proofpoint.

KURZVORSTELLUNG

Proofpoint User Protection

Schulung Ihrer Mitarbeiter und erweiterter Schutz vor Kontoübernahmen und Phishing auch jenseits von E-Mails

Wichtige Vorteile

- **Phishing-Schutz**, der nicht nur E-Mails abdeckt
- **Verbesserter Schutz** durch integrierte Bedrohungsdaten von Proofpoint
- **Geschulte Mitarbeiter**, die im Bedrohungsfall die richtige Entscheidung treffen
- **Automatisierte Reaktionen** auf Kontoübernahmen

Cyberkriminelle nehmen Ihre Mitarbeiter nach wie vor per Social Engineering ins Visier und versuchen, sie durch Tricks oder Drohkulissen zum Preisgeben ihrer Anmeldedaten oder Ausführen von schädlichem Code zu verleiten. E-Mail ist weiterhin der bevorzugte Angriffsvektor, jedoch werden mittlerweile auch zahlreiche andere digitale Kanäle von den Angreifern ausgenutzt, darunter Collaboration- und Messaging-Tools wie Slack, Microsoft Teams, LinkedIn und Zoom. Ziel der Angriffe ist es, Anwenderkonten zu kompromittieren und zu übernehmen. Laut einer 2024 von Proofpoint durchgeführten Studie sind 99 % der Unternehmen regelmäßig Ziel von versuchten Kontoübernahmen – und bei 62 % sind diese Angriffe erfolgreich.[1] Die Ergebnisse zeigen, dass Unternehmen einen ganzheitlichen Ansatz benötigen, um ihre Mitarbeiter zu schützen und das Risiko für Kontenkompromittierungen zu reduzieren.

Proofpoint User Protection bietet Ihren Mitarbeitern mehrschichtigen Schutz, der über E-Mail hinausgeht. Die Lösung automatisiert risikobasiertes Lernen für die Top Clicker und Very Attacked People (VAPs) in Ihrem Unternehmen, bietet eine nahtlose Anwendererfahrung und blockiert schädliche URL-Links, die über Collaboration- und Messaging-Tools verbreitet werden. Durch KI-basierte Erkennung und automatisierte Behebungsmaßnahmen bietet sie wirksamen Schutz vor Kontoübernahmen und beschleunigt die Reaktion auf Bedrohungen.

1. Proofpoint-Forschungsdaten, Stichprobengröße n > 5.000 Unternehmen, 2024

Stärkerer Schutz durch verbesserte Transparenz

Mit Proofpoint User Protection können Sie das Potenzial der Proofpoint Human-Centric Security-Plattform nutzen, d. h. Ihnen stehen unsere Bedrohungsdaten und risikobezogenen Erkenntnisse zur Verfügung, sodass Sie von stärkerem Schutz und umfassenden Einblicken zu besonders gefährdeten Personen und schädlichen Aktivitäten profitieren.

Proofpoint User Protection nutzt Proofpoint Nexus®, eine umfassende Plattform für Bedrohungsdaten, die künstliche Intelligenz (KI), Machine Learning und Echtzeit-Bedrohungsdaten nutzt. Proofpoint User Protection erweitert diese branchenführenden Erkennungstechnologien um Blockierungsfunktionen für alle schädlichen URL-Links – unabhängig davon, auf welchem Weg sie eingeschleust werden. Die Lösung kann dabei Kontoübernahmen in Tools wie Microsoft 365, Google Workspace und Okta zuverlässig identifizieren und analysiert das Verhalten Ihrer Anwender sowie deren Abschneiden bei Sicherheitsschulungen und Bedrohungssimulationen, sodass Sie erfahren, welche Mitarbeiter besonders gefährdet sind. Darüber hinaus überprüft die Risikoanalyse, ob Anzeichen für aktive Kontenkompromittierungen vorhanden sind.

