Proofpoint Security Awareness Training

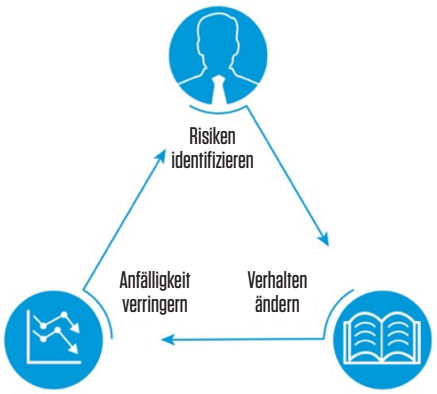
WICHTIGE VORTEILE

- Nachhaltige Änderung des Anwenderverhaltens und dadurch geringeres Risiko durch Phishing- und andere Cyberangriffe
- Bereitstellung weltweit einheitlicher Schulungen in einer Vielzahl an Sprachen
- Priorisierung und Verbesserung der Reaktionen auf Zwischenfälle
- Überwachung des Fortschritts mit dynamischem Reporting; Berichts-API
- Verringerung der Zahl erfolgreicher Phishing-Angriffe und Malware-Infektionen um bis zu 90 %

Mit den Proofpoint Security Awareness Trainings (PSAT) gewährleisten Sie, dass die richtigen Personen zum richtigen Zeitpunkt die richtigen Schulungen erhalten. Dadurch werden Ihre Endnutzer zur letzten starken Verteidigungslinie bei der Erkennung von Cyberangriffen und beim Schutz Ihres Unternehmens.

Da sich mehr als 90 Prozent aller Cyberangriffe gegen Anwender richten[1], steht und fällt der Schutz Ihres Unternehmens mit Ihren Mitarbeitern. Sicherheitstechnologien erkennen und blockieren Bedrohungen, bevor sie Ihre Anwender erreichen, können aber nicht alles stoppen. Ihre Mitarbeiter müssen darauf vorbereitet werden, Phishing-Angriffe und CEO-Betrug (Business Email Compromise) zu erkennen und angemessen zu reagieren. Mit der Proofpoint Security Awareness Training-Lösung lernen Ihre Anwender, Cyberangriffe erfolgreich zu erkennen und damit zu stoppen. Die Lösung bietet folgende Vorteile:

- Identifizierung von Anwenderrisiken
- Änderung des Mitarbeiterverhaltens
- Reduzierung der Angriffsfläche Ihres Unternehmens



1 Verizon: „2019 Data Breach Investigations Report“ (Untersuchungsbericht zu Datenkompromittierungen 2019), Juli 2019.

IDENTIFIZIEREN VON RISIKEN

Stellen Sie fest, welche Mitarbeiter im Unternehmen angegriffen werden, und bewerten Sie deren Kompetenz im Umgang mit Cyberbedrohungen.

Mit den Proofpoint Very Attacked People™ (VAP)-Berichten erhalten Sie einen Überblick über die besonders durch Cyberangriffe gefährdeten Mitarbeiter Ihres Unternehmens. Diese Berichte sind Bestandteil von Proofpoint Targeted Attack Protection (TAP) und zeigen zum Beispiel, wer mit welchen Bedrohungen gezielt angegriffen wird.

Mit ThreatSim®-Phishing-Simulationen können Sie anhand simulierter Phishing-E-Mails die reale Anfälligkeit Ihres Unternehmens für verschiedene Ausprägungen von Phishing-Angriffen feststellen. Mit tausenden unterschiedlichen Phishing-Vorlagen in 13 Kategorien können Sie Ihre Anwender in Bezug auf eine Vielzahl an Bedrohungsarten testen, darunter:

- Schädliche Anhänge
- Eingebettete schadhafte Links
- Anfragen zur Weitergabe sensibler oder personenbezogener Daten

Jede Woche kommen neue Vorlagen hinzu, damit auch die neuesten Angriffstrends immer berücksichtigt werden. Unsere Phishing-Vorlagen basieren auf Proofpoint-Bedrohungsdaten, werden aber auch auf konkreten Kundenwunsch erstellt und greifen zudem saisonbezogene Themen auf, wie sie auch von echten Cyberkriminellen benutzt werden. So wird sichergestellt, dass simulierte Phishing-E-Mails den realen Angriffen weitestgehend ähneln.

