ENPM686: FINAL PROJECT – PAPER

SECURITY SOLUTIONS DESIGN PAPER FOR LIFECARE HOSPITAL

Submitted By: -
Krupa Solanki (118291208)
Ratan Gupta (118195773)

TABLE OF CONTENTS

1. ABSTRACT

LifeCare Hospital has been a victim of many security attacks in recent months including a severe ransomware attack and many DDoS (Distributed Denial of Service) attacks. The attacks have drastically impacted hospital services and patients. Patients' PII (Personal Identifiable Information) and PHI (Protected Health Information) were stolen, and hospital services were rendered unavailable for use. The purpose of this design paper is to evaluate the overall security posture of LifeCare Hospital and identify vulnerabilities that led to the recent attacks and that can be potential vectors for future attacks. The paper also recommends security solutions to improve the overall security posture of LifeCare Hospital and build resilience against future attacks and mitigate risks. Lastly, the paper includes the budget allocated for infrastructure assessment and solutions design and provides an estimated cost for the recommended solutions.

2. ASSUMPTIONS

The following assumptions were made about the hospital, its employees, and weaknesses that exist -

1. The hospital has 150 employees including doctors, nurses, administrative staff, receptionists, accounting staff, etc.
2. Employees do not use multi-factor authentication.
3. The firewall is very simple and not very secure.

4. Hospital personnel are not aware of basic security practices and are untrained in the ways of following the best security practices.
5. Workstations do not have antimalware software downloaded.
6. Many systems in the internal network are unpatched and have not been updated to the latest version of Windows.
7. Absence of a logging and monitoring tool.
8. Absence of advanced security technologies such as Intrusion Prevention System (IPS), etc.
9. Sensitive data is not encrypted.
10. Absence of a proper security team that can help the hospital comply with security policies and regulations by helping them follow security guidelines, implementing best security practices, conducting account auditing, performing risk assessments, etc.

These assumptions render the hospital non-compliant with HIPAA (Health Insurance Portability and Accountability Act). In the United States of America, it is mandatory for healthcare institutions such as hospitals to comply with HIPAA's policies and regulations.

The architecture on the next page is based on the above assumptions and the ideas given in the project handout. It is completely hypothetical.

3. CURRENT ARCHITECTURE

The following diagram illustrates the current computer network architecture of LifeCare Hospital.

