Cyber Security

Wie sicher sind Bildungseinrichtungen?

[18.07.2023] Sind Schulen, Universitäten und Forschungsinstitute tatsächlich verstärkt im Visier von Cyber-Kriminellen? Und wenn ja: Woran liegt das? Fünf IT-Sicherheitsexperten aus fünf Unternehmen geben ihre Einschätzung zur Risikolage im Bildungssektor.

Nicht nur Unternehmen, Versorgungsbetriebe und Behörden werden immer wieder Ziel von Cyber-Angriffen – auch Bildungsinstitute scheinen zunehmend betroffen. Zumindest die Schlagzeilen legen diesen Befund nahe: So zum Beispiel angesichts eines Angriffs auf sieben Schulen in der Stadt Karlsruhe, das Münchner Helmholtz-Zentrum oder flächendeckende Attacken auf Hochschulen in Nordrhein-Westfalen. Doch erobern sich Hacker wirklich zunehmend Schulen, Universitäten und Forschungseinrichtungen? Und wenn ja: warum? Die meisten Experten sehen Schulen, Universitäten und andere Bildungseinrichtungen nicht als vorrangige, attraktive Ziele für Hacker. Generell suchen Cyber-Kriminelle zunächst nach Schwachstellen und erst dann nach Branchen. Dennoch sehen die Experten durchaus eine gewisse Attraktivität von Bildungsinstitutionen – was nicht nur mit mangelnden IT-Ressourcen zu tun hat.

Unis und Forschung als lohnende Opfer

Nach Einschätzung von Tom Haak, CEO beim IT-Sicherheitsunternehmen Lywand, wissen Hacker meist gar nicht, welche Einrichtungen sie angreifen. Cyber-Kriminelle arbeiten kaum zielgerichtet, sondern operieren nach dem Prinzip der Nutzenmaximierung, indem sie ihre Angriffskampagnen breit und automatisiert ausrollen. Sie suchen nicht gezielt den Weg in bestimmte Branchen, sondern den Weg des geringsten Widerstands. Die IT-Architekturen an Universitäten, Schulen oder Forschungsinstituten sind im gleichen Maße gefährdet wie die IT von kleinen und mittelständischen Unternehmen, meint Thomas Krause, Regional Director DACH beim Cyber-Sicherheitsspezialisten ForeNova. „Hacker wissen, dass sich auch Bildungsträger eine Unterbrechung ihres Betriebs und vor allem einen Vertrauensverlust in einer sensiblen Öffentlichkeit durch Offenlegen personenbezogener Daten nicht erlauben können. Für ihre Erpressungsgelder können sie also eine grundsätzliche Zahlungsbereitschaft vermuten.“ Eine Schule mag für Hacker vielleicht wirtschaftlich nicht sehr interessant sein, eine Universität aber durchaus.
Zu ähnlichen Schlüssen kommt Ari Albertini, CEO beim Datensicherheitsunternehmen FTAPI Software. Schulen erwische es oft aufgrund von Phishing-Mails oder aktueller Cyber-Viren. „Allerdings werden auch Schulen immer digitaler und öffnen damit neue Einfallstore. Anders bei Universitäten und Hochschulen: Sie verarbeiten kritische Daten aus der Forschung und Entwicklung, die für Cyber-Kriminelle sehr lukrativ sein können.“ Zudem verfügen Universitäten auch über mehr Budget. Ähnlich ist die Lage bei Forschungsinstituten: Einrichtungen, die sich etwa mit KI befassen, versprechen kapitalisierbare Informationen, sie verfügen über die finanziellen Mittel und verspüren genügend Druck, um auch ein hohes Lösegeld schnell bezahlen zu können. Für Albertini gehen Hacker durchaus auch Branchen gezielt an: „Die Cyber-Kriminellen eignen sich Wissen über bestimmte Branchen an und nutzen dieses, um gefundene Schwachstellen bestmöglich auszunutzen.“

