Maintaining a Secure Network in an Educational Environment

Larry Jackson Jr

ICTN 6865

Dr. Phil Lunsford

Fall 2015

Abstract

In this paper I will discuss the network security issues associated with securing school networks and the common methods of minimizing risks. I will focus on security issues surrounding the WAN, LAN, Wireless devices, BYOD, antivirus and mobile devices. I will discuss the legal obligations in contrast to the needs of the district when dealing with the storage and accessing of student data. I will look into new trends associated with the transmission of malware through social media outlets and the procedures or policies that can be put into place to limit the occurrences. Finally, I will discuss ways to secure your guest networks or limit access to external users.

Maintaining a Secure Network in an Educational Environment

Today, school systems across the United States have implemented technology into almost all facets of their planned curriculum. This implementation contains computers, smart boards, printers, laptops, tablets, document cameras, etc. A major part of the effectiveness of this implementation and continued stable use of these devices is a secure and robust network infrastructure. The network, to the average user, isn’t something they think about until the moment they can’t access data or a particular device. Just like any other business, the network inside a school district has a need for some type of security. But unlike other business, school networks have other aspects that need to be addressed. For instance, schools must take into account privacy, confidentiality, data integrity, content filtering, and cyber bullying. A school has to balance the need for internet access with the need to keep its users safe. While this is similar to other businesses, schools have to abide by special rules set forth by their state boards when it comes to the transmission and storage of student data. Balancing rules with needs and wants is a difficult task but when done correctly a smooth operating environment can be achieved.

Securing the WAN

Securing the access to and from your network is one of the most important tasks for any network professional. The wide area network (WAN) is the gateway to the internet and to combat unwanted traffic a firewall is used to restrict it. A firewall can be a hardware device or software ran on a router. A school district may also choose to implement internal firewalls to separate servers from the internal users (Penner, 2003). A commodity often seen utilized in school districts is the use of virtual private networks (VPN), which is software that is used to extend a private network across a public network like the internet. VPN’s are used by teachers and other administrators to access school resources securely. Special techniques can be used to ensure the security of this access and that includes the use of intrusion detection systems (IDS). An IDS or IPS (intrusion prevention system) can be used to detect and/or prevents unauthorized access to your secure school network. The firewall can also be used to set limits on the types of data being sent out of the schools network and limit the type of data being downloaded from outside the network. The firewall is an integral part of keeping your network secure.

Securing the LAN

The LAN or local area network is the connected group of devices within your school or immediate area. The LAN can be considered a smaller version of the WAN and it too has special security needs. The LAN is used to connect your computers, printers, wireless devices, and security systems so they are able to communicate with each other. You network has to be flexible while maintaining performance and security. According to Cisco, "The wired LAN is the principal means of connection for the high-speed school LAN—even in an integrated wired and wireless environment" (Cisco Mobile Office Net Software). Your network must secure its data and applications, which can be achieved through hardware like switches. Switches can restrict the movement of data to those places only authorized by the network administrators. Segmenting your network into groups or VLANs allows for easier administration of security policies. Segmenting also allows the use of mixed trust zones which allow different users different levels of access, allows protection of servers and applications, while simplifying network management. The same hold true for the up and coming brother to the wired LAN, wireless LAN.

According to a solution overview from tech giant Netgear they state that "wireless connectivity has become a necessity in educational institutions of all levels" (2015). Because more and more mobile devices are being used in the classroom and throughout the school, the use of a wireless network has become a necessity. Wireless works off the same principals as the wired LAN but differs in the fact that anyone with a wireless network card has the potential to intercept the data being transmitted across the network. Because it is difficult for individual schools to control the types of devices they utilize, best practices should be used to ensure compliance with schoolboard policies since a variety of device manufacturers may be used at any time. In order to secure the WLAN the first step is to secure access, which is securing who can connect and who cannot connect to your network. A separate VPN for wireless devices is a great way to limit and manage the traffic being sent over your network. Next, you need to control the standards that are used on the network, which entails using protocols to encrypt the data being sent and received. For a school system WPA and WPA2 standards are encouraged to be used because of their ability to provide a higher degree of encryption protection. The use of approved hardware and ensuring software is kept up to date is a measure that should be taken to make sure hackers can’t take advantage of any flaws. The biggest way to secure your wireless is through the education of your users. “The biggest threats to computer security are often an organization’s own employees” (Hanna, 2005). Your users will take their devices to and utilize them in public places or at home where security levels may not be up to par with the schools. This will leave the machine vulnerable and when it is connected to the schools network hackers may be able to exploit those devices in malicious ways. Having good antivirus and local machine firewalls can help alleviate the risks associated with roaming devices.