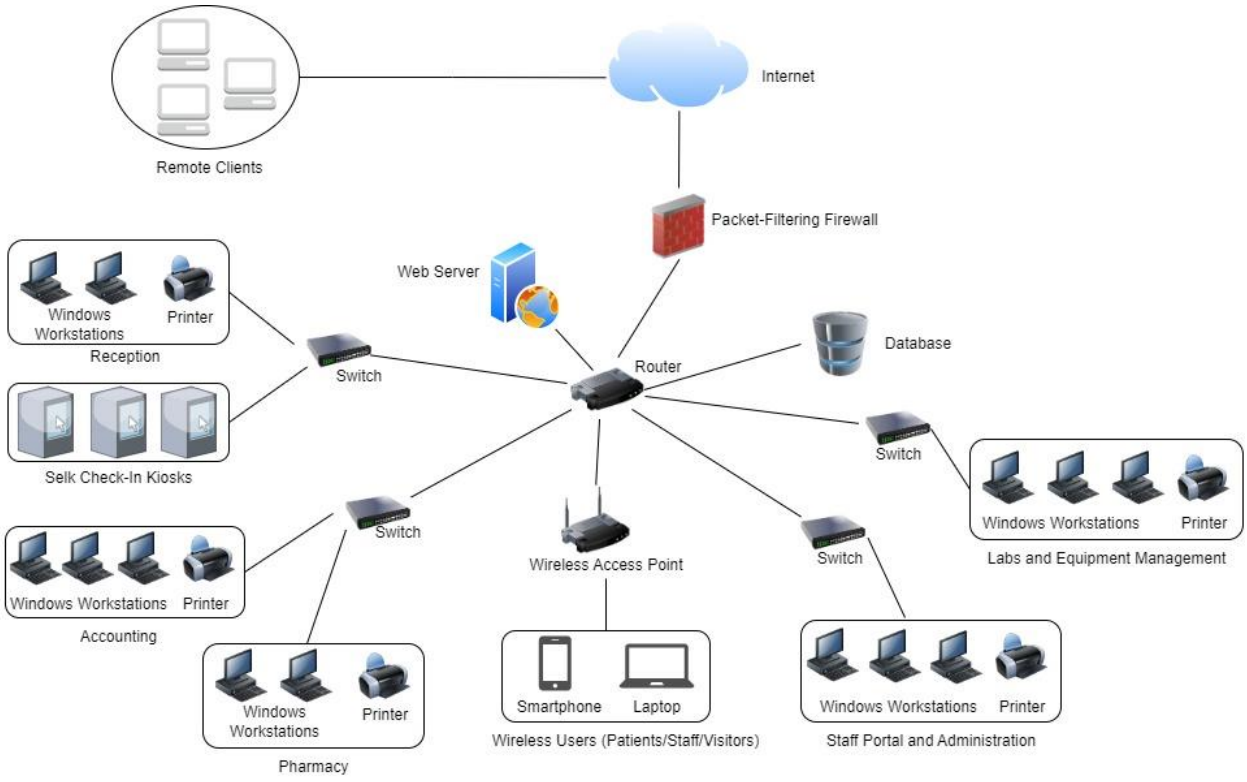

Figure 1: Current System Architecture of LifeCare Hospital

A Packet-Filtering Firewall (Layer 2 Firewall) lies between the Internet and the hospital's LAN. All traffic from the hospital's internal network and the Internet passes through this firewall and rules are defined on the firewall to filter this network traffic. A router connects different devices and departments of the hospital with the help of many switches. An on-premises web server is used to host the hospital's website and mobile application. A database is used to store patient information and medical records, staff information, pharmacy data, accounting data, etc. All the systems in the internal network use Windows

Operating System. There is a wireless access point for users (patients/staff/visitors) to connect their personal devices with the hospital's Wi-Fi.

4. RECENT COMPROMISES

The hospital has been the victim of a severe ransomware attack. Most of the computers were affected, and sensitive information of patients was stolen. The attackers were able to get into the system by stealing an employee's credentials using a social engineering technique called phishing. Patients' PII and PHI were stolen, and the attackers demanded a hefty ransom in exchange for the information.

In the past months, the hospital was subjected to a huge DDoS attack as well. The attackers attempted to overload the hospital's server by sending a barrage of traffic to it. The attack exhausted server resources and it led to the website and mobile application to be unavailable to the users. The hospital not only faced financial losses, but the attack also negatively affected the hospital's reputation. Moreover, patients were inconvenienced as they could access the website or the application.

To summarize, the hospital has been recently affected by -

1. Ransomware attack,
2. DDoS attack, and
3. Social Engineering attack.

4.1. Causes

The causes of the attacks are the weaknesses assumed in section 2 of this paper. Since hospital personnel are not trained to adopt the best security policies, they are the easiest targets of social engineering attacks. Moreover, security-unaware staff pose a threat to the safe operations of the hospital as they can inadvertently introduce risks. Secondly, the use of a very basic firewall, insecure network, and absence of scalable resources can result in DDoS attacks. Lastly, workstations without antimalware software and unpatched systems can be easily infected with malware. This can lead to ransomware, privilege escalation, data exfiltration, spreading worms, system crashes, etc.

5. OBJECTIVES

The primary objective of this paper is to recommend security solutions that will help mitigate risks and improve the overall security posture of LifeCare Hospital. The goal is to protect the hospital's assets including its infrastructure, private and important information, patients' PII and PHI, employees' PII, reputation, medical equipment, computer systems, etc. while ensuring that the daily operations and services are not affected. Moreover, the recommended security solutions will help prevent attacks and are aimed towards building resiliency, scalability, and maintainability.

A budget was allocated for the implementation of the recommended security controls that include purchasing services, deploying security devices, training employees, hiring

security personnel, etc. The paper aims to provide a viable security plan that offers the best level of security for the given cost restraints.

6. PROPOSED SECURITY SOLUTIONS

6.1. Security Awareness Training for Employees

Security Awareness training for employees helps them understand the importance of protecting important data and teaches them how to recognize and prevent potential security threats. It provides an understanding of the importance of security within an organization. Hospitals are subject to various regulations, such as HIPAA (Health Insurance Portability and Accountability Act). Understanding these HIPAA regulations will help ensure that employees understand their role in compliance and how to follow security policies and procedures. Cyber-attacks like ransomware attacks and data breaches can be prevented if employees are trained to recognize and respond to potential cyber threats, such as phishing emails and social engineering attacks.

LifeCare Hospital should make it a requirement for the employees to take the SANS awareness training. **SANS Security Awareness Professional (SSAP)** is a popular platform that offers a wide range of training resources including video modules, posters, newsletters, and games [1]. The platform covers a variety of topics such as secure password management, email security, and online privacy.

