Final Project

Jose Flores

Michael Njamfa

CSOL-510-03-SP22: Applied Cryptography

Dr. Umesh Varma

April 18, 2022

Table of Contents

Executive Summary

With technology advancing every day, the increase of cyber threats also increases. Cryptography secures network communications and protects critical information, such as Personally Identifiable Information (PII), at storage. PII can be stored in different devices such as computers, universal serial buses (USB), compact disks (CD), memory cards, and external hard drives. While encrypting information is essential, protecting and handling the information is just as important. There must be firewalls, a virtual private network (VPN), department training, disaster plans, and backup plans. The Health Insurance Portability and Accountability Act (HIPAA) follow three rules: Privacy, Breach Notification, and Security. The Privacy Rule addresses what information is protected and how it may be disclosed to promote quality health care (OCR, 2013). The Breach Notification Rule is the standard and approaches HIPAA will take if protected health information (PHI) is compromised or accessed by an unauthorized user (OCR, 2013). The Security Rule requires all PHI to have the appropriate administrative, technical, and physical safekeeping (OCR, 2013). The Security Rules Foundation is organized by following the National Institute of Standards and Technology (NIST) special publications 800 -111, “Guide to Storage Encryption Technologies for End User Devices” and 800 -53 “Security and Privacy Controls for Information Systems and Organizations” (HHS, 2016).

Implementing multiple NIST special publications to the HIPAA three rules will help identify the company’s security goals and meet HIPAA compliance requirements. Understandings our vulnerabilities and weakness will support created security policies and guidelines for the company.

Introduction

Health Inc. is an insurance company that uses security standards and policies to ensure company practices are compliant and beneficial to the overall mission statement of the organization. Cyber threats are highly prevalent in healthcare organizations, so it is important to follow standard security practices to mitigate all vulnerabilities and cyber threats to systems and networks. Healthcare organizations must comply with two regulations: Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act. HIPAA is a security standard to protect electronic protected health information (EPHI). Any organization that requires HIPAA compliance must comply with the Security rule, which focuses on the confidentiality, availability, and integrity of electronic protected health information (EPHI). The (HITECH) act, signed on February 17, 2009, was enacted to strengthen the privacy and security of private information transfer and enforce HIPAA rules. Organizations can potentially face a fine of $1.5 million for any violations of the act. Complying with HIPAA and (HITECH) will allow Health Inc. to implement administrative, technical, and physical safeguards that will uphold our systems' confidentiality, integrity, and availability.

Organizational Threats, Risks, and Policies

Technological advancements have allowed healthcare organizations to store most of their data on the Internet. These advancements, however, have caused numerous cyber threats that must be protected against. Healthcare organizations are prime targets for cyber threats because of the plethora of (PHI) and (PII) such as social security numbers, credit card information, and bank account numbers stored in their systems. A cyber-attack can be financially devastating for organizations costing $408 per stolen healthcare record, three times more than other industries (Riggi, n.d.).

One of the main threats to Health Inc. is insider threats. Insider threats stem from data breaches manufactured within an organization. This usually happens when a user with high privileges unknowingly or knowingly exposes sensitive data. According to *Verizon's Protected Health Information Data Breach Report*, 58% of all healthcare data breaches and incidents result from insiders. The potential organizational risk from insider threats includes heavy fines for breaching HIPAA rules, violations of patient privacy, and the irremediable loss of patients' trust (*How to Defend Against Insider Threats in Healthcare*, 2020).

Another main threat to Health Inc. is hackers. Hackers use various malicious methods to compromise systems and steal data. One method, phishing, involves hackers using emails to trick employees into clicking on a malicious email by acting as if they were someone they are not. Their goal is to eventually have the employee send them sensitive information or spread malware on their computer to set up another attack, such as ransomware. Ransomware attacks occur when hackers gain access to the system to steal sensitive information, encrypt it, and demand money to decrypt it. Health Inc. contains a lot of sensitive consumer information, so any potential losses due to ransomware can be detrimental to the organization and the consumers (Ellis, 2021).

