Proofpoint Security Awareness Training Enterprise

PRODUKTE

- Proofpoint Security Awareness Training Enterprise
- Proofpoint Targeted Attack Protection
- Proofpoint Threat Response Auto-Pull

WICHTIGE VORTEILE

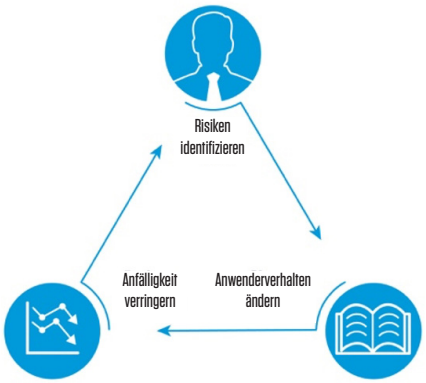
- Verringerung der Zahl erfolgreicher Phishing-Angriffe und Malware-Infektionen um bis zu 90 %
- Geringeres Risiko durch Phishing und andere Cyberangriffe durch Änderung des Anwenderverhaltens
- Maximale Effektivität der Maßnahmen durch gezielte und maßgeschneiderte Anwenderschulungen
- Geringe Anfälligkeit und Entlastung der IT dank informierter Anwender und automatisierter Reaktion auf Zwischenfälle
- Überwachung des Fortschritts mit dynamischem Reporting und Benchmark-Analysen

Da sich mehr als 90 Prozent aller Cyberangriffe gegen Anwender richten[1], steht und fällt der Schutz Ihres Unternehmens mit Ihren Mitarbeitern. Sicherheitstechnologien erkennen und blockieren Bedrohungen, bevor sie Ihre Anwender erreichen, können aber nicht alles stoppen. Ihre Mitarbeiter müssen darauf vorbereitet werden, Phishing-Angriffe und CEO-Betrug (Business Email Compromise) zu erkennen und angemessen zu reagieren. Mit der Proofpoint Security Awareness Training-Lösung lernen Ihre Anwender, Cyberangriffe erfolgreich zu erkennen und damit zu stoppen.

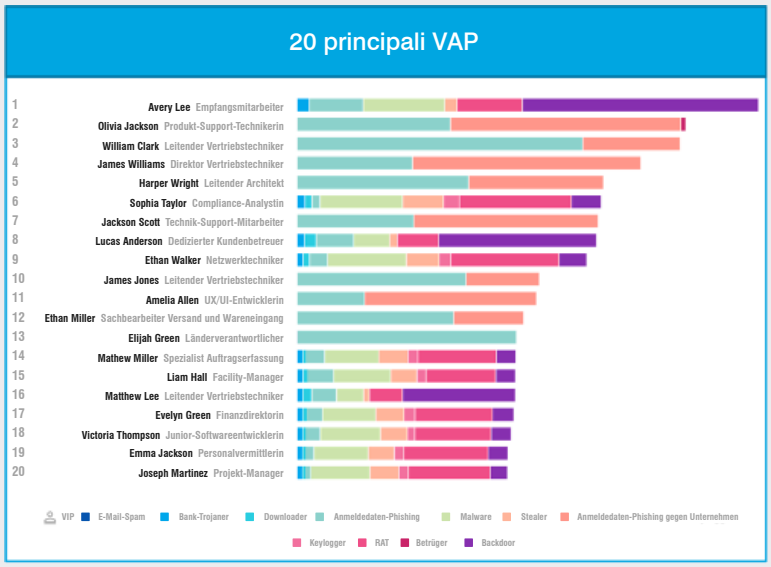
Mit Proofpoint Security Awareness Training Enterprise gewährleisten Sie, dass die richtigen Personen zum richtigen Zeitpunkt die richtigen Schulungen erhalten, damit sie richtig auf aktuelle Angriffe reagieren können. Damit werden Ihre Anwender zu einer starken Verteidigungslinie, die Ihr Unternehmen proaktiv schützt.

