DTS
Security Awareness Training

Security Awareness Training

Die moderne IT-Bedrohungslandschaft weist neben technischen Faktoren eindeutig auch eine Reihe von menschlichen Elementen auf. Dieser „Faktor Mensch" ist ein beliebtes Ziel für Cyberangriffe. Ein Großteil dieser Attacken beginnt mit einer E-Mail. Zwar gibt es Technologien zur Erkennung und Blockierung gefährlicher E-Mails, die letzte Sicherheitsinstanz ist allerdings der Endbenutzer. Sie gilt es als finale Hürde zu überwinden, denn mit ihnen steht und fällt die Sicherheit von sensiblen Unternehmensdaten. Aus diesem Grund sind Security Awareness Trainings unverzichtbar, um die Wahrscheinlichkeit erfolgreicher Phishing- oder Ransomware-Angriffe durch effektive Bedrohungssimulationen und weiterbildende Maßnahmen zu verringern. Unser Proofpoint Security Awareness Training (PSAT) ist einzigartig auf diesem Gebiet und nutzt branchenführende Risikoinformationen und wissenschaftliche Lernprinzipien, um die richtige Ausbildung zur richtigen Zeit an die richtigen Personen zu vermitteln. Wir stärken Ihre letzte Verteidigungslinie erheblich.

- Ganzheitliches Security Awareness Training
- Individuelle, zielgerichtete, interaktive Schulungsmodule mit voller Flexibilität
- Phishing-Simulationen
- Optimierung des Benutzerverhaltens & der Reaktion auf Phishing-Angriffe
- Reporting
- Unbegrenzte Plattformnutzung
- DTS Managed Services

Das PSAT beruht auf einer vierteiligen Methodik, erfunden von drei Forschern und Fakultätsmitgliedern der Carnegie Mellon University. Bei ihren Forschungen für die National Science Foundation und das Verteidigungsministerium erkannten sie, dass traditionelle Schulungsmethoden nicht wirksam sind, um das Risiko und die Anfälligkeit für Cyberangriffe tatsächlich zu reduzieren. Stattdessen entwickelten sie ein kontinuierliches Training, mit kurzen, interaktiven und spielbasierten Schulungen sowie dem Einsatz von simulierten Phishing-Angriffen. Dies hat sich bei Verhaltensänderungen nachweislich als wirksamer erwiesen.

Das ganzheitliche Security Awareness Training identifiziert im ersten Schritt das Risiko, wer angegriffen wird und welche Schutz-Fähigkeiten vorhanden sind. Hierzu können mit ThreatSim und CyberStrength Attacken simuliert und Grundwissen erfragt werden. Die branchenführenden Bedrohungsinformationen von Proofpoint greifen auf die Daten von Milliarden von B2B- und B2C-E-Mails zu. So können realistische Dynamic Threat Simulation Phishing Vorlagen erstellt werden. Alles in allem entsteht auf diese Art eine Grundlinienmessung zur Identität der Very Attacked People (VAP) und der Angriffe, die sie sehen. Auf diese Weise können entscheidende Prioritäten gesetzt werden.

