Helping to Secure Education Networks

Schools and colleges are particularly vulnerable to attacks by cyber criminals. Here’s what education leaders can do to help prevent these incidents.

Education has become the second leading target in cyber security attacks, according to Trend Micro—and it’s not hard to understand why: They serve a diverse and highly susceptible population who connect to the network from a mix of devices, and in many cases their networks are not as well protected as those in other sectors.
Here are some of the most high-profile network security breaches among educational institutions since 2015 alone:

- **A public school district in South Carolina** reportedly had its network held for ransom by hackers who blocked access to the district’s computer system. The hackers used high-level encryption to lock up the district’s data, then demanded that the district pay nearly $10,000 via Bitcoin for the decryption key. District officials apparently decided to pay the ransom after considering the amount of time it would take to restore access to the files on their own.²

- **Additionally, a school district in Washington** was reportedly the victim of an email scam that compromised the personal information for more than 2,000 employees—including some 90 student workers under the age of 18. An email message, configured to look like it came from the district Superintendent, was apparently sent to an employee requesting a list of employee names, addresses, salary information, and Social Security numbers. The worker was fooled by the scam and supplied the requested information. The district is reportedly providing free credit monitoring services for all who were affected.³

- **Additionally, a university has dealt** with a series of expensive attacks that have crippled its network services. The attacks were launched by a hacker who calls himself “Exfocus,” an individual that claimed to have been paid by someone with an axe to grind against the university. After four such attacks during the 2014-15 school year, the university reportedly spent $3 million to upgrade its network security and was forced to raise tuition by 2.3 percent. But the upgrades failed to protect the university from another attack in September 2015, which once again prevented students and staff from accessing the Internet or any e-learning tools.⁴

These types of attacks can cause widespread harm, but there are steps that education leaders can take to help safeguard their networks from cyber criminals. This white paper will explore some of the most common threats to network security, as well as strategies for dealing with these threats successfully.

Educational has become the second leading target in cyber security attacks.¹
Why Are Schools and Colleges Such Attractive Targets?

A key reason educational institutions have become prime targets for hackers is because they’re often easier to attack than other entities. They retain hundreds or thousands of records with personally identifiable information, and yet their networks must allow access by a young, inexperienced, and largely mobile user base with a rapid turnover rate as new students cycle through.

“Schools have a lot of entry points to their network,” says Terry Hect, Chief Security Strategist for AT&T. “Students and faculty might be accessing the network with their own personal devices, for instance. There are many different vectors into the network that school IT staff might not be looking at.”

Not only are school networks often difficult to help secure, but resources also can pose a challenge—especially for public K-12 schools.

“The biggest problem that school districts face is a talent shortage,” Hect says. “They have very limited assets to identify and remediate problems in a timely manner. Additionally, the security technologies they use typically require a lot of care and feeding. Network security doesn’t just require a lot of skill; it also requires a significant amount of time.”

Most Common Types of Attacks

Schools and colleges may be vulnerable to many different kinds of attacks, and here are some of the most common.

Distributed Denial of Service (DDoS). A DDoS attack occurs when a hacker takes control of thousands of computers and aims them at a single server, overwhelming that network with traffic and ultimately knocking it offline.

DDoS attacks are very common; about one in five businesses reportedly have been hit with a DDoS attack, resulting in several hours of downtime. Common reasons for DDoS attacks include extortion, revenge, mischief, business competition, and hacktivism, or the act of breaking into a computer system for social or political purposes.

“Students are now able to buy their own DDoS attacks online and attack their own schools on any day they choose,” says Hect. “We’re seeing it frequently happen near test time; students will attack their school’s network so the tests are postponed.”

Ransomware. This is a type of malicious software, or malware, designed to block access to a computer system until a sum of money is paid to the person who unleashed it.

Ransomware is among the fastest-growing types of cybercrime. “In 2015 alone, we received about 2,400 of these complaints with a total estimated loss of about $24 million,” said Rich Jacobs of the FBI’s Cyber Division.
Phishing scams. These are typically fraudulent email messages appearing to come from a legitimate source, such as a bank, a service provider, or the recipient’s employer. The messages usually direct the recipient to a spoofed website or otherwise get him or her to divulge private information that can be used to commit identity theft or fraud.

Olympia School District was victimized by a certain type of phishing scam the FBI calls “CEO fraud,” in which the attacker skillfully mimics an email message from an employee’s manager or executive. The FBI recently issued a public service announcement warning that “CEO fraud” is on the rise, with corporate losses exceeding $3 billion since October 2013. The agency said it has seen a 270% increase in these so-called CEO scams since January 2015.7

Why Education Leaders Should Be Concerned
Network security breaches can be costly to rectify. They can result in the theft of students’ private information, putting schools in violation of the Family Educational Rights and Privacy Act (FERPA). They can do lasting damage to a school’s reputation and even result in liability lawsuits.

The Ponemon Institute estimates that the average cost of responding to a network security breach in higher education is $294 per student record, writes Rich Murphy for EDUCAUSE. That means the compromise of 10,000 student records would cost nearly $3 million to remediate. This figure doesn’t include the loss of revenue that could result from the negative publicity such a breach would generate.8

While DDoS attacks can cause far-ranging damage on their own, research suggests that they also open the door to secondary attacks. According to a survey by Kaspersky Lab, 32% of serious DDoS attacks coincided with a network intrusion, resulting in the loss or theft of sensitive data.9

“We Need Enterprise-Level Protection”

Pike County Schools

Having highly secure and reliable internet access is mission-critical for Kentucky’s Pike County Schools, as it is for most school systems nationwide. This district of about 8,500 students relies on Internet connectivity for its online state testing, as well as for daily instruction, communication through email and a Voice Over IP system, monitoring of IP-based surveillance cameras, and other operations.

