Proofpoint Security Awareness Enterprise

Durch einen bedrohungsbezogenen Ansatz höhere Anwenderresilienz erreichen

Wichtige Vorteile

- 40 % weniger Klicks in E-Mails mit echten Bedrohungen innerhalb von weniger als sechs Monaten
- Metriken als Nachweis über die erfolgreiche Risikominimierung gegenüber CISOs
- Verhaltensänderungen dank personalisierter Lernerlebnisse
- Automatische Analyse der von Anwendern gemeldeten Bedrohungen ohne zusätzlichen Aufwand für IT-Team

Proofpoint Security Awareness Enterprise hilft Ihnen, eines der dringendsten Probleme von Unternehmen zu lösen: die Reduzierung des von Menschen ausgehenden Sicherheitsrisikos. Laut dem Proofpoint State of the Phish-Bericht 2023, unserer jährlichen Untersuchung zu Phishing, sensibilisieren 98 % aller Unternehmen ihre Mitarbeiter in irgendeiner Form für Sicherheit. Das lässt darauf schließen, dass die Bedeutung des Themas weite Anerkennung gefunden hat. Doch Schulungen allein führen nicht immer zu mehr Sicherheit.

Sicherheitsprogramme sind nur dann wirklich effektiv, wenn sich die Anwender aktiv einbringen und anschließend in der Lage sind, in der Praxis sichere Entscheidungen zu treffen, sodass ihr Verhalten einen messbaren Einfluss auf die Sicherheit hat.

Proofpoint Security Awareness Enterprise kann Sie dabei unterstützen. Wir stellen uns dieser Herausforderung mit dem ACE-Framework, unserem ganzheitlichen Ansatz zur Sensibilisierung für Sicherheit. Das Framework besteht aus drei grundlegenden Phasen: die Bewertung von Anwenderschwachstellen (Assess), die Änderung des Anwenderverhaltens (Change Behavior) und die Evaluierung der Wirksamkeit des Programms (Evaluate). Unsere Lösung bietet Sicherheitsadministratoren operative Effizienz und die Möglichkeit zur globalen Skalierung.

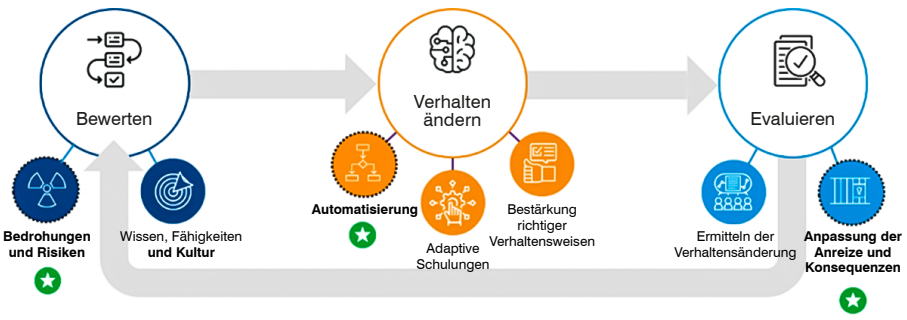

Abb. 1: Das ACE-Framework.

Anwendung branchenführender Bedrohungsdaten

Proofpoint Security Awareness Enterprise wird durch unsere umfangreichen Bedrohungsdaten unterstützt, die aus den Systemen unserer zahlreichen Kunden erfasst werden. Wir nutzen diese Daten, um Sie beim Erstellen eines effektiven Schulungsprogramms zu unterstützen, mit dem Sie reale Angriffe mit raffinierten Phishing-Simulationskampagnen imitieren. Sie können Ihre häufig angegriffenen Personen (Ihre Very Attacked People™, VAPs) identifizieren und sie für die Bedrohungen sensibilisieren, von denen sie häufig ins Visier genommen werden. Außerdem können Sie nachverfolgen, wie sich die Anwender bei realen Bedrohungen verhalten, und Ihre Mitarbeiter in Newslettern auf Angriffstrends hinweisen.

