Assignment 1: Action Plan for Network Security

Sarah Gillard

CS202: Network and System Security

March 13, 2024

Assignment Prompt

In your role as a novice network security professional, you are assigned the responsibility of crafting a comprehensive network security plan for your organization. Detail 3-5 prominent threats that the network is bound to encounter and provide a strategic action plan to mitigate these risks. Ensure that your paper falls within the specified word range of 1,500 to 2,000 words.

Threat Analysis

Network security is paramount for organizations to safeguard assets and sensitive information from threats. I will identify and analyze a few key threats that networks commonly face.

1. **Malware**:

   Malware combines the words “malicious” and “software.” It is used to describe any type of bad code found on a computer. Any software that gets installed on your device that performs some unwanted or harmful task qualifies as malware (Nott, C., 2017). There are many types of malware, but I will identify some types that are more frequently found.

   A computer virus is a type of software that spreads (like a human virus) and affects one area of a computer system before making copies of itself throughout the system. A virus can begin in the network router and spread, damaging and destroying files and continuing to spread through email messages. A user usually has to perform an action, such as opening a malicious link to spread.

   A worm is a type of malware that can spread without any human interaction, unlike a virus which usually begins with a human action such as visiting a malicious website (Nott, C., 2017). A worm can spread throughout the devices on a network and allow hackers to remotely access your computer. Worms and viruses both cause damage to computer systems and should be prevented.

   A trojan horse is a computer program that hides malware such as a virus or worm. It may appear to be doing something, such as downloading software you wanted when it’s unleashing malware to damage your computer.

   Spyware can spread like a virus or worm, but it has a specific intent to steal private information from your computer for a third party (Nott, C., 2017). Spyware can even track what keys you type, assisting in stealing your most confidential information. Spyware often causes a system to slow down and is a major privacy concern.

2. **Internet Protocol Spoofing**:

   Internet Protocol Spoofing (IP Spoofing) occurs when hackers alter the message header of a sent email and edit the source address to make it appear that the emails the hacker is sending are from a trusted source (Griffin, L., 2017). There are two types of IP Spoofing-man-in-the-middle attacks and denial-of-service attacks.

A man-in-the-middle attack occurs when a hacker gains unauthorized access to the network infrastructure and positions themself between two communicating devices (Weda, M., 2021). The access can be gained through exploiting vulnerabilities in the network such as gaining access to the router or cracking weak security measures, or through an insecure Wi-Fi network. Once inside the network, the “man-in-the-middle” can manipulate traffic and intercept sensitive information and exchanges between two devices. A victim can be deceived into thinking a received message is authentic and from the sender who is compromised when it is the hacker.

A denial of service (DoS) attack occurs when a hacker intercepts the message packet between a sender and receiver with a spoofed source address. The recipient is flooded with more packets than their bandwidth can support, overloading and shutting down the victim’s system (Griffin, L., 2017).

3. **Phishing Attacks:** Phishing attacks exploit human vulnerabilities by tricking individuals into sharing sensitive information such as passwords or financial data. This is often done through the use of deceptive email messages or websites (Beckert, K., 2016). An email may appear to come from a reputable business but it’s a hacker committing a social engineering attack.
4. **Zero-Day Vulnerabilities:** A zero-day vulnerability arises when hackers exploit an undiscovered security flaw in software, which is unknown to the developers. The term originates from the fact that developers have “zero days” to address the issue since it’s already active. The immediate focus for the software team is to limit unauthorized access to sensitive data, typically through the swift deployment of a patch (Oglesby, K., 2016). Efforts are directed toward understanding the root cause of the vulnerability and implementing proactive measures to detect and mitigate potential future vulnerabilities before they act.

Malware, IP spoofing, phishing attacks, and zero-day vulnerabilities are all some of the major threats to your network. They all cause operational disruptions. Malware targets various endpoints and systems. IP Spoofing targets servers and websites. Phishing uses social engineering to manipulate and deceive to carry out an attack. Phishing can cause reputational damage as it targets users on the server. Zero-day vulnerabilities expose and utilize security flaws in software to carry out attacks. Some of these security threats involve a user opening deceiving links, while others involve a user being manipulated and deceived through social engineering attacks like phishing. Other threats like some forms of malware and IP spoofing can occur due to weak network security. As you can see, there are many different threats to the network caused by different weaknesses in security, so it is vital to analyze the network and plan proper security measures.

Action Plan

Network intrusion detection, firewalls, encryption, wireless security, and authentication are essential components to prevent various network security threats such as malware, IP spoofing, phishing attacks, and zero-day attacks. Each of these technologies can contribute to mitigating these threats, as well as other threats to the network.

