

Kompromittiertes Konto erkennen und aufräumen: das Playbook für den Tag, an dem es passiert ist

Es beginnt fast nie mit einem Alarm. Es beginnt damit, dass eine Kollegin sagt: „Du, komisch, der Kunde behauptet, ich hätte ihm gestern eine neue Bankverbindung geschickt.“ Oder damit, dass jemand aus dem Vertrieb sich wundert, warum eine Antwort auf seine Mail nie angekommen ist, obwohl der Empfänger schwört, geantwortet zu haben. Der Alarm kommt später. Manchmal gar nicht.

Ein übernommenes Microsoft-365-Konto ist der unspektakulärste Sicherheitsvorfall, den es gibt — und gleichzeitig der teuerste im Verhältnis zum Aufwand des Angreifers. Kein Exploit, keine Sicherheitslücke, kein raffinierter Schadcode. Jemand hat sich angemeldet. Mehr ist nicht passiert. Und genau deshalb sieht in den Protokollen erst einmal alles völlig normal aus.

Dieser Beitrag ist ein Playbook. Er beschreibt, woran du eine Kontoübernahme erkennst, in welcher Reihenfolge du aufräumst und warum diese Reihenfolge nicht verhandelbar ist. Er beschreibt außerdem, wie du hinterher belegst, was tatsächlich passiert ist — und wem du das Ganze innerhalb welcher Frist erzählen musst. Was dieser Beitrag nicht ist: eine Anleitung zur Schuldzuweisung. Die Person, die geklickt hat, ist deine wichtigste Informationsquelle. Behandle sie entsprechend.

FAKTEN · Wo dieser Beitrag hingehört

Kompromittierte Konten sind Handlungsfeld D in unserer Reihe zu [Microsoft 365 Security](#). Wenn du gerade mitten in einem Phishing-Vorfall steckst und die ersten sechzig Minuten noch vor dir liegen, lies zuerst [Phishing-Vorfall: die ersten 60 Minuten](#) — dieser Beitrag hier setzt danach ein, wenn feststeht, dass ein Konto tatsächlich übernommen wurde.

Woran du merkst, dass das Konto nicht mehr dir allein gehört

Die unangenehme Wahrheit zuerst: Ein Angreifer, der ein gültiges Kennwort und ein gültiges Sitzungscookie hat, verhält sich technisch wie ein Mitarbeiter. Er meldet sich an, liest Mails, sucht in SharePoint, lädt Dateien herunter. Es gibt kein Ereignis mit dem Namen „Angreifer hat sich angemeldet“. Es gibt nur Abweichungen vom Gewohnten — und die musst du kennen, um sie zu sehen.

Die Signale verteilen sich auf vier Ecken deines Tenants. Keine einzelne davon beweist etwas. Zwei aus zwei verschiedenen Ecken sind praktisch immer ein Vorfall.

Erkennungszeichen: vier Ecken, ein Befund

Kein Signal beweist allein etwas. Zwei aus zwei Ecken sind ein Vorfall.

Identität · Entra ID

- Risky Sign-in: unbekannte Anmeldeeigenschaften
- Anmeldung aus zwei Ländern in 20 Minuten
- Anomalous Token: Lebensdauer passt nicht
- Erfolg nach Password Spray
- Leaked Credentials — immer hohes Risiko

Postfach · Exchange Online

- Neue Regel mit Namen „.“ oder „a“
- Verschieben nach Notizen oder RSS-Feeds
- ForwardingSmtpAddress plötzlich gesetzt
- Gesendet-Ordner voller fremder Nachrichten
- Postfach darf nicht mehr senden

Anwendungen · Consent

- Neue Unternehmensanwendung ohne Ticket
- Zustimmung zu Mail.Read oder Mail.Send
- Offline-Zugriff für eine unbekannte App
- App-Registrierung mit frischem Geheimnis
- Berechtigung übersteht Passwortwechsel

Faktoren und Geräte

- Zusätzliche Authenticator-App registriert
- Fremde Telefonnummer als SMS-Methode
- Neu registriertes Gerät aus fremdem Netz
- Alternative E-Mail für Selbstbedienung
- App-Kennwort neu angelegt

Zwei Signale aus zwei verschiedenen Ecken = kompromittiert, bis das Gegenteil bewiesen ist.

Ein einzelnes Signal = prüfen. Null Signale und trotzdem ein mulmiges Gefühl = auch prüfen.

Quelle der Signalnamen: Entra ID Protection, Defender for Office 365, Purview Audit.

Skizze 1: Die vier Ecken, in denen sich eine Kontoübernahme zeigt. Die Postfach-Ecke fällt in der Praxis am häufigsten zuerst auf — meistens, weil jemand von außen anruft.

Risky Sign-ins lesen, ohne im Rauschen zu ertrinken

Entra ID Protection wirft dir eine ganze Reihe von Risikoerkennungen vor die Füße, und sie sind nicht gleich viel wert. Wer alle gleich behandelt, hat nach zwei Wochen eine Benachrichtigungsregel, die niemand mehr liest — das ist die eigentliche Gefahr an dieser Stelle.

Ganz oben stehen die Erkennungen mit hoher Trefferquote. „Leaked Credentials“ ist immer hohes Risiko, weil Microsoft die gefundenen Zugangsdaten gegen die aktuell gültigen Kennworthashes deines Tenants prüft und die Meldung nur dann erzeugt, wenn es wirklich passt. Das ist kein Verdacht, das ist ein Treffer. „Password Spray“ mit erfolgreicher Anmeldung bedeutet, dass jemand breit gestreut geraten hat und bei dir fündig geworden ist.

In der Mitte liegen die Erkennungen, die Kontext brauchen. „Unfamiliar sign-in properties“ vergleicht die aktuelle Anmeldung mit der Historie: IP-Adresse, Netzbetreiber, Standort, Gerät, Browser. Das trifft auch die Kollegin, die zum ersten Mal aus dem Urlaub in Portugal arbeitet. Besonders aufmerksam solltest du werden, wenn diese Erkennung bei einer nicht-interaktiven Anmeldung auftaucht — dann riecht es nach wiedergespieltem Token. „Anomalous token“ ist genau dafür gebaut: ungewöhnliche Token-Lebensdauer, Token von einem unbekannten Ort. Diese Erkennung war historisch die lauteste; Microsoft hat nachjustiert, aber bei niedrigem und mittlerem Risiko sind Fehlalarme weiterhin wahrscheinlicher als anderswo.

TIPP · Die Zwei-Signale-Regel

Bewerte nie eine einzelne Risikoerkennung isoliert. Nimm die Erkennung und schau sofort in eine

zweite Ecke: Gibt es im gleichen Zeitfenster eine neue Postfachregel, eine neue Anwendungsberechtigung oder eine zusätzlich registrierte MFA-Methode? Wenn ja, ist die Diskussion beendet und das Playbook beginnt.

- › Anmeldeprotokoll: IP, Standort, Netzbetreiber, Zeitpunkt, Erfolg oder Fehlschlag
- › Überwachungsprotokoll: Set-Mailbox, New-InboxRule, Set-InboxRule, Consent to application
- › Nachrichtenverfolgung: Wer hat in diesem Fenster was verschickt?