Bewertung der Anwenderschwachstellen

Mit Proofpoint Security Awareness Enterprise können Sie feststellen, wie es um das Wissen, die Fähigkeiten und die Einstellungen Ihrer Anwender rund um das Thema Cybersicherheit steht. Zudem zeigt die Lösung, inwieweit sie ein attraktives Ziel darstellen. All dies hilft Ihnen, besonders gefährdete Anwender zu identifizieren und festzustellen, ob sie in der Lage sind, sich richtig zu verhalten. So haben Sie einen Überblick darüber, wer den größten Schulungsbedarf hat. Anschließend können Sie ein Programm zusammenstellen, das auf die individuellen Wissenslücken und das erwartete Verhalten zugeschnitten ist.

Proofpoint Security Awareness Enterprise bietet folgende Vorteile:

- Identifizierung von Wissenslücken mit kurzen und zielgerichteten Quizfragen, die auf unseren umfangreichen Bedrohungsdaten basieren
- Durchführung von Phishing-Tests mit Bedrohungen, die in der Praxis beobachtet wurden
- Analyse von Schwachstellen aus Teilnahme, Leistung und der Wahrscheinlichkeit für Angriffe
- Aufdeckung der Einstellungen zum Thema Sicherheit, um Mitarbeiter bestmöglich für richtiges Verhalten motivieren zu können
- Identifizierung der VAPs und Top Clicker (bei Integration in die Proofpoint-Plattform)

Finden Sie heraus, was Ihre Anwender wissen

Mit unseren adaptiven Wissenstests können Sie feststellen, was Ihre Anwender wissen und wo sie Probleme haben. Die Tests bestehen aus konkreten Lerneinheiten, die knapp und präzise gehalten sind. Sie haben die Wahl aus einer Vielzahl von Quizfragen, die sich an bestimmten Lernzielen orientieren, und Mikrolernmodulen mit verschiedenen Schwierigkeitsgraden.

Finden Sie heraus, wie sich Ihre Anwender verhalten

Unsere Phishing-Simulationen bereiten Ihre Anwender auf reale Bedrohungen vor. Proofpoint nutzt Bedrohungsdaten, die aus den mehr als 2,6 Milliarden E-Mails stammen, die wir täglich beobachten. Durch diesen umfassenden Überblick können wir Ihnen tausende Phishing-Vorlagen anbieten, die mehrere Bedrohungstypen simulieren. Darüber hinaus können Sie Vorlagen an die Bedrohungsarten in Ihrer Umgebung anpassen. Zudem haben Sie die Möglichkeit, allen Anwendern, die eine Phishing-Simulation nicht bestehen, automatisch Schulungen zuzuweisen.

Finden Sie heraus, was Ihre Anwender denken

Um eine starke Sicherheitskultur aufzubauen, müssen Sie wissen, was Ihre Anwender über Cybersicherheit denken. Anhand unserer Bewertungen der Sicherheitskultur können Sie den aktuellen Stand in Ihrem Unternehmen einschätzen. Dazu führen Sie kurze Umfragen durch, die sich auf die drei wichtigsten Faktoren für die Kultur konzentrieren: Verantwortung, Stellenwert und Befähigung. Anschließend können Sie ein maßgeschneidertes Programm erstellen, das die Überzeugungen und Motivation Ihrer Mitarbeiter beeinflusst und ihnen dabei hilft, das gelernte Wissen praktisch umsetzen zu können.

