



Sophos State of Ransomware Report 2024: 97 Prozent der von Ransomware betroffenen Unternehmen wenden sich an Behörden

Enorm viele Unternehmen wenden sich bei einer Cyberattacke an behördliche Einrichtungen. Der aktuelle Sophos State of Ransomware Report bestätigt, dass weit über die Hälfte der Betroffenen neben der reinen Meldung auch Beratung oder Anleitung zur Wiederherstellung ihrer Daten suchen.

Wiesbaden, 14. Mai 2024 – Laut dem jährlichen [State of Ransomware 2024](#) Report arbeiteten 97 Prozent der befragten Organisationen, die im letzten Jahr Opfer von Ransomware waren, mit Strafverfolgungsbehörden oder anderen amtlichen Stellen zusammen. Dieser eindrucksvoll hohe Prozentsatz gilt gleichermaßen für die weltweiten als auch die DACH-Umfrageergebnisse. Mehr als die Hälfte (59 Prozent weltweit und 56 Prozent in DACH) dieser so operierenden Unternehmen fand den Prozess recht einfach. Nur 10 Prozent weltweit und 13 Prozent in DACH empfanden ihn als sehr schwer.

Dem Report nach wandten sich angegriffene Unternehmen auch an Behörden, um Unterstützung und Hilfsmaßnahmen zur Aufarbeitung nach ihrer Ransomware Attacke zu erhalten. 61 Prozent weltweit und 55 Prozent in DACH erhielten Beratung, 60 Prozent weltweit und 52 Prozent in DACH nutzen Hilfe bei der Untersuchung des Angriffs. Aus internationaler Perspektive wurden 58 Prozent derjenigen mit verschlüsselten Daten seitens der Behörden bei der Wiederherstellung ihrer Daten unterstützt. In Deutschland und Österreich war dieser Anteil mit 56 Prozent beziehungsweise 64 Prozent ähnlich, Lediglich in der Schweiz nutzten nur 45% diese Unterstützung.

Meldung bei den Behörden ist kein rotes Tuch mehr

„Traditionell scheuen sich Betriebe davor, sich an Strafverfolgungsbehörden zu wenden, aus Sorge, dass der Fall publik wird. Wenn bekannt wird, dass sie Opfer einer Cyberattacke wurden, könnte das Einfluss auf ihre Unternehmensreputation haben und eine prekäre Situation damit noch verschlimmern. Diese Betroffenenscham ging lange mit einer Attacke einher, aber es gibt Fortschritte, sowohl innerhalb der Sicherheits-Community als auch auf Regierungsebene. Neue Regulierungen zu [Cyber Incident Reporting](#) scheinen dazu beigetragen zu haben, die Hürden für eine Kooperation mit der Strafverfolgung zu senken. Die aktuellen Ergebnisse des Reports zeigen, dass Organisationen den Schritt in die richtige Richtung machen. Wenn der öffentliche und private Sektor eine Gruppe zur Unterstützung betroffener Unternehmen bilden, sind wir in der Lage, unsere Fähigkeiten zur schnellen Wiederherstellung zu verbessern. Zudem ist es möglich, Erkenntnisse zu sammeln, um andere zu schützen oder im Idealfall sogar diejenigen zur Verantwortung zu ziehen, die diese Angriffe durchführen“, ordnet Chester Wisniewski, Field CTO Sophos, die Ergebnisse ein.

Starke Zusammenarbeit von öffentlichem und privatem Sektor nötig, weltweit

„Die Mühlen der Justiz mahlen teilweise frustrierend langsam. Aber die Strafverfolgungssysteme passen sich immer besser an die Cybercrime-Bekämpfung an und die verbesserte Kooperation und Zusammenarbeit von Unternehmen mit den Behörden nach einer Attacke ist eine gute Entwicklung. Allerdings müssen wir uns alle von der reinen Symptombehandlung von Ransomware hin zur Prävention vor diesen Angriffen weiterentwickeln. Unser kürzlich veröffentlichter [Active Adversary Report](#) belegt, dass viele Organisationen immer noch daran scheitern, Schlüssel-Sicherheitsmaßnahmen zu implementieren, die ihr Gesamtrisiko nachweislich verringern können. Das beinhaltet rechtzeitiges Patchen der Geräte und die Verwendung von Multifaktor-Authentifizierungen. Die

Strafbehörden hatten zwar Erfolg mit Auflösungen und Inhaftierungen bei LockBit und Qakbot. Diese Erfolge zeigen sich aber eher als vorübergehende Unterbrechungen, denn als längerfristige oder dauerhafte Erfolge.



Der Erfolg der Kriminellen beruht zum Teil auf dem Umfang und der Effizienz, mit der sie arbeiten. Um sie zu besiegen, müssen wir auf beiden Gebieten mit ihnen gleichziehen. Das bedeutet für die Zukunft sogar eine noch stärkere Zusammenarbeit von privatem und öffentlichem Sektor – und zwar auf weltweitem Level“, fordert Wisniewski.

Über den Sophos State of Ransomware Report 2024

Der State of Ransomware 2024 Report wurde von einem unabhängigen Marktforschungsunternehmen unter 5.000 Cybersicherheits-/ IT-Führungskräften in 14 Ländern aus Amerika, EMEA und dem Asia-Pazifikraum durchgeführt. Die Befragung der Unternehmen zwischen 100 und 5.000 Mitarbeitern fand zwischen Januar und Februar dieses Jahres statt.

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