Incident Handler's Journal Entry

Date: 2025-05-14
Entry Number: 1

Description:
A ransomware attack targeted a small U.S. health care clinic, significantly disrupting business operations by encrypting critical files. Employees were unable to access medical records or essential software, halting business functions. A ransom note indicated that the files were encrypted by a known hacker group that targets healthcare and transportation organizations, demanding payment for the decryption key.

Tool(s) Used:
None reported at the time of the incident.

The 5 W's:
Who: An organized group of unethical hackers, known for targeting healthcare and transportation industries.
What: A ransomware attack that encrypted critical files and disrupted business operations.
When: Tuesday at approximately 9:00 a.m.
Where: A small U.S. health care clinic specializing in primary-care services.
Why: The attack was made possible through a targeted phishing email containing a malicious attachment, which was downloaded by an employee.

Additional Notes:
The phishing attack highlights the need for enhanced email security protocols and employee training on recognizing malicious emails. Consider collaborating with cybersecurity experts to conduct a thorough vulnerability assessment and initiate incident response measures.