

Proofpoint Nexus People Risk Explorer

Personenzentrierte Cybersicherheitsrisiken identifizieren, bewerten und beheben

WICHTIGE VORTEILE

- Verständnis der eigenen mitarbeiterbezogenen Sicherheitsrisiken für alle Bedrohungsvektoren und Risikofaktoren
- Optimierte Risikominimierung und Kosteneinsparungen bei der Bereitstellung neuer Sicherheitskontrollen
- Überwachung der Fortschritte und Benchmarking der eigenen personenzentrierten Sicherheitsrisiken mit denen anderer Unternehmen

Mit Proofpoint Nexus People Risk Explorer erhalten Sicherheitsexperten einen Überblick über das Risiko, das Menschen für den Rest des Unternehmens darstellen. Mithilfe dieses Tools können Kunden personenzentrierte Cybersicherheitsrisiken identifizieren, bewerten und beheben.

Unsere Arbeitsweise ändert sich und Cyberbedrohungen passen sich daran an. Gleichzeitig gilt es, neue Compliance-Vorschriften zu beachten. Unverändert sollen Sie jedoch Ihre Mitarbeiter und Ihr Unternehmen vor Sicherheits- und Compliance-Risiken schützen. Ihre Mitarbeiter sollen lokale Systeme und Cloud-Anwendungen sicher nutzen können – unabhängig davon, von welchem physischen Ort aus sie die Verbindung herstellen. Deshalb müssen die Menschen in den Fokus jeder modernen Cybersicherheitsstrategie rücken. Für die Bereitstellung eines personenzentrierten Sicherheitsprogramms benötigen Sie Transparenz, die richtigen Kontrollen und Integrationen.

Der Proofpoint Nexus People Risk Explorer unterstützt Sie dabei. Wir bieten einen einheitlichen Überblick über Ihre mitarbeiterbezogenen Sicherheitsrisiken mit Informationen aus der gesamten Proofpoint-Suite sowie Drittanbieterprodukten.

Mit dem Proofpoint Nexus People Risk Explorer lassen sich die folgenden drei Kernfragen beantworten:

1. Wie muss ich die verschiedenen Bedrohungstypen priorisieren, mit denen meine Mitarbeiter angegriffen werden?
2. Wie kann ich Risiken schneller minimieren, ohne dabei die Geschäftsabläufe zu stören?
3. Wie kann ich meine Sicherheitsinvestitionen begründen und zukünftige Investitionen priorisieren?

Zusätzlich zu den Sicherheitsvorteilen profitieren Sie davon, dass Sie den Verantwortlichen sowie dem Vorstand den Schutz aus Mitarbeiterperspektive täglich verdeutlichen und die Auswirkungen auf das Unternehmen aufzeigen können, ohne dabei technische Kenntnisse voraussetzen zu müssen.

