Managed Services für Proofpoint Security Awareness Training – Enterprise

Schulungen zur Sicherheitssensibilisierung für Unternehmen mit mehr als 2.500 Anwendern

Konzentrieren Sie sich auf Ihre geschäftlichen Aktivitäten – wir kümmern uns um die Gestaltung, Umsetzung und Dokumentation Ihres Programms zur Sensibilisierung für Sicherheit. Managed Services für Proofpoint Security Awareness Training – Enterprise richten sich an Unternehmen mit mehr als 2.500 Anwendern und sorgen mit Expertenwissen dafür, dass Ihr Sicherheitsprogramm mit regelmäßigen Maßnahmen Ihre Cybersicherheit verbessert.

Wir möchten, dass die Schulungen für Sie einfach und für Ihr Unternehmen effektiv sind. Dazu setzen wir auf einen bewährten, disziplinierten und individuellen Schulungsansatz, der Ihre Endnutzer das ganze Jahr über anspricht. Mit unserer Expertise und den bewährten Methoden können Sie sicher sein, dass Ihre Programme hervorragende Ergebnisse liefern.

Planung

Unser Managed Services-Team übernimmt die Verwaltung Ihres Programms zur Sensibilisierung für Sicherheit. Anfangs treffen Sie sich jede Woche mit einem Ihnen zugewiesenen Teammitglied, das als Ihr persönlicher Vertreter agiert und Ihr wichtigster Kontakt ist. Gemeinsam konzipieren und implementieren wir ein individuelles-Programm, das die Kultur und Ziele Ihres Unternehmens berücksichtigt.

Entdeckung

Bei einem Treffen mit Ihrer Kontaktperson besprechen Sie Ihre aktuellen Bedrohungen und Sorgen in Bezug auf die Cybersicherheit und klären detailliert, was Sie an bisherigen Security-Awareness-Aktivitäten schätzten und was Sie störte. Dazu gehören Schulungsprogramme, Penetrationstests sowie Phishing-Simulationen. Außerdem sprechen wir über frühere Ergebnisse, Rückmeldungen aus dem Unternehmen sowie Probleme.

Sie teilen uns Ihre aktuellen und zukünftigen Ziele beim Sicherheitsbewusstsein mit, die uns als Richtlinien für die Entwicklung eines angepassten Programms dienen. Am Ende dieser Erstgespräche steht eine klar definierte Liste von Zielen, die das Programm erfüllen soll.

Anschließend unterhalten wir uns über die Pläne für die Einbindung wichtiger Verantwortlicher wie die Personal- und IT-Abteilung. Ihre Kontaktperson stellt eine Reihe von Leitfäden, Tools und Vorlagen bereit, die Sie für das Programm nutzen können: Dazu gehören:

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

Kommunikation

Wir empfehlen dringend die Ausarbeitung eines durchdachten Kommunikationsplans für alle Verantwortlichen. Dieser Plan sollte die Ziele des Programms formulieren und eine Kontaktperson nennen, 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 sie 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. Effektive Kommunikation klärt Zuständigkeiten und steigert die Akzeptanz wichtiger Schulungserlebnisse.

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 und legen fest, ob die Anwenderliste mit dem End-User Sync-Tool synchronisiert werden kann. Wenn dies nicht möglich ist, fordern wir eine Anwenderliste mit Datenelementen wie E-Mail-Adresse, Vor- und Nachname, Geschäftsbereich, Gruppe, Standort und weiteren Eigenschaften an, da diese Angaben für Ihre Berichte wichtig sind. 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:

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

Weitere Informationen zu den in Proofpoint Security Awareness Training enthaltenen Produkten finden Sie hier: proofpoint.com/de/product-family/security-awareness-training.

Implementierung

Die von Proofpoint simulierten Angriffe ermitteln eine realistische Einschätzung der Anfälligkeit Ihres Unternehmens in Bezug auf verschiedene Angriffsvektoren. Da Sie wissen müssen, wie anfällig Ihre Anwender für Angriffe sind, stellt Ihre Kontaktperson simulierte Phishing-Angriffe parallel zu Wissenstests bereit.

Phishing-Simulationstests

Ihre Kontaktperson ist der unmittelbar zuständige Administrator des Tools für simulierte Phishing-Tests und wählt gemeinsam mit Ihnen für jede Kampagne Phishing-Vorlagen und Belehrungen aus. Wir erstellen, planen und implementieren jede Kampagne entsprechend den geplanten Anforderungen 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 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. Diese werden jeweils mit Belehrungen ergänzt, damit alle Anwender, die auf einen Phishing-Angriff hereinfallen, sofortige und effektive Rückmeldungen erhalten.

Phishing-Simulationstests mit USB-Geräten

Ihre Kontaktperson erstellt die Phishing-Simulationskampagne mit USB-Geräten, legt gemeinsam mit Ihnen die Namen der Köderdateien fest, die auf die Geräte geladen werden sollen, und wählt die Belehrung aus bzw. passt sie an. Anschließend senden wir Ihnen die ZIP-Datei mit den benötigten Dateien über Secure Share zu. Die USB-Geräte werden von Ihnen bereitgestellt und die Dateien von Ihnen darauf geladen. Nutzen Sie dabei die mitgelieferte Tabelle, um ihre Verteilung zu organisieren. Sobald die Geräte verteilt wurden, wird Ihre Kontaktperson nach dem vereinbarten Zeitplan Aktivitätsberichte senden.

