Schüler- und Studentendaten als beliebte Beute: Ransomware-Angriffe auf Bildungseinrichtungen nehmen weltweit zu

Internationale Sophos Studie zeigt:
Bildungssektor leidet weltweit unter der höchsten Datenverschlüsselungsrate und der längsten Wiederherstellungszeit
Hochschulen benötigen besonders lange für die Datenrekonstruktion
Die Wiederherstellungsrate sinkt insgesamt

Wiesbaden, 12. Juli 2022 – Sophos hat neue Studienergebnisse veröffentlicht: The State of Ransomware in Education 2022. Die Resultate basieren auf den Erfahrungen der befragten Einrichtungen über den Zeitraum des zurückliegenden Jahres hinweg und zeigen, dass weltweit Bildungseinrichtungen jeder Art zunehmend von Ransomware betroffen sind. So waren im Jahre 2021 rund 60 Prozent das Ziel von Angriffen währen diese Zahl im Jahr zuvor noch bei 44 Prozent lag. Bildungseinrichtungen waren mit der höchsten Datenverschlüsselungsrate (73 Prozent) im Vergleich zu anderen Sektoren (65 Prozent) und der längsten Wiederherstellungszeit konfrontiert: 7 Prozent benötigten zwischen drei und sechs Monaten, um die Daten wiederherzustellen – fast doppelt so lange wie durchschnittlich in anderen Branchen oder Sektoren (4 Prozent).

Weitere Ergebnisse der Studie beinhalten:

- **Bildungseinrichtungen verzeichnen im Vergleich zu anderen Sektoren die meisten betrieblichen und kommerziellen Auswirkungen von Ransomware**; 97 Prozent der Befragten im Hochschulbereich und 94 Prozent der Befragten im unteren Bildungsbereich geben an, dass die Angriffe ihre Betriebsfähigkeit beeinträchtigt haben, während 96 Prozent der Befragten im Hochschulbereich und 92 Prozent der befragten Privatschulen im Primärbereich darüber hinaus über Geschäfts- und Umsatzeinbußen berichten.
- **Die Wiederherstellungsrate sinkt**: Unter 2 Prozent der Bildungseinrichtungen konnten alle verschlüsselten Daten wiederherstellen, nachdem sie ein Lösegeld gezahlt hatten (gegenüber 4 Prozent im Jahr 2020); im Durchschnitt konnten die Bildungseinrichtungen 62 Prozent der verschlüsselten Daten wiederherstellen, nachdem sie Lösegeld gezahlt hatten (gegenüber 68 Prozent im Jahr 2020).
- **Hochschuleinrichtungen melden die längste Wiederherstellungszeit für Daten**; während rund 40 Prozent aller Bildungseinrichtungen angeben, dass die Wiederherstellung der durch einen Ransomware-Angriff betroffenen Daten rund einen Monat dauert (20 Prozent für andere Sektoren), berichten 9 Prozent, dass hierfür drei bis sechs Monate benötigt werden, das ist im Branchenvergleich der höchste Wert.

Fundgrube an persönlichen Daten mit wenig Schutz

„Schulen gehören zu denen, die am stärksten von Ransomware betroffen sind. Sie sind ein bevorzugtes Ziel für Angreifer, da sie über keine starken Sicherheitsvorkehrungen verfügen und eine wahre Fundgrube an persönlichen Daten sind", sagt Chester Wisniewski, Principal Research Scientist bei Sophos. „Bildungseinrichtungen haben eine geringere Wahrscheinlichkeit als andere, laufende Angriffe zu erkennen, was natürlich zu höheren Angriffserfolgen und Verschlüsselungsraten führt. Selbst wenn ein Teil der Daten wiederhergestellt wird, gibt es keine Garantie dafür, welche Daten die Angreifer zurückgeben werden. Die einzige Möglichkeit, ihnen zuvorzukommen, besteht darin, dem Aufbau einer Anti-

Ransomware-Abwehr eine höhere Priorität einzuräumen, um Angriffe zu erkennen und zu entschärfen, bevor eine Verschlüsselung möglich ist."

Bildungswesen mit höchsten Auszahlungsraten bei Versicherungen
Interessanterweise melden Bildungseinrichtungen die höchste Auszahlungsquote der Cyberversicherung bei Ransomware-Schäden (100 Prozent im Hochschulbereich, 99 Prozent im unteren Bildungsbereich). Insgesamt hat der Sektor jedoch eine niedrigere Rate von Cyber-Versicherungsschutz gegen Ransomware als andere Branchen (78 % im Vergleich zu 83 % in anderen Sektoren).

Anforderungen der Cyberversicherungen steigen
„Vier von zehn Schulen geben an, dass weniger Versicherungsanbieter ihnen Versicherungsschutz anbieten, während fast die Hälfte (49 %) berichtet, dass das Niveau der Cybersicherheit, das sie benötigen, um sich für den Versicherungsschutz zu qualifizieren, gestiegen ist", so Wisniewski. „Die Anbieter von Cyberversicherungen werden bei der Aufnahme von Kunden immer wählerischer, und Bildungseinrichtungen brauchen Hilfe, um diese höheren Standards zu erfüllen. Angesichts begrenzter Budgets sollten die Schulen eng mit vertrauenswürdigen Sicherheitsexperten zusammenarbeiten, um sicherzustellen, dass die Ressourcen für die richtigen Lösungen eingesetzt werden."

Sophos´ grundsätzliche Empfehlungen gegen Ransomware lauten:

- **Installation und Pflege von hochwertigen Schutzmaßnahmen** an allen Stellen der Umgebung. Überprüfen Sie die Sicherheitskontrollen regelmäßig und stellen Sie sicher, dass sie weiterhin den Anforderungen des Unternehmens entsprechen.
- **Proaktive Bedrohungssuche, um Angreifer zu identifizieren und zu stoppen**, bevor sie Angriffe ausführen können - wenn das Team nicht die Zeit oder die Fähigkeiten hat, dies intern zu tun, sollten Sie ein MDR-Team (Managed Detection and Response) beauftragen
- **Härtung der IT-Umgebung durch Finden und Schließen wichtiger Sicherheitslücken**: ungepatchte Geräte, ungeschützte Rechner und offene RDP-Ports, zum Beispiel. Extended Detection and Response (XDR)-Lösungen sind für diesen Zweck ideal
- **Planung des Worst Case Szenarios** und Bereithaltung eines aktualisierten Plans für den schlimmsten Fall
- **Erstellung von Sicherungskopien und Übung der Wiederherstellung**, um Unterbrechungen und Wiederherstellungszeiten zu minimieren.

Über die Studie
"State of Ransomware in Education 2022" ist Teil der branchen- und sektorenübergreifenden State of Ransomware 2022 Studie, bei der 5.600 IT-Fachleute in mittelgroßen Organisationen (100-5.000 Mitarbeiter) in 31 Ländern zu ihren Erfahrungen über das vergangene Jahr hinweg befragt wurden, darunter 320 Befragte aus dem unteren und 410 Befragte aus dem oberen Bildungsbereich.

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