Ahlem Tamssaout

Prof: DeAndre Favors

Network defense essentials- CCA

August 03, 2022

Research project

With the explosive growth of technology, the information security cannot be overstated. It is important that companies develop a proper security improvement to protect their critical assets and information systems from unauthorized access or evolving threats to business and costumers. Altamaha Tech incorporated the company that specializes in the development of wearable medical devices did a security report providing a high-level overview of the operational details of the organization. Based on the security report I will create a plan to resolve the security issues of the company that include assessment techniques to determine threats and vulnerabilities, physical and technical security threats, provide the required policies to protect information systems, policies and procedures used for continuous security monitoring, training and continuing education policies implementation, and a continuity of operations plan to keep the key system operational during a disaster.

According to the report, Altamaha Tech Inc locked most security policies which is a high-level document that describes the important security controls needed to protect the company and maintain the CIA triad of confidentiality, integrity, and availability. To fix this issue, the company should implement EISP like application policy, backup and restore policy, and system security policy. ISSP like remote access and wireless policies, incident response plan, password policies, and MDM policies, next to SSSP that will direct users while configuring or maintaining a system for example DMZ policy, encryption policy, policies for intrusion detection and prevention. Also, the company should implement internet access policy such as prudent policy that provides maximum security. Furthermore, to supplement the cyber security awareness training and education that should involve all of security policy, physical security, social engineering and data classification, the company need to implement POLP the principle of least privilege that will provide the employees exactly the need-to-know level of access. In addition to identity and access management that provide the right individual with the right access at the right time which is based on authentication, authorization, identity management and identity repository, and because of the high turnover of key employees it is important update passwords.

Determining vulnerabilities and threats can be designed with the proper implementation of assessments techniques from preventive techniques like access control mechanisms such as a firewall; admission control mechanisms such as Network Access Control and Network Access protocol; cryptographic applications such as IPsec and SSL; authentication methods such as 2FA or multi-factor authentication, and reactive approaches like including security monitoring methods such as IDS which detect attacks by capturing and analyzing network pockets, IPS which can detect an intrusive activity and can also attempt to stop activity, ideally before it reaches its targets, SIMS, and TRS, in addition to including protocol analyzers and traffic monitors, security forensic techniques such as CSIRT and CERT, post-mortem analysis mechanism including risk and legal assessment, threat intelligence and risk assessment methods, and perform a full vulnerability assessment to review the entire network weaknesses.

There are Physical security threats and vulnerabilities to consider, and the most common physical security threats, the organization should protect against are environmental threats like fires, floods temperature and humidity, and man-made threats both intentional and unintentional like vandalism, theft, hackers, and human errors depending on where the company is located. Physical security threats are commonly outside risks, but also internal risks are equally important, human errors are the leading cause of security breaches, “accounting for approximatively 88% OF incidence, according to Stanford university study”. That’s why it’s important to update a list of threats and vulnerabilities, and use physical security controls that provide physical protection for all physical assets of an organization including information and buildings to reduce chances of attacks, an example of physical security controls is paying attention to firefighting systems, physical barriers( fences, bollard, turnstiles), security personals (Guards, plant’s security officer, safety officer, chief information security officer), physical locks, mantrap, warning signs alarm system, video surveillance, lightning system, and power supply.

Logical security threats and vulnerabilities are those that may damage the organization software systems, data, or network. Due to the high turnover of key employees, some security threats and vulnerabilities may face the organization including File system intrusion when any modification or deletion of the file occurs it is a sign that the system is a target of an attack; Network intrusion if a sudden increase of bandwidth consumption is detected; System intrusion for example gaps in system accounting. In addition to threats like malware such as Trojans, viruses. Moreover, social engineering attacks in case of the turnover of key employees, employers may give personal information such as username and password, and some types of social engineering are phishing emails, shoulder surfing, and dumpster diving. Additionally, Outdated, or unpatched software that exposes the systems running the application and potentially the entire network. Furthermore, the misconfigured firewalls or operating systems that allow or have default policies enabled, since firewalls are the front line of defense that monitors inbound and outbound traffic. When these vulnerabilities are unchecked, it can lead to advance attacks such as DDoS (distributed denial of services) attack.

