**7-2 Project Three: Network System Security Plan Recommendation**

Joshua Merren

Southern New Hampshire University

CYB-230-11349-M01 Operating System Security C-3

Professor Joshua Brogdon

20 June 2024

The Helios Health Insurance network currently operates workstations and laptops with unencrypted hard drives, which presents a significant risk to data integrity. Integrity ensures that the data is accurate and untouched by unauthorized persons. When drives are unencrypted, anyone who physically acquires a device can access and possibly alter or delete sensitive information without authorization. This scenario is particularly concerning in a health insurance context where data accuracy and confidentiality are critical for operational integrity and compliance with privacy laws. Unauthorized changes to data could lead to incorrect medical billing, improper patient care decisions, and breaches of confidential patient information. The lack of encryption may also expose the organization to legal and financial repercussions if sensitive data is compromised. Furthermore, if a device is lost or stolen, its data becomes immediately accessible, increasing the risk of data breaches. The current setup must align with best security practices that mandate data encryption to safeguard sensitive information. Implementing full-disk encryption would significantly enhance security by ensuring that all data stored on these devices is accessible only to those with proper authorization, thereby maintaining the data's integrity even if the device's physical security is compromised (Trivedi, 2024).

I recommend implementing full-disk encryption across all company workstations and laptops to address the significant risk posed by unencrypted hard drives in the Helios Health Insurance network. Full disk encryption converts all data on devices into a format only the correct decryption key, typically a password or security token can read. This measure will prevent unauthorized individuals from accessing or modifying the data, thus protecting its integrity. Encryption also helps ensure compliance with data protection regulations, which require protective measures for handling sensitive information such as patient health records. By encrypting the data, Helios Health Insurance will also mitigate potential damage from data breaches, as encrypted data remains secure even if the device is compromised. Furthermore, this approach will enhance the company’s reputation for taking proactive steps to protect client information. Implementing a central management system for encryption will allow the IT department to maintain control over encryption keys and ensure that security policies are uniformly applied across the organization (Saim, 2024).

A critical software-based deficiency in the Helios Health Insurance network is the need for regular updates and patches for end-user computers, despite these systems having full access to the internet. This deficiency exposes the network to malware and other cyber threats that can exploit vulnerabilities in outdated software, potentially leading to unauthorized modifications or data destruction. Maintaining data integrity is a critical component of network security, which requires that all systems are up-to-date to defend against such threats. With regular updates, the organization can avoid introducing errors into their systems, resulting in incorrect data processing and decision-making, affecting operational effectiveness and client trust. Additionally, failure to update software can violate compliance requirements for data protection, further exposing the organization to legal and regulatory penalties. Implementing consistent software updates would not only close security gaps but also enhance the overall reliability and performance of the network (Echols, 2024).

To effectively address the deficiency of outdated software on end-user computers within the Helios Health Insurance network, it is crucial to establish a stringent patch management policy. This policy should mandate regular automatic updates for all software, ensuring that the latest security patches and updates are applied as soon as they are available. Automating this process removes the reliance on end-users to perform updates, which can often be overlooked or delayed. Regular updates will protect the network from known vulnerabilities and cyber threats, maintaining the integrity and security of data. Additionally, this approach will streamline IT operations and ensure that all network components are consistently protected, reducing the risk of security breaches and data corruption. It might also be beneficial to invest in a centralized management system that can monitor and report on the updated status of each device, providing clear visibility into the network’s security posture (Echols, 2024).

References

Saim, H. (2024, May 24). Exploring Data Encryption : Benefits and best practices. *RedSwitches*. https://www.redswitches.com/blog/data-encryption/

Echols, T. (2024, March 26). The crucial role of data encryption in safeguarding your network | Stability Networks. *Stability Networks*. https://stabilitynetworks.com/data-encryption-in-safeguarding-your-network/

Trivedi, V. (2024, January 25). *Full Disk Encryption: Securing data effectively*. Technodized. https://technodized.com/security/full-disk-encryption-guide/