nicht.

TIPP — Filter vorbereiten, nicht improvisieren

Lege dir heute — im ruhigen Zustand — die drei Ansichten an, die du im Vorfall brauchst: eine gespeicherte Explorer-Abfrage auf Klicks der letzten 24 Stunden, eine Abfrage in der erweiterten Suche auf UrlClickEvents mit Verdikt, und einen gefilterten Blick auf erfolgreiche Anmeldungen außerhalb deiner üblichen Länder. Drei Lesezeichen, zehn Minuten Arbeit, und im Ernstfall sparst du dir die Phase, in der du unter Druck Filtersyntax suchst.

Minute 30 bis 50: Zugriff kappen, Persistenz suchen

Du hast eine Liste betroffener Konten. Jetzt geht es darum, den Zugriff zu beenden — und zwar vollständig. Das ist der Abschnitt, in dem die meisten Vorfälle falsch abbiegen, weil eine Teilmaßnahme sich anfühlt wie eine ganze.

Erst die Sitzung, dann das Passwort — und beides zusammen

Ein zurückgesetztes Passwort verhindert neue Anmeldungen. Es beendet keine Sitzung, die bereits läuft. Wer nur das Passwort tauscht, hat dem Angreifer eine Unannehmlichkeit bereitet und sonst nichts. Umgekehrt gilt: Wer nur die Sitzungen widerruft, aber das Passwort stehen lässt, schaut zu, wie sich der Angreifer neu anmeldet.

Die Reihenfolge in der Praxis: Konto sperren oder Passwort zurücksetzen, unmittelbar danach die Aktualisierungstoken widerrufen. Im Entra-Admin-Center findest du auf der Übersichtsseite des Benutzers den Punkt „Sitzungen widerrufen“. Für mehrere Konten ist PowerShell schneller: Update-MgUser mit AccountEnabled auf false, danach Revoke-MgUserSignInSession. Registrierte Geräte lassen sich über Get-MgUserRegisteredDevice und Update-MgDevice im selben Zug deaktivieren.

WICHTIG — Warum der Widerruf nicht sofort wirkt

Zugriffstoken von Entra ID sind standardmäßig eine Stunde gültig. Ein Widerruf der Aktualisierungstoken verhindert die Erneuerung, macht aber ein bereits ausgestelltes Zugriffstoken nicht ungültig — es läuft ab. Genau deshalb gibt es die fortlaufende Zugriffsauswertung, die Continuous Access Evaluation: Bei einem kritischen Ereignis wird das Token bei unterstützten Diensten typischerweise innerhalb von rund 15 Minuten ersetzt. Exchange Online, SharePoint, OneDrive, Teams und Microsoft Graph unterstützen das.

Für dein Playbook heißt das: Nach dem Widerruf ist nicht sofort Ruhe. Plane eine Nachkontrolle in den Anmeldeprotokollen ein — und behandle die 15 Minuten danach als Zeitraum, in dem noch etwas passieren kann.

In hybriden Umgebungen kommt der Weg über das lokale Active Directory dazu: Konto deaktivieren, Passwort zurücksetzen — laut Microsoft-Empfehlung zweimal hintereinander, um Pass-the-Hash-Risiken bei verzögerter Replikation zu begrenzen. Wer sich fragt, warum Kerberos-Tickets dabei eine eigene Rolle spielen, findet den Hintergrund im

Kompetenzbereich Kerberos. Für die erste Stunde reicht die Faustregel: Ein deaktiviertes Konto ist nicht dasselbe wie ein Konto ohne gültige Tickets.

Postfachregeln und Weiterleitungen: die stille Persistenz

Wenn ein Angreifer ein Postfach übernimmt, ist eine der ersten Handlungen fast immer eine Regel. Nicht um Schaden anzurichten, sondern um Spuren zu verwischen. Klassische Muster: Nachrichten mit bestimmten Stichwörtern werden in den RSS-Ordner verschoben, Sicherheitswarnungen werden direkt gelöscht, Antworten auf die vom Angreifer versendeten Mails landen in einem Unterordner, den niemand ansieht.

Prüfe deshalb für jedes betroffene Postfach die Regeln — über Get-InboxRule in der Exchange-Online-PowerShell oder direkt im Postfach. Auffällig sind Regeln ohne Namen, Regeln mit einem einzelnen Buchstaben oder Punkt als Namen, Regeln mit Zielordner „RSS-Feeds“ und alles, was Nachrichten löscht oder als gelesen markiert.

