



## Ransomware-Angriffe im Bildungssektor überdurchschnittlich hoch

*Weitere Ergebnisse des Reports [The State of Ransomware in Education 2024](#): Auch die Zahl kompromittierter Backups sowie die Datenverschlüsselungsraten durch Ransomware sind im Vergleich zum Vorjahr gestiegen. Die Wiederherstellungskosten nach einem Angriff waren sogar doppelt bzw. viermal so hoch.*

Laut aktuellen Zahlen des Sophos-Reports [The State of Ransomware in Education 2024](#) sind Bildungseinrichtungen nach wie vor stark von Ransomware und deren Auswirkungen gefährdet. Zwar sind im Vergleich zum Vorjahr die Ransomware-Angriffe auf Organisationen im unteren Bildungsbereich (Schulen) von 80 Prozent auf 63 Prozent und im oberen Bildungsbereich (Hochschulen) von 66 Prozent auf 79 Prozent gesunken, doch die Angriffsraten liegen nach wie vor über dem weltweiten, branchenübergreifenden Durchschnitt von 59 Prozent.

### **Zweithöchste Rate bei kompromittierten Backups**

95 Prozent der Bildungseinrichtungen, die im vergangenen Jahr von Ransomware betroffen waren, gaben an, dass die Cyberkriminellen während des Angriffs versuchten, ihre Backups zu kompromittieren. Davon waren 71 Prozent erfolgreich, was nach dem Energie-, Öl-/Gas- und Versorgungssektor die zweithöchste Rate an erfolgreichen Backup-Kompromittierungen in allen Sektoren darstellt.

### **Datenverschlüsselungsraten weiter gestiegen**

85 Prozent der Ransomware-Angriffe auf Einrichtungen im unteren Bildungsbereich und 77 Prozent auf Einrichtungen im oberen Bildungsbereich führten im letzten Jahr zu einer Datenverschlüsselung, das sind etwas mehr als 81 Prozent bzw. 73 Prozent im Vorjahr. Für Bildungseinrichtungen ist dies das zweite Jahr in Folge, in dem die Verschlüsselungsrate gestiegen ist. Nur bei den Landes- und Kommunalbehörden war die Wahrscheinlichkeit mit 98 Prozent höher, dass die Daten bei einem Angriff verschlüsselt werden.

### **Kostenexplosion für die Wiederherstellung**

Die durchschnittlichen Kosten für die Behebung eines Ransomware-Angriffs beliefen sich 2024 bei Organisationen im unteren Bildungsbereich auf 3,76 Millionen US-Dollar, mehr als doppelt so viel wie im Jahr zuvor (1,59 Millionen US-Dollar). Organisationen aus dem oberen Bildungsbereich meldeten durchschnittliche Kosten von 4,02 Millionen US-Dollar, fast viermal so viel wie im Jahr 2023 (1,06 Millionen US-Dollar).

### **Nutzung von Backups steigt, leider aber auch die Bereitschaft für Lösegeldzahlungen**

62 Prozent der Befragten aus dem unteren Bildungssektor zahlten das Lösegeld, um verschlüsselte Daten zurückzubekommen, während 75 Prozent verschlüsselte Daten mithilfe von Backups wiederherstellten. 67 Prozent der Einrichtungen aus dem höheren Bildungsbereich zahlten das Lösegeld für die Wiederherstellung von Daten, während 78 Prozent Backups verwendeten. Die Drei-Jahres-Sicht auf den Bildungssektor zeigt eine Zunahme der Backup-Nutzung. Im Jahr 2023 gehörte der Hochschulbereich zu den drei Sektoren mit den niedrigsten Backup-Nutzungen weltweit und kletterte 2024 auf den zweiten Platz, neben den Landes- und Kommunalbehörden. Leider hat die Bereitschaft, das Lösegeld zu zahlen, in den letzten drei Jahren sowohl für Organisationen aus dem unteren als auch dem oberen Bildungsbereich schrittweise zugenommen.

## **Die Opfer zahlen selten die ursprünglich geforderte Lösegeldsumme**



Nur 13 Prozent der von Ransomware betroffenen Einrichtungen gaben an, dass die Höhe ihrer Zahlung der ursprünglichen Forderung entsprach. 32 Prozent der Befragten aus dem unteren Bildungsbereich und 20 Prozent der Befragten aus dem oberen Bildungsbereich zahlten weniger als ursprünglich gefordert; 55 Prozent der Einrichtungen aus dem unteren Bildungsbereich und 67 Prozent der Hochschuleinrichtungen zahlten mehr Lösegeld als gefordert. Weltweit ist die Hochschulbildung der Sektor, in dem am ehesten mehr gezahlt wird als ursprünglich von den Erpressern gefordert.

## **Über die Studie**

Die Daten der Studie „State of Ransomware in Education 2024“ stammen aus einer herstellerunabhängigen Umfrage unter 5.000 Führungskräften im Bereich Cybersicherheit/IT, die zwischen Januar und Februar 2024 durchgeführt wurde. Die Befragten stammten aus 14 Ländern in Nord- und Südamerika, EMEA und dem asiatisch-pazifischen Raum. 500 Unternehmen aus Deutschland standen Rede und Antwort. 600 Befragte kamen aus Bildungseinrichtungen, aufgeteilt in 300 aus dem unteren Bildungssektor (Schüler bis 18 Jahre) und 300 aus dem oberen Bildungssektor (Studenten über 18 Jahre). Alle Befragten repräsentieren Unternehmen mit 100 bis 5.000 Mitarbeitern. Die Umfrage wurde von Januar bis Februar 2024 vom Forschungsspezialisten Vanson Bourne durchgeführt, und die Teilnehmer wurden gebeten, auf der Grundlage ihrer Erfahrungen im Vorjahr zu antworten.

## **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](https://twitter.com/sophos_info)

## **Pressekontakt:**

Sophos

Jörg Schindler, Senior PR-Manager EMEA Central

[joerg.schindler@sophos.com](mailto:joerg.schindler@sophos.com), +49-721-25516-263

TC Communications

Arno Lucht, +49-8081-954619

Thilo Christ, +49-8081-954617

Ulrike Masztalerz, +49-30-55248198

Ariane Wendt +49-172-4536839

[sophos@tc-communications.de](mailto:sophos@tc-communications.de)