Vier Schritte zur **Bewältigung von Cyberrisiken im Hochschulwesen**

Der dramatische Anstieg von Ransomware-Angriffen und anderen Verstößen gegen die Cybersicherheit stellt für Hochschulen und die Cyberversicherer, mit denen sie Verträge abgeschlossen haben, eine Katastrophe dar.

Steigende Risiken und wie man darauf reagiert

Der Bildungssektor ist nach wie vor überproportional häufig von Ransomware und anderen Angriffen betroffen.[1] Hochschulen stehen zudem vor besonderen IT-Herausforderungen, darunter spezielle aufsichtsrechtliche Anforderungen seitens unterschiedlicher Interessengruppen aus Wissenschaft, Verwaltung, Forschung und Gesundheitswesen.

Gleichzeitig haben höhere Lösegeldforderungen bei Ransomware-Angriffen, die sich im letzten Jahr mit durchschnittlich 2,2 Millionen USD pro Angriff mehr als verdoppelt haben[2] – für Cyberversicherer ähnliche Auswirkung wie Naturkatastrophen für andere Versicherer. „Auf Extremzustände, sei es beim Wetter oder Risiko, reagiert die Branche mit entsprechend höheren Versicherungsbeiträgen", sagt Stephen Singh, der bei Zscaler den Bereich Fusionen, Übernahmen, Desinvestitionen, Private Equity und Cyberrisiken leitet.

Angesichts dieser Faktoren sollten die Verantwortlichen im Hochschulwesen die Cybersicherheitslage ihrer Einrichtungen verbessern, Cyberrisiken mindern und die Wahrscheinlichkeit erfolgreicher Angriffe verringern. Dazu sind vier Schritte erforderlich:

1. Implementierung von Best Practices und Kontrollen

Der erste Schritt zur Verbesserung des Cybersicherheitsstatus – und damit zur Verringerung des Risikos für Versicherer – besteht darin, sicherzustellen, dass Ihr Institut die branchenspezifischen Best Practices befolgt. Diese reichen von Endpunktsicherheit und Multifaktor-Autorisierung (MFA) über das Patchen vorhandener Systeme, zuverlässige Backups und die Verhinderung von Datenverlusten bis hin zur Schulung von Studierenden und Mitarbeitern.

Mehrere Studien haben ergeben, dass diese Praktiken bei vielen Unternehmen entweder gar nicht oder falsch umgesetzt werden.

„Die effektive Umsetzung ist sehr wichtig, insbesondere wenn Sie versuchen, Risiken zu messen, zu verwalten und zu versichern", bekräftigt Singh.

Dokumentieren Sie die implementierten Kontrollen und Strategien sowohl für den internen Gebrauch als auch für Cyberversicherer. „Die bloße Implementierung reicht nicht aus", mahnt Singh an. „Setzen Sie sie mit einer Zuordnungsebene ein, die für Ihr Unternehmen und diejenigen, die diese Informationen möglicherweise zur Urteilsbildung verwenden, aussagekräftig ist."

2. Umstellung auf Zero Trust

Im Hinblick auf die Cyberabwehr haben die meisten Institutionen „eine harte Außenschale und ein sehr weiches Inneres" geschaffen, meint Singh. „Wenn böswillige Akteure diese harte Schale erst einmal durchbrochen haben, können sie sich ungehindert bewegen."

Stattdessen sollten Institutionen Zero Trust als Sicherheitsrahmen übernehmen. Zero Trust ist ein Ansatz, der die Identität jedes Users beim Navigieren durch das Netzwerk ständig überprüft. Singh betont, dass es sich dabei nicht um ein Produkt, sondern um einen Prozess handle.

Eine Zero-Trust-Architektur gewährleistet, dass User nur auf die Systeme und Daten zugreifen können, die sie benötigen. Dadurch wird die Wahrscheinlichkeit, dass ganze Systeme oder Datenspeicher kompromittiert werden, deutlich verringert. „Wenn Sie Ihre Angriffsfläche reduzieren, die laterale Ausbreitung verhindern und Datenverluste stoppen, verringern Sie das Risiko für Ihr System enorm", erläutert Singh.

Auf Zero Trust basierende IT-Architekturen liefern außerdem Analyse- und Telemetriedaten, um verdächtiges Verhalten kontinuierlich zu überwachen und je nach potenziellem Risiko automatisch zu reagieren. Künstliche Intelligenz und maschinelles Lernen (KI/ML) ergänzen diese Fähigkeiten und stellen zugleich Empfehlungen dazu bereit, in welchen Bereichen Institutionen Zeit und Ressourcen investieren sollten.

3. Quantifizierung von Cyberrisiken

Der nächste Schritt erfordert einen Mentalitätswandel seitens der Institutionen. Die Quantifizierung von Cyberrisiken stellt einen Paradigmenwechsel dar, da Risiken aus finanzieller Perspektive bewertet werden. Institutionen nutzen Risikobewertungen und Analysen, um die potenziellen Kosten eines Verstoßes vorherzusagen – oft in zweistelliger Millionenhöhe.

„Dieser Grad der Differenzierung ermöglicht Ihnen einen viel besseren Einblick in Ihr tatsächliches Risiko", so Singh.