Weiterleitungen sind der zweite Hebel und existieren in mehreren Ausprägungen, die man getrennt prüfen muss: als Postfachregel, als Weiterleitungsadresse am Postfach selbst und als Nachrichtenflussregel auf Organisationsebene. Die Suche im Überwachungsprotokoll nach den Aktionen New-InboxRule, Set-InboxRule, UpdateInboxRules, Set-Mailbox, New-TransportRule und Set-TransportRule deckt alle drei ab.

WARNUNG — Nicht nur löschen, erst dokumentieren

Die Versuchung ist groß, eine gefundene Weiterleitungsregel sofort zu entfernen. Mach vorher einen Screenshot oder einen Export. Die Regel ist der Beleg dafür, dass ein unbefugter Zugriff stattgefunden hat, und die Zieladresse ist ein Indikator, nach dem du im gesamten Tenant suchen willst — vielleicht taucht sie in einem zweiten Postfach auf, von dem du noch gar nichts weißt.

Consent-Grants: der Zugriff, den kein Passwortwechsel beendet

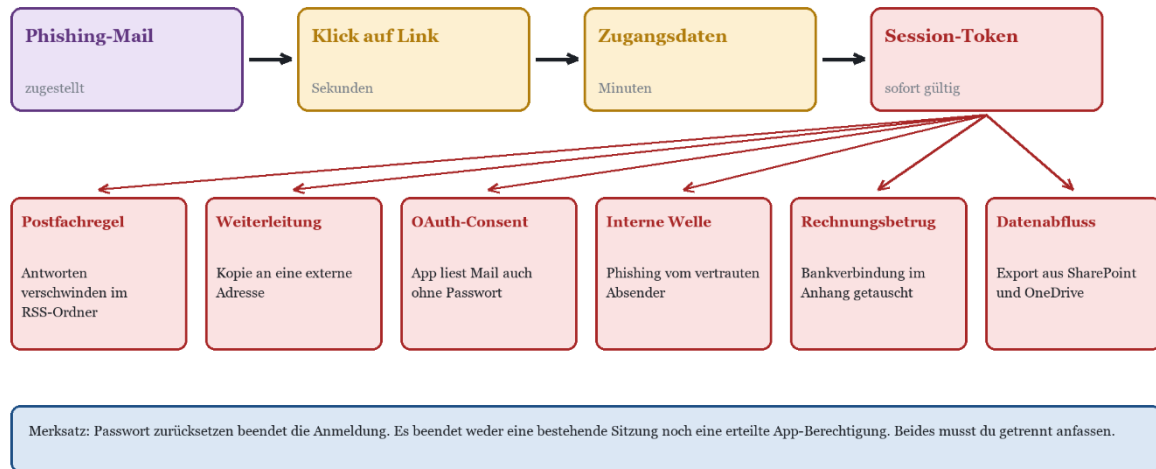
Der unangenehmste Teil kommt zum Schluss. Moderne Phishing-Kampagnen zielen nicht mehr nur auf Zugangsdaten, sondern auf Zustimmung. Die Person landet nicht auf einer nachgebauten Anmeldeseite, sondern auf einer echten Microsoft-Zustimmungsseite, auf der eine App um Berechtigungen bittet. Wer dort zustimmt, gibt einer fremden Anwendung dauerhaften Zugriff auf Postfach, Dateien und Kontakte.

Microsoft formuliert das ungewöhnlich deutlich: Die üblichen Gegenmaßnahmen — Passwort zurücksetzen, Multifaktor-Authentifizierung erzwingen — sind gegen diese Angriffsart wirkungslos, weil die App außerhalb der Organisation liegt und mit eigenen Token arbeitet. Du musst die Zustimmung aktiv entziehen.

Der Weg im Portal führt über Unternehmensanwendungen zur betroffenen Anwendung und dort zu Berechtigungen. In PowerShell entfernst du delegierte Berechtigungen mit Remove-MgOAuth2PermissionGrant und Anwendungsrollenzuweisungen mit Remove-MgServicePrincipalAppRoleAssignment. Wichtig ist, beides zu prüfen: Eine App kann sowohl im Namen des Nutzers als auch mit eigenen Anwendungsberechtigungen arbeiten.

Was aus einem Klick in einer Stunde werden kann

Die Kette oben ist schnell, die Fächerung unten ist teuer



Skizze 4: Vom Klick zur Persistenz. Die Kette oben läuft in Minuten, die Fächerung unten beschäftigt dich wochenlang.

Eskalationsstufe	Auslöser	Maßnahmen in dieser Stunde
Stufe 1 — Zugestellt	Mail im Postfach, kein Klick	Bereinigen, dokumentieren, Absender blockieren
Stufe 2 — Geklickt	Verdikt zugelassen oder überschrieben	Zusätzlich: Anmeldeprotokoll prüfen, Gerät bewerten
Stufe 3 — Eingegeben	Zugangsdaten auf der Landing Page	Zusätzlich: Passwort zurücksetzen, Sessions widerrufen
Stufe 4 — Angemeldet	Erfolgreiche fremde Anmeldung	Zusätzlich: Regeln, Weiterleitungen, Geräte, Datenzugriffe
Stufe 5 — Zustimmung	App-Consent erteilt	Zusätzlich: Berechtigungen entziehen, App sperren, Tenant-weit suchen

Tabelle 4: Fünf Stufen, kumulativ zu lesen. Stufe 5 erbt alle Maßnahmen der Stufen darunter — und fügt die einzige hinzu, die ein Passwortwechsel nicht abdeckt.

Wenn du an dieser Stelle merkst, dass in deinem Tenant jede beliebige Person jeder beliebigen App Zugriff auf ihr Postfach geben darf, hast du das eigentliche Ergebnis dieses Vorfalls gefunden. Wie man das ohne Vollbremsung geraderückt, steht unter [App-Registrierungen und Consent-Governance](#). Für die vertiefte Aufarbeitung eines übernommenen Kontos über die erste Stunde hinaus geht es weiter bei [Kompromittiertes Konto erkennen und aufräumen](#).

TIPP — Der Nebenkriegsschauplatz, den du jetzt nicht eröffnest

Irgendwann in dieser Phase kommt die Frage auf, ob man nicht gleich die Conditional-Access-Richtlinien überarbeiten sollte. Antwort: nein, nicht jetzt. Eine unter Druck gebaute Richtlinie sperrt zuverlässig die falschen Leute aus, meistens die, die gerade den Vorfall bearbeiten. Notiere die Idee, arbeite den Vorfall ab, und nimm dir das Thema in der kommenden Woche in Ruhe vor.

Minute 50 bis 60: Kommunikation und Meldepflichten

Die letzten zehn Minuten sind die, die über den Ruf deiner IT entscheiden. Technisch ist vieles erledigt, organisatorisch fängt es an.

Die Nachricht an die Belegschaft

Jetzt — und erst jetzt — geht die Warnung raus. Sie ist kurz, konkret und frei von Schuldzuweisung. Sie enthält: den Betreff der Mail, den Absender, wie die Mail aussah, was zu tun ist, wenn man geklickt hat, und an wen man sich meldet. Sie enthält nicht: Formulierungen wie „wie bereits mehrfach kommuniziert“ oder „eigentlich sollte jedem klar sein“. Wer Menschen beschämt, bekommt beim nächsten Vorfall keine Meldung mehr, sondern eine stille Hoffnung, dass es schon gut geht.

Ein Satz, der sich bewährt hat: „Wenn du geklickt hast, melde dich — es passiert dir nichts, und du hilfst uns.“ Das ist keine Sozialromantik, sondern Betriebswirtschaft. Die Person, die sich nach zehn Minuten meldet, kostet dich eine Stunde. Die Person, die sich nach drei Tagen meldet, kostet dich eine Woche.

Was du für diese Kommunikation brauchst, sind vorbereitete Textbausteine. Und was du langfristig brauchst, ist eine Belegschaft, die Phishing erkennt, weil sie es geübt hat — dazu passt [Attack Simulation Training: Phishing-Übungen richtig aufsetzen](#) ebenso wie eine strukturierte [Schulung Microsoft 365 Security](#) für alle, die im Ernstfall am Portal sitzen.

Die Uhren, die schon seit Minute 0 laufen

Meldepflichten sind unbequem, weil sie an einem Zeitpunkt anknüpfen, den du nicht wählen kannst: der Kenntnis vom Vorfall. Nicht der abgeschlossenen Analyse, nicht der Bestätigung durch ein Gutachten. Kenntnis. Das ist in aller Regel der Moment, in dem im Teams-Chat „Ich glaub, ich hab da was angeklickt“ stand.

