Role of Network Security in Information Security Management

Brian Martin

East Carolina University

Introduction

The purpose of this paper is to show how crucial network security is to an organization by showing various attacks a network could face and by offering some solutions and best practices to help guard against them. In today's environment, cyber threats are growing faster than what security specialists can keep up with. According to a poll conducted on behalf of Trustwave, a survey of over 1,000 security specialists cited mounting pressures due to shortages in necessary skills, employee education and budget crunches. Close to 50 percent of these same professionals noted that organizations were steering towards cloud-based services instead of in-house systems (Auchard, 2015). The pressure to defend from these cyber attacks are mounting because they are costly to profits and images to businesses around the world. In 2013, Target suffered a massive data breach of 110 million customers due to poor information security management. This breach caused profits to drop from $921 million to $520 million, resulting in a loss of over $400 million (Harris, 2014). The aftermath additionally cost them over 100 million in settlements with VISA, Mastercard, multiple federal banks and states (Garcia, 2015). This is an enormous amount of money to lose due to poor network security. Some of the various attacks on networks include hacking, denial-of-service, viruses, worms, and trojan horses, which this paper will cover. Being able to limit an organization's exposure to these attacks greatly reduce the chances of being a victim like Target was. It is up to Networking or Information Security Management to provide a robust network to help limit security breaches. Finally, this paper will cover a few ways to help secure the organization's network is through firewalls, anti-virus software, intrusion detection systems, and VPNs (Virtual Private Network).

Denial of Service/Distributed Denial of Service

One of the first attacks to cover is denial-of-service (DOS) attacks and distributed denial-of-service (DDOS) attacks. These attacks occur when an attacker prevents users from accessing a networks data or services. The key difference between a DOS and DDOS attack are that multiple devices are used during a DDOS attack. These multiple devices can consist of other attackers helping or compromised machines that can launch these attacks on command. DOS attacks generally come either in the form of crashing services or flooding services. In flooding services, the attacker will consume bandwidth and router resources that eventually cause the network to congest or ultimately fail. In crashing services, the attacker will exhaust server resources to ultimately cause the server to crash rendering it's applications unavailable to users (Zagar, Joshi, Dipper, 2013).

For DDOS attacks, there are basically three types that are used. First is an application layer attack that targets software vulnerabilities that crash the server. The second type is a protocol DDOS attack that includes such tactics as Synfloods and Pings of Death. The third type of DDOS attack is a volume-based attack that includes Internet Control Message Protocol (ICMP), User Datagram Protocol (UDP) floods, and other floods of spoofed packets (Shankdhar, 2018).

Trojan Horses

Next, Trojan Horses are programs that have malicious code embedded inside legitimate programs or data. They infect systems when users open these malicious email attachments or download programs they think are legit. Trojans are like viruses in similar ways in that they are harmful programs that can damage, copy, block, or modify data as well as disrupt computer

performance. Unlike viruses though, Trojans do no replicate themselves and they are hard to detect because they appear to be useful programs or applications (Al-Saadoon & Al-Bayatti, 2011).

Trojans do not always show up immediately and can remain dormant until initiated. In 2014, Department of Homeland Security announced that hacked software had been found on critical infrastructure systems. This Trojan named "Black Energy" had been dormant on systems since 2011 without any attempt to activate it, but it was believed to be part of a Russian cyber-espionage effort (Cloherty & Thomas, 2014). Trojans can be broken down into three main categories. Hopping and McCallion (2018) describe these categories as backdoor Trojans, downloaders, and banking Trojans. Backdoor trojans allow an attack to access and control a user's computer remotely. Banking Trojans generally target financial data and uses stored cookies to redirect victims to scam sites to steal login credentials. A downloader Trojan acts as a dropship for other malware to be loaded onto a victim's computer (Hopping & McCallion, 2018)

Worms

Continuing with malware threats, computer worms are another tool used to exploit network security and flaws in computer services. A computer worm is a program that spreads itself across various platforms and networks by targeting other systems and replicating itself. The main difference between a worm and a virus are that viruses generally require user actions to help propagate itself while most worms do not (Weaver, Paxson, Stanford, & Cunningham, 2003). A computer worm has a life cycle that follows several phases. In phase one, the worm scans for a victim by way of a target discovery. Once a target is found, its second phase is exploiting the victim by means of malicious code that allows access to a victim's computer. The

third phase is when the worm executes its payload that the creator wrote. This can include opening backdoors, deleting files, stealing passwords, and other malicious actions with negative impacts. Once the payload has been executed, the fourth phase of the worm cycle means copying itself onto the victim so that it can discover and spread to other victims. The last phase is what makes worms so deadly. In this phase, the worm uses stealth techniques to mask its presence on the victim's computer. They can hide processes that are running, delete logs, and other assorted actions to cover its tracks (Rajesh, Reddy, & Reddy, 2015). Worms are not new to technology and have been around since the beginning of the internet. The first main worm hit back in 1988 and ended up infecting around 60,000 machines (Eichen,& Rochlis, 1988). This was named the Morris worm after Robert Tappan Morris and it targeted DEC VAX machines and Sun machines (running BSD Unix) that were connected to the internet (Rajesh, Reddy, & Reddy, 2015). Not only can worms create havoc on the software platforms, but now they can be used to target crucial hardware as well. The first known weaponized worm was discovered in 2009 and was named Stuxnet. What made this worm so unique is that it was designed to limit its spread to a local network, and to machines that were running software called Simatic WinCC Step 7 by Siemens. Iran happened to be the intended target of this worm, and the engineers were using the software to control its nuclear centrifuges. Not until several centrifuges had been replaced, and a couple of computers acting weird did they reach out to find what could be the cause. After much research, it was finally discovered that this worm was done by the work of professionals, and that it included many "zero day" exploits within this one worm. Zero-day exploits are vulnerabilities not yet known in software and they are very rare. (Zetter, 2011)

Viruses

Computer viruses have become a growing nuisance with the internet expanding, and they cause billions in damages annually. Sivanandam & Rajarajes (2014) note that a virus is a computer program designed to replicate and spread itself to other devices without users knowing. Unlike computer worms, the main point about viruses is that they require user actions to be executed. Viruses often attach itself to system files, which could result in the deletion, modification, or overwriting of these files. They then seek to replicate itself onto other hosts on the network while masking its presence in system files and processes. Viruses will continue to advance in its methods as technology moves along (Sivanandam & Rajarajes,2014). Although viruses cannot damage computer hardware, they can delete files, destroy data, format hard drives and even replace or modify boot records, Viruses spread in numerous ways and some of them include infected flash drives or disks, email attachments, infected websites, pirated software and networks (Khan, 2013). The important aspect is that users are trained in being able to detect symptoms of a virus. These following indicators from Khan are a few signs that one might be infected with a virus:

- Computer runs slower than normal.
- Computer stops responding, locks up frequently, crashes or restarts on its own.
- Applications and software that does not work correctly.
- Unable to access disks or drives.
- Errors in printing items.
- Random and unusual error messages.
- Double extensions on attachments.

- Anti-virus disabled on its own, nor can it be restarted.
- Anti-virus program cannot be installed on computer.
- New icons that appear on desktop.
- Windows Task Manager unavailable.
- Insufficient memory error messages even though there is plenty of RAM.
- Programs disappear from the computer without being removed by user or other staff.
- Strange sounds or music plays randomly.

Armed with this knowledge, users can help identify when a virus has infected their machine so that network and security staff can investigate further (Khan, 2012).

Hackers

Lastly, hackers have been around for quite a while, but its meaning has not always been the same. The term "hacker" was originally coined in the 1960's to reference someone capable of developing incredible solutions to a programming problem. This definition eventually morphed over decades to represent a programmer with criminal intent (Knight, 2006). Madore (2016) lists three different types of hackers. First, the "black hat hackers" are ones that generally seek profit or do their work for nefarious means. When we think of hackers, this the type that is generally associated with the term hacker. Not all black hat hackers are criminals either, some work for state agencies whose job is to infiltrate systems in other countries to carry out government missions. The next type of hacker is the "white hat hacker". These individuals generally hack to help expose exploits, so these holes can be closed. They often share their work on various communities and websites dedicated to exposing bugs and vulnerabilities found in various applications. Often these good deeds are rewarded financially by organizations. The last type of

hacker is called the “gray hat hacker “and they generally straddle the line between white and black hat hacking. It’s possible that a gray hat could perform a white hat hack and a black hat hack in the same day. Motivations vary greatly when it comes to hacking. Some have a noble purpose such as Edward Snowden, and others may have a mischievous or nefarious motive (Madore, 2016).

