Wie Proofpoint Security Awareness Training Ihre Anwender anspricht

Etablieren Sie sichere Verhaltensweisen, die Risiken minimieren

Produkte

- Proofpoint Security Awareness Training
- Proofpoint Targeted Attack Protection

Vorteile

- Gezielte Schulungsmaterialien schließen individuelle Wissenslücken
- Schulungsprogramm spricht weltweite Zielgruppen mit kultur- und sprachspezifischen Inhalten an
- Anwender werden durch wiederholtes und kurzes Mikrolernen dazu motiviert, die Schulungsinhalte im täglichen Leben zu nutzen

Es kann äußerst schwierig sein, Anwender mit einem Security-Awareness-Programm dauerhaft anzusprechen – schließlich haben sie beruflich und privat viele Aufgaben, die gleichzeitig ihre Aufmerksamkeit fordern. Und da viele Unternehmen nur maximal zwei Stunden pro Jahr für die Schulung ihrer Mitarbeiter aufwenden, steht den Sicherheitsverantwortlichen gar nicht die Zeit zur Verfügung, um das Verhalten ändern zu können. Bei weltweit tätigen Unternehmen wird die Situation zusätzlich dadurch erschwert, dass zwischen den Anwendern große kulturelle und sprachliche Unterschiede bestehen.

Proofpoint Security Awareness Training kann hier helfen. Die darin enthaltenen Schulungen fördern nachhaltige Cyberverhaltensweisen, mit denen Ihre Mitarbeiter sich selbst und Ihr Unternehmen schützen. Wir erleichtern die Identifizierung von Anwendern, die zusätzliche Aufmerksamkeit benötigen. Mit unserer Lösung können Sie zudem Ihr Programm erweitern und skalieren, sodass Sie eine starke Sicherheitskultur aufbauen können, die Verhaltensänderungen fördert.

Proofpoint verwendet für die Security-Awareness-Schulungen einen ganzheitlichen Ansatz. Unser ACE-Framework – das den aktuellen Status Ihrer Sicherheitslösung analysiert, das Anwenderverhalten ändert und die Ergebnisse bewertet – fördert Verhaltensänderungen und verbessert Ihr Sicherheitsprogramm im Laufe der Zeit.

Abb. 1: Das Proofpoint-ACE-Framework (Tests, Verhaltensänderung, Bewertung).

Diese Kurzvorstellung beschreibt, wie Sie mit Proofpoint Security Awareness Training folgende Ziele erreichen:

- Ansprechen Ihrer Anwender
- Bestmögliche Nutzung der begrenzten Schulungszeit für Anwender
- Festigung positiver Verhaltensweisen und Verbesserung des Lernerfolgs
- Erweiterung und Skalierung Ihres Security-Awareness-Programms

Adaptiver Schulungsansatz

Unser durchdachter und anpassbarer Lernansatz unterstützt Sie dabei, Ihre Anwender mit personalisierter Wissensvermittlung zu motivieren. Dabei berücksichtigt er die individuellen Wissenslücken, Unternehmenspositionen, Lernstile und Schwachstellen. Nachfolgend gehen wir detailliert darauf ein.

Individuelle Wissenslücken

Wir stellen Schulungen zu verschiedenen Kernbereichen und Spezialthemen bereit. Da sie mit variablem Schwierigkeitsgrad verfügbar sind, können Sie Anwendern je nach ihrem Wissensstand unterschiedliche Lernmodule zuweisen. Die Schulungen decken unter anderem folgende Bereiche ab:

- E-Mail und Social Engineering
- Mobilgeräte
- Cloud- und Internet-Sicherheit
- Kennwörter und Authentifizierung
- Datenverarbeitung und Datensicherheit
- Sichere Entwicklung
- Sichere Geschäftsprozesse
- Physische Sicherheit und Arbeit im Homeoffice
- Bedrohungen durch Insider
- Compliance

Unternehmenspositionen

Sie können bestimmten Nutzergruppen rollenbasierte Schulungen zuweisen. Wir bieten verschiedene Vorlagen und Module für konkrete Aufgabenbereiche wie Finanz-, Personal-, Rechtsabteilung, Angestellte mit Remote/Hybrid-Arbeitsplätzen und mehr. Sie können für diese Unternehmensbereiche Schulungen suchen und bereitstellen.

