Module 7 Lecture Assignment

by Daniel A. Moreno

Policy Statement 1: Remote Access

1 Overview and Purpose:

In the modern world, remote access to the corporate network is essential to maintaining the company's productivity and efficiency. This policy will establish the information security standards for the remote accessing of XYZ's corporate network in an effort to ensure the confidentiality, integrity, availability, and regulatory compliance of the protected health information therein.

2 Scope:

This policy applies to all XYZ employees, contractors, vendors, business partners, and agents with a company-owned or personally-owned computer that is used to remotely connect to the corporate network. This policy applies to remote access connections used to do work on behalf of XYZ, including reading or sending email and viewing intranet web resources. The is policy covers any and all technical implementations of remote access used to connect to the corporate networks.

3 Policy:

3.1 Session Termination

3.1.1 The system must provide a logout capability for any session that required authentication to begin. This should securely terminate the session such that all session keys are canceled and a replay attack cannot be conducted.

3.1.2 The system must display an explicit logout message to ensure that the user is aware of whether the session securely and properly terminated. This will prevent session hijacking or errors with certain protocols like FTP which require final logout messages prior to termination.

3.2 Confidentiality and Integrity

3.2.1 All remote access of the corporate network should utilize an acceptable encryption as defined by the transmission confidentiality and integrity policy.

3.2.2 The remote access traffic should be routed through authorized and managed points. The number of these points should be minimized to reduce the attack surface.

3.2.3 Secure methods of authentication for users and remote commands should be implemented to prevent unauthorized commands and the replay of authorized commands. Multi-factor authentication and randomly generated session keys are a significant portion of this.

3.2.4 The remote access technology should be used in tunnel mode, thereby protecting both the header and payload of the transmitted packet. This helps to obscure the topology of the corporate network from footprinting and fingerprinting efforts.

3.3 Remote Computers

3.3.1 When a computer is remotely connected to the corporate network, authorized users must ensure that the remote host is not simultaneously connected to any other network. The

exceptions are personal networks completely controlled by them or another authorized party.

3.3.2 All hosts remotely connected to the corporate network through a remote access technology should meet the requirements stated in the hardware and software configuration policy. This includes but is not limited to updated anti-virus software and an up-to-date operating system.

3.3.3 Access to the remote host should be restricted such that the authenticated user has a unique account.

3.3.4 The remote host should only use known and trusted software.

3.4 Monitoring

3.4.1 All usage of remote access methods should be logged, and these logs should be regularly reviewed to detect attacks and ensure compliance with other policies.

Policy Statement 2: Boundary Protection

1 Overview and Purpose:

An effective system of boundary protection addresses both internal and external risks. While the Internet and the threats inherent to it are beyond the control of XYZ, we possess the responsibility to mitigate these external threats. In addition, well-designed boundary protection can prevent data exfiltration by employees and other insider threats. This policy will establish the information security standards for traffic between the Internet and intranet in an effort to ensure the confidentiality, integrity, availability, and regulatory compliance of the hardware, software, and firmware within the intranet.

2 Scope:

This policy applies to all XYZ employees, contractors, vendors, business partners, and agents with a company-owned or personally-owned computer that communicate through the boundary of the internal network, whether it be inbound or outbound. This policy applies to all connections and traffic between the Internet and intranet along with the technical controls that separate the Internet and intranet.

3 Policy:

3.1 Demilitarized Zone

3.1.1 The DMZ should contain everything that is publicly accessible by those that are not employed by XYZ.

3.1.2 All Internet of Things devices and wireless access points should be placed within the DMZ to compensate for their weak security status.

3.1.3 When placing nonsecurity-related functions and services in the DMZ, the number and complexity of the functions should be minimized. This will reduce what must be trusted and what needs to be monitored by security personnel.

3.1.4 For a DMZ to function properly, the DMZ's contents must be sufficiently separated from the Internet and the internal corporate network. The DMZ should be placed on a physically distinct subnet. With a firewall filtering traffic from the Internet, the DMZ will be a screened subnet with an n-tier configuration functioning as a buffer between the uncontrollable Internet and the confidential intranet.

