„Es gibt keinen Weg zurück. Die Zukunft könnte genauso beispiellos sein wie die Vergangenheit."
(Chester Wisniewski, Principal Research Scientist, Sophos)

Gute Nachricht für die Cybersecurity: IT-Teams gehen weltweit gestärkt aus dem Pandemiejahr hervor

Sophos-Studie beleuchtet Auswirkungen der Herausforderungen in 2020 auf IT-Teams:

- *61 Prozent der weltweiten und 64 Prozent der deutschen IT-Teams bestätigen mehr Cyberattacken auf ihre Organisation im Jahr 2020*
- *82 Prozent aller befragten Teams fühlen sich heute besser gegen Cyberbedrohungen gerüstet*
- *52 Prozent weltweit und 42 Prozent in Deutschland sagen, dass das Krisenjahr gut war für die Team-Moral*

Wiesbaden, 10. Juni 2021 – Sophos hat in seiner Studie "The IT Security Team: 2021 and Beyond" die Auswirkungen der pandemiebedingt erhöhten Sicherheitsherausforderungen auf IT-Teams in den unterschiedlichen Regionen der Welt beleuchtet. Für die Umfrage wurden 5.400 IT-Entscheidungsträger in mittelständischen Unternehmen in 30 Ländern in Europa, Nord- und Südamerika, Asien-Pazifik und Zentralasien, dem Nahen Osten und Afrika befragt.

Gut für die Expertise, gut für die Moral
Die Zunahme von Cyberangriffen während der Pandemie wirkte sich laut der Studie positiv auf das Wissen und die Security-Fähigkeiten von IT-Teams aus. Alle, die sich im Laufe des Jahres 2020 mit einer Zunahme von Cyberangriffen und einem höheren Sicherheitsaufkommen konfrontiert sahen, und dies waren 82 Prozent, bestätigen ihre Sicherheitsfähigkeiten und -kenntnisse ausgebaut zu haben.
Trotz der stärkeren Herausforderungen stellten 52 Prozent aller befragten und immerhin 42 Prozent der deutschen IT-Teams für 2020 zudem sogar eine gesteigerte Team-Moral und besseres Teamplay fest.

„Das Jahr 2020 war außergewöhnlich für IT-Teams“, sagt Chester Wisniewski, Principal Research Scientist bei Sophos. „Sie haben dafür gesorgt, dass so schnell wie möglich mobile Heimarbeit, digitale Sprechstunden, Online-Shopping-Services, digitale Behördengänge, oder Lernen von zuhause realisiert werden konnten. Sie haben sichergestellt, dass trotz Lockdown der Geschäftsbetrieb am Laufen blieb. Vieles davon in kürzester Zeit, mit begrenzter Ausrüstung und knappen Ressourcen und vor dem Hintergrund einer steigenden Flut von Cyberangriffen auf das Netzwerk, die Endpunkte und die Mitarbeiter.“

Und dies hatte seinen Effekt: Insgesamt fühlen sich 82 Prozent der befragten IT-Profis aus 30 Ländern durch 2020 besser gerüstet für die Herausforderungen der Zukunft.

Die wichtigsten Studienergebnisse im Überblick:

- **Die Anforderungen an die IT-Teams sind gestiegen.** Die gesamte IT-Arbeitslast (ohne Sicherheit) stieg für 63 Prozent (Deutschland 62 Prozent) der IT-Teams, während 69 Prozent (Deutschland 74 Prozent) einen Anstieg der Arbeitslast im Bereich Cybersecurity verzeichneten.

- **Angreifer nutzten die Chancen, die sich durch die Pandemie boten**: 61 Prozent aller befragten und 64 Prozent der deutschen IT-Teams berichteten von einem Anstieg der Cyberangriffe auf ihre Organisation im Laufe des Jahres 2020.

- **Die höhere Zahl von Cyberangriffen bot IT-Teams die Möglichkeit, ihre Fähigkeiten und Kenntnisse in der Cybersecurity auszubauen**. Vieles in dieser Entwicklung basiert auf „Learning by doing“ anhand neuer Technologien und Sicherheitsanforderungen, oft unter großem Druck und fernab vom normalen Arbeitsplatz.

- **Die Bewältigung der Herausforderungen stärkte die Moral**. Mehr als die Hälfte (52 Prozent) bestätigten eine Stärkung der Team-Moral im Laufe des Jahres 2020, für Deutschland lag diese Zahl mit 42 Prozent etwas darunter. In vielen Fällen schien dieser Faktor mit einer Intensivierung von Arbeitsbelastung und Angriffen einherzugehen. So war die Wahrscheinlichkeit, dass Ransomware-Opfer einen Anstieg der Teammoral erlebten, deutlich höher als bei denjenigen, die nicht betroffen waren (60 Prozent gegenüber 47 Prozent).