Altamaha Tech is lacking some policies and procedures that address issues with compliance with information privacy laws and regulation. To fix this issue the company should implement HIPAA, since the company is dealing with medical devices that contain sensitive data of patients. This “privacy rule standards address the use and disclosure of individuals ‘health information (known as protected health information for PHI) by entities subject to the privacy rule. These individuals and organizations are called “covered entities”. Also, implementing GDPR that is considered as the toughest privacy and security law in the world, based on protection principle like integrity and confidentiality, lawfulness, fairness, and transparency which will help to protect the sensitive data of patients that utilize the devices manufactured and sold by the company. Any information that can be used to distinguish one person from another and can be used to deanonymize previously anonymous data is considered Personal Identifiable Information (PII), as the Altamaha organization continuously collect, store, and distribute PII and other sensitive data, employees, administrators, and third-party contractors need to understand the repercussions of mishandled data and be held accountable. Predictive analytics and artificial intelligence (AI) are in use at organizations to sift through large data sets so that any data stored is compliant with all PII rules.

Customers of Altamaha Tech Inc are using credit cards or corporate cards as a payment method, and to secure the information of cardholders the company need to ensure compliance with PCI DSS that stands for Payment Card Industry Data Security Standard “is a global forum that brings together payments industry stockholders to develop and drive adoption of data security standards and recourses for safe payments worldwide”. PCI security standards council has developed and maintains a high-level overview of PCU DSS requirements like build and maintain secure network, protect cardholder data, maintain a vulnerability management program, and maintain an information security policy, and failure to meet the requirement may result in fines or the termination of payment-card processing privileges. Security policy document that describes how the Altamaha Tech Inc accepts the payments in accordance with PCI DSS, that should maintain confidentiality, availability and integrity and asset values, to enhance data and network security and for better network performance.

Altamaha Tech Inc is providing internet access to employees. So before granting the access to the network they should sign an AUP (Acceptable Use Policy) that outlines the appropriate use of access to the company network and describes what users can or cannot do when accessing the network for example, do not attempt to hack the security of the network or users on the network. The purpose of AUT is to prevent cyber security threats and focus on productivity.

Because the company mobile devices access critical business data, that can threaten security if hacked, stolen, or lost. So, the mobile device management MDM is very important to manage all company devices and keep all devices secure. MDM include concepts like mobile application management that controls and secure organizational data with features like remote wiping in case of theft or loss, remote activation or deactivation of devices, and the IT admins can apply privacy policies on mobile application in case of using mobile devices for both work and personal use. Additionally, mobile content management to safeguard the content or data on mobile devices. Furthermore, mobile email management that offers a secure access to the organization email infrastructure and data on an employee’s mobile device. Moreover, enterprise mobility management to secure data in employees’ personal BYOD and organizational devices. Finally mobile security management that protects the organization’s network access and enables secure access to the organization’s email.

To maintain a proper data backup security in the company, information system secure backup strategies should be implemented. Firstly, identify the critical business data here is the sensitive data of patients. Secondly, selecting the backup media. Thirdly, selecting a backup technology by using RAID Redundant Array of Independent Disks technology. Fourthly, selecting the appropriate RAID level. Fifthly, selecting the appropriate backup method, hot backup when the application database or system is running and available to users, and cold backup when it’s not running, or warm backup a combination of both. Sixthly, selecting the backup types. Seventhly, choosing the right backup solution full, differential, or incremental. Finally, conducting a recovery drill test.