Unsere Lösungen bieten folgende Vorteile:

- Identifizierung von Anwenderrisiken
- Änderung des Mitarbeiterverhaltens
- Reduzierung der Angriffsfläche Ihres Unternehmens



1 Verizon: „2019 Data Breach Investigations Report“ (Untersuchungsbericht zu Datenkompromittierungen 2019), Juli 2019.



Ein Beispiel eines Very Attacked People-Berichts. Kunden können hochriskante Anwender mit simulierten Phishing-Angriffen zu den neuesten Angriffstrends schulen, und Anwender, die auf Simulationen hereinfallen, automatisch für Schulungen anmelden.

Risiken identifizieren

Sie stellen fest, wer angegriffen wird, und bewerten die Selbstschutz-Kompetenz.

Nicht alle Mitarbeiter werden gleich stark angegriffen. Es gibt viele Faktoren, die Angestellte zu einem begehrten Ziel für Cyberangriffe machen. Durch die Integration mit Proofpoint Targeted Attack Protection (TAP) können sich Ihre Administratoren auf die Bereiche mit dem höchsten Risiko konzentrieren und maximale Effektivität gewährleisten. Dies gelingt durch ein strenges und wirkungsvolles Programm zur Sensibilisierung für Sicherheit, das auf den realen Risiken in der E-Mail-Umgebung Ihrer Mitarbeiter basiert.

Die leistungsfähige Integration liefert Ihnen Details zu Ihren VAPs (den Very Attacked People, also den besonders häufig angegriffenen Personen) und den Top Clickers (den Personen, die am häufigsten auf unsichere Links klicken). Sie erhalten zudem Einblick in die Bedrohungsarten, mit denen Ihre Mitarbeiter in Kontakt kommen. Anhand dieser Informationen können Sie Anwender zur Risikoeinschätzung zu Simulationen und Wissenstests anmelden oder ihnen Schulungen zuweisen, die darauf ausgelegt sind, das Verhalten zu ändern.

Mit ThreatSim®-Phishing-Simulationen können Sie anhand simulierter Phishing-E-Mails die reale Anfälligkeit Ihres Unternehmens für verschiedene Ausprägungen von Phishing-Angriffen feststellen. Mit tausenden unterschiedlichen Phishing-Vorlagen in 13 Kategorien können Sie Ihre Anwender in Bezug auf eine Vielzahl an Bedrohungsarten testen, darunter:

- Schädliche Anhänge
- Eingebettete schadhafte Links
- Anfragen zur Weitergabe sensibler oder personenbezogener Daten

Jede Woche kommen neue Vorlagen hinzu, damit auch die neuesten Angriffstrends immer berücksichtigt werden.

Unsere Phishing-Vorlagen basieren auf Proofpoint-Bedrohungsdaten, werden aber auch auf konkreten Kundenwunsch erstellt und greifen zudem saisonbezogene Themen auf, wie sie auch von echten Cyberkriminellen benutzt werden. Die Proofpoint-Lösung zum Echtzeit-Austausch von Bedrohungsdaten ist eine der unter den Fortune 100, Fortune 1000 und Global 2000 am weitesten verbreitete Lösungen. Sie profitieren davon, dass Vorlagen immer einen Bezug zu realen Angriffen auf Anwender haben.

Wenn Anwender auf einen simulierten Angriff hereinfallen, erhalten sie sofort relevante Hinweise und erfahren Folgendes:

