**Incident handler's journal**

|  |  |
| --- | --- |
| **Date:**  05-05-2025 | **Entry:**  1 |
| Description | Ransomware incident: Hackers brought down systems and are holding critical data at ransom. |
| Tool(s) used | * Ransomware * Phishing kits |
| The 5 W's | ● **Who:** An organized group of unethical hackers  **● What:** A ransomware security incident  **● Where:** At a health care company  **● When:** Tuesday 9:00 a.m.   * **Why:** The incident happened because unethical hackers were able to access the company's systems using a phishing attack. After gaining access, the attackers launched their ransomware on the company's systems, encrypting critical files. The attackers' motivation appears to be financial because the ransom note they left demanