Managed Service für Proofpoint Security Awareness Training für mittlere Unternehmen

Branchenführende Expertise für die Einrichtung und Verwaltung Ihres Security Awareness-Programms

Produkte

- Proofpoint Security Awareness Training

Wichtige Vorteile

- Unterstützung durch dedizierte Experten, die die Risiken durch Ihre Anwender schneller reduzieren, indem sie ein Best Practice-basiertes erstklassiges Programm zur Sensibilisierung für Sicherheit implementieren
- Umfassende Schulungsmaterialien (einschließlich Tools zur Festigung), um das Anwenderverhalten und die Unternehmenskultur zu verbessern
- Detaillierte und nützliche Berichte, die einen ganzheitlichen Überblick über das Security Awareness-Programm Ihres Unternehmens und die Bereitschaft Ihrer Anwender liefern

Konzentrieren Sie sich auf Ihre geschäftlichen Aktivitäten – wir kümmern uns um Ihr Programm zur Sensibilisierung für Sicherheit. Der Managed Service für Proofpoint Security Awareness Training für mittlere Unternehmen übernimmt die Konzeption, Umsetzung und Dokumentation von Schulungsprogrammen bei kommerziellen Kunden mit bis zu 2.500 Anwendern. Wir stellen Ihnen dedizierte Experten an die Seite, die Sie mit einem wirksamen, individuellen Ansatz bei der Einrichtung und Durchführung Ihrer Schulungen zur Sensibilisierung für Sicherheit unterstützen. Gemeinsam entwickeln wir ein einfaches Programm, mit dem Sie Ihre Endnutzer über das gesamte Jahr hinweg effektiv ansprechen können.

Planung

Unser Expertenteam übernimmt die Verwaltung Ihres Programms zur Sensibilisierung für Sicherheit. Dabei konzentrieren sich unsere dedizierten Experten auf die Implementierung eines vorab definierten Programms, das auf bewährten Methoden basiert. Von Anfang an treffen Sie sich einmal monatlich mit Ihnen zugewiesenen Teammitgliedern, die als Ihre persönlichen Vertreter und wichtigste Kontaktpersonen agieren.

Launch

Wir entwickeln initiale Pläne, die Sie für Interaktionen mit wichtigen Verantwortlichen wie Personal-, IT- und Sicherheitsabteilungen und für die Vorstellung des Programms bei Ihren Anwendern nutzen können. Ihre Kontaktpersonen stellen eine Reihe von Leitfäden, Tools und Vorlagen bereit, die Sie für das Programm verwenden können. Zu diesen Materialien gehören:

- Leitfaden mit bewährten Methoden
- Kalender mit bewährten Methoden
- Beispielvorlagen für Phishing-Simulationen
- Vorlagen für Benachrichtigungen über zugewiesene Schulungen
- Vorlagen zur IT- und Helpdesk-Kommunikation
- Safelist-Dokumente

Kommunikation

Kommunikation ist für den Erfolg aller Maßnahmen wichtig. Wir empfehlen dringend die Ausarbeitung eines durchdachten Kommunikationsplans, der alle Verantwortlichen einbezieht. Dieser Plan sollte die Ziele des Programms formulieren und eine Kontaktperson innerhalb Ihres Unternehmens benennen, die bei jeglichen Fragen oder Sorgen angesprochen werden kann. Wir können gern Ihre internen IT- und Helpdesk-Teams darüber benachrichtigen, wann Kampagnen geplant sind. Dadurch erhalten die entsprechenden Teams detaillierte Informationen über die Kampagnen sowie die involvierten Gruppen und können sich auf Anfragen und Rückmeldungen von Anwendern vorbereiten. Wir können auch Beispielkommunikation bereitstellen, mit der Sie die Anwender über Ihr Security Awareness-Programm informieren. Das klärt die Zuständigkeit und steigert die Akzeptanz dieses wichtigen Schulungserlebnisses.

Technische Bereitschaft

Wir stellen Dokumente mit IP-Adressen bereit, die Sie in die Safelist Ihrer E-Mail-Server aufnehmen und anhand derer Sie Spam-Filter-Tests durchführen können. Außerdem müssen möglicherweise Ausnahmeregeln für die Firewalls oder Sicherheits-Appliances erstellt werden, damit Datenverkehr zu unseren Servern durchgelassen wird.