Zwei Regelwerke laufen dabei nebeneinander. Aus der Datenschutz-Grundverordnung ergibt sich nach Artikel 33 die Meldung einer Verletzung des Schutzes personenbezogener Daten an die Aufsichtsbehörde binnen 72 Stunden, sofern ein Risiko für die betroffenen Personen besteht; bei voraussichtlich hohem Risiko kommt nach Artikel 34 die unverzügliche Benachrichtigung der Betroffenen hinzu. Aus dem NIS-2-Umsetzungsgesetz, das am 6. Dezember 2025 in Kraft getreten ist, folgt für betroffene Einrichtungen ein dreistufiger Meldeprozess an das BSI nach dem novellierten BSIG: Frühwarnung binnen 24 Stunden, Folgemeldung binnen 72 Stunden, Abschlussbericht binnen eines Monats.

Die Uhren, die parallel zu deinem Playbook laufen

Startpunkt ist die Kenntnis vom Vorfall, nicht das Ende der Analyse

Frühwarnung an das BSI

nur bei erheblichem Vorfall nach BSIG

24 Stunden

Meldung an die Aufsichtsbehörde

Artikel 33 DSGVO bei Risiko für Betroffene

72 Stunden

Folgemeldung an das BSI

Bewertung, Ursache, ergriffene Maßnahmen

72 Stunden

Benachrichtigung der Betroffenen

Artikel 34 DSGVO bei hohem Risiko

unverzüglich

Abschlussbericht an das BSI

Ursachenanalyse und dauerhafte Maßnahmen

1 Monat

Kenntnis

Die Fristen laufen unabhängig davon, ob dein Team gerade noch Postfachregeln aufräumt. Wer die Uhr erst nach der Technik startet, hat sie schon halb verbraucht.

Skizze 5: Fünf Fristen, ein Startpunkt. Die Skala ist logarithmisch, damit 24 Stunden neben einem Monat überhaupt sichtbar bleiben.

Frist	Grundlage	Was hineingehört	Wer liefert zu
24 Stunden	BSIG, Frühwarnung	Erste Einschätzung, Verdacht auf rechtswidrige Handlung, mögliche grenzüberschreitende Auswirkung	Incident Lead und Leitung
72 Stunden	BSIG, Folgemeldung	Bewertung des Vorfalls, Schwere, Auswirkungen, Indikatoren	Incident Lead und Administration
72 Stunden	Artikel 33 DSGVO	Art der Verletzung, Kategorien und ungefähre Zahl der Betroffenen, Folgen, Maßnahmen	Datenschutzbeauftragte Person
Unverzüglich	Artikel 34 DSGVO	Klare, einfache Sprache, konkrete Empfehlungen an die Betroffenen	Datenschutz und Kommunikation
Ein Monat	BSIG, Abschlussbericht	Ursachenanalyse, ergriffene und geplante Maßnahmen, grenzüberschreitende Auswirkungen	Gesamtes Team

Tabelle 5: Der Fristenkalender im Überblick. Ob dich die BSIG-Pflichten treffen, hängt von Größe und Sektor deiner Einrichtung ab — das klärst du vorher, nicht im Vorfall.

WARNUNG — Die Registrierungsfaller

Die Meldepflicht nach BSIG setzt voraus, dass du weißt, ob deine Einrichtung überhaupt betroffen ist. Die Registrierungspflicht beim BSI ergab sich für die zum Inkrafttreten betroffenen Einrichtungen aus einer Dreimonatsfrist, die am 6. März 2026 endete. Wer diese Prüfung nie gemacht hat, klärt im Ernstfall unter maximalem Zeitdruck eine Rechtsfrage, während parallel die 24-Stunden-Uhr läuft. Das ist keine gute Kombination.

Übergabe statt Abschluss

Nach 60 Minuten ist der Vorfall nicht erledigt. Er ist stabilisiert. Der Unterschied ist wichtig, auch für die Kommunikation nach oben. Was jetzt folgt, ist die eigentliche Aufarbeitung: vollständige Prüfung der betroffenen Postfächer, Auswertung der Datenzugriffe, Bewertung, ob Daten abgeflossen sind, und die Frage, warum die Mail überhaupt durchkam.

Übergib schriftlich. Ein halbseitiges Lagebild mit dem Stand nach einer Stunde, den offenen Punkten und den nächsten Schritten. Wer das nicht tut, verbringt den Nachmittag damit, dieselbe Geschichte fünfmal mündlich zu erzählen, jedes Mal ein bisschen anders.

