Hohe Anforderungen bei Cyberversicherungen – 76 Prozent der Unternehmen investieren daher in ihre Cyberabwehr

Der aktuelle Cyber-Insurance-Report von Sophos belegt: rund dreiviertel aller Unternehmen verbessern ihre Abwehrmaßnahmen gegen Netzangriffe. Und zwar nicht nur für sich, sondern auch, um sich für eine Cyberversicherung zu qualifizieren. Da die Wiederherstellungskosten den Versicherungsschutz übersteigen, stellen die Versicherer mittlerweile hohe Anforderungen an die Versicherungsnehmer.

Wiesbaden, 26. Juni 2024 – Sophos veröffentlicht heute die aktuellen Ergebnisse seines Reports „Cyber Insurance and Cyber Defenses 2024: Lessons from IT and Cybersecurity Leaders“. Dieser offenbart, dass 97 Prozent der Unternehmen mit einer Cyber-Police in ihre Abwehrmaßnahmen investiert haben, um die Versicherung zu unterstützen. 76 Prozent geben an, sich dadurch für eine Deckung qualifiziert zu haben. 67 Prozent erhielten so günstigere Preise und 30 Prozent verbesserten ihre Vertragsbedingungen.

Wiederherstellungskosten übersteigen Deckungswerte
Der Report enthüllt auch: Die Wiederherstellungskosten nach einer Cyberattacke übersteigen die Versicherungsabdeckung. Nur bei 1 Prozent derjenigen mit Schadensmeldung trug der Versicherer 100 Prozent der Kosten, die bei der Behebung des Vorfalls entstanden sind. Der häufigste Grund für nicht vollständige Erstattung ist, dass die finale Rechnung das Versicherungslimit übersteigt. Laut des diesjährigen Ransomware-Reports von Sophos wuchsen die Wiederherstellungskosten nach einem Ransomware-Angriff im Vergleich zum Vorjahr um 50 Prozent auf rund 2,55 Millionen Euro.

Organisationen mangelt es an Cybersecurity-Grundlagen
„Der Sophos Active Adversary Report hat wiederholt gezeigt, dass viele Cyberversicherungs-Anbieter eine Situation vorfinden, in der grundlegende, bewährte Vorgehensweisen für die Cybersicherheit nicht implementiert wurden; zum Beispiel rechtzeitiges Einspielen von Patches“, betont Chester Wisniewski, CTO Sophos. „In unserer aktuellen Erhebung belegen kompromittierte Zugangsdaten den ersten Platz, wenn es um die Ursachen für eine Attacke geht. Diese Lücke könnte durch eine Multi-Faktor-Authentifizierung effektiv gestopft werden, allerdings haben laut unserer Erkenntnisse nur43 Prozent der Unternehmen eine solche zusätzliche Sicherheitsstufe eingeführt.“

„Die Tatsache, dass 76 Prozent der Betriebe in ihre Cyberabwehr investiert haben, um sich für eine Cyberversicherung zu qualifizieren, zeigt, dass die Versicherer die Firmen zwingen, einige dieser essenziellen Sicherheitsmaßnahmen einzuführen. Das macht einen Unterschied und hat eine insgesamt positive Auswirkung auf die Cyberresilienz von Unternehmen insgesamt. Allerdings muss klar sein: auch wenn eine Cyberversicherung für Betriebe viele Vorteile bringt, ist sie nur ein Teil einer effektiven Strategie zur Risikominimierung. Unternehmen müssen weiterhin ihre Abwehr aufrüsten. Denn eine Cyberattacke kann tiefgreifende Auswirkungen für eine Organisation haben, sowohl im Bereich Betriebsführung als auch bei der Reputation. Und eine Cyberpolice wird das alleine nicht ändern“.

Investitionen in Cyberabwehr haben positive Nebeneffekte
Von den 5.000 befragten IT- und Cybersicherheits-Führungskräften geben 99 Prozent derjenigen, die ihre Abwehrmaßnahmen für eine Police verbessern, an, dass sie auch Sicherheitsvorteile jenseits der Versicherungsabdeckung erlangen. Dazu gehören ein verbesserter Schutz, freigesetzte IT-Ressourcen und weniger Warnmeldungen.

„Investitionen in die Cyberabwehr scheinen positive Nebenwirkungen zu haben, da sie Einsparungen bei der Versicherung freisetzen, die die Unternehmen in andere Schutzmaßnahmen investieren können, um ihre Sicherheitslage zu verbessern. Mit der Verbreitung von Cyberversicherungen wird sich – hoffentlich – auch die Sicherheit der Unternehmen verbessern. Eine Police lässt Ransomware-Angriffe nicht verschwinden, aber sie könnte durchaus Teil der Lösung sein“, prophezeit Wisniewski.

Zum Cyber Insurance Report
In der herstellerunabhängigen Befragung nahmen 5.000 Führungskräfte der IT und Cybersicherheit zwischen Januar und Februar 2024 teil. 14 Länder aus Amerika, EMEA und dem Asia Pazifik Raum beteiligten sich mit Organisationsgrößen von 100 und 5.000 Mitarbeitern. Der Umsatz variiert zwischen weniger als 10 Millionen und mehr als 5 Milliarden US-Dollar.

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/
X/Twitter: @sophos_info

Über Sophos
Sophos ist ein weltweit führender und innovativer Anbieter fortschrittlicher Lösungen zur Abwehr von Cyberangriffen, darunter Managed Detection and Response (MDR) sowie Incident Response Services. Das Unternehmen bietet ein breites Portfolio an Endpoint-, Netzwerk-, E-Mail- und Cloud-Sicherheitstechnologien, das bei der Abwehr von Cyberangriffen unterstützt. Als einer der größten auf Cybersecurity spezialisierten Anbieter schützt Sophos mehr als 600.000 Unternehmen und mehr als 100 Millionen Anwender weltweit vor aktiven Angriffen, Ransomware, Phishing, Malware und vielem mehr.

Die Dienste und Produkte von Sophos sind über die cloudbasierte Management-Konsole Sophos Central verbunden und werden vom bereichsübergreifenden Threat-Intelligence-Expertenteam Sophos X-Ops unterstützt. Die Erkenntnisse von Sophos X-Ops erweitern das gesamte Sophos Adaptive Cybersecurity Ecosystem. Dazu gehört auch ein zentraler Datenspeicher, der eine Vielzahl offener APIs nutzt, die Kunden, Partnern, Entwicklern und anderen Anbietern von Cybersecurity und Informationstechnologie zur Verfügung stehen.

Sophos bietet Cybersecurity-as-a-Service für Unternehmen an, die vollständig verwaltete, schlüsselfertige Sicherheitslösungen benötigen. Kunden können ihre Cybersecurity auch direkt mit der Security Operations Platform von Sophos verwalten oder einen hybriden Ansatz verfolgen, indem sie ihre internen Teams mit Sophos Services ergänzen, einschließlich Threat Hunting und Systemwiederherstellung.

Sophos vertreibt seine Produkte über Reseller und Managed Service Provider (MSPs) weltweit. Der Hauptsitz von Sophos befindet sich in Oxford, U.K.

Weitere Informationen unter: www.sophos.de

Pressekontakt:

Sophos
Jörg Schindler, Senior PR-Manager EMEA Central
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