Bildungseinrichtungen bieten viel Angriffsfläche

Michael Eder, Business Development Manager beim Hardware-Distributor Concept International, der auch im Bildungsbereich tätig ist, sieht Bildungseinrichtungen „nicht auf den beliebtesten Plätzen bei Hackerangriffen, weil weniger geschäftskritische Schäden verursacht werden als bei einem multinationalen Konzern“. Dennoch gebe es spezifische Risiken und Motivationen für den direkten Zugriff auf Hardware. Das liege einerseits an einem oft laxen Umgang mit Sicherheitsstandards, aber auch daran, dass Whiteboards, Konferenzeinrichtungen, Informations- und Kontaktdisplays im öffentlichen oder halböffentlichen Raum direkt zugänglich sind. Zudem sei nicht jeder Hacker auf Geld aus – oft reiche als Motivation der Erfolg.
Bogdan Botezatu, Director of Threat Research and Reporting bei Bitdefender erkennt Konkurrenzmechanismen unter Hackern als einen Grund für zunehmende Angriffe auf Bildungsinstitutionen. „Das Aufkommen von Malware-as-a-Service hat den natürlichen Wettbewerb um Ziele zwischen Cyber-Kriminalitätsgruppen verstärkt.“ Jede Branche, unabhängig von ihrer Größe, sei ein wertvolles Ziel für Cyber-Kriminelle. Sein Unternehmen sehe Forschung und Bildung daher auf Rang zwei der angegriffenen Branchen, mit einem Anteil von 22 Prozent, so Botezatu. Bildung und Forschung seien stärker im Fokus der Hacker als Regierungsbehörden (17 Prozent) oder Technologie-Unternehmen (13 Prozent). Und sie leben über viermal so gefährlich wie der Retail-Bereich (4 Prozent).
Bildungseinrichtungen haben zudem eine größere Angriffsfläche, die sich über Endpunkte, Server, BYOD und Cloud-Dienste erstreckt, die selten zentral verwaltet werden. „Kleine IT-Sicherheitsteams, die oft in Abteilungen mit Serviceleistungen eingegliedert sind, werden mit der Verteidigung solch großer Angriffsflächen überfordert. Nicht zuletzt sind die Sicherheitsbudgets klein und lassen nicht allzu viel Spielraum für Verbesserungen oder wenig Möglichkeiten für eine Gegenwehr.“

Gelegenheit macht (Daten)diebe

Auch wenn strittig ist, ob Hacker sich ihre Opfer gezielt suchen oder nicht – die Gefährdung nimmt zu. Für Tom Haak von Lywand „lässt sich eine allgemein erhöhte Bedrohungslage festhalten. Sie ist auch für den Bildungsbereich ein ernst zu nehmendes Phänomen“. So ist die unterschiedliche IT-Kompetenz von Bildungseinrichtungen ein Sorgenkind für die Experten. Für Ari Albertini von FTAPI steht die Digitalisierung des Bildungsbereiches noch am Anfang – und mit ihr die digitale Kompetenz der Mitarbeitenden. Hinzu kommt, dass digitale Angebote häufig zentral gesteuert oder vorgegeben werden – und dann vorausgesetzt wird, dass auch die IT-Sicherheit zentral gesteuert wird. Doch ein solches Mindestmaß an zentraler Sicherheit reicht nicht aus, wenn Malware über kompromittierte E-Mail-Anhänge oder Links direkt in das lokale System gelangt und sich die Verantwortlichen vor Ort dafür nicht zuständig fühlen, es nicht sein können oder es diese Zuständigen gar nicht gibt.
Fehlende IT-Sicherheitskompetenz und -ressourcen sind die Achillesferse der Systeme in diesem Bereich. Neben dem Healthcare-Bereich sind Forschung und Bildung die Sektoren, die am stärksten vom Personal- und Geldmangel in der IT betroffen sind, stellt Thomas Krause vom Cyber-Sicherheitsunternehmen ForeNova fest. „Universitäten und Schulen haben allein schon bei Grundlagen der Digitalisierung Nachholbedarf. Wie soll es da um die Lage der IT-Sicherheit besser bestellt sein?“ Hinzu komme, dass komplizierte Ausschreibeverfahren „zu einer gewissen Starre im Bildungsbereich führen, da neue Technologien nicht einfach ausprobiert werden können, selbst wenn sie nicht immersiv sind und mit anderen Lösungen zusammenarbeiten“.

(sib)

Stichwörter: IT-Sicherheit, Schul-IT, Hochschul-IT, Bitdefender, Concept International, Forenova, FTAPI, Lywand Security