Scenario

Review the following scenario. Then complete the step-by-step instructions.

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 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 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 essential data of the patient, causing significant disruptions in their business operations. The company was forced to shut down its computer systems and contact several organizations to report the incident and receive technical assistance.

Incident handler's journal

Instructions

Date: 2023-09-30	**Entry**: 1
Description	Security incident at a small U.S. healthcare clinic
Tool(s) used	None yet
The 5 W's	• **Who** caused the incident? An organized group of unethical hackers • **What** happened? The hackers deployed ransomware on the clinic's network, encrypting critical files. • **When** did the incident occur? Tuesday, 9:00 AM • **Where** did the incident happen? A small U.S. healthcare clinic • **Why** did the incident happen? The hackers used targeted phishing emails to access the clinic's network.
Additional notes	• The incident has severely disrupted the clinic's business operations. • The clinic is unable to access critical patient data. • The clinic has been forced to shut down its computer systems. • The clinic has contacted several organizations to report the incident and receive technical assistance.