

Attack Simulation Training: Phishing-Übungen richtig aufsetzen

Es gibt zwei Sorten von Phishing-Übungen. Die erste sieht so aus: Jemand aus der IT verschickt an einem Dienstagmorgen eine gefälschte Mail über eine angebliche Gehaltsanpassung, freut sich diebisch über eine Klickrate von 31 Prozent, schickt die Namensliste an die Geschäftsführung, und drei Wochen später weiß die halbe Belegschaft, dass die IT sie hereinlegen wollte. Gelernt hat niemand etwas, außer: der IT nicht mehr trauen. Die zweite Sorte sieht langweiliger aus, produziert schlechtere Schlagzeilen im Führungskreis und funktioniert tatsächlich.

Dieser Beitrag beschreibt die zweite Sorte. Werkzeug ist Attack Simulation Training aus Microsoft Defender for Office 365 Plan 2, das in Microsoft 365 E5 enthalten ist. Es gehört im Aufbau der Serie [Microsoft 365 Security](#) ins Handlungsfeld B: Menschen und Prozesse. Nicht, weil Technik unwichtig wäre, sondern weil du hier ein technisches Werkzeug einsetzt, dessen Wirkung ausschließlich davon abhängt, wie du mit Menschen umgehst. Ein falsch aufgesetztes Übungsprogramm richtet mehr Schaden an als gar keines — und zwar an genau der Stelle, an der du im Ernstfall auf Mithilfe angewiesen bist.

Wir gehen die Reihenfolge durch, in der das Ganze aufgesetzt gehört: erst Freigaben und Vorarbeit, dann die drei Techniken, die du wirklich brauchst, dann eigene Landingpages, dann die Trainingszuweisung — und am Ende die einzige Kennzahl, die du nach oben meldest. Vorweg der Spoiler: Es ist nicht die Klickrate.

Bevor du die erste Mail abschickst

Die Versuchung ist groß, im Defender-Portal einfach loszulegen. Der Assistent ist gut gemacht, in zwölf Minuten steht eine Simulation, und der Knopf heißt einladend „Launch this simulation as soon as I'm done“. Genau dieser Knopf hat schon Betriebsvereinbarungen gekostet. Die Vorarbeit dauert länger als die Simulation selbst, und das ist auch richtig so.

Lizenzen, Rollen und wo das Ding überhaupt liegt

Attack Simulation Training setzt Microsoft Defender for Office 365 Plan 2 voraus, entweder als Zusatzlizenz oder als Bestandteil von Microsoft 365 E5. Du findest es im Microsoft Defender Portal unter „E-Mail und Zusammenarbeit“ und dort unter „Attack simulation training“. Mit E3 bekommst du eine Testvariante, die auf Credential Harvest und zwei Trainingserfahrungen beschränkt ist — für ein ernsthaftes Programm reicht das nicht.

Bemerkenswert ist, was es nicht gibt: PowerShell-Cmdlets. Wer gewohnt ist, alles zu skripten, muss hier über den Assistenten oder über die Microsoft-Graph-API arbeiten (Berechtigungen AttackSimulation.Read.All und AttackSimulation.ReadWrite.All). Auch die vereinheitlichte rollenbasierte Zugriffssteuerung von Microsoft Defender XDR greift für dieses Modul derzeit nicht. Du brauchst also klassische Entra-Rollen:

Rolle	Darf	Darf nicht
Attack Simulation	Simulationen, Automatisierungen,	Nichts Wesentliches — das ist die

Administrator	Inhalte und globale Einstellungen anlegen und ändern; alle Berichte sehen.	Arbeitsrolle für das Programm.
Attack Payload Author	Payloads erstellen und ändern, die später jemand anderes startet.	Simulationen oder Trainingskampagnen anlegen, globale Einstellungen ändern, mandantenweite Berichte sehen.
Security Operator / Security Reader	Alle Aspekte der Kampagnen lesen, Daten über Lese-APIs abrufen.	Simulationen anlegen oder ändern, Inhalte bearbeiten, Schreib-APIs nutzen.
Security Administrator	Alles, was der Attack Simulation Administrator darf — plus sehr viel mehr im Rest des Mandanten.	Aus Gründen der minimalen Rechtevergabe: nicht die Rolle der Wahl für ein Übungsteam.

FAKTEN • Wo die Daten liegen

Attack Simulation Training ist in den Regionen APC, EUR und NAM verfügbar; Deutschland gehört zu den unterstützten Ländern. Für die zuletzt hinzugekommenen Standorte — darunter Deutschland — sind alle Funktionen verfügbar mit Ausnahme der Telemetrie zu gemeldeten Mails. Ausgerechnet die Kennzahl, um die es in diesem Beitrag geht, kann dort also noch fehlen. Prüfe das in deinem Mandanten, bevor du sie zur Leitkennzahl erklärst.

Simulationsmetadaten und Nutzeraktivitäten werden 18 Monate aufbewahrt, sofern du die Simulation nicht vorher löschst. Wird der gesamte Mandant gelöscht, verschwinden die Daten nach 90 Tagen.

Der Betriebsrat kommt vorher an den Tisch, nicht hinterher

Attack Simulation Training erzeugt personenbezogene Leistungs- und Verhaltensdaten. Der Export einer einzigen Simulation enthält pro Person: Zeitstempel des Klicks, IP-Adresse, Browser, Gerät, Zeitstempel der Eingabe von Zugangsdaten, ob und wann gemeldet, gelesen, gelöscht, weitergeleitet oder geantwortet wurde, dazu Abteilung, Titel, Standort und Vorgesetzter aus Microsoft Entra ID. Wer das ohne Beteiligung des Betriebsrats einführt, hat kein Awareness-Programm, sondern ein Mitbestimmungsproblem mit angeschlossenem Awareness-Programm.

Die gute Nachricht: Das Gespräch ist einfacher, als du denkst, wenn du mit einem konkreten Vorschlag hineingehst statt mit einem Werkzeug. Was gehört hinein? Zweck, Häufigkeit, Auswertungstiefe, Aufbewahrung, wer die Namensliste sehen darf und was ausdrücklich nicht passiert — keine arbeitsrechtlichen Konsequenzen, keine Weitergabe an Vorgesetzte, keine Ranglisten nach Abteilungen an der Kaffeeküchenwand. Welche Punkte tatsächlich mitbestimmungspflichtig sind und wie eine tragfähige Vereinbarung aussieht, steht im Beitrag [Security-Monitoring und Betriebsrat: was mitbestimmungspflichtig ist](#).

Ein praktischer Trick aus der Beratungspraxis: Nimm die Betriebsratsmitglieder in die erste Welle mit auf. Nicht als Zielgruppe zum Vorführen, sondern als Beteiligte, die sehen, wie die Mail aussieht, was der Bericht zeigt und wo die Grenze verläuft. Misstrauen entsteht aus Intransparenz, und Intransparenz ist hier vollkommen unnötig.

