

Verringerung des Risikos mit personenzentrierter Sicherheit:

Entdecken Sie eine bessere Strategie, mit der Sie auf den nächsten Cyberangriff vorbereitet sind

Wichtige Vorteile

Transparenz und Kontrolle durch Erkenntnisse zu folgenden Fragen:

- Wie werden Ihre Mitarbeiter angegriffen?
- Mit welchen risikoreichen Methoden arbeiten Ihre Mitarbeiter?
- Wie greifen Ihre Mitarbeiter auf wertvolle Daten zu?

Die heutige Bedrohungslandschaft wird wesentlich von Social Engineering bestimmt. Heutige Angriffe richten sich immer weniger gegen Technologien oder Infrastruktur, sondern verstärkt gegen Menschen. Der Wechsel in die Cloud verschärft das Problem zusätzlich. Proofpoint kann Ihnen einen Überblick verschaffen, Einblicke geben und anpassbare Kontrollen basierend auf Ihrem größten Cybersicherheitsrisiko anwenden: Ihren Mitarbeitern. Dazu gehören nicht nur die einzelnen Personen, sondern auch die Daten, auf die sie Zugriff haben, sowie die Verhaltensweisen, mit denen sie zeigen, dass sie auf einen aktuellen Social-Engineering-Angriff hereinfallen werden.

Angreifer zielen auf Menschen ab

Angreifer sind heute sehr geschickt darin, ihre zielgerichteten Kampagnen gegen Unternehmen mit Internetrecherchen und unter Verwendung von Google und LinkedIn vorzubereiten. Sie nutzen dazu raffiniertere Angriffstaktiken und führen ihre Angriffe in großem Maßstab durch. Die meisten IT- und Cybersicherheitsexperten stützen sich immer noch auf die Absicherung ihres Netzwerks. Durch die digitale Transformation und den damit verbundenen Wechsel zu Remote-Arbeitsplätzen wird die Situation noch komplexer, da die Anwender jenseits der Unternehmensnetzwerke auf Firmendaten zugreifen – und herkömmliche Sicherheitsansätze bieten hier nicht den gleichen Schutz. Deshalb sehen die Angreifer die Welt nicht als Netzwerkdiagramm. Hinzu kommt, dass die Zunahme von Cloud-Anwendungen und Plattformen wie Microsoft 365 und Google Workspace den auf das Netzwerk ausgerichteten Schutzansatz an seine Grenzen treibt. Cloud-Anwendungen enthalten wertvolle Unternehmensinformationen, die im Internet übertragen werden, ohne dabei Firewalls und andere Netzwerkkontrollen zu passieren. Dadurch ist es schwierig, einen Überblick über alle gegen Mitarbeiter gerichteten Bedrohungstypen zu erhalten und Warnungen sowie Zwischenfälle entsprechend ihres relativen Risikos für das Unternehmen zu priorisieren.

Quantifizieren des Risikos mit dem Proofpoint Attack Index

Eine mögliche Kennzahl für die Quantifizierung des personenbasierten Risikos ist der Proofpoint Attack Index. Mit dem Proofpoint Attack Index können Sie gezielt angegriffene Personen identifizieren und zwischen den vielzähligen alltäglichen Bedrohungsaktivitäten relevante Bedrohungen aufdecken. Beim Attack Index handelt es sich um eine gewichtete zusammengefasste Bewertung aller Bedrohungen, die an eine Person im Unternehmen gesendet wird. Er basiert auf vier wichtigen Faktoren:

- **Angriffsaufkommen:** Wie hoch ist die Zahl der Angriffe?
- **Art des Angriffs:** Welche Art von Malware wird verwendet? Dabei wird berücksichtigt, wie gefährlich eine Bedrohung ist und wie viel Aufwand in den Angriff gesteckt wurde. So würden zum Beispiel ein Remote-Zugriffs-Trojaner (RAT) oder ein Informationsdieb eine höhere Punktzahl erhalten als eine simple Phishing-Aktion.
- **Angriffsziele:** Wie stark gezielt erfolgt der Angriff? War der Angriff auf einen Nutzer zugeschnitten oder wurde er auf breiter Front ausgerollt? War der Angriff auf einen bestimmten Anwender bzw. eine bestimmte Firma, Branche oder Region gerichtet? Oder handelte es sich um eine volle Breitseite, die um die halbe Welt ging? Je zielgerichteter ein Angriff, desto höher die Punktzahl.
- **Raffinesse des Akteurs:** Wie raffiniert geht der Angreifer vor? So würde zum Beispiel ein Akteur, der als hochentwickelte permanente Bedrohung (Advanced Persistent Threat, APT) eingestuft wird, eine höhere Punktzahl erhalten als ein Kleinkrimineller.

Mithilfe des Angriffsindex können Sie das Risiko einzelner Personen oder aller Mitarbeiter bewerten und dokumentieren und anschließend die effektivste Möglichkeit zur Beseitigung dieser Bedrohungen auswählen.

