proofpoint.

E-BOOK

So messen Sie den langfristigen Erfolg von Schulungen zur Sensibilisierung für Sicherheit

Ein Leitfaden für CISOs und IT-Führungskräfte

proofpoint.com/de

Einführung

Für IT- und Sicherheitsverantwortliche war der Anfang dieses Jahrzehnts eine turbulente Zeit voller Herausforderungen und Veränderungen. Das Jahr 2020 war geprägt von hektischen Bemühungen, aufgrund des Pandemie-Lockdowns sichere Verbindungen für die Belegschaft im Homeoffice herzustellen, sowie einem sprunghaften Anstieg von Phishing-Angriffen, mit denen Angreifer das Chaos ausnutzten. Doch das war nur der Anfang einer neuen beängstigenden Ära der Cyberbedrohungen.

In einer aktuellen Umfrage unter Tech-Experten gaben 57 % an, dass ihr Unternehmen 2020 einen erfolgreichen Phishing-Angriff verzeichnete – im Vorjahr waren es noch 55 %.[2] Und in ähnlicher Weise geht es weiter: Eine zunehmende Zahl medienwirksamer Ransomware-Angriffe und Datenschutzverletzungen zwingt Unternehmen momentan dazu, ihre Risikobereitschaft zu überdenken.

Kompromittierungen haben für die Opfer unangenehme Folgen. Bei den Verantwortlichen und beim Vorstand können sie jedoch auch dringend erforderliche Diskussionen über Cybersicherheit und die Rolle von Anwendern bei der Sicherheit des Unternehmens auslösen.

Die meisten Bedrohungen müssen erst durch einen Menschen aktiviert werden. Deshalb können effektive Programme zur Sensibilisierung für Sicherheit – und Veränderungen des Anwenderverhaltens – die bestehenden Risiken maßgeblich verringern.[3] Viele Sicherheitsverantwortliche sind sich dessen grundsätzlich bewusst. Allerdings ist es nicht immer ganz einfach, die Effekte solcher Programme auch auszuwerten und die Ergebnisse an die Führungskräfte zu kommunizieren.

In diesem E-Book werden die langfristig angelegten Programme zur Sensibilisierung für Sicherheit im Detail untersucht. Wir zeigen Strategien auf, mit denen Sie bei Führungskräften die Akzeptanz und Unterstützung für diese Maßnahmen erreichen, auswerten und fördern können. Zudem erfahren Sie, wie Sie diese wichtige Investition optimal nutzen.

85 %

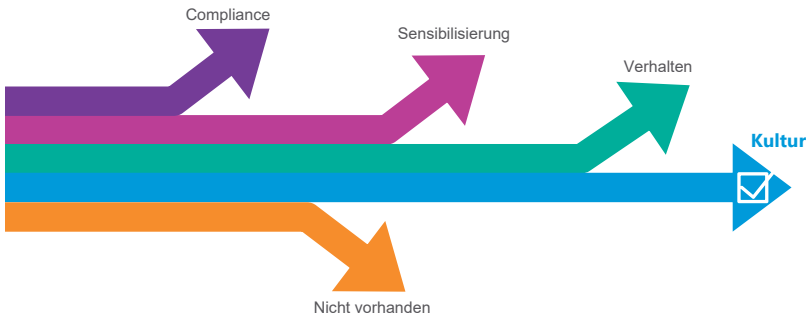
der US-amerikanischen CFOs gaben an, dass in ihren Vorständen die neuesten Cybersicherheitsangriffe und deren Folgen offiziell besprochen werden.[1]

[1] CNBC: „CNBC Global CFO Council Survey“ (Weltweite Umfrage unter CFOs), Juli 2021.
[2] Proofpoint: „State of the Phish 2021“, Februar 2021.
[3] Proofpoint: „Schutz der Anwender“, Februar 2019.

Der aktuelle Stand der Sensibilisierung für Sicherheit

Das Sicherheitsbewusstsein nimmt bei der Finanzplanung häufig einen niedrigeren Stellenwert ein als technische Kontrollen. Das muss jedoch nicht so sein: Mit überzeugenden Kennzahlen und einer wirksamen Darstellung können Sie zwei wichtige Ziele erreichen. Zunächst lassen sich damit ganz konkret Risiken verringern. Außerdem können Sie den CISOs und anderen Verantwortlichen veranschaulichen, warum das Sicherheitsbewusstsein für die Sicherheit des Unternehmens so wichtig ist.