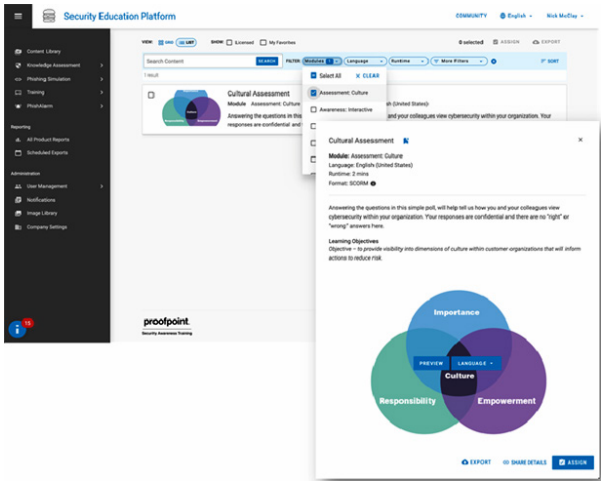

Abb. 2: Bewertung der Sicherheitskultur und Bibliothek für erweiterte Inhalte und Filterung.

Identifizierung besonders gefährdeter Anwender

Durch die Integration in die Proofpoint Threat Protection-Plattform können Sie mit unserer Lösung die VAPs und Top Clicker in Ihrem Unternehmen aufdecken und erhalten damit die Möglichkeit, Ihre am häufigsten angegriffenen Anwender gezielt für die Bedrohungen zu schulen, die für sie relevant sind. Die Integration mit Proofpoint Nexus People Risk Explorer bietet Ihnen zusätzliche Einblicke zu besonders gefährdeten Anwendern, denn die Lösung bewertet ihre Anfälligkeit, den Angriffsindex und Berechtigungen. Mithilfe dieser Erkenntnisse können Sie Ihr Programm und Ihre Ressourcen an die tatsächlichen Risiken für Ihr Unternehmen anpassen.

Weitere Informationen über Inhalte für gezielte Schulungen mit Proofpoint Security Awareness Enterprise finden Sie in der Kurzvorstellung **Wie Proofpoint Security Awareness Training Ihre Anwender anspricht**.

Änderung des Anwenderverhaltens

Sobald Sie wissen, was Ihre Anwender wissen, tun und denken, können Sie anfangen, unsicheres Verhalten zu beeinflussen. Proofpoint Security Awareness Enterprise hilft Ihnen, Verhalten durch maßgeschneiderte Schulungen und Bestärkung zu verändern. Jede Person erhält das, was sie benötigt, und wird in den Inhalten geschult, die für sie relevant sind. Dadurch können Sie die begrenzte Zeit, die für Schulungen zur Verfügung steht, optimal nutzen, und die Schulungen können ihre Wirkung besser entfalten.

Proofpoint Security Awareness Enterprise bietet folgende Vorteile:

- Motivation von Anwendern durch personalisierte Lernerlebnisse
- Erstellung prägnanter und spezifischer Schulungen für die jeweiligen Lernziele
- Bereitstellung ansprechender Inhalte auf Basis der aktuellen Bedrohungslage
- Verstärkte Lerneffekte durch Schulungen im richtigen Moment

Schulungen mit adaptivem Framework und Mikrolerneinheiten

Proofpoint Security Awareness Enterprise nutzt ein adaptives Schulungsframework – das Gegenteil einer Einheitslösung. Das Framework bietet schrittweise Sicherheitsschulungen auf vier Ebenen – von den Grundlagen bis hin zu fortgeschrittenen Konzepten. Auf diese Weise erhalten Ihre Anwender die erforderlichen Schulungen mit dem richtigen Schwierigkeitsgrad.

Das adaptive Framework ist zudem in Mikrolerneinheiten eingebunden. Das sind 3-minütige Module mit prägnanten und spezifischen Lernzielen, die Ihre Anwender kontinuierlich und leicht verständlich schulen. Die Module sind zudem auf individuelle Faktoren wie die Position im Unternehmen, den Lernstil, die Kompetenz, den Grad der Anfälligkeit und die Sprache zugeschnitten.

