Intelligent Risk-Based Security in Higher Ed

Hackers are targeting higher ed. This is what colleges can do about it.

Last year, when the Covid-19 virus was a global priority, UCSF's School of Medicine found itself under attack. Hackers had infiltrated servers used by its epidemiology and biostatistics departments, just as the university was hoping to develop a vaccine for Covid-19. Ultimately, UCSF agreed to pay a ransom of $1.14 million because the stolen data was, "important to some of the academic work we pursue as a university serving the public good."

Sensing vulnerability during the pandemic, hackers have targeted higher education. Colleges are facing an unprecedented wave of cyber espionage, email hacks and ransomware attacks. Malware and ransomware strikes are rocketing up by 300% every year, while brute force password attacks—where hackers try to guess users' passwords—rose by 100% over the past 12 months. The fact that some colleges have buckled and paid ransoms has driven the cost of attacks higher. In 2020, the average demand reached $447,000, an increase of 100% over 2019, and the education sector faces the highest recovery costs for ransomware attacks according to the latest Sophos report.

"A perfect storm"

Steve Faehl, security chief technology officer for Microsoft U.S., Public Sector says cyber criminals' focus on higher education creates (and feeds on) a unique set of issues. Like much of the public sector, colleges are subject to financial constraints.

"In many cases they have funding challenges combined with adversary attention, if you will, so that really is a perfect storm, which makes cyber security very difficult in the EDU space but also public sector overall," he says.

It's a terrifying prospect for university leaders; but there are solutions. Having a structured approach to long-term security is key, along with an overview of the institution's assets and the threats it is most likely to face. "What we advocate for institutions is to take a risk-based perspective," Faehl says.

Increasingly, colleges are adopting a zero trust security model (which is also promoted by the US government), renouncing implicit trust in any user or element and continually monitoring systems in search of malicious activity. This set of principles assumes that a worst-case scenario is not just likely but already

happening—that bad actors have breached the network, and that the college may already be the target of a ransomware attack.

When they successfully enter a system, hackers typically spend months lurking within it—figuring out its weakest spots and greatest vulnerabilities, almost as if it were a computer game.

> **"It's almost as if they're running through a maze, finding things that are valuable and encrypting them or rendering them useless in the environment before getting to the final stage, where they know that they have everything they need to make that environment cripple and force the victim to pay." Corey Lee, Zero Trust Architect at Microsoft**

This is why zero trust must be a board-level discussion, experts say. Zero trust is about applying appropriate levels of security. Building a house with a strong foundation is important but afterwards we also need to go back and ensure there are locks on the windows and doors. Review the Zero Trust Adoption report to learn more about the benefits of Zero Trust and how organizations across diverse markets and industries measure the impact of their Zero Trust journey.

Establishing a Safe Learning Environment

When the pandemic struck in spring 2020, education was pushed online and transformed forever. As colleges scrambled to maintain the quality of student learning, questions of security were far from the minds of administrators and educators. This fall, many institutions are operating with a blend of in-person and hybrid learning. With thousands of laptops and smartphones in use both on and off campus, and a revolving-door population of students, digital learning presents security teams with a complex landscape.

Bad actors like to wait for a critical moment, when school staff and IT teams are stressed and distracted, Corey Lee says. It may be just before the academic year begins, or in the midst of exams, when students are relying on certain applications to complete coursework or take their tests. If they cannot log in, or teaching cannot commence, it can create, "quite a frenzy," as Lee puts it.

What can colleges do? Solutions like Microsoft Defender can detect threats in emails, links and collaboration tools and prevent the loss of student data. Educational institutions can plan and map the types of controls and protections aligning to their specific needs with the help of Microsoft's Zero Trust assessment.

Trusted Research Spaces

Academic research is just as hard to protect. Intellectual property is desirable to hackers. Researchers may be targets, either because they are high-profile individuals, or because of their areas of expertise—such as Covid-19 treatments or military technologies like drones.