“Technology is embedded throughout education now,” said Director of Technology Clayton Potter. “It’s just as essential as electricity or water. Teachers rely on the Internet for their lessons. You might as well close the school down if you don’t have a reliable connection.”

Pike County has invested heavily in its network infrastructure, with 1 Gigabit-per-second (Gbps) connections between buildings and a 10 Gbps pipeline to the Internet. Keeping this network safe from disruption is a key priority for Potter and his staff.

“We have to make sure we have technologies in place to keep intrusion out,” he said. “We need enterprise-level threat protection.” And AT&T’s DDoS Defense system is an important aspect of this security plan.

DDoS Defense is designed to block and remove malicious traffic in the cloud, before it reaches a school district’s network. The system helps thwart attacks in real time and keeps network services up and running.

The Kentucky Department of Education has supplied AT&T DDoS Defense for all of its K-12 districts. AT&T monitors the traffic flowing to each district’s network, and when there is evidence that an attack might be starting, the district is put into mitigation. All of this occurs so seamlessly that Potter has not had to worry about a Denial of Service attack since the service began.

“There have been a few instances where AT&T has notified us of a broadcast storm and has done some throttling or restriction for us,” he said. “But this all happens in the background, and we haven’t had to give it another thought.”

He added: “We have been really pleased with the service.”
Six Steps to Better Network Security

Fortunately, a combination of technology and common-sense practices can help lessen the dangers of security breaches. Here are six strategies for education leaders to consider.

1. Educate users. You could have the most up-to-date security technologies in place, but the easiest obstacles to breach are unsuspecting staff or students. Make sure you educate all network users to remain alert for possible email scams and verify all requests for sensitive information.

   If an executive or supervisor “appears to be emailing you for a list of company employees, check it out before you respond,” said IRS Commissioner John Koskinen in a press release. “Everyone has a responsibility to remain diligent about confirming the identity of people requesting personal information about employees.”

2. Keep all operating systems up to date, and apply regular security patches. If you’re still using older versions of operating systems that are no longer supported, you’re likely missing out on several security patches. This can make your network more prone to an attack.

3. Practice “defense in depth.” This is an IT security concept that involves multiple layers of defense, such as antivirus software, firewalls, intrusion detection systems, and more. “Defense in depth—using multiple technologies that help protect in different ways—is the cornerstone of a robust security plan,” Hect says. “If you don’t apply this concept, then I only have to figure out a way to get around one type of device. But if you implement a mix of technologies, then it’s much harder for malicious activity to exploit multiple types of devices.”

4. Consider using multifactor authentication. This is a security method in which users are only granted network access after successfully presenting two or more separate pieces of evidence to verify their identity, such as a password, an answer to a question, and/or a security token. Multifactor authentication provides more security than just password-protected access, however it’s also more costly to implement.

5. Pay attention to security in the cloud. “Cloud-based highly secure email and web filtering are very important,” Hect says. “A cloud security provider can scrub the malware out of a school’s email in the cloud, so only the clean, non-impacted email is delivered to your school.”

6. Invest in DDoS security. “You can’t fight a DDoS attack on your premises as your network becomes overwhelmed,” Hect says. “Even if you’re dropping all of that DDoS traffic at your gateway, sooner or later the pipe from the Internet provider to the school will get saturated, so public facing resources will become unavailable.” A provider-delivered DDoS solution in the cloud can help address the problem.

Most Common Cyber Attacks

- DDoS
- Ransomware
- Phishing Scams
How AT&T Can Help

AT&T offers a variety of network security solutions that are carrier-agnostic, meaning schools can take advantage of these services regardless of who provides their network or Internet services. Here’s a brief summary of these services.

Cloud Web Security Service provides near real-time protection against viruses, malware, and website hackers. It gives students and employees safer and more reliable Internet connectivity and offers a simple way to manage their access to applications. With Cloud Web Security Service, you can help protect network users and their devices from advanced malware and unsafe websites; provide higher secure, reliable connectivity for remote network users; enable blocking of suspicious websites; and set user privileges for individual applications. AT&T’s Cloud Web Security Service typically ranges in price from $80-$300 per user depending on deal specifications.

Secure Email Gateway is designed to block email threats before they reach your network. It helps secure your email data, stop spam, and guard against “click-this-link” malware attacks and other inbound threats—while also helping to prevent inappropriate or sensitive content from going out. AT&T’s Secure Email Gateway typically costs $60-$300 per seat per user depending on monthly plan purchased.

Threat Manager—Log Analysis Service uses advanced log analytics to provide near real-time visibility into the malicious activity on your network, as well as expert threat analysis and mitigation. “We take all of the logs from a school’s servers, routers, firewalls, and security appliances, aggregate this information, apply carrier-grade security analytics to the data, and then provide remediation activities based on the results of our analysis,” Hect says. “It’s an ongoing service that monitors a school’s network 24 hours a day. We baseline the data to determine what it normally looks like, and anything outside of that, we would recognize as an anomaly—and we would look into what that activity is. If we think it’s malicious, we’ll notify school leaders that we think they have a problem—and we’ll recommend a solution.”

DDoS Defense is designed to detect the presence of a DDoS attack in near real time; supports blocking of malicious packets while working to maintain the flow of legitimate network traffic; and helps stop denial-of-service traffic floods before they can choke your network. AT&T’s DDoS Defense services typically range from $1,500-$40,000 per month depending on mitigation plan.

Learn more about how AT&T can help meet your schools’ network security needs.

att.com/security

9 Seals.