Cybersecurity Incident Report:

Ransomware Attack on Employee Workstations

Part 1: Provide a summary of the problem found in the Workstation Logs.
The network analysis reveals that: An employee's workstation was infected with ransomware following the opening of a suspicious email attachment. The malicious file was downloaded from an external email source pretending to be a vendor. This is based on the results of the log analysis, which show that: • The ransomware executed immediately after an employee downloaded a file named "Invoice_Sept2024.pdf.exe." • All files on the infected workstation were encrypted with the ".locked" extension. The ransomware affected: Multiple files in the "Documents" folder and other business-critical data. The most likely issue is: The employee opened a malicious attachment from an unverified email, which executed the ransomware and began encrypting the files on the local system. Additionally, the system did not have up-to-date antivirus protection or recent backups.
Part 2: Explain your analysis of the data and provide at least one cause of the incident.
Time the incident occurred: The incident was reported at 9:30 a.m. on September 22, 2024, when an employee was unable to access their files and noticed a ransom note on their screen. **How the IT team became aware of the incident**: Several employees reported receiving a message demanding payment in Bitcoin to decrypt their files. This message was accompanied by the inability to open work-related documents. **Actions taken by the IT department to investigate the incident**: • The IT team isolated the infected workstation from the network to prevent further spread. • Network traffic logs were analyzed using monitoring tools, and the malicious email attachment was identified as the source of the ransomware infection. • Affected systems were inspected for signs of further malware or lateral movement across the network. **Key findings of the IT department's investigation**:

- The ransomware was traced back to a phishing email sent from a spoofed address, prompting the employee to download a file that executed malicious code.
- The file, once executed, initiated the encryption process on the local system, with files renamed to include the ".locked" extension.
- Antivirus software on the affected systems was not up-to-date, allowing the malware to bypass security measures.

Likely cause of the incident:

1. The employee unknowingly downloaded and executed a malicious file.
2. The ransomware exploited vulnerabilities in unpatched software on the workstation.
3. Lack of up-to-date antivirus protection and recent backups exacerbated the impact of the attack.

This ransomware incident emphasizes the need for improved email security, prompt software updates, and regular data backups to protect against similar threats in the future.