proofpoint.

PROOFPOINT-SECURITY AWARENESS-TRAINING

WICHTIGE VORTEILE

- Änderung des Anwenderverhaltens und dadurch geringeres Risiko durch Phishing- und andere Cyberangriffe
- Priorisierung und Verbesserung der Reaktionen auf Zwischenfälle
- Bereitstellung weltweit einheitlicher Schulungen in mehreren Sprachen
- Nachverfolgung der Ergebnisse und Fortschritte mit Echtzeitberichten
- Verringerung der Zahl erfolgreicher Phishing-Angriffe und Malware-Infektionen um bis zu 90 %

Mit Proofpoint-Security Awareness-Training (ehemals Wombat Security) können Sie den richtigen Personen zum richtigen Zeitpunkt die richtigen Schulungen bereitstellen. Das macht aus Ihren Endnutzern eine starke letzte Verteidigungslinie, die Cyberangriffe erkennt und so Ihr Unternehmen schützt.

Da mehr als 90 Prozent aller Cyberangriffe mit einer E-Mail beginnen, steht und fällt die Sicherheit Ihrer Mitarbeiter und Daten mit aufmerksamen Endnutzern. Selbst wenn die Lösung des Problems auch Technologien zur Erkennung und Blockierung schädlicher E-Mails umfasst, können Sie die Wahrscheinlichkeit erfolgreicher Phishing- oder Ransomware-Angriffe mit effektiven Security Awareness-Trainings weiter reduzieren.

SCHUTZ IHRES UNTERNEHMENS MIT THREATSIM-PHISHING-SIMULATIONEN

Mit ThreatSim®-Phishing-Simulationen können Sie die Anfälligkeit Ihres Unternehmens für verschiedene Phishing- und Spearphishing-Angriffe feststellen. Mit tausenden verschiedenen Phishing-Vorlagen in 13 Kategorien können Sie Ihre Anwender in Bezug auf mehrere Bedrohungsarten testen, darunter:

- Schädliche Anhänge
- Eingebettete Links
- Anfragen zur Weitergabe personenbezogener Daten

Jeden Monat kommen neue Vorlagen hinzu. Unsere Phishing-Vorlagen für dynamische Bedrohungssimulationen basieren auf Proofpoint-Bedrohungsdaten und einige beziehen sich auf Kundenanfragen und saisonale Themen.

Anwender, die auf einen simulierten Angriff hereinfallen, erhalten sofort relevante Hinweise. So erfahren sie, welchen Zweck die Übung hat, welche Gefahren damit bei realen Angriffen verbunden sind und wie diese Fallen in Zukunft vermieden werden können. Zusätzlich können Sie Ihre am stärksten gefährdeten Anwender unterstützen, indem Sie allen Personen, die auf eine Phishing-Simulation hereinfallen, interaktive Schulungen zuweisen.

SCHWACHSTELLENTESTS MITHILFE VON CYBERSTRENGTH

CyberStrength® ist ein leistungsstarkes webbasiertes Tool für Wissenstests, mit denen Sie die potenziellen Schwachstellen Ihrer Mitarbeiter aufdecken können, ohne simulierte Phishing-Angriffe durchführen zu müssen. Nachdem Sie die Grundlagen für den Kenntnisstand Ihrer Mitarbeiter festgelegt haben, behalten Sie mit regelmäßigen Nachtests einen Überblick über den Fortschritt und über wichtige Themenbereiche, die in den Fokus weiterer Schulungen rücken sollten.

Wir bieten eine Bibliothek mit mehr als 200 Fragen zu verschiedensten wichtigen Cybersicherheitsthemen. Zusätzlich können Sie eigene Fragen zu den Richtlinien und Vorgehensweisen in Ihrem Unternehmen erstellen. Mit CyberStrength können Sie feststellen, wo Ihr Unternehmen, Ihre jeweiligen Abteilungen und sogar die einzelnen Mitarbeiter besonders für Angriffe anfällig sind.

SCHULUNG IHRER MITARBEITER MIT ANSPRECHENDEN UND RELEVANTEN SCHULUNGSINHALTEN

Unsere kontinuierlich wachsende und aktualisierte Inhaltsbibliothek umfasst interaktive Schulungsmodule, Videos, Poster und Bilder in mehr als 35 Sprachen, die konsistente, umsetzbare und für weltweit tätige Unternehmen relevante Botschaften vermitteln. Unsere anpassbaren Schulungsinhalte basieren auf wissenschaftlich bestätigten Lernprinzipien und decken eine Vielzahl an Sicherheitsrisiken ab, die von Phishing-Angriffen bis zu Insider-Risiken reichen.

Die interaktiven Schulungsmodule sind auf Abruf verfügbar und für Mobilgeräte geeignet, damit Ihre Anwender unsere Schulungen jederzeit, überall und auf allen vernetzten Geräten nutzen können. Das verbessert die Effizienz und gewährleistet die bequeme Nutzung. Die Länge der einzelnen Module liegt bei lediglich 5 bis 15 Minuten, damit die täglichen Arbeitsabläufe möglichst wenig unterbrochen werden. Unsere Module entsprechen den Standards U.S. Section 508 sowie den Web Content Accessibility Guidelines (WCAG) 2.0 AA.

