proofpoint.

Proofpoint Threat Protection

Schutz für Ihre Mitarbeiter vor aktuellen Bedrohungen

Wichtige Vorteile

- Schnellere Erkennung und Blockierung aktueller E-Mail-Bedrohungen
- Zuverlässigeres Stoppen neuer Bedrohungen dank kontinuierlicher KI-gestützter Analysen
- Erkenntnisse zu Risiken durch personenbezogene und bedrohungsbezogene Risiken
- Verbesserte operative Effizienz
- Schulungen für Ihre Mitarbeiter und Förderung von Verhaltensänderungen

E-Mail ist der wichtigste Risikovektor bei Cybersicherheitsbedrohungen. Derzeit nehmen unzählige Malware-, Phishing- und Social-Engineering-Angriffe Ihre Mitarbeiter ins Visier. Laut dem Verizon Data Breach Investigations Report 2023 gehen 74 % aller Datenschutzverletzungen mit einer menschlichen Komponente einher.[1] Mit Proofpoint Threat Protection können Sie Ihre Mitarbeiter vor aktuellen Bedrohungen schützen.

Cyberkriminalität ist ein Wachstumsmarkt

Cyberkriminalität boomt, da sie bei minimalen Risiken enorme Gewinne verspricht. Cybersecurity Ventures geht davon aus, dass Cybercrime-Aktivitäten bis 2025 Kosten in Höhe von 10,5 Billionen pro Jahr verursachen werden.[2] Cybercrime-Organisationen gehen – als gewinnorientierte Unternehmen – gezielt vor und versuchen, wertvolle persönliche Informationen und Unternehmensdaten zu stehlen, Identitätsdiebstahl zu begehen und E-Mail-Angriffe zu starten, die auf Finanzbetrug abzielen. E-Mails sind für den Geschäftsbetrieb moderner Unternehmen unverzichtbar und werden daher als wichtigster Angriffsvektor gegen Ihre Mitarbeiter genutzt. Die kriminellen Akteure entwickeln ihre Taktiken permanent weiter. Und da sie kaum abgewehrt werden können, fällt es selbst großen und gut ausgestatteten IT-Abteilungen äußerst schwer, die Belegschaft vor diesen aktuellen Bedrohungen zu schützen. Doch Proofpoint kann Ihnen helfen.

1 Verizon: *2023 Data Breach Investigations Report* (Untersuchungsbericht zu Datenkompromittierungen 2023), 2023.
2 Steve Morgan *(Cybercrime Magazine)*: „Cybercrime To Cost The World 10.5 Trillion Annually By 2025“ (Die weltweiten Kosten für Cyberkriminalität werden bis 2025 10,5 Billionen US-Dollar pro Jahr betragen), November 2020.

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

84 %

der Fortune 100 vertrauen beim Schutz ihrer Mitarbeiter vor Bedrohungen auf Proofpoint.

Quelle: Proofpoint, 2023

Schnellere Identifizierung und Blockierung von E-Mail-Bedrohungen mit Erkennung vor der Zustellung

Durch unsere Erkennung vor der Zustellung können Sie bekannte und unbekannte Bedrohungen in Ihrem gesamten Unternehmen identifizieren und stoppen. Das bedeutet, dass raffinierte Bedrohungen wie die folgenden gar nicht erst die Posteingänge Ihrer Mitarbeiter erreichen:

- Komplexes Anmeldedaten-Phishing
- Malware
- Ransomware
- Business Email Compromise (BEC)
- Schädliche URLs
- QR-Code
- Anhänge
- und mehr

Wenn diese Funktionen mit unserer automatisierten Erkennung und Behebung nach der Zustellung kombiniert werden, können Sie Ihre Mitarbeiter mit einer einzigen, umfassenden Lösungen vollständig schützen.

Identifizierung von Bedrohungen mit KI-gestützter, mehrschichtiger Erkennung

Wir nutzen mehrschichtige Erkennungstechnologien, die Bedrohungsdaten, Machine Learning, verhaltensbasierte KI-gestützte Sandbox-Erkennung sowie Semantik- und Inhaltsanalysen (LLMs) umfassen. Diese arbeiten zusammen, um mehrere aktuelle Bedrohungsarten zu erkennen und eine hohe Erkennungsrate von 99,99 % bei besserer Erklärbarkeit zu erreichen. Im Gegensatz zu „einschichtigen“ Lösungen zur Erkennung von E-Mail-Bedrohungen generiert Proofpoint Threat Protection weniger False Negatives und False Positives, d. h. schädliche Nachrichten werden zuverlässig gestoppt, ohne legitime Nachrichten zu blockieren und Ihre Geschäftsabläufe zu beeinträchtigen.

Abb. 1: Die KI-gestützte, mehrschichtige Proofpoint-Technologie zur Erkennung von Bedrohungen vor der Zustellung in Aktion.

