

Tabletop-Übung:

Phishing- und Whaling-Angriffe aufdecken

🕒 Überblick

Bei Phishing-Angriffen werden Emotionen wie Angst, Hilfsbereitschaft oder Respekt vor Autoritäten ausgenutzt, um Mitarbeitende so zu manipulieren, dass sie die Sicherheit der Organisation aufs Spiel setzen. Bei dieser Aktivität liegt der Schwerpunkt auf einer bestimmten, sehr zielgerichteten Form des Phishings: „Whaling“ oder „CEO-Betrug“. Bei solchen Angriffen geben sich Kriminelle als hochrangige Führungskräfte wie CEO oder CFO aus, um die Position als Autorität auszunutzen und eine sofortige emotionale Reaktion auszulösen.

Moderne Bedrohungsakteurinnen und -akteure nutzen generative künstliche Intelligenz (KI), um Phishing-E-Mails mit täuschend echt wirkenden Organisationslogos und ohne Grammatikfehler zu generieren. Die Teilnehmenden sollten weiterhin die Augen nach offensichtlichen Rechtschreib- oder Branding-Fehlern offenhalten, doch lernen sie hier darüber hinaus, dass sie sich nicht mehr nur auf diese oberflächlichen Phishing-Anzeichen verlassen können.

👥 Rollen

Moderation:

Steuert den Ablauf der Übung, leitet Diskussionen und bezieht, für eine aktive Mitarbeit, alle mit ein.

Teilnehmende:

Besprechen offen ihre Gedankengänge und reagieren im Rahmen der Regeln der Übung auf die verschiedenen Szenarien.

Einführung

Stellen Sie den Teilnehmenden das Szenario vor: Seeblick Logistik weitet den Geschäftsbetrieb auf Europa aus. Der CEO Markus Wagner reist schon die ganze Woche durch Deutschland, um einen wichtigen Mietvertrag für ein Lager zu unterzeichnen. Alle in der Organisation wissen, dass dieser Geschäftsabschluss oberste Priorität hat. Die CFO Helena Frey befindet sich auf einem 10-stündigen Flug zurück zum Hauptsitz und ist gerade nicht erreichbar. Tanja Reiter, Leiterin der Kreditorenbuchhaltung, erhält eine verdächtige E-Mail.

Teil 1: Identifizieren von Warnsignalen

🕒 **Dauer:** 15 Minuten

Materialien:

- Timer oder Stoppuhr
- Szenario-Handouts
- Stifte

Anweisungen:

- Teilen Sie die Anwesenden in kleine Gruppen ein.
- Händigen Sie jeder Gruppe die E-Mail-Ausdrucke und Stifte aus.
- Weisen Sie die Gruppen an, Elemente zu unterstreichen, die falsches Vertrauen aufbauen. Beispiele: richtige E-Mail-Signaturen, Erwähnungen echter interner Projekte oder ein authentischer Tonfall einer Führungskraft.
- Weisen Sie die Gruppen an, Verhaltenswarnsignale **einzukreisen**. Beispiele: extreme Dringlichkeit, Forderung, die Anfrage geheim zu halten, oder Anweisungen, die üblichen Zahlungsportale zu umgehen.
- Geben Sie den Gruppen 15 Minuten Zeit, die E-Mail zu lesen, zu besprechen und Warnsignale zu identifizieren.

Teil 2: Diskussion

 **Dauer:** 10 Minuten

Fragen:

- Welche Indikatoren für falsches Vertrauen haben Sie festgestellt und inwiefern haben sich diese auf die subjektive Glaubwürdigkeit der E-Mail ausgewirkt?
- Welche konkreten Verhaltenswarnsignale haben den Betrugsversuch entlarvt?
- Welche Gefühle oder Reaktionen sollen diese Verhaltensauslöser hervorrufen?

Mögliche Antworten/Prompts:

- Indikatoren für falsches Vertrauen: Phishing-Angreifende durchsuchen LinkedIn oder Unternehmens-Websites nach echten Projektnamen, damit die E-Mail authentischer wirkt.
- Warnsignale: Die Mitarbeiterin wird in der Phishing-E-Mail aufgefordert, Standardverfahren zu umgehen. Es wird verlangt, dass sie ihrer direkten Vorgesetzten gegenüber etwas geheim hält.
- Wichtigste Erkenntnis: Die authentisch aussehenden Elemente sind nur Tarnung. Die Verhaltenswarnsignale weisen auf die tatsächliche Gefahr hin.

Fazit

 **Dauer:** 5 Minuten

Schließen Sie die Übung ab, indem Sie die Konzepte in direkten Zusammenhang mit alltäglichen Gegebenheiten in Ihrer Organisation stellen. Erklären Sie, dass das Erkennen von Warnsignalen nur der erste Teil der Abwehr ist. Der zweite Teil besteht darin, die richtigen Maßnahmen in Einklang mit den Verfahren der Organisation zu ergreifen.

Beantworten Sie mögliche Fragen der Teilnehmenden zur internen Meldung solcher Betrugsversuche und zu den Tools, Kanälen und der Dokumentation, die zur Meldung solcher Vorfälle zur Verfügung stehen.

Anhang – Szenario-Handout

 **Verfassen**

 Posteingang

 Entwürfe

 Gesendet

 Markiert

 Spam

 Papierkorb

 Archiv

 Alle E-Mails

 Archivieren

 Spam

 Löschen

 Mehr

 Antworten

 Weiterleiten

Von: Markus Wagner <m.wagner@seeblick-logistik-intern.com>

An: Tanja Reiter

Betreff: **DRINGEND: Kaution für Lager in Berlin**

Hallo Tanja,

ich sitze gerade mit der Maklerfirma in Berlin zusammen. Wir könnten den Mietvertrag für das Lager, den wir im Meeting am Montag besprochen haben, sofort unterzeichnen.

Allerdings haben wir ein großes Problem. Ein anderes Unternehmen hat gerade ein Angebot für den Standort eingereicht. Die Maklerfirma sagt, wenn wir die Kaution von 50.000 € nicht in der nächsten Stunde überweisen, wird der Mietvertrag an das andere Unternehmen vergeben.

Helena Frey ist gerade im Flugzeug unterwegs und ich kann nicht auf ihre Freigabe warten. Die Maklerfirma wird noch nicht in unserem Anbieterportal geführt. Das Anlegen würde zu lange dauern.

Ich muss dich bitten, umgehend eine Direktüberweisung an die unten angehängten Kontodaten vorzunehmen. Das Ganze sollte unter uns bleiben, bis Helena landet, damit keine Panik entsteht und der Deal nicht platzt. Gib mir bitte Bescheid, sobald die Überweisung erledigt ist.

Mit freundlichem Gruß

Markus

 Anhang: Überweisungsdetails.pdf

Indikatoren für falsches Vertrauen: Standort des Absenders (Berlin), Erwähnung eines echten Projekts (Mietvertrag für ein Lager/Meeting), kennt Status und Name der CFO (Helena ist im Flugzeug unterwegs). **Verhaltenswarnsignale:** Extreme Dringlichkeit (nächste Stunde/anderes Unternehmen erhält sonst den Zuschlag), Umgehen von Verfahren (nicht im Anbieterportal), Geheimhaltung (sollte unter uns bleiben).