According to Chuck Brooks, 2016 was an alarming year for increases in security breaches. He goes on to point out some eye-popping stats that include the following:

1. There is a hacking attack every 39 seconds.
2. One in three Americans were hacked in 2016.
3. Government, retail, and technology industries accounted for 95% of data breaches.
4. An estimated one billion records were compromised worldwide in 2016.
5. Small businesses account for 43% of cyber-attacks.
6. Cybercrime will cost businesses over $2 trillion by 2019.
7. Info-security spending will exceed $1 trillion from 2017-2021.
8. Over 75% of the health care industry has been infected with malware in the past year.
9. Average time to detect a malicious or criminal attack was 170 days.
10. Around 50 billion devices are expected to be connected to the internet by 2020.

These are just a few of the statistics out there that show just how important safeguarding against hacking has become. These threats will only continue to grow, especially in the areas of social engineering and phishing (Brooks, 2017) Network security is of crucial importance in information security management. As documented earlier in this paper, there are many threats that network and security administrators have to guard for to keep the integrity of their networks.

There is a lot of pressure on these administrators because these breaches and attacks are generally reflected in lost revenue. There are ways that networking and security management can reduce the likelihood of their networks being penetrated or compromised. Firewalls, anti-virus software, intrusion detection and prevention systems, and virtual private networks (VPN) are a few ways to help secure a network.

Firewalls

According to the United States Computer Emergency Readiness Team (US-CERT), a firewall is defined as a device that "provides protection against outside attackers by shielding your computer or network from malicious or unnecessary network traffic and preventing malicious software from accessing the network." (US-CERT, 2015) Firewalls are an integral part of any organization's network or information security defense. How effective they are depends on the engineers that configure them, and the security policies that drive them. With so much riding on the security of an organization, some practices should be implemented to minimize breaches and maximize performance. Harvey (2018) mentions some of these practices that include the following:

1. Document firewall rules and changes.
2. Follow a change procedure for any firewall configuration modifications.
3. Re-access firewall rules routinely.
4. Discard unused or repetitive firewall rules
5. Audit the logs
6. Keep up to date on firewall software and firmware.
7. Maximize performance by using routers to filter some traffic blocking.

Expanding on these, we first start with the documenting practice. Documentation is key to any network or security team. This allows other team members or management to see the purpose of the rules, the services, devices and users it affects, when the rule was added and who added it. Secondly, whenever any firewall configuration changes need to be made, follow department or organizational procedures in making these modifications. This includes letting the other departments and management know of the changes being made, when they will be made, and the potential impacts it could have on other services. Thirdly, since exploits often change frequently, it is best course of action to review firewall rules regularly and update them as necessary. This made include adding recently exploited TCP or UDP ports not currently on the firewall rules. Another reason to review the rules regularly is because of changes in the organization. New users, new devices, departments moving from one building to another. These are some examples why it is imperative to stay current on the firewall rules. This ties into the fourth practice of discarding unused or repetitive rules. During the rules review, it is prudent to delete any unused or repetitive rule found. This cuts back on unnecessary processing by the firewall and allows the engineer to maximize its performance. Fifthly, auditing firewall logs helps a network or security team check for any anomalies that could suggest modifications made to the firewall, and they can help with detecting false positive readings that can be minimized by adjusting the firewall rules. Sixthly, keep the firewall's software and firmware updated regularly. Make sure to research any code or firmware that will be upgraded. Newer versions of code not properly tested can end up leaving a network or security team exposed. In the case of Cisco products, they normally have a star next to the newest code that they recommend (Harvey, 2018).

VPNs

In addition to firewalls, Virtual Private Networks (VPN) offer a good way to secure traffic from remote clients or branches to an organization's network. VPNs create an IP Security (IPSec) or Secure Sockets Layer (SSL) tunnel between you and the VPN server (Vaughan-Nichols,2018). This traffic is encrypted keeping the data traversing this tunnel secured. These tunnels are ideal for InfoSec managers in organizations with remote branch offices, users that work remotely, or vendors that may need access to organizational resources. A major point about VPN security is that data is only secured from point A to point B. If networks or devices at either end points are compromised, then the data will also be potentially compromised as well. VPNs should be thought of as an addition to network security that helps secure the traffic flowing between remote sites and users. Securing the networks and devices at each end should not be neglected due to simply having a VPN. Bourque (2017) article lists the following five benefits to organizations using VPNs:

1. VPNs greatly reduce risk of security breaches and cyber-attacks
2. VPNs encourage productivity with workers feeling more secure while on public networks.
3. VPNs make clients feel secure about collecting and sharing data.
4. VPNs let you travel abroad internationally and still be "local".
5. VPNs are affordable.

