Bildungssektor von Ransomware besonders betroffen

Laut einer Studie von Sophos erfolgten 2020 im Bildungssektor die meisten Angriffe und es entstanden die höchsten Wiederherstellungskosten

Sophos untersucht in seiner Studie "Sophos State of Ransomware in Education 2021" das Ausmaß und die Auswirkungen von Ransomware-Angriffen auf Bildungseinrichtungen weltweit im Jahr 2020.

Die jüngsten Ransomware-Angriffe, die sich auch auf den Bildungsbereich auswirken, bestätigen die Forschungsergebnisse der Sophos-Studie und die besondere Anfälligkeit von Bildungseinrichtungen für Cyber-Bedrohungen. So sorgte der REvil-Ransomware-Angriff via Kaseya bei Schulen in Neuseeland für Wirbel, das FBI sowie das britischen National Cyber Security Centre sprechen Warnungen für den Bildungssektor aus und auch das BSI hat sich das sichere Arbeiten im digitalen Schulalltag auf seine Fahnen geschrieben.

Die wichtigsten Forschungsergebnisse im Überblick:

- Das Bildungswesen war zusammen mit dem Einzelhandel im Jahr 2020 am stärksten von Ransomware-Angriffen betroffen (44 Prozent der Unternehmen im Vergleich zu 37 Prozent über alle Branchen hinweg).
- Für Bildungseinrichtungen waren die finanziellen Auswirkungen eines Ransomware-Angriffs im Jahr 2020 besonders lähmend. Die Gesamtrechnung für die Behebung eines Ransomware-Angriffs im Bildungssektor, unter Berücksichtigung von Ausfallzeiten, Personalzeit, Gerätekosten, Netzwerkkosten, entgangenen Geschäftsmöglichkeiten, gezahltem Lösegeld und mehr, lag im Durchschnitt bei 2,73 Millionen US-Dollar – der höchste Wert über alle untersuchten Sektoren und 48 Prozent über dem weltweiten Durchschnitt.
- Mehr als die Hälfte (58 Prozent) der Bildungseinrichtungen, die von Ransomware betroffen waren, gaben an, dass es den Angreifern gelungen sei, ihre Daten zu verschlüsseln.
- Mehr als ein Drittel (35 Prozent) der betroffenen Einrichtungen gaben den Forderungen der Angreifer nach und zahlten das Lösegeld. Nur in den Sektoren Energie, Öl/Gas und Versorgungsunternehmen (43 Prozent) sowie die Kommunalverwaltung (42 Prozent) waren mehr Erpresste bereit zu zahlen.
- Die durchschnittliche Lösegeldzahlung betrug 112.435 US-Dollar (niedriger als der weltweite Durchschnitt von 170.404 US-Dollar). Diejenigen, die zahlten, erhielten jedoch im Durchschnitt nur etwa zwei Drittel (68 Prozent) ihrer Daten zurück, wobei fast ein Drittel der Daten unzugänglich blieben. Nur 11 Prozent erhielten alle verschlüsselten Daten zurück.
- Von den Institutionen, die im letzten Jahr nicht von Ransomware betroffen waren (55 Prozent der Befragten), erwarten mit 61 Prozent mehr als die Hälfte der Befragten, dass sie in Zukunft zur Zielscheibe werden. Als Hauptgründe dafür gaben sie an, dass Cyberangriffe mittlerweile so ausgeklügelt (meinten 46 Prozent) und weit verbreitet (meinten 42 Prozent) sind, dass sie kaum noch zu stoppen sind.

„Der Bildungssektor ist schon lange ein attraktives Ziel für Cyber-Kriminelle", sagt Chester Wisniewski, Principal Research Scientist bei Sophos. „Die Budgets für IT und Cybersicherheit sind oft sehr knapp bemessen und die IT-Teams kämpfen mit begrenzten Tools und Ressourcen, um die oft veraltete Infrastruktur zu schützen. Hinzu kommt das riskante Verhalten der Endbenutzer, wie z.B. das Herunterladen von Raubkopien. All diese Faktoren

erhöhen das Risiko ohnehin in jedem Jahr. Im Pandemie-Jahr 2020 mussten Bildungseinrichtungen aber außerdem kurzfristig auf virtuelle Lernumgebungen umstellen. Zeit, um über Sicherheit nachzudenken oder grundlegende Cybersicherheitsschulungen für alle neu hinzugekommenen Benutzer durchzuführen blieb dabei nur sehr wenig. Dies hat die Anfälligkeit des Sektors noch einmal erheblich gesteigert. Angreifer nutzten diese Gelegenheit schnell und ließen die Opfer beim Aufbau der IT-Infrastruktur von Grund auf mit enormen finanziellen Auswirkungen zurück. Um das Netzwerk vor Ransomware zu schützen, raten wir IT-Teams, ihre Ressourcen auf drei kritische Bereiche zu konzentrieren: den Aufbau einer stärkeren Abwehr gegen Cyberbedrohungen, die Einführung von Sicherheitsschulungen für Benutzer und, wo möglich, die Investition in eine widerstandsfähigere Infrastruktur."

Das vollständige Dokument „Sophos State of Ransomware in Education 2021" ist verfügbar unter:
https://www.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-in-education-2021-wp.pdf

Über die Studie:
Für die Studie "Sophos State of Ransomware in Education, 2021" wurden 5.400 IT-Entscheider, darunter 499 IT-Manager im Bildungswesen, in 30 Ländern in Europa, Nord- und Südamerika, Asien-Pazifik und Zentralasien, dem Nahen Osten und Afrika befragt.

Neu: 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