East Carolina University

Implementing Effective Security Techniques Using Best Practices in Networking Management

Larry Jackson Jr

ICTN 6885

Dr. John Pickard

Spring 2016

Abstract

This paper seeks to review current trends associated with securing an enterprise network and demonstrate an effective plan for doing so. With the continued rapid increase of information technology and application usage in the business world comes the need for improved techniques to ensure effective management of vital networks. Because the network plays such a pivotal role in today's business environment the need for administrators to find effective means of securing it is more necessary than ever. Best practices can be used to ensure administrators effectively use their time and resources to solve or preempt problems before they can grow to an overwhelming size. The best practices used in ensuring security of the network can fall under three broad categories, preparation, prevention and response. These categories, along with good software and hardware to support it, can assist any network administrator in securing their network. Reducing risk across the network can be seen as a leading objective of administrators and by utilizing sound and effective techniques administrators can be ensured that the policies, equipment and proper strategies they have in place will help to lessen if not eliminate risk. Finally, this paper will attempt to make an educated guess as to the future trends surrounding network security and the possible challenges that will be faced by administrators. Because technology will continue to evolve and businesses will have to evolve along with it there will always be a tremendous need for network administrators to ensure functionality of their network and its resources.

Targeted Publications:

Security & Privacy, IEEE Journal
International Journal of Information and Network Security (IJINS)

Best Practices Base Line

Three basic areas can help network administrator's setup and ensure an efficient network design, preparation, prevention and response. These areas can serve as a baseline or guideline on implementing strategies throughout your network environment. The first area, preparation, deals with the steps that are needed prior to implementing any security policy. Creating usage policy statements that show users roles and responsibilities in regard to security should be the first step. This document should be used to provide the company a general understanding of the security policies, definitions, guidelines and any specific actions that could result in disciplinary action against employees if they decide to disregard policies. An acceptable use document should be made next, this will give all users guidance as to what is expected of them while utilizing company equipment and advise them of what constraints or practices they must agree to in order to utilize the company's equipment and network. Finally, conducting risk analysis is a great way to identify risks to your network design, resources and its data. The goal here is to identify and assign threat ratings to portions of your network which in turn will allow you to better balance the needs of your users against the security needs of the network itself.

Prevention involves the monitoring of your network for security risks. You need to first determine what you need to monitor and why. You then need to determine what you need to monitor in real time and those areas that don't require real time monitoring. Policies should be made for things such as failed login attempts, changes to firewalls, new connections through firewalls, and of course unusual traffic. Your policies should address not only what and how to monitor but who to notify if the set thresholds are reached or a breach is detected. Email, paging alerts or automated voice calls are examples of how an individual or team can be notified in the case of an issue.

Finally, response, which deals with your actions to a discovered violation or threat. When a violation is found you need to be ready to confront and remedy this issue and having pre-made procedures in place will help the security team immensely. Your plan can include items like what changes can be made by the responding team without prior approval, who to contact outside the company, whether law enforcement should be contacted, whether systems should be isolated or repaired in place as well as who and what departments inside the organization should be contacted. Your policy should also contain details on how you plan to secure and make available any normal backup during down time. This policy should complement any that you already have in place regarding the backing up of systems, not change any. It should also be noted for reference if approval is needed before backup can be restored and who should be contacted for that approval. Lastly a review of the individual incidents and responses should be conducted to determine if the procedures need to be adjusted for efficiency. Polices should be considered fluid and ever evolving and if a policy can be altered to benefit the company that it should be and by conduction an effective review of incidents you can gain the need data to help you make the determination if a change is necessary.