Bewertung Ihrer menschlichen Angriffsfläche

Durch die Konzentration auf Bedrohungen, die Menschen ins Visier nehmen und sie ausnutzen, kann Proofpoint Ihnen bei der Verringerung Ihrer Sicherheitsrisiken helfen. Dies beginnt bei Ihren besonders häufig angegriffenen Personen – den Very Attacked People (VAPs). Doch die Identifizierung der VAPs ist nur der erste Schritt. Anschließend müssen Sie sich einen Überblick über das Risiko verschaffen, das die einzelnen VAPs darstellen. Da dieses Risiko durch mehrere Faktoren bestimmt wird, unterstützt Proofpoint Sie strategisch mit dem Nexus People Risk Explorer, der folgende Informationen liefert:

- **Welche riskanten Vorgehensweisen zeigen Ihre Mitarbeiter?** Klicken sie häufiger absichtlich oder versehentlich auf schädliche Links bzw. Anhänge oder nutzen sie risikoreiche Anwendungen?
- **Wie werden Ihre Mitarbeiter angegriffen?** Sind Ihre Mitarbeiter das Ziel sehr gezielter, sehr raffinierter oder zahlreicher Angriffe?
- **Wie greifen Ihre Mitarbeiter auf wertvolle Daten zu?** Wenn sie vertrauliche Systeme oder Daten nutzen bzw. verwalten, können sie eher Gefahr laufen, Daten über geschäftskritische Systeme oder Drittanbieter-Apps falsch zu verwenden, zu verlieren oder zu kompromittieren.

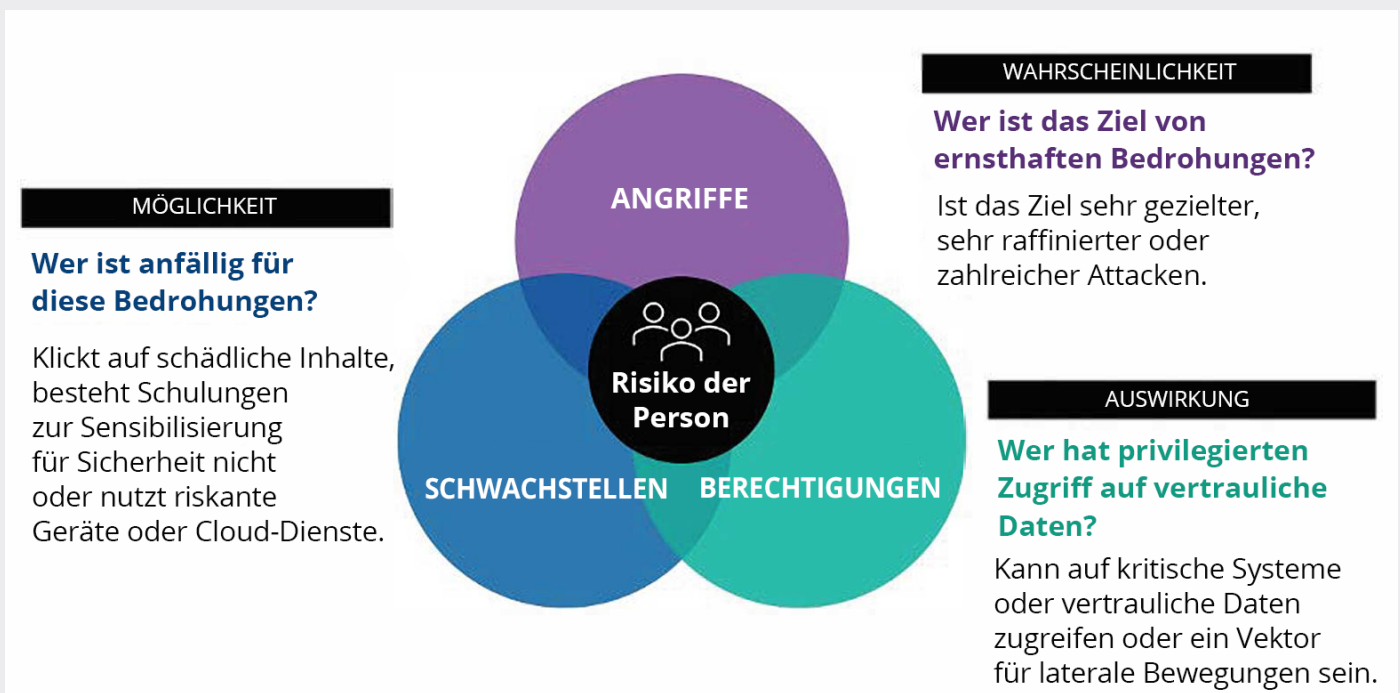


Abb. 1: So sieht Proofpoint die Faktoren, die das Risiko ausmachen.

