Neue Sophos-Studie „State of Ransomware 2022“ Studie: 60 Prozent der Schweizer Unternehmen von Erpressermalware betroffen

Die Umfrage zeigt, dass das durchschnittlich gezahlte Lösegeld in der Schweiz um 6 Prozent auf 84.052 CHF gesunken ist.
35% der Schweizer Unternehmen, deren Daten bei einem Ransomware-Angriff verschlüsselt wurden, haben das Lösegeld gezahlt.

Zürich, 27. April 2022 – Sophos veröffentlicht heute seine jährliche Studie "State of Ransomware 2022", die einen Überblick über die Ransomware-Entwicklung in der Praxis gibt. Der Report zeigt, dass 60% der in der Schweiz befragten Unternehmen (global 66%) im Jahr 2021 von Ransomware betroffen waren, gegenüber 46% im Jahr 2020. Das durchschnittliche Lösegeld, das von Schweizer Unternehmen gezahlt wurde, deren Daten bei ihrem größten Ransomware-Angriff verschlüsselt wurden, hat sich um rund 6% verringert und beträgt 84.052 CHF (89.147 CHF im Vorjahr). 35% (global 46%) der Schweizer Unternehmen, deren Daten verschlüsselt wurden, zahlten das Lösegeld, um ihre Daten zurückzubekommen, auch wenn sie über andere Mittel zur Datenwiederherstellung verfügten, z. B. Backups.

Der Bericht fasst die Auswirkungen von Ransomware auf 5.600 mittelständische Unternehmen in 31 Ländern in Europa, Nord- und Südamerika, Asien-Pazifik und Zentralasien, dem Nahen Osten und Afrika zusammen, wobei international 965 (in Schweiz 7) Unternehmen konkrete Angaben zu Ransomware-Zahlungen machten.

„Neben den eskalierenden Zahlungen zeigt die Umfrage auch, dass der Anteil der zahlungswilligen Opfer weiter ansteigt, selbst wenn sie andere Optionen zur Verfügung haben", sagt Chester Wisniewski, Principal Research Scientist bei Sophos. „Dafür kann es mehrere Gründe geben, etwa unvollständige Backups oder das Verhindern der Veröffentlichung gestohlener Daten auf einer Public-Leaks-Seite. Nach einem Ransomware-Angriff besteht oft ein großer Druck, den Betrieb so schnell wie möglich wieder aufzunehmen. Die Wiederherstellung verschlüsselter Daten mit Hilfe von Backups kann ein schwieriger und zeitaufwändiger Prozess sein. Daher ist es scheinbar verlockend, ein Lösegeld für die Datenentschlüsselung zu zahlen, weil dies als eine schnelle Option erscheint. Dieses Vorgehen ist aber mit hohen Risiken verbunden. Unternehmen wissen nicht, was die Angreifer außer der Ransomware-Attacke eventuell noch im Netzwerk getan haben, beispielsweise Hintertüren für künftige Angriffe installiert oder Kennwörtern kopiert. Wenn Unternehmen die wiederhergestellten Daten nicht gründlich bereinigen, haben sie am Ende im Worst Case immer noch potenziell schädliche Programme in ihrem Netzwerk und sind möglicherweise einem erneuten Angriff ausgesetzt."

Die wichtigsten Ergebnisse der „State of Ransomware 2022“-Studie im Überblick:

- **Höhe der Lösegeldzahlungen:** Im Jahr 2021 gaben keine der Schweizer Unternehmen an, dass sie Lösegeld in Höhe von 1 Million US-Dollar oder mehr gezahlt haben, im Gegensatz zu 11% aus globaler Sicht. Die meisten Schweizer Unternehmen (ca. 72%) bezahlten Summen zwischen 47.834 und 239.175 CHF (50.000 und 250.000 US-Dollar).

- **Mehr Opfer zahlen Lösegeld**: Im Jahr 2021 zahlten 35% (global 46%) der Schweizer Unternehmen, deren Daten durch einen Ransomware-Angriff verschlüsselt wurden, das Lösegeld. Aus globaler Sicht zahlten 26% der Unternehmen, die im Jahr 2021

verschlüsselte Daten mithilfe von Backups wiederherstellen konnten, ebenfalls das Lösegeld.

- **Die Auswirkungen eines Ransomware-Angriffs können immens sein**: Die durchschnittlichen Kosten für die Wiederherstellung nach einem Ransomware-Angriff im Jahr 2021 betrugen für Schweizer Unternehmen 1.568.986 CHF (global 1,4 Millionen US-Dollar / 1.339.379 CHF). Es dauerte im Durchschnitt einen Monat, um den Schaden und die Geschäftsunterbrechung zu beheben. 93% (global 90%) der Schweizer Unternehmen gaben an, dass der Angriff ihre Betriebsfähigkeit beeinträchtigt hat, und 87% der Opfer in der Privatwirtschaft gaben an, dass sie aufgrund des Angriffs Geschäfts- und/oder Umsatzeinbußen erlitten haben.