Mit unserer Attack Spotlight-Reihe können Sie Ihre Anwender ganz einfach über besonders relevante Phishing-Angriffe und Köder informieren. Mithilfe dieser kurzen und zeitnah bereitgestellten Inhalte können Ihre Anwender aktuelle Bedrohungen erkennen und rechtzeitig abwehren.

RISIKOMINIMIERUNG DURCH PHISHALARM, PHISHALARM ANALYZER UND CLEAR

Mit dem E-Mail-Client-Add-in PhishAlarm® können Anwender verdächtige Nachrichten mit einem einzigen Mausklick melden. Anwender, die eine E-Mail melden, erhalten sofort positive Bestärkung in Form einer Popup-Meldung oder E-Mail mit einem Dankeschön. Mithilfe von PhishAlarm Analyzer werden gemeldete Nachrichten automatisch analysiert und ihr Kontext mit verschiedenen Proofpoint-Bedrohungsdaten sowie Reputationssystemen angereichert. Dabei werden sie als schädlich, verdächtig, Massen-E-Mails oder Spam eingestuft.

Unsere Lösung CLEAR (Closed-Loop Email Analysis and Response) sendet gemeldete Nachrichten an TRAP (Threat Response Auto-Pull). In dieser Lösung können klassifizierte Nachrichten automatisch isoliert oder Warnungen an Vorfallreaktionsteams zur Untersuchung weitergegeben werden. Mithilfe von TRAP lassen sich aktive Angriffe dank der Unterstützung durch geschulte Endnutzer innerhalb von Minuten aufhalten.

ANALYSEERGEBNISSE DURCH REPORTING MIT VOLLEM FUNKTIONSUMFANG

Unsere Berichterstellungsfunktionen bieten den detaillierten und umfassenden Überblick, den Sie über die Interaktionen Ihrer Mitarbeiter mit den Tests, simulierten Angriffen sowie Schulungsaufgaben benötigen. Wir bieten schnelle und verständliche Berichte über eine moderne Benutzeroberfläche. Sie erfahren nicht nur, wer Schulungen abgeschlossen hat, sondern können auch den Fortschritt bewerten, die Rendite berechnen und die Anwenderkompetenz per Benchmark auswerten, nachverfolgen sowie im Verlauf betrachten. Über unsere Dashboards können Sie unkompliziert Daten filtern, Zuweisungen vergleichen, Auswertungsfaktoren schnell hinzufügen und entfernen sowie vieles mehr.

Sie können die Daten auch herunterladen und exportieren, um die Business Intelligence an andere Verantwortliche weiterzugeben, detailliertere Analysen durchzuführen sowie Kennzahlen zu anderen Sicherheitsereignissen auszuwerten. Unsere Funktion für automatisierte Meldungen vereinfacht den Exportprozess, d. h. Sie können festlegen, dass Berichte automatisch regelmäßig an Ihre eigene Adresse sowie an festgelegte Personen innerhalb Ihres Unternehmens zugestellt werden.

INFORMATIONEN ZU UNSEREM ANSATZ DER KONTINUIERLICHEN SCHULUNG

Untersuchungen haben ergeben, dass sich der Kampf gegen Cyberangriffe mit einmal jährlich stattfindenden Präsenzschulungen nicht gewinnen lässt. Unser einzigartiger Ansatz der kontinuierlichen Schulung umfasst einen Zyklus, der Anwender zu empfohlenen Vorgehensweisen sowie darin schult, wie sich diese auf reale Sicherheitsbedrohungen anwenden lassen.

Mit einem kontinuierlichen Zyklus aus Tests, Schulungen, Festigung und Auswertung werden die Lernergebnisse maximiert. Außerdem wird sichergestellt, dass sie dauerhaft gefestigt sind. Unser Ansatz steht im starken Kontrast zum „Einmal und fertig“-Ansatz und bietet Ihnen die Flexibilität, Ihr Programm im Laufe der Zeit weiterzuentwickeln, konkrete anfällige Bereiche zu identifizieren sowie zu besonders wichtigen Zeitpunkten oder Bereichen gezielte Schulungen anzubieten.

INFORMATIONEN ZU PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT) ist ein führendes Cybersicherheitsunternehmen. Im Fokus steht für Proofpoint dabei der Schutz der Mitarbeiter. Denn diese bedeuten für ein Unternehmen zugleich das größte Kapital aber auch das größte Risiko. Mit einer integrierten Suite von Cloud-basierten Cybersecurity-Lösungen unterstützt Proofpoint Unternehmen auf der ganzen Welt dabei, gezielte Bedrohungen zu stoppen, ihre Daten zu schützen und IT-Anwender in den Unternehmen für Risiken von Cyberangriffen zu sensibilisieren. Führende Unternehmen aller Größen, darunter mehr als die Hälfte der Fortune-1000-Unternehmen, verlassen sich auf Proofpoint, um ihre wichtigsten Sicherheits- und Compliance-Risiken bei der Nutzung von E-Mails, der Cloud, Social Media und dem Internet zu minimieren. www.proofpoint.com/de