Durch den besseren Überblick über personenbezogene Risiken lassen sich für Anwender mit unterschiedlichem Risikoprofil adaptive Sicherheitskontrollen anwenden. So können Sie beispielsweise Ihre VAPs, Top Clicker oder potenzielle Zielpersonen automatisch einer auf ihre Bedürfnisse zugeschnittenen Sicherheitsschulung zuweisen. Sollte es dennoch zu einer Kontoübernahme gekommen sein, können Sie automatisierte Behebungsmaßnahmen durchführen und beispielsweise Zugriffsrechte widerrufen, Kennwörter zurücksetzen oder Konten unter Quarantäne stellen. Auch das Widerrufen des Zugriffs durch Drittanwendungen und Rückgängigmachen schädlicher Änderungen an Postfach-Regeln ist möglich.

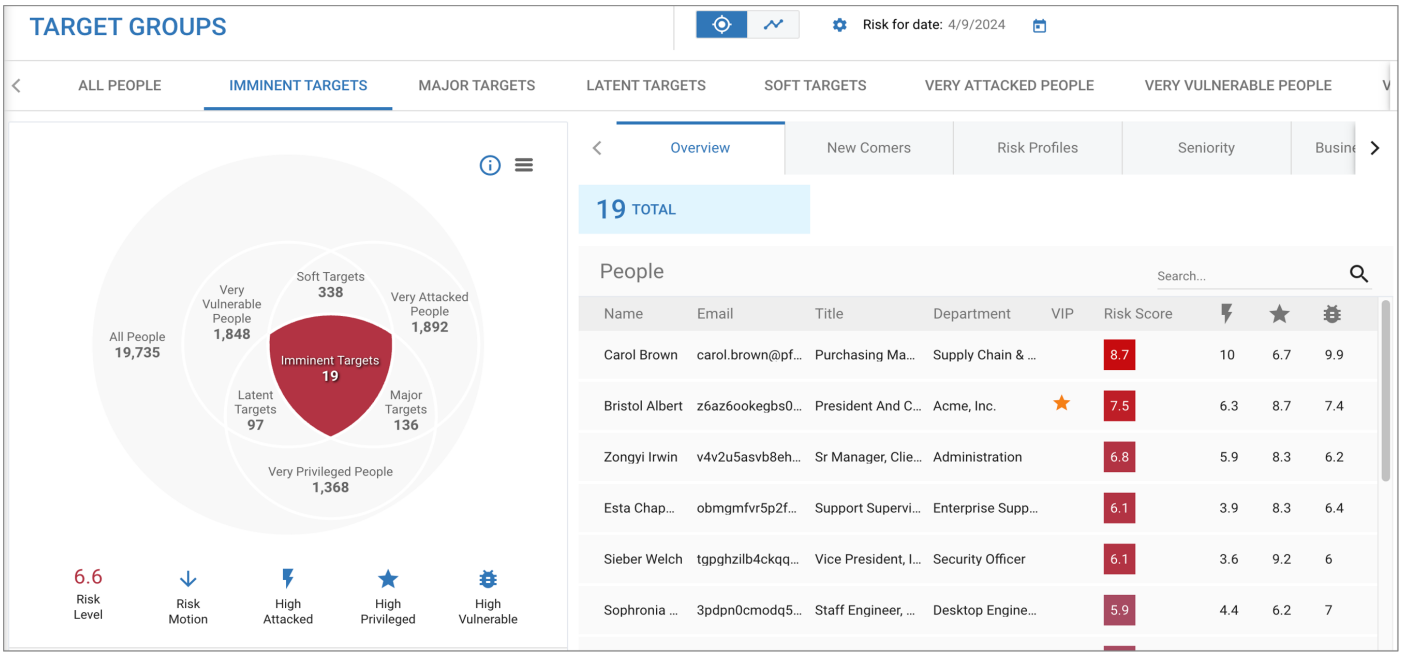

Abb. 1: Proofpoint User Protection identifiziert besonders gefährdete Anwender mit einem Risikowert, der die personenbezogenen Risiken berücksichtigt. Dank der verbesserten Transparenz lassen sich Sicherheitsmaßnahmen priorisieren, adaptive Sicherheitskontrollen anwenden und besonders gefährdete Personen gezielt schulen.

Verbesserte Resilienz gegenüber neuen Bedrohungen

Mit Proofpoint User Protection erhalten Ihre Mitarbeiter nicht nur die erforderlichen Tools und Kenntnisse, sondern sie werden auch dazu motiviert, sich bei dynamischen Social-Engineering-Taktiken resilienter zu verhalten.