Die Postfachregel mit dem Namen „.“

Das klassischste aller Erkennungszeichen ist die Postfachregel, die niemand angelegt hat. Angreifer bauen sie, weil sie zwei Probleme gleichzeitig lösen: Die Beute fließt automatisch ab, und der eigentliche Besitzer des Postfachs merkt nichts, weil die relevanten Antworten gar nicht erst im Posteingang landen.

Typisch sind Regelnamen, die aus einem einzelnen Zeichen bestehen — ein Punkt, ein Buchstabe, ein Leerzeichen —, weil sie in der Regelliste kaum auffallen. Typisch sind außerdem Zielordner, in die kein Mensch freiwillig etwas verschiebt: Notizen, Junk-E-Mail, RSS-Feeds. Und typisch sind Filter auf Wörter, die nach Geld riechen: Rechnung, Zahlung, IBAN, Mahnung, invoice, payment. Wenn der Angreifer gar keinen Filter setzt und einfach alles weiterleitet, ist das übrigens genauso verdächtig — nur unauffälliger im Blick auf die Regelbedingungen.

Was viele nicht wissen: Ein Teil dieser Regeln ist über Outlook und Outlook im Web gar nicht sichtbar. Sie liegen als versteckte Regeln im Postfach und tauchen nur auf, wenn du in der Exchange Online PowerShell ausdrücklich danach fragst. Wer nur in der Oberfläche nachschaut und dort nichts findet, hat nicht bewiesen, dass es keine Regel gibt. Er hat bewiesen, dass er in der Oberfläche nachgeschaut hat.

Erkennungszeichen	Wo sichtbar	Aussagekraft	Nächster Schritt
Leaked Credentials	Entra ID Protection, Risikoerkennungen	Sehr hoch: Kennwort bestätigt geleakt	Kennwort sofort, unabhängig von weiteren Signalen
Erfolgreiche Anmeldung nach Password Spray	Entra ID Protection	Hoch	Sitzungen widerrufen, Konto prüfen
Anmeldung aus unmöglicher Entfernung	Anmeldeprotokoll, Defender for Cloud Apps	Hoch, sofern kein VPN im Spiel ist	Zweites Signal suchen, dann Playbook starten
Unbekannte Anmeldeeigenschaften	Entra ID Protection	Mittel: braucht Kontext	Person anrufen. Wirklich anrufen, nicht mailen
Anomalous Token	Entra ID Protection	Mittel, bei niedriger Stufe oft Fehlalarm	Nicht-interaktive Anmeldungen im Umfeld prüfen
Neue Postfachregel, unauffälliger Name	Purview Audit, Get-InboxRule -IncludeHidden	Sehr hoch	Regel sichern, dann löschen. Playbook starten
Externe Weiterleitung neu gesetzt	Get-Mailbox, Berichte zu automatischer Weiterleitung	Sehr hoch	Weiterleitung entfernen, Zeitraum eingrenzen
Neuer Consent für eine unbekannte App	Entra ID, Unternehmensanwendungen	Hoch	Berechtigungen ansehen, Zustimmung entziehen

Zusätzliche MFA-Methode registriert	Entra ID, Authentifizierungsmethoden	Sehr hoch, wenn zeitlich passend	Methode entfernen, bevor du das Kennwort setzt
Postfach darf nicht mehr senden	Defender, Eingeschränkte Entitäten	Hoch: es wurde bereits Spam verschickt	Erst aufräumen, dann Sperre aufheben

Tabelle 1: Erkennungszeichen, sortiert nach dem, was du daraus ableiten kannst. Die rechte Spalte ist die Frage, die du als Nächstes beantwortest.

Wenn du dir die Kette einmal von der anderen Seite ansiehst, wird klar, warum die Postfachregel und der App-Consent so wichtig sind: Sie sind die beiden Bausteine, mit denen sich der Angreifer unabhängig von deinem Kennwort macht.

Die Kette: von der Mail zur falschen Rechnung

Typischer Verlauf eines Kontoübernahme-Falls. Die Zeitangaben sind Erfahrungswerte, keine Garantie.



Der bittere Teil

Bemerkt wird die Sache meistens erst bei Stufe 6 — wenn ein Kunde anruft und fragt, warum die Kontonummer im Impressum eine andere ist als in der Rechnung. Zwischen Stufe 3 und diesem Anruf liegen im Mittelstand oft Wochen. Die Stufen 4 und 5 sind genau die, die dein Aufräumen später wieder zunichtemachen, wenn du sie überspringst.

Angreifer brauchen keine Sicherheitslücke. Sie brauchen eine Sitzung.

Skizze 2: Der typische Verlauf. Die Stufen 4 und 5 sind die Rückversicherung des Angreifers — und genau die Schritte, die beim Aufräumen am häufigsten vergessen werden.

WARNUNG · Der teuerste Irrtum in diesem Thema

„Wir haben das Kennwort geändert, damit ist die Sache erledigt.“ Nein. Eine Postfachregel läuft ohne jede Anmeldung weiter. Eine OAuth-Zustimmung hat einen eigenen Token mit eigenem Lebenszyklus. Ein App-Kennwort wird beim Zurücksetzen nicht automatisch widerrufen. Wer nur das Kennwort tauscht, hat die Vordertür abgeschlossen und die Terrassentür offen gelassen.

Die Aufräumreihenfolge: acht Schritte, in genau dieser Folge

Die Reihenfolge ist kein Ordnungsfimmel. Jeder Schritt sichert das Ergebnis des vorherigen ab, und jeder übersprungene Schritt erzeugt eine Lücke, durch die die Arbeit wieder zunichtegemacht wird. Wer mit dem Kennwort anfängt, während die Sitzung des Angreifers noch läuft, hat dem Angreifer gerade mitgeteilt, dass er entdeckt wurde — und ihm die Zeit gelassen, sich eine zweite Tür einzubauen.

