Top 5 Cybersecurity Threats for Schools

PHISHING

Description: Over 90%* of cyberattacks start with phishing, the practice of sending legitimate-seeming emails that will entice users to reveal personal information or click on links that install malicious software. Phishing e-mails are becoming increasingly sophisticated and difficult to detect.

There are several different types of phishing:

Deceptive - emails from legitimate-seeming companies asking you to verify your account and enter personal details

Spear - similar to deceptive but with personal information such as your position, name, etc. to make the email appear more legitimate

Superintendent Fraud - akin to CEO fraud or whaling, using an email similar to the Superintendent's to get the recipient to send proprietary information

Response: Training staff to detect and report suspicious e-mails is the first and most important step to deal with phishing. Make sure you have a well-advertised process in place for reporting suspicious e-mails. When a staff member clicks on a malicious link, quick action is necessary to quarantine malicious software before it spreads - it is critical that staff feel safe reporting such mistakes immediately.

Firewalls and email systems should be configured to have rules that don't allow bad attachments.

(*PhishMe Enterprise 2016 Phishing Susceptibility and Resiliency Report)

DDOS

Description: A distributed denial-of-service (DDoS) attack occurs when multiple systems flood the bandwidth or resources of the district servers.

Response: Though DDoS attacks can't be prevented, it is possible to purchase cloud services that do traffic scanning and analysis to mitigate the attack - cloud mitigation could be focused on protecting the underlying internet connection or to protect the higher level web servers. Districts need to be sure that purchased cloud services are focused on their specific needs. This can be an expensive measure. The key for most districts is to monitor the network to detect threats early and to have procedures in place with key information and contact person needed to get help from your service provider. It is then possible to determine where the attack is being targeted and to limit the amount of traffic that is coming through.

DATA BREACH

Description: A data breach is the release of secure confidential information.

Response: There are Data Loss Prevention (DLP) solutions that detect and prevent data breaches, though these tend to be expensive. Districts should:

- Train end users in what data they are responsible for protecting and how to handle data.
- Use encryption services for any data that needs to be sent via email.
- Train staff on security procedures and ensure everyone feels confident they won't be punished for protecting data.
- Establish processes for what to do if a data breach occurs.
- Consider insurance to cover the cost of mitigating the damage in the case a data breach should occur.
- Consider getting a 3d party to audit your security systems.

RANSOMWARE

Description: Ransomware is a type of malicious software that encrypts the district's data and requires a ransom to be paid in order to regain access to the data. The threat of releasing the data is also sometimes made unless a ransom is paid. Recently schools have seen this threat escalate to threatening e-mails sent to parents and students with ransom being demanded from the schools.

Response: The best response to regain access to data is to backup data on a server that is not accessible by the rest of the network and therefore not vulnerable to the ransomware encryption agent. Policies should be in place in advance to address ransomware should it occur.

IOT VULNERABILITIES

Description: IOT (Internet of Things) devices include district owned equipment such as security cameras and other devices that may be student or teacher owned such as watches or cloud-based voice service devices. These devices often lack security or are not updated on a regular cycle.

Response: Consider isolating devices on a separate VLAN (Virtual Local Area Network) where they can be watched and don't have access to the rest of the network. Always change the default password to IOT devices.

Consortium for School Networking 1325 G St, NW, Suite 420, Washington, DC 20005