Wenn Anwender auf einen simulierten Angriff hereinfallen, erhalten sie sofort relevante Hinweise. So erfahren sie, welchen Zweck die Übung hat, welche Gefahren damit bei realen Angriffen verbunden sind und wie sie solche Köder in Zukunft besser erkennen können, um nicht mehr auf sie hereinzufallen. Zusätzlich können Sie allen Personen, die auf eine Phishing-Simulation hereinfallen, Schulungen zuweisen.

Außerdem haben Sie die Möglichkeit, die Kenntnisse Ihrer Mitarbeiter in anderen Bereichen, z. B. im Hinblick auf infizierte USB-Sticks, zu testen. Mit ThreatSim-USB-Simulationen lernen Ihre Mitarbeiter, die Gefahren infizierter USB-Geräte zu kennen. Sie können jederzeit und in beliebigem Umfang auf USB-Simulationen zugreifen, bei denen Anwender, die auf die Simulation hereinfallen, direkt relevante Hinweise erhalten, wodurch die Lernerfahrung deutlich verstärkt wird.

Der leistungsstarke CyberStrength®-Wissenstest überprüft die Schwachstellen Ihrer Anwender zu verschiedensten wichtigen Sicherheitsproblemen jenseits von E-Mails und USB-Sticks. Zu den Themen gehören der Umgang mit mobilen Endgeräten, das Erkennen von Social Engineering-Betrug sowie sicheres Surfen im Web. Ihnen steht für den Wissenstest eine Bibliothek mit hunderten vordefinierten Fragen in mehr als 35 Sprachen zur Verfügung. Zudem besteht die Möglichkeit, Anwender basierend auf den Testergebnissen entsprechend der dadurch eruierten Schwachstellen automatisch für die entsprechende Schulung anzumelden. Zusätzlich können Sie eigene Fragen zu den Richtlinien und Vorgehensweisen in Ihrem Unternehmen hinzufügen, um das Wissen Ihrer Anwender dazu zu ermitteln. Sobald Sie anhand des grundlegenden Wissenstests die Schwachstellen ermittelt haben, erhalten Sie Empfehlungen zur Verringerung der Risiken in den verschiedenen Bereichen.

ÄNDERN DES ANWENDERVERHALTENS

Mit Proofpoint Security Awareness Training können Sie Ihren Anwendern Schulungen basierend auf tatsächlichen Bedrohungen, dem Umgang der Mitarbeiter mit simulierten Angriffen sowie erfassten Wissenslücken bereitstellen.

Solide und relevante Inhalte sind für effektive Schulungen unabdingbar und die beste Möglichkeit, das Verhalten von Anwendern zu ändern. Mittels des Customization Centers in unserer Plattform können Sie die verfügbaren Inhalte selbst so anpassen, dass Sie für Ihre Anwender höchst relevant sind. Sie haben die Möglichkeit, die Texte, Bilder, Fragen, Bildschirminhalte und weitere Bestandteile des Schulungsmaterials anzupassen. Der Learning Science Evaluator prüft dabei, dass für alle angepassten Inhalte ein effektives Schulungserlebnis gewährleistet bleibt.

Ihre Anwender können die Schulungen jederzeit, überall und von jedem angeschlossenen Endgerät aus abrufen. Die Länge der einzelnen Module liegt bei lediglich 5 bis 15 Minuten, damit die täglichen Arbeitsabläufe möglichst wenig unterbrochen werden und höchste Aufmerksamkeit gewährleistet bleibt. Die interaktiven Module sind für Mobilgeräte geeignet und entsprechen den Standards U.S. Section 508 sowie den Web Content Accessibility Guidelines (WCAG) 2.0 AA.

Die Proofpoint-Schulungsmodule basieren auf wissenschaftlich bestätigten Lernprinzipien und decken ein breites Spektrum an Sicherheitsrisiken von Phishing-Angriffen bis zu Bedrohungen durch Insider ab. Folgende Materialien sind enthalten:

- **Schulungsmodule** mit Videos, Interaktionen und Gamification-Elementen. Sie stehen in mehr als 35 Sprachen zur Verfügung und enthalten lokalisierte Referenzen.
  - Inhalte zu speziellen Compliance- und Datenschutzanforderungen werden von unserem Partner TeachPrivacy zur Verfügung gestellt.
  - Um die Vielseitigkeit zu erhöhen und Anwender mit neuen Methoden zu unterhalten, wurden Inhalte von The Defence Works, einem durch Proofpoint übernommenen britischen Anbieter, hinzugefügt.
- **Materialien zur Steigerung des Sicherheitsbewusstseins** umfassen Videos, Infografiken, Newsletter, Artikel, Poster, Bilder und mehr, um die Wirkung der Schulungsprogramme zu verstärken.
- **Materialien zum Schulungsprogramm** bieten Administratoren nützliche Informationen zur Umsetzung eines effektiven Schulungsprogramms.

