Bildungssektor gut gewappnet gegenüber Ransomware – auf Kosten seines IT-Personals

Der Sophos State of Ransomware-Report belegt, dass der Bildungssektor sich gut gegenüber Ransomware-Angriffen aufgestellt hat: 97 Prozent der von Datenverschlüsselung betroffenen Einrichtungen konnten ihre Daten wiederherstellen und Lösegeldzahlungen sanken rapide. Doch der Erfolg hat auch eine Kehrseite: das Personal ist am Limit.

Die Ergebnisse des jährlichen „Sophos State of Ransomware in Education" liegen vor und belegen, dass der Bildungssektor messbare Fortschritte bei der Verteidigung gegenüber Ransomware-Angriffen gemacht hat: weniger Lösegeldzahlungen, drastisch gesunkene Kosten und schnellere Erholungsraten. Diese Ergebnisse gehen jedoch mit steigendem Druck auf die IT-Teams einher. Die Mitarbeiter berichten von Stress, Burnout und beruflichen Konflikten nach Angriffen – fast 40 Prozent der Befragten geben an, dass sie mit Ängsten zu kämpfen haben.

In den letzten fünf Jahren hat sich Ransomware zu einer der dringendsten Bedrohungen im Bildungsbereich entwickelt. Sowohl Grundschulen als auch weiterführende Bildungseinrichtungen werden von Cyberkriminellen als leichte Ziele eingestuft – oft unterfinanziert, unterbelegt und mit sehr sensiblen Daten. Die schwerwiegenden Konsequenzen sind gestörtes Lernen, knappe Budgets und eine wachsende Angst des Personals. Ohne stärkere Abwehrmaßnahmen riskieren Schulen nicht nur eine effektive Aufrechterhaltung des Schulalltags, sondern auch das öffentliche Vertrauen.

Anzeichen von Erfolg gegenüber Ransomware
Die aktuelle Sophos-Studie beinhaltet allerdings einen Lichtblick, hat der Bildungssektor doch insbesondere seine Fähigkeiten bei Reaktion und Antwort auf Ransomware-Attacken verbessert und zwingt damit die Cyberkriminellen, ihre Angriffe weiterzuentwickeln. Die Daten zeigen einen Anstieg von Angriffen, bei denen Angreifer versuchen, Geld zu erpressen, ohne Daten zu verschlüsseln. Zwar werden Lösegelder noch immer von über der Hälfte der Betroffenen gezahlt, allerdings sinken die Zahlungsbeträge rapide. Diejenigen Einrichtungen, die eine Datenverschlüsselung verzeichnen mussten, waren zu 97 Prozent in der Lage, ihre Daten zu retten.

Die Reportanalyse ergibt mehrere wichtige Indikatoren für den Erfolg im Kampf gegen Ransomware im Bildungswesen:

- **Verhindern weiterer Angriffe**: Bei der Abwehr von Angriffen bevor Dateien verschlüsselt werden können, melden sowohl weiterführende Schulen als auch Hochschulen ihre höchste Erfolgsquote seit vier Jahren (67 Prozent bzw. 38 Prozent der Angriffe).
- **Geringere Lösegeldzahlungen**: Im letzten Jahr sanken die Lösegeldforderungen um 73 Prozent (ein durchschnittlicher Rückgang von 2,4 Millionen Euro), während die durchschnittlichen Zahlungen im Primar- und Sekundarschulbereich von 5,1 Millionen Euro auf 682.000 Euro und im Hochschulbereich von 3,4 Millionen Euro auf 395.000 Euro sanken.
- **Sinkende Wiederherstellungskosten**: Abgesehen von Lösegeldzahlungen sanken die durchschnittlichen Wiederherstellungskosten im Hochschulbereich um 77 Prozent und im Grundschulbereich um 39 Prozent. Trotz dieses Erfolgs meldet der Grundschulbereich die höchsten Wiederherstellungskosten aller untersuchten Branchen.

Klassische Sicherheitslücken weiter im Fokus
Während der Bildungssektor Fortschritte darin macht, die Auswirkungen einer Ransomware-Attacke zu verringern, bleibt gerade bei den Schutzvorrichtungen noch einiges zu tun: Die Sophos Studie dokumentiert, dass 64 Prozent der Betroffenen fehlende oder ineffiziente Schutzmaßnahmen beklagen. 66 Prozent verweisen auf einen Mangel an Personal (entweder Fachwissen oder Kapazität), um Angriffe stoppen zu können. 67 Prozent geben Sicherheitslücken zu. Diese Risiken betonen die dringende Notwendigkeit für Schulen, sich auf Prävention zu konzentrieren, da Cyberkriminelle neue Techniken entwickeln, darunter auch KI-gestützte Angriffe.

