Addressing Record Breaking Cyberattacks in Schools

Buffalo Public Schools, New York, was the victim of a cyberattack that forced the district to cancel classes for a few days until key systems, equipment and applications targeted were restored.[3]

Introduction

For many reasons, 2020 was an unusual and challenging year that continues to carry over.

While attacks on infrastructure have taken center stage, what is less publicized is the rise in cyberattacks on schools. In 2020, K-12 schools alone saw a rise of 18% to 408 breaches.[1] Indeed, schools faced a barrage of attacks such data breaches, leaks, ransomware and phishing attacks, as well as an alarming new threat in the form of invasions of online classrooms.

In 2020 and 2021 ransomware attacks on schools and districts included:

- Broward County Public Schools, Florida, the 6th-largest school district in the US, was hacked and threatened with leaking student and teacher information online if a $40 million ransom wasn't paid. They did not pay the ransom.[2]
- Buffalo Public Schools, New York, was the victim of a cyberattack that forced the district to cancel classes for a few days until key systems, equipment and applications targeted were restored.[3]
- Judson Independent School District in Texas paid an undisclosed ransom amount to regain control of its computers.[4]
- Rockwood School District in Missouri, was the victim of a malware attack that shut down the entire network in the district with more than 21,000 students and 4,000 staff.[4]
- North Carolina, Oklahoma, Virginia, Connecticut, Maryland, Nevada and California also had districts hit by malicious actors.

Attacks weren't limited to only K-12, universities also were victims of cyberattacks in 2020 and 2021:

- The University of Utah experienced a ransomware attack on its computer servers and paid more than $450,000 to an unknown hacker.
- Hackers attacked the computer servers at the University of California, San Francisco (UCSF) School of Medicine. To regain access to their data, the school paid $1.14 million in Bitcoin.
- Some of the other universities experiencing cyberattacks include University of Colorado, University of Maryland, Baltimore Campus (UMBC), and the University of California, Merced.[5]

The consequences of any cyberattack can be devastating and extremely costly, but an attack on an educational institution can also impact students' personal information, research data, financial information, etc. All of this can be held for leverage or ransom, affect school operations and actually cause the school to shut down for a period during containment and recovery.

Why are schools targeted?

2020 proved to be a record year for cyberattacks against schools and universities. The attacks took advantage of several factors including the quick switch to online learning, new devices given hastily to students and teachers, and the reliance on home networks. The transition to online learning was anything but smooth as schools faced a barrage of attacks such data breaches, leaks, ransomware attacks, and phishing attacks, as well as an alarming new threat in the form of invasions of online classrooms.

As students returned to the classroom in 2021 the attacks continued. The transition back to schools and universities from online learning often brought unauthorized technology used during online learning as well as new personal devices onto the school network. Additionally, tech savvy students may have the latest devices, yet they often don't follow good cyber hygiene practices such as password management, using MFA and installing software updates right away. These circumstances posed a challenge to IT departments, and an opportunity for cyber criminals, as these devices could unknowingly contain malware and bring it back to the school's network or provide an entry point to hackers.

Beyond the unique circumstances of 2020 and 2021, there are other factors that make schools a target to malicious actors. Many organizations run on legacy systems that can't protect them from evolving threats because they don't have the necessary financial or staff resources that many large corporations have, to keep systems up to date and all staff trained on cyber threats.

While classroom learning transformed significantly in the past few years, the systems to protect school networks haven't changed much at all. Text and workbooks have been replaced with laptops and tablets, lesson plans are shared over the internet with media-rich resource material, and student and IoT devices continue to increase year after year.

And, as more education data migrates to the cloud, a report from ManagedMethods and administered by the EdWeek Research Center, "What You Don't Know Can Hurt You: New Survey Identifies Gaps in K-12 Cloud Security," reveals half of respondents either did not have a security platform in place or did not know if a platform had been implemented in their district. In a field where 86% of respondents reported using or planning to use cloud-based learning systems, these gaps may present security vulnerabilities for cyber criminals to take advantage of.[6]

Not only have learning tools and processes transformed, other school departments such as facility management, transportation, administration, etc., employee software, apps and devices. Together with those used for education, these tools provide additional points of entry for cyber criminals.

Unfortunately the network and its security that underpins these assets is often overlooked in budget planning and tasks are distributed amongst other roles. These factors also leave the network vulnerable to cybercriminals.

Lastly, schools often don't feel they have anything valuable for cyber criminals, and therefore don't need extra resources for security. The EDTECH Leadership Survey Report from CoSN also highlighted how many educational institutions have underestimated cybersecurity risks with 84% of respondents not rating any threats as high risk.[7] However, school's systems hold staff and student information, alumni databases, supplier details, research data, etc. All of these are assets that malicious actors find valuable and can be a source of new, sellable data on the dark web and make schools targets of cyberattacks.