Die Lösung nutzt die weltweiten Bedrohungsdaten von Proofpoint, sodass Sie sofortige Einblicke in die hochdynamische Bedrohungslandschaft erhalten und Ihre VAPs und andere Anwender über neue Bedrohungen und Trends in Kenntnis setzen können, etwa in Form von Schulungen, Bedrohungssimulationen und Benachrichtigungen. Dabei können Sie die Schulungen exakt für die jeweilige Rolle, das gezeigte Verhalten und das Risikoprofil der Anwender maßschneidern.

Außerdem können Sie besonders gefährdete Anwender über adaptive Gruppen (Adaptive Groups) und die Pfade-Funktion (Pathways) automatisch bestimmten Kampagnen zuweisen. Auf diese Weise bauen Sie in kürzester Zeit ein effektives Programm zur Verhaltensänderung auf und stellen sicher, dass Ihre Mitarbeiter bei einer Bedrohung die richtige Entscheidung treffen.

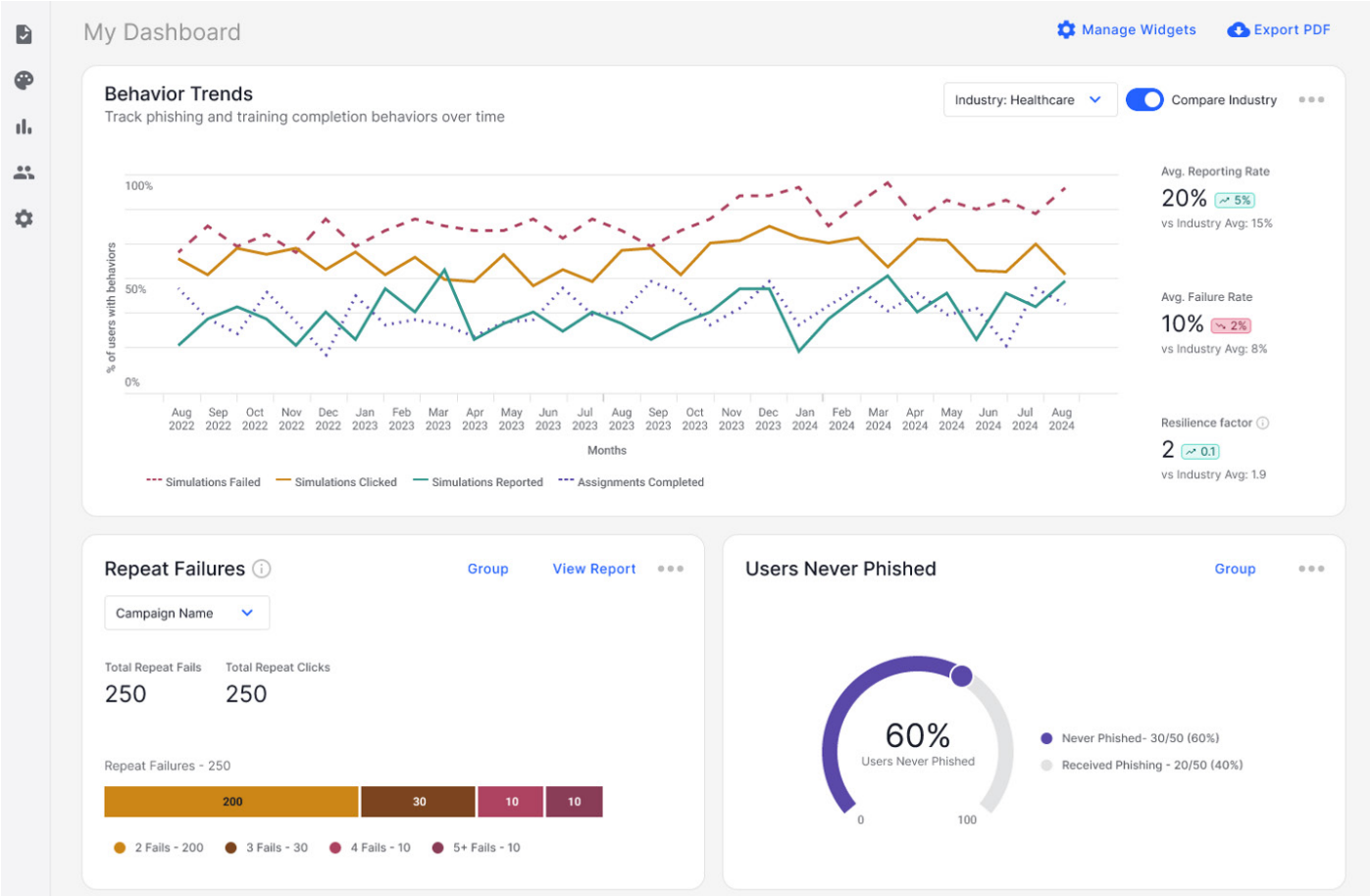

Abb. 2: Proofpoint User Protection nutzt die globalen Bedrohungsdaten von Proofpoint und bietet sofortige Einblicke in die dynamische Bedrohungslandschaft. Schulen Sie Ihre Anwender zu neuen Bedrohungen und erfassen Sie Verhaltenstrends im Zeitverlauf.

Blockierung schädlicher Links auf mehreren Plattformen

Abgesehen von E-Mail nutzen Cyberkriminelle mittlerweile auch weitere digitale Kanäle wie Microsoft Teams, Zoom, Slack, LinkedIn und andere Social-Media-Plattformen. Proofpoint User Protection blockiert auch in all diesen Kanälen schädliche URLs und bietet auf diese Weise erweiterten Schutz.

Dabei nutzt die Lösung unsere Proofpoint Nexus-Plattform, die jedes Jahr mehr als 21 Billionen URLs analysiert. Aufbauend auf diesen Erkenntnissen überprüft Proofpoint User Protection die URL-Reputation und analysiert die URLs im Browser. Wenn ein Mitarbeiter versucht, einen Link in einem Collaboration- und Messaging-Tool aufzurufen, analysiert Proofpoint User Protection die URL in Echtzeit und blockiert sie, falls sie als schädlich erkannt wird. Auf diese Weise sind Ihre Anwender zuverlässig vor schädlichen Websites und Inhalten geschützt.