Alleviating BYOD Security Issues

With the continued widespread use of wireless technology, bring your own device (BYOD) policies have been implemented at many school systems across the U.S. to give users the ability to use devices they are familiar and comfortable with. Some of the threats that face a schools network through the use of a BYOD policy are unknown third-party access via mobile apps, the inability to track data, data segregation and lost or stolen devices. Authorized BYOD users may at some point, outside of your network, install third party software that in turn has unregulated access to any data on that user’s machine. According to Amit Sinha, the CTO at Zscaler, one way to address this risk is by implementing black lists of at-risk software or by adopting effective bring your own application (BYOA) strategies which entails enforcing security features by only allowing consumer-grade apps that utilize high security standards. When faced with the inability to track data, schools can choose to use content security tools that utilize discovery and monitoring tools to protect against data loss. A less complex means of battling data loss is reducing what information is allowed to be stored or accessed on a device. The idea of data segregation comes from the need to ensure data is stored in secure places when dealing with cloud type environments. Formal agreements that detail the security strategies for the hosting companies of cloud storage providers are a must. To guarantee compliance with both schoolboard and local and state polices any vendor that has access to school data must have rigorous safeguards in place to protect that data. Probably the most widespread problem you will face when implementing a BYOD policy is the mishandling (losing) or stealing of a personal device that has access to or stores school data. In a 2014 article about the security risks of moving data in BYOD area noted that mobile devices get lost more often than PCs due to their smaller form factor, which means users tend to bring them everywhere (Phneah, 2013). Because of the inherent ability of mobile devices to go anywhere, people will tend to use them everywhere, making securing them that much harder. Devising and enforcing a mobile device security policy that would require a minimum level of security on the device before being able to connect or access information on the networks is a great way to start. Requirements like having lock or pin controlled access to the device or having a lock screen in place will help alleviate potential issues.

BYOD can be a great asset to inspiring creativity through the use of devices that the users are comfortable using. But they also are harder to secure than a static pc or enterprise level device that has built in security. The best practices to secure them are to ensure there are policies in place that help lessen the chance of breaches.

Antivirus as an Asset

Antivirus software is a necessity these days. Long gone are the days when a school system could use a firewall only. To combat the onslaught of viruses, malware, Trojans and other malicious programs a flexible antivirus must be used at all times on any device that has access to or store information. According to Shawn Wyman, of the SANS Institute, what an educational institution requires is a cost-effective and centrally managed “defense-in-depth” approach to virus protection. Education and security do not always go hand in hand resulting in school administrators who do not want to inhibit student learning with security restrictions (Wyman, 2001). This defense-in0depth is an idea that antivirus just can be ran on desktops to get a perception of security. Antivirus must be ran on any devise that stores or retrieves data. Firstly, your software should be centrally managed to remove the user from the equation when it comes to scanning and updating. Risk assessments need to be taken into consideration when deciding to design a security policy, which will be the basis for any IT related decisions. Of course desktop ran antivirus will help with individual machines, but it has to be able to scan removable media and block items from starting up on machines without permission. Real time protection at the network layer has to be considered as well. Email and SMTP attack are common methods used by hackers to gain access to data. By having executables set to not automatically download on your network can assist in confronting those infections that propagate through those executables. An effective antivirus can only do so much if your users aren't educated in the ways of safely navigating and using resources. User education will play a major part in when and how you respond to infections, because even with the most up to date software it is inevitable that a machine will one day fall victim to malicious intent. Virus protection in an educational environment is a difficult idea because network managers and administrators have to find a balance between safety and inhibiting a user's access. This balance, although difficult, needs to be achieved in order to have a secure network that can be utilized effectively by its users.

Integration of Mobile Devices

With an efficient wireless network in place users will be drawn to the use of more mobile devices and not just the standard laptop. Tablets, smartphones, smart watches and other devices can aid users in their attempts to access data, but where do network administrators draw the line, if at all. Allowing users to bring in or by giving users mobile devices you add more risks of your data and network being breached. According to a journal article written by Jason Rouse, "mobile devices are essentially highly miniaturised desktops, and they are also set to become the principle interface between people and business" (March, 2012). An attraction of this type of device is the use of mobile applications that can extend or enhance the abilities of mobile devices making them an asset to the users in your district. Mobile devices can fall victim to flawed design applications, cross-site scripting (XSS) attacks and SQL injection attacks among other vulnerabilities.

An inherent design flaw recently found in Apple mobile devices was the Zero-Day bug that allowed the theft of Apples password management system and applications passwords. A team of researchers from Indiana University, Peking University and the Georgia Institute of

Technology, found that inter-app interactions like that of Apples keychain, can be exploited to steal confidential information like passwords from email, iCloud, bank accounts, and apps like Evernote. This type of design flaw can allow intruders to gain access to your secure network through these mobile device flaws and intercept any data found. Best practices to prevent this from happening, as of now, is to not download apps from unknown developers. A similar flaw was found in Androids Swift keyboard app which allowed hackers to remotely access resources on the phone and secretly install malicious apps or eavesdrop on communications. These types of attacks can be potentially devastating to a school district and that is why security measures have to be in place to prevent and/or limit the frequency of these types of attacks.