Zwei Themen gehören unmittelbar an diese Übergabe angeschlossen. Erstens: Wenn im Vorfall Schadsoftware im Spiel war oder auch nur im Raum stand, prüfst du die Wiederherstellbarkeit — siehe [Ransomware-Vorsorge in Microsoft 365](#). Zweitens: Alles, was du in dieser Stunde manuell zusammensuchen musstest, gehört als automatische Benachrichtigung eingerichtet, damit die nächste Meldung nicht aus dem Teams-Chat kommt, sondern aus dem System — dazu passt [Alert Policies und Benachrichtigungen richtig aufsetzen](#).

WICHTIG — Vor der Auswertung: das Gespräch mit dem Betriebsrat

Auswertungen von Klickdaten und Anmeldeprotokollen sind personenbezogen. Sie zeigen, wer wann was angeklickt hat. In der akuten Gefahrenabwehr ist das regelmäßig zulässig — als dauerhaft eingerichtete Auswertung ist es mitbestimmungspflichtig. Kläre das im Normalbetrieb, nicht im Vorfall.

Weiterlesen

- › [Microsoft 365 Security — Übersicht und Einstieg](#)
- › [Kompromittiertes Konto erkennen und aufräumen](#)
- › [Ransomware-Vorsorge in Microsoft 365](#)
- › [Incident-Response-Plan für Microsoft 365](#)
- › [Security-Monitoring und Betriebsrat: was mitbestimmungspflichtig ist](#)
- › [Tenant-Härtung: die 20 wichtigsten Schrauben](#)
- › [Dossier TerminalFix und der Berlin-Hack](#)

Häufige Fragen

Muss ich wirklich zuerst die Mail entfernen und nicht zuerst das Konto sperren?

Das hängt davon ab, was du schon weißt. Wenn eine erfolgreiche fremde Anmeldung dokumentiert ist, hat das Konto Vorrang — Sitzungen widerrufen, Passwort zurücksetzen, sofort. Wenn du nur weißt, dass eine Phishing-Mail unterwegs ist, hat die Mail Vorrang, weil jede weitere Minute weitere Klicks bedeutet. Der Regelfall in der Praxis: Beides läuft parallel, weil zwei Personen daran arbeiten. Genau dafür verteilst du in Minute 2 die Rollen.

Reicht es nicht, wenn ZAP die Mail automatisch aufräumt?

Manchmal ja, verlassen darfst du dich nicht darauf. ZAP schaut 48 Stunden zurück und handelt nur, wenn sich das Verdikt ändert und die Aktion in deinen Richtlinien das hergibt. Bei einfachem Phishing mit der Einstellung „X-Header hinzufügen“ passiert schlicht nichts. Außerdem greift ZAP nicht bei Postfächern, die on premises liegen. Prüfen kostet zwei Minuten, sich blind darauf verlassen kostet mehr.

Woran erkenne ich, dass jemand nicht nur geklickt, sondern auch Daten eingegeben hat?

Direkt siehst du das nicht — die Eingabe passiert auf dem Server des Angreifers. Du erschließt es indirekt: über eine erfolgreiche Anmeldung, die zeitlich unmittelbar auf den Klick folgt, über eine ungewöhnliche Quell-IP oder über eine Risikoerkennung in Entra ID. Und über das Gespräch. Frag die Person direkt und ohne Vorwurf. Die Antwort ist die schnellste Datenquelle, die du hast.

Wie lange dauert es, bis ein Widerruf der Sitzungen tatsächlich wirkt?

Neue Token gibt es sofort keine mehr. Bereits ausgestellte Zugriffstoken laufen standardmäßig innerhalb einer Stunde ab. Bei Diensten mit fortlaufender Zugriffsauswertung — Exchange Online, SharePoint, OneDrive, Teams, Microsoft Graph — wird das Token bei einem kritischen Ereignis typischerweise binnen rund 15 Minuten ersetzt. Rechne also mit einem Zeitfenster und kontrolliere danach noch einmal die Anmeldeprotokolle.

Warum hilft ein Passwortwechsel nicht gegen eine erteilte App-Zustimmung?

Weil die App gar nicht mit dem Passwort arbeitet. Sie hat eine eigene Berechtigung erhalten und arbeitet mit eigenen Token. Solange du den Consent-Grant nicht entziehst, greift sie weiter auf Postfach und Dateien zu — auch nach einem Passwortwechsel und auch mit aktiver Mehrfaktor-Authentifizierung. Deshalb steht die Prüfung der Berechtigungen als eigener Schritt in diesem Playbook und nicht als Fußnote.