Vorher: drei Entscheidungen in fünf Minuten

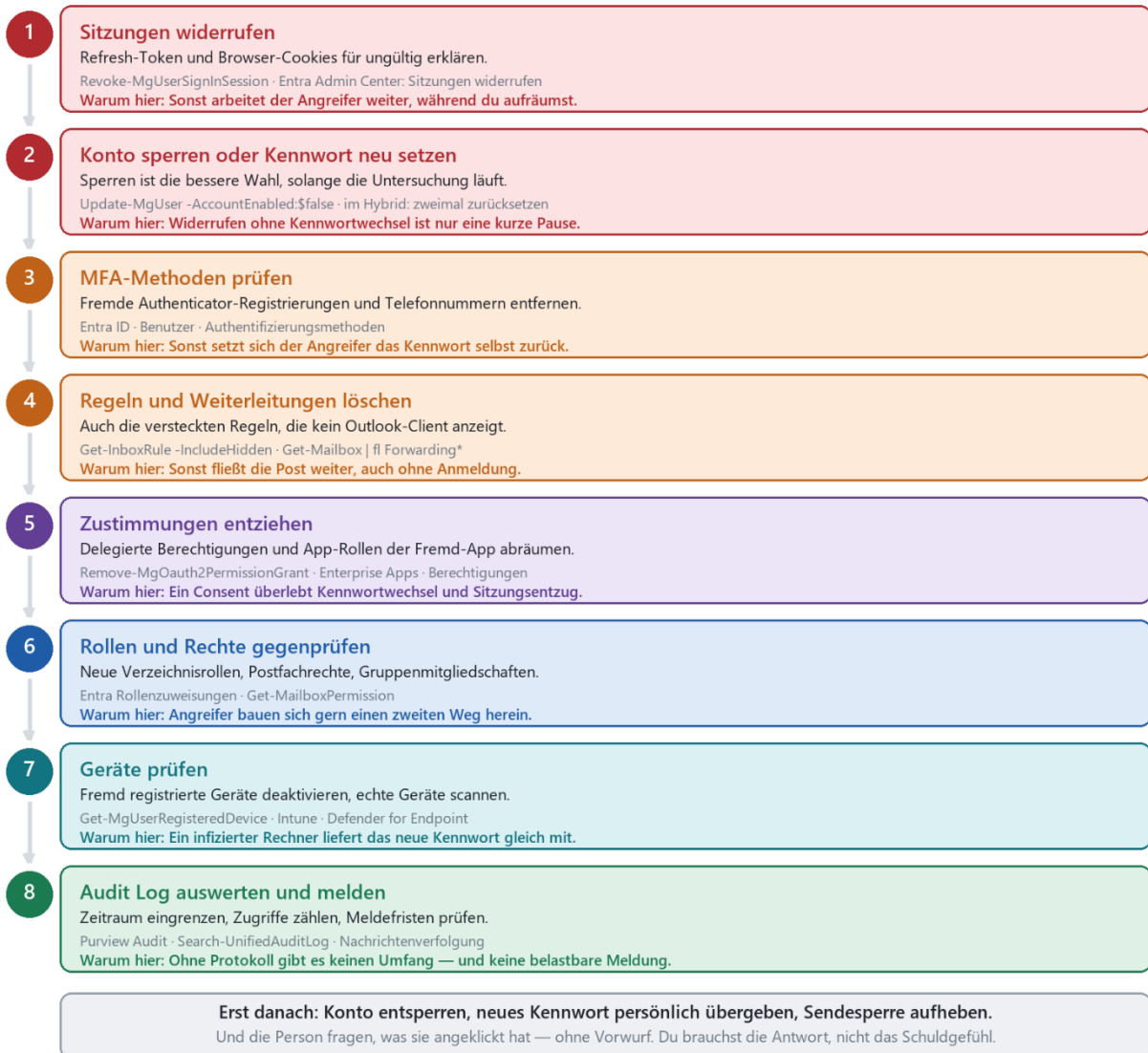
Erstens: sperren oder nur widerrufen? Solange die Untersuchung läuft, ist das Sperren des Kontos die deutlich bessere Wahl, und Microsoft empfiehlt genau das als ersten Schritt. Es kostet die betroffene Person einen halben Arbeitstag und dir zwei unangenehme Telefonate, verhindert aber, dass du gegen einen aktiven Angreifer aufräumst. Wenn es sich um die Geschäftsführung am Tag der Bilanzpressekonferenz handelt, triffst du eine andere Entscheidung — aber triff sie bewusst und schreib sie auf.

Zweitens: Wer darf das eigentlich? Für das Deaktivieren normaler Konten reicht die Rolle „Benutzeradministrator“. Für administrative Konten brauchst du „Privilegierter Authentifizierungsadministrator“, für das Deaktivieren von Geräten mindestens „Cloudgeräteadministrator“. Diese Zuordnung klärst du besser vorher als um 22 Uhr am Freitag. Wenn deine Notfallkonten nicht sauber sind, wird es an dieser Stelle schmerzhaft — dazu mehr in unserem Beitrag zu Break-Glass-Konten.

Drittens: Beweise sichern, bevor du löschst. Die Postfachregel, die du gleich entfernst, ist dein bester Beleg dafür, dass es sich um einen Vorfall und nicht um ein Missverständnis handelt. Exportiere sie, bevor sie weg ist. Das Gleiche gilt für die Liste der Anwendungsberechtigungen und für die Anmeldeereignisse des betroffenen Zeitraums. Der Ablauf gehört in deinen [Incident-Response-Plan für Microsoft 365](#) — nicht in den Kopf des einen Kollegen, der gerade im Urlaub ist.

Die Aufräum-Reihenfolge

Von oben nach unten abarbeiten. Wer eine Zeile überspringt, fängt später von vorn an.



Reihenfolge nach der Praxis; Schritte 1 bis 6 entsprechen dem Ablauf in der Microsoft-Dokumentation.

Skizze 3: Die Aufräum-Reihenfolge. Von oben nach unten, ohne Auslassungen. Die Zeile „Warum hier“ ist der Grund, aus dem die Reihenfolge nicht beliebig ist.

Schritt 1 und 2: Sitzungen widerrufen, Konto stilllegen

Diese beiden Schritte gehören zusammen und sollten innerhalb derselben Minute passieren. Das Widerrufen der Sitzungen entwertet die Aktualisierungstoken und setzt die Gültigkeit der Browser-Sitzungscookies zurück. Das Sperren verhindert, dass sich der Angreifer mit dem weiterhin bekannten Kennwort einfach neu anmeldet. Nur eines von beiden zu tun, ist ungefähr so wirksam wie eine Hälfte eines Türschlosses.

```
# Microsoft Graph PowerShell
Connect-MgGraph -Scopes "User.ReadWrite.All", "User.RevokeSessions.All"

$u = Get-MgUser -Search "UserPrincipalName:anna.beispiel@contoso.de" -ConsistencyLevel eventual
```

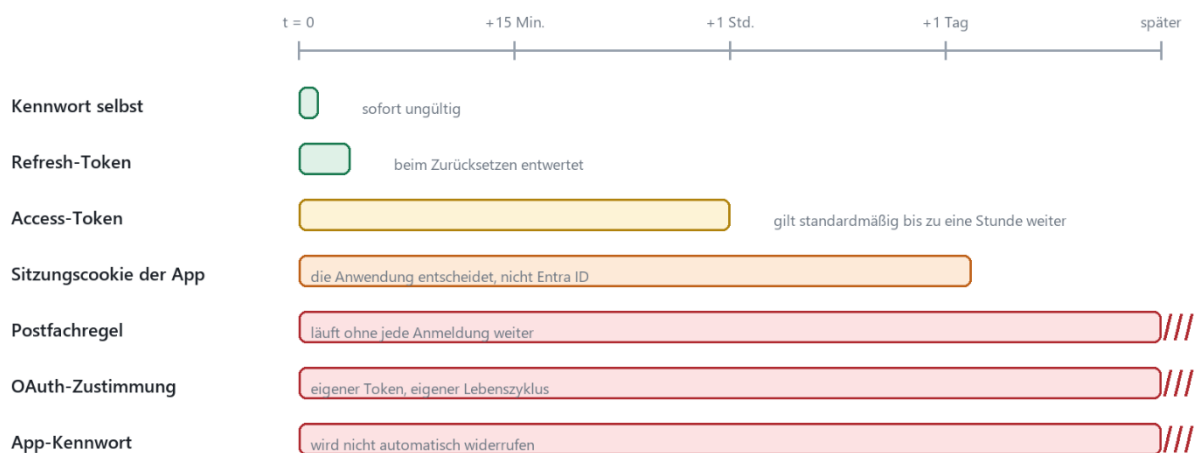
```
# 1. Sitzungen widerrufen: Refresh-Token und Browser-Cookies entwerten
Revoke-MgUserSignInSession -UserId $u.Id
```

```
# 2. Konto sperren, solange die Untersuchung läuft
Update-MgUser -UserId $u.Id -AccountEnabled:$false
```

Was du dabei im Kopf behalten musst: Zugriffstoken sind standardmäßig bis zu eine Stunde gültig, und Entra ID kann ein Sitzungstoken, das eine Anwendung selbst ausgestellt hat, gar nicht widerrufen. Das erledigt die Anwendung nach ihren eigenen Regeln. Continuous Access Evaluation verkürzt dieses Fenster für unterstützte Anwendungen auf wenige Minuten — das ist einer der handfestesten Gründe, warum du CAE aktiv haben willst, bevor du sie brauchst.

Was nach dem Kennwortwechsel noch lebt

Zeitstrahl ab dem Moment, in dem du das neue Kennwort gesetzt hast.



Deshalb die Reihenfolge

Der Kennwortwechsel schließt die Vordertür. Regel, Zustimmung und App-Kennwort sind Fenster im Erdgeschoss, die davon gar nichts mitbekommen. Continuous Access Evaluation verkürzt die gelbe Zone auf wenige Minuten — aber nur für Anwendungen, die es unterstützen, und nur für Token, nicht für Regeln.

Token-Lebensdauern nach der Microsoft-Dokumentation; Access-Token standardmäßig eine Stunde.

Skizze 4: Was nach dem Kennwortwechsel noch weiterläuft. Die roten Balken enden nicht von selbst — sie enden nur, wenn du sie beendest.

Schritt 3: das Kennwort — und der Doppelreset im Hybrid

Jetzt erst kommt das neue Kennwort. Es muss stark sein, es darf keines der letzten fünf sein, und es geht auf keinen Fall per E-Mail an die betroffene Person — der Angreifer sitzt möglicherweise noch im Postfach und liest mit. Telefon. Persönlich. Notfalls über die Führungskraft. Aber nicht über den Kanal, der gerade kompromittiert ist.

Wenn das Konto aus dem lokalen Active Directory synchronisiert wird, setzt du das Kennwort dort zurück, und zwar zweimal hintereinander. Der Grund ist die Replikation und das Risiko von Pass-the-Hash-Angriffen: Ein einzelner Reset kann unter ungünstigen Umständen einen alten Hash noch eine Weile brauchbar lassen. Bei föderierten Identitäten gilt ohnehin, dass die Änderung in der lokalen Umgebung erfolgen muss. Und die App-Kennwörter, falls in deinem Tenant noch

welche existieren, musst du gesondert löschen und neu anlegen — die werden beim Zurücksetzen nicht automatisch ungültig.

WICHTIG · App-Kennwörter sind ein Warnsignal für sich

Wenn in deinem Tenant überhaupt noch App-Kennwörter im Einsatz sind, hast du ein zweites Problem: Es gibt dort Anwendungen, die modernes Authentifizierungsverfahren nicht beherrschen. Diese Baustelle löst du nicht im Vorfall, sondern davor — siehe [Legacy Authentication endgültig abschalten](#).

Schritt 4: MFA-Methoden prüfen — der am häufigsten vergessene Schritt

Hier scheitern in der Praxis die meisten Aufräumaktionen. Ein Angreifer, der einmal drin war, registriert sich gern eine eigene Authenticator-Instanz oder hinterlegt eine Telefonnummer als SMS-Methode. Danach kann er die Selbstbedienungsfunktion für Kennworrücksetzung benutzen — und sich das Kennwort, das du gerade so sorgfältig gesetzt hast, selbst wieder ändern. Du merkst das typischerweise dann, wenn die betroffene Person zwei Tage später erneut anruft.

Also: In den Authentifizierungsmethoden des Kontos jede Methode durchgehen und mit der Person abgleichen. Alles, was sie nicht zuordnen kann, fliegt raus. Danach lässt du sie die verbliebene Methode neu registrieren — am besten gleich mit einem phishing-resistenten Verfahren, wenn dein Tenant das hergibt. Eine Kontoübernahme ist der Moment, in dem der Widerstand gegen Passkeys erfahrungsgemäß am geringsten ist.

Schritt 5: Regeln und Weiterleitungen, auch die unsichtbaren

Jetzt das Postfach. Zwei verschiedene Mechanismen sind zu prüfen, und sie liegen an unterschiedlichen Stellen: die Weiterleitung auf Postfachebene und die Posteingangsregeln.

```
# Exchange Online PowerShell
Connect-ExchangeOnline

# a) Weiterleitung auf Postfachebene (SMTP-Forwarding)
Get-Mailbox -Identity anna.beispiel@contoso.de |
  Format-List Forwarding*Address,DeliverTo*

# b) Alle Regeln, inklusive der versteckten
Get-InboxRule -Mailbox anna.beispiel@contoso.de -IncludeHidden |
  Format-List Name,Enabled,RedirectTo,Forward*,Identity

# c) Eine verdächtige Regel im Detail ansehen, bevor du sie löschst
Get-InboxRule -Identity "anna\10210541742734704641" -IncludeHidden | Format-List
```

Bei der Weiterleitung auf Postfachebene achtest du auf drei Eigenschaften. „ForwardingAddress“ mit Inhalt bedeutet Weiterleitung an einen internen Empfänger. „ForwardingSmtpAddress“ mit Inhalt bedeutet Weiterleitung nach außen — das ist der Klassiker. Und „DeliverToMailboxAndForward“ verrät dir, ob die Nachricht zusätzlich noch im Postfach ankommt: Steht dort „False“, sieht die betroffene Person gar nichts mehr, was ein sehr eindeutiges Signal ist.

Bei den Regeln interessieren dich „RedirectTo“, „ForwardTo“ und „ForwardAsAttachmentTo“. Jeder nicht leere Wert ist ein Befund. Der Parameter „-IncludeHidden“ ist dabei nicht optional, sondern der eigentliche Punkt der Übung: Ohne ihn siehst du genau das, was auch die Anwenderin in Outlook sieht — und das ist bekanntlich nichts.

TIPP · Nicht nur löschen, auch weiterdenken

Wenn du eine Zieladresse gefunden hast, such im gesamten Tenant nach anderen Regeln, die auf dieselbe Adresse zeigen. In der erweiterten Suche in Defender XDR geht das in einer einzigen Abfrage über die Tabelle CloudAppEvents und die Aktionstypen New-InboxRule, Set-InboxRule und Set-Mailbox. Sehr oft ist nicht ein Konto betroffen, sondern drei — und die anderen beiden hat bisher niemand bemerkt.

