Incident handler's journal

Scenario

A small U.S. health care 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 were unable to access the files and software needed to do their job. 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 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 were able to gain access into the company's network by using targeted phishing emails, which were sent to several employees of the company. 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 their ransomware, which encrypted critical files. The company was unable to access critical patient data, causing major disruptions in their business operations. The company was forced to shut down their computer systems and contact several organizations to report the incident and receive technical assistance.

Date: June 23, 2024	**Entry:** 1
Description	Security incident involving ransomware attack on a small U.S. health care clinic
Tool(s) used	List any cybersecurity tools that were used.
The 5 W's	Capture the 5 W's of an incident. • **Who** : An organized group of unethical hackers known to target healthcare and transportation industries. • **What**: Ransomware was deployed by using a phishing attack encrypting the clinic's computer files. A ransom note demanding a large sum of money for the decryption key was displayed. • **When**: The incident occurred on a Tuesday morning at approximately 9:00 a.m. • **Where**: The incident happened at a small U.S. health care clinic specializing in delivering primary-care services. • **Why:** The incident happened because the attackers used targeted phishing emails to gain access to the clinic's network and deploy ransomware, leading to the encryption of critical files and disruption of business operations.
Additional notes	A thorough review of email security policies and employee training on recognizing phishing attempts is necessary to prevent future incidents. Regular backups and an incident response plan are crucial for minimizing the impact of such attacks.