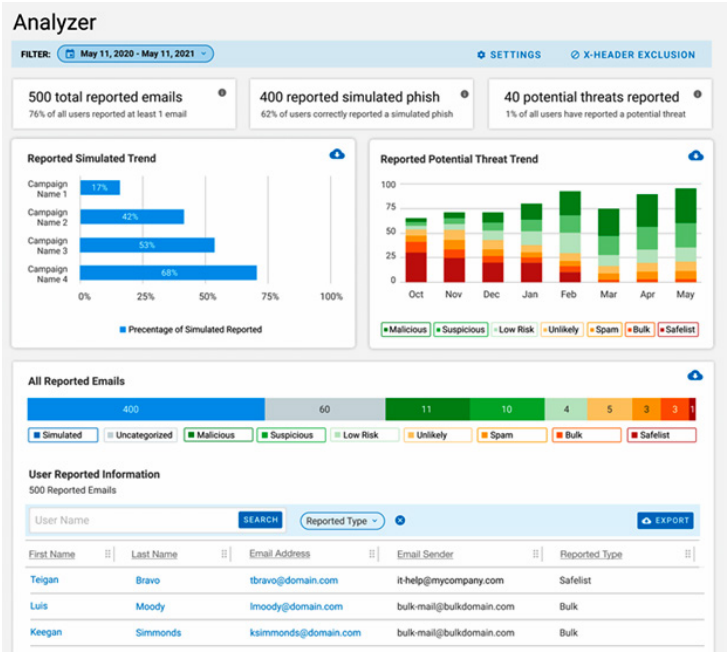

Abb. 3: Echtzeitberichte über das Verhalten bei simulierten Phishing-Tests und echten Bedrohungen.

Bereitstellung von bedrohungsbezogenen Inhalten und gezielten Schulungen

Die Inhalte von Proofpoint Security Awareness Enterprise basieren auf den Trends und Taktiken der aktuellen Bedrohungslandschaft, damit Sie Ihre Anwender besser auf aktuelle reale Bedrohungen vorbereiten können. In unseren wöchentlichen Bedrohungswarnungen erläutern wir die neuesten Angriffe, die wir bei unseren Kunden beobachten. Außerdem bereichern unsere Attack Spotlight-Materialien Ihr Programm mit aktuellen Schulungsinhalten.

Wenn Proofpoint Security Awareness Enterprise in die umfassende Proofpoint-Plattform integriert ist, können Sie Ihren Anwendern kontextbezogene Hinweise bereitstellen und sie positiv bestärken. Popup-Belehrungen erläutern den Anwendern, warum sie nicht auf Links einer Phishing-Simulation klicken sollten, während Warnhinweise in E-Mails auf potenziell schädliche Nachrichten aufmerksam machen. Die Schaltfläche „Report Suspicious" (Verdächtiges melden) setzt zudem unseren automatisierten CLEAR-Workflow (Closed-Loop Email Analysis and Response) in Gang, der Anwendern individuelle Rückmeldungen über die von ihnen gemeldeten E-Mails gibt.

Bewertung der Ergebnisse Ihres Programms

Sie müssen bewerten können, welchen Einfluss Ihr Security-Awareness-Programm auf Ihre Sicherheit hat. Proofpoint Security Awareness Enterprise bietet Verhaltensmetriken, die zeigen, wie gut Ihre Mitarbeiter abschneiden und wie sich das Programm auswirkt. Zudem können Sie die besseren Sicherheitsergebnisse mit anderen Unternehmen vergleichen. Zum Beispiel verzeichnen unsere Kunden innerhalb von sechs Monaten einen Rückgang der Klicks auf echte Bedrohungen um 40 %, während die Zahl der von Anwendern gemeldeten E-Mails um das Dreifache steigt. Diese Metriken helfen Ihnen, den Erfolg des Programms gegenüber dem CISO zu demonstrieren und sich die Unterstützung für weitere Investitionen zu sichern.