Lernstile

Wir bieten Inhalte in unterschiedlichen Kategorien und Medien wie Animationen, Live-Aufnahmen, Humor, Interaktionen, Abenteuer und Spielstile sowie Formate (z. B. Poster, Newsletter und Flyer) an, damit Sie den für Ihre Unternehmenskultur optimalen Stil finden und Ihre Anwender ansprechen können. Das bedeutet, dass Sie stets die richtigen Inhaltstypen für alle Anwender in Ihrem Unternehmen finden.

Schwachstellen

Proofpoint verfügt über umfangreiche Bedrohungsdaten, die Sie für bedrohungsorientierte Schulungen nutzen können. Bei Integration in unsere Proofpoint Threat Protection-Plattform bietet unsere Security-Awareness-Lösung einen Überblick über Ihre Top Clicker und Very Attacked People™ (VAPs), also Ihre am häufigsten angegriffenen Anwender. Sie können Ihren VAPs gezielte Schulungen basierend auf den Bedrohungen bereitstellen, mit denen sie wahrscheinlich zu tun haben, damit sie in Zukunft weniger anfällig dafür sind.

Bedrohungsdaten und bedrohungsbezogene Inhalte

Mit unseren bedrohungsbezogenen Inhalten können Sie Ihre Anwender auf typische Angriffe vorzubereiten, die gerade im Umlauf sind. Wir bieten umgehende Bedrohungswarnungen bei Attacken, die wir bei unseren Kunden registrieren. Ebenso veröffentlichen wir regelmäßig Attack Spotlight-Materialien, mit denen Sie Ihre Sicherheitsprogramme ergänzen und Schulungen bereitstellen können, damit Ihre Anwender wachsam bleiben.

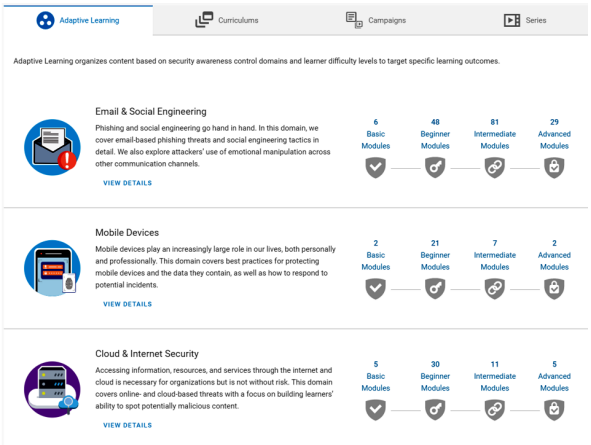

Abb. 2: Der adaptive Schulungsansatz bietet Schulungen für verschiedene Themengebiete und Schwierigkeitsgrade, um Anwender mit unterschiedlichen Wissenslücken zu erreichen.

Abb. 3: Proofpoint bietet eine Vielzahl an Schulungsstilen und -formaten, damit Sie den Anforderungen Ihrer Anwender optimal Rechnung tragen können.

Diese Materialien sind für alle Kunden und auch ohne Integration in Proofpoint Targeted Attack Protection (Proofpoint TAP) verfügbar.