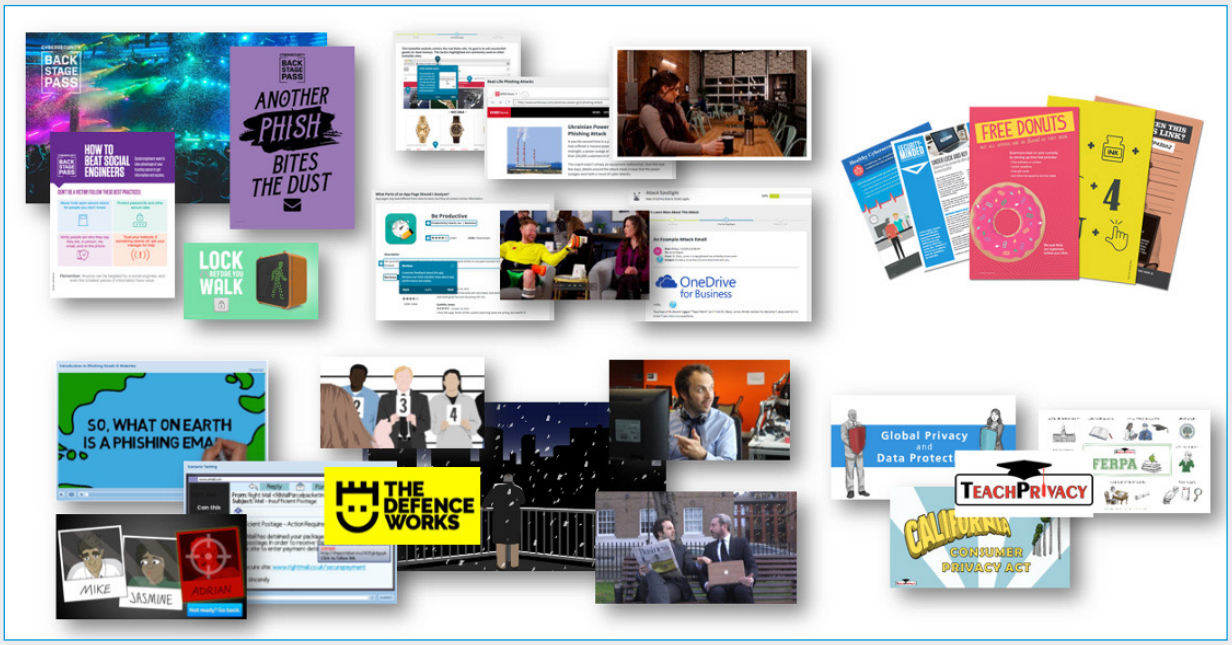
- Den Zweck der Übung
- Die Gefahren, die damit bei realen Angriffen verbunden sind
- Wie sie solche Köder in Zukunft besser erkennen können, um nicht mehr auf sie hereinzufallen.

Zusätzlich können Sie allen Personen, die auf eine Phishing-Simulation hereinfallen, automatisch weitere Schulungen zuweisen.

Außerdem haben Sie die Möglichkeit, die Kenntnisse Ihrer Mitarbeiter in anderen Bereichen, z. B. in Hinblick auf infizierte USB-Sticks, zu testen. Mit ThreatSim-USB-Simulationen lernen Ihre Mitarbeiter die Gefahren infizierter USB-Geräte kennen. Sie können jederzeit und in beliebigem Umfang auf USB-Simulationen zugreifen, bei denen Anwender, die auf die Simulation hereinfallen, direkt relevante Hinweise erhalten. Dadurch wird die Lernerfahrung deutlich verstärkt.

In Simulationen können allerdings immer nur bestimmte Risiken dieser Bedrohungsvektoren vermittelt werden. Das leistungsstarke Wissenstest-Tool CyberStrength® bietet folgende Funktionen:

- Überprüfen Sie die Schwachstellen Ihrer Anwender zu verschiedensten wichtigen Sicherheitsproblemen jenseits von E-Mails und USB-Sticks. Zu den Themen gehören der Umgang mit mobilen Endgeräten, das Erkennen von Social-Engineering-Betrug, Kennwörter sowie sicheres Surfen im Web.



- Ihnen steht für den Wissenstest eine Bibliothek mit hunderten vordefinierten Fragen in mehr als 40 Sprachen zur Verfügung. Zudem besteht die Möglichkeit, Anwender basierend auf den Testergebnissen entsprechend der dadurch eruierten Schwachstellen automatisch für die entsprechende Schulung anzumelden.
- Sie können eigene Fragen zu den Richtlinien und Vorgehensweisen in Ihrem Unternehmen hinzufügen, um das Wissen Ihrer Anwender dazu zu ermitteln.
- Folgen Sie Empfehlungen zur Minimierung Ihrer Anwenderrisiken in getesteten Themenbereichen, sobald eine Einschätzung vorliegt.

Anwenderverhalten ändern

Sie stellen Schulungen basierend auf Echtzeit-Bedrohungen, Benutzerverhaltensweisen und Wissenslücken bereit.