The SSAP is an efficient and all-inclusive approach for professionals in security awareness to advance their careers in managing risks and create a lasting impact on their organization's security.

The cost of this training is $175/person/year [2]. Therefore, the total cost will be approximately $26,000 per year for 150 employees.

6.2. Implementing Multi-Factor Authentication

Multi-Factor Authentication (MFA) is a security method that requires users to use two or more authentication factors to authenticate themselves. This approach adds extra layers of security during the authentication process. The verification factors can include password or PIN, security token or smartphone, biometric data like a fingerprint or facial recognition.

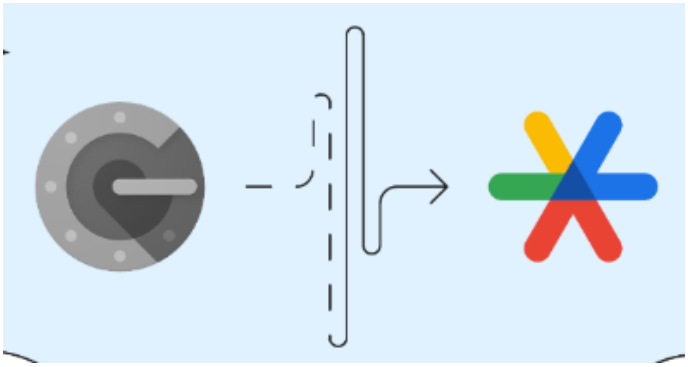

Figure 2: Google Authenticator

Google Authenticator is an application developed by Google that is widely trusted and provides multi-level verification services which can be implemented by LifeCare Hospital to add an extra level of difficulty for attackers attempting to access sensitive information.

Even if an attacker successfully guesses or hacks an employee's password, they will still need to pass through another layer of authentication if Google Authenticator is in use.

6.3. Hiring Security Professionals

Having an effective security team in place can assist a hospital in adhering to security policies and regulations by guiding them in following and implementing security protocols, adopting optimal security measures, monitoring account activity, conducting risk evaluations, and other related actions.

Additionally, a new Cyber Threat Hunter will be appointed to focus on identifying, analyzing, and countering advanced threats. Preventing attacks requires threat intelligence and skillful personnel who can efficiently manage and utilize various security technologies. Hence, the appointment of security engineers, including security administrators and the threat analyzer is justified.

6.4. Using a Secure Firewall

A secure firewall will help LifeCare Hospital to ensure the confidentiality, integrity, and availability of patient data by controlling the flow of information and preventing unauthorized data access or modification. One such firewall is the **Juniper Networks SRX Series firewall**. The **SRX1500** is equipped with hardware-based security features, such as stateful firewall, intrusion prevention system (IPS), a virtual private network

(VPN), and advanced threat prevention capabilities like application security, anti-virus, anti-spam, and web filtering.

Figure 3: SRX1500 Firewall

SRX 1500 is a next generation firewall and has features like advanced threat prevention capabilities, network segmentation features, high availability, and management and reporting tools that can help hospitals improve their network security posture.

Key Features	Performance Vectors
Firewall performance (max)	9.2 Gbps
IPS performance	3.3 Gbps
VPN performance	4.5 Gbps
Maximum concurrent sessions	2 million

6.5. Deploying IPS and Antimalware Software

Norton LifeLock 360 is an anti-malware software that provides advanced threat protection against malware, ransomware, and other cyber threats that can compromise hospital systems and data. It monitors the dark web and other sources for stolen personal information and alerts hospital staff if any suspicious activity is detected.

Norton LifeLock 360 can help hospitals protect their critical systems and sensitive data from cyber threats and help maintain compliance with regulatory requirements.

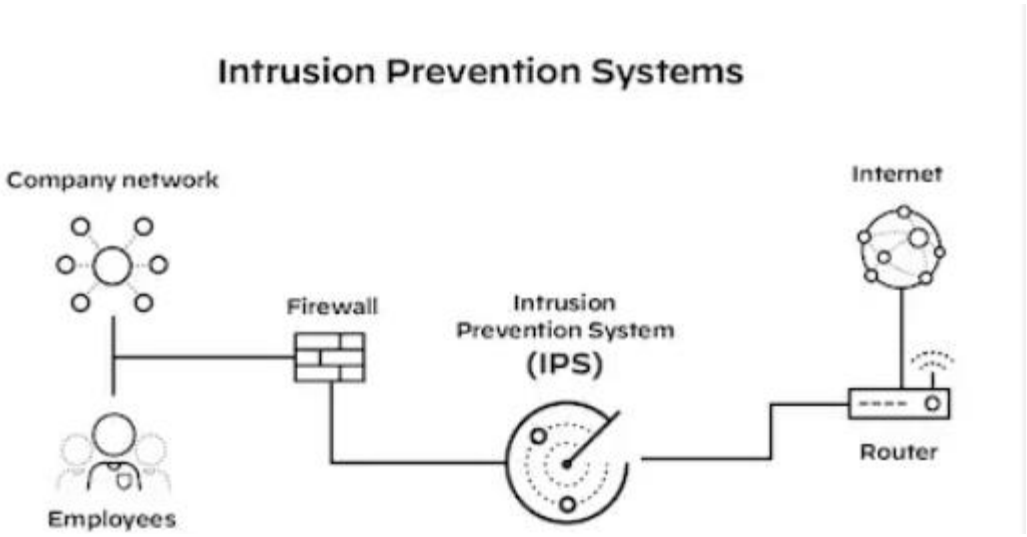

Figure 4: Intrusion Prevention System

Another solution is to install an IPS (Intrusion Prevention System). Intrusion Prevention Systems (IPSs) are highly efficient at identifying and stopping attempts to exploit vulnerabilities. IPS technology can help by quickly identifying and blocking such attacks, minimizing the window of opportunity for exploitation.

IPS solutions can help hospitals meet these compliance requirements by providing a layer of protection against data breaches and unauthorized access to sensitive data. **Palo Alto Networks Next-Generation IPS** is a great tool that can be used for this purpose.

6.6. Endpoint Detection and Response

CrowdStrike Falcon XDR (Extended Detection and Response) is an XDR solution that provides threat detection and response capabilities by integrating data from endpoints, email, and network security. XDR tools can detect ransomware attacks at different stages, such as during the delivery of the ransomware, the exploitation of vulnerabilities, or the encryption of files. When an XDR tool identifies a ransomware attack, it can quarantine the infected endpoint, isolate it from the network, and terminate the malicious process to prevent further damage.

Figure 5: CrowdStrike XDR

6.7. Encrypting and Hashing Sensitive Data

Strong encryption and hashing algorithms are essential for protecting sensitive data and ensuring its confidentiality, integrity, and authenticity. Encryption algorithms like **Advanced Encryption Standard (AES)** and **Rivest-Shamir-Adleman (RSA)** can help protect sensitive information, such as patient health records, from unauthorized access and data breaches. **Bitdefender's GravityZone** encryption tool offers full disk encryption, file and folder encryption, and removable media encryption. It also includes features like vulnerability assessment, patch management, and full disk encryption. Hashing algorithms like **SHA-3** and **BLAKE2** can be used to securely store passwords and other sensitive data, making it more difficult for hackers to obtain and use the information.

6.8. Complying with HIPAA Rules

Some of the key HIPAA regulations that hospitals must comply with include:

1. **Privacy Rule**: This rule governs the use and disclosure of Protected Health Information (PHI) which requires hospitals to implement policies and procedures to protect the privacy of patient PHI (Protected Health Information).
2. **Security Rule**: The rule implements administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of electronic PHI (ePHI) which requires hospitals to implement security measures, such as access controls, encryption, and backup and recovery procedures, to protect ePHI.
3. **Breach Notification Rule**: This rule requires hospitals to implement policies and procedures to identify and respond to breaches of PHI.

4. **Omnibus Rule**: This rule includes several updates to the Privacy, Security, and Breach Notification Rules, including requirements related to business associates.

7. BUDGET PLAN

The aggregate financial allocation to this undertaking amounts to $600,000, while the expenditure incurred and used is $363,027. The individualized budget designated for tools has been precisely computed by factoring in the average number of employees within the organization to 150. The insights to the budget distribution are depicted through the below table and pie chart.

Security Solution	Total Cost
Security Awareness Training by SANS	$26,000
Juniper Networks SRX1500 Firewall	$18,900
Norton LifeLock 360	$15,000
Palo Alto Networks Next-Generation IPS	$3,737
Hiring Security Professionals (First Year Salary)	$150,000
Cyber Threat Hunter	$120,000
CrowdStrike XDR	$18,000

Nessus Vulnerability Assessment Scan Pro	$2,390
GravityZone Business Security	$9,000

The estimated budget for the recommended security solutions is $363,027.

The following pie chart illustrates the distribution of the budget between different solutions.