Maximale Nutzung begrenzter Schulungszeiten durch Mikrolernmodule

Wir bieten Mikrolernmodule an, mit denen Sie sicherstellen können, dass die für Schulungen vorhandene Zeit effektiv genutzt wird. Viele dieser Module haben eine Dauer von höchstens drei Minuten, wobei für jedes Modul klare Ziele und Lernergebnisse vorgegeben sind. sie decken wichtige Bereiche und Themen ab, sodass Sie sicherstellen können, dass alle Ihre Anwender über ein solides Verständnis der Grundlagen für sicheres Verhalten verfügen. Unsere Grundlagenschulung mit Mikrolernmodulen kann innerhalb von (insgesamt) etwa einer Stunde absolviert werden. Anwender können diese kurzen und gezielten Schulungen leicht in ihre täglichen Abläufe integrieren. Am besten ist jedoch, dass Sie flexibel individuelle Lernpfade für Ihre Anwender erstellen können, die aus relevanten Mikrolernelemente sowie den entsprechenden Tests bestehen.

Proofpoint erstellt und erweitert die Schulungsangebote im Rahmen von Schulungsplänen. Dabei handelt es sich um eine kuratierte Auswahl von Inhalten, die bestimmte Aufgaben erfüllen und erleichtern sollen, damit Sie die Schulungsprogramme gezielt einsetzen und Anwender unkompliziert über gängige Best Practices für Sicherheit sowie zentrale Themen wie NIST und ISO informieren können.

Abb. 4: Durch die Integration in das TAP-Dashboard erhalten Administratoren (im Dashboard) Einblicke in die Top Clicker und anfälligen Anwender. Dadurch können Sie auf der Schulungsplattform einen gezielten Schulungsplan für die betreffenden Anwender erstellen.

Die Belehrungen werden als Popup-Meldung angezeigt, wenn Angestellte auf Phishing-Simulationen hereinfallen. Diese Hinweise umfassen auch einen kurzen Kommentar dazu, warum sie nicht auf die simulierte E-Mail hätten klicken sollen. Auf diese Weise erzielen Sie einen Lerneffekt mit einem praktischen Beispiel in einer sicheren Umgebung.

Festigung positiver Verhaltensweisen und Verbesserung des Lernerfolgs

Dieser Abschnitt zeigt einige Methoden, mit denen Proofpoint positives Verhalten festigt.

Sofortige relevante Hinweise

Mit der Belehrungen-Funktion von Proofpoint können Sie Popup-Meldungen anzeigen, wenn Angestellte auf Phishing-Simulationen hereinfallen. Diese Hinweise umfassen auch einen kurzen Kommentar dazu, warum sie nicht auf die simulierte E-Mail hätten klicken sollen. Auf diese Weise erzielen Sie einen Lerneffekt mit einem praktischen Beispiel in einer sicheren Umgebung. Sie können unsere Vorlagen für Belehrungen verwenden oder die Nachrichten an Ihre Anforderungen sowie Ihre konkrete simulierte Phishing-E-Mail anpassen. Dadurch können Sie genau kontrollieren, was Ihre Schulungsteilnehmer erhalten und angezeigt bekommen.

Angepasste Rückmeldungen für Anwender

Wenn Anwender einen simulierten Phishing-Versuch melden, benachrichtigen wir sie darüber, dass sie den Phishing-Test bestanden haben. Wenn Anwender eine verdächtige reale E-Mail melden, können Sie die Rückmeldung mit unserer CLEAR-Lösung (Closed-Loop Email Analysis and Response) anpassen und die Empfänger automatisch darüber informieren, ob die gemeldete E-Mail tatsächlich schädlich war. Das motiviert sie, weiterhin potenzielle Bedrohungen zu melden, und baut eine Beziehung zwischen Ihnen und den Endnutzern auf.

Kontextbezogene Hinweise

Wenn unsere Lösung in die Proofpoint Threat Protection-Plattform integriert ist, bietet sie Warnhinweise in E-Mails, die Anwendern Kontext zu unklaren E-Mails geben. Sie erinnern die Anwender daran, innezuhalten und zu überprüfen, ob eine E-Mail verdächtig erscheint, bevor sie weitere Aktionen vornehmen. Die Schaltfläche zur Meldung verdächtiger Inhalte im Hinweis erinnert die Anwender auch daran, potenzielle Bedrohungen zu melden. Diese beiden Funktionen verbessern gemeinsam die Meldungsrate und die Richtigkeit gemeldeter E-Mails.