Proofpoint Security Awareness Enterprise bietet folgende Vorteile:

- Nachverfolgung des Anwenderverhaltens beim Melden echter Bedrohungen
- Vergleich wichtiger Metriken mit denen Ihrer Mitbewerber
- Dokumentation positiver Änderungen des Anwenderverhaltens, um Unterstützung der Geschäftsführung zu erhalten

Übersicht über Verhalten bei simulierten und echten E-Mails

Unser einzigartiges CISO-Dashboard zeigt, welchen Einfluss die Schulungen auf das Mitarbeiterverhalten haben. Es gibt Ihnen einen Überblick über die von Anwendern gemeldeten E-Mails und zeigt Veränderungen im Zeitverlauf, sodass sie nachvollziehen können, wie sich das Verhalten verbessert hat. Metriken wie die Meldungsrate verdächtiger E-Mails und die Zuverlässigkeit dieser Meldungen helfen Ihnen, das Verhalten von Anwendern über die Abschlussquote für Schulungen hinaus zu bewerten.

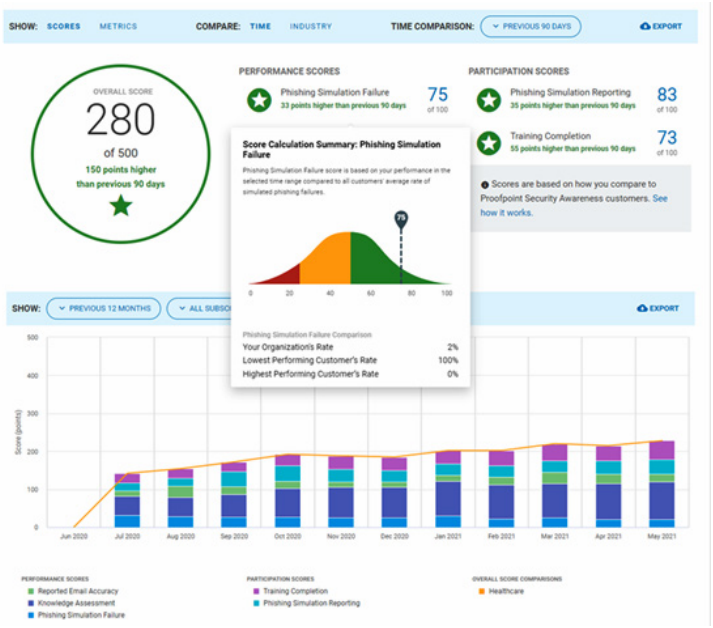

Abb. 4: Zusammenfassung der Programmleistung im CISO-Dashboard.

Vergleich mit anderen Branchenvertretern

Das CISO-Dashboard bietet eine Möglichkeit, den Erfolg Ihres Programms mit dem von Ihren Mitbewerbern zu vergleichen. Sie können dabei Änderungen beim realen Verhalten Ihrer Anwender sehen, z. B. den Anteil der Anwender, die verdächtige E-Mails melden. Anschließend können Sie die Zuverlässigkeitsquote mit der in anderen Unternehmen vergleichen und auf diese Weise feststellen, welche Wirkung Ihr Programm im Vergleich zu anderen Unternehmen hat. Mit diesen Übersichten lässt sich der Erfolg leicht nachweisen.

Meldung für Wiederholungstaten

Proofpoint Security Awareness Enterprise stellt täglich Daten über interne Tests und externe Bedrohungen bereit. Dazu gehört auch eine Übersicht über Wiederholungstäter. Unsere Lösung ermöglicht das Herausfiltern und Gruppieren von Anwendern, die in einem bestimmten Zeitraum mehrfach auf eine Phishing-Simulation hereingefallen sind. Dadurch stehen den Administratoren aktuelle und zuverlässige Informationen für weitere Maßnahmen (z. B. die Zuweisung weiterer Schulungen) zur Verfügung.

