

Proofpoint Security Awareness Enterprise

Bedrohungsbezogener Ansatz für personenzentrierte Cybersicherheit

Wichtige Vorteile

- 40 % weniger Klicks in E-Mails mit echten Bedrohungen innerhalb von sechs Monaten
- Förderung von Verhaltensänderungen durch bedrohungsbezogene, maßgeschneiderte Inhalte und positive Verstärkung
- Genaue Identifizierung von Anwenderschwachstellen, damit sich das Sicherheitsteam auf riskante Anwender konzentrieren kann
- Wichtige Verhaltenskennzahlen wie Branchen-Benchmarks als Nachweis für die Risikominimierung gegenüber CISOs
- Aufbau einer Sicherheitskultur, die die Verhaltensweisen und Überzeugungen Ihrer Anwender verändert

Proofpoint Security Awareness Enterprise löst ein strategisches Problem, das alle Unternehmen haben: die Reduzierung des von Mitarbeitern ausgehenden Sicherheitsrisikos. Laut dem Proofpoint State of the Phish-Bericht 2024, unserem jährlichen Sicherheitsbericht, haben 68 % der berufstätigen Erwachsenen 2023 schon einmal eine riskante Aktionen durchgeführt, obwohl sie sich der Gefahren bewusst waren. Das deutet darauf hin, dass sich Anwender oft für ihre eigene Bequemlichkeit statt für Sicherheit entscheiden, was sie für Cyberangriffe anfällig macht.

Proofpoint Security Awareness Enterprise geht diese Herausforderung an. Die marktführende Lösung für Sicherheitsschulungen verändert mit einem ganzheitlichen Ansatz, wie Menschen über Bedrohungen denken und wie sie darauf reagieren. Dazu setzen wir auf unser ACE-Framework mit drei Phasen: die Bewertung von Anwenderschwachstellen (Assess), die Änderung des Anwenderverhaltens (Change Behavior) und die Evaluierung der Wirksamkeit des Programms (Evaluate). Dieser bewährte Lernzyklus ermöglicht reale Sicherheitsverbesserungen, da die Resilienz der Anwender gegenüber personenzentrierten Bedrohungen gestärkt wird.



Abb. 1: Das ACE-Framework, unser bedrohungsbezogener, adaptiver Ansatz für Sicherheitsschulungen.

Diese Lösung ist Teil der integrierten Proofpoint Human-Centric Security-Plattform, die sich auf die Behebung der vier wichtigsten personenbezogenen Risiken konzentriert.



Anwendung branchenführender Bedrohungsdaten

Proofpoint Security Awareness Enterprise wird durch unsere umfangreichen realen Bedrohungsdaten unterstützt, die wir aus mehr als 3 Milliarden täglich analysierten Kunden-E-Mails gewinnen und für den Aufbau eines effektiven Programms nutzen. Wir unterstützen Sie bei folgenden Aufgaben:

- Durchführung ausgeklügelter Phishing-Kampagnen, die reale Angriffe nachahmen
- Identifizierung besonders gefährdeter Anwender und Schulung dieser Anwender zu den Bedrohungen, die sie ins Visier nehmen
- Überwachung von realen Verhaltensänderungen, einschließlich Meldungsraten und Richtigkeit der Meldungen
- Aktuelle Einblicke in Angriffstrends dank wöchentlicher Warnmeldungen und monatlicher Kurzinformationen

Bewertung Ihrer Anwenderschwachstellen

Der erste wichtige Schritt ist die Analyse des aktuellen Stands Ihres Programms. Dazu müssen Sie herausfinden, was Ihre Anwender über Sicherheit wissen, wie Anwender bei Bedrohungen wahrscheinlich reagieren würden und wie sie über Sicherheit denken. Proofpoint Security Awareness Enterprise identifiziert Ihre am stärksten gefährdeten und am häufigsten angegriffenen Anwender, damit Sie ein wirkungsvolles Programm aufbauen und Ihre Maßnahmen auf die Wissenslücken und riskanten Verhaltensweisen der Anwender konzentrieren können, die mehr Unterstützung benötigen. Unsere Lösung bietet folgende Vorteile:

- Adaptive Schulungstests zur genauen Identifizierung von Wissenslücken und kurze Tests zur Sicherheitskultur, um die Einstellung der Mitarbeiter zum Thema Sicherheit festzustellen
- Einbeziehung realer Bedrohungen wie schädliche QR-Codes, Links oder Anhänge bei Phishing-Simulationen, um das wahrscheinliche Anwenderverhalten bei einem Angriff zu testen
- Nutzung von Machine Learning und NIST-Phish Scale, um den richtigen Schwierigkeitsgrad für Leveled Phishing-Simulationen zu bestimmen und die Anwenderleistung kontinuierlich zu verbessern
- Analyse der Anwendergefährdung durch Angriffe, inklusive Berichten zu Ihren besonders stark angegriffenen Personen (Very Attacked People™ bzw. VAPs) und Top Clickern
- Zusätzliche Einblicke zu besonders gefährdeten Anwendern, einschließlich Attack Index und Berechtigungen (mit Proofpoint Threat Protection)

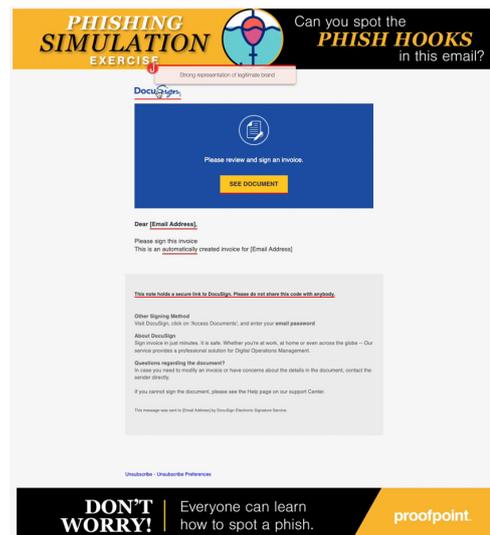
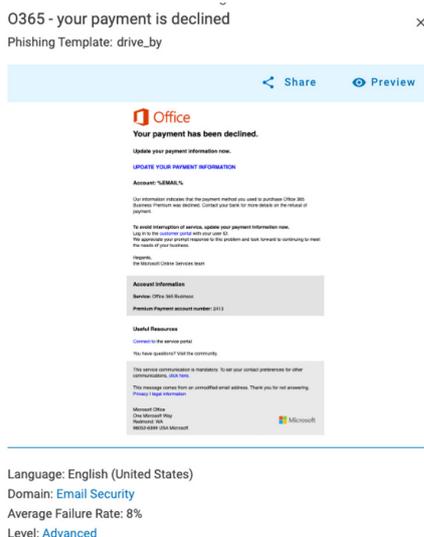


Abb. 2: Machine Learning und NIST-basierte Hinweise zur Auswahl geeigneter Phishing-Simulationen.

Änderung des Anwenderverhaltens

Sobald Sie wissen, was Anwender über Sicherheit wissen und denken bzw. dafür tun, können Sie anfangen, unsicheres Verhalten zu beeinflussen. Proofpoint Security Awareness Enterprise bietet Schulungen, die für die Schwachstellen und Wissenslücken Ihrer Anwender maßgeschneidert wurden. Außerdem wird richtiges Verhalten positiv verstärkt. Unser adaptiver Schulungsansatz ermöglicht ein personalisiertes, progressives Lernerlebnis, sodass Anwender ihre begrenzte Zeit maximal nutzen. Außerdem wird damit die Wirksamkeit der Schulungen gesteigert. Proofpoint Security Awareness Enterprise bietet folgende Vorteile:

- Erstellung von ansprechenden Inhalten, die speziell auf individuelle Faktoren wie die Position im Unternehmen, die Branche, das Hintergrundwissen, den bevorzugten Stil sowie die bevorzugte Sprache zugeschnitten sind
- Bereitstellung kontinuierlicher Kurzschulungen mit spezifischen Lernzielen, z. B. Mikrolernmodule mit weniger als 3 Minuten oder Nanolernmodule mit 1 Minute Länge
- Durchführung von Phishing-Simulationen basierend auf realen Phishing-Beispielen, um praktische Erfahrungen mit QR-Code-Betrug, der Nachahmung von Marken und anderen Taktiken zu bieten
- Sofortige kontextbezogene Rückmeldungen wie Phishing-Hooks (Erläuterungen zu Phishing-Tests) und Warnhinweise bei potenziell schädlichen E-Mails
- Motivation der Anwender durch Informationen zu relevanten Bedrohungstrends bei wöchentlichen Bedrohungswarmmeldungen und monatlichen Attack Spotlight-Materialien

Bewertung der Wirksamkeit Ihres Programms

Es ist wichtig zu wissen, welchen Beitrag Sicherheitsschulungen für das Risiko Ihres Unternehmens leisten. Proofpoint liefert Verhaltenskennzahlen, die die Verbesserung der Sicherheit verdeutlichen, z. B. einen Rückgang der Klicks auf echte Bedrohungen um 40 % innerhalb von sechs Monaten. Mithilfe dieser Kennzahlen können Sie personenbezogene Risiken besser kommunizieren und die Wirksamkeit des Programms gegenüber dem CISO nachweisen. Proofpoint Security Awareness Enterprise bietet folgende Vorteile:

- Nachverfolgung von Verhaltenskennzahlen mit unserem leistungsstarken CISO-Dashboard für reale Bedrohungen und simulierte Phishing-Tests
- Entscheidungsrelevante Erkenntnisse zu langfristigen Verhaltensänderungen, z. B. Klickrate, Meldungsrate und Richtigkeit der Meldungen
- Verwaltung gezielter Schulungs- und Eskalationspläne mit Echtzeit-Kennzahlen zu Meldungen, z. B. wiederholte Nichterkennung von simulierten Bedrohungen
- Vergleich wichtiger Metriken mit denen von Mitbewerbern, damit Sie die Programmleistung an Führungskräfte und andere Verantwortliche kommunizieren können

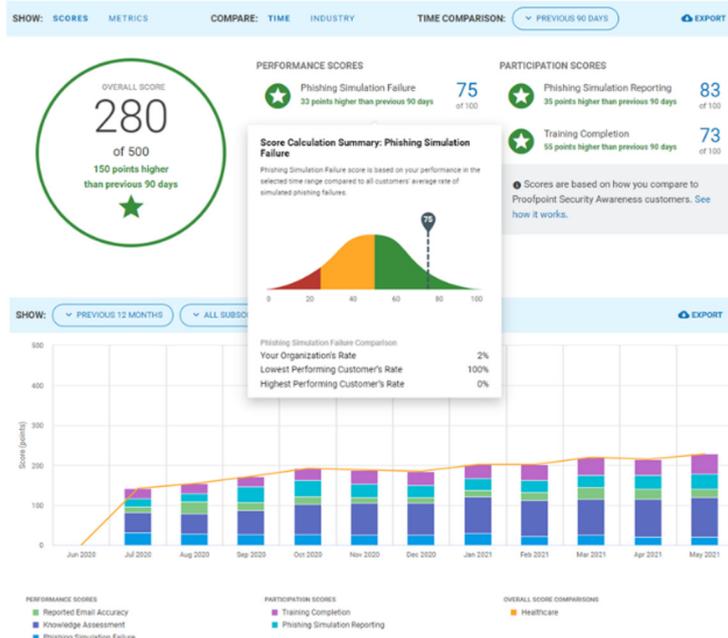


Abb. 3: Zusammenfassung der Programmleistung im CISO-Dashboard.