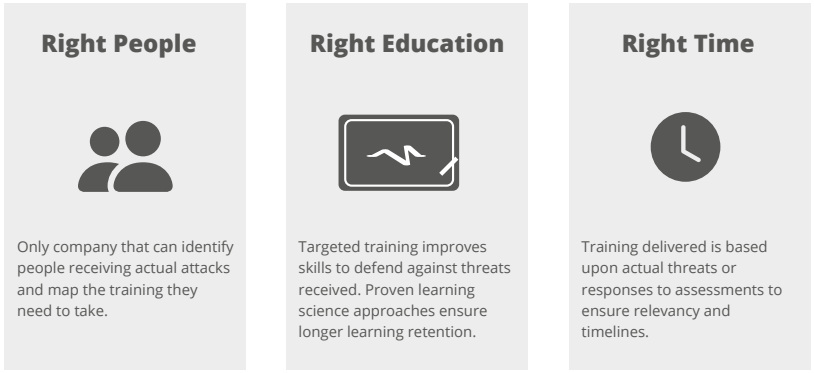
Im nächsten Schritt kann gezielt durch interaktive Trainingsmodule das Bewusstsein geschult werden, um Verhaltensänderungen zu bewirken. Die Schulung von Proofpoint ist hierbei einzigartig. Sie wird als Reaktion auf tatsächliche Bedrohungen und das Benutzerverhalten mit Learning Science Principles konzipiert. Die Schulungsinhalte werden kontinuierlich aktualisiert, um sich entwickelnde bewährte Verfahren und aktuelle Angriffstrends, die durch die Bedrohungsanalyse identifiziert wurden, widerzuspiegeln. Die effektiven, interaktiven, videobasierten und Gaming-Schulungsmodule fördern die Lernenden darin, Wissenslücken über Cybersicherheitsbedrohungen am Arbeitsplatz und darüber hinaus zu schließen. Sie bieten auch sofortiges Feedback.

Sobald Ihre Anwender geschult sind, sind sie in der Lage potenzielle Angriffe zu melden. Hierdurch verringert sich die Angriffsfläche. Die Closed-Loop Email Analysis and Response (CLEAR) rationalisiert in einem weiteren Schritt die Berichterstattung der Endbenutzer und die Sicherheitsreaktion auf Phishing-Angriffe. Somit sinkt die Zeit, welche zur Neutralisierung einer aktiven Bedrohung benötigt wird. Zu diesem Zweck sind die E-Mail-Reporting-Schaltfläche, PhishAlarm, und die Priorisierungs-Engine PhishAlarm Analyzer mit der Threat Response Auto-Pull (TRAP) verbunden.

Vervollständigt wird das PSAT durch die Reporting-Tools. Sie liefern alle Informationen zu den Endbenutzerrisiken, so dass Sie sich auf die Bereiche, Themen und Best Practices konzentrieren können, von denen Sie am meisten profitieren. Die Reports verfolgen den Wissensstand der Benutzer, die Gesamtleistung einer Phishing-Kampagne, detaillierte Informationen über die User-Leistung in den einzelnen Trainingsmodulen und ermöglichen das Sortieren und Filtern aller Berichte auf der Grundlage benutzerdefinierter Eigenschaften. Diese Einblicke helfen Administratoren, personalisierte Schulungen gezielt zu vergeben und so messbare Ergebnisse zu erzielen.

PSAT kombiniert Wissensbewertungen, simulierte Angriffe, interaktive Schulungsmodule, Berichterstattung und Verwaltungsfunktionen in einem einzigen, leicht zu bedienenden System. Natürlich kann die gesamte Plattform während der Lizenzlaufzeit unbegrenzt genutzt werden, um so beliebig viele Schulungsaufträge personalisiert zu erstellen und diese jederzeit zuweisen zu können. Ihre Administratoren haben die volle Flexibilität, die richtige Schulung den richtigen Personen zur richtigen Zeit zu vermitteln. Durch Anpassungsoptionen können die Schulung immer weiter individualisiert werden:

- Customization Center
  - Bearbeiten von Schulungsinhalten, inkl. Text/Fragen
  - Hinzufügen bzw. Entfernen von Bildern oder Fragen
- Hinzufügen von Richtlinien, Zertifikaten und mehr durch die Training-Jackets
- Modulkonfiguration



Die Assessments, simulierten Angriffe und interaktiven Schulungsmodule sind in mehr als 35 Sprachen verfügbar. Hierbei werden die Inhalte nicht einfach nur übersetzt. Sie werden entsprechend den Konventionen lokalisiert. Elemente wie Domänen, Marken oder Logos, Charaktere, Währungen und regionale Bezüge sind sprachlich angemessen und schaffen eine persönliche, relevante und ansprechende Schulungserfahrung für den Endbenutzer.