Die Bedenken der oberen Managementebene hängen vom Zustand und den Zielen des bestehenden Sicherheitsprogramms ab. Bei Compliance-Programmen beispielsweise steht vor allem das Abhaken von Checklisten-Features zur Einhaltung von Vorschriften im Vordergrund. Verhaltensbasierte Programme bewerten den Erfolg dagegen anhand von Kennzahlen wie der Klick- und Meldungsrate in Phishing-Simulationen.



Reifegrade von Programmen zur Sensibilisierung für Sicherheit

So bauen Sie eine Sicherheitskultur auf

Die meisten Unternehmen (98 %) verfügen über ein Programm zur Sensibilisierung für Sicherheit.[4] Doch 64 % von ihnen führen nur formelle Schulungen (entweder persönlich oder virtuell) durch und nutzen keine anderen Möglichkeiten zur Förderung des Sicherheitsbewusstseins. Lediglich 23 % nutzen eine bunte Mischung aller verfügbaren Bewertungs-, Schulungs- und Kommunikationsmedien.

Eine kontinuierliche Interaktion über verschiedene Kanäle trägt dazu bei, das Gelernte auch zu behalten und das Sicherheitsbewusstsein zu steigern. Deshalb empfehlen wir dringend, so viele Kanäle wie möglich zu verwenden.

Ein zentrales Element zur Steigerung des Sicherheitsbewusstseins ist der Aufbau einer Kultur, in der die Anwender davon überzeugt sind, dass nicht nur das Unternehmen von einer hohen Sicherheit profitiert, sondern auch sie persönlich. Dies lässt sich bewerkstelligen, indem Sie Aktivitäten kombinieren, die das Bewusstsein fördern, Verhalten ändern und ein Gefühl der Verantwortung für den „Kampf gegen Übeltäter“ zum Wohle aller erzeugen. Dazu sollten die Schulungen für Anwender relevant und hilfreich sein – und zwar kontinuierlich, nicht nur ein oder zwei Mal im Jahr.

Aktuelle Ansätze zur Förderung des Sicherheitsbewusstseins:[5]

29 %
verwenden ausschließlich simulierte Phishing-Tests

41 %
verwenden ausschließlich formelle Schulungen

7 %
verwenden ausschließlich Informationsinhalte

23 %
verwenden Kombination aus verschiedenen Inhaltstypen

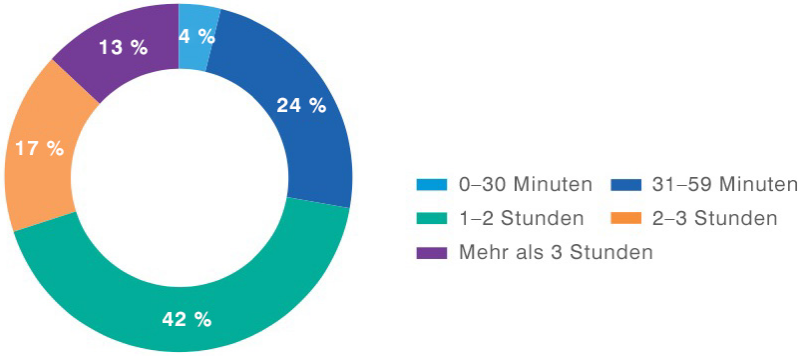
[4] Proofpoint: „State of the Phish 2021“, Februar 2021.
[5] ebd.

Implementieren eines wirkungsvollen Programms

Je mehr Zeit ein Unternehmen in die Förderung des Sicherheitsbewusstseins investiert, desto größer sind die Erfolgschancen.

Zeit, die Unternehmen in Sicherheitsbewusstsein investieren

Die meisten Unternehmen wenden im Jahr weniger als zwei Stunden je Anwender für Schulungen auf.



Jedes Jahr gibt es immer mehr Unternehmen, die die Häufigkeit der Sensibilisierungsmaßnahmen erhöhen.

Konzentrieren Sie sich auf anfällige Anwender

Wenn Sie versuchen, Ihr Programm zur Sensibilisierung für Sicherheit auszuweiten, stoßen Sie in einigen Fällen möglicherweise auf Widerstand. Eventuell wird befürchtet, dass das Programm zu viele Anwender belastet, und zwar besonders die, die kein erhöhtes Risiko darstellen.