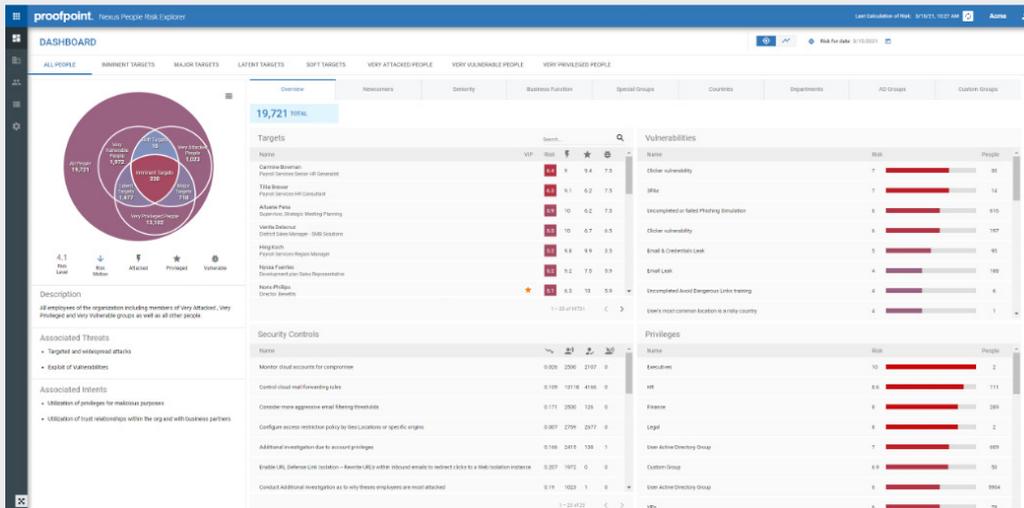


Abb. 1: Die Landing Page von Nexus People Risk Explorer zeigt ein Mengendiagramm sowie eine Liste der Ziele, Schwachstellen und Berechtigungen.

Der Prozess

Die Risikominimierung erfolgt in mehreren Schritten. Im ersten Schritt werden Daten aus den Sicherheitsprodukten in Ihrer Umgebung analysiert und die Bereiche identifiziert, in denen Anwender Ihr Unternehmen gefährden. Anschließend werden Ihre Mitarbeiter entsprechend ihrem Gesamtrisikoprofil segmentiert und geeignete Sicherheitskontrollen für jede Gruppe empfohlen. Durch diesen Schritt können Sie Ihre Ressourcen basierend auf den tatsächlichen Risiken konzentrieren und priorisieren.

Folgende Produkte sind integriert:

- Proofpoint Targeted Attack Protection
- Proofpoint Security Awareness Training
- Proofpoint Cloud Account Defense
- Proofpoint Cloud App Security Broker (CASB)

FAKTOR	ATTRIBUTE	BEDEUTUNG
Wie wird diese Person angegriffen ? (Wahrscheinlichkeit)	Die Person ist das Ziel sehr gezielter, sehr raffinierter oder zahlreicher Attacken.	Dieser Faktor weist darauf hin, dass Angreifer sehr an dieser Person interessiert sind.
Wie stark gefährdet ist diese Person? (Möglichkeit)	Die Person neigt dazu, auf schädliche Inhalte zu klicken, besteht Security-Awareness-Tests nicht oder nutzt riskante Geräte oder Cloud-Dienste.	Dieser Faktor weist darauf hin, dass die Person wahrscheinlich auf einen Angriff hereinfallen würde.
Wie umfassend sind die Zugriffsrechte dieser Person? (Auswirkung)	Die Person kann auf kritische Systeme oder vertrauliche Daten zugreifen und stellt daher für Cyberkriminelle einen hervorragenden Ausgangspunkt für laterale Angriffsbewegungen dar.	Dieser Faktor weist darauf hin, dass eine Kompromittierung der Person großes Schadenspotenzial für das Unternehmen birgt.

Der Risikowert verdeutlicht die Vielfalt und den Schweregrad der Sicherheitsbedrohungen, Schwachstellen in den individuellen Verhaltensweisen und als dritten Faktor die jeweiligen Zugriffsberechtigungen. Damit erhalten Sie ein umfassendes Bild des Risikos, das jede einzelne Person in Ihrem Unternehmen darstellt. Mit diesen Erkenntnissen können Sie die Risiken von Personen einfach vergleichen und Ihre Maßnahmen, Strategien und Budgets entsprechend priorisieren.

Optimierung Ihrer Ressourcen und Technologie-Investitionen

Die Implementierung neuer Sicherheitskontrollen im gesamten Unternehmen ist weder für alle Anwender geeignet noch kosteneffektiv. Wir unterstützen Sie dabei, Ihre Maßnahmen zu priorisieren und neue Kontrollen nur für die Mitarbeiter zu implementieren, die das größte Risiko darstellen. Dazu segmentieren wir Ihre Mitarbeiter entsprechend ihren Abteilungen, Dienstgraden und Risikofaktoren, wobei wir für jedes Segment Behebungsmaßnahmen empfehlen, die auf Ihre individuellen Sicherheitsanforderungen und Richtlinien zugeschnitten sind.

