Activity - Incident handler's journal

Activity Overview

This project documents the process of analyzing and responding to a security incident involving ransomware at a healthcare clinic. The journal highlights key steps, findings, and recommendations made during the incident response process. It demonstrates the ability to identify, contain, and mitigate security threats while maintaining clear and concise documentation for stakeholders.

Scenario

A small U.S. healthcare clinic specializing in delivering primary-care services experienced a security incident on a Tuesday morning at approximately 9:00 a.m. Several employees reported that they were unable to use their computers to access files like medical records. Business operations shut down because employees could not access the files and software needed to do their jobs.

Additionally, employees also reported that a ransom note was displayed on their computers. The ransom note stated that all the company's files were encrypted by an organized group of unethical hackers who are known to target organizations in the healthcare and transportation industries. In exchange for restoring access to the encrypted files, the ransom note demanded a large sum of money in exchange for the decryption key.

The attackers gained access to the company's network by sending targeted phishing emails to several employees. The phishing emails contained a malicious attachment that installed malware on the employee's computer once it was downloaded.

Once the attackers gained access, they deployed the ransomware, which encrypted critical files. The company was unable to access essential patient data, causing major disruptions in its business operations. It was forced to shut down its computer systems and contact several organizations to report the incident and receive technical assistance.

Incident Handler Report

Date: July 23, 20xx	Entry: 1
Description	Documenting a cybersecurity incident
Tool(s) used	None.
The 5 W's	● Who: An organized group of unethical hackers ● What: A ransomware security incident ● Where: At a healthcare company specializing in primary care ● When: Tuesday, 9:00 a.m. ● Why: The attackers used a phishing attack to install ransomware. After

	gaining access, they encrypted critical files, preventing business operations. Their motivation seems financial, as the ransom note demanded payment for the decryption key.
Additional notes	1. Preventative Measures: • Implement mandatory cybersecurity awareness training focusing on phishing email detection. • Deploy multi-factor authentication (MFA) for all employee accounts to minimize the risk of unauthorized access. • Regularly update and patch systems to mitigate vulnerabilities that could be exploited by ransomware. • Backup critical files and data regularly in an isolated, secure location, ensuring availability even after an attacked. 2. Ransom Payment Decision: • The company should avoid paying the ransom, as paying it does not guarantee that the files will be decrypted and might encourage further attacks. Instead, they should contact law enforcement and cybersecurity professionals to attempt file recovery and assess the situation.

Conclusion: The Incident Handler's Journal provides a detailed account of the steps taken to investigate, contain, and remediate a ransomware attack at a healthcare clinic. The project demonstrates skills in incident response, forensic analysis, and stakeholder communication. It highlights the importance of proactive security measures to mitigate future risks.