Technische Vorarbeit, damit die Zahlen überhaupt stimmen

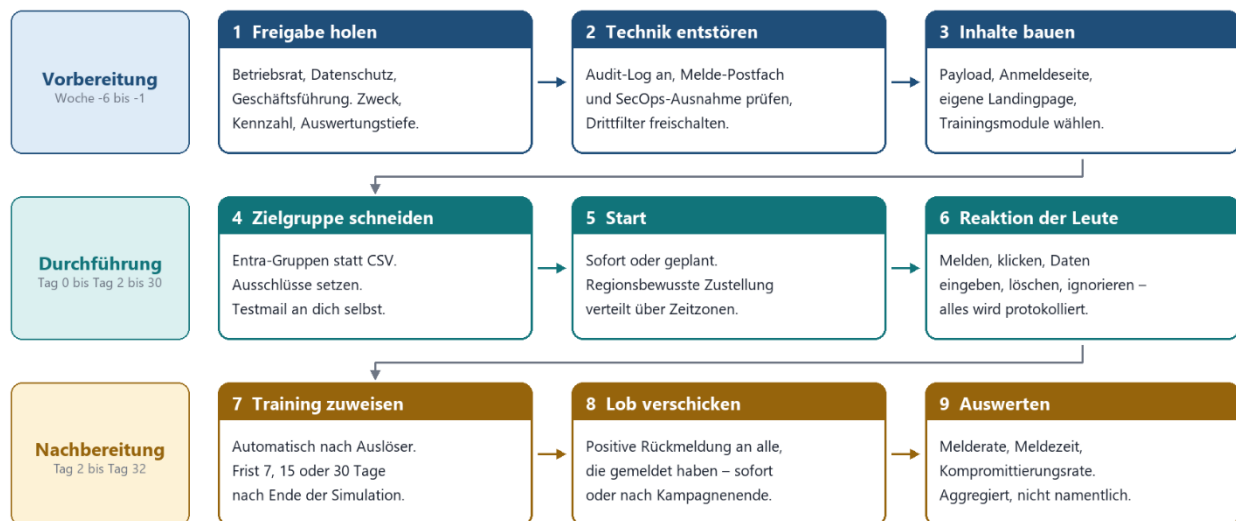
Eine erschreckende Anzahl von Übungsprogrammen misst Unsinn, weil im Hintergrund etwas nicht sauber konfiguriert ist. Die häufigsten Stolpersteine, alle vermeidbar:

- **Überwachungsprotokollierung muss aktiv sein.** Ist das Audit-Log aus, bleiben die Berichte leer und Trainingszuweisungen werden blockiert, weil schlicht keine Daten da sind. Standardmäßig ist die Protokollierung an — prüfen kostet zwei Minuten.
- **Mindestens eine aktive E5-Lizenz.** Ohne das erscheinen ebenfalls leere Aktivitätsdetails.
- **Das Melde-Postfach muss Sicherheitsprüfungen überspringen.** Nutzt du ein eigenes Postfach für gemeldete Nachrichten, ohne die vorgeschriebenen Ausnahmen zu setzen, detonieren Safe Links oder Safe Attachments die gemeldete Simulationsmail — und deine Leute bekommen ausgerechnet dafür ein Training zugewiesen, dass sie richtig gehandelt haben. Details zu den beiden Schutzmechanismen findest du im Beitrag [Defender for Office 365: Safe Links und Safe Attachments](#).
- **Keine Nachrichtenflussregel darf die Rückmeldung an Microsoft blockieren.** Betroffen sind junk@office365.microsoft.com, abuse@messaging.microsoft.com, phish@office365.microsoft.com und not_junk@office365.microsoft.com. Blockiert eine Transportregel diese Adressen, tauchen gemeldete Nachrichten in den Simulationsberichten nie auf.
- **Ein dediziertes SecOps-Postfach gehört in die Richtlinie für erweiterte Zustellung,** damit Nachrichten dort ungefiltert ankommen.
- **Fremdfilter, Outlook-Add-ins und Endpunktschutz brauchen Ausnahmen.** Sonst siehst du Klicks wenige Sekunden nach der Zustellung von Leuten, die schwören, nichts angeklickt zu haben — und sie haben recht. Ein Blick in die Spalten EmailLinkClicked_IP und EmailLinkClicked_TimeStamp im Export entlarvt solche Fehlmessungen zuverlässig.

Eine Besonderheit noch: Attack Simulation Training nutzt Safe Links, um Klicks sicher zu erfassen — auch dann, wenn in deinen Safe-Links-Richtlinien die Nachverfolgung von Benutzerklicks abgeschaltet ist. Umgekehrt umschließt Safe Links die Simulations-URLs nicht, weshalb du Klickdaten in der erweiterten Suche über UrlClickEvents nicht vollständig wiederfindest. Für die Auswertung nimmst du die eingebauten Berichte, nicht die Jagdabfragen.

Ablauf einer Phishing-Simulation

Von der Freigabe bis zur Auswertung – neun Stationen, drei Phasen



Skizze 1 – Neun Stationen. Station 1 wird am häufigsten übersprungen und rächt sich am teuersten.

Skizze 1: Der komplette Ablauf einer Simulation — die ersten drei Stationen entscheiden über den Rest.

TIPP • Der Test an dich selbst

Auf der letzten Seite des Assistenten gibt es die Schaltfläche „Send a test“. Damit schickst du dir die Simulationsmail selbst zu und siehst genau das, was deine Kollegen sehen werden. Nutze das immer. Es ist der billigste Weg, um zu merken, dass Outlook die Bilder blockiert, dass der Absendername unfreiwillig komisch wirkt oder dass die Landingpage in der falschen Sprache erscheint.

Drei Techniken, die für den Anfang völlig reichen

Attack Simulation Training kennt sieben Techniken für Sozialtechnik. Sechs davon stammen aus dem MITRE-ATT&CK-Rahmenwerk, die siebte — „How-to Guide“ — ist gar kein Test, sondern eine Kurzanleitung, die direkt im Postfach gelesen wird. Für ein Programm im Mittelstand brauchst du davon zunächst drei. Die anderen sind nicht schlechter, sie erzeugen nur Aufwand, den du am Anfang nicht brauchst.

Credential Harvest: der Klassiker, und zwar zu Recht

Eine Mail mit Link, dahinter eine nachgebaute Anmeldeseite. Wer dort Benutzername und Kennwort eintippt, gilt als kompromittiert. Das ist die Technik, die dem echten Angriff auf Microsoft-365-Konten am nächsten kommt, und sie hat einen entscheidenden Messvorteil: Klick und Kompromittierung sind zwei getrennte Ereignisse. Du siehst also, wie viele Leute neugierig geklickt und dann doch gestutzt haben.

Was Microsoft mit den eingegebenen Daten macht: nichts. Die Eingaben werden stillschweigend verworfen, protokolliert wird ausschließlich das Ereignis selbst. Diesen Satz solltest du auswendig können, denn er kommt in jeder Betriebsratssitzung und in jeder zweiten Kaffeeküchendiskussion vor. Und ja, das ist auch der Moment, in dem du dir überlegen darfst, warum ein abgegriffenes

Kennwort in deinem Mandanten überhaupt noch reicht, um irgendwo hineinzukommen — siehe [MFA in Microsoft 365 richtig einführen](#) und, eine Stufe weiter, [Passwordless: FIDO2 und Passkeys in der Praxis](#).

Drive-by URL: wenn der Klick schon der Schaden ist

Hier führt der Link auf eine Seite, die im Hintergrund Code ausführen will — der klassische Wasserloch-Angriff. Für die Messung heißt das: Der Klick allein ist bereits die Kompromittierung, eine Eingabe braucht es nicht. Genau deshalb ergibt der Trainingsauslöser „Clicked payload“ bei dieser Technik keinen eigenen Sinn; Microsoft empfiehlt hier ausdrücklich, das Training an „All users“ oder „Compromised“ zu hängen.

Optional kannst du eine Zwischenseite einblenden, bevor die eigentliche Landingpage kommt. Dieses Overlay gibt es nur bei Drive-by URL, und es ist didaktisch nützlich: Es zeigt kurz das, was ein echter Angriff gezeigt hätte, bevor die Aufklärung folgt. Wer es nicht will, lässt das Kästchen leer und landet direkt auf der Landingpage.

OAuth Consent Grant: die Lücke, an die kaum jemand denkt

Eine bössartige Anwendung bittet um Zugriff auf Daten. Der Link in der Mail führt nicht zu einem Anmeldeformular, sondern zum Zustimmungsdialo. Wer zustimmt, gilt als kompromittiert. Diese Technik ist die lehrreichste der drei, weil sie eine Denkweise angreift, die durch Kennwortregeln und Zwei-Faktor-Schulungen überhaupt nicht abgedeckt wird: „Ich habe doch gar kein Kennwort eingegeben, also ist nichts passiert.“ Doch, ist es.

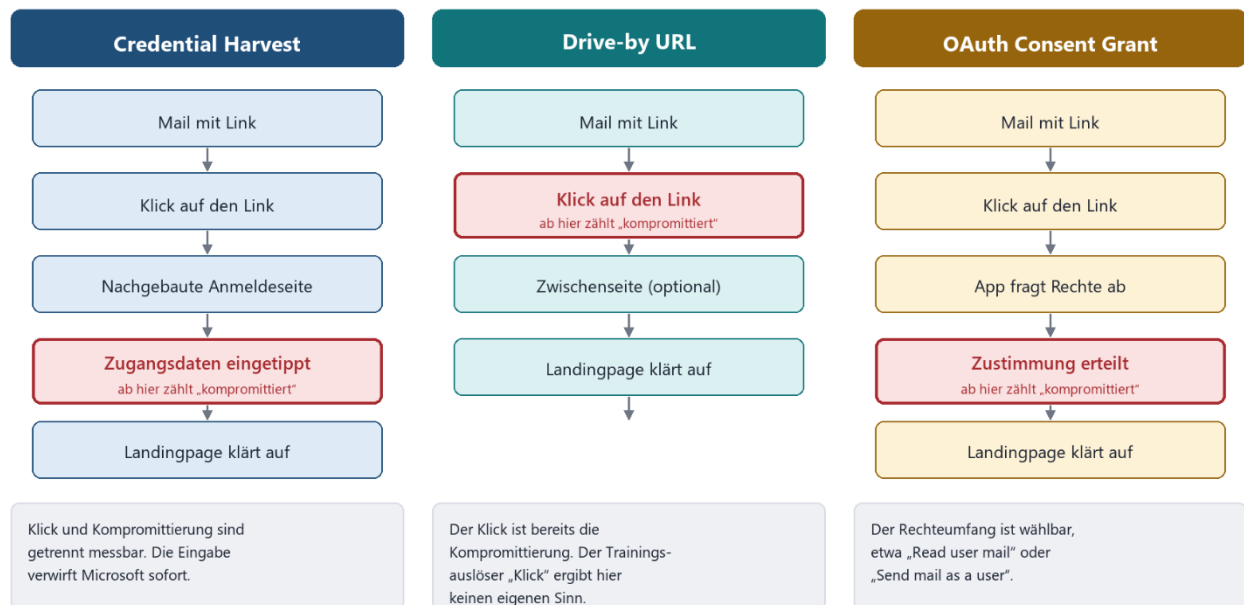
Beim Aufsetzen wählst du einen App-Namen, lädst ein Logo hoch (PNG, JPEG oder GIF) und legst den Berechtigungsumfang fest. Zur Wahl stehen unter anderem „Read user mail“, „Read all files that user can access“, „Read all chat messages“ und, wenn du es richtig unangenehm machen willst, „Send mail as a user“. Die technische Gegenmaßnahme zu dieser Angriffsart beschreibt der Beitrag [App-Registrierungen und Consent-Governance](#) — Übung und Härtung gehören hier zusammen, sonst trainierst du Leute darauf, eine Gefahr zu erkennen, die du auch technisch hättest abstellen können.

Technik	Kompromittiert gilt, wenn ...	Sinnvoller Trainingsauslöser	Wofür du sie nimmst
Credential Harvest	Zugangsdaten auf der Anmeldeseite eingegeben werden.	Beliebig: All users, Clicked payload oder Compromised.	Einstieg, Verlaufsmessung über mehrere Wellen, breite Zielgruppen.
Drive-by URL	der Link angeklickt wird. Punkt.	All users oder Compromised — Clicked payload ist hier redundant.	ClickFix-artige Szenarien, gekaperte Webseiten, Werbeanzeigen.
OAuth Consent Grant	der Zustimmung zum Rechteumfang zugestimmt wird.	Beliebig; Clicked payload trennt Neugier von Zustimmung.	Fortgeschrittene Wellen, Zielgruppen mit vielen Cloud-Anwendungen.
Malware Attachment	der Anhang geöffnet und die Bearbeitung aktiviert	All users oder Compromised — es gibt	Später, wenn dein Programm steht und die

	wird.	kein Klickereignis.	Zielgruppe es aushält.
How-to Guide	gar nichts — es ist kein Test.	Entfällt; es gibt nur die positive Rückmeldung.	Zwischen zwei Wellen, um das Melden zu erklären statt es zu prüfen.

Wann gilt jemand als kompromittiert?

Drei Techniken, drei verschiedene Auslöser – und deshalb drei verschiedene Kennzahlen



Skizze 2 – Wer Drive-by URL fährt und stolz die Klickrate meldet, meldet die Kompromittierungsrate.

Skizze 2: Drei Techniken, drei Auslöser. Wer das verwechselt, berichtet die falsche Zahl.

TIPP • QR-Codes gehören inzwischen dazu

Bei Credential Harvest, Link to Malware, Drive-by URL, OAuth Consent Grant und How-to Guide kann der Link durch einen QR-Code ersetzt werden. Der Dienst erzeugt beim Start einen individuellen Code je Person; im Export unterscheidet die Spalte EmailLinkClicked_ClickSource zwischen PhishingURL und QRCode. Passend dazu gibt es die Trainingsmodule zu böartigen digitalen und gedruckten QR-Codes sowie eine Kurzanleitung zum Erkennen und Melden von QR-Phishing.

Eigene Landingpages: der einzige Moment, in dem wirklich gelernt wird

Die Simulationsmail ist nicht die Lehrveranstaltung. Das Training später ist es auch nur halb, weil ein Teil der Leute es abnickt, ohne hinzuschauen. Der eine Augenblick, in dem jemand tatsächlich aufmerksam ist, dauert etwa vier Sekunden und beginnt in dem Moment, in dem die Landingpage aufgeht und die Erkenntnis einsetzt: „Oh.“ Wenn du in diesen vier Sekunden eine generische englische Standardseite zeigst, hast du sie verschenkt.

Was die eingebauten Seiten können — und wo sie aufhören

In der Inhaltsbibliothek liegen unter „Phish landing pages“ zwei Registerkarten. Auf „Global landing pages“ findest du fünf unveränderbare Vorlagen von Microsoft, lokalisiert in mehr als zwölf Sprachen. Sie sind ordentlich, du kannst ein Logo hinterlegen und die Standardsprache wählen — mehr aber nicht. Für die erste Welle reicht das. Ab der zweiten willst du eigene Seiten, und die liegen auf der Registerkarte „Tenant landing pages“.

Wichtig für die Sprachlogik, weil das regelmäßig für Verwirrung sorgt: Die Landingpage richtet sich nach der Spracheinstellung des Microsoft-365-Kontos, Trainingsmodule nach der Browsersprache, Benachrichtigungen nach der Postfachsprache — und die Payload-Sprache legst du beim Anlegen selbst fest. In einem gemischtsprachigen Unternehmen legst du für deine eigene Landingpage also Übersetzungen an, sonst schaut ein Teil der Belegschaft auf eine Seite, die sie nicht liest.

So baust du eine Seite, die etwas bewirkt

Der Assistent ist schlicht: Name und Beschreibung, dann Inhalt in der Standardsprache, dann optional Übersetzungen, dann Prüfen und Absenden. Der eigentliche Hebel steckt in zwei Details. Erstens den dynamischen Platzhaltern: `{userName}`, `{firstName}`, `{department}`, `{manager}`, `{FromName}`, `{EmailSubject}` und, der wichtigste von allen, `{EmailContent}`. Letzterer fügt den Inhalt der Simulationsmail direkt in die Landingpage ein. Zweitens der Option „Add payload indicators to email“ bei der Auswahl der Landingpage: Sie markiert im eingebetteten Mailinhalt genau die Stellen, an denen man die Fälschung hätte erkennen können. Beide zusammen ergeben eine Seite, die nicht sagt „Du bist auf Phishing hereingefallen“, sondern „Hier, genau dieser Absendername und dieser Link hätten dich stutzig machen sollen“.

Drei Dinge, die auf jede gute Landingpage gehören und auf keiner Standardvorlage stehen: der Satz, dass es keine Konsequenzen gibt und niemand namentlich gemeldet wird. Der Hinweis, wie man im Ernstfall meldet — mit der Beschreibung des tatsächlichen Melde-Knopfes in eurer Outlook-Version, nicht abstrakt. Und eine echte Ansprechstelle mit Namen, denn die Frage „Ich glaube, ich habe letzte Woche auf so etwas geklickt, was jetzt?“ ist genau die Frage, die du hören willst. Wie es dann weitergeht, steht in [Phishing-Vorfall: die ersten 60 Minuten](#).

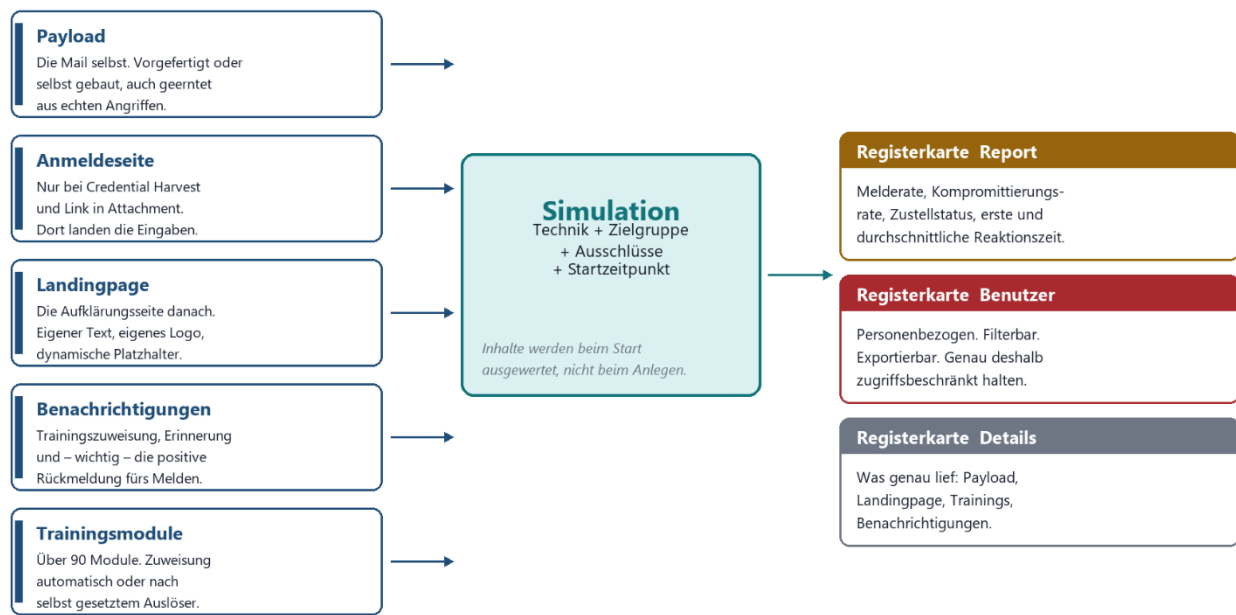
Payloads: selbst bauen oder ernten lassen

Neben den vorgefertigten Payloads kannst du eigene anlegen, vorhandene kopieren und anpassen — und, die eleganteste Variante, echte Phishing-Mails ernten. Die Payload-Automatisierung nimmt tatsächlich in deinem Mandanten aufgeschlagene Angriffsmails und macht daraus harmlose Vorlagen. Das ist aus zwei Gründen besser als jede Vorlage: Der Ton stimmt, und die Übersetzung ins Deutsche hat freundlicherweise der Angreifer erledigt. Microsoft empfiehlt genau das ausdrücklich, weil maschinell übersetzte Standard-Payloads an Treffsicherheit verlieren.

Zur Einschätzung, wie schwer ein Payload ist, blendet der Dienst die vorhergesagte Kompromittierungsrate ein. Sie schätzt auf Basis anonymisierter historischer Daten aus Microsoft 365, welcher Anteil der Empfänger voraussichtlich hereinfällt. Ist ein Köder zu perfekt, fallen fast alle darauf herein und niemand lernt etwas; ist er zu plump, fällt niemand darauf herein und niemand lernt etwas. Die Kennzahl hilft dir, die Mitte zu treffen — und später den Ist- mit dem Erwartungswert zu vergleichen.

Die Bausteine einer Simulation

Alles links liegt in der Inhaltsbibliothek und ist wiederverwendbar



Skizze 3 – Die Registerkarte „Benutzer“ ist der Teil, über den du mit dem Betriebsrat sprichst.

Skizze 3: Payload, Anmeldeseite, Landingpage, Benachrichtigungen und Trainings sind eigenständige Bausteine.

WARNUNG · Was der Payload-Editor nicht mitmacht

Payloads mit den Begriffen IRS, I.R.S., Internal Revenue Service, Inland Revenue Service oder Treasury werden blockiert — das hängt an Beschränkungen zu behördlichen Marken und Symbolen. Ebenfalls entfernt werden die HTML-Elemente applet, base, basefont, command, embed, frame, frameset, iframe, keygen, link, meta, noframes, noscript, param, script, object und title. Wenn dein sorgfältig gebautes HTML beim Speichern auf einmal anders aussieht, liegt es meistens daran.

Und der unangenehme Teil: Microsoft stellt die Payloads bereit, gibt aber ausdrücklich keine Rechtsberatung. Ob du fremde Marken und Logos in einer Übung verwenden darfst — auch in den mitgelieferten Vorlagen — musst du selbst klären. Ein nachgebautes Paketdienst-Logo in einer internen Übung ist etwas anderes als ein nachgebautes Logo deines größten Kunden. Im Zweifel nimmst du interne Motive: Urlaubsantrag, Zeiterfassung, IT-Wartungsfenster. Die funktionieren ohnehin besser.

Trainingszuweisung und die Kennzahl, die tatsächlich zählt

Jetzt der Teil, an dem die meisten Programme kippen — nicht technisch, sondern kulturell. Es geht darum, was nach dem Klick passiert und welche Zahl du hinterher weitergibst.

Training zuweisen, ohne zu bestrafen

Auf der Seite „Assign training“ hast du drei Grundoptionen: die Microsoft-Trainingserfahrung (empfohlen), eine Weiterleitung auf eine eigene URL — praktisch, wenn du ein bestehendes Lernmanagementsystem hast — oder gar kein Training. Die letzte Variante ist fast immer die falsche. Innerhalb der Microsoft-Erfahrung wählst du zwischen „Assign training for me (Recommended)“, wobei die Zuweisung auf Basis früherer Ergebnisse erfolgt, und der

Eigenauswahl aus über 90 Modulen, die in Zusammenarbeit mit Terranova Security entstanden sind. Die Frist setzt du auf 7, 15 oder 30 Tage nach Ende der Simulation; Standard sind 30.

Wählst du selbst aus, legst du je Modul den Auslöser fest. Nicht jeder Auslöser passt zu jeder Technik:

Auslöser	Bedeutung	Wann er passt	Wann er Unsinn ist
All users	Alle Zielpersonen bekommen das Modul, unabhängig vom Verhalten.	Kurze Module, neue Themen, erste Welle, Malware Attachment und Drive-by URL.	Bei langen Modulen und großen Zielgruppen — das erzeugt Frust.
Clicked payload	Nur wer den Link angeklickt hat.	Credential Harvest, Link in Attachment, Link to Malware, OAuth Consent Grant.	Bei Drive-by URL (Klick ist schon Kompromittierung) und Malware Attachment (kein Klickereignis).
Compromised	Nur wer Zugangsdaten eingegeben, zugestimmt oder den Anhang aktiviert hat.	Immer sinnvoll, für alle Techniken verfügbar.	Als einziger Auslöser zu schmal, wenn du niemanden erreichen willst, der knapp vorbeigeschrammt ist.

Zwei globale Einstellungen solltest du kennen. Die Trainingsschwelle verhindert, dass dieselben Module innerhalb eines Zeitraums erneut zugewiesen werden; Standard sind 90 Tage. Microsoft empfiehlt, sie größer zu wählen als die Bearbeitungsfrist — sonst bekommt jemand ein Modul zugewiesen, das er noch gar nicht abschließen konnte. Der Wert 0 hebt die Schwelle auf und weist immer zu. Und die Wiederholungstäter-Schwelle steht standardmäßig auf 2: Wer in zwei aufeinanderfolgenden Simulationen kompromittiert wurde, landet in der entsprechenden Liste.

WICHTIG · Die Wiederholungstäter-Liste ist kein Personalinstrument

Die Liste existiert, sie ist exportierbar, und sie enthält Namen, Mailadressen, Anzahl der Wiederholungen und den Status des letzten Trainings. Sie ist ein hervorragendes Werkzeug, um gezielt Hilfe anzubieten — ein Vor-Ort-Termin, eine kurze Schulung im Team, eine andere Technik in der nächsten Welle. Sie ist ein katastrophales Werkzeug, um Gespräche mit Vorgesetzten zu führen. Lege in der Betriebsvereinbarung fest, wer sie sehen darf, und halte dich daran, auch wenn danach gefragt wird. Es wird danach gefragt.

Warum die Klickrate die falsche Leitkennzahl ist

Die Klickrate misst Neugier unter Zeitdruck. Sie sinkt zuverlässig, wenn du langweilige Payloads verschickst, und sie steigt zuverlässig, wenn du gute verschickst. Sie belohnt also das Falsche. Vor allem aber misst sie einen Zustand, den du im Ernstfall nicht verhindern kannst: Irgendwer klickt immer. Das ist keine Niederlage, das ist Wahrscheinlichkeitsrechnung bei dreistelligen Belegschaftsgrößen.

Die Melderate misst etwas anderes: ob dein Unternehmen einen funktionierenden Reflex hat. Sie ist die einzige Kennzahl aus einer Phishing-Übung, die direkt auf die Reaktionsfähigkeit im

Ernstfall einzahlt — denn eine Meldung nach vier Minuten bedeutet, dass dein Team den Angriff bearbeitet, bevor der zwanzigste Empfänger die Mail überhaupt öffnet. Und sie hat einen angenehmen Nebeneffekt: Sie lässt sich steigern, ohne jemanden zu beschämen.

Im Bericht findest du beides im Abschnitt „Simulation impact“, der kompromittierte Personen und meldende Personen nebeneinanderstellt. Ein Detail, das man leicht übersieht: Meldungen über nicht von Microsoft stammende Werkzeuge werden in den Simulationsberichten nicht erfasst. Wer ein Fremdprodukt als Melde-Knopf einsetzt, muss das in den Benutzermeldeeinstellungen sauber konfigurieren, sonst zeigt die wichtigste Kennzahl hartnäckig null. Nebenbei: Die alten Add-ins „Nachricht melden“ und „Phishing melden“ sind im Wartungsmodus und werden abgekündigt; der eingebaute Melde-Knopf in Outlook ist der Weg nach vorn.