Wenn Sie sich auf anfällige Anwender in kleineren Zeitabständen konzentrieren, anstatt nach dem Gießkannenprinzip alle Mitarbeiter zu schulen, können diese Bedenken ausgeräumt werden. Durch einen zielgerichteten Ansatz wird den Verantwortlichen bewusst, dass es einen guten Grund für zusätzliche Schulungen und Sensibilisierungsmaßnahmen gibt. Zudem erkennen die Anwender, warum sie geschult werden.

Andere Entscheidungsträger machen sich gegebenenfalls weniger Sorgen um die Zahl der betroffenen Mitarbeiter, sondern um die Zeit, die für Schulungen erforderlich ist. Zum Glück gibt es Sensibilisierungsmaßnahmen, die Anwender nicht unnötig belasten.

Newsletter, Betriebsversammlungen, Wiki-Seiten und E-Mail-Benachrichtigungen sind zeitsparende Sensibilisierungsmaßnahmen.

Kennen Sie Ihre am meisten gefährdeten Anwender?

Bei Proofpoint beschreiben wir mit dem Begriff Very Attacked People™ (VAPs) die Anwender, die von Cyberangreifern außergewöhnlich häufig ins Visier genommen werden. Dies kann umfangreiche Attacken, gezielte Bedrohungen und hochentwickelte Taktiken umfassen – oder alles zusammen. Obwohl alle Anwender ein potenzielles Ziel darstellen, sind VAPs aufgrund ihrer spezifischen beruflichen Kontakte und der privilegierten Zugänge zu Daten, Systemen und anderen Ressourcen besonders wertvoll.

VAPs werden
3 bis 12 Mal
häufiger als andere Anwender attackiert

Unserer Erfahrung nach sind die VAPs eines Unternehmens nicht immer VIPs wie beispielsweise leitende Führungskräfte, sondern sie befinden sich mitunter in der Personal-, Presse-, Marketing- oder Forschungsabteilung. Jeder, der über relevante Zugangsberechtigungen verfügt, stellt ein wertvolles Ziel dar.

Sind Ihre VAPs einmal identifiziert, sollten Sie die Lücken im Sicherheitswissen mit äußerst gezielten Schulungen schließen. Beispielsweise können Sie VAPs, die Ziel von Anmeldedaten-Phishing sind, simulierte Phishing-Angriffe schicken. Sollten sie auf die Simulation hereinfallen, bieten Sie zusätzliche Schulungen an. Auf diese Weise lassen sich personenbasierte Risiken gezielt und ohne unnötigen Zeitaufwand verringern.

Sicherheitsbewusstsein lässt sich nicht mit einer einmaligen Maßnahme steigern. Ihre Anwender müssen mit umfassenden kontinuierlichen Schulungen, die auf aktuelle, für sie relevante Cyberbedrohungen zugeschnitten sind, sensibilisiert werden. Zu diesem Prozess gehört Folgendes:

- Regelmäßige Bewertungen
- Schulungen
- Aktivitäten zur Festigung
- Auswertung

Um auf Kurs zu bleiben und die Verantwortlichen zu überzeugen, sollten Sie einen Plan erstellen, der die Aktivitäten, Kanäle, Mitteilungen und Themen Ihres Programms festlegt.

Bewertung des Sicherheitsbewusstseins

Viele Programme messen den Erfolg allein an den abgeschlossenen Schulungen (für Compliance) und der Fehlerquote bei simulierten Angriffen. Doch um das Anwenderverhalten nachhaltig zu verändern und Risiken zu verringern, benötigen Sie noch weitere Informationen, zum Beispiel umfassendere Anwenderrisiko-Profile. Die folgenden Kennzahlen helfen Ihnen, die realen Auswirkungen Ihrer Maßnahmen zu quantifizieren:

Meldungsrate bei Simulationen

Diese Kennzahl gibt einen Überblick darüber, wie gut Endnutzer böswillige Nachrichten meiden, vor allem aber auch ob sie richtig handeln. Das heißt, sie müssen ihr in den Schulungen gelerntes Wissen anwenden, wenn sie etwas Verdächtiges sehen.

Reale Klickrate

Mit Proofpoint-Lösungen für erweiterte E-Mail-Sicherheit können Sie die Klickrate für unsichere Inhalte sehen, auch wenn die URL aus Sicherheitsgründen blockiert oder umgeschrieben wurde. Diese Kennzahl deckt das Anwenderwissen in der Praxis auf. Anhand dieser Daten können Sie nachvollziehen, ob sich Ihre Anwender beim Aufspüren tatsächlich unsicherer Inhalte verbessern.

