proofpoint.

PROOFPOINT PHISHING-SIMULATION UND SICHERHEITSBEWUSSTSEIN

VORTEILE

- Ändern des Benutzerverhaltens zur Verringerung von Risiken durch Phishing- und Ransomware-Angriffe
- Priorisieren und Verbessern der Reaktion auf Vorfälle
- Weltweite Bereitstellung einheitlicher Schulungen durch mehrsprachigen Support
- Protokollieren der Ergebnisse und des Fortschritts durch Echtzeit-Berichterstellung

Proofpoint Phishing-Simulation und Sicherheitsbewusstsein hilft Ihnen, Ihre Mitarbeiter über die Taktiken bei E-Mail-Angriffen zu testen und weiterzubilden. Sie erhalten eine zusätzliche Sicherheitsstufe, die Folgendes bietet:

- Stärkung des Bewusstseins
- Verringerung der erfolgreichen Phishing-Angriffe und Malware-Infektionen
- Vermeidung zukünftiger Datenschutzverletzungen

Mehr als 90 % der Cyberangriffe beginnen mit einer E-Mail. Der Schutz Ihres Personals und Ihrer Daten ist unerlässlich. Lösungen, die schädliche E-Mails erkennen und blockieren, sind ein Teil der Lösung. Sie können zudem die Wahrscheinlichkeit erfolgreicher Phishing- oder Ransomware-Attacken durch effektive Bedrohungssimulationen und Schulungen über das Sicherheitsbewusstsein verringern.

SCHUTZ IHRER ORGANISATION MIT THREATSIM PHISHING-SIMULATIONEN

Erfahren Sie mithilfe von ThreatSim® Phishing-Simulationen, welche Mitarbeiter für Phishing- und Spear-Phishing-Angriffe anfällig sind. ThreatSim ermöglicht Sicherheitsteams Phishing-Angriffe zu simulieren. Sie erhalten mehr als 500 verschiedene Phishing-Vorlagen in 30 Sprachen und 13 Kategorien. Sie können Benutzer hinsichtlich mehrerer Bedrohungen beurteilen, beispielsweise:

- Schädliche Anlagen
- Eingebettete Links
- Anforderungen personenbezogener Daten
- Und mehr

Wir fügen jeden Monat basierend auf Kundenanfragen, saisonbedingten Themen und Phishing-E-Mails aus der Praxis neue Vorlagen hinzu.

Benutzer, die auf einen simulierten Angriff hereingefallen sind, erhalten zeitnahe praktische Unterweisungen. Sie erfahren mehr über den Zweck der Übung, die Gefahren tatsächlicher Angriffe sowie Anweisungen, wie diese in Zukunft verhindert werden können. Sie können Ihren verletzbarsten Benutzern helfen, indem Sie Mitarbeitern, die sich durch eine ThreatSlim-Simulation haben täuschen lassen, automatisch interaktive Schulungen zuweisen.

WEITERBILDUNG DER MITARBEITER MITTELS INTERAKTIVER SCHULUNGSMODULE

Sie erhalten mehr als 30 interaktive Schulungsmodule in mehr als 30 Sprachen. Benutzer erhalten in spielerischen und szenarienbasierten Modulen praktische Erfahrung beim Erkennen und Vermeiden zahlreicher unterschiedlicher Phishing-Angriffe und anderer Social Engineering-Betrügereien. Durch unsere anpassbaren Anfangs- und Endsegmente können Sie zu Beginn eines jeden Moduls Inhalt hinzufügen und die einzelnen Module abschließen.

Schulungen sind auf Abruf verfügbar. Jedes Modul kann in 5 bis 15 Minuten abgeschlossen werden, um die Unterbrechung der täglichen Arbeit gering zu halten.

REDUZIEREN DER RISIKEN MIT PHISHALARM UND PHISHALARM ANALYZER

PhishAlarm® bringt Phishing-Schutz auf den Desktop. Das PhishAlarm E-Mail-Client-Add-In ist in ThreatSim inbegriffen, damit Ihre Mitarbeiter verdächtige Nachrichten mit einem Mausklick melden können. Benutzer, die eine E-Mail melden, erhalten umgehend eine positive Bestätigung in Form einer „Dankesmeldung“ als Popup-Dialog oder E-Mail.

PhishAlarm Analyzer priorisiert gemeldete Nachrichten und verbessert die Reaktion auf Vorfälle. Er ermöglicht Administratoren die schnelle Prüfung wichtiger Details und hilft ihnen Entscheidungen zu treffen und Maßnahmen einzuleiten. Mit PhishAlarm und PhishAlarm Analyzer können Sie das Gefahrenpotenzial aktiver Phishing-Angriffe verringern.

BEWERTEN VON SCHWACHSTELLEN MIT CYBERSTRENGTH

Cyberstrength® ist ein leistungsstarkes, webbasiertes Bewertungstool, das Bereiche identifiziert, in denen Ihre Mitarbeiter anfällig für Angriffe sind, ohne dass Sie einen simulierten Angriff ausführen müssen. Cyberstrength etabliert einen Basislinienwert über das Verständnis kritischer Cybersicherheitsthemen Ihrer Mitarbeiter. Von diesem Ausgangspunkt aus kann in regelmäßigen Abständen neu bewertet werden, welche Fortschritte erzielt wurden und welche Schwachstellen noch nachgebessert werden müssen.

Wir bieten eine Bibliothek mit mehr als 175 Fragen. Sie können zudem Ihre eigenen Fragen verfassen, um abzuschätzen, wie gut die Mitarbeiter Ihrer Organisation die Richtlinien und Verfahren kennen. Mit Cyberstrength können Sie identifizieren, wo Schwachstellen vorhanden sind — auf organisatorischer Ebene bis hinunter zu einzelnen Mitarbeitern.

Unsere Lösungen zur Bedrohungssimulation und zum Sicherheitsbewusstsein sind in verschiedenen Paketen erhältlich, die Ihr Risikoprofil durch Mitarbeiterschulungen und Tests verbessern.

Funktionen	Anti-Phishing	Grundlagen	Enterprise
ThreatSim	✔	✔	✔
PhishAlarm	✔	✔	✔
PhishAlarm Analyzer			✔
CyberStrength		✔	✔
Anzahl der Schulungsmodule	3	12	Alle

ÜBER PROOFPOINT

Proofpoint Inc. (NASDAQ: PFPT), ein Unternehmen für Internetsicherheitslösungen der nächsten Generation, ermöglicht Organisationen, das Arbeitsumfeld ihrer Mitarbeiter gegenüber fortschrittlichen Bedrohungen und Compliance-Risiken zu verteidigen. Proofpoint hilft Internetsicherheitsexperten dabei, ihre Anwender vor den hochentwickelten Angriffen zu schützen, die in E-Mails, mobilen Apps und in den sozialen Netzwerken gegen sie gerichtet werden. Das Unternehmen schützt die von den Mitarbeitern erstellten wichtigen Daten und stattet Teams mit den richtigen Informationstools aus, die ihnen bei Problemen eine schnelle Reaktion ermöglichen. Führende Unternehmen aller Größenordnungen, darunter mehr als 50 Prozent der Fortune 100-Unternehmen, vertrauen auf Proofpoint-Lösungen, die für die mobilen und von den sozialen Netzen geprägten Umgebungen der heutigen Zeit konzipiert sind. Zur Bekämpfung der modernen Bedrohungen stützen sich die Lösungen sowohl auf die Macht der Cloud als auch auf eine große datengesteuerte Analyseplattform.