Current Security Trends

Today network administrators are faced with the daunting task of securing their networks from fast changing threats in the forms of viruses and malware and from denial of service (DDos) attacks where attackers flood the network with illegitimate traffic in an attempt to bring down services. Almost fifteen years ago David Piscitello and Lisa Phifer stated that “there are no short-cuts or cookie-cutter approaches, but there are concrete steps that can tighten your network security”, when opening their paper on securing enterprise networks and this still holds true today (32). There are no one size fits all approaches to network security and with increased

threats, there will never be. In the recent past many, if not all, mega companies have fallen victim to some form of attack. Fortune 500 companies who have a huge foot print in the modern world seem to be at the greatest risk because of their ability to impact so many other industries. Companies like Sony, eBay, Microsoft, and Nationwide Insurance have all been attacked and have had customer data stolen or compromised. Many of the attacks have come at the hands of hackers who either attempted to steal data or stop others from accessing their own data. In the cases of Sony and Microsoft, their gaming divisions have been the popular target of attackers because of the very nature of the attack type, DDoS. Denial of service attacks allow individuals to take control of many computers at once, through backdoors or malware, and use those machines to flood a network or resources with connection requests. This flooding technique is very difficult to fight against because the requests sent are almost indistinguishable from legitimate requests made by genuine customers.

Attacks geared toward data storage in the cloud are also on the rise and one major reason is because of the rapid expansion of the number of cloud subscribers. Long gone are the days where an administrator must store their data on server farms located in a dark basement at the base of their center of operations. Cloud storage offers a solution known as Infrastructure as a Service (IaaS), whereby the customers is able to utilize space that is owned and managed by a third party, mitigating any overhead that would usually accompany the storage and maintenance of that same data. This type of service is not without its own risks. Over the past 5 years' cloud services have begun to be a well-known target for hackers as well. Companies like Microsoft (OneDrive), Google (Googled Drive) and Dropbox have fallen victim to what is known as a Man in the Cloud (MITC) attack. This attacks occurs when hackers attack the security token stored on your local machine in an attempt to gain access to your cloud storage folders which are usually

synced to your local machine. These types of attacks are particularly hard to detect because hackers do not need the Internet in order to attack an unsuspecting target, they can infiltrate accounts by altering registry keys, so users won't be aware of the breach either.

Finally, a major attack vector that network administrators are forced to combat is the securing of the network for use with mobile devices and social networks. Mobile devices have become common place in most all businesses and most have integrated them into the everyday workings. Administrators are now forced to deal with not just the security of their network but the devices that access their networks and the data stores and transmitted over it. Mobile device software is often attacked using similar means as when attacking a desktop computer or server. Android operating system is an avenue that seems to fall victim to exploits more than others in the mobile device realm. In recent news an exploit known as "Stagefright" was one of the largest ways a hacker could gain access to a user's device. This exploit supposedly allowed an attacker to take control of an Android device simply by sending a text message to the device. In short, since the Android Operating System (OS) found that media processing is a time sensitive task it uses native code (C++) in its media library to implement it. This is said to be more prone to memory corruption according to Joshua Drake, a researcher at the mobile security firm Zimperium who initially found the exploit in 2015. The researcher found that by sending a MMS message to the target phone, which contains a media file designed to secretly install malware without the user ever knowing, the hacker was able to gain access to the device. These types of attacks are hard to defend against because the user doesn't have to take any action to become vulnerable. At one time almost 95% of all android devices were said to be vulnerable to this attack. Network administrators have to be aware that devices that have been compromised may be used on their networks and may lead to their networks becoming vulnerable as well. Effective

planning and strategies can assist any administrator in lessening down time and risks. Ensuring patches are done on mobile devices and software is kept up to date us a good starting point for defense.

Securing the Network

As stated earlier, there are no magic one size fits all ways to secure an enterprise network but by having sound strategies and policies in place your risks of being down due to outside influence can be greatly reduced. Back in the mid 1990's an article written by James Triplett in the Telecommunications Americas Journal stated that there were "five domains of network security" and they were Internet, workgroup, mobile users, remote office and integrated enterprise security (38-40). Today this ideology still holds true and these five domains still encompass most of what todays enterprise network administrators defend against.