Anwenderverwaltung

Sie und Ihre Kontaktperson klären die Anwenderbasis des Programms ab. Sie legen fest, ob die Anwenderliste mit dem End-User Sync-Tool direkt aus dem Active Directory (AD)- oder Azure-Verzeichnis Ihres Unternehmens in unsere Plattform übernommen werden kann. Wenn dies nicht möglich ist, fordern wir eine Anwenderliste mit Datenelementen wie E-Mail-Adresse, Vor- und Nachname, Geschäftsbereich, Gruppe, Standort und bis zu drei weiteren Eigenschaften an. Wir korrelieren Ihre Berichtsanforderungen mit relevanten Informationen, die wir in unseren Gesprächen erhalten haben. Wir besprechen auch, wie Anwenderinformationen im Laufe der Zeit aktualisiert werden, um Neuanstellungen, ausgeschiedene Mitarbeiter sowie Positions- oder Abteilungswechsel zu berücksichtigen.

Komponenten des Security Awareness-Programms

Ihr Programm zur Sensibilisierung für Sicherheit kann (je nach den von Ihnen lizenzierten Produkten) folgende Komponenten enthalten:

- Simulationen von Angriffen
- Wissenstests
- Schulungen
- Materialien zur Sensibilisierung
- Tools zur Festigung

Implementierung

Die Proofpoint-Analysen ermitteln eine realistische Einschätzung der Anfälligkeit Ihres Unternehmens in Bezug auf verschiedene Angriffsvektoren.

Phishing-Simulationen

Ein Proofpoint-Experte fungiert als unmittelbar zuständiger Administrator des Tools für Phishing-Simulationen. Wir erstellen, planen und implementieren jede Kampagne entsprechend dem Plan im Laufe Ihrer Lizenzlaufzeit. Vor dem Start jeder Kampagne besprechen wir auch deren Umfang sowie die mit Phishing-Tests zu überprüfenden Anwender. Ein simulierter Phishing-Blindangriff (der Anwender beim Klicken zu einer 404-Fehlerseite führt) wird zu Beginn der Lizenzlaufzeit an Ihre Anwender gesendet, um erste Ausgangswerte zu erhalten. Anschließend führen wir über die Lizenzlaufzeit hinweg simulierte Phishing-Angriffe durch. Zudem werden alle Anwender, die auf den Phishing-Link klicken, auf eine Landing Page geleitet, die über das falsche Verhalten belehrt.

Wissenstests

Wissenstests liefern einen Überblick über die Kenntnisse der Mitarbeiter Ihres Unternehmens und ermitteln die Effektivität von Schulungen. Wir empfehlen die Durchführung eines Wissenstests zu Beginn der Lizenzlaufzeit mit allgemeinen Themen sowie im weiteren Verlauf zusätzliche Wissenstests anstelle regulärer Schulungen.

Security Awareness-Training

Proofpoint weist Anwendern, die auf Phishing-Angriffe hereingefallen sind, automatisch Phishing-Schulungen zu. Wir schlagen außerdem Schulungsmodule vor und erstellen für jeden Anwender passende Tests – abhängig davon, ob sie auf einen simulierten Angriff hereingefallen sind. Bei diesem differenzierten Ansatz werden nicht nur konkrete Problembereiche identifiziert und angegangen, sondern auch die Schutzmaßnahmen als Ganzes gestärkt, da alle Ihre Anwender Schulungen erhalten. Wir erinnern die Anwender regelmäßig daran, den Termin für ihre Schulungsaufgabe einzuhalten. Außerdem ermitteln wir den Kenntnisstand der Anwender, um ihre nächsten Tests und Schulungsmodul-Aufgaben zu planen.

Hinweis: Wenn Sie Ihr eigenes Learning Management System (LMS) für einige oder alle Schulungsaufgaben verwenden, werden Anwenderverwaltung, Aufgaben und Berichte in diesem LMS von Ihnen und nicht von Ihrer Kontaktperson übernommen. Training Jackets und automatische Anmeldung sind für LMS-basierte Module nicht verfügbar.

