**Incident handler's journal**

|  |  |
| --- | --- |
| **Date:**  30/01/2025 | **Entry:**  01 |
| Description | This journal entry documents a ransomware attack on a small U.S. health care clinic initiated through a phishing email. The attack severely disrupted business operations, and the attackers demanded a ransom for file decryption. |
| Tool(s) used | Network Monitoring tool (WireShark)  Incident Response Platform (IBM Resilient)  Email filtering tool (Mimecast)  Endpoint detection and response |
| The 5 W's | * **Who** caused the incident?   An organized group of unethical hackers.   * **What** happened?   A phishing email containing a malicious attachment was opened leading to the deployment of a ransomware that encrypted the clinic’s computer files.   * **When** did the incident occur?   Tuesday at 9:00 AM   * **Where** did the incident happen?   At the small U.S. health care clinic infrastructure.   * **Why** did the incident happen?   The phishing email successfully bypassed email security measures, and the malicious attachment was downloaded, likely due to lack of employee awareness or insufficient email filtering. |
| Additional notes | The clinic did not have a robust incident plan which lead to the delay in containment and recovery efforts.  Regular training on phishing could have prevented this incident. |