Gemeldete Nachrichtentypen

Mithilfe eines E-Mail-Add-ins können Anwender verdächtige schädliche Inhalte melden – ähnlich wie bei einem Abuse-Postfach. Proofpoint Targeted Attack Protection (TAP) zeigt Ihnen, wie verschiedene E-Mail-Typen klassifiziert wurden (z. B. schädlich, Spam, geringes Risiko). Damit können Sie erkennen, ob Anwender im Laufe der Zeit besser darin werden, potenziell schädliche Nachrichten zu melden.

Reale Auswirkungen

Dies ist die wichtigste aller Kennzahlen. Die Kennzahl „Reale Auswirkungen“ verfolgt, was Anwender tatsächlich tun, also ob es wirklich weniger erfolgreiche Phishing-Angriffe, Anmeldedaten-Kompromittierungen, Insider-Zwischenfälle und Malware-Angriffe gibt. Das ist der ultimative Maßstab für Kompetenz und der Schlüssel für eine dauerhafte Unterstützung von Programmen zur Sensibilisierung für Sicherheit.

Antwort auf die Frage: Wo sollte unsere Klick- und Meldungsrate liegen?

Proofpoint-Empfehlungen:

<5 %
Fehlerquote/ Klickrate

>70 %
Meldungsrate

Effektive Kommunikation mit dem CISO und wichtigen Verantwortlichen

Bei Berichten an die Führungsebene sollten Angst, Unsicherheit und Zweifel nur begrenzt eingesetzt werden. Richtig ist: Cyberbedrohungen müssen abgewehrt werden. Doch wenn Sie zu viel Angst schüren und Bedrohungen aufbauschen, besteht die Gefahr, dass Sie irgendwann unglaubwürdig wirken und dadurch Schaden anrichten.

So kommunizieren Sie die Effektivität der Sensibilisierungsmaßnahmen

Quantitativ

Kontext ist wichtig. Die Mitarbeiter sollten wissen, wie gut die allgemeine Effektivität ist und wie sie untereinander abschneiden. Konzentrieren Sie sich beim Vergleich der Kollegen auf positive statt negative Kennzahlen wie die Simulations-Klickrate.

Beispiele für positive Kennzahlen:

- Steigerung der Anwender-Meldungsraten für simulierte Phishing-Angriffe
- Verbesserungen bei Wissenstests zum Sicherheitsbewusstsein
- Höhere Genauigkeit der von Anwendern gemeldeten, wirklich schädlichen Nachrichten
- Höhere Beteiligungsquoten von Anwendern bei Sensibilisierungsmaßnahmen

Qualitativ

Mit Daten angereicherte Storys verdeutlichen, dass Sensibilisierung mehr ist als eine vorgeschriebene Compliance-Maßnahme. Damit können Sie zeigen, dass sich das Verhalten der Anwender ändert, dass sich die Kultur mit zunehmendem Verständnis für die Risiken wandelt und dass diese Maßnahmen den Schutz des Unternehmens verbessern.

Beispiele für Storys:

- Ein Anwender hat einen realen hochentwickelten Phishing-Angriff gestoppt
- In einer Feedback-Umfrage äußern sich Anwender positiv über das Sensibilisierungsprogramm
- Eine Führungskraft oder eine bekannte Person erzählt der Belegschaft etwas über Sicherheitsbewusstsein

Übersicht über das Sicherheitsbewusstsein in einem Dashboard

Die Steigerung des Sicherheitsbewusstseins ist eine der wichtigsten Maßnahmen zum Schutz Ihres Unternehmens. Das ist einer der Gründe, warum wir ein CISO-Dashboard für Proofpoint Security Awareness entwickelt haben. Mit diesem Dashboard haben IT- und Sicherheitsteams Zugang zu Kennzahlen dazu, wie Sicherheitsprogramme Verhaltensweisen verändern und die Sicherheitskultur fördern. Anhand dieser Maßstäbe für Erfolg lässt sich die Rendite – ein Argument für zukünftige Investitionen – sehr viel einfacher verdeutlichen.