Best practices for mobile device integration dictate that administrators ensure device policies are in place to define what resources will be available for access while utilizing mobile devices. Defining what types of devices will be allowed to access resources can help ensure only known platforms are used. Testing of mobile devices before allowing on the network can aid in determining if said devices should be allowed on the network. Aspects such as connectivity, authentication, application functionality, logging and performance should be tested before approving any device use. Ensuring district issued devices are fully functional and secured before being issued can assist users and administrators in maintaining the device at a level that won’t compromise your network. Finally, regular maintenance, including updates, patches and scanning can prevent small localized issues from becoming large district wide issue. Being proactive is the key to securing the mobile devices across the network and again, users education will be of great benefit to combat any malicious acts against devices used on your network.

Social Media in Education

As technology continues to evolve so will the methods used in the classroom to teach students of the ever evolving world around them. Some educators believe that by leveraging social media and some of its largest tools like Facebook, Twitter and Pinterest they can ensure students succeed in class by using these tools to study effectively (Blair & Serafini, 2013). Along with the use of these tools comes the undeniable intent of malicious acts by outsiders or even your users. Like all other forms of technology school districts need to understand and have good policies in place to try and circumvent any malicious intent. The tools and devices used to access social media are the same devices you may already have on your network and therefore won't necessarily need specific strategies of defense. A good overall security awareness program in combination with technical and administrative safeguard can be utilize to prevent most attacks seen through the use of social media. According to a 2011 article from the website 'Government Technology: Solutions for state and local government and speaking on social media use it is stated that two of the greatest risks to organizations are malware and inadvertent disclosure of sensitive information (Waxer). These will also be the greatest threats when using social media in the classroom. Proactive training and those security measures already present in your network that are used to protect your users when on the Internet or using email can be effective strategies at protecting data while using social media.

Conclusion

Technology will continue to grow and the need and want to use this technology will grow with it. By being proactive and ensuring that you have good policies in place alongside robust equipment you can mitigate almost any attack against your network. Due diligence and well thought out designs should be used at all times since this will be your best chance at ensuring your network is secure for use. The need to protect information will always be present in this environment so education for your users about best practices associated with usage is key since users will make up the largest security risk group in your district. The network in a an educational environment is a complicated thing, but with proper attention and a willingness to protect your assets it can be secures like any other.

References

Blair, R., & Serafini, T. (2014). Integration of Education: Using Social Media Networks to Engage Students. Journal of Systemics, 12(6), 28-31.*

Chabrow, E. (2013). 6 Steps to Secure Mobile Devices. Retrieved December 3, 2015, from http://www.bankinfosecurity.com/6-steps-to-secure-mobile-devices-in-enterprise-a-5857

Cisco Mobile Office Net Software. (n.d.). Retrieved November 17, 2015, from http://www.cisco.com/en/US/products/sw/wirelssw/ps1953/products_quick_reference_guide09186 a00800 a8484.html

Hanna, G. (2005). Securing Wireless Networks Against Intruders. The CPA Journal, 4, 68-69.*

Implementing a Secure Wireless Network in an Educational Setting. (2010). Retrieved November 17, 2015, from http://www.netgear.com/images /Solution_ Educational _Setting18-9457.pdf

Pascucci, M. (2013, November 12). Tips to Secure the LAN: A Look at the Network Layer - AlgoSec Blog. Retrieved November 17, 2015, from http://blog.algosec.com/2013/11/tips-protect-harden-lan-look-network-layer.html

Penner, R. (2003, October 25). Securing the Network in a K-12 Public School Environment. Retrieved November 17, 2015, from https://www.sans.org/reading-room/whitepapers/bestprac/securing-network-k-12-public-school-environment-1292

Phneah, E. (2013, February 4). Five security risks of moving data in BYOD era | ZDNet. Retrieved November 21, 2015, from http://www.zdnet.com/article/five-security-risks-of-moving-data-in-byod-era/

Rouse, J. (2012). Mobile devices – the most hostile environment for security? Network Security, 2012(3), 11-13.

Waxer, Cindy. (February 2011). CIOs Struggle With Social Media's Security Risks. Public CIO. Retrieved March 3, 2011 from World Wide Web: http://www.govtech.com/pcio/CIOs-Social-Media-Security-Risks-021111.html

Wyman, S. (2001, December 6). Anti-Virus Strategy in a Public K-12 Educational Environment. Retrieved November 21, 2015, from http://www.sans.org/reading-room/whitepapers/infosec/anti-virus-strategy-public-k-12-educational-environment-603