Angriff auf die Synapsen –
Bildungseinrichtungen mit höchster Ransomware-Rate

Der Sektor Bildung kommt beim Thema Ransomware nicht gut weg. Wie Sophos im Rahmen seiner globalen Analyse The State of Ransomware in Education 2023 *herausfand, sind hier nach den häufigsten Angriffen auch mit die höchsten Lösegeldzahlungen zu finden.*

Sophos stellt seinen jährlichen Ransomware-Report für das Bildungswesen vor. The State of Ransomware in Education 2023 macht sichtbar, dass Bildungseinrichtungen weltweit die höchste Rate an Ransomware Attacken hatten.

79 Prozent des Hochschulbereichs sowie 80 Prozent der niedrigeren Bildungseinrichtungen berichteten, Opfer von Ransomware geworden zu sein – dies entspricht einem Wachstum von 64 bzw. 56 Prozent gegenüber dem Vorjahr.

Bei mehr als drei Viertel der Bildungseinrichtungen (81 Prozent im unteren Bildungsbereich; 73 Prozent im Hochschulbereich), die von Ransomware betroffen waren, wurden zudem Daten verschlüsselt. Darüber hinaus berichteten 27 Prozent der Institutionen im unteren Bildungsbereich sowie 35 Prozent im Hochschulbereich, dass ihre verschlüsselten Daten auch gestohlen wurden. Besorgniserregend ist hierbei, dass die Verwendung von Backups zur Wiederherstellung verschlüsselter Daten im Bildungswesen im letzten Jahr zurückging, während die Lösegeldzahlungen von Jahr zu Jahr zunahmen.

Erkenntnis 1: Lösegeld zu zahlen, macht alles noch schlimmer
Der Bildungssektor zahlt die höchsten Lösegelder: 56 Prozent im höheren Bildungssegment, 47 Prozent im niedrigeren. Die Überweisung der Summen erhöhte für beide Bereiche signifikant die Wiederherstellungskosten. Diese (exklusive der Lösegeldzahlungen) betrugen für die höheren Bildungseinrichtungen, die die Forderung der Kriminellen beglichen, 1.31 Millionen US-Dollar – bei Wiederherstellung der Daten aus Backups hingegen nur 980.000 US-Dollar. Bei niedrigeren Bildungseinrichtungen lagen die Wiederherstellungskosten im Durchschnitt bei 2.18 Millionen US-Dollar, wenn sie vorab zahlten, bei 1.37 Millionen US-Dollar, wenn sie nicht zahlten.

Die Zahlung der Lösegeldsumme hat sogar noch einen weiteren Nachteil: Die Wiederherstellungszeit verlängert sich ebenfalls. Für Hochschulen gilt: 79 Prozent derjenigen, die Backups verwendeten, erholten sich innerhalb eines Monats, während nur 63 Prozent mit Ransomware-Zahlung sich innerhalb dieser Zeitspanne wieder einsatzfähig machen konnten. Bei niedrigeren Einrichtungen ist der Gegensatz mit 63 zu 59 Prozent nicht ganz so stark.

„Obwohl die meisten Schulen über wenig Bargeld verfügen, sind sie dennoch sehr beliebte Ziele mit unmittelbar weitreichenden Folgen für ihre Umgebungen. Der Druck, die Türen offen zu halten und auf „Machen Sie doch etwas“-Anrufe von Eltern zu reagieren, führt eher dazu, das Problem schnell lösen zu wollen ohne Rücksicht auf die Kosten. Unglücklicherweise unterstützen die vorliegenden Daten nicht die These, dass die Zahlung von Lösegeld diese Attacken schneller behebt. Aber es ist wahrscheinlich ein Faktor für die Kriminellen bei der Auswahl ihrer Opfer“, erläutert Chester Wisniewski, Field CTO bei Sophos.