Unsere Schulungen sollen eine Verhaltensänderung bewirken und sind daher für ein maßgeschneidertes und wirkungsvolles Schulungserlebnis optimiert. Der Schwerpunkt unseres Programms liegt auf hochriskanten Bereichen. Schulungen werden VAPs oder Top Clickers zugewiesen, die von Proofpoint Targeted Attack Protection (TAP) identifiziert wurden. Zudem können Schulungen auf Anwender konzentriert werden, die in Simulationen durchgefallen sind oder eine gewisse Punktzahl im Wissenstest unterschritten haben.

Die erstklassigen Inhalte von Proofpoint haben bereits Millionen von Anwendern geholfen, sich für Bedrohungen zu wappnen und zu einer starken Verteidigungslinie für ihr Unternehmen zu werden. So stellen wir sicher, dass unsere Inhalte Verhaltensänderungen bewirken:

Methoden und Nutzbarkeit

- Anwendung bewährter Methoden zur Verhaltensänderung bei Erwachsenen
- Inhalte lassen sich über unsere Content-Bibliothek problemlos abrufen und durchsuchen
- Abwechslungsreiche Inhalte mit hunderten Schulungsmodulen und Materialien zum Schulungsprogramm
- Von CISOs geleitete grundlegende Schulungspläne zum Aufbau der nötigen Fähigkeiten, abhängig vom Anwendertyp (privilegiert, rollenbasiert und andere)

Internationale und multikulturelle Unterstützung

- Mehr als 40 Sprachen und regionale Referenzen (Domänen, Namen usw.) für alle grundlegenden Schulungspläne
- Inklusivität und Diversität in Texten und Bildern

Vorbereitung auf neue Bedrohungen

- Verwendung der besten Bedrohungsdaten auf dem Markt, um Angreifern einen Schritt voraus zu bleiben
- Täglich Milliarden untersuchte Bedrohungen aus E-Mail, Cloud und sozialen Netzwerken
- Auf realen Bedrohungen basierende Inhalte wie unsere Warnmeldungen zu Bedrohungen, Attack Spotlight-Module und Simulationsvorlagen

Abwechslungsreichtum spielt eine große Rolle bei der Bereitstellung geeigneter Inhalte für Ihre Anwender. Proofpoints schnell wachsende Bibliothek umfasst mehr als 200 Schulungsmodule. Unsere Schulungsmaterialien enthalten hunderte PDF-Dateien, Infografiken, Videos, Meme und anderes. Durch die Übernahme von The Defence Works im Mai 2020 und die Partnerschaft mit TeachPrivacy stehen Ihnen noch viel mehr Inhalte zur Verfügung, die sich mit ihren verschiedenen Stilen für jede Unternehmenskultur eignen. Unsere bewährten Methoden, Kampagnen und Schulungspläne unterstützen Sie bei der Zusammenstellung interaktiver, breit gefächerter Schulungserlebnisse.

Um Beispiele für verfügbare Inhalte anzusehen, laden Sie die Lösungsübersicht zu den Proofpoint Security Awareness Training-Inhalten herunter.

Fehlerquote/Klickrate

< 5 %

Meldungsrate

> 70 %

High Reporting Rates, Low Failure Rates

Subject Line	Template Style	Number of Messages Sent	Failure Rate	Reporting Rate
Someone has your password	Data entry	798	<1%	86%
Please DocSign this document: Contract_Change	Attachment	441	2%	85%
COMPANY CONFIDENTIAL: Upcoming public announcement	Link	442	2%	83%
Toll Violation Notice*	Link	676	4%	81%
Network Access Attempt	Data entry	360	1%	80%

Dieses Ziel soll Ihr Unternehmen erreichen

Tatsächliche Kundenergebnisse von den erfolgreichsten Unternehmen aus dem „State of the Phish“-Bericht 2020 von Proofpoint.

Bereitstellung der Inhalte

Mittels des Customization Centers in unserer Plattform können Sie die verfügbaren Inhalte so anpassen, dass Sie für Ihre Anwender höchst relevant sind. Die Lösung bietet folgende Möglichkeiten:

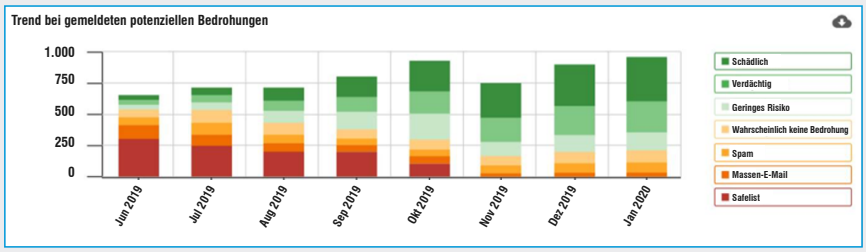
- Sie können die Formulierungen, Bilder und Fragen der Schulungen für die Bedürfnisse Ihrer Anwender maßschneidern.
- Sie haben die Möglichkeit, Module, Lektionen und Seiten schnell zu klonen und zu modifizieren, um die notwendigen Änderungen vorzunehmen – und das alles in Echtzeit.
- Die Module können sogar mit einem Schalter von Schulungsmodulen (mit Fragen) in Sensibilisierungsmodule umgewandelt werden.
- Um die Effektivität zu gewährleisten, überprüft unser Learning Science Evaluator Ihre Änderungen und liefert Feedback. Wenn zum Beispiel die Länge, Menge von Inhalten auf einem Bildschirm oder Anzahl von Fragen in einer Aufgabe von den Empfehlungen abweichen, weisen wir Sie darauf hin.

Bei Unternehmen mit einem eigenen Learning Management System (LMS), das SCORM-basierte Dateien nutzt, können Administratoren die Schulungsmodule problemlos anpassen und in ihr LMS exportieren. Sie haben die Möglichkeit, mehrere Module zu einem einzigen Modul zusammenzuführen und können auch festlegen, in welcher Reihenfolge sie bevorzugt bearbeitet werden sollen.

Anfälligkeit verringern

Geschulte Anwender melden potenzielle Bedrohungen und verringern so die Angriffsfläche.

Ermöglichen Sie Ihren Mitarbeitern, verdächtige Nachrichten mit einem einzigen Klick über unser E-Mail-Client-Add-in PhishAlarm® zu melden. Anwender, die eine E-Mail melden, erhalten sofort positive Bestärkung in Form einer Popup-Meldung mit einem Dankeschön. Dank des PhishAlarms müssen E-Mails nicht samt Header und Anhang an ein Abuse-Postfach weitergeleitet werden. Die üblichen Meldungsraten für Unternehmen liegen zwischen 10 und 20 %. Dank geschulter Anwender haben bei erfolgreichen Kunden stets mehr als 70 % und in einigen Fällen sogar 80 % der Anwender simulierten Angriffe gemeldet.

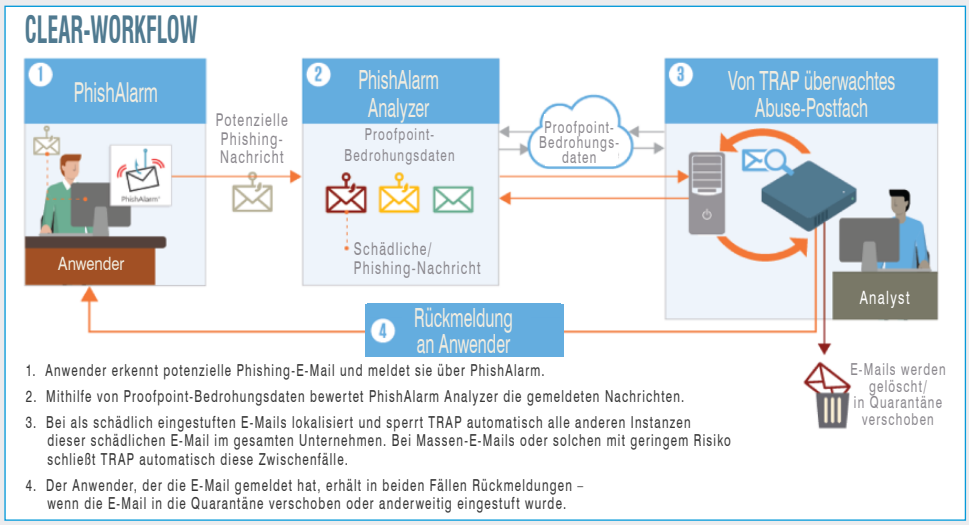


Durch einen Überblick über gemeldete Nachrichtenarten werden die Änderungen im Anwenderverhalten besser verständlich.

Umsetzbare Informationen für das Incident-Response-Team.