Kennzahl	Woher sie kommt	Wohin sie gehört	Realistische Entwicklung
Melderate	Abschnitt „Simulation impact“, Spalte „Reported“ auf der Registerkarte „Benutzer“.	Leitkennzahl. Gehört aggregiert ins Führungsberichtswesen.	Welle 1 oft unter 10 %. Ziel nach vier Wellen: 40 % und mehr.
Zeit bis zur ersten Meldung	Zeitstempel „Phishing Reported On“ im Export, verglichen mit der Zustellung.	Leitkennzahl Nummer zwei. Sie sagt mehr über Reaktionsfähigkeit als jede Quote.	Von „gar nicht“ über „nach zwei Stunden“ zu „unter zehn Minuten“.
Kompromittierungsrate	Abschnitt „Simulation impact“, plus Vergleich mit der vorhergesagten Rate.	Internes Steuerungsmaß für die Auswahl der nächsten Payloads.	Sinkt, aber langsam und nicht monoton. Erwarte Rückschläge.
Klickrate	„All user activity“, Ereignis „Clicked message link“.	Arbeitszahl für dich. Nicht ins Führungsberichtswesen.	Schwankt mit der Qualität des Payloads, nicht mit dem Lernstand.
Trainingsabschluss	Registerkarte „Training completion“ im Bericht zur Angriffssimulation.	Pflichtnachweis, etwa gegenüber Auditoren.	Steigt mit Erinnerungen; bleibt selten über 90 %.
Wiederholungstäter	Registerkarte „Repeat offenders“, Standardschwelle 2.	Nur ins Übungsteam. Nirgendwo sonst hin.	Kleine, hartnäckige Gruppe. Braucht ein anderes Format, keinen Druck.

Was die Geschäftsführung sieht — und was nicht

Die Regel ist einfach und sie hält jeder Diskussion stand: Nach oben gehen ausschließlich aggregierte Zahlen. Melderate, Meldezeit, Kompromittierungsrate im Trend, Trainingsabschluss — jeweils für das Gesamtunternehmen. Keine Namen. Keine Abteilungsranglisten. Auch dann nicht, wenn der Export die Felder Abteilung, Titel, Standort und Vorgesetzter freundlich mitliefert und die Auswertung technisch zwei Klicks entfernt ist.

Der Grund ist nicht nur rechtlich. Sobald eine Abteilungsrangliste kursiert, verändert sich das Verhalten: Man meldet nicht mehr, weil es richtig ist, sondern man warnt sich intern vor der

Übungsmail. Ab diesem Moment misst du gar nichts mehr. Wie ein Bericht aussieht, der aussagekräftig und trotzdem anonym ist, behandelt der Beitrag [Security-Reporting für die Geschäftsführung](#). Für die datenschutzrechtliche Einordnung der Protokollierung insgesamt lohnt der Blick in den [Kompetenzbereich Microsoft Purview](#).

Ein Wort zur positiven Rückmeldung, weil sie das am meisten unterschätzte Werkzeug im ganzen Modul ist. Du kannst einstellen, dass jede Person, die die Simulationsmail meldet, sofort eine Bestätigung bekommt — nicht erst nach Kampagnenende. Genau das ist der Hebel für die Melderate. Wer meldet und binnen Sekunden ein „Danke, genau richtig“ bekommt, meldet beim nächsten Mal wieder. Wer meldet und nichts hört, fragt sich, ob es überhaupt jemanden interessiert hat.

FAKTEN • Wann die Zahlen im Portal stehen

Die Berichte aktualisieren sich nicht sofort. Nach dem Übergang in den Zustand „In progress“ dauert es bis zu 30 Minuten, danach wird in Intervallen aktualisiert: alle 10 Minuten in der ersten Stunde, alle 15 Minuten bis Tag zwei, alle 30 Minuten bis Tag sieben, danach stündlich. Wer eine Stunde nach dem Start ins Portal schaut und panisch wird, weil dort fast nichts steht, hat einfach zu früh geschaut.

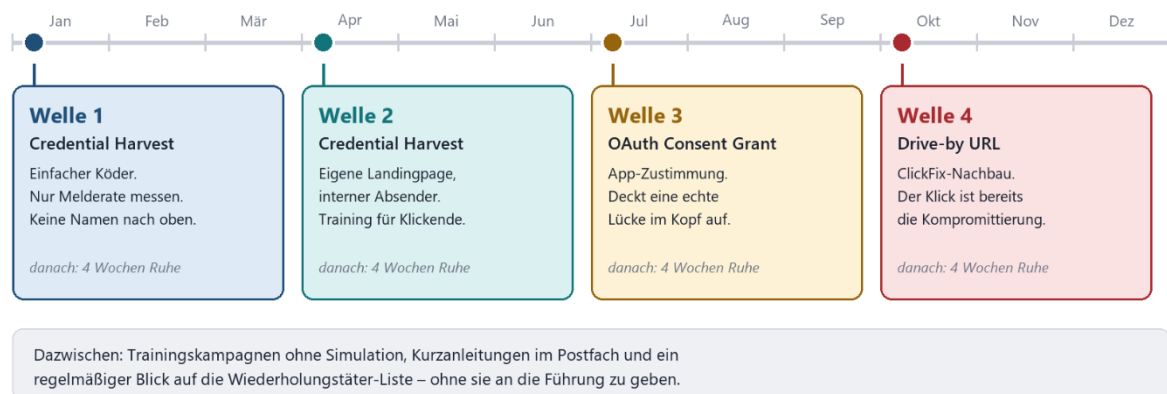
Bei Postfächern, die noch lokal liegen, fehlen Angaben dazu, ob eine Mail gelesen, weitergeleitet oder gelöscht wurde — und, für dieses Thema entscheidend, die Zahl der meldenden Personen. In hybriden Umgebungen musst du deine Leitkennzahl also entweder auf die Cloud-Postfächer eingrenzen oder ehrlich mit der Lücke umgehen.

Der Jahresplan und ein Vorschlag für Welle vier

Ein Übungsprogramm ist kein Ereignis, sondern eine Kadenz. Zu selten, und der Reflex schläft ein. Zu häufig, und die Belegschaft entwickelt eine gesunde Gleichgültigkeit gegenüber allem, was nach IT-Mail aussieht — inklusive der echten. Vier bis sechs Wellen im Jahr sind die Spanne, in der beides funktioniert.

Ein Jahresplan, der niemanden zermürbt

Vier Wellen, steigender Schwierigkeitsgrad, dazwischen Luft zum Atmen



Skizze 4 – Mehr als vier bis sechs Wellen pro Jahr erzeugen nur Abstumpfung.

Skizze 4: Ein Jahr in vier Wellen. Zwischen den Wellen wird trainiert, nicht getestet.

Zur Steuerung stehen dir zwei Werkzeuge zur Verfügung. Simulationen sind Einzelkampagnen mit genau einer Technik und einem Start- sowie Enddatum; die Laufzeit stellst du zwischen 2 und 30 Tagen ein. Simulationsautomatisierungen können mehrere Techniken und Payloads kombinieren und bringen einen echten Zeitplan mit, inklusive zufälliger Verteilung. Für den Einstieg nimmst du Einzelsimulationen, weil du dabei mehr siehst. Ab Jahr zwei ist die Automatisierung die bequemere Wahl.

Eine Empfehlung zur Zustellung: Schalte die regionsbewusste Zustellung ein, wenn deine Standorte über Zeitzone verteilt sind. Sie liefert jeder Person die Mail zur eingestellten Ortszeit ihres Postfachs aus, nach einer „nicht davor“-Logik — ist die Uhrzeit am Starttag lokal schon vorbei, kommt die Mail am Folgetag zur selben Ortszeit. Das verhindert nebenbei den Effekt, dass sich die halbe Belegschaft binnen zehn Minuten gegenseitig warnt. Wer noch gründlicher streuen will, nutzt unterschiedliche Payloads in derselben Welle.

