



Cyber Security Awareness Kampagne – Gezielt für den Ernstfall trainieren und nachhaltigen Schutz aufbauen

Allgemeine Informationen zur Kampagne

Nach Abschluss der ersten Phishing-Simulation (etwa dritter Monat im Serviceablauf) wird die Cyber Security Awareness Kampagne mit Ihnen besprochen und vorbereitet. Das 10-wöchige Programm ergänzt perfekt unsere soluzione Cyber Security E-Learning-Kurse. Es hilft, die in der Phishing-Simulation aufgedeckten Wissenslücken Ihrer Belegschaft schnell zu schließen und so den IT-Schutzschild des Unternehmens nachhaltig zu stabilisieren.

Beratung und Vorbereitung

Mithilfe der Phishing-Simulation haben Sie Einblick in solche Themen, auf die Ihre Mitarbeitenden nicht hereinfallen, sowie auf Beispiele, die häufiger angeklickt wurden. Ihr zuständiger Berater bereitet die Cyber-Security-Awareness-Inhalte passend zum Ergebnis der ersten Welle der Phishing-Simulation vor und stimmt diese detailliert mit Ihnen ab.

Themenplanung und Inhaltsabstimmung

Sie erhalten nun einen ausgearbeiteten Kommunikationsplan für insgesamt 10 Wochen. Zeitgleich wird die soluzione Kampagnen-Bibliothek regelmäßig aktualisiert und um aktuelle Themen erweitert. Beispielsweise empfehlen wir für den Wissensaufbau zum Thema Phishing folgenden Themenplan:

Woche 1: Welcome E-Mail mit Infos zum Ablauf und erste Fakten zum Thema „Phishing“

Woche 2: Woran erkenne ich Phishing-E-Mails?

Woche 3: Was ist Typosquatting?

Woche 4: Woran erkenne ich gefälschte Login-Seiten?

Woche 5: Wie kann ich die tatsächliche URL hinter einer Verlinkung erkennen?

Woche 6: Phishing E-Mails entlarven

Woche 7: Verhaltensweise, wenn eine Phishing-E-Mail geöffnet wurde

Woche 8: Welche E-Mail-Anhänge sind gefährlich und wie erkenne ich diese?

Woche 9: Achtung: Telefon- und SMS-Phishing

Woche 10: Phishing-Detektiv! Ich finde alle Fehler!

Unser Erfolgsversprechen:

- schnelle Nutzeraktivierung
- einfache Umsetzung in den Arbeitsalltag
- hohe Akzeptanz bei den Mitarbeitenden
- Aufbau nachhaltiger Gewohnheiten



Individuelle Awareness-Inhalte

Keine Organisation gleicht der anderen – das gilt auch für die Ergebnisse einer Phishing-Simulation. Aus genau diesem Grund bieten wir Ihnen Spielraum für individuelle Anpassungen. Um Ihren IT-Sicherheitsschutz so schnell wie möglich zu stärken, ersetzen wir bis zu drei Themen durch individuelle soluzione Security-Learning-Nuggets. So können Sie vorhandene Wissenslücken schließen und gleich für die nächsten Simulationen Verbesserungen erzielen. Unsere Empfehlung für diese Anpassung erfolgt im Beratungsgespräch.



Inhaltliche und technische Vorbereitung



Nach Abschluss der Inhaltsklärung startet das soluzione Content-Team mit der Ausarbeitung der Kampagnenbausteine – inklusive der für Sie passenden individuellen Themen. Parallel dazu kümmern sich fachliche Experten um die technische Implementierung der Kampagne. Die fertigen Individual-Themen werden Ihnen vor dem Start der Kampagne extra vorgestellt.

Kampagnenstart und -ablauf

Gemeinsam mit Ihnen legen wir nun das genaue Datum für den Start der Kampagne fest. Ab diesem Zeitpunkt verschicken wir über die nächsten 10 Wochen jeweils eine E-Mail mit Awareness-Nuggets an Ihre Mitarbeitenden. Darin leiten wir das für die Woche geplante Thema ein und verlinken eine Detailseite mit weiterführenden Erklärungen, Videos und Tipps.



Statistik und Auswertung



Sie erhalten für jede umgesetzte Phishing-Welle einen Report mit speziell aufbereiteten Ergebnisberichten. Nach Abschluss der dritten Welle konsolidiert Ihr Consultant die Daten für eine erste Live-Besprechung und bietet eine nähere Analyse: Verteilung der Klickzahlen pro Simulation bzw. im Gesamtverlauf, Ableiten eines Trends oder einer Tendenz usw. Er berät auch zur Planung weiterer Schritte und bereitet darauf aufbauend die nächste Phishing-Welle vor.