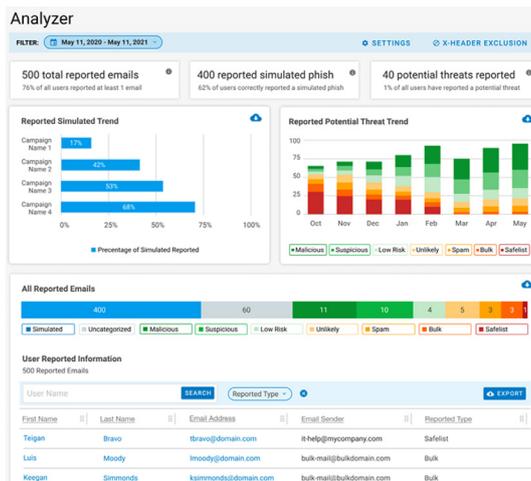


Abb. 4: Anwenderverhalten beim Melden von Phishing-Tests und echten E-Mails.

Erweiterung und Skalierung Ihres Programms

Proofpoint Security Awareness Enterprise unterstützt Sie durch Automatisierung und Skalierbarkeit und optimiert die Administration mit vereinfachten Workflows sowie automatisierten Prozessen, die Ihnen bei Ihren Abläufen mehr Kontrolle und Flexibilität geben. Zudem kann die Lösung für weltweite oder verteilte Niederlassungen skaliert werden. Proofpoint Security Awareness Enterprise bietet folgende Vorteile:

- Zeitersparnis dank automatisierter Untersuchung von Nachrichten, die von Anwendern gemeldet wurden (und automatisierter Behebung mit Proofpoint Threat Protection)
- Ansprechen einer globalen Zielgruppe durch Unterstützung von mehr als 40 Sprachen und Customization Services, mit denen Sie Ihrem Programm ein eigenes Gesicht geben können
- Optimierung des Multistreaming-Programms mit mandantenfähigen Verwaltungsoptionen, die einen unternehmensweiten Überblick und angepasste Administratorberechtigungen ermöglichen
- Mehr Effizienz dank Funktion für automatische Anmeldungen mit adaptiven Zuweisungen, bei denen Mitarbeitern bei Erfüllung bestimmter vordefinierter Kriterien automatisch passende Schulungen zugewiesen werden

- Festigung positiver Verhaltensweisen, indem Anwender nach dem Melden verdächtiger E-Mails angepasste Rückmeldungen erhalten (mit Proofpoint Threat Protection)

Optimierung und Entwicklung Ihres Programms

Für den Schutz Ihres Unternehmens müssen Sie personenzentrierte Risiken reduzieren. Unsere Premium Services für Security Awareness helfen Ihnen bei der Klärung und schnelleren Umsetzung Ihrer Strategie sowie bei der Stärkung Ihrer Maßnahmen gegen dynamische Cyberbedrohungen. Proofpoint Security Awareness Enterprise bietet folgende Vorteile:

- Kombination der empfohlenen Vorgehensweisen zu personenbezogenen Risiken und der Bedrohungsdaten von Proofpoint, um Ihre Sicherheitskultur aufzubauen und personenzentrierte Risiken in Ihrem Unternehmen zu minimieren
- Zusammenarbeit mit unseren Experten, um eine Strategie und ein Programm umzusetzen, die die Ziele Ihres Unternehmens berücksichtigen
- Identifizierung und Einführung von Verhaltensweisen und Schulungen, mit denen das Risiko reduziert und Sicherheit zu einem festen Bestandteil der Unternehmenskultur und -abläufe wird

MEHR ERFAHREN

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 85 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, Inc. Proofpoint ist eine Marke von Proofpoint, Inc. in den USA und anderen Ländern. Alle weiteren hier genannten Marken sind Eigentum ihrer jeweiligen Besitzer.