70% mehr Ransomware-Attacken bei Behörden

Im Rahmen seiner jährlichen, weltweiten Ransomware-Analyse hat Sophos die staatlichen und lokalen Behörden unter die Lupe genommen. Wie in nahezu allen Branchen haben auch hier die Attacken stark zugenommen. Behörden hinken bei der Aufdeckung und dem Stoppen modernen Cyberattacken im Branchenvergleich hinterher.

Wiesbaden, 27. September 2022 – Die jährliche Studie von Sophos zu den Ransomware-Erfahrungen von IT-Fachleuten in den staatlichen und kommunalen Verwaltungen zeigt, dass die Angriffsumgebung immer komplexer wird und die finanzielle und betriebliche Belastung der Opfer durch Ransomware zunimmt. Die Analyse wirft auch ein neues Licht auf die Beziehung zwischen Ransomware und Cyber-Versicherungen, einschließlich der Rolle, die die Versicherung bei der Weiterentwicklung der Cyberabwehr spielt.

70 Prozent mehr Ransomware-Angriffe
58 Prozent der Kommunalverwaltungen waren 2021 von Ransomware betroffen, 2020 lag die Rate noch bei 34 Prozent – ein Anstieg von 70 Prozent innerhalb eines Jahres. Ein Beleg dafür, dass die Angreifer inzwischen wesentlich besser in der Lage sind, die wichtigsten Attacken in großem Maßstab auszuführen.

Allerdings meldeten staatliche und kommunale Behörden im Jahr 2021 eine der niedrigsten Ransomware-Angriffsraten aller untersuchten Sektoren. Zum Vergleich: 66 Prozent der Befragten über alle Branchen hinweg gaben an, im letzten Jahr von Ransomware betroffen gewesen zu sein, sprich ein oder mehrere Geräte waren betroffen, aber nicht unbedingt verschlüsselt.

Eine der höchsten Verschlüsselungsraten
Während die Angriffsrate unter dem branchenübergreifenden Durchschnitt lag, meldeten staatliche und kommunale Behörden eine der höchsten Raten an Datenverschlüsselung nach einem Angriff: Fast drei Viertel (72 Prozent) der Befragten gaben an, dass es den Angreifern gelungen sei, Daten zu verschlüsseln. Weltweit, über alle Branchen hinweg, führten 65 Prozent der Angriffe zu einer Verschlüsselung der Daten, ein Anstieg um 20 Prozent gegenüber 54 Prozent in 2020. Nur jede fünfte (20 Prozent) Behörde war in der Lage, den Angriff zu stoppen, bevor die Daten verschlüsselt wurden. Diese Zahl liegt deutlich unter dem weltweiten Durchschnitt von 31 Prozent. Dies deutet darauf hin, dass staatliche und kommunale Behörden bei den Fähigkeiten, moderne Angriffe zu erkennen und zu stoppen, bevor sie Schaden anrichten, noch hinterherhinken.

Starke Kostenreduzierungen bei Behörden, um zum Normalbetrieb zurückzukommen
Insgesamt gaben 90 Prozent der befragten staatlichen und kommunalen Behörden an, dass ihre Organisation Lösegeldzahlungen von weniger als 100.000 US-Dollar geleistet hat.
Die Gesamtrettungskosten waren die niedrigsten aller Sektoren mit einer Abschlussrechnung von 660.000 US-Dollar. Dies ist ein Rückgang um fast 1 Million Dollar gegenüber den durchschnittlichen Kosten von 1,64 Millionen Dollar, die der Sektor im Jahr 2020 gemeldet hat.
Bei der Wiederherstellungszeit sind die Behörden mit dem weltweiten Durchschnitt auf Augenhöhe: Rund die Hälfte der Ämter (52 Prozent) waren nach einer Woche wieder einsatzbereit.

Cyber-Versicherungsschutz gegen Ransomware unter dem Durchschnitt
Acht von Zehn der Befragten hatten eine Versicherung gegen Ransomware. Weltweit liegt die Quote hier nur wenig höher bei 83 Prozent, zeigt aber mit 51 Prozent einen deutlichen Anstieg im öffentlichen Sektor gegenüber dem Vorjahr. Für 90 Prozent der Befragten hat sich der Versicherungsprozess in den letzten 12 Monaten stark verändert: weniger Anbieter, höhere Qualifizierungslevel, komplexere Policen, längere Abläufe und höhere Kosten stehen an der Tagesordnung.
Diese Veränderungen hängen eng mit dem starken Anstieg der Ransomware-Attacken zusammen, die den größten Anteil an Ansprüchen bei einer Cyberversicherung ausmacht. In den letzten Jahren sind die Lösegelder und damit die Auszahlungen in die Höhe geschossen. Das Ergebnis dieser Entwicklung ist, dass einige Versicherungsanbieter den Markt verlassen haben, weil er für sie schlichtweg zu unrentabel geworden ist. Das hat auch die Marktbedingungen verändert und die Anbieter können ihre Kunden selektiver aussuchen.

Cyberversicherung als Katalysator für verbesserten Cyberschutz
Bis zu welcher Höhe die Cyberversicherung zahlt, ist unterschiedlich. Staatliche und lokale Behörden gaben aber eine Auszahlungsquote von 95 Prozent an (branchenübergreifend sind es 98 Prozent). Jedoch deckte die Versicherung in dieser Branche in nur 44 Prozent die Sanierungskosten, die niedrigste Quote aller Sektoren. Der Branchendurchschnitt beträgt immerhin 77 Prozent. Es gilt eben auch zu bedenken, dass eine Cyberversicherung nicht alles abdeckt. Die Investitionen in modernere Technologien und Dienste, die zukünftige Angriffe verhindern, liegen bei den Organisationen selbst. Und so haben 96 Prozent der staatlichen und lokalen Behörden, die über eine Cyberversicherung verfügen, ihre Cyberabwehr (und damit auch ihre Versichertenposition) verändert. 63 Prozent implementierten neue Technologien und Services, 56 Prozent verstärkten Mitarbeiterschulungen und jeder Zweite (51 Prozent) hat sein Verhalten den neuen Bedingungen angepasst.

Über die Studie
Sophos beauftragte das Marktforschungsunternehmen Vanson Bourne mit der Durchführung einer unabhängigen, herstellerunabhängigen Umfrage unter 5.600 IT-Fachleuten in 31 Ländern, darunter 199 aus staatlichen und lokalen Behörden. Die Umfrage wurde im Januar und Februar 2022 durchgeführt.

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 Anwendern 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 http://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