Muss ich jeden Phishing-Vorfall melden?

Nein. Eine abgefangene Mail ohne Klick ist kein meldepflichtiger Vorfall. Meldepflicht entsteht, wenn personenbezogene Daten betroffen sind und ein Risiko für die betroffenen Personen besteht — dann greift die 72-Stunden-Frist aus der Datenschutz-Grundverordnung. Für Einrichtungen im Anwendungsbereich des novellierten BSI-Gesetzes kommt bei einem erheblichen Vorfall die 24-Stunden-Frühwarnung an das BSI hinzu. Ob das dein Haus betrifft, klärst du vorher mit Recht und Datenschutz und schreibst es in den Notfallplan.

Was mache ich, wenn der Vorfall am Freitagabend auffällt?

Dasselbe wie sonst, nur mit weniger Leuten. Die 60 Minuten schrumpfen dann nicht, sie werden wichtiger: Mail entfernen, Sitzungen widerrufen, Passwörter zurücksetzen, Regeln und Zustimmungen prüfen. Das ist die harte Kernmenge. Alles Weitere kann bis Montag warten — die Meldefristen allerdings nicht. Deshalb gehört in jeden Bereitschaftsplan eine erreichbare Person aus Recht oder Datenschutz.

Brauche ich für dieses Playbook Defender for Office 365 Plan 2?

Für den vollen Umfang ja. Der Threat Explorer mit der Ansicht für alle E-Mails, die Kampagnenansicht und die manuelle Bereinigung gehören zu Plan 2. Mit Plan 1 stehen dir die Echtzeiterkennungen zur Verfügung, die auf Erkennungen zum Zustellzeitpunkt beschränkt sind. Ohne Defender for Office 365 bleiben Nachrichtenverfolgung, Überwachungsprotokoll und Anmeldeprotokolle — das reicht für eine Reaktion, kostet aber deutlich mehr Zeit.

Wer sollte dieses Playbook im Haus können?

Mindestens zwei Personen, besser drei. Ein Playbook, das nur eine Person beherrscht, ist kein Playbook, sondern ein Personenrisiko. Und es sollte einmal im Jahr geübt werden, mit Stoppuhr und einem realistischen Szenario. Wer dabei Unterstützung von außen möchte: Genau dafür gibt es die

[Microsoft 365 Security Beratung](#) — eine begleitete Übung deckt in einem halben Tag mehr Lücken auf als drei Monate Dokumentenpflege.

Fazit

Die ersten 60 Minuten nach einem Phishing-Vorfall entscheiden nicht über Sieg oder Niederlage. Sie entscheiden über die Größe der Aufräumarbeit. Wer strukturiert vorgeht — Rollen klären, Mail identifizieren, ZAP-Wirkung prüfen, bereinigen, Klicker finden, Konten bewerten, Sitzungen widerrufen, Passwörter tauschen, Regeln und Zustimmungen kontrollieren, kommunizieren, Fristen starten — hat nach einer Stunde eine stabile Lage und ein sauberes Protokoll.

Wer stattdessen mit dem Passwortwechsel beginnt und danach improvisiert, hat nach einer Stunde ein zurückgesetztes Passwort, eine weiterhin aktive Angreifersitzung, eine unentdeckte Weiterleitungsregel und eine App, die fröhlich weiter das Postfach ausliest. Der Unterschied zwischen beiden Verläufen ist keine Frage des Budgets. Es ist eine Frage der Reihenfolge und der Vorbereitung.

Die drei Dinge, die du nach diesem Artikel tun solltest, sind unspektakulär: Leg dir die drei gespeicherten Abfragen an. Prüfe, wer in deinem Haus die Rolle für die Bereinigung besitzt und ob diese Person nachts erreichbar ist. Und kläre einmal in Ruhe, welche Meldepflichten deine Einrichtung überhaupt treffen. Zusammen kosten diese drei Punkte einen halben Tag — und sie sind der Unterschied zwischen einem geordneten Vormittag und einer Woche, über die man später ungern spricht.

Dieser Beitrag gehört zum Handlungsfeld Reaktion und Notfall der Reihe [Microsoft 365 Security](#).
Dort findest du die übrigen Handlungsfelder von Identität und Zugriff über Härting bis
Nachweisführung — und die Reihenfolge, in der sie sinnvollerweise angegangen werden.