Schritt 6: Zustimmungen entziehen

Der App-Consent ist die eleganteste Hintertür, die Microsoft 365 zu bieten hat, und zwar deshalb, weil sie vollkommen legitim aussieht. Die Anwendung heißt „Mail Backup Pro“ oder „O365 Security Scanner“, sie hat delegierte Berechtigungen auf Mail.Read und offline_access, und sie funktioniert nach dem Kennwortwechsel munter weiter. Kein Sitzungswiderruf berührt sie, weil sie ihre eigenen Token besitzt.

```
Connect-MgGraph -Scopes "Application.ReadWrite.All", "DelegatedPermissionGrant.ReadWrite.All",
    "AppRoleAssignment.ReadWrite.All"

$sp = Get-MgServicePrincipal -Filter "displayName eq 'Mail Backup Pro'"

# Delegierte Berechtigungen entfernen
Get-MgOAuth2PermissionGrant -All |
    Where-Object { $_.ClientId -eq $sp.Id } |
    ForEach-Object { Remove-MgOAuth2PermissionGrant -OAuth2PermissionGrantId $_.Id }

# Anwendungsberechtigungen (App-Rollen) entfernen
Get-MgServicePrincipalAppRoleAssignment -ServicePrincipalId $sp.Id -All |
    Where-Object { $_.PrincipalType -eq "ServicePrincipal" } |
    ForEach-Object { Remove-MgServicePrincipalAppRoleAssignedTo -ServicePrincipalId $sp.Id -
        AppRoleAssignmentId $_.Id }
```

Wichtig zu wissen: Das Entziehen einer Zustimmung hindert die Anwendung nicht daran, sie beim nächsten Mal einfach wieder anzufordern. Wenn du das verhindern willst, musst du die App im Tenant blockieren oder die Zustimmung durch Anwender grundsätzlich einschränken. Wie du das so einrichtest, dass es die Fachbereiche nicht lähmt, steht in [App-Registrierungen und Consent-Governance](#). Wenn dir dieser Vorfall gerade zeigt, dass jeder in deinem Tenant beliebigen Apps beliebige Rechte geben darf, hast du dort deine nächste Hausaufgabe gefunden.

Schritt 7 und 8: Rollen und Geräte

Prüfe, ob dem Konto in der fraglichen Zeit neue Verzeichnisrollen, Postfachberechtigungen oder Gruppenmitgliedschaften zugewachsen sind. Angreifer, die etwas mehr Zeit hatten, bauen sich gern einen zweiten Weg herein — ein Vollzugriffsrecht auf ein anderes Postfach etwa, das nach dem Aufräumen des ersten Kontos munter weiterfunktioniert.

Dann die Geräte. Registrierte Geräte, die die betroffene Person nicht kennt, deaktivierst du. Umgekehrt gilt: Wenn das Kennwort nicht über eine Phishing-Seite, sondern über einen Infostealer auf dem Arbeitsplatzrechner abgefließen ist, nützt dir das gesamte Aufräumen im Tenant nichts — das nächste Kennwort geht denselben Weg. Ein Blick in Defender for Endpoint auf das Gerät der betroffenen Person gehört deshalb zum Playbook, nicht in die Kategorie „machen wir, wenn wir Zeit haben“.

```
# Registrierte Geräte auflisten und bei Bedarf deaktivieren
Get-MgUserRegisteredDevice -UserId $u.Id -All |
  ForEach-Object { Update-MgDevice -DeviceId $_.Id -AccountEnabled:$false }
```

#	Schritt	Werkzeug	Benötigte Rolle	Dauer
1	Sitzungen widerrufen	Entra Admin Center oder Graph PowerShell	Benutzeradministrator	1 Min.
2	Konto sperren	Update-MgUser -AccountEnabled:\$false	Benutzeradministrator	1 Min.
3	Kennwort neu setzen	Admin Center, im Hybrid Set-ADAccountPassword (zweimal)	Benutzeradministrator, im Hybrid AD-Rechte	5 Min.
4	MFA-Methoden prüfen	Entra ID, Authentifizierungsmethoden	Authentifizierungsadministrator	10 Min.
5	Regeln und Weiterleitungen	Get-InboxRule -IncludeHidden, Get-Mailbox	Exchange-Administrator	15 Min.
6	Zustimmungen entziehen	Unternehmensanwendungen, Graph PowerShell	Cloudanwendungsadministrator	15 Min.
7	Rollen und Geräte	Rollenzuweisungen, Get-MgUserRegisteredDevice, Intune	Cloudgeräteadministrator	20 Min.
8	Audit Log auswerten	Purview Audit, Nachrichtenverfolgung	Auditprotokolle lesen	30 Min. bis Tage

Tabelle 2: Die acht Schritte mit Werkzeug, Rolle und realistischem Zeitbedarf. Die Summe liegt bei einer geübten Person unter zwei Stunden — vorausgesetzt, die Berechtigungen sind vorher geklärt.

WARNUNG · Das Konto ist noch nicht fertig, wenn die Liste abgehakt ist

Nach dem Aufräumen kommt das Zurücksetzen in den Normalbetrieb: Konto entsperren, neues Kennwort persönlich übergeben, und falls über das Postfach Spam verschickt wurde, das Konto von der Seite mit den eingeschränkten Entitäten entfernen. Diese Sendesperre hebst du erst auf, wenn alles andere erledigt ist — sonst verschickt der nächste Durchlauf des Angreifers gleich weiter.

Das Audit Log: vom Bauchgefühl zum belastbaren Umfang

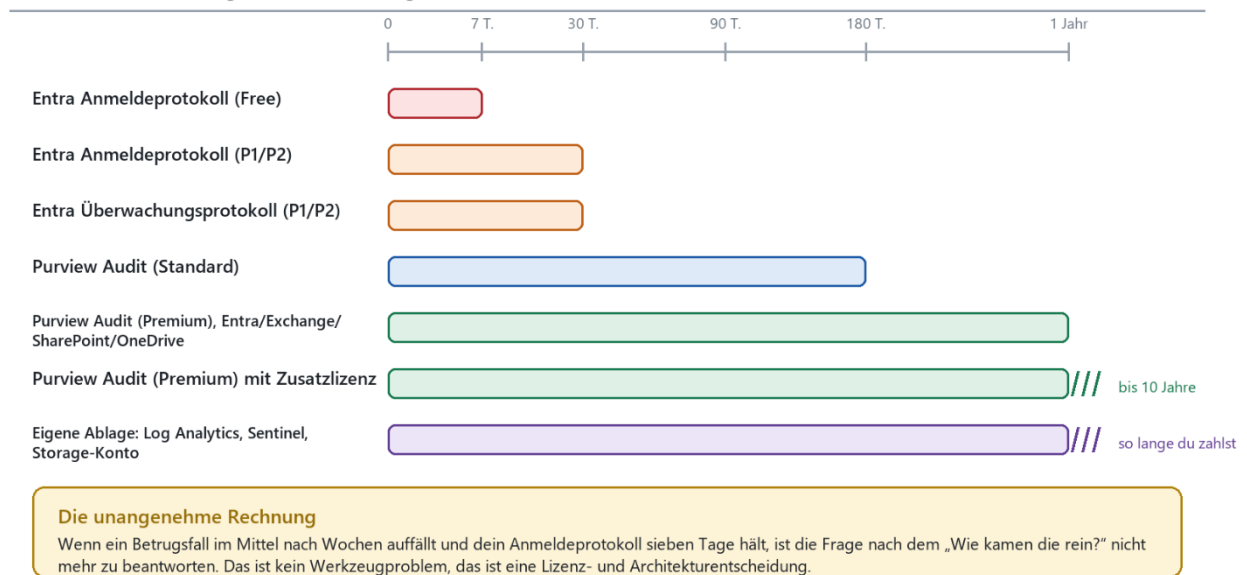
Bis hierher hast du den Angreifer draußen. Was du noch nicht hast, ist eine Antwort auf die Frage, die dir als Nächstes gestellt wird: Was hat er gesehen? Diese Frage kommt garantiert — von der Geschäftsführung, vom Datenschutzbeauftragten, im schlimmeren Fall von einer Aufsichtsbehörde. „Wir wissen es nicht“ ist eine zulässige Antwort, aber eine sehr teure.