Erkenntnis 2: Kompromittierte Zugangsdaten laden Cyberkriminelle ein
Für den Bildungssektor lässt sich feststellen, dass die Ursachen für Ransomware-Angriffe denen der anderen Segmente ähnlich sind, aber es gibt hier eine auffallend höhere Anzahl an Ransomware-Attacken, bei denen kompromittierte Zugangsdaten für Hochschul- (37 Prozent)

wie niedrigere (36 Prozent) Bildungs-Bereiche involviert waren. Branchenübergreifend liegt der Durchschnitt bei 29 Prozent.

Weitere Ergebnisse der Ransomware in Education-Analyse 2023:

- Schwachstellen und kompromittierte Zugangsdaten machten mehr als 77 Prozent der Ransomware Angriffe gegen höhere Bildungsinstitute aus (niedrigere Einrichtungen zu 65 Prozent).

- Die Verschlüsselungsrate blieb bei höheren Einrichtungen mit 73 Prozent im Vergleich zu 74 Prozent im Vorjahr nahezu gleich. Aber: bei den niedrigeren Instituten erhöhte sie sich von 72 Prozent auf 81 Prozent.

- Hochschulbetriebe berichteten eine geringere Rate (63 Prozent) an Backup- Nutzung als der branchenübergreifende Durchschnitt (70 Prozent). Dies bedeutet die drittniedrigste Quote über alle Sektoren hinweg. Aber: Untere Bildungseinrichtungen setzen mit 73 Prozent dagegen sogar etwas mehr Backups ein als der weltweite Durchschnitt.

„Bildungseinrichtungen sollten noch mehr Maßnahmen ergreifen, um sich besser gegen Ransomware und andere Cyberangriffe zu schützen. So ist etwa der Missbrauch gestohlener Zugangsdaten in allen Branchen für Ransomware-Kriminelle üblich, aber zum Beispiel steigert die fehlende Anwendung von Multi-Faktor-Authentifizierung (MFA) Technologien gerade im Bildungssektor hier die Gefahr. Es ist daher an der Zeit für Bildungseinrichtungen aller Größen, MFA für die Lehrkräfte, Schüler und Studenten einzusetzen. Damit gehen sie mit gutem Beispiel voran und es ist zudem ein simpler Weg, viele dieser Attacken schon vor der Schultür abzufangen," sagt Chester Wisniewski.

Sophos empfiehlt außerdem folgende Schritte zur besseren Abwehr von Ransomware und anderen Cyberangriffen:

1. Verwendung von Sicherheitstools, die vor den häufigsten Angriffsvektoren schützen, einschließlich Endpunktschutz mit starken Anti-Exploit-Funktionen, um die Ausnutzung von Schwachstellen zu verhindern, und Zero Trust Network Access (ZTNA), um den Missbrauch kompromittierter Anmeldeinformationen zu verhindern
2. Einsatz Adaptiver Technologien, die automatisch auf Angriffe reagieren, Gegner stören und den Verteidigern Zeit verschaffen, um zu reagieren
3. Eine 24/7-Bedrohungserkennung, -untersuchung und -reaktion, entweder intern oder durch einen spezialisierten Anbieter von Managed Detection and Response (MDR)
4. Optimierung der Angriffsvorbereitung, einschließlich regelmäßiger Backups, Übungen zur Wiederherstellung von Daten aus Backups und Pflege eines aktuellen Reaktionsplans für Zwischenfälle
5. Aufrechterhaltung einer guten Sicherheitshygiene, einschließlich rechtzeitiger Patches und regelmäßiger Überprüfung der Konfigurationen von Sicherheitstools

Über die Studie

Die Daten der Studie „State of Ransomware 2023" stammen aus einer herstellerunabhängigen Umfrage unter 3.000 Führungskräften im Bereich Cybersicherheit/ IT, darunter 400 aus dem Bildungssektor, die zwischen Januar und März 2023 durchgeführt wurde. Die Befragten stammen aus 14 Ländern in Nord- und Südamerika, EMEA und dem asiatisch-pazifischen Raum. Die interviewten Unternehmen beschäftigen zwischen 100 und 5.000 Mitarbeiter und generieren einen Umsatz zwischen weniger als 10 Millionen und mehr als 5 Milliarden US-Dollar.

Die Sophos-Studie „State of Ransomware 2023" steht unter sophos.com als Download zur Verfügung.

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

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