Incident Handler's Journal

Date: 19/04/2025

Entry: #1

# Description

Cybersecurity Incident

# Tool(s) used

Phishing emails, malware (ransomware)

# The 5 W's

Who: Malicious hacking group known to target the healthcare and transportation sectors.

What: Sent phishing emails with malicious attachments that installed ransomware.

When: Tuesday at approximately 9:00 a.m.

Where: The internal network and systems of the U.S. healthcare clinic.

Why: The phishing emails tricked employees into downloading a malicious attachment. This installed ransomware that encrypted critical data. The ransom note indicated financial motivation, demanding a large sum of money in exchange for a decryption key.

# Additional Notes

How can the company prevent future similar attacks?

- Conduct regular phishing awareness and training programs for employees.  
- Implement email filtering and attachment scanning solutions.  
- Utilize endpoint detection and response (EDR) tools.  
- Apply regular software updates and patches.  
- Maintain and test offline backups frequently.  
- Segment networks to minimize damage in case of compromise.

Are there any backups?

This must be verified. The company should assess the availability and integrity of recent backups.

Should the company pay the ransom to retrieve the decryption key?

It is generally discouraged to pay the ransom, as it incentivizes further attacks and does not guarantee data recovery. Instead, the incident should be reported to law enforcement and cybersecurity professionals should be consulted.