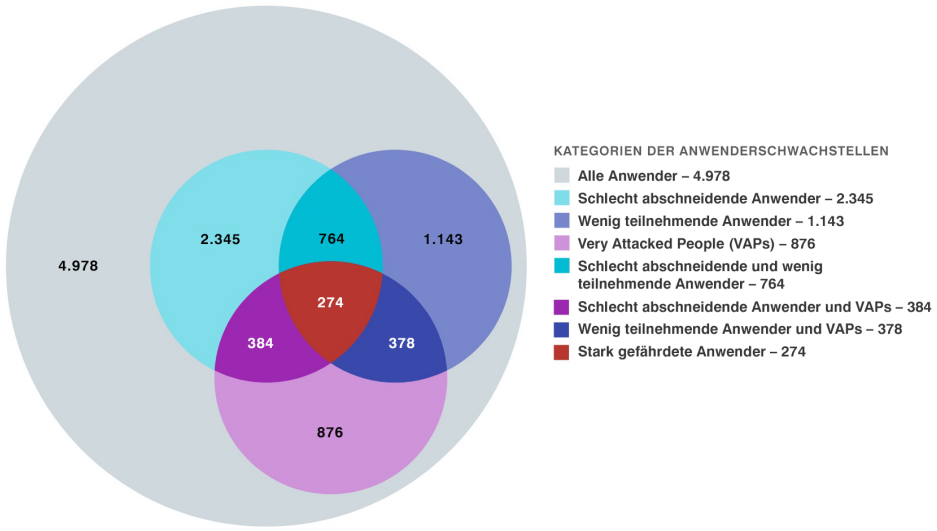
Mit dem Proofpoint CISO-Dashboard haben Sie Zugang zu Kennzahlen wie Anwenderschwachstellen und Ihre Sicherheitsprogramm-Bewertung.

Anwenderschwachstellen

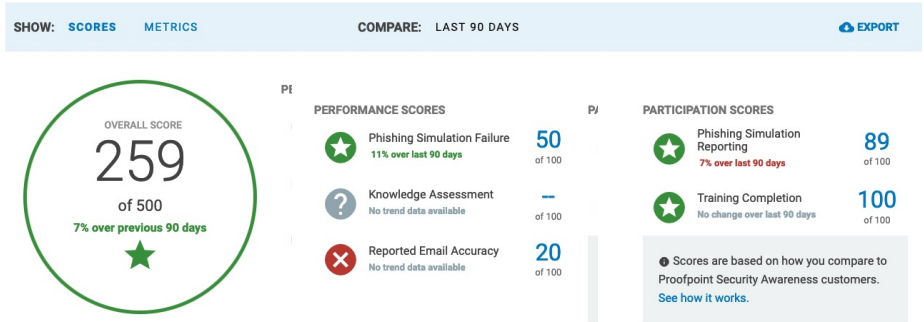
Sie erhalten eine Übersicht der Anwender mit schlechten Ergebnissen und solcher, die auf echte schädliche Nachrichten klicken. Sind Anwender in Proofpoint Targeted Attack Protection als VAP eingestuft, werden diese Daten integriert, sodass Sie einen besseren Überblick über das gesamte Risikoprofil eines Anwenders erhalten.

Sicherheitsprogramm-Bewertung

Die Ergebnis- und Beteiligungsbewertung zeigt, wie gut Ihr Unternehmen in jedem Bereich abgeschnitten hat und wie sich die allgemeine Bewertung verändert hat. Durch Symbole in Ampelfarben können Sie auf einen Blick erkennen, wo Sie in jedem Bereich stehen und wo es Verbesserungspotenzial gibt.