Weitere Erkenntnisse der Studie:

- **KI-gestützte Bedrohungen**: Grundschulen berichten, dass 22 Prozent der Ransomware-Angriffe ihren Ursprung in Phishing hatten. Da KI überzeugendere E-Mails, Sprachbetrug und sogar Deepfakes ermöglicht, laufen Schulen Gefahr, zu Testfeldern für neue Taktiken zu werden.
- **Wertvolle Daten**: Hochschuleinrichtungen, die über KI-Forschungsdaten und große Sprachmodell-Datensätze verfügen, bleiben ein bevorzugtes Ziel, wobei ausgenutzte Schwachstellen (35 Prozent) und Sicherheitslücken, die dem Anbieter nicht bekannt waren (45 Prozent), die wichtigsten Schwachstellen sind, die von Angreifern ausgenutzt wurden.
- **Menschliche Opfer:** Jede Einrichtung mit verschlüsselten Daten meldete Auswirkungen auf das IT-Personal. Mehr als jeder vierte Mitarbeiter nahm nach einem Angriff Urlaub, fast 40 Prozent geben an, unter erhöhtem Stress zu leiden, und mehr als ein Drittel fühlt sich schuldig, weil sie die Sicherheitsverletzung nicht verhindern konnten.

„Ransomware-Attacken in Bildungseinrichtungen stören nicht nur den Unterricht, sondern auch die Gemeinschaft aus Schülern, Familien und Lehrern“, führt Alexandra Rose, Director, CTU Threat Research, Sophos aus. „Während es ermutigt zu sehen, dass Schulen ihre Reaktionsfähigkeit verbessern, muss doch die eigentliche Priorität darin bestehen, diese Angriffe von vornherein zu verhindern. Dies erfordert eine solide Planung und enge Zusammenarbeit mit vertrauenswürdigen Partnern, insbesondere da die Angreifer neue Taktiken anwenden, darunter auch KI-gesteuerte Bedrohungen.“

Konzentration auf die bisherigen Erfolge
Basierend auf ihrer Arbeit zum Schutz Tausender Bildungseinrichtungen empfehlen die Experten von Sophos verschiedene Maßnahmen, um einen möglichst effektiven Schutz gewährleisten zu können:

- **Fokus auf Prävention**: Der große Erfolg der Schulen bei der Abwehr von Ransomware-Angriffen bevor die Angreifer Daten verschlüsseln können, liefert eine Blaupause für größere Organisationen des öffentlichen Bereichs. Diese müssen ihre Bemühungen zur Erkennung und Reaktion mit der Prävention von Angriffen verbinden, bevor diese die Organisation gefährden.
- **Strategien vereinheitlichen**: Bildungseinrichtungen sollten koordinierte Ansätze für ihre weitläufigen IT-Umgebungen verfolgen, um Sichtbarkeitslücken zu schließen und Risiken zu reduzieren, bevor Angreifer diese ausnutzen können.
- **Mitarbeiter entlasten:** Ransomware stellt eine große Belastung für IT-Teams dar. Schulen können den Druck reduzieren und ihre Kapazitäten erweitern, indem sie mit vertrauenswürdigen Anbietern für Managed Detection and Response (MDR) zusammenarbeiten.
- **Reaktion stärken**: Selbst mit einer stärkeren Prävention müssen Schulen darauf vorbereitet sein, bei Vorfällen zu reagieren. Sie können sich schneller erholen, indem sie dedizierte Pläne für die Reaktion auf Vorfälle erstellen, Simulationen durchführen,

um sich auf reale Szenarien vorzubereiten, und ihre Bereitschaft mit 24/7/365-Diensten wie MDR verbessern.

Über die Studie
Die Daten für „State of Ransomware in Education“ basieren auf einer unabhängigen, anbieterneutralen Befragung von 441 IT- und Cybersicherheitsverantwortlichen, die im letzten Jahr Opfer einer Ransomware-Attacke wurden; 243 aus Grund- und weiterführenden Schulen, 198 aus Hochschulen. Die befragten Organisationen beschäftigen jeweils zwischen 100 und 5.000 Mitarbeiter in 17 Ländern. Die Erhebung wurde zwischen Januar und März 2025 durchgeführt. Grundlage waren die Erfahrungen der Befragten aus den vergangenen zwölf Monaten.

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

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