Zielgruppen schneiden, ohne sich zu verheben

Als Zielgruppe kannst du alle Personen im Unternehmen wählen (derzeit für Organisationen unter 40.000 Personen), einzelne Konten benennen, eine CSV-Datei mit einer Adresse je Zeile importieren oder — die einzig vernünftige Variante auf Dauer — Entra-Gruppen verwenden. Unterstützt werden Microsoft-365-Gruppen (statisch und dynamisch) sowie Verteilerlisten und mailaktivierte Sicherheitsgruppen jeweils in statischer Form. Das Importlimit liegt bei 40.000 Empfängern, die technische Obergrenze bei 400.000; empfohlen sind höchstens 200.000 je Simulation.

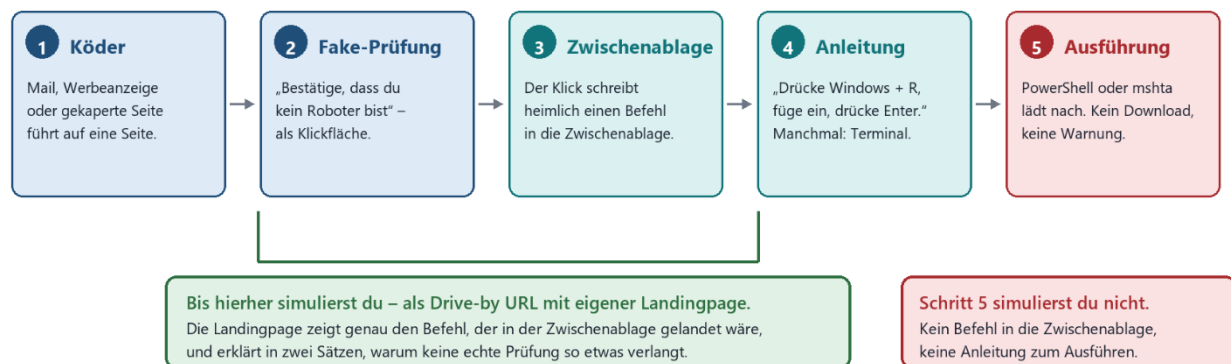
Automatisch ausgeschlossen werden ungültige Adressen, Gäste und in Entra ID nicht mehr aktive Konten. Freigegebene Postfächer werden derzeit nicht unterstützt. Und auf der Seite „Exclude users“ nimmst du gezielt Leute heraus — sinnvollerweise das Übungsteam selbst, den Bereitschaftsdienst während einer laufenden Störung und Personen in besonders belastenden Situationen. Diese Ausschlussliste ist übrigens im Bericht einsehbar; sie ist kein Geheimnis und sollte auch keines sein.

Das ClickFix-Szenario als Kür

Wenn dein Programm steht, kommt die Welle, in der es unangenehm wird — im guten Sinne. ClickFix ist die Sozialtechnik, die in den vergangenen zwei Jahren am schnellsten gewachsen ist, und sie umgeht praktisch alles, was deine Leute bisher gelernt haben. Das Muster: eine gefälschte Prüfung „Bestätige, dass du kein Roboter bist“, ein Klick, der heimlich einen Befehl in die Zwischenablage schreibt, und die Anleitung, ihn mit Windows und R einzufügen und auszuführen. Kein Download, keine Datei, keine Sicherheitswarnung — das Opfer führt den Befehl selbst aus. Die Variante TerminalFix schickt die Leute stattdessen ins Windows Terminal oder in die PowerShell, weil dort auch mehrzeilige Skripte zuverlässig durchlaufen. Wie so eine Kette in der Praxis aussieht und was sie anrichtet, zeichnet das [Dossier TerminalFix und der Berlin-Hack](#) nach.

Das ClickFix-Muster – und wo deine Simulation endet

Der Angriff bringt das Opfer dazu, den Befehl selbst auszuführen. Deine Übung hört vorher auf.



Skizze 5 – Die Übung endet an der Stelle, an der sie sonst selbst zur Anleitung würde.

Skizze 5: Die Übung bildet die Schritte eins bis vier nach – und hört genau davor auf, selbst zur Anleitung zu werden.

So setzt du es auf: Technik ist Drive-by URL, weil der Klick allein zählt und du keine Zugangsdaten abfragen willst. Als Payload nimmst du etwas Alltägliches – eine geteilte Datei, eine Besprechungsaufzeichnung, eine Rechnung im Portal. Die Zwischenseite blendest du ein; sie zeigt die gefälschte Prüfung. Die Landingpage baust du selbst und sie tut genau eine Sache: Sie zeigt den Befehl, der jetzt in der Zwischenablage gelandet wäre, und erklärt in zwei Sätzen, dass keine echte Prüfung, kein Browser-Update und kein Erweiterungsfehler jemals verlangt, etwas in ein Systemfenster einzufügen. Dieser eine Satz ist die ganze Lektion.

Was du nicht tust: den Befehl tatsächlich in die Zwischenablage schreiben oder eine funktionierende Schritt-für-Schritt-Anleitung zeigen. Eine Übung, die versehentlich zur Bedienungsanleitung wird, ist keine Übung. Flankierend gehört dazu, was Microsoft ohnehin empfiehlt: das Ausführen-Fenster per Gruppenrichtlinie entfernen, wo es niemand braucht, Regeln zur Verringerung der Angriffsfläche gegen verschleierte Skripte aktivieren und das Windows Terminal so einstellen, dass es beim Einfügen mehrzeiliger Inhalte warnt. Simulieren und härten sind zwei Hälften derselben Maßnahme – die Übersicht dazu steht in der [Tenant-Härtung: die 20 wichtigsten Schrauben](#).

Und wenn du wissen willst, ob dein Team die eingehende Meldung auch verarbeitet bekommt: Das ist eine andere Übung. Dafür gibt es die [Feuerwehübung: Security-Notfälle im Team trainieren](#) und, eine Stufe härter, die [Red-Team-Übung: der kontrollierte Angriff](#). Attack Simulation Training testet die Belegschaft. Diese beiden testen dich.

Häufige Fragen

Brauche ich wirklich Plan 2, oder geht das auch mit Plan 1?

Es braucht Plan 2 oder Microsoft 365 E5. Mit E3 gibt es eine Testvariante, die auf Credential Harvest und die beiden Trainingserfahrungen „ISA Phishing“ und „Mass Market Phishing“ beschränkt ist. Damit kannst du ausprobieren, wie sich das Werkzeug anfühlt, aber kein Programm betreiben. Ob sich der Sprung lohnt, hängt weniger an diesem Modul als am Gesamtpaket – die Abwägung besprechen wir gern in der [Beratung zu Microsoft 365 Security](#).

Wie viele Leute darf ich in einer Simulation adressieren?

„Alle Personen im Unternehmen“ steht derzeit Organisationen mit weniger als 40.000 Personen offen. Beim Import aus einer CSV-Datei oder beim einzelnen Hinzufügen liegt das Limit ebenfalls bei 40.000 Einträgen, wobei ein Eintrag auch eine Gruppe sein kann. Die technische Obergrenze liegt bei 400.000 Personen, empfohlen sind höchstens 200.000 je Simulation. Praktisch arbeitest du mit Entra-Gruppen, weil die Verwaltung sonst zur Zumutung wird.