Die Zukunft: Noch mehr menschliche und künstliche Intelligenz im Gleichschritt
Die Erfahrungen aus dem Jahr 2020 haben die Ambitionen für größere IT-Teams und den Einsatz fortschrittlicher Tools wie künstliche Intelligenz (KI) verstärkt. In der Studie rechnen 68 Prozent (Deutschland ebenfalls 68 Prozent) der IT-Teams mit einer Aufstockung des internen IT-Sicherheitspersonals bis 2023 und 56 Prozent (52 Prozent in Deutschland) gehen für denselben Zeitraum von einer Ausweitung der externen IT-Sicherheitsmitarbeiter aus. Eine überwältigende Mehrheit (86 Prozent) erwartet, dass KI bei der Bewältigung der wachsenden Anzahl und/oder Komplexität von Bedrohungen helfen wird. Dies könnte zum Teil darauf zurückzuführen sein, dass 54 Prozent der IT-Teams der Meinung sind, dass Cyberangriffe inzwischen zu weit fortgeschritten sind, als dass das interne Team sie allein bewältigen könnte.

Den Schwung jetzt nutzen
„Die Umfrage zeigt, dass diese Herausforderungen in vielen Fällen nicht nur zu besser ausgebildeten, sondern auch zu motivierteren IT-Teams geführt haben“, so Chester Wisniewski. „Da immer mehr Länder mit der Planung für das Leben nach den Pandemiebeschränkungen beginnen, besteht jetzt die Chance, neue IT- und Sicherheitsrichtlinien zu implementieren, moderne Tools zur Verwaltung von Mitarbeitern und Abläufen jenseits des IT-Perimeters einzuführen, Expertenteams aus internen und externen Talenten aufzubauen und Sicherheitsplattformen einzuführen, die intelligente Automatisierung mit menschlicher Expertise bei der Bedrohungsjagd kombinieren. Es gibt keinen Weg zurück. Die Zukunft könnte genauso beispiellos sein wie die Vergangenheit."

Über die Studie:
Die Studie "IT Security Team: 2021 and Beyond"-Studie wurde von Vanson Bourne, einem unabhängigen Spezialisten für Marktforschung, im Januar und Februar 2021 durchgeführt. Befragt wurden 5.400 IT-Entscheider in 30 Ländern, in den USA, Kanada, Brasilien, Chile, Kolumbien, Mexiko, Österreich, Frankreich, Deutschland, Großbritannien, Italien, den Niederlanden, Belgien, Spanien, Schweden, der Schweiz, Polen, der Tschechischen Republik, der Türkei, Israel, den VAE, Saudi-Arabien, Indien, Nigeria, Südafrika, Australien, Japan, Singapur, Malaysia und den Philippinen. Alle Befragten stammten aus Organisationen mit 100 bis 5.000 Mitarbeitern.

Die Auswertungen der Studie "IT Security Team: 2021 and Beyond" steht zum Download zur Verfügung unter: https://secure2.sophos.com/en-us/content/the-it-security-team-2021-and-beyond.aspx

Neu: Social Media von Sophos für die Presse
Wir haben speziell für Sie als Journalist*in unsere Social-Media-Kanäle angepasst und aufgebaut. Hier tauschen wir uns gerne mit Ihnen aus. Wir bieten Ihnen Statements, Beiträge und Meinungen zu aktuellen Themen und natürlich den direkten Kontakt zu den Sophos Security-Spezialisten.
Folgen Sie uns auf und

LinkedIn: https://www.linkedin.com/groups/9054356/
Twitter: @sophos_info

Über Sophos
Sophos ist ein weltweit führender Anbieter von Next Generation Cybersecurity und schützt mehr als 500.000 Unternehmen und Millionen von Verbrauchern in mehr als 150 Ländern vor den modernsten Cyberbedrohungen. Basierend auf Threat Intelligence, KI und maschinellem Lernen aus den SophosLabs und von SophosAI bietet Sophos ein breites Portfolio an fortschrittlichen Produkten und Services, um Anwender, Netzwerke und Endpoints vor Ransomware, Malware, Exploits, Phishing und einer Vielzahl anderer Cyberattacken zu schützen. Sophos bietet mit Sophos Central eine einzige, integrierte und cloudbasierte Management-Konsole. Sie ist das Herzstück eines anpassungsfähigen Cybersecurity-Ökosystems mit einem zentralen Data Lake, der eine Vielzahl offener API-Schnittstellen bedient, die Kunden, Partnern, Entwicklern und anderen Cybersecurity-Anbietern zur Verfügung stehen. Sophos vertreibt seine Produkte und Services über Partner und Managed Service Provider (MSPs) weltweit. Der Sophos-Hauptsitz ist in Oxford, U.K. Weitere Informationen unter www.sophos.de.

Pressekontakt:

Sophos
Jörg Schindler, PR-Manager Central & Eastern Europe
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de