Internet Security

The Internet is the most vulnerable part of any network today because it gives anyone who is connected to it a means in to which they can gain access to your data. Because most businesses have integrated the internet into large portion of their business model finding ways to ensure your data and traffic is safe while utilizing it should be a high priority. Network administrators should always control the data flow to and from the Internet. This starts by having security policies in place that not only protect your network from outside attacks but from those originating inside your network environment. A great start at securing this valuable asset is through the use of application level firewalls. These types of firewalls give administrators the tools needed to fight against attacks like cross-site scripting (XSS) and SQL injection among many others. "Traditional firewalls do not understand attacks directed at the code of the

application using the normal channels through which the application is reached legitimately: usually HTTP and HTTPS (SSL) for web applications" (Rowan,4). Because of this limitation no matter what the traffic, the traditional type of firewall gets sent to a particular port that is open, it will be allowed through. For instance, if it sees traffic for TCP port 80 while it is set to open then all traffic with that destination will be allowed through no matter what type of code it holds. Utilizing an application level firewall in conjunction with sound strategies like ensuring applications are up to date, penetrations testing, and loggings will help protect the data and traffic that lets your business grow.

Work Group Security

Security at the workgroup level is very similar to that of the Internet but its primary focus is on securing the data from unauthorized access from within the organization. Workgroups can encompass a single building or multiple sites around the world, all connected via the Internet. A popular and effective means at maintaining the security at this level is through the use of virtual private networks better known as VPN's. VPN's are logical private networks that allow secure communication over the internet. In a sense it allows users to connect to a company's resources while physically still a far distance away. By using a VPN, you can ensure that only authorized users are able to access the data you need to secure. IP based VPN's provide confidentiality, authentication and message integrity through the use of protocols such as IPsec, SSL/TLS, DTLS, and SSH. These protocols are used to encrypt, decrypt, and transport data packets over the highly unsecure Internet while maintaining a high level of privacy and security. Some starting points to consider for getting the most benefit out of your VPN are identifying who needs access, what equipment type do they have, make sure all antirust is up to date and running correctly, finally ensure they only have access to what they need. Having a sound and consistent

way of checking for compliance of hardware and software is also a good thing to consider when deciding and/or setting up a VPN. These considerations will help to lessen the chances of unauthorized users using those with VPN access as a means to enter and disrupt your network. VPNs are a great way to bolster your security when access to resources are needed within your workgroup but like every other aspect of security it alone will not save your network from malicious attackers.

Mobile Devices

While authorized users may be able to gain access to needed network resources remotely the devices they use to access that data can be considered a vulnerability when they do. Mobile devices have become a staple of almost every business model these days. Cell phones, laptops, tablets, eReaders, among many others have made a foothold in technology and business use. These devices, like their older counterparts, the desktop computers and mainframes, are vulnerable to malware and hacking attacks. While these devices make life and work much easier, the job of the network administrator is made that much harder because of the new responsibilities associated with managing and defending these devices. "The network administrator is faced with a three-fold problem: ensuring that authorized users can access only approved LANs and/or individual servers, ensuring that authorized users can access only approved applications, and making sure that only authorized users are using the portable PCs" (Triplett, 40). Ensuring authorized users can only access authorized network resources is pretty straight forward. Administrators have to determine what and why users need access to resources and/or other network devices. They then would authorize and setup access for those user with the appropriate read and write permissions. One thing to remember is that when users leave the company or move into another position they would need to be reexamined for what resources they need

access to so again, they only have access to what is needed to complete their tasks. Ensuring users can only access approved applications is something that were are seeing more and more of since mobile applications can be developed easier and cheaper than ever before. This is even more important when users leave your protected network and try to access company resources from less secure environment like their homes or public Wi-Fi access points. Having approved application lists are a good start and combining this with some form of application verification, whereby applications can only be physically installed if they are signed off by administrators or on the approved list already, is a great start. An approved applications list can be made by researching and testing requested applications and comparing their security with the security needs of the organization and then comparing the risks to rewards of using those apps in your environment. The use of a mobile application management system or MAM can be used to manage the physical devices deployment and use of applications. A major benefit of a MAM is the ability it gives administrators to remotely wipe data and apps from an end user's device. Finally, ensuring that authorized users can only access devices is something that should be done at all levels of network security. The basic, and one of the most widely used, forms of this authorization is through the use of passcodes. Passcodes offer a quick and efficient way of locking a device while not making it over cumbersome for the user to use. Passcodes should be centrally managed and have requirements in place so that they are not easily broken by malicious users. Devices should, if possible, be able to be remotely wiped of all data if they become stolen or lost and all data stored on any mobile device should be encrypted. Data encryption can be achieved through many means but whatever is used it should be seamless and run on the device without it having a detrimental impact on performance otherwise user would possible seek to circumvent the very software setup to protect the network. All in all, standard security practices

are often effective but particular aspects should be tailored to the device to ensure full integration.