For every threat to an organization, many risks can happen. The Risk Management Framework (RMF) must be implemented to mitigate these risks. The RMF allows IT professionals to balance protective measures' operational and economic costs to uphold an organization's mission statement. This framework allows an organization to find the likelihood of a future adverse event and analyze threats to an IT system in conjunction with the potential vulnerabilities and the controls in place for the IT system. This framework contains a 6 step process: System categorization, selection of baseline controls, implementation of control, assessment of controls, authorization, and monitoring of the effectiveness of the controls (NIST, 2020).

Using NIST 800-53, security and privacy controls can be identified to provide a baseline security standard for systems. To ensure users only have access to the information they need to see, one of the controls that must be implemented for Health Inc. is least privilege. Least Privilege (AC-6) ensures that employees will have access to systems and operate at privilege levels no higher than they need to be to adhere to the organization's mission statement. This would help prevent the threat of insiders by having few employees have access to highly classified information. This would also mitigate the chance that any potential malware propagating through the network will not reach critical systems. Another control that should be implemented for Health Inc. is awareness training. Awareness training for policies and procedures (AT-1) involves. Establishing policies and procedures to comply with security standards is the first step in running a secure organization. The employees must be trained to adhere to these security standards to ensure our business is not exposed to malware and other malicious threats. Having poorly trained employees will result in data breaches that can ruin the company. The last control that must be implemented for Health Inc. is physical access authorizations. Physical access authorizations (PE-2) develop a list of authorized individuals allowed access to various facilities such as server rooms. By using ID badges, identification cards, or smart cards, Health Inc. can ensure that only authorized individuals access areas that contain items critical to business practices. This will lessen the threat of insiders because only a select few have access to sensitive information. In the event of a data breach from one of these areas, using security cameras can also identify intruders and prevent insider threats.

Component Policies

The first policy that should be established for customers (#1), providers (#2), and remote workers (#3) is an acceptable use policy. The access agreements policy (PS-6) forces users to sign agreements before granting access to the network. This would ensure that users adhere to all the security standards implemented. Users could invite malware and other threats by accessing malicious sites without this policy. This could risk company data being exposed. To protect customers, providers, and remote workers from unwanted access, phishing, and malware, S/MIME should be implemented. According to NIST 800-45, S/SMIME is a protocol that sends emails encrypted and with a signature. This will let users know exactly who is sending them a message to avoid potential malware injection attempts via email. Along with S/MIME, strict cryptographic standards should be implemented to ensure maximum protection and compliance with HIPAA and HITECH. The cipher suite that should be implemented is AES 256. AES is the government standard encryption suite that all systems should use. Off-site backups (#4) are critical when main systems fail. According to NIST Sp 800-53, system backup (CP-9) policies should be implemented to protect the confidentiality, integrity, and availability of backup systems. If backups are not immediately available, customers may face outages in their services which would negatively affect the organization. A way that this organization should separate networks with different security requirements and prevent unwanted traffic is by implementing firewalls. According to NIST 800-41, outer firewalls (#5) act as routers for traffic between the WAN and LAN paths. Implementing a demilitarized zone (DMZ) to the outer network and web servers (#6) will provide an extra layer of security by restricting access to sensitive data and servers. Having a DMZ in place will separate critical servers from the rest of the network and prevent them from getting exposed to a data breach. Another control we can add to the DMZ are honeypots. Honeypots are established to attract hackers to learn and understand their attack methods. This will give the organization a better insight into what the main threat actors are and how to protect against them optimally (Scafone, 2009).