Adaptive Schulungstests

Proofpoint bietet adaptive Schulungstests an. Dabei handelt es sich um kurze und zielgerichtete Quizfragen, mit denen Sie die Kenntnisse Ihrer Anwender zu bestimmten Themen einfach ermitteln können. Sie können den Test basierend auf einem von drei Modultypen durchführen. Diese Module werden alle mit dem gleichen Lernziel entwickelt und können zuverlässig ermitteln, was Anwender bereits wissen und womit sie noch Schwierigkeiten haben. Sie können festlegen, ob diese Tests vor oder nach den jeweiligen Mikrolernmodulen angezeigt werden. Die Ergebnisse können auf der Plattform in Echtzeit in den Testdetails angezeigt werden.

Abb. 5: Sich überschneidende Faktoren, die zur Sicherheitskultur beitragen.

Erweiterung und Skalierung Ihres Security-Awareness-Programms

Bewertung der Sicherheitskultur

Da Sie die Einstellung Ihrer Anwender dank Proofpoint genauer erfassen können, können Sie Ihr Schulungsprogramm gezielt erweitern. Dies ist ein wichtiger Schritt beim Aufbau einer starken Sicherheitskultur. Wir bei Proofpoint betrachten die Sicherheitskultur als Schnittmenge von drei wesentlichen Faktoren:

- **Verantwortung:** Haben die Mitarbeiter das Gefühl, dass sie und ihre Kollegen für die Prävention von Cyberbedrohungen mitverantwortlich sind?
- **Bedeutung:** Ist den Mitarbeitern bewusst, dass eine Bedrohung sie persönlich betreffen könnte?
- **Kompetenz:** Fühlen sich die Mitarbeiter in der Lage, verdächtiges Verhalten zu identifizieren und zu melden?

Anhand unserer Bewertung der Sicherheitskultur können Sie den aktuellen Stand in Ihrem Unternehmen einschätzen und feststellen, was die Anwender über Cybersicherheit denken. Im Rahmen der Bewertung wird die Verhaltensänderung im Laufe der Zeit ermittelt und die Wahrscheinlichkeit geschätzt, mit der Anwender die richtige Aktion durchführen. Basierend auf dem zugehörigen Bericht können Sie Ihre Informationen und Schulungen für bestimmte Anwendergruppen anpassen, damit sie relevanter und wirksamer sind.

Unterstützte Sprachen

Damit große Unternehmen ihre Sicherheitsschulungen skalieren können, unterstützt Proofpoint bei den Grundlagenschulungen mit Mikrolernmodulen mehr als 40 Sprachen, was auch die Untertitel und Sprechertexte umfasst. Zudem sind viele unserer anderen Schulungsmodule in mindestens 11 Sprachen lokalisiert. Unsere mehrsprachige SCORM-Exportfunktion vereinfacht das Herunterladen oder Hosten von Schulungsinhalten für weltweite Zielgruppen mit wenigen Klicks. Mit unseren verschiedenen Schulungsvideos und -modulen bieten wir einen Ansatz, der auf Vielfalt und Inklusion setzt und Anwender aus verschiedensten Kulturen und Ländern anspricht.

Zusammenfassung

Die Schulung von Anwendern, die nur wenig Zeit und kaum vereinbare Prioritäten haben, erfordert angesichts immer neuer Bedrohungen eine Security-Awareness-Lösung, die Wissenslücken effizient schließt. Mit Proofpoint Security Awareness Training können Sie Ihren Anwendern schnelle und gezielte Schulungen bereitstellen. Dadurch werden sichere Verhaltensweisen entwickelt, die sich am Arbeitsplatz und im Privatleben als wichtig erweisen. Damit werden die Anwender für das Unternehmen zu einer starken Verteidigungslinie und bleiben stets wachsam, sodass sie das Sicherheitsteam unterstützen.

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 75 Prozent der Fortune-100-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**.