NEXT-GEN SECURITY AWARENESS TRAINING

VALUE PROPOSITION & USPs

HORNETSECURITY

ESI® als Benchmark

Der Employee Security Index (ESI®) ist ein wissenschaftlich fundiertes und patentiertes Verfahren zur standardisierten und transparenten Messung des Sicherheitsverhaltens in einem Unternehmen sowie für den abteilungs- und branchenübergreifenden Vergleich.

Für die Berechnung des ESI® messen und vergleichen wir nicht einfach Klickraten. Mit unserem Security Awareness Training simulieren wir Angriffsszenarien verschiedener Schwierigkeitslevel. Die resultierenden Klickraten werden unterschiedlich gewertet, um den herrschenden Sicherheitsstandard möglichst genau abzubilden. Somit wird das komplexe Thema des menschlichen Sicherheitsbewusstseins auf einer Skala von 1 bis 100 messbar, von Abteilung zu Abteilung sowie Unternehmen zu Unternehmen vergleichbar und intern sowohl mit der Geschäftsführung als auch Mitarbeitern kommunizierbar.

USP

Der ESI® ermöglicht es den Kunden, eine konkrete Zielvereinbarung zu treffen - also einen Wert für das angestrebte Zielsicherheitsniveau festzulegen, den man mit der Awareness Security Suite erreichen möchte.

Der ESI ® als klare und leicht verständliche KPI in Ampel-Farben ermöglicht auch für Laien ein einfaches Verständnis, wie das aktuelle Sicherheitsniveau aktuell dasteht. Damit wir die Kommunikation mit dem Endkunden, der Geschäftsführung und den Mitarbeitern vereinfacht.

Zeitsparend Trainieren (Awareness Engine – Training im Autopiloten)

IT-Sicherheitsverantwortliche bzw. IT-Leiter müssen Sie sich nicht mit der konkreten Steuerung und Umsetzung der Trainings beschäftigen.

USP

Die preisgekrönte Awareness Engine setzt stattdessen Best Practices direkt um und schont somit die Ressourcen des IT-Security Teams, das sich nicht in die psychologischen und didaktischen Feinheiten einarbeiten muss.

Individuelles Training (Single User & Productivity Booster)

Die Awareness Engine identifiziert Nutzer mit besonderem Lernbedarf. Damit wird sichergestellt, dass Mitarbeiter mit zusätzlichem Lernbedarf nicht zu kurz kommen und intensiver geschult werden.

USP

Die Awareness Engine bietet die Möglichkeit für individuelle Lernpfade und trainiert User mit erhöhtem Lernbedarf automatisch intensiv weiter. Umgekehrt werden User mit gutem Lernerfolg weniger trainiert, wenn sie schon auf einem guten Sicherheitsniveau sind.

Spear-Phishing-Simulation bis zu Level 7 (Spear-Phishing-Engine)

Wie ein echter Angreifer nutzt die Spear-Phishing-Engine verschiedene psychologische Manipulationsfaktoren sowie öffentlich zugängliche Daten des Unternehmens (z. B. aus Arbeitgeberportalen) und mitarbeiterbezogene Informationen, um die Spear-Phishing-Simulation noch gezielter zu gestalten. So kann eine große Bandbreite an realitätsnahen und aktuellsten Angriffsszenarien abgebildet werden, die notwendig sind, um die Aufmerksamkeit zu erhöhen, das Security Mindset der Mitarbeiter im Alltag zu schärfen und die Mitarbeiter so gut wie möglich auf ausgeklügelte Spear-Phishing-Angriffe vorzubereiten.

USP

Die patentierte Spear-Phishing-Engine simuliert sogar ausgeklügelte Phishing-Angriffe, die einen realistischerscheinenden Antwortverlauf enthalten, wie es zum Beispiel der Fall sein könnte, wenn ein Geschäftspartner oder Kollege gehackt wurde.

Einzigartig am Markt: In Kombination mit Hornetsecurity 365 Total Protection oder Spam und Malware Protection kann die Spear-Phishing-Engine sogar die individuellen User-Mail-Postfächer auslesen und in den Phishing-Szenarien Bezug zu Themen herstellen, welche der Empfänger selbst gerade bearbeitet, z. B. ein Status-Update zu einem laufenden Projekt, an dem der Empfänger beteiligt ist.