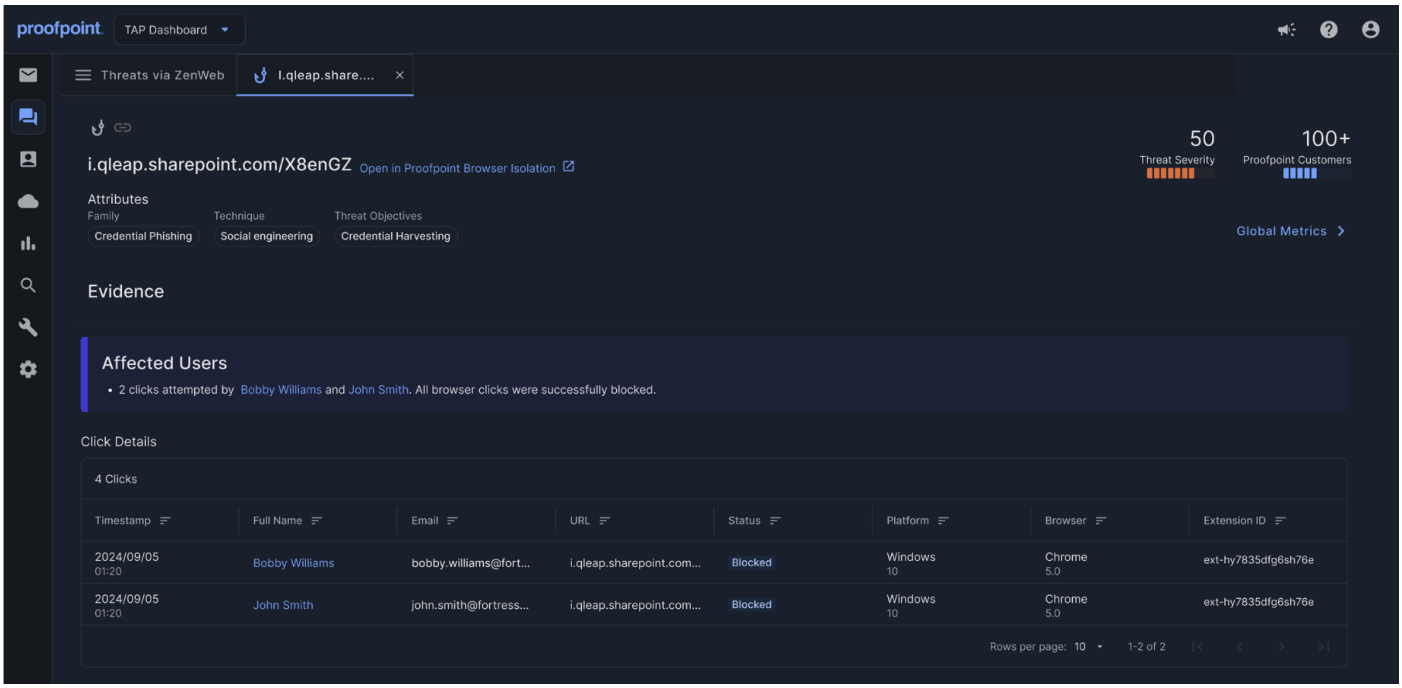

Abb. 3: Proofpoint erweitert den Phishing-Schutz auf Bereiche jenseits von E-Mails und blockiert auch schädliche URLs, die auf Collaboration- und Messaging-Plattformen geteilt werden.

Schnelle Erkennung und Behebung kompromittierter Konten

Sollte es dennoch zu einer Konten-kompromittierung in Microsoft 365, Google Workspace oder Okta kommen, können Sie ganz entspannt bleiben, denn Proofpoint User Protection reagiert auf den Zwischenfall, bevor Schaden entsteht. Mithilfe von KI, Machine Learning, Verhaltensanalyse und den Bedrohungsdaten von Nexus erkennt Proofpoint User Protection verdächtige Aktivitäten in Cloud-Konten und korreliert sie mit E-Mail-Bedrohungen. So lässt sich die betreffende Kontoübernahme genauer bestimmen und rückgängig machen.

Mitbewerberlösungen sind nur begrenzt in der Lage, auf Aktivitäten nach erfolgter Kontoübernahme zu reagieren, während Proofpoint bei einer erkannten Kontoübernahme sofort Reaktionsmaßnahmen ermöglicht. Die unerlaubten Änderungen werden identifiziert und der Zugang der Angreifer unterbunden. Die Lösung erzwingt Kennwortzurücksetzungen, macht Änderungen an Postfach-Regeln und MFA-Einstellungen rückgängig und trennt die Verbindung zu schädlichen Drittanwendungen. Etwaige vom Bedrohungsakteur hochgeladene Dateien werden unter Quarantäne gestellt und entfernt.