Wo welches Protokoll liegt und wie lange

Microsoft 365 protokolliert an mehreren Stellen mit unterschiedlichen Aufbewahrungsfristen, und das ist der Punkt, an dem Lizenzentscheidungen aus der Vergangenheit plötzlich sehr gegenwärtig werden. Die Anmeldeprotokolle in Entra ID werden in der kostenfreien Ausgabe sieben Tage aufbewahrt, mit P1 oder P2 dreißig Tage. Das unified audit log in Microsoft Purview hält in der Standardvariante 180 Tage — das war bis Oktober 2023 übrigens noch 90 Tage. Mit Audit (Premium) werden Ereignisse aus Entra ID, Exchange, SharePoint und OneDrive standardmäßig ein Jahr lang aufbewahrt, und mit einer zusätzlichen Lizenz sind zehn Jahre möglich.

Wie lange dein Beweismaterial überlebt

Die Frist läuft ab dem Ereignis, nicht ab dem Tag, an dem du es merkst.



Aufbewahrung nach Microsoft-Dokumentation, Stand September 2026.

Skizze 5: Aufbewahrungsfristen im Vergleich. Die Frist läuft ab dem Ereignis. Wenn der Vorfall vier Wochen alt ist, sind einige dieser Balken bereits abgelaufen.

Rechne das einmal gegen die Realität: Zwischen der Übernahme eines Kontos und dem Moment, in dem jemand den Betrug bemerkt, liegen im Mittelstand regelmäßig Wochen. Wenn dein Anmeldeprotokoll sieben Tage hält, ist die Frage „Wie sind die reingekommen?“ zu diesem Zeitpunkt nicht mehr beantwortbar. Das ist kein Werkzeugproblem, sondern eine Architekturentscheidung, die du am besten triffst, bevor du sie brauchst. Alles Wichtige zu den Auswertungswerkzeugen findest du im [Kompetenzbereich Microsoft Purview](#); ob sich eine Weiterleitung in ein SIEM lohnt, klärt [Microsoft Sentinel anbinden: wann es sich lohnt](#).

Die drei Fragen, die du beantworten musst

Halte die Auswertung fokussiert. Es geht nicht darum, das gesamte Protokoll zu lesen, sondern drei Fragen zu beantworten.

1. Wann hat der Zugriff begonnen und wann endete er? Setz den Suchzeitraum bewusst früher an als das erste auffällige Ereignis und filtere zunächst nicht auf einzelne Aktivitäten. Angreifer melden sich oft Tage vorher zum ersten Mal an, um zu schauen, ob die Zugangsdaten überhaupt funktionieren.

2. Was wurde gelesen oder abgezogen? Mit Audit (Premium) gibt es das Ereignis MailItemsAccessed, das dir zeigt, welche Elemente im Postfach angefasst wurden — inklusive der Vertraulichkeitsbezeichnung des Elements. Für SharePoint und OneDrive gibt es die entsprechenden Zugriffs- und Downloadereignisse.
3. Was wurde verschickt? Die Nachrichtenverfolgung im Defender-Portal und der Ordner „Gesendete Elemente“ zeigen dir, was in deinem Namen hinausgegangen ist. Diese Liste brauchst du für die Frage, wen du informieren musst — deine Kundschaft interessiert nämlich weniger dein Tenant als die Frage, ob die Rechnung von letzter Woche echt war.

FAKTEN · Ein Detail, das oft übersehen wird

Prüfe im Überwachungsprotokoll ausdrücklich die Aktivitäten „New-InboxRule“, „Set-InboxRule“, „Set-Mailbox“, „Add-MailboxPermission“ und „Consent to application“. Diese fünf erzählen dir, ob der Angreifer nur geschaut oder sich eingerichtet hat — und das ist der Unterschied zwischen einem ärgerlichen Zwischenfall und einem meldepflichtigen Vorfall.

Mitbestimmung: wer darf da eigentlich hineinschauen?

Ein Punkt, den technische Playbooks gern auslassen: Die Auswertung von Anmelde- und Aktivitätsprotokollen einer namentlich bekannten Person ist in Deutschland kein rein technischer Vorgang. Im akuten Vorfall ist die Rechtslage in der Regel unproblematisch, weil ein berechtigtes Interesse an der Aufklärung besteht — aber „wir schauen mal eben ins Protokoll“ als Dauerzustand ist etwas anderes als eine anlassbezogene Auswertung. Welche Regelungen du dafür brauchst und wie eine tragfähige Vereinbarung aussieht, steht in [Security-Monitoring und Betriebsrat: was mitbestimmungspflichtig ist](#). Kläre das vorher. Im Vorfall ist die Diskussion mit dem Betriebsrat der denkbar schlechteste Zeitpunkt.

Quelle	Beantwortet	Aufbewahrung	Voraussetzung
Entra Anmeldeprotokoll	Wann, von wo, mit welchem Gerät, erfolgreich?	7 Tage (Free), 30 Tage (P1/P2)	im Tenant vorhanden
Entra Überwachungsprotokoll	Welche Verzeichnisänderungen, welche Consents?	7 bzw. 30 Tage	im Tenant vorhanden
Purview Audit (Standard)	Postfach-, SharePoint-, Teams-Aktivitäten	180 Tage	standardmäßig aktiv
Purview Audit (Premium)	Zusätzlich MailItemsAccessed, Suchvorgänge, Send	1 Jahr, mit Zusatzlizenz 10 Jahre	E5, Purview Suite oder Add-on
Nachrichtenverfolgung	Was ging hinaus, an wen, mit welchem Ergebnis?	90 Tage (Detailsuche kürzer)	Exchange Online
Defender for Cloud Apps	Verhaltensauffälligkeiten, unmögliche Reisen	abhängig von der Konfiguration	Lizenz und Anbindung nötig
Log Analytics oder Sentinel	Alles, was du dorthin weiterleitest	so lange du zahlst	Diagnoseeinstellungen konfiguriert

Tabelle 3: Welche Quelle welche Frage beantwortet. Wenn eine Zeile in deinem Tenant nicht verfügbar ist, weißt du, wo deine Auskunftsfähigkeit endet.

Meldepflicht: die Uhren, die parallel laufen

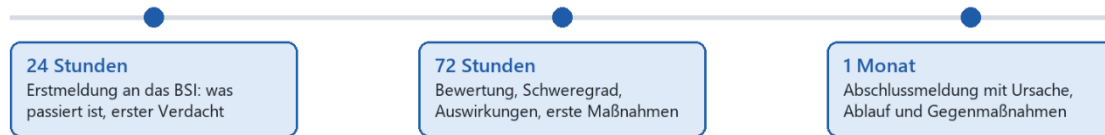
Sobald klar ist, dass ein Konto tatsächlich übernommen wurde, starten Fristen — und zwar mehrere gleichzeitig, mit unterschiedlichen Adressaten. Die schlechte Nachricht: Sie beginnen mit

der Kenntnis vom Vorfall, nicht mit dem Abschluss deiner Analyse. Die gute: Eine unvollständige Meldung innerhalb der Frist ist immer besser als eine vollständige danach.