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 zusätzliche Wissenstests basierend auf den Ergebnissen des ersten Tests. So können Sie sich auf zuvor ermittelte Gefährdungsbereiche konzentrieren.

Schulungsmodule

Proofpoint weist Anwendern, die auf Phishing-Angriffe hereingefallen sind, Schulungsmodule zu, wobei nur Schulungsmodule für die von Ihnen lizenzierten Produkte zugewiesen werden. Außerdem erstellen wir für jeden Anwender individuelle Aufgaben, unabhängig davon, ob er auf einen simulierten Angriff hereingefallen ist. Damit soll sichergestellt werden, dass alle Anwender von den Schulungen profitieren.

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.

Ihre Kontaktperson weist Schulungsmodule mit Sicherheits- und Compliance-Themen zu, einschließlich Aufgaben mit automatischer Anmeldung. Die Aufgaben werden entsprechend den ermittelten Risikobereichen zugewiesen und umfassen mehrere Module.

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 Anmeldungen für Schulungseinheiten sind für LMS-Module nicht verfügbar.

Festigung

PhishAlarm bietet Anwendern, die einen potenziellen Phishing-Angriff gemeldet haben, eine positive Bestärkung. Das PhishAlarm-Add-in für E-Mail-Clients 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 ist eine wichtige Kennzahl zur Überwachung des Verhaltens, Sicherheitsbewusstseins und Engagements von Endnutzern über einen längeren Zeitraum. Security-Awareness-Materialien sind so konzipiert, dass sie die wichtigsten Prinzipien aus unseren Schulungsmodulen untermauern, sodass bewährte Methoden betont und vermittelte Inhalte gefestigt werden. Proofpoint passt das Security-Awareness-Material an die Bereiche an, die bei den Wissenstests besonders schlecht abgeschnitten haben.

Analysen

Gemeinsam bieten die Ergebnisse der Wissenstests, der simulierten Phishing-Angriffskampagnen sowie der PhishAlarm-E-Mail-Meldungen 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 bisherige bzw. neue Problembereiche aufzuzeigen. Die in den Berichten aufgeführten Eigenschaften (entsprechend den Absprachen aus der ersten Planungssitzung) werden in Bezug auf eine Korrelation von Risiken für Abteilungen, Regionen, Rollen oder Vorgesetzte analysiert. Diese Analyse wird in weiteren Planungs- und Strategiesitzungen diskutiert und bestimmt die nächsten Schritte. Sofern verfügbar, stellt Ihre Kontaktperson Branchen- und Vorlagen-spezifische Benchmark-Analysen bereit.

Fokus auf VAPs

Bei Kunden mit Proofpoint Targeted Attack Protection (TAP) übernimmt die Kontaktperson folgende Aufgaben:

- Analyse eines quartalsweisen VAP™-Berichts (Very Attacked People) aus dem TAP-Dashboard
- Identifizierung der am häufigsten angegriffenen Personen in Ihrem Unternehmen
- Segmentierung Ihrer VAPs basierend auf Daten zu gezielten Bedrohungen
- Erstellung quartalsweiser VAP-Schulungen und Sensibilisierungsaktivitäten basierend auf den identifizierten Bedrohungen
- Analyse von VAPs und ihrer Performance im Security-Awareness-Programm über einen längeren Zeitraum

Berichte

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

Kalender für das Security-Awareness-Programm

Dieser Kalender bietet eine Übersicht über den von uns empfohlenen Plan zur Implementierung unseres Ansatzes der kontinuierlichen Schulung. Dabei hängt der Zeitplan von Ihren lizenzierten Produkten, der Laufzeit und den spezifischen Anforderungen und Zielen Ihres Programms ab.

1. QUARTAL	1. MONAT	2. MONAT	3. MONAT
Wissenstest	1. grundlegender Wissenstest Erstgespräche		
Phishing	1. Phishing-Blindtest	1. Kampagne mit automatischer Anmeldung	
Schulungen		Schulungen mit automatischer Anmeldung	Nicht-Klicker
Security-Awareness-Materialien		Ausgewähltes Thema	

2. QUARTAL	4. MONAT	5. MONAT	6. MONAT
Wissenstest			
Phishing	2. Kampagne	3. Kampagne	4. Kampagne
Schulungen		Ergänzende Schulungen*	Nicht-Klicker
Security-Awareness-Materialien		Neues Thema	

3. QUARTAL	7. MONAT	8. MONAT	9. MONAT
Phishing		5. Kampagne	6. Kampagne
Schulungen	Nicht-Klicker		Ergänzende Schulungen*
Security-Awareness-Materialien		Neues Thema	

4. QUARTAL	10. MONAT	11. MONAT	12. MONAT
Wissenstest			1. wiederholter Wissenstest
Phishing	7. Kampagne	8. Kampagne	

1. QUARTAL	1. MONAT	2. MONAT	3. MONAT
Schulungen		Nicht-Klicker	Ergänzende Schulungen*
Security-Awareness-Materialien		Neues Thema	
Smishing	1. Smishing-Kampagne		

* Ergänzende Schulungsthemen werden entsprechend den Wissenstest-Ergebnissen bestimmt. Phishing-Simulationen mit USB-Geräten können jederzeit während der Lizenzlaufzeit verteilt 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**.

proofpoint.