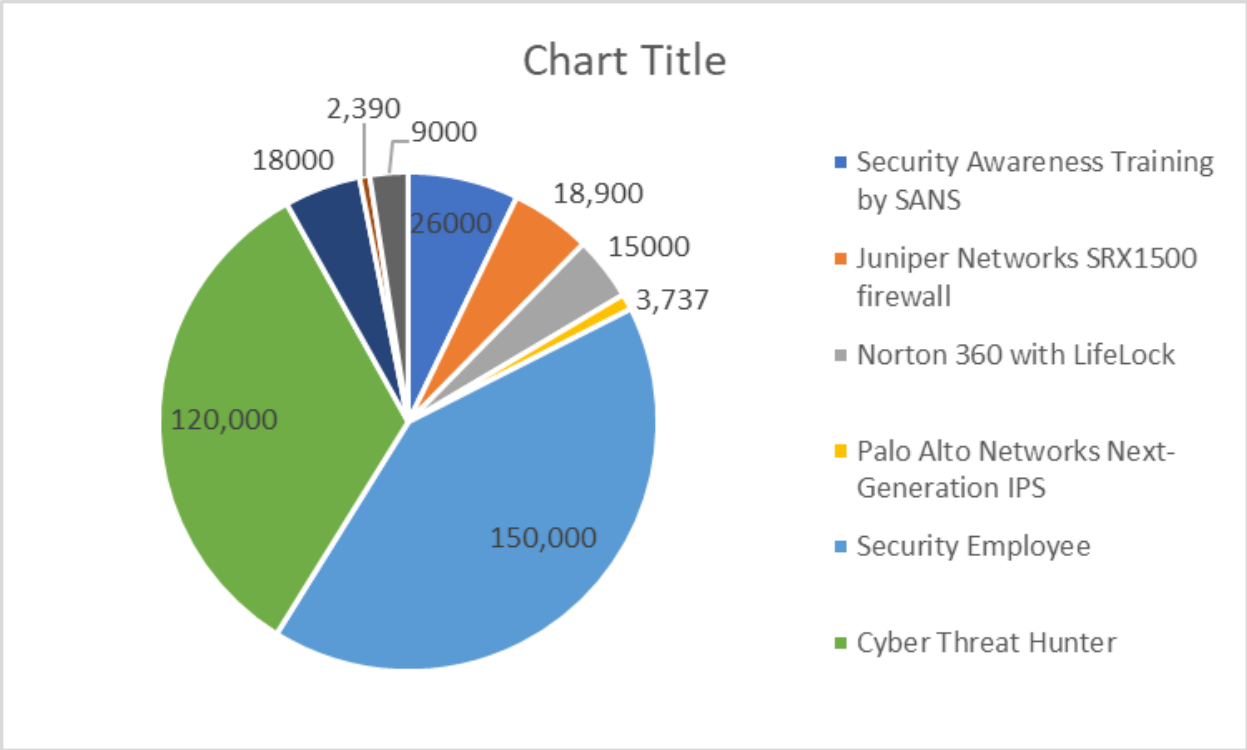

Figure 6: Budget Distribution

8. Conclusion

LifeCare Hospital has suffered a plethora of drastic malicious attacks in the past. The recommended security solutions construct a defense-in-depth model and are expected to protect the hospital at many different levels. They aim to decrease the probability of experiencing devastating attacks in the future by detecting, preventing, and mitigating them. The proposed budget for the recommended solutions is well within the maximum allocated budget and can be used for future security solutions when required.

9. REFERENCES

1. SANS Institute. "Security Awareness Training." SANS Institute, https://www.sans.org/security-awareness-training/. [Accessed 7 May 2023.]
2. “The Sans Security Awareness Professional (SSAP).” SANS Security Awareness, www.sans.org/security-awareness-training/career-development/credential/. [Accessed 15 May 2023.]
3. https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-prevention-system-ips. [Accessed 15 May 2023.]
4. Palo Alto Networks. “What Is an Intrusion Prevention System? - Palo Alto Networks.” Paloaltonetworks.com, 2018, www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-prevention-system-ips. [Accessed 15 May 2023.]
5. “CrowdStrike Falcon Insight XDR | Products.” Crowdstrike.com, www.crowdstrike.com/products/endpoint-security/falcon-insight-xdr/. [Accessed 15 May 2023.]
6. U.S. Department of Health & Human Services. “The HIPAA Privacy Rule.” HHS.gov, 16 Apr. 2015, www.hhs.gov/hipaa/for-professionals/privacy/index.html.