

# Proofpoint Essentials – Security Awareness

## WICHTIGE VORTEILE

- Verringerung der Zahl erfolgreicher Phishing-Angriffe und Malware-Infektionen um bis zu 90 %
- Änderung des Anwenderverhaltens
- Bereitstellung einheitlicher Schulungen, die für KMUs optimiert sind
- Schulungsinhalte in mehr als 35 Sprachen
- Nachverfolgung der Ergebnisse und Fortschritte mit leicht verständlichen Berichten

Mit Proofpoint Essentials – Security Awareness gewährleisten KMUs, dass die richtigen Personen zum richtigen Zeitpunkt die richtigen Schulungen erhalten, damit die Endnutzer zu einer starken letzten Verteidigungslinie gegen Cyberangriffe werden.

Mehr als 90 % der aktuellen Cyberangriffe richten sich per E-Mail gegen Anwender.<sup>1</sup> Doch obwohl die technischen Schutzmaßnahmen wichtig sind, können sie nicht alle Bedrohungen abwehren. Deshalb benötigen Sie gut geschulte Mitarbeiter als starke letzte Verteidigungslinie. Ihre Anwender müssen Phishing, Business Email Compromise (BEC, auch Chefmasche genannt) und andere Bedrohungen erkennen und vermeiden können. Ein effektives Schulungsprogramm zur Steigerung des Sicherheitsbewusstseins zeigt Ihren Mitarbeitern, wie sie Bedrohungen zuverlässig erkennen.

Proofpoint Essentials – Security Awareness wurde speziell für die Anforderungen von KMUs optimiert. Mit unserem personenorientierten Ansatz können Sie das Verhalten Ihrer Mitarbeiter effizient ändern, sodass das Risiko von Kompromittierungen für Ihr Unternehmen reduziert und Ausfallzeiten für Ihre Mitarbeiter minimiert werden.

## SCHUTZ IHRES UNTERNEHMENS MIT THREATSIM-PHISHING-SIMULATIONEN

Ein erfolgreiches Programm zur Steigerung des Sicherheitsbewusstseins beginnt damit, dass Ihre Anwender die richtigen Schulungen erhalten. Mit unseren ThreatSim®-Phishing-Simulationen können Sie die Anfälligkeit Ihrer Anwender für verschiedene Phishing- und Spearphishing-Angriffe feststellen. Mit tausenden unterschiedlichen Vorlagen in 13 Kategorien können Sie Ihre Anwender in Bezug auf eine Vielzahl von Bedrohungsarten testen, darunter:

- Schädliche Anhänge
- Unsichere URLs
- Anfragen zur Weitergabe sensibler oder personenbezogener Daten

Sie müssen außerdem gewährleisten, dass die Schulungen an die sich stets ändernden Bedrohungen angepasst werden. Wir fügen jede Woche neue Vorlagen hinzu, damit auch die neuesten Angriffstrends immer berücksichtigt werden. Unsere Phishing-Vorlagen für dynamische Bedrohungssimulationen basieren auf:

- Proofpoint-Bedrohungsdaten
- Anfragen von Kunden
- Saisonalen Trends

Wenn Anwender auf einen simulierten Angriff hereinfallen, erhalten sie sofort relevante Hinweise. So erfahren sie, welchen Zweck die Übung hat, welche Gefahren damit bei realen Angriffen verbunden sind und 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, Schulungen zuweisen.

<sup>1</sup> Verizon: „Data Breach Investigations Report“ (Untersuchungsbericht zu Datenkompromittierungen), Mai 2019.

## Schulung Ihrer Mitarbeiter mit ansprechenden und relevanten Schulungsinhalten

Unsere Schulungsinhalte basieren auf wissenschaftlich bestätigten Lernprinzipien und decken ein breites Spektrum an Sicherheitsrisiken ab. Zudem erweitern wir unsere Content-Bibliothek kontinuierlich mit interaktiven Schulungsmodulen und Inhalten mit Gamification-Elementen, damit auch die neuesten Angriffstrends immer berücksichtigt werden. Die Botschaften sind konsistent und die Materialien in mehr als 35 Sprachen verfügbar.

Ihre Anwender können unsere Schulungen jederzeit, überall und von jedem angeschlossenen Endgerät aus abrufen, wobei pro Modul jeweils nur 5 bis 15 Minuten erforderlich sind. Dadurch bleiben Ihre Mitarbeiter motiviert und müssen ihre Arbeitsroutine nicht unterbrechen. Unsere interaktiven Module entsprechen den Standards U.S. Section 508 sowie den Web Content Accessibility Guidelines (WCAG) 2.0 AA.

## Analyseergebnisse durch Reporting mit vollem Funktionsumfang

Unsere Berichte liefern einen vollen Überblick über die Schwachstellen und Verhaltensweisen Ihrer Anwender. Deren Interaktionen, Reaktionen auf simulierte Angriffe und die Ergebnisse der Schulungsaufgaben zeigen Ihnen den Fortschritt der Mitarbeiter.

Unsere responsiven, leicht verständlichen Berichte sind über die vertraute Proofpoint Essentials-Benutzeroberfläche abrufbar und bieten folgende Möglichkeiten:

- Download und Export von Daten
- Weitergabe der Ergebnisse an die jeweiligen Verantwortlichen
- Durchführung detaillierterer Analysen
- Vergleich der Kennzahlen von anderen Sicherheitsereignissen

## WEITERE INFORMATIONEN

Weitere Informationen finden Sie unter [proofpoint.com/de](https://www.proofpoint.com/de).

### INFORMATIONEN ZU PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT) ist ein führendes Cybersicherheitsunternehmen. 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 personenorientierten 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](https://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.