Von simulierten Angriffen geht nicht die gleiche Gefahr wie von echten Bedrohungen in Ihrer Umgebung aus. Wir verfügen über erstklassige Bedrohungsdaten und Sandbox-Analysen. Mit einem übersichtlichen Bedrohungsbericht informieren wir Sie automatisch darüber, welche von Anwendern gemeldeten Nachrichten schädlich sind und welche nicht – und was genau an den Nachrichten schädlich ist, sodass Ihre Incident-Response-Teams Zeit sparen. Sie erhalten zudem einen Einblick darin, wie Ihr Awareness-Programm E-Mail-basierte Risiken verringert. Unsere Bedrohungsdaten basieren auf der unter den Fortune 100, Fortune 1000 und Global 2000 am weitesten verbreiteten Lösung, die branchenführende Aggregation und Korrelation von Bedrohungsdaten zu E-Mails, Cloud, Netzwerken sowie sozialen Netzwerken bietet.

Unsere automatisierte Lösung CLEAR (Closed-Loop Email Analysis and Response) sendet gemeldete Nachrichten an TRAP (Threat Response Auto-Pull). In TRAP können diese Nachrichten automatisch unter Quarantäne gestellt oder geschlossen werden. Bei Bedarf können sie zur weiteren Analyse auch an Ihr Incident-Response-Team geschickt werden. Administratoren können je nach Nachrichtenklassifikation individuelle Antwortnachrichten für die Anwender erstellen. Diese Nachrichten verstärken richtiges Verhalten und fördern den Aufbau einer sicherheitsbewussten Kultur.



1. Anwender erkennt potenzielle Phishing-E-Mail und meldet sie über PhishAlarm.
2. Mithilfe von Proofpoint-Bedrohungsdaten bewertet PhishAlarm Analyzer die gemeldeten Nachrichten.
3. Bei als schädlich eingestuften E-Mails lokalisiert und sperrt TRAP automatisch alle anderen Instanzen dieser schädlichen E-Mail im gesamten Unternehmen. Bei Massen-E-Mails oder solchen mit geringem Risiko schließt TRAP automatisch diese Zwischenfälle.
4. Der Anwender, der die E-Mail gemeldet hat, erhält in beiden Fällen Rückmeldungen – wenn die E-Mail in die Quarantäne verschoben oder anderweitig eingestuft wurde.

Erfassen und anpassen

Erkennen Sie, wie sich Anwenderverhalten auf wichtige Ergebnisse auswirkt

Unsere umfassenden Berichte halten Sie über Änderungen im Anwenderverhalten auf dem Laufenden und zeigen Ihnen, wie Ihr Unternehmen im Vergleich zu anderen abschneidet. Sehen Sie, wie Mitarbeiter mit folgenden Maßnahmen interagieren:

- Tests
- Simulationen von Angriffen
- Schulungszuweisungen
- E-Mail-Berichte und Analysen (inkl. Einstufungen)

In den Berichten können Sie problemlos Daten filtern, Tests vergleichen, Maßnahmen ändern und eigene Ansichten einrichten.

Beantworten Sie wichtige Fragen wie:

- Welche Personen in meinem Unternehmen sind am anfälligsten für simulierte Phishing-Angriffe?
- Welche Wissenslücken hat meine Anwenderbasis bei den wichtigsten Sicherheits- und Compliance-Themen?
- Wie gut schneiden meine Anwender in den Schulungen ab?
- Wie viele und welche Art von Nachrichten melden Anwender (schädliche E-Mails, Massen-E-Mails, Spam usw.)?

Sie können Berichte herunterladen, exportieren und automatisch an andere übermitteln lassen. Dadurch kann Ihr Unternehmen Einblicke einfacher verfolgen und die Ergebnisse automatisch an die Verantwortlichen Ihres Programms weitergeben.

Mit unserer ebenfalls enthaltenen Berichts-API erhalten Sie Zugriff auf Berichte und Analysen zu Schulungen, Phishing, Wissenstests, Anwendern und E-Mails. Diese Informationen lassen sich in gängige Business-Intelligence-Tools und Learning-Management-Systeme integrieren.

WEITERE INFORMATIONEN

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

proofpoint.

0204-005-01-01 1/21