- **Viele Unternehmen verlassen sich auf eine Cyber-Versicherung, um sich von einem Ransomware-Angriff zu erhole**n: In der Schweiz hatten 83% (global 83%) der befragten Unternehmen eine Cyber-Versicherung, die sie im Falle eines Ransomware-Angriffs abdeckt. In 100 % der Schweizer Vorfälle zahlte der Versicherer einige oder alle entstandenen Kosten, lediglich bei 38% wurde die gesamte Lösegeldforderung abgedeckt)

- **Vierundneunzig Prozent derjenigen, die eine Cyberversicherung abgeschlossen haben, gaben an, dass sich ihre Erfahrungen beim Abschluss einer solchen Versicherung in den letzten zwölf Monaten verändert haben:** Dieses Empfinden äußert sich vor allem durch höhere Anforderungen an Cyber-Sicherheitsmaßnahmen, komplexere oder teurere Policen und weniger Unternehmen, die Versicherungsschutz anbieten.

„Die Ergebnisse deuten darauf hin, dass wir möglicherweise einen Höhepunkt in der Entwicklung von Ransomware erreicht haben, wo die Gier der Angreifer nach immer höheren Lösegeldzahlungen frontal mit einer Verhärtung des Cyberversicherungsmarktes kollidiert. Die Versicherer versuchen zunehmend ihr Ransomware-Risiko und ihre Exponierung zu reduzieren", sagt Wisniewski. „In den letzten Jahren ist es für Cyberkriminelle immer einfacher geworden, Ransomware einzusetzen, da fast alles als Service verfügbar ist. Zudem haben viele Cyber-Versicherungsanbieter eine breite Palette von Wiederherstellungskosten aufgrund von Ransomware, einschließlich des Lösegelds, abgedeckt, was wahrscheinlich zu immer höheren Lösegeldforderungen beigetragen hat. Die Ergebnisse deuten auch darauf hin, dass die Cyber-Versicherungen härter werden und die Opfer von Ransomware in Zukunft möglicherweise weniger bereit oder weniger in der Lage sein werden, extrem hohe Lösegelder zu zahlen. Leider ist es unwahrscheinlich, dass dies das Gesamtrisiko eines Ransomware-Angriffs verringert. Ransomware-Angriffe sind nicht so ressourcenintensiv wie andere, handwerklich ausgefeiltere Cyberattacken. Daher ist jedes Lösegeld ein lohnender Gewinn, der sich lohnt, und Cyberkriminelle werden sich auch weiterhin die leicht erreichbaren Ziele aussuchen."

Sophos empfiehlt die folgenden Best Practices zum Schutz vor Ransomware und ähnlichen Cyberattacken:

1. Installation und Pflege hochwertiger Schutzmaßnahmen im gesamten Unternehmen. Regelmäßige Prüfungen und Sicherheitskontrollen stellen sicher, dass die Sicherheitsvorkehrungen dauerhaft den Anforderungen des Unternehmens entsprechen.
2. Aktive Suche nach Bedrohungen, um Angreifer zu identifizieren und zu stoppen, bevor sie ihre Attacken ausführen können. Wenn das IT- oder Security-Team nicht die Ressourcen oder die Kenntnisse hat, dies selbst zu tun, sollten Spezialisten für Managed Detection and Response (MDR) beauftragt werden.
3. Härtung der IT-Umgebung durch Aufspüren und Schließen gefährlicher Sicherheitslücken, wie beispielsweise ungepatchte Geräte, ungeschützte Rechner, oder offene RDP-Ports, werden durch Extended Detection and Response (XDR)-Lösungen identifiziert und eliminiert.

4. Auf das Schlimmste vorbereitet sein. Unternehmen sollten wissen, was zu tun ist, wenn ein Cybervorfall eintritt und den Notfallplan stets auf dem neuesten Stand halten.
5. Erstellen von Backups und das Testen der Wiederherstellung, damit das Unternehmen so schnell wie möglich und mit minimalen Unterbrechungen den Betrieb wieder aufnehmen kann.

Hier steht der "The State of Ransomware 2022" mit den vollständigen globalen Ergebnissen und Daten nach Branchen zum Download bereit.

Über die Studie
Die State of Ransomware 2022 Studie befasst sich mit Ransomware-Vorfällen und Erfahrungen im Jahr 2021. Die Umfrage wurde von Vanson Bourne, einem unabhängigen Spezialisten für Marktforschung, im Januar und Februar 2022 durchgeführt. Befragt wurden 5.600 IT-Entscheidungsträger in 31 Ländern, in den USA, Kanada, Brasilien, Chile, Kolumbien, Mexiko, Österreich, Frankreich, Deutschland, Ungarn, Großbritannien, Italien, den Niederlanden, Belgien, Spanien, Schweden, der Schweiz, Polen, der Tschechischen Republik, der Türkei, Israel, den Vereinigten Arabischen Emiraten, Saudi-Arabien, Indien, Nigeria, Südafrika, Australien, Japan, Singapur, Malaysia und den Philippinen. Alle Befragten stammten aus mittelständischen Unternehmen mit 100 bis 5.000 Mitarbeitern.

Hinweis: Für die globale Umfrage wurde "von Ransomware betroffen" definiert als ein oder mehrere Geräte, die von einem Ransomware-Angriff betroffen sind, aber nicht unbedingt verschlüsselt wurden. Wenn nicht anders angegeben, wurden die Befragten gebeten, über ihren wichtigsten Angriff zu berichten.

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 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