Barriers to cybersecurity in education

The main barriers education institutions face stem from the aforementioned lack of resources. The absence of adequate funding directly impacts not being prepared for cyberattacks. While education leaders are realizing the importance of increasing their network security to guard against breaches, budgets don't often meet the needs of schools, districts, and universities and they are left unprepared with underequipped technology and less in-house skilled network security professionals. According to surveys from the Consortium for School Networking (CoSN), only one in every five school districts has a full-time staff person dedicated to cybersecurity.[8] Education leaders are left with the challenge of how to balance technology, personnel and risks when determining their cybersecurity investments.

In addition, the increasing sophistication of cyber threats poses a barrier to cybersecurity for education. To improve the effectiveness of attacks, while making them harder to detect, malicious actors have learned to use AI more effectively, including using it for initiating attacks and gathering business intelligence. Hackers also are using AI to conceal malicious code that is programmed to execute at a later date and to create malware programs that can adapt accordingly during an attack. With limited budgets and personnel, schools find themselves challenged to keep up with evolving threats.

A third significant barrier is the human factor. Schools are often breached by hackers who take advantage of the lack of cyber training for staff and students and aim their attacks at careless employees or students who trustingly reply, click on unknown links, or download files or unauthorized applications. The most common schemes are phishing and social engineering emails asking for credentials, payments or account details.

For example, the comptroller at the San Felipe Del Rio Consolidated Independent School District in Texas received a malicious email claiming to be a representative of the financial institution that the school made bi-annual bond payments to. The comptroller fell for the scheme, leading to district officials mistakenly wiring more than $2 million dollars to the cyber criminal's account.[9]

Since the start of the pandemic, social engineering schemes; phishing campaigns that are more polished in their targeting often using a familiar person or emotional appeal, have increased. Recently, university students received emails from hackers posing as school administrators asking for vaccination status along with other personal information. From these emails, students could click on malicious links, download suspect files or provide personal data setting off malware or having their information compromised.

Top cyber threats to schools

What are the top cyber threats to schools and universities? Below are the most common threats schools need to monitor for and protect against.

1. **Phishing and social engineering**
   As previously mentioned, to deploy malware, criminals use tactics such as phishing and social engineering to entice people to unsuspectingly download malicious software and give them a path to enter the network. Phishing emails appear to be similar to other emails reaching one's inbox and may look like it is from a trusted source, however, there are tell-tale signs it is a hacker:

   - Incorrect domain name in email address
   - Urgent or threatening language
   - Suspicious attachments or incorrect links
   - Misspelled words or grammatical errors
   - Mismatched URLs

   Social engineering emails on the other hand are more specific and polished in their targeting and appear to be a personal email. For example, the hackers send an email that looks like it's from a district official to staff, however, it's a fraudulent email usually with a malicious link or document to download.

2. **Third-party vendor issues**
   To breach a district or university, malicious actors may hack a smaller vendor to infiltrate the school's network. Like businesses, schools are digitally connected with many vendors having access to their systems to conduct business such as transactions, share information, etc. Hackers see these connections as a way to exploit vulnerabilities and access the school's network.

3. **Unpatched and outdated software**
   Updating and installing all software patches and updates expediently is paramount to avoid a breach. Once attackers are aware of a new vulnerability, they work to exploit and gain access to the victim's system and run their own malicious code on it.

   The Pulse Secure cyberattack in April 2021 is an example of what can happen if updates are not expediently applied. While hackers did exploit a zero-day vulnerability, they also were able to exploit three further vulnerabilities by looking for organizations that had not followed best practices to keep software up to date. These further vulnerabilities would not have been compromised if the organizations had upgraded their systems.

4. **Internet of things**
   The internet of things (IoT) is a network of intertwined devices, software, and other 'things'. With different departments and audiences using a variety of tools in education, it can be hard to tell how many IoT devices are connected to the network at once. What is important is that they are all secure. If not, attackers can take advantage and find access points to gain an entry point to the school's network, putting academic and personal information at risk.

It's time to protect schools

When it comes to network security educational institutions already have unique challenges, starting with small IT teams and strict budgets. However, cyberattacks will continue to evolve and target educational institutions. To protect students, staff and valuable data, these challenges and barriers must be addressed and changed. To this end, the Biden Administration has enacted the K-12 Cybersecurity Act into law to enhance the cybersecurity of our Nation's K-12 educational institutions. This law put into motion efforts by CISA to examine the cybersecurity risks associated with K-12 educational institutions as well as provide tools and guidance.

In addition, to stay ahead of evolving threats and hackers, schools can implement these steps to protect their students, staff and networks:

1. **Update Software**
   Maintaining software updates for all devices is crucial to ensure any vulnerabilities found are swiftly mitigated.
2. **Lock Down Administrative Control**
   By preventing students and teachers from downloading applications that could house malware, you can minimize the exposure and protect the network.
3. **Separate Backups**
   Always have backups of critical data in a separate location. In the event of a malware or ransomware attack, schools can quickly get their data and configurations restored without paying the ransom.
4. **Separate Network for Guest/student Devices**
   By separating the main school network from all the guest and student devices that you don't control, you can quickly mitigate any issues that may happen on the guest network without impacting the school network's performance.