Auf dieser Grundlage ermitteln die Institutionen, inwieweit sich diese Verluste durch Investitionen in unterschiedliche Cybersicherheitsstrategien verringern lassen. „Jeder dieser Schritte ist eine Möglichkeit, die Kosten auf einen niedrigeren Betrag zu reduzieren", erläutert Singh, „basierend darauf, wie viel potenziellen finanziellen Verlust Sie mit den von Ihnen implementierten Kontrollen abmildern können."

Durch die Konzentration auf finanzielle statt auf technologische Fragen ermöglicht die Quantifizierung von Cyberrisiken Führungskräften im Bildungswesen, Strategien aus betriebswirtschaftlicher Perspektive zu diskutieren. „Dadurch wird das Thema für die oberste Führungsebene und den Vorstand verständlich", so Singh. „Auf dieser Basis wird eine zielführende Diskussion mit Ihrem Führungsteam über die Neuausrichtung Ihrer Investitionsstrategie zur Abwehr von Cyberrisiken möglich."

In diesen auf Daten basierenden Gesprächen legen die Führungskräfte fest, wie hoch das finanzielle Risiko ist, das das Institut einzugehen bereit ist bzw. das es durch Investitionen in Cybersicherheitskontrollen mindern oder an Cyberversicherungen übertragen kann.

„Die Betrachtung des finanziellen Verlusts führt Sie zur besten statt zur erstbesten Wahl. Je mehr Sie das Risiko mindern können, desto weniger Risiko müssen Sie akzeptieren und desto weniger müssen Sie an den Versicherer übertragen", sagt Singh. „Dadurch lassen sich auch die Cyberversicherungsbeiträge senken, weil man nun die gleiche Sprache spricht."

65 % der Unternehmen verfügen noch immer nicht über einen Cyber-Resilienz- oder Vorfallreaktionsplan, um auf Angriffe reagieren zu können, die in Bildungseinrichtungen so gut wie unvermeidlich sind.

4. Zusammenarbeit mit Cyberversicherungen

Die Leistungen von Cyberversicherern gehen über die Deckung von Datenschutzverletzungen und Angriffen hinaus. Viele bieten mittlerweile ein breites Spektrum an Dienstleistungen an, darunter Risikobewertung und -technik, Reaktion auf Vorfälle und Managed Services. Einige bieten im Falle eines Verstoßes sogar Rechtsberatung und Unterstützung bei der Presse- und Öffentlichkeitsarbeit an.

Seien Sie auf den Ernstfall vorbereitet

Hinsichtlich der akuten Bedrohungslage dürfen Sie sich keinen Illusionen hingeben. Laut Singh verfügen 65 % der Unternehmen immer noch nicht über einen Cyber-Resilienz- oder Vorfallreaktionsplan, um auf Angriffe reagieren zu können, die in Bildungseinrichtungen so gut wie unvermeidlich sind.

„Jede Einrichtung sollte davon ausgehen, dass sie bereits kompromittiert wurde oder jederzeit kompromittiert werden kann, und einen Aktionsplan haben", betont er. „Die Bedrohungen, Risiken, Schwachstellen, Verstöße und Erpressungen haben sich noch nie so schnell verändert wie heute. Überlegen Sie, welches Modell das richtige ist, damit Sie mit Ihrem begrenzten Budget in Ihrem gesamten Umfeld den größtmöglichen ROI erzielen."

Fußnoten:
1. https://news.sophos.com/en-us/2023/07/20/the-state-of-ransomware-in-education-2023/
2. https://www.zdnet.com/article/ransomware-payments-heres-how-much-falling-victim-will-now-cost-you/

Dieser Beitrag wurde vom Center for Digital Education Content Studio mit Informationen und Unterstützung von Zscaler verfasst und erstellt.

Verfasser: CENTER FOR DIGITAL EDUCATION

Das Center for Digital Education ist ein nationales Forschungs- und Beratungsinstitut, das sich auf Technologietrends, Bildungspolitik und Finanzierung im Schul- und Hochschulbereich spezialisiert hat. Das Center liefert Führungskräften im Bildungs- und Industriebereich Entscheidungshilfe und umsetzbare Erkenntnisse zur effektiven Integration zukunftsfähiger Technologien.

www.centerdigitaled.com

Gesponsert von: zscaler™ aws

Zscaler, ein AWS Advanced Tier-Softwarepartner, ist die weltweit größte Inline-Sicherheits-Cloud-Plattform. Die Zscaler Zero Trust Exchange fungiert als Schaltzentrale, die User standort- und geräteunabhängig sicher direkt mit Anwendungen und Workloads (niemals mit dem Netzwerk) verbindet und so branchenführende Zero-Trust-Sicherheit gewährleistet. Zscaler reduziert Geschäftsrisiken, verbessert die User-Produktivität und nutzt branchenführende KI-gestützte betriebswirtschaftliche und cybertechnische Erkenntnisse, um Daten in Wissen umzuwandeln. Durch proaktives Digital Experience Monitoring bleiben die User produktiv und die Anzahl der Support-Tickets wird reduziert. Darüber hinaus eliminiert Zscaler die Kosten, Komplexität und Sicherheitsrisiken, die mit herkömmlichen VPNs, Firewalls und Einzelprodukten verbunden sind.

www.zscaler.de

ADOBESTOCK.COM