Die Uhren, die parallel laufen

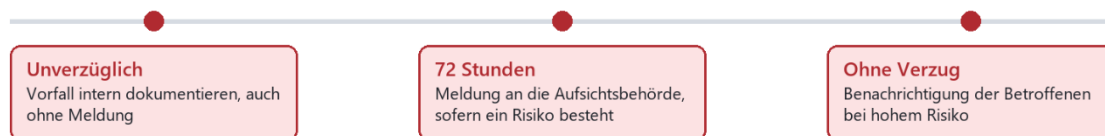
Beginn ist die Kenntnis vom Vorfall, nicht der Abschluss der Analyse.

§ 32 BSIG (NIS2) — nur für besonders wichtige und wichtige Einrichtungen



Das NIS2-Umsetzungsgesetz gilt in Deutschland seit dem 6. Dezember 2025. Rund 29.500 Einrichtungen fallen darunter.

Art. 33 und 34 DSGVO — für jeden, der personenbezogene Daten verarbeitet



Ein übernommenes Postfach enthält fast immer personenbezogene Daten Dritter. Die Frist läuft auch am Wochenende.

Keine Rechtsberatung. Sprich die Fristen mit Datenschutzbeauftragung und Rechtsabteilung ab.

Skizze 6: Zwei Fristenlogiken, die nebeneinander laufen. Welche für dich gilt, hängt von deiner Branche und von der Art der betroffenen Daten ab — häufig gelten beide.

Die datenschutzrechtliche Uhr betrifft praktisch jeden. Ein übernommenes Postfach enthält fast immer personenbezogene Daten Dritter: Kundendaten, Bewerbungsunterlagen, Krankmeldungen, Gehaltsabrechnungen. Nach Artikel 33 DSGVO ist die Verletzung des Schutzes personenbezogener Daten innerhalb von 72 Stunden nach Bekanntwerden an die zuständige Aufsichtsbehörde zu melden, sofern ein Risiko für die Betroffenen besteht. Besteht ein hohes Risiko, kommt nach Artikel 34 die Benachrichtigung der betroffenen Personen dazu. Auch wenn du zu dem Schluss kommst, nicht melden zu müssen, dokumentierst du den Vorfall intern — die Entscheidung selbst musst du begründen können.

Die zweite Uhr ist neu und trifft deutlich mehr Häuser, als vielen bewusst ist. Das NIS2-Umsetzungsgesetz gilt in Deutschland seit dem 6. Dezember 2025, eine materielle Übergangsfrist gibt es nicht. Nach § 32 des neu gefassten BSI-Gesetzes gilt ein gestuftes Verfahren: Erstmeldung binnen 24 Stunden, Folgemeldung mit Bewertung binnen 72 Stunden, Abschlussmeldung binnen eines Monats nach der 72-Stunden-Meldung. Rund 29.500 Einrichtungen fallen in Deutschland darunter. Ob du dazugehörst und was das technisch bedeutet, klärt [NIS2 aus Security-Sicht: technische Maßnahmen in M365](#).

Adressat	Auslöser	Frist	Inhalt
Aufsichtsbehörde Datenschutz	Risiko für Betroffene	72 Stunden ab Kenntnis	Art und Umfang, Kategorien und Zahl der Betroffenen, Folgen, Maßnahmen
Betroffene Personen	hohes Risiko	unverzüglich	verständliche Beschreibung, Ansprechpartner, Empfehlungen
BSI	erheblicher Sicherheitsvorfall, sofern NIS2-pflichtig	24 h / 72 h / 1 Monat	Erstmeldung, Bewertung, Abschlussbericht

Geschäftsführung	immer	sofort	Was ist passiert, was ist der mögliche Schaden, was läuft gerade
Versicherung	wenn Cyberpolice vorhanden	laut Vertrag, oft 24 bis 72 Stunden	Verspätete Meldung kann den Versicherungsschutz kosten
Kundschaft und Partner	wenn in ihrem Namen kommuniziert wurde	so schnell wie möglich	Konkrete Warnung vor gefälschten Rechnungen oder Bankdaten

Tabelle 4: Wer wann was erfährt. Die letzte Zeile ist die, die im Playbook am häufigsten fehlt — und die mit dem größten Effekt auf den tatsächlichen Schaden.

WICHTIG · Die Warnung nach außen ist keine Kür

Wenn aus dem Postfach heraus Nachrichten an Kunden gegangen sind, ist die schnelle, konkrete Warnung an genau diese Empfänger die wirksamste Schadensbegrenzung, die dir zur Verfügung steht. Sie kostet dich eine unangenehme Stunde. Eine überwiesene Zahlung auf ein fremdes Konto kostet erheblich mehr — und lässt sich nach wenigen Tagen praktisch nicht mehr zurückholen.

Damit der nächste Fall langweiliger wird

Ein Vorfall ist ein schlechter Lehrer, aber ein sehr überzeugender. Nutze das Zeitfenster, in dem alle noch beeindruckt sind, für die zwei oder drei Maßnahmen, die dieselbe Kette beim nächsten Mal früher unterbrechen. Nicht für zwanzig.

Die drei Maßnahmen mit dem besten Verhältnis

Erstens: Sitzungsschutz statt nur zweiter Faktor. Der beschriebene Angriff funktioniert, weil das Sitzungscookie gestohlen wird — die MFA-Abfrage hat der Angreifer ja bestanden, du hast sie ihm nur durchgereicht. Dagegen helfen phishing-resistente Verfahren und Richtlinien, die Gerätekonformität verlangen. Der Einstieg steht in [Passwordless: FIDO2 und Passkeys in der Praxis](#) und in [Conditional Access: Baselines, die nicht nerven](#).

Zweitens: Benachrichtigungen, die tatsächlich jemand liest. Eine neue externe Weiterleitung, eine neue Regel mit Weiterleitung, ein neuer Consent mit weitreichenden Berechtigungen — das sind drei Ereignisse, für die du eine Alarmierung haben willst, und zwar mit einem benannten Empfänger. Wie du das aufsetzt, ohne im Rauschen zu ertrinken, steht in [Alert Policies und Benachrichtigungen richtig aufsetzen](#).

Drittens: die Übung. Der beschriebene Ablauf funktioniert nur, wenn die Berechtigungen vorher geklärt sind, die Skripte griffbereit liegen und jemand weiß, wo die Telefonnummer der Datenschutzbeauftragten steht. Das trainierst du nicht im Ernstfall. Wie eine solche Übung abläuft, beschreibt [Feuerwehrübung: Security-Notfälle im Team trainieren](#); wie du deine Belegschaft auf die Köder vorbereitest, ohne sie zu beschämen, steht in [Attack Simulation Training: Phishing-Übungen richtig aufsetzen](#).