For a continuous security monitoring, the company should implement policies and procedures such as relying on security rating that informs cyber security experts about the security posture of the organization. Adding to that, identifying all digital assets; monitor security risks such as poor email security, open ports, domain hijacking, and leak data. Accompanying security monitoring with continuous monitoring of servers and network to anticipate It\T disruptions and find ways to restore services as quickly as possible; find solution and mitigation measures for exposed problems; improve resources where necessary to boost overall security and monitoring. If necessary, train employees to adopt new security measures and include the standards in the organization’s policies.

Implementing a proper training and continuing education policies in this organization play an important part to maintain its security. Starting from employee awareness and training since employee is one of the primary assets of the organization, a well-trained employee can help protecting and securing a company, but untrained employee is considered a threat to the company. Employee awareness training starts during orientation and periodically by following security policies and procedures for working with information technology, know whom to contact if they discover a security threat and should be able to identify the nature of data based on data classification. Furthermore, security policy training teaches employees how to perform their duties and to comply with the security policy to make employees aware of new updates on probable vulnerabilities that can occur if they do not follow the policies. Moreover, the company should provide physical security training to all employees by providing methods to reduce attacks, examine all devices and the chances of a data attack, teach the risk of carrying sensitive information, and the importance of having security personnel. Next to that, social engineering awareness training to remind employees about the organization’s policies like physical social engineering and changing passwords. Finally, train employees how to classify data.

To keep a system operational during a disaster the company should implement a business continuity plan that focuses on keeping business operational during a disaster to limit operational downtime. The business continuity plan ensures all IT systems, software and applications are accessible and recoverable, it aims at ensuring business operations continue during and after a disaster by switching critical IT systems over to remote, assessment of damage to physical facilities, notifying costumers, press and suppliers.

The company first objective focuses on the possibility of internal and external threat due to high turnover of key employees, and to achieve that, it’s necessary to determine threats and vulnerabilities through assessment techniques and knowing the exact physical and logical security threats that the organization is passing by. After discovering the threats and the vulnerabilities it should implement proper policies to protect all the information system, besides to policies and procedures for continuous security monitoring. To maintain security in the organization it should train and educate all employees continuously, and in case of a disaster it should pursue a business continuity plan to limit operational downtime. Developing a proper security improvement will protect critical assets and information systems.

Works Cited

Bernstein, C. *What is pii (personally identifiable information)? definition from* TechTarget *searchsecurity*. SearchSecurity.2021, September 24. <https://www.techtarget.com/searchsecurity/definition/personally-identifiable-information-PII>

Centers for Disease Control and Prevention. *Health Insurance Portability and accountability act of 1996 (HIPAA)*. <https://www.cdc.gov/phlp/publications/topic/hipaa.html#:~:text=The%20Health%20Insurance%20Portability%20and,the%20patient's%20consent%20or%20knowledge>

Council, EC. Network Defense Essentials. Version 1 ed. EC Council, 2021

CSRC Content. (n.d.). *Intrusion detection system (IDS) - glossary: CSRC*. From <https://csrc.nist.gov/glossary/term/intrusion_detection_system>

*Disaster recovery and business continuity plans*. Cloudian. (2022, May 11). from <https://cloudian.com/guides/disaster-recovery/disaster-recovery-and-business-continuity-plans/>

Ellis, R. (). *Continuous Security Monitoring - what, why, how.* Website Monitoring Server Monitoring Blog. 2021, October 28. <https://www.websitepulse.com/blog/continuous-security-monitoring>

Firch, J. *What are the common types of network vulnerabilities?* PurpleSec. (2022, June 2). <https://purplesec.us/common-network-vulnerabilities/>

*How to identify security vulnerabilities in businesses*. Consolidated Technologies, Inc. (2022, March 25). <https://consoltech.com/blog/identifying-business-security-vulnerabilities/amp/>

*Official PCI Security Standards Council Site*. PCI Security Standards Council. 22July,2022. <https://www.pcisecuritystandards.org/>

Physical Security Guide. *What is physical security? measures & planning guide + PDF*.

<https://www.openpath.com/physical-security-guide>