3.1.5 All communication between the DMZ and the intranet should be encrypted before passing through a firewall and a IPX/SPX protocol switching deadzone to prevent a variety of attack classes. This traffic can be handled by proxy servers which function as intermediaries and can log everything for later auditing. In addition, these measures prevent the discovery of internal components.

3.2 Traffic Filtering

3.2.1 All firewalls should be set to block traffic by default and allow by exception. All such exceptions should be clearly documented in the appropriate policy. In some cases, it is prudent to explicitly deny certain traffic.

3.2.2 Based on an IP or email address' reputation, you may want to explicitly block traffic from that source. This could be private reputation where the system recognizes it as the source of a previous attack or a reputation established by a blacklist purchased from a vendor. This list may change dynamically as the IDPS responds to emergent threats. In addition, all incoming traffic from an internal IP address should be blocked under the assumption that it is spoofed.

3.2.3 Unless a session was initiated internally, traffic should not be permitted beyond the DMZ into the intranet.

3.2.4 Both inbound and outbound traffic should be filtered in accordance with HIPAA, PCI DSS, and other similar data loss prevention regulations.

3.2.5 Due to the fact that a firewall cannot filter encrypted traffic, the outer firewall should be the endpoint for all encrypted traffic. This will allow it to properly analyze its contents and forward it to the correct destination, should the traffic not be blocked.

3.2.6 Controls should be in place to prevent unauthorized changes to the filtering rules. This includes but is not limited to out-of-band management and unique administrative credentials.

3.3 Transmission Protocol Measures

3.3.1 The boundary protection controls should enforce adherence to protocol formats. Malformed packets should not be permitted, regardless of whether the malicious alteration exists in the header or payload.

Policy Statement 3: Transmission Confidentiality & Integrity

1 Overview and Purpose:

As a healthcare organization that is paid with credit cards, XYZ's network must transmit a large quantity of sensitive information which it has a high regulatory obligation to protect. This policy will establish the information security standards for the transmissions on XYZ's corporate network in an effort to ensure the confidentiality, integrity, availability, and regulatory compliance of the protected health information therein.

2 Scope:

This policy applies to all XYZ employees, contractors, vendors, business partners, and agents with a company-owned or personally-owned computer that transmit messages on the internal network or through the boundary on to the Internet. This policy applies to all connections and traffic between the devices on the internal corporate network, along with transmissions to the Internet.

3 Policy:

3.1 Transmission Protocols

3.1.1 The Transmission Control Protocol (TCP) should be utilized to help ensure the integrity of all messages transmitted. Due to the three-way handshake and variety of error-checking functions, TCP will automatically detect when a packet is unsuccessfully transmitted or is altered during transmission, prompting it to resend that packet.

3.2 Encryption

3.2.1 All traffic should be encrypted using end-to-end encryption technologies, like TLS or IPSec, to ensure that intercepted information is unusable. Encryption prevents the modification of the transmission since one would need to understand the text to alter it. This encryption should extend to the packet header and routing information such that information regarding the intranet's topology is not revealed should the packet be captured.

3.2.2 All messages of a certain sensitivity should contain message digest generated by a cryptographic hashing function and encrypted with the sender's private key. This will allow the recipient to determine the message's integrity and authenticity.

3.3 Wire Protection

3.3.1 Fiber-optic cables should be used to transmit any data that requires a high level of confidentiality. They offer a greater degree of acoustical, electrical, and electromagnetic protection, partially due to the difficulty associated with terminated or splitting a fiber-optic cable. Also, the electrons moving through a twisted-pair network cable to transmit data will generate electromagnetic radiation. From up to a half-mile away without any physical access, an attacker can detect that radiation and translate it into understandable bits.

3.3.2 TEMPEST shielding should be installed in data centers that require an especially high level of security. This shield will prevent Van Eck phreaking and the detection of EMR generated by traditional copper-based cabling as data is viewed and transmitted.