Weiterlesen zu diesem Handlungsfeld

- › [Phishing-Vorfall: die ersten 60 Minuten](#) — was vor diesem Playbook passiert
- › [App-Registrierungen und Consent-Governance](#) — damit Schritt 6 beim nächsten Mal nicht nötig ist
- › [Kompetenzbereich Microsoft Purview](#) — Auditprotokolle, Aufbewahrung, Auswertung

- › [Incident-Response-Plan für Microsoft 365](#) — der Rahmen, in den dieses Playbook gehört
- › [Tenant-Härtung: die 20 wichtigsten Schrauben](#) — die Basis, die diesen Fall unwahrscheinlicher macht
- › [Defender for Cloud Apps im Mittelstand](#) — Verhaltenserkennung für genau diese Muster
- › [Ransomware-Vorsorge in Microsoft 365](#) — wenn aus dem Konto mehr wird
- › [Dossier: TerminalFix und der Berlin-Hack](#) — wie so etwas in der Praxis eskaliert

TIPP • Wenn du das nicht allein machen willst

Wir begleiten Kontoübernahmen von der Erkennung bis zur Abschlussmeldung und bauen anschließend die Härtung, die den gleichen Weg schließt — siehe [Microsoft 365 Security Beratung](#). Für Teams, die das selbst können sollen, gibt es die passende [Schulung Microsoft 365 Security](#), in der dieses Playbook einmal komplett am Tenant durchgespielt wird.

Häufige Fragen

Wie schnell muss ich reagieren, wenn ich einen Verdacht habe?

Sitzungen widerrufen und Konto sperren dauert zusammen zwei Minuten und ist umkehrbar. Wenn sich der Verdacht als Fehlalarm herausstellt, hat es die betroffene Person einen halben Vormittag gekostet. Wenn er sich bestätigt und du gewartet hast, hat es dich möglicherweise eine fünfstellige Überweisung gekostet. Die Rechnung ist eindeutig: Bei begründetem Verdacht handelst du sofort und klärst danach.

Reicht es nicht, das Kennwort zu ändern und MFA einzuschalten?

Nein, und das ist der wichtigste Satz in diesem Beitrag. Eine Postfachregel läuft ohne jede Anmeldung weiter. Eine OAuth-Zustimmung besitzt eigene Token und interessiert sich nicht für dein neues Kennwort. Eine zusätzlich registrierte MFA-Methode erlaubt dem Angreifer, das Kennwort selbst wieder zurückzusetzen. Kennwort und MFA sind Schritt 3 und 4 von acht — nicht das ganze Playbook.

Woher weiß ich, ob es versteckte Posteingangsregeln gibt?

Nur über die Exchange Online PowerShell mit dem Parameter „-IncludeHidden“. Weder Outlook noch Outlook im Web zeigen diese Regeln an. Wenn du in der Oberfläche nachschaust und nichts findest, ist das kein Freispruch. Der Befehl steht weiter oben im Abschnitt zur Aufräumreihenfolge.

Was mache ich, wenn der Vorfall schon Wochen zurückliegt?

Erst aufräumen, dann rekonstruieren, was noch rekonstruierbar ist. Anmeldeprotokolle sind je nach Lizenz nach sieben oder dreißig Tagen weg, das unified audit log hält in der Standardvariante 180 Tage. Was fehlt, fehlt — dokumentiere die Lücke ehrlich, statt sie zu überspielen. Für die Meldung an eine Aufsichtsbehörde ist „Umfang aufgrund abgelaufener Protokollierung nicht abschließend feststellbar“ eine schmerzhaft, aber korrekte Aussage. Und ein guter Anlass, die Aufbewahrung zu ändern.

Sollte ich das Konto sperren oder nur das Kennwort ändern?

Sperren, solange die Untersuchung läuft — so empfiehlt es auch Microsoft. Das Sperren ist die einzige Maßnahme, bei der du sicher sein kannst, dass dir während des Aufräumens niemand dazwischenfunkt. Wenn geschäftliche Gründe dagegensprechen, ist das eine legitime Abwägung — dann dokumentierst du sie und arbeitest die Schritte besonders zügig ab.

Wie erkenne ich, ob weitere Konten betroffen sind?

Über zwei Wege. Erstens die Zieladresse: Such im Tenant nach anderen Regeln oder Weiterleitungen, die dieselbe externe Adresse verwenden. Zweitens die Herkunft: Such nach anderen Anmeldungen aus derselben IP-Adresse oder demselben Netzbetreiber im fraglichen Zeitraum. In der Praxis ist es selten nur ein Konto — dieselbe Phishing-Welle hat meistens mehrere Personen erwischt.

Muss ich den Vorfall wirklich melden?

Das ist keine IT-Entscheidung. Die Bewertung nach Artikel 33 DSGVO trifft die Datenschutzbeauftragte zusammen mit der Rechtsabteilung oder der Geschäftsführung — deine Aufgabe ist es, ihnen innerhalb weniger Stunden belastbare Fakten zu liefern: Zeitraum, betroffene Datenkategorien, Zahl der Betroffenen, was nachweislich abgeflossen ist. Wenn dein Haus unter NIS2 fällt, läuft parallel die 24-Stunden-Frist gegenüber dem BSI. Beide Uhren starten mit der Kenntnis, nicht mit dem Abschluss der Analyse.

Was sage ich der Person, deren Konto übernommen wurde?

Dass es nicht ihre Schuld ist, und dass sie dir jetzt sehr helfen kann. Moderne Phishing-Seiten sind vom Original nicht zu unterscheiden, und die MFA-Abfrage haben sie ja durchgereicht. Wer Schuldgefühle erzeugt, bekommt beim nächsten Mal keine Meldung mehr, sondern ein stilles Hoffen, dass es schon nichts war. Genau das ist der Zustand, in dem aus zwei Stunden Aufräumen ein Schadensfall wird.

Fazit

Eine Kontoübernahme in Microsoft 365 ist kein technisch anspruchsvoller Angriff. Sie ist eine Anmeldung, die nicht hätte stattfinden dürfen — und alles, was danach kommt, ist normale Nutzung des Systems mit fremden Absichten. Genau deshalb funktioniert das Aufräumen auch nicht nach Gefühl, sondern nur nach Liste.

Die Reihenfolge ist der eigentliche Inhalt dieses Playbooks: erst die Sitzungen, dann das Konto, dann die Faktoren, dann die Regeln, dann die Zustimmungen, dann Rollen und Geräte, dann das Protokoll. Wer bei Schritt drei aufhört, weil das Kennwort ja jetzt neu ist, hat den Angreifer nicht ausgesperrt, sondern nur kurz irritiert.

Das Zweite, was hängen bleiben sollte: Deine Auskunftsfähigkeit entscheidet sich lange vor dem Vorfall. Ob du in vier Wochen noch sagen kannst, was passiert ist, hängt an Lizenzen und Aufbewahrungsrichtlinien, die du heute konfigurierst — nicht an dem, was du am Tag des Vorfalls tust. Ein Playbook ohne Protokolle ist eine Aufräumaktion ohne Bericht.

Und das Dritte: Übe das. Zwei Stunden mit dem Team an einem Testkonto, einmal im Jahr, ersetzen jede Aufregung am echten Tag. Wenn die Rollen geklärt sind, die Befehle griffbereit liegen und jeder weiß, wer die Geschäftsführung anruft, ist eine Kontoübernahme das, was sie sein sollte: ein unangenehmer, aber beherrschbarer Vormittag.