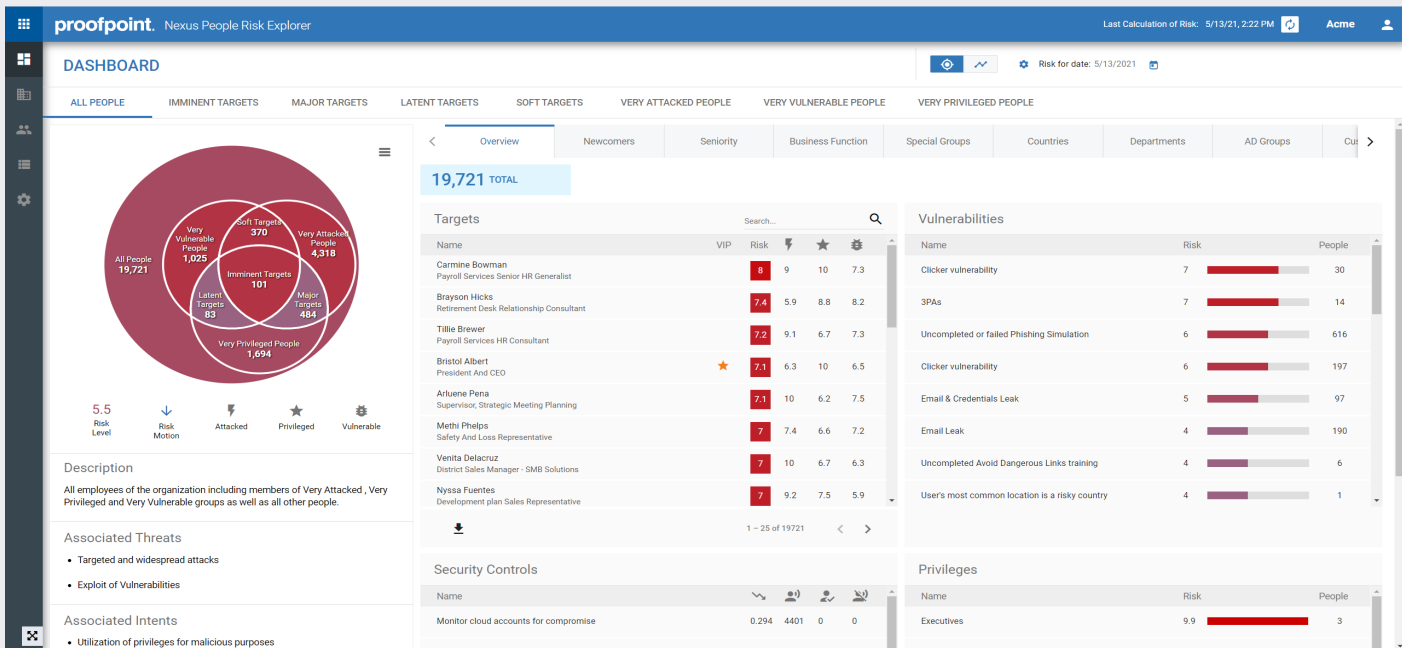


Abb. 2: Startbildschirm des Nexus People Risk Explorer-Dashboards mit Informationen zum Risiko Ihrer Mitarbeiter.

Implementierung eines personenzentrierten Sicherheitsansatzes

Proofpoint bietet Lösungen an, die Ihr Unternehmen beim Aufbau stärkerer personenzentrierter Sicherheitsmaßnahmen unterstützen.

Schutz Ihres wichtigsten Bedrohungsvektors und Erkenntnisse zu Ihren VAPs

Beginnen Sie mit der Abwehr von E-Mail-Bedrohungen in der gesamten Angriffskette – von der Erkennung bis zur Reaktion. Erfahren Sie, wer wie angegriffen wird, ob diese Personen auf Phishing-Köder klicken, solche E-Mails melden oder kompromittiert wurden.

Erweiterung Ihrer personenzentrierten Schutzmaßnahmen und grundlegender Schutz für Cloud-Konten

Schützen Sie sich vor Bedrohungen und Datenverlusten in allen personenzentrierten Bedrohungsvektoren, darunter externe und interne E-Mails, Cloud-Konten und private Webmails. Mit den Schulungen werden Ihre Mitarbeiter zu Ihrer letzten Verteidigungslinie. Geben Sie ihnen die Mittel in die Hand, um Phishing-Angriffe zu erkennen sowie zu melden, und schulen Sie sie zu bewährten Methoden für den Schutz ihrer Identitäten, Anmeldedaten und Daten.

Aufbau eines umfassenden personenzentrierten Sicherheitsprogramms

Weiten Sie Ihren Schutz noch stärker aus, sodass er die gesamte menschliche Angriffsfläche abdeckt, einschließlich Ihres Geschäftsökosystems. Stellen Sie sicher, dass die Menschen, mit denen Sie zu tun haben, das Unternehmen nicht gefährden. Integrieren Sie zudem Ihr Sicherheitsökosystem, damit Sie Ihre vorhandenen Investitionen optimal nutzen können. Schützen Sie Ihre VAPs mit stärker integrierten, adaptiven Kontrollen und Quarantänefunktionen.

WEITERE INFORMATIONEN

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