Data Storage standards must be strictly followed due to the exorbitant amount of PHI and PII data stored on the network. According to NIST SP 800-209, corporate data (#12) and Data (#9) should be stored on cloud-based systems. These storage systems allow for easy collaboration of files of various permissions throughout the network and advanced data protection services such as mirroring, archiving, auditing, and encryption with AES 256. A storage area network (SAN) will be implemented for the physical data servers to have block-level access to network storage. Making sure software for storage devices is updated is essential to eliminate any existing exploitable vulnerabilities (Chandramouli, 2020). Throughout the premises of the on-site campus, IEEE 802.11 standard WLAN will be implemented to provide wireless networking services for all. A substandard WLAN exposes APs (#11) to threats such as wardriving and evil twin attacks. According to NIST 800-153, separate WLANs should be implemented for guests and internal users to prevent anyone from spying on sensitive data (Souppaya, 2012)

Interfaces

VPNs (#7) are commonly used to encrypt traffic and provide user authentication and integrity checking. VPN gateways should be implemented to connect different offices. For remote users to connect to VPN (#15), a host-gateway VPN must be enacted. This provides a secure connection to the network for remote users located outside of the organization. For VPN to firewall (#18) connections, VPNs allow the firewall to decide which users can access the network using policies. RADIUS must be implemented with authentication credentials such as usernames, passwords, digital signatures, and hardware tokens to do this. Authenticating using RADIUS lowers the chance of someone gaining access to information they do not need to see. All VPN connections should be secured with AES 256 and TLS 1.3. Each VPN connection also contains asymmetric cryptography, which uses separate keys for encryption and decryption (Frankel 2005). Using SHA 256 will ensure that the hash of encrypted messages never changes and that its integrity is kept in place. For customers (#13), providers (#14), and firewalls-web servers (#16) they should connect to the network by first going through a Host-Based Firewall, which can limit traffic to necessary connections.

Host-Based firewalls can also act as IPS systems to detect and act on malicious traffic. This will limit the spread of malware within the internal network (Scarfone, 2009). Access lists and privileges must be set when connecting to a corporate LAN (#19) from an inner firewall and AP (#22) SSH authentication mechanisms. Also, port security features such as DHCP snooping, IP Source Guard, and ARP security to protect from cyber threats. Inner firewalls to data (#20), corporate LAN to data (#22), and corporate LAN to data (#23) should all use a private IEEE 802.1 Q VLAN port to segregate connections on the network. Using SSH to communicate is pivotal because SNMP, TFTP and FTP are insecure. These implementations will prevent several layer two attacks, such as VLAN attack, and DHCP attacks, and allow VLAN connections to be compliant with security standards (*Layer 2 security threat*s)

Conclusion

In conclusion, Health Inc. is an insurance company that must comply with PHI and HIPAA standards due to the high amount of personal data. Threats are mitigated by adhering to security controls from the NIST publications. Using the RMF, an organization can classify and select controls for a component to ensure it complies with government standards to abide by its mission statement.

Glossary

AES	is a cipher, meaning that it is a method or process used to change raw information (usually human readable) into something that cannot be read. This part of the process is known as encryption
Vulnerabilities	is a weakness that can be exploited by cybercriminals to gain unauthorized access to a computer system
Cryptography	is the study of secure communications techniques that allow only the sender and intended recipient of a message to view its contents.
Hackers	is the act of compromising digital devices and networks through unauthorized access to an account or computer system.
Ransomware	is a type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files until a ransom is paid
LAN	A local area network (LAN) consists of a series of computers linked together to form a network in a circumscribed location.
S/MIME	is an email encryption and signing industry standard widely used by corporations to enhance email security.
WAN	is a large network of information that is not tied to a single location.
DMZ	is a perimeter network that protects and adds an extra layer of security to an organization's internal local-area network from untrusted traffic. A common DMZ is a subnetwork that sits between the public internet and private networks.
SAN	is a specialized, high-speed network that provides block-level network access to storage.
Honeypot	A system (e.g., a web server) or system resource (e.g., a file on a server) that is designed to be attractive to potential crackers and intruders, like honey is attractive to bears.
AP	A device that logically connects wireless client devices operating in infrastructure to one another and provides access to a distribution system, if connected, which is typically an organization's enterprise wired network.