In addition, the densely networked nature of research makes it tricky for security teams to monitor, with scholars collaborating with colleagues at different institutions or working with various funding bodies. It is important for administrators to take an inventory, ensuring that they understand where platforms and IT for research are procured.

As Faehl puts it, centralized IT teams need to ask, — "Do I know that there is 10-year-old technology being used over here somewhere, sitting underneath someone's desk?"

To further minimize the likelihood of a breach, colleges can offer scholars trusted research environments, secure cloud-hosted spaces, to enable researchers to safely share data and expertise.

The Crown Jewels: Backups, Servers and SIS

The most critical piece of a higher education institution is its broader infrastructure, which underpins the entire digital environment, and supports learning outcomes and research. This is what Lee calls the "holy grail" for hackers. It may include student information systems (SIS), or backups.

"There's this concept of what we call the crown jewels — the most critical assets," he says. "Services that, if, for whatever reason become inaccessible, or if they are down, can have severe impact on operations as well as teaching and learning. What would that mean for an educational institution?"

Systems and behavior should be monitored, so that if for instance, an administrator appears to enter a secure environment and inexplicably starts deleting backups, alarms should be set to go off. Fortunately much of this can be automated with security solutions like Azure Sentinel, Lee notes. "We want to ensure that institutions don't just see blinking lights go off but that they can also take quick action in an automated fashion."

Time Saving

With some teams fielding millions of incidents a month, automation is a key part of security capabilities, liberating beleaguered security teams from completing the same manual tasks, over and over. Research published by Microsoft showed that better integrated security systems (like its Office 365) could save IT workers more than 27,000 hours each year.

With Microsoft, organizations can take advantage of security solutions like those found in its Microsoft 365 suite which include email and identity protection as well as a host of other tools to help

manage and protect data, devices and users. Microsoft Security offers guidance about how to optimize your Zero Trust strategy with an optimization model and the solutions tailored to your organization's specific needs. Additionally, a cloud service called Azure Sentinel allows institutions to get 24/7 monitoring included with their M365 security bundle. This service can be expanded to help monitor other systems or cloud environments using flexible pay-as-you go pricing.

"You have security teams that are already stretched," Faehl says, "digging up threat intelligence, remediating machines, cleaning out email inboxes, removing malicious mail. Utilizing our built-in automation you can do all of those things and now the analyst is able to achieve the 15 steps to remediate a device in the push of a button. Or set a policy to say, just do it for me."

Future proofing

Last May, the US government issued an executive order on cyber security, and it is insisting that organizations it partners with comply with standards like the Cyber Maturity Model Certification (CMMC). Institutions producing research for the government — working with the Department of Defense or developing software that becomes part of the broader IT supply chain — will need to comply with its requirements. In this way, the US government is using its buying power to move the industry forward.

Experts, including those working for the US government, expect the threat to grow and increase in complexity. Faehl says that individual hackers are now so well-funded that they can operate on par with nation states. This means that they can detect and exploit weaknesses with greater efficacy than before. "These are human operated, they're not automated campaigns, so you have a human at the keyboard, specifically looking to compromise your organization and hold your data for ransom."

Luckily security experts are becoming increasingly sophisticated in their response, leveraging AI and other capabilities to make their tools more powerful and sensitive. "Organizations that are able to utilize Microsoft technology don't have to worry about future proofing to achieve that zero trust strategy—they can know that each of our components is working towards that same objective," says Faehl.

Even for colleges burdened with legacy systems, securing their digital assets is possible, Faehl says. Every update improves the system. "Anywhere that you can modernize, modernize. Because modernization is security. We get better at protecting things as time goes on."

Countering hackers is a journey for colleges, Faehl observes. "This is not something that you light up overnight. The nice thing about the Microsoft ecosystem is that we are thinking about how to plug those pieces together holistically."

Read how the College of Southern Nevada is addressing a jump in cybersecurity threats. Contact your Microsoft representative for more information or to schedule a security workshop. Learn more at https://aka.ms./highered