Erweiterung und Skalierung Ihres Programms

Proofpoint Security Awareness Enterprise unterstützt Sie durch Automatisierung und Skalierbarkeit. Automatisierte Prozesse reduzieren den manuellen Aufwand und ermöglichen flexiblere und effizientere Abläufe. Durch ihre Skalierbarkeit kann unsere Lösung zudem weltweit eingesetzt werden.

Proofpoint Security Awareness Enterprise bietet folgende Vorteile:

- Besseres Administrationserlebnis dank flexibler automatisierter Prozesse
- Kommunikation mit globaler Zielgruppe in der bevorzugten Sprache
- Erweiterte Sprachunterstützung für Ihr Security-Awareness-Programm
- Nutzung bewährter Methoden und tägliche Unterstützung durch Proofpoint Managed Services
- Einfachere Möglichkeit für Anwender, verdächtige E-Mails zu melden, und schnelles positives Feedback
- Automatische Untersuchung und Behebung der von Anwendern gemeldeten E-Mails durch Integration in die Proofpoint-Plattform

Unterstützung für mehrere Sprachen

Sie können mit Ihrer Zielgruppe weltweit in der jeweiligen bevorzugten Sprache kommunizieren. Proofpoint Security Awareness Enterprise bietet über 40 Sprachen für unsere Schulungsmodule und die Customization Services, einschließlich Untertitel und Sprachaufnahmen. Außerdem werden kontinuierlich weitere Sprachen hinzugefügt.

Flexible Ausführung dank Mandantenfähigkeit

Mit den mandantenfähigen Verwaltungsoptionen erhalten Sie eine schlanke, optimierte Installation, die flexibel implementiert und für Ihren konkreten Anwendungsfall konfiguriert werden kann. Ihr Sicherheitsteam überwacht das Programm und trifft unternehmensweite Entscheidungen. Einzelne Gruppen (z. B. regionale Niederlassungen oder Geschäftsbereiche) können die Schulungen für die Anwender und konkreten Gegebenheiten vor Ort anpassen. Dieser Workflow ist ideal für komplexe Großunternehmen mit weltweiten oder verteilten Niederlassungen.

Höhere Produktivität durch Services

Proofpoint ergänzt Ihr Sicherheitsteam und hilft Ihnen bei der Anwendung bewährter Sicherheitsmethoden. Mit den **Managed Services** übernehmen wir den täglichen Betrieb Ihres Security-Awareness-Programms und die Erstellung von Berichten. Dadurch kann sich Ihr Sicherheitsteam auf seine Hauptaufgaben konzentrieren. Mit den **Proofpoint Security Awareness Customization Services** können Sie Ihrem Programm ein eigenes Gesicht verleihen und Ihre Sicherheitskultur durch individuell gestaltete Mikrolernmodule fördern. Dazu gehören firmenspezifische Logos, Farben, Bildmaterial, Texte, Sprachaufnahmen und Übersetzungen.

Automatisierung von Anwendermeldungen und Reaktionen auf Bedrohungen

Wenn Anwender eine verdächtige E-Mail über ihren E-Mail-Client melden, analysiert die Proofpoint-Bedrohungserkennung automatisch die E-Mail, sodass Sie besser vor unbemerkten Phishing-Versuchen geschützt sind. Dies verringert zudem den manuellen Aufwand und steigert die Effizienz Ihrer Abläufe. Wenn unsere Bedrohungserkennung eine verdächtige E-Mail als Bedrohung kennzeichnet und die Lösung in die Proofpoint-Plattform integriert ist, wird unser automatisierter CLEAR-Workflow in Gang gesetzt. Er veranlasst die Behebung der E-Mail und sendet eine Rückmeldung an die Anwender, die die E-Mail gemeldet haben. Dieser Prozess stärkt das positive Verhalten der Anwender und verringert den Behebungsaufwand für Administratoren um bis zu 90 %.

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.

proofpoint.

0204-005-04-04 3/23