Über unsere Attack Spotlight-Reihe können Sie Ihre Endnutzer mit aktuellen Kurzinhalten vor Angriffen und Ködern warnen, die laut den Proofpoint-Bedrohungsdaten aktuell am relevantesten sind. Diese Inhalte vermitteln zudem, wie Anwender derzeit aktuelle Bedrohungen erkennen und vermeiden können.

VERRINGERUNG DER ANFÄLLIGKEIT

Geschulte Endnutzer melden potenzielle Bedrohungen und verringern so die Angriffsfläche.

Mit dem im E-Mail-Client als Add-in integrierten PhishAlarm® können Anwender verdächtige Nachrichten mit einem einzigen Klick melden. Anwender, die eine E-Mail melden, erhalten sofort positive Bestärkung in Form einer Popup-Meldung oder E-Mail mit einem Dankeschön. Dank des PhishAlarms müssen E-Mails nicht samt Header und Anhang an ein Abuse-Postfach weitergeleitet werden.

Mithilfe von PhishAlarm Analyzer werden gemeldete Nachrichten automatisch mit Proofpoint-Bedrohungsdaten angereicht sowie mittels der Proofpoint Reputationssysteme analysiert. Sie erhalten einen übersichtlichen Bedrohungsbericht mit detaillierten Informationen zur Nachricht und zu deren Kategorie (schädlich, Spam oder anderes), sodass Ihre Incident-Response-Teams Nachrichten nicht mehr einzeln untersuchen beziehungsweise priorisieren müssen. So lässt sich viel wertvolle Zeit einsparen. Proofpoint bietet Bedrohungsdaten mit einzigartigem Detailgrad, Umfang und besonderer Praxisrelevanz. Mehr als 100 Mitarbeiter bei Proofpoint analysieren mehr als jede fünfte der täglich weltweit versendeten B2B- und B2C-E-Mails sowie Cloud-bezogene und Social-Media-Bedrohungen.

Unsere automatisierte Lösung CLEAR (Closed-Loop Email Analysis and Response) sendet gemeldete Nachrichten an TRAP (Threat Response Auto-Pull). Mit dieser Lösung werden E-Mails automatisch unter Quarantäne gestellt, freigegeben oder an Ihr Incident Response Team weitergegeben. Außerdem können Administratoren benutzerdefinierte Antworten erstellen, die an Endnutzer gesendet werden. Damit wird richtiges Verhalten gestärkt und eine sicherheitsbewusste Kultur aufgebaut.

ANALYSEERGEBNISSE DURCH REPORTING MIT VOLLEM FUNKTIONSUMFANG

Unsere umfassenden Berichte halten Sie über den Fortschritt Ihrer Anwender auf dem Laufenden. Sie sind übersichtlich aufgebaut, bewerten den Fortschritt, berechnen die Rendite und behalten die Entwicklung der Anwenderkompetenz im Blick. Durch den detaillierten und umfassenden Überblick erhalten Sie ein vollständiges Bild. Außerdem sehen Sie, wie Ihre Mitarbeiter mit Tests, simulierten Angriffen und Schulungsaufgaben interagiert haben. Über Dashboards lassen sich schnell Daten filtern, Tests vergleichen, Auswertungsfaktoren ändern sowie vieles mehr.

Die Berichte können für die Weitergabe an andere Personen oder für detailliertere Analysen und Vergleiche heruntergeladen und exportiert werden. Das ist zum Beispiel nützlich, wenn Sie Kennzahlen gemeinsam mit anderen Sicherheitsereignissen auswerten möchten. Außerdem haben Sie die Möglichkeit, die Berichterstellung zu automatisieren und die automatische Übermittlung von Berichten in regelmäßigen Intervallen an sich selbst und zuständige Verantwortliche zu planen.

Mit unserer ebenfalls enthaltenen Berichts-API erhalten Sie Zugriff auf Berichte und Analysen zu Schulungen, Phishing, Wissenstests, Anwendern und E-Mails. Diese Informationen lassen sich in gängige Business-Intelligence-Tools und Learning-Management-Systeme integrieren.

WEITERE INFORMATIONEN

Weitere Informationen finden Sie unter **proofpoint.com/de**.