VPN	A virtual network built on top of existing networks that can provide a secure communications mechanism for data and IP information transmitted between networks.
WLAN	A group of wireless access points and associated infrastructure within a limited geographic area, such as an office building or building campus, that is capable of radio communications. WLANs are usually implemented as extensions of existing wired LANs to provide enhanced user mobility.
TLS	An authentication and encryption protocol widely implemented in browsers and Web servers. HTTP traffic transmitted using TLS is known as HTTPS.
RADIUS	An authentication and accounting system used to control access to an Internet Service Provider (ISP) system.
Host-Based Firewall	A software-based firewall installed on a server to monitor and control its incoming and outgoing network traffic.
SSH	enables two computers to communicate (c.f http or hypertext transfer protocol, which is the protocol used to transfer hypertext such as web pages) and share data.
DHCP	is an under-the-covers mechanism that automates the assignment of IP addresses to fixed and mobile hosts that are connected wired or wirelessly.
VLAN	A single physical local area network (LAN) can be logically partitioned into multiple, independent VLANs; a group of devices on one or more physical LANs can be configured to communicate within the same VLAN, as if they were attached to the same physical LAN.
SNMP	is a protocol for management information transfer in networks, for use in LANs especially, depending on the chosen version.
TFTP	is a simple protocol used for transferring files. TFTP uses the User Datagram Protocol (UDP) to transport data from one end to another.
FTP	The term file transfer protocol (FTP) refers to a process that involves the transfer of files between devices over a network.

References

Chandramouli, R. Pinhas, D. (20200. NIST Special Publication 800-209, Security Guidelines Storage Infrastructure. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-209.pdf

Ellis, M. (2021, October 7). The Biggest Cybersecurity Threats Facing Healthcare Organizations —and How to Protect Yourself. Recorded Future. Retrieved April 17, 2022, from https://www.recordedfuture.com/biggest-cybersecurity-threats-facing-healthcare-organizations/

Frankel, S., Kent, K., Lewkowski, R., Orebaugh, A. D., Ritchey, R. W., & Sharma, S. R. (2005). Guide to IPsec VPNs:.

How to Defend Against Insider Threats in Healthcare. (2020, May 19). HIPAA Journal. Retrieved April 17, 2022, from https://www.hipaajournal.com/how-to-defend-against-insider-threats-in-healthcare/

HIPAA Security Rule Crosswalk to NIST cybersecurity framework - hhs.gov. (2016). Retrieved April 18, 2022, from https://www.hhs.gov/sites/default/files/nist-csf-to-hipaa-security-rule-crosswalk-02-22-2016-final.pdf

Layer 2 Security Best Practices > Security Features on Switches. (n.d.). Cisco Press. Retrieved April 17, 2022, from https://www.ciscopress.com/articles/article.asp?p=1181682&seqNum=12

National Institute of Standards and Technology (NIST). (2020, September). Retrieved from NIST Special Publication 800-53r5: Security and Privacy Controls For Information

Systems and Organizations https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

(OCR), O. for C. R. (2013). Breach notification rule. HHS.gov. Retrieved April 16, 2022, from https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html

(OCR), O. for C. R. (2013). Summary of the HIPAA security rule. HHS.gov. (2013). Retrieved April 17, 2022, from https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

(OCR), O. for C. R. (2013). Summary of the HIPAA privacy rule. HHS.gov. Retrieved April 16, 2022, from https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html

Riggi, J. (n.d.). The importance of cybersecurity in protecting patient safety | Cybersecurity | Center | AHA. American Hospital Association. Retrieved April 17, 2022, from https://www.aha.org/center/cybersecurity-and-risk-advisory-services/importance-cybersecurity-protecting-patient-safety

Scarfone, K., & Hauffman, P. Guidelines on Firewalls and Firewall Policy, Recommendations of the National Institute of Standards and Technology (NIST). Special Publication, 800-41.

Souppaya, Murugiah & Scarfone, Karen & Networks, Area. (2012). NIST Special Publication 800-153, Guidelines for Securing Wireless Local Area Networks (WLANs).

Y. (2020, June 16). ▷ Layer 2 Security Threats ». CCNA 200–301. Retrieved April 17, 2022, from https://ccna-200-301.online/layer-2-security-threats/