5. **Captive Portal to Gain Visibility to Guest/student Devices**
   Use a Captive Portal page that requires users to log in before gaining access to the network. You can then create rules and policies for what those devices can access while connected.

6. **Threat Intelligence**
   Utilizing solutions that have built-in threat intelligence engines that proactively protect against unknown and emerging threats is critical for schools to stay protected against hackers and malware.

7. **Next-generation Firewall**
   Next-gen firewall solutions provide protection at the gateway in an all-in-one solution that encompasses web content and application filtering, bandwidth shaping, advanced threat protection, and VPN connectivity options.

8. **Reporting**
   Data-driven reporting is a key aspect for schools to showcase their CIPA compliance. Ensure reporting includes detailed audit logs of every traffic event occurring on the network.

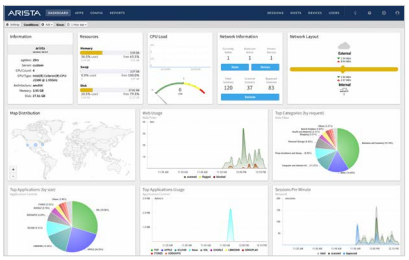
Sources

1. https://www.k12six.org/
2. https://www.businessinsider.com/large-florida-school-district-hit-by-ransomware-attack-2021-4
3. https://buffalonews.com/news/local/education/buffalo-public-schools-was-victim-of-ransomware-attack/article_e9efa01c-8335-11eb-9b7a-83dd46be27ee.html
4. https://www.bloomberg.com/news/features/2021-08-09/schools-brace-for-more-cyberattacks-after-record-2020
5. https://www.zdnet.com/article/ransomware-group-targets-universities-of-maryland-california-in-new-data-leaks/
6. https://www.securitymagazine.com/articles/96533-study-finds-knowledge-gaps-in-k-12-cloud-security
7. https://www.cosn.org/tools-and-resources/resource/edtech-leadership-survey-report-2021/
8. https://www.governing.com/security/cyber-attacks-on-schools-in-2020-were-record-breaking-report.html
9. https://www.bloomberg.com/news/features/2021-08-09/schools-brace-for-more-cyberattacks-after-record-2020

- https://corporatetraining.usf.edu/blog/top-5-k-12-cybersecurity-threats-schools-are-facing
- https://www.edsurge.com/news/2019-01-07-are-school-districts-starting-to-understand-the-scope-of-security-threats
- https://gcn.com/Articles/2021/09/15/k12-college-cyberattacks.aspx?Page=2
- https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/08/statement-of-president-joe-biden-on-signing-the-k-12-cybersecurity-act-into-law/?
- https://www.zdnet.com/google-amp/article/biden-signs-school-cybersecurity-act-into-law/
- https://www.tasbrmf.org/learning-news/insiderm/home/coverage/privacy-information-security/6-cyber-threats-for-the-2021-school-year.aspx
- https://enterprise.verizon.com/en-nl/resources/articles/cyber-security-threats-to-schools-and-how-to-prevent-them/
- https://www.rm.com/blog/2018/september/five-biggest-cyber-threats

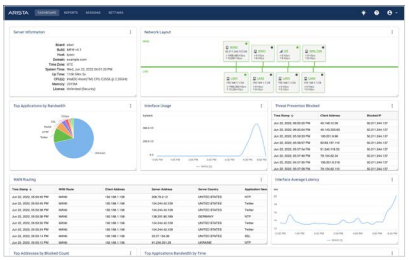
About Arista Edge Threat Management

Arista's Edge Threat Management solutions help small-to-medium businesses and distributed enterprises optimize their networks while safeguarding their data and devices. Edge Threat Management provides cloud-managed security and connectivity options that work together seamlessly to ensure protection, monitoring, and control across the entire digital attack surface from headquarters to the network edge. The award-winning products are trusted by thousands of customers and protect millions of people and their devices. We are committed to bringing open, innovative and interoperable solutions to customers through a rapidly growing ecosystem of technology, managed services, and distribution partners worldwide.



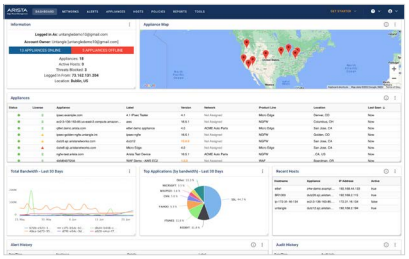
Advanced Security

- Protection, encryption, control & visibility anywhere
- NG Firewall, IPS, VPN & more
- Onboard security for small network appliances & IoT devices
- Full security processing on-premises or in the cloud



Intelligent Edge Optimization

- Secure, WAN-optimized connectivity for every location
- Seamless scalability
- Optimal predictive routing technology for first packet, dynamic path selection
- Centrally manage one or many appliances



Cloud Management at Scale

- Zero touch deployment
- Configure & push policies
- Advanced alerting & reporting
- Visibility across globally dispersed networks & endpoints

Santa Clara—Corporate Headquarters
5453 Great America Parkway,
Santa Clara, CA 95054

Phone: +1-866-233-2296
Email: edge.sales@arista.com