Securing Remote Offices

Remote office security should be undertaken the same way as your main facility and data centers. Security at this level should be centrally managed from main offices if at all possible. Centrally managed security allows administrators to consistently manage and control policies that are to be enforced throughout the organization without regard to the location. Data storage should not be on site if at all possible unless there is security in place to guard against physical theft. Night guards and/or 24-hour security surveillance can assist in securing data if it must be stored on site. According to a 2013 report by Nuspire, a managed network security provider, a problem with remote office security is the fact that internal spamming is found to be a major issue that poses a threat to network performance, security, and reliability (Chao, 2013). The reason behind this seems to stem from businesses not being able to fund or man traditional monitoring and analysis of the network at remotes sites as they do at main facilities. Again, centralization and implementation of assets that can be disseminated, monitored and enforced from a single location is a valuable practice for any business with satellite locations. Being able to gather log information from remote locations will give administrators the ability to react and make needed changes even if there are no administrators on site. Centralization is the key to securing remote offices. If you have sound policies and procedures in place at your main facilities these same policies and procedures should be able to be remotely enforced to ensure your satellite offices don't become the weak point of your network.

Integrated Security

Integrated security at the enterprise level encompasses all of the other areas of security and brings together the underlying tone throughout this paper, centralization. Centralization can offer ease of deployment, monitoring, configuration and authorization when used to defend against network attacks. The goal of network security is to protect your data and users from malicious intent and by utilizing a centralized approach you ensure that all arms of your corporation are at the same security level at all times. The key here is to find solutions that can ultimately balance the needs of the company with the security needs of the network. Best practices to achieve a secure network would dictate at least ten areas that will need to be addressed: physical security, authentication, content inspection, systems & data integrity, access control, intrusion/prevention/detection/rejection and auditing and logging.

- Physical Security entails going beyond the normal measures actively seen in most office spaces. It includes the safeguarding of access cards or tokens, the elimination of rogue WiFi access points and other network peripherals and the inclusion of any anti-theft equipment that can be used in conjunction with mobile devices.
- Authentication, in this scenario, is the enforcement of robust password/code policies, the use of two-factor verification measures and the security hardening of any device used to access your networks
- Content Inspection can be seen as any measure that can block malicious code from starting in your network environment. Antivirus software is a start but gateway software and firewalls should be set accordingly to deny as much malicious traffic as possible. The goal of content inspection is to not allow this code entry into your network where it can ultimately cause irreparable damage.

- Systems and Data Integrity can be thought of as additional means to secure those areas through the use of third party, non-built-in software. While many servers have built in security, often times hackers have access to those same pieces of hardware and can, at their leisure, find ways to gain unrestricted access to them. Software like *Tripwire* can be used to deliver advanced threat, security and compliance solutions that help detect, prevent, and respond to cyber threats (Tripwire, 2016).
- Access Controls are used to ensure only those individuals that need resources to complete their tasks are given access. No one should be given blanket rights to every part of your network or its information, therefore individual access should be denied and only given when there is a legitimate need.
- Intrusion Prevention, Detection and Rejection are as set of standards to which network devices should be tested against. The goal here is to prevent, detect and reject infections and other malicious acts through the use of monitoring and correction tools. The use of a multi-agent system (MAS-IDS) is seen as an excellent way to conquer the daunting task of processing traffic data by dividing the traffic into manageable subsets and analyzing them simultaneously with the aid of distributed analysis agents spread throughout your environment (Al-Yaseen, Othman, Nazri 89).
- Audition and Logging can be one of the most critical means to safeguarding and ensuring your network is efficient at all times. The use of auditing and logging tools can effectively tell you what is going on inside and to your network and its devices, in turn this information can be used to strengthen against attacks or show administrators trends that can that ultimately make your network even more efficient.