Da sich all diese Maßnahmen mit Proofpoint User Protection automatisieren lassen, bleibt Ihnen mehr Zeit, den potenziellen Schaden für Ihr Unternehmen möglichst gering zu halten.

Abb. 4: Proofpoint User Protection gibt Aufschluss über schädliche Aktionen an betroffenen Konten vor und nach dem Zugriff.

Optimieren Sie mit unserem Know-how Ihr Sicherheitsprogramm

Für effektiven Bedrohungsschutz ist Technologie unverzichtbar – doch ein moderner Ansatz muss auch Mitarbeiter und Prozesse berücksichtigen. Mit den richtigen Kompetenzen, optimierten Lösungen und einer starken Sicherheitskultur gelingt es Unternehmen, sich an die dynamische Bedrohungslandschaft anzupassen.

Kombinieren Sie Ihre Proofpoint-Lösungen mit Proofpoint Premium-Services, um Zugang zu einem Expertenteam zu erhalten, das Sie bei der Bereitstellung und Verwaltung einer umfassenden, personenzentrierten Strategie für Bedrohungsschutz unterstützt. Von Beratungen bis zur praktischen Umsetzung hilft Ihnen das Proofpoint Premium-Services-Team, spürbare Sicherheitsverbesserungen zu erreichen und die Wertschöpfung zu beschleunigen.

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.

Verbinden Sie sich mit Proofpoint: X | LinkedIn | Facebook | YouTube

LERNEN SIE DIE PROOFPOINT-PLATTFORM KENNEN →