Programmplan

1. QUARTAL	2. QUARTAL	3. QUARTAL	4. QUARTAL
Kickoff-Meeting	Phishing-Test	Meeting: Customer Business Review	Phishing-Test
Plattformverwaltung: Anwender	Phishing-Schulung mit automatischer Registrierung	Phishing-Test	Phishing-Schulung mit automatischer Registrierung
Phishing-Test	Schulung oder Wissenstest	Schulung oder Wissenstest	Schulung oder Wissenstest
Plattformverwaltung: Benachrichtigungen			Meeting: abschließendes Review

Festigung

Materialien zur Sensibilisierung für Sicherheit sind in verschiedensten Formaten wie Infografiken, Artikeln und Videos verfügbar und können heruntergeladen sowie angepasst werden. Diese Materialien sind so konzipiert, dass sie die wichtigsten Prinzipien aus unseren Schulungsmodulen untermauern, sodass bewährte Methoden betont und vermittelte Inhalte gefestigt werden. Proofpoint empfiehlt Security Awareness-Materialien speziell für die Bereiche, die bei den Wissenstests besonders schlecht abgeschnitten haben.

Das PhishAlarm-Add-in für E-Mail-Clients bietet Anwendern, die einen potenziellen Phishing-Angriff gemeldet haben, eine positive Bestärkung. Es informiert Sicherheits- und Reaktionsteams mit einem Klick auf eine Schaltfläche über verdächtige Phishing-E-Mails. Dies verkürzt Dauer und Auswirkungen aktiver Phishing-Angriffe und festigt gleichzeitig Verhaltensweisen, die in Ihrem Security Awareness-Schulungsprogramm vermittelt wurden. Die Meldung von Phishing-Versuchen (Meldungsrate) ist eine wichtige Kennzahl zur Überwachung des Verhaltens, Sicherheitsbewusstseins und Engagements von Endnutzern über einen längeren Zeitraum.

Analyse

Die Ergebnisse der Wissenstests, der simulierten Phishing-Kampagnen, der Schulungen sowie der PhishAlarm-E-Mail-Meldungen bieten einen umfassenden Überblick über die Anwenderkenntnisse und die Anfälligkeit für Angriffe. Mithilfe dieser Daten können Sie die am stärksten gefährdeten Bereiche identifizieren und einen Plan ausarbeiten, mit dem Sie den Wissensstand Ihrer Mitarbeiter verbessern. Ihre Kontaktperson überprüft die Ergebnisse aller Tests und Schulungsaufgaben mit früheren Ergebnissen, um Verbesserungstrends oder Problembereiche aufzuzeigen. Die in den Berichten aufgeführten Eigenschaften (entsprechend den Absprachen aus der Planungs-Erstsitzung) werden in Bezug auf eine Korrelation von Risiken für Abteilungen, Regionen, Rollen oder Vorgesetzte analysiert. Sofern verfügbar, stellt Ihre Kontaktperson Branchen- und Vorlagen-spezifische Benchmark-Analysen bereit.

Berichte

Im Verlauf des Programms werden zu jeder Aktivität Berichte bereitgestellt, die Ihr Projektverantwortlicher jederzeit abrufen kann. Bestimmte Berichte können regelmäßig generiert und Ihnen auf sichere Weise per E-Mail zugesendet werden.

WEITERE INFORMATIONEN

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

INFORMATIONEN ZU PROOFPOINT

Proofpoint, Inc. ist ein führendes Unternehmen für Cybersicherheit und Compliance. Im Fokus steht für Proofpoint dabei der Schutz der Mitarbeiter, denn diese bedeuten für ein Unternehmen sowohl das größte Kapital als auch das größte Risiko. Mit einer integrierten Suite von Cloud-basierten Lösungen unterstützt Proofpoint Unternehmen auf der ganzen Welt dabei, gezielte Bedrohungen zu stoppen, ihre Daten zu schützen und ihre IT-Anwender für Risiken von Cyberangriffen zu sensibilisieren. Führende Unternehmen aller Größen, darunter mehr als die Hälfte der Fortune-1000-Unternehmen, setzen auf die personenzentrierten Sicherheits- und Compliance-Lösungen von Proofpoint, um ihre größten Risiken in den Bereichen E-Mail, Cloud, soziale Netzwerke und Web zu minimieren. Weitere Informationen finden Sie unter **www.proofpoint.de**.