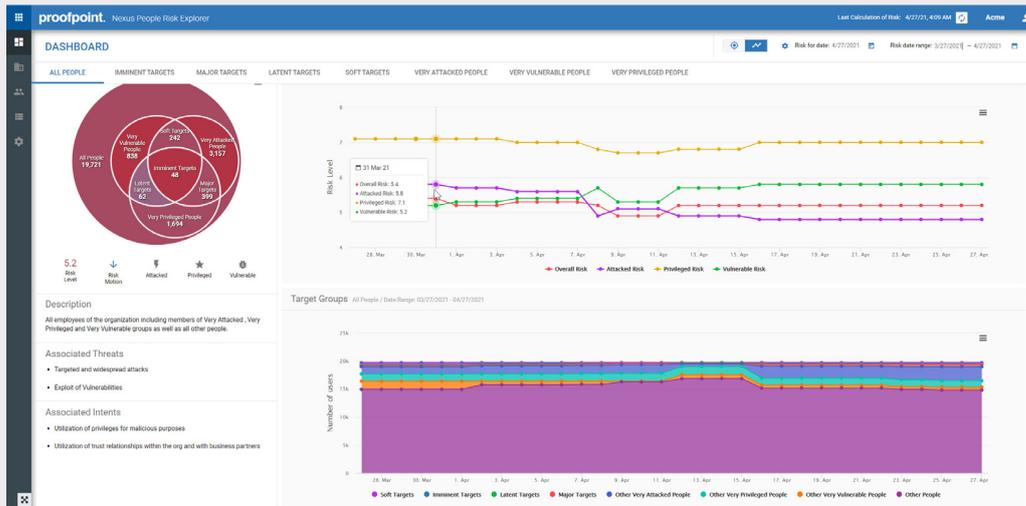


Abb. 2: Nexus People Risk Explorer bietet eine Trendansicht, in der alle Daten in Liniendiagrammen zusammengefasst sind.

Bei der detaillierten Segmentierung werden Personen mit ähnlichen Risikostufen, die die gleichen Kontrollen benötigen, zu Gruppen zusammengefasst. Diese Gruppen machen meist 1–5 % der gesamten Belegschaft aus, sodass sich der Umfang Ihrer Projekte deutlich eingrenzen lässt. Durch die Konzentration auf einen kleinen Teil Ihrer Anwender können Sie die bestehenden Risiken kostengünstiger und effizienter minimieren.

Überwachung der Verbesserungen anhand von Benchmarks

Mit Nexus People Risk Explorer können Sie für einzelne Personen, Gruppen und Ihr Unternehmen als Ganzes täglich personenzentrierte Risikowerte berechnen. Und in der Zukunft können Sie anhand externer Benchmarks vergleichen, wie Ihr Unternehmen abschneidet. Dabei sehen Sie die Ergebnisse anderer Mitarbeiter, Abteilungen, ähnlich großer Unternehmen sowie Ihrer Region.

Außerdem unterstützen wir Ihre Sicherheitsteams dabei, die Veränderung Ihrer personenzentrierten Risiken im Laufe der Zeit zu überwachen. Sie sehen Ihren Fortschritt und können messen, wie effektiv die eingeleiteten Maßnahmen beziehungsweise welche Anpassungen nötig sind.

Mehr erfahren

Im neuen Zeitalter der Cybersicherheit steht der Mensch im Mittelpunkt. Mit Nexus People Risk Explorer erhalten Sie die Transparenz, Kontrollen und Integrationen, die Sie zur Minimierung moderner Bedrohungen und Compliance-Risiken benötigen. Es genügt nicht, die am häufigsten angegriffenen Personen zu kennen. Sie benötigen einen einheitlichen Blick auf mitarbeiterbezogene Risiken sowie angepasste Sicherheitskontrollen für Ihre am stärksten gefährdeten Anwender und müssen Ihren Fortschritt mit Peergroups vergleichen können.

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 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 mehr als die Hälfte der Fortune-1000-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.