Christian Mamutt 12/30/24

Incident handler's journal

Scenario 1

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: December 30, 2024	**Entry:** 1
Description	Documenting a ransomware attack on a small U.S. healthcare clinic that disrupted operations and encrypted critical patient data.
Tool(s) used	None initially (to be updated after forensic analysis or incident response begins).
The 5 W's	• **Who caused the incident?** An organized group of unethical hackers targeting healthcare and transportation sectors. • **What happened?** The attackers gained network access via a phishing email containing a malicious attachment. This installed malware that deployed ransomware, encrypting the clinic's files and displaying a ransom note. • **When did the incident occur?** Tuesday at approximately 9:00 a.m. • **Where did the incident happen?** A small U.S. healthcare clinic specializing in primary care. • **Why did the incident happen?** The clinic fell victim to targeted phishing emails, leading to the execution of ransomware after an employee downloaded a malicious attachment.
Additional notes	Immediate action is required to isolate infected systems and prevent further damage. Consider implementing employee cybersecurity awareness training to mitigate future phishing attempts. Investigate the use of anti-phishing tools and endpoint protection to detect and block malicious emails and attachments. Explore the feasibility of recovering encrypted files through backups before considering communication with the attackers.