Wirksamkeit von E-Learnings + Trainings

Die Security Awareness Suite legt Wert darauf, dass zunächst das Security Mindset – die Grundlage und Motivation für das Awareness Training – bei den Mitarbeitern aufgebaut wird. Auf der Basis wird anschließend das Skillset trainiert - also die konkreten Fähigkeiten der Mitarbeiter, Angriffe zu vermeiden, zu erkennen und richtig zu reagieren.

USP

Indem wir zunächst das Verständnis – das Mindset - für die eigene Verantwortung stärken, schaffen wir die Basis für eine nachhaltige Sicherheitskultur. Die Mitarbeiter lernen so am besten, sich vor Cyber-Angriffen wirksam zu schützen und sich in bestimmten situativen Momenten richtig zu verhalten.

Just-in-Time-Training: Most Teachable Moment

Die Security Awareness Suite bietet den Nutzern nach Klick auf eine schadhafte E-Mail eine Erklärseite, auf der sie erfahren, anhand welcher Merkmale sie die Spear-Phishing-Mail hätten erkennen können und welche manipulativen Tricks genutzt wurden. Dies geschieht im "Most Teachable Moment", ein Moment, in dem Mitarbeiter besonders empfänglich für Aufklärung und Verhaltensänderung sind.

USP

Mitarbeiter erhalten ihr Security Awareness Training genau dann, wann sie es brauchen: im Most Teachable Moment. So wird besonders effektiv und effizient trainiert.

Vergleich und Gamification: Security Hub

Mitarbeiter haben im Security Hub die Möglichkeit, ihre detaillierte Phishing-Auswertung einzusehen und über den gesamten Trainingszeitraum auf sämtliche ihrer individuellen Phishing-Mails zurückzugreifen. So erfahren sie, über welche manipulativen Tricks sie besonders angreifbar sind. Das gibt ihnen auch die Möglichkeit, die individuellen Phishing-Mails, Trainings und Quizze jederzeit zu wiederholen und somit wichtige Lernbestandteile zu festigen.

Zudem können Sie in ihrer Gamification Forschritts-Anzeige ihr Sicherheitsniveau einsehen und ein individuelles Teilnahme-Zertifikat generieren.

USP

Mitarbeiter werden dank Gamification in einen Wettbewerb hineingezogen und können jederzeit den aktuellen Stand ihres Sicherheitsverhaltens einsehen. Damit wird die Motivation & Lernbereitschaft gestärkt.

Attraktive Konditionen für Partner und Kunden

Die Security Awareness Suite ist von vornherein für eine längerfristige Nutzung konzipiert, da die Etablierung einer nachhaltigen Sicherheitskultur, in dem das Unternehmen auch auf Mitarbeiterseite wirksam vor Cyber-Risiken geschützt wird, nicht von heute auf morgen, sondern nur über ein kontinuierliches Training über einen längeren Zeitraum stattfinden kann und gleichzeitig die Nutzung von E-Mail Security und Backup-Lösungen von Hornetsecurity den Lebenszyklus der IT-Sicherheit ganzheitlich abdeckt.

USP

Partner und Kunden von Hornetsecurity erhalten attraktive Nachlässe, wenn sie vorab Mehrjahresverträge abschließen, und damit das am Markt leistungsfähigste Cloud E-Mail Security und Backup-Portfolio zu günstigeren Konditionen als beim Wettbewerber abschließen und zentral aus dem CP heraus aktivieren und managen können.

Hornetsecurity GmbH · Am Listholze 78 · 30177 Hannover
Tel.: +49 511 515 464-0 · info@hornetsecurity.com · www.hornetsecurity.com
Umsatzsteuer-ID: DE256599255 · Geschäftsführer: Daniel Hofmann, Daniel Blank · Amtsgericht Hannover · HRB 201937
Hannoversche Volksbank · IBAN: DE74 2519 0001 0573 5742 00 · BIC: VOHADE2H