Die Zusammenfassung der Anwenderschwachstellen im CISO-Dashboard



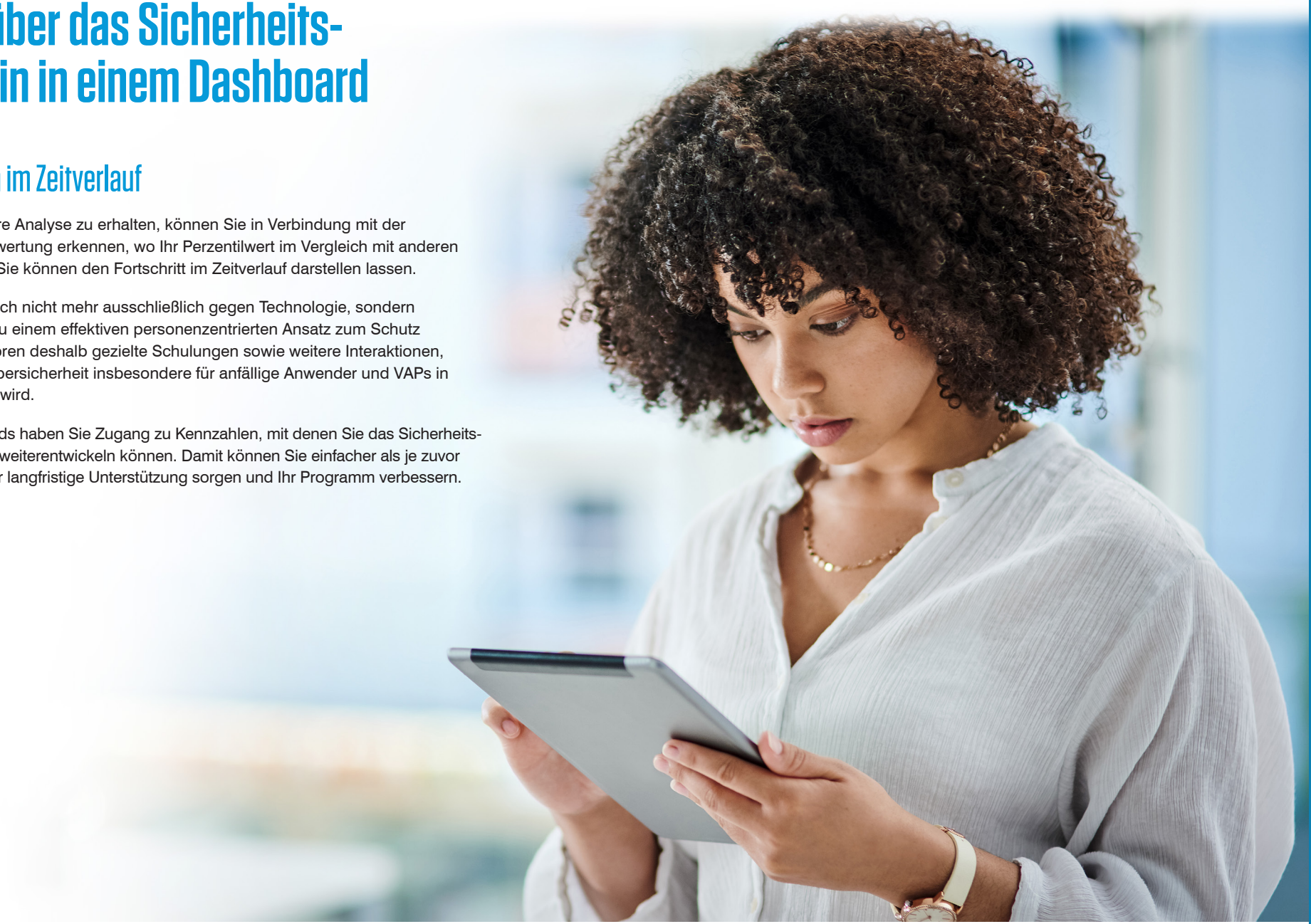
Übersicht über das Sicherheits-bewusstsein in einem Dashboard

Perzentil-Vergleich im Zeitverlauf

Um eine Grundlage für Ihre Analyse zu erhalten, können Sie in Verbindung mit der Sicherheitsprogramm-Bewertung erkennen, wo Ihr Perzentilwert im Vergleich mit anderen Branchenvertretern liegt. Sie können den Fortschritt im Zeitverlauf darstellen lassen.

Heutige Angriffe richten sich nicht mehr ausschließlich gegen Technologie, sondern auch gegen Menschen. Zu einem effektiven personenzentrierten Ansatz zum Schutz Ihres Unternehmens gehören deshalb gezielte Schulungen sowie weitere Interaktionen, mit denen das Thema Cybersicherheit insbesondere für anfällige Anwender und VAPs in den Vordergrund gerückt wird.

Dank des CISO-Dashboards haben Sie Zugang zu Kennzahlen, mit denen Sie das Sicherheits-bewusstsein steigern und weiterentwickeln können. Damit können Sie einfacher als je zuvor Ihren CISO informieren, für langfristige Unterstützung sorgen und Ihr Programm verbessern.



Weitere Informationen dazu, wie Proofpoint Sie dabei unterstützen kann, das Verhalten Ihrer Anwender zu verändern und Cybersicherheit zum Kernelement Ihrer Unternehmenskultur zu machen, finden Sie unter proofpoint.com/de.

INFORMATIONEN ZU 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 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.

0504-002-01-01 09/21