**Incident handler's journal**

**Instructions**

As you continue through this course, you may use this template to record your findings after completing an activity or to take notes on what you've learned about a specific tool or concept. You can also use this journal as a way to log the key takeaways about the different cybersecurity tools or concepts you encounter in this course.

|  |  |
| --- | --- |
| **Date:**  20th November 2023 | **Entry:**  1 |
| Description | A small U.S. healthcare clinic experienced a ransomware attack that encrypted critical patient records and business files. The attack was executed via phishing emails sent to employees, which contained a malicious attachment that installed malware upon opening. This led to business operations shutting down as employees were unable to access critical data. |
| Tool(s) used | * Antivirus & Endpoint Detection and Response (EDR): To scan and identify the ransomware. * Firewall & Intrusion Detection System (IDS): To analyze potential unauthorized network traffic. * Backup & Recovery System: To restore encrypted data where possible. |
| The 5 W's | Who caused the incident?  An organized group of unethical hackers known for targeting the healthcare and transportation industries.  What happened?  Attackers gained access to the company’s network through phishing emails containing malicious attachments. Once opened, malware was installed, allowing the hackers to deploy ransomware that encrypted important company files. A ransom note was displayed demanding a large sum of money for the decryption key.  When did the incident occur?  On a Tuesday morning, at approximately 9:00 AM.  Where did the incident happen?  At a small U.S. healthcare clinic specializing in primary-care services.  Why did the incident happen?  Employees unknowingly downloaded and opened a phishing email attachment, allowing malware to infiltrate the network. The clinic lacked adequate email security measures to prevent malicious attachments from reaching employees. |
| Additional notes | Business operations were completely halted due to file encryption, preventing employees from accessing medical records. |

|  |
| --- |
| Reflections/Notes: The organization should strengthen email security and employee training to recognize phishing attempts and conduct a forensic investigation to determine the full extent of the breach. They should also establish a comprehensive incident response and business continuity plan. |