Network intrusion detection systems (NIDS) monitor network traffic in real-time to identify and alert network administrators about suspicious activities or potential security breaches. IDS can detect and block known signatures, anomalies that indicate IP spoofing attempts, and patterns associated with phishing attacks. IDS can also help detect zero-day vulnerabilities as it monitors for anomalies in real-time. There are two types of intrusion detection systems. A network intrusion detection system is placed within the network at various points and secures resources on the network, but the IDS at various points can cause bottlenecks that make it a slower IDS than host intrusion detection (Gloag, D., 2017). A host intrusion detection system is placed at each device on a network so that all access points are fully covered. This provides better coverage but requires more money and maintenance (Gloag, D., 2017).

Firewalls act as a barrier between the trusted internal network and untrusted external networks by filtering incoming and outgoing network traffic based on security rules set by an administrator (Cruz, L., 2016). Firewalls can block suspicious connections from devices infected with malware, prevent IP spoofing by filtering out spoofed packets, and restrict access to known phishing websites. Firewalls help prevent unauthorized access to network resources and reduce the attack potential for zero-day vulnerabilities.

Encryption ensures the confidentiality and integrity of data by encoding it in a format that can only be deciphered by authorized recipients. Secure Socket Layer (SSL) provides encryption and authentication mechanisms for securing communication over the internet through the use of a private key and a public key (Gibbs, M., 2016). SSL encryption protects against man-in-the-middle attacks by encrypting data exchanged between clients and servers, mitigating the risk of tampering. Encryption protects sensitive information stored in databases or transmitted over wireless networks, which reduces the likelihood of data breaches from SQL injection (when hackers write malicious SQL queries and create malicious changes to a database). The Secure Hypertext Transfer Protocol (HTTPS) defines the set of rules that the web server and browsers need to follow (Aravindan, S., 2015). HTTPS encrypts data transmitted between clients and servers, ensuring confidentiality and

integrity. HTTPS is recommended as HTTP transmits data in plaintext. HTTPS uses the Advanced Encryption Standard (AES) to secure the communication.

Authentication mechanisms such as passwords, biometrics, and multi-factor authentication validate user identity and devices accessing network resources. An iris scan is a good way to utilize biometric authentication as it is not as invasive of employees as the retina scan which can reveal employee health information. An iris scan recognizes the color pattern of your iris. A fingerprint is another biometric authentication tool that may work well, but it can have issues if a nefarious employee or outsider uses tape or a gummy bear to obtain a coworker's fingerprint. Passwords should be at least 10 characters long and have uppercase and lowercase letters as well as symbols. Strong authentication procedures help prevent unauthorized access to sensitive information and reduce the risk of phishing attacks that may target user credentials.

These technologies can help the organization enhance network security and mitigate the risks posed by malware, IP spoofing, phishing attacks, zero-day vulnerabilities, and other security threats. This plan will help safeguard sensitive information from network threats.

References

Aravindan, S. (2015, October 6). *Hypertext Transfer Protocol | HTTP Definition & Process.* Study.com. https://study.com/learn/lesson/what-is-hypertext-transfer-protocol-examples.html

Beckert, K. (2016, October 3). *Network Security Threats: Types & Vulnerabilities*. Study.com. https://study.com/academy/lesson/network-security-threats-types-vulnerabilities.html

Cruz, L. (2016, July 2). *What is a Firewall in Network Security? - Role & Use*. Study.com. https://study.com/academy/lesson/what-is-a-firewall-in-network-security-role-use.html

Gibbs, M. (2016, June 16). *IPsec vs. SSL*. Study.com. https://study.com/academy/lesson/ipsec-vs-ssl.html

Gloag, D. (2017, May 1). *Intrusion Detection Systems (IDS) in Data Security*. Study.com. https://study.com/academy/lesson/intrusion-detection-systems-ids-in-data-security.html

Griffin, L. (2017, April 11). *Spoofing Attack | Definition & Types*. Study.com. https://study.com/academy/lesson/what-is-a-spoofing-attack-definition-types.html

Nott, C. (2017, September 7). *Malware | Meaning, Types & Examples*. Study.com. https://study.com/academy/lesson/what-is-malware-definition-examples-types.html

Oglesby, K. (2016, July 1). *What is Zero Day Vulnerability?* Study.com. https://study.com/academy/lesson/what-is-zero-day-vulnerability.html

Weda, M. (2021, November 15). *Cybersecurity Overview, Principles & Policies*. Study.com. https://study.com/learn/lesson/cybersecurity-overview-principles.html