Securing a network can be considered a huge task that is never really achievable. The best that network administrators can ultimately do is ensure that they have policies and procedures in place that limit down time while being able to combat the problems that they may face. Because hacker trends change often so must the procedures used to fight them and therefore administrators should continue to evolve and rely on their network analysis and market trends to help them ensure that their networks are effective as can be at all times.

Future Network Security Challenges

Network technology has rapidly evolved over the last few years and will continue to do so with the widespread use of networked devices. Predicting the future threat types is a hard task yet using known information and current trends and analysis administrators can have a good idea of what is to come. A few areas where we will see growth include the commercialization of cybercrime, the threat to consumer grade cloud solutions, snowshoe spam attacks and new types of web exploits.

Cybercrimes will continue to directly affect networks and through commercialization cybercrimes have become readily available to anyone, even those who have no skills in committing the actual acts. According to a 2014 report from Europol's European Cybercrime Center, "a service-based criminal business model drives innovation and provides access to a wide range of services facilitating cybercrime" (5). With this trend continuing to grow, those who have long been a part of the traditional styled organized crime communities can now venture over into cybercrime by purchasing the needed tools or skills of those hackers who put them up for sale. Because the authors of these malicious programs hide deep within the dark web, there is often little to no information on how to identify them for prosecution. Because legislation is still varied from country to country it would be extremely difficult and resource

intensive to prosecute individuals if they were found. It is going to take a new approach from the international community to find an effective means of identifying and shutting down these types of activities.

Consumer grade cloud solutions, as discussed earlier, are still one of the fastest expanding facets of technology. Because these solutions are often cost effective and easy to use the masses flock to them and utilize them often. There is nothing inherently wrong with using these solutions, other than the fact that they are often built on a one size fits all model. This model, by design, gives anyone who pays for the services access to the same products as everyone else and hackers take advantage of this. Those who seek to exploit this software can take their time and develop a means to attack legitimate subscribers, often without them ever knowing. A key idea to keep in mind is to tailor your software to your network and the needs of your customers, this will help alleviate those attack vectors that are left open by those one-size fits all products. If possible, work with vendors or internal personnel to come up with effective solutions that are based on your current network design and that can be easily integrated.

Snowshoe spamming is a technique in which spammers are using a wide array of IP addresses in order to spread spam without detection. Because the spam is coming from a huge number of different addresses spam detection software often can't determine that it is in fact spam and thusly allows it through your spam filter. These types of attacks are considered an annoyance or hindrance because they take time to sift through but some spam can hold malicious code inside the email as attachments or links. When there is a Trojan or other infection attached to the spam it turns your device into a vulnerability for the network and when you get spammed from hundreds of different addresses it can overwhelm your network security features and allow even more of the infections to take over. According to Michael Kerner of eWeek, "the

distributed nature of snowshoe spam and the low volume of email and complaints per IP address pose challenges". This is because of the nature of the spammers using multiple IP addresses and anti-spamming services not being able to differentiate between spam and legitimate traffic. These attack types can once again become a huge problem for users who don't have access to full spectrum approaches which allow companies to not only look at both volume and the number of complaints but allows them to analyze relationship patterns of domain registrants coming across their networks. It's a known fact that modern mail filters can catch most spam when sent to users, but overall when used as a directed attack, snowshoe spamming can outnumber and overcome almost any defense network administrators have in place.

Finally, new web exploits kits are on the rise every day. Once, java exploits were seen as the biggest threat to networking and technology as a whole but now hackers are turning to integrated software like Microsoft's Silverlight as a means of entry into unsuspecting networks and computers. A major attack type that utilizes a Silverlight flaw was found in July 2015 after a spyware company known as Hacking Team purchased a 0-day vulnerability from a hacker and used it for over two years. Ultimately the spyware company itself was hacked and the exploits along with 400Gb of its internal data was released to the public via the file sharing source, Bit Torrent. These exploits have the ability to run remote code on both Windows and OS X machines. Silverlight vulnerabilities aren't nearly as common as those found in Adobes Flash or Java but it has the ability to do as much, if not more, harm because of its wide spread use and once thought of invulnerability to attack.

Conclusion

Securing an enterprise network is and will always be an ongoing and relentless task for network administrators to achieve. By using past knowledge and best common practices

administrators can limit their risks of intrusion and downtime of resources. There will never be an all-in-one fix that can be used on every network type, therefor you must be willing and able to put in the needed time in planning and devising an effective network structure. To achieve an efficient and purposeful network you also have to find solutions that benefit your network even if it means they have to be tailored to your specific needs, which takes time. Networks should be fluid and unobtrusive to the average user yet have enough security features in place to protect all of your assets. Educating your users on best practices can help alleviate a huge security hole, the users themselves, while ensuring all users are knowledgeable on the polices that are in place. Monitoring your environment has to play a huge role in your network design. Finally, threat and stress testing should be completed to ensure your network is as effective as the first day it went in to use. Network design is a balance of needs versus wants but by ensuring you have sound polices in place efficient administrators can maintain a healthy balance while keeping the network secure.

References

"About Tripwire - Leadership, Partners, Careers | Tripwire." Tripwire. Web. 08 Mar. 2016.

Al-Yaseen, Wathiq Laftah, Zulaiha Ali Othman, and Mohd Zakree Ahmad Nazri. "Real-Time Intrusion Detection System using Multi-Agent System." IAENG International Journal of Computer Science 43.1 (2016): 80-90. Web.

Chao, Jude. "Mitigating Network Security Vulnerabilities at Offsite Locations." Mitigating Network Security Vulnerabilities at Branch Offices and Remote Locations. Web. 05 Mar. 2016.

"Experts Found a Unicorn in the Heart of Android." Zimperium Mobile Security Blog Experts Found a Unicorn in the Heart of Android Comments. Web. 01 Mar. 2016.

Goodin, Dan. "Malicious Websites Exploit Silverlight Bug That Can Pwn Macs and Windows." Ars Technica. 25 Feb. 2016. Web. 10 Mar. 2016.

"How Many Fortune 500 Companies Have Been Hacked?" Money Morning We Make Investing Profitable. 2015. Web. 01 Mar. 2016.

Kerner, Michael. "Snowshoe Spam--a New Type of Junk Email--Starting to Clog Inboxes." Snowshoe Spam--a New Type of Junk Email--Starting to Clog Inboxes. 03 June 2014. Web. 10 Mar. 2016.

"Man-In-The-Cloud (MITC) Attacks ; Risk and Solution - Cloudmask." Cloudmask. 2015. Web. 01 Mar. 2016.

Mohamed, M. A., M E A Abou-El-Seoud, and A. M. El-Feki. "A Survey of VPN Security Issues." International Journal of Computer Science Issues (IJCSI) 11.4 (2014): 106. Web.

"Network Security Policy: Best Practices White Paper." Cisco. 4 Oct. 2005. Web. 01 Apr. 2016.

Piscitello, David M., and Lisa Phifer. "Best Practices for Securing Enterprise Networks." Business Communications Review; 32.0. (2002): 32-37. Web.

Rowan, Tom. "Application Firewalls: Filling the Void." Network Security 2007.4 (2007): 4-7. Web.

Singh, Jitendra. "Comprehensive Solution to Mitigate the Cyber-attacks in Cloud Computing." IJCSDF International Journal of Cyber-Security and Digital Forensics 3.2 (2014): 84-92.

Sobh, Tarek S., and Yasser Aly. "Effective and Extensive Virtual Private Network." Journal of Information Security 2.1 (2011): 39-49. ProQuest. 3 Mar. 2016 .

"The Internet Organised Crime Threat Assessment (iOCTA)." The Internet Organised Crime Threat Assessment (iOCTA). 29 Sept. 2014. Web. 10 Mar. 2016.

"Trends to Watch in 2014." IT Security Trends. Web. 01 Mar. 2016.

Triplett, James. "Securing the Enterprise Network." Telecommunications 30.4 (1996): 38. ProQuest. 3 Mar. 2016 .

"The Internet Organised Crime Threat Assessment (iOCTA)." The Internet Organised Crime Threat Assessment (iOCTA). 29 Sept. 2014. Web. 10 Mar. 2016.