Warum sehe ich Klicks von Leuten, die nicht geklickt haben?

Weil etwas anderes geklickt hat. Sicherheitsgeräte, Fremdfilter, Outlook-Add-ins, Endpunktschutz und automatisierte Reaktionsabläufe prüfen Weblinks in Nachrichten und erzeugen dabei Klickereignisse. Typisches Muster: viele Klicks wenige Sekunden nach der Zustellung. Im Export verrät dir EmailLinkClicked_IP, ob die Adresse überhaupt zu deinem Unternehmen oder zu Microsoft gehört. Abhilfe: alle Simulations-URLs und die Domänen deiner eigenen Payloads in den betroffenen Systemen ausnehmen.

Speichert Microsoft die Kennwörter, die jemand auf der Übungsseite eintippt?

Nein. Eingaben auf der Anmeldeseite werden stillschweigend verworfen; erfasst wird ausschließlich das Ereignis, um die Kompromittierung zu zählen. Microsoft sammelt, protokolliert und speichert die Eingaben nicht. Diesen Punkt schreibst du am besten wörtlich in die Betriebsvereinbarung, dann musst du ihn nicht dreimal erklären.

Was passiert, wenn jemand die Übungsmail weiterleitet oder beantwortet?

Sie wird wie jede andere Mail behandelt, inklusive Detonation durch Safe Links und Safe Attachments. Der Bericht zeigt, ob weitergeleitet oder geantwortet wurde. Weil jede URL personengebunden ist, werden Detonationen als Klick der ursprünglich adressierten Person gewertet — ein weiterer Grund, die eigenen Melde- und SecOps-Postfächer sauber auszunehmen.

Kann ich Trainings zuweisen, ohne jemanden vorher hereinzulegen?

Ja, und das solltest du zwischen den Wellen auch tun. Trainingskampagnen weisen Module direkt zu, ohne Simulation. Zusätzlich gibt es die Technik „How-to Guide“: eine leichte Lerneinheit, die direkt im Postfach gelesen wird, etwa die Kurzanleitung zum Melden von Phishing oder zum Erkennen von QR-Phishing. Diese Formate sind der Kitt zwischen zwei Wellen und sie kosten fast nichts.

Wie erkläre ich der Geschäftsführung, dass die Klickrate gestiegen ist?

Mit der vorhergesagten Kompromittierungsrate. Sie zeigt, wie schwer ein Payload ist, und erlaubt den Vergleich zwischen Erwartung und Ergebnis. Eine gestiegene Klickrate bei einem deutlich anspruchsvolleren Köder ist ein Fortschritt, kein Rückschritt — vorausgesetzt, die Melderate ist mitgestiegen. Genau deshalb berichtest du beide Zahlen nie einzeln.

Was tue ich mit denen, die immer wieder hereinfallen?

Ihnen helfen. Die Wiederholungstäter-Liste ist dafür da, ein anderes Format anzubieten: eine kurze Sitzung im Team, ein persönliches Gespräch aus der IT heraus, eine leichtere Technik in der

nächsten Welle. Was du nicht tust, ist die Liste weiterreichen. Wenn im Unternehmen Bedarf an strukturierter Wissensvermittlung entsteht, ist die [Schulung Microsoft 365 Security](#) der geeignetere Weg als Druck.

Meine Simulations-URL wird vom Browser blockiert. Was nun?

Google Safe Browsing stuft einzelne der von Microsoft verwendeten Simulationsadressen gelegentlich als betrügerisch ein und zeigt in Chrome eine Warnung; Microsoft Edge ist davon nicht betroffen. Prüfe die konkrete Adresse in den bei euch eingesetzten Browsern, bevor du sie in einer Kampagne verwendest, und gib sie in der Browserverwaltung frei. Zusätzlich können Firewalls, Web Application Firewalls und Filtertreiber die Adressen blockieren — auch das gehört auf die Prüfliste vor der ersten Welle.

Was ist mit Postfächern, die noch lokal liegen?

Die werden unterstützt, aber mit eingeschränkter Berichterstattung. Ob eine Mail gelesen, weitergeleitet oder gelöscht wurde, ist nicht verfügbar — und die Zahl der meldenden Personen ebenso wenig. Für ein Programm, dessen Leitkennzahl die Melderate ist, bedeutet das: Entweder du grenzt die Auswertung auf Cloud-Postfächer ein, oder du benennst die Lücke offen. Beides ist besser, als eine Zahl zu berichten, die nur einen Teil des Unternehmens abbildet.

Fazit

Attack Simulation Training ist ein gutes Werkzeug mit einer eingebauten Falle. Die Falle heißt Klickrate, sie ist prominent platziert, sie lässt sich hübsch in Balken darstellen, und sie verleitet dazu, ein Awareness-Programm in ein Beschämungsprogramm zu verwandeln. Wer stattdessen die Melderate und die Zeit bis zur ersten Meldung zur Leitgröße macht, misst das, was im Ernstfall tatsächlich hilft: dass jemand den Hörer in die Hand nimmt, bevor der Angriff Fahrt aufnimmt.

Die Reihenfolge ist dabei nicht verhandelbar. Erst die Freigabe durch den Betriebsrat mit klar geregelter Auswertungstiefe, dann die technische Vorarbeit, damit die Zahlen stimmen, dann drei Techniken statt sieben, dann eigene Landingpages, weil dort der einzige Lernmoment stattfindet, und erst ganz zum Schluss die Kür mit ClickFix. Wer diese Reihenfolge umdreht und mit der spektakulären Simulation anfängt, bekommt eine spektakuläre erste Welle und danach ein Jahr Gegenwind.

Und die vielleicht wichtigste Einstellung im ganzen Modul ist die unscheinbarste: die positive Rückmeldung, sofort nach der Meldung zugestellt. Sie kostet nichts, sie steht in keinem Sicherheitsstandard, und sie verändert das Verhalten deiner Belegschaft mehr als jedes Pflichttraining.

Weiter im Thema

- › [Microsoft 365 Security](#) – die Übersicht über alle Handlungsfelder der Serie
- › [Security-Monitoring und Betriebsrat: was mitbestimmungspflichtig ist](#) – die Grundlage, ohne die du nicht startest
- › [Phishing-Vorfall: die ersten 60 Minuten](#) – was passiert, wenn eine Meldung echt ist
- › [Kompromittiertes Konto erkennen und aufräumen](#) – der Schritt danach

- › [Defender for Office 365: Safe Links und Safe Attachments](#) – die Technik hinter der Klickerfassung
- › [App-Registrierungen und Consent-Governance](#) – die Härtung zur OAuth-Simulation
- › [Dossier TerminalFix und der Berlin-Hack](#) – warum das ClickFix-Szenario keine Theorie ist
- › [Security-Reporting für die Geschäftsführung](#) – aggregiert berichten, ohne Aussagekraft zu verlieren
- › [Beratung zu Microsoft 365 Security](#) – wenn du das Programm nicht allein aufsetzen willst
- › [Schulung Microsoft 365 Security](#) – strukturiertes Wissen statt Druck