Requirements for Controls Listed Above

To implement the three control classes detailed above, there exists a variety of requirements. Three controls exist across the policies that build upon each other: authentication, encryption, and secure logout. Multifactor authentication necessitates specialized equipment since a Type I authentication measures only uses a keyboard while Type II measures need card readers or token ports. Type III measures utilize biometric scanners that are extremely advanced and expensive, which must be accounted for should we choose to use them. While encryption protects data at rest and in motion very effectively, the processing necessary to encrypt and decrypt information can be very time consuming, especially since it must be done every time that data is read or written. This is only enhanced by the fact that traffic encryption should affect both the header and the payload of the packets. Also, encryption keys must be stored in a secure manner along with backups, should the originals be corrupted or lost. All of these incentive thin clients where all processing and data management occurs in a physically distinct and secure location. This would allow XYZ to acquire the necessary TPM chips and ASICs for efficient encryption handling at a lower price than if we implemented these measures for every workstation. They can also handle the calculation of message digests which are attached to a message to prove authenticity and integrity. In addition, firewalls will need to be set as encryption and remote access tunnel endpoints as they still need to filter that type of traffic. Proper logout procedures will ensure that the session is correctly terminated in such a way that attackers cannot hijack or restart it. All traffic will need to be routed through the proxy servers in the DMZ, unless its ultimate destination is a server within the DMZ. A properly-constructed DMZ compensates for the lack of inherent security in many devices as well as the risk-filled nature of allowing outside users to access any part of the corporate network. With firewalls on each side of the DMZ and a protocol switching deadzone, traffic can be properly filtered while proxy servers log everything that passes through them. The creation of this deadzone is difficult since IPX/SPX components are uncommon and require special transformers to convert between them and TCP/IP for the Internet and intranet. However, this eliminates a massive variety of attacks that require on specific packet types. The filter rules should be set to deny everything and allow by exception. Suggested allowances can be acquired from vendors and professional organizations. An IDPS should be linked to the firewall, allowing it to dynamically tweak the filter rules to block attacks. Due to the importance of firewalls, strict measures should be put in place, like three factor authentication and separation of roles, to ensure that only authorized individuals alter the ruleset. Due to the sensitivity of radiation and energy detectors, special measures must be taken to ensure confidentiality on this level. Fiber-optic cables and TEMPEST shielding for both cables and the room will prevent EMR translation and Van Eck phreaking. While these are extremely useful and can be the only way to guarantee physical confidentiality or compliance in certain situations, the necessary optical couplers, transformers, signal filters, and Faraday cages tend to be expensive. These are a brief list of the requirements associated with the three policy statements for remote access, boundary protection, and transmission confidentiality and integrity.

Works Cited

Consensus Policy Resource Community. *Remote Access Policy*. SANS Institute, Oct. 2022, assets.contentstack.io/v3/assets/blt36c2e63521272fdc/bltc96a4c2cb0dcef43/636db4142e16be076e6e003f/Remote_Access_Policy.pdf.

HIPAA and HITECH Requirements for Remote Access to a Healthcare Facility. SecureLink, 2020, www.hipaajournal.com/wp-content/uploads/2020/09/WhitePaper_HIPAA_HITECH_Compliance.pdf.

"Information Security." *George Washington University*, compliance.gwu.edu/information-security. Accessed 23 Feb. 2023.

Joint Task Force. *NIST Special Publication 800-53B: Control Baselines for Information Systems and Organizations.* National Institute of Standards and Technology, Oct. 2020, doi.org/10.6028/NIST.SP.800-53B.

Joint Task Force. *NIST Special Publication 800-53 Revision 5: Security and Privacy Controls for Information Systems and Organizations*. National Institute of Standards and Technology, Sep. 2020, doi.org/10.6028/NIST.SP.800-53r5.

Lammle, Todd. *CompTIA Network+ Study Guide*. 4th ed., John Wiley & Sons, Inc., 2018.

PCI Security Standards Council, LLC. *PCI DSS Quick Reference Guide*. PCI SSC, 2018, listings.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf.

Scholl, Matthew, et al. *NIST Special Publication 800-66 Revision 1: An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*. National Institute of Standards and Technology, Oct. 2008, www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/nist80066.pdf.

Whitman, Michael E. and Herbert J. Mattord. *Management of Information Security*. E-book, 6th ed., Cengage Learning, Inc, 2019.