Umfassender Überblick über personenbezogene Risiken und Bedrohungen

Mit Proofpoint erhalten Sie einzigartige Erkenntnisse zu Ihren Very Attacked People™ (VAPs) und den Bedrohungen gegen Ihr Unternehmen, sodass Sie gezielte adaptive Kontrollen implementieren können, einschließlich Browser-Isolierung, Security-Awareness-Schulungen, zusätzliche Authentifizierungsmaßnahmen und mehr. In Kombination mit unserem Überblick über Ihre personenzentrierten Risiken erhalten Sie wertvolle Informationen zu Ihren Mitarbeitern – wie häufig werden sie angegriffen, wie anfällig sind sie für Angriffe und über welche Berechtigungen verfügen sie. Außerdem analysiert Proofpoint pro Jahr mehr als 3 Billionen E-Mail-Nachrichten bei insgesamt mehr als 230.000 Kunden, Partnern sowie innerhalb des Anbieter-Ökosystems. Dank unserer Bedrohungsdaten und Forschung erhalten Sie außerdem Frühwarnungen zu neuen, bislang unbekannten Bedrohungen.

Verbesserte operative Effizienz

Mit Proofpoint können Sie automatisch E-Mails erkennen und beheben, die sich nach der Zustellung als schädlich erweisen. Die automatische Triagierung von Nachrichten und Entfernung von E-Mails mit Schaddaten vereinfacht die schnelle und effiziente Identifizierung sowie Beseitigung von Bedrohungen. Ganz gleich, ob es sich um unerwünschte E-Mails von intern kompromittierten Konten, um weitergeleitete E-Mails oder um E-Mails handelt, die ursprünglich andere Anwender erhalten haben, erhalten Sie bei Proofpoint automatische Warnmeldungen, Vergleichsanalysen sowie entscheidungsrelevante Bedrohungsansichten. Dies reduziert den Aufwand für die Behebung, sodass Ihr Team entlastet und somit effizienter wird. Zudem haben die Anwender die Möglichkeit, verdächtige E-Mails ganz einfach mit einem Klick über einen Warnhinweis in E-Mails oder eine PhishAlarm-Schaltfläche zu melden. Wird eine von einem Anwender gemeldete Nachricht als schädlich erkannt, kann sie – einschließlich aller Kopien – automatisch unter Quarantäne gestellt werden. Anwender erhalten wiederum eine E-Mail-Benachrichtigung mit der Information, dass die Nachricht als schädlich eingestuft und automatisch entfernt wurde. Dieses Benachrichtigungssystem hilft, richtiges Verhalten zu fördern und Ihre Mitarbeiter zu motivieren, ähnliche Nachrichten auch weiterhin zu melden.

Schulungen für Ihre Mitarbeiter und Förderung von Verhaltensänderungen

Mit Proofpoint können Sie personenbezogene Risiken zusätzlich verringern, indem Sie riskante Verhaltensweisen ändern und sichere Verhaltensweisen fördern. Unsere umfangreichen Bedrohungsdaten fließen auf unterschiedliche Weise in Ihr Security-Awareness-Programm ein, z. B. durch die Gestaltung realistischer Phishing-Simulationen, durch gezielte Schulungen für Top Clicker und die am häufigsten angegriffenen Mitarbeiter sowie durch die automatisierte Untersuchung von Anwendern gemeldeter Nachrichten.

Abb. 2: Proofpoint bietet Ihnen einen Überblick über Ihre personenzentrierten Risiken, einschließlich Ihrer Very Attacked People™ (VAPs).

Dank personalisierter Lernerlebnisse bleiben Ihre Mitarbeiter langfristig motiviert. Gleichzeitig trägt der adaptive Ansatz dazu bei, dass das Gelernte gefestigt wird und sichere, nachhaltige Verhaltensweisen umgesetzt werden. Mit Statistiken zu realen Verhaltensänderungen und Benchmark-Vergleichen mit anderen Unternehmen helfen wir Ihnen, die personenbezogenen Risiken sowie die Wirksamkeit Ihres Programms besser gegenüber Führungskräften zu kommunizieren.

Proofpoint Managed Services-Angebote

Zu Proofpoint Threat Protection bietet Ihnen Proofpoint die folgenden Managed Services an:

- **Managed Email Threat Protection:** Umfasst proaktive Expertise, kontinuierlich verfügbares Personal sowie Einblicke für Führungskräfte. Wir übernehmen die Verwaltung Ihrer E-Mail-Sicherheitslösung, führen tägliche Statusprüfungen durch und nutzen unsere Bedrohungsdaten proaktiv.
- **Managed Abuse Mailbox:** Reduziert den Aufwand für manuelle Prüfungen von Anwendern gemeldeter verdächtiger Nachrichten. Unser Team führt Analysen durch und stuft alle nicht automatisch klassifizierten Nachrichten eindeutig als legitim oder gefährlich ein.
- **Managed Security Awareness:** Wir unterstützen Sie bei der Optimierung Ihrer Sicherheitsschulungen, indem wir Ihre Programmstrategie darauf ausrichten, dass das Verhalten Ihrer Anwender geändert und eine robustere Sicherheitskultur aufgebaut wird.

Weitere Informationen hierzu finden Sie unter **www.proofpoint.com/de/products/aegis**.

WEITERE INFORMATIONEN

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

0203-007-04-01 3/24