There is essentially no reason not to use a VPN if your organization has remote workers, clients or off-site locations. The benefits outweigh any potential negative for not having it.

Anti-Virus Software

Anti-virus software is in more demand than ever as internet viruses and malware threats grow. While they are not full proof, they provide the bare necessity that devices need to guard against malware. Hoffman (2016) notes some good practices when it comes to using anti-virus software on an organization's network. The software should be loaded onto each computer and server with real time protection turned on. The software also should be set to automatically download the virus definitions regularly, with full scans scheduled periodically. Limiting user rights on the machines is key to helping with unwanted scripts or executable programs being ran. It also helps with allowing any settings in the anti-virus program to be changed by users that could potentially expose it to harmful attacks. Anti-virus software bases its detecting off signatures of viruses, trojans and other malware. Similar patterns and signatures will produce an alert from the software of potential malicious software and would prevent it from running by quarantining it.

Intrusion Detection and Prevention Systems

The final equipment covered in this paper will be the Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS). Snyder (2018) relates IPS devices to firewalls in that they both sit between two networks and allow data to pass through based on implemented policies. The main reason for an IPS being on the network is so that known attacks can be blocked across the network. This is great for system administrators when patches for systems must be applied when new exploits hit. The IPS will allow admins time to secure the devices by blocking the exploit and securing the network in the meantime. IDS systems on the other hand sit

on the side and monitor traffic at designated points. They help detect intrusions as they are happening, and offer a security team visibility to some of the following:

- Security policy violations
- Infections, viruses or trojan horses.
- Information leakage such as key loggers and spyware
- Configuration errors on systems. (security/firewall)
- Unauthorized clients or rogue DHCP/DNS servers.

There are manufacturers that make devices that encompass both IPS and IDS capabilities so choosing which device is right is a decision that the network and security team will have to decide on. (Snyder, 2018) There are some general best practices that should be considered when deploying IDS/IPS devices. Pappas (2008) notes some of these practices in his SANS Institute article. He first suggests using network segregations for your organization to help provide additional security. It also helps InfoSec teams to isolate compromised machines faster, while allowing the uncontaminated zones to operate as normal. Next, IPS devices are connect to the network via in-line method. This means that all the data flows through the device as it comes and goes. The main drawback to this is that all network traffic will cease if the device fails. To overcome this limitation, they do have models that allow traffic pass through even in the event of power failure. Next, he mentions when connecting an IDS, the optimum way to monitor traffic is through a span port on a managed switch. This prevents having an outage with an in-line setup and still allows all the data passing through to potentially be monitored on that span port. Lastly, he suggests the potential of pairing up IDS/IPS systems at the same location or in multiple strategic locations throughout the network. This would allow an InfoSec team to run a detection

and prevention system simultaneously while updating policies or rules in real time. Obviously, this solution would be costly and would be something management would have to consider when weighing their options on network security. (Pappas, 2008)

In conclusion, there are many ways and paths for information security management to take when it comes to protecting an organization's networks. Do the costs justify the benefits or do the risks outweigh the costs? These questions are entirely dependent on an organization's value on network and data integrity and should be made collectively when deciding. As technology grows though, security will eventually have to enter the discussion regardless of the organization. There are other cyber threats and protection not covered in this paper which good network and security teams should seek out. Being prepared to handle a threat is half the battle.

References

*Al-Saadoon, G. & Al-Bayatti, H. (2011). A Comparison of Trojan Virus Behavior in Linux and Windows Operating Systems. *World of Computer Science and Information Technology Journal, 1(3), 56-62.* Retrieved from *http://pub.wcsit.org/1.3.2011*

Auchard, E. (2015). Fast-Changing Security Threats Overwhelm IT Managers: Survey. Retrieved from www.reuters.com/article/us-cybersecurity-survey-idUSKBN0M727H20150311.

Bourque, A. (2017). 5 Ways your Company Can Benefit from Using a VPN. Retrieved from https://www.computerworld.com/article/3184651/networking/5-ways-your-company-can-benefit-from-using-a-vpn.html

Brooks, C. (2017). Keep Calm And… Here Is A List of Alarming Cybersecurity Statistics. Retrieved from https://www.itspmagazine.com/from-the-newsroom/keep-calm-and-here-is-a-list-of-alarming-cybersecurity-statistics

Cloherty, J. & Thomas, P. (2014). 'Trojan Horse' Bug Lurking in Vital US Computers Since 2011. Retrieved from https://abcnews.go.com/US/trojan-horse-bug-lurking-vital-us-computers-2011/story?id=26737476

Cooper, M. (2016). Adventures in ethical hacking. *Itnow, 58*(3), 36-37. doi:10.1093/itnow/bww074

Durrani, A. (2016). How Blizzard Should Prepare for Next Wave of DDos Attacks. Retrieved from https://venturebeat.com/2016/08/31/how-blizzard-should-prepare-for-next-wave-of-ddos-attacks/

Eichin, M. & Rochlis, J (1989). With Microscope and Tweezers: An Analysis of the Internet Virus of November 1988. Retrieved from https://ieeexplore.ieee.org/document/36307/

Garcia, A. (2015). Target Settles for $39 Million over Data Breach. Retrieved from https://money.cnn.com/2015/12/02/news/companies/target-data-breach-settlement/index.html.

Harris, E. (2014). Data Breach Hurts Profit at Target. Retrieved from www.nytimes.com/2014/02/27/business/target-reports-on-fourth-quarter-earnings.html.

Harvey, C. (2018). Fine-tuning Firewall Rules: 10 Best Practices. Retrieved from https://www.esecurityplanet.com/network-security/firewall-types.html

Hoffman, C. (2016). How Antivirus Software Works. Retrieved from https://www.howtogeek.com/125650/htg-explains-how-antivirus-software-works/

Hopping, C. & McCallion, J. (2018). What is a Trojan Virus? Retrieved by http://www.itpro.co.uk/security/30081/what-is-a-trojan-virus

*Khan, I. (2012). An introduction to computer viruses: problems and solutions. *Library Hi Tech News, Vol. 29 Issue: 7, pp.8-12,* https://doi.org/10.1108/07419051211280036

Khan, J. (2013). What is a Computer Virus?. Retrieved from http://www.byte-notes.com/what-computer-virus#simple-table-of-contents-1

Knight, W. (2006). Introduction: Computer Viruses. Retrieved from https://www.newscientist.com/article/dn9920-introduction-computer-viruses/

Madore, P.H. (2016). What is a Hacker? An Overview of Hacking History and the Evolution of the Term Hacker. Retrieved from https://hacked.com/hacker/

McDowell, M. (2009). Understanding Denial-of-Service-Attacks. Retrieved from https://www.us-cert.gov/ncas/tips/ST04-015

*Natarajan, S., & Rajarajesware, S. (2014). Computer Virus: A Major Network Security Threat. *International Journal of Innovative Research and Development*, *3*(7), 299-302. Retrieved from http://www.ijird.com/index.php/ijird/article/view/51690

Pappas, N. (2008). Network IDS & IPS Deployment Strategies. Retrieved from https://www.sans.org/reading-room/whitepapers/intrusion/network-ids-ips-deployment-strategies-2143

*Rajesh, B., Reddy, J. & Reddy, B. (2015). A Survey Paper on Malicious Computer Worms. *International Journal of Advanced Research in Computer Science & Technology*, *3(2),161-167.* http://ijarcst.com/doc/vol3issue2/ver2/brajesh.pdf

US-CERT Publications. (2015). Security Tip (ST04-004) Understanding Firewalls. Retrieved from https://www.us-cert.gov/ncas/tips/ST04-004

Vaughan-Nichols, S. J. (2018). How to Use a VPN to Protect Your Internet Privacy. Retrieved from https://www.zdnet.com/article/how-to-use-a-vpn-to-protect-your-internet-privacy/

Shankdhar, P. (2018). Best DOS Attacks and Free DOS Attacking Tools. Retrieved from https://resources.infosecinstitute.com/dos-attacks-free-dos-attacking-tools/

Snyder, J. (2009). Do You Need an IDS or IPS, or Both? Retrieved from https://searchsecurity.techtarget.com/Do-you-need-an-IDS-or-IPS-or-both

Weaver, N., Paxson, V., Staniford-Chen, S., & Cunningham, R.K. (2003). A Taxonomy of Computer Worms. *Proceedings of the ACM CCS First Workshop on Rapid Malcode (WORM 2003), 11-18.* DOI: https://doi.org/10.1145/948187.948190

Zargar, S.T., Joshi, J. & Tipper, D. (2013). A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks. *IEEE Communications Surveys & Tutorials, 15(4), 2046-2069*. DOI: 10.1109/SURV.2013.031413.00127

Zetter, Kim. (2011). How Digital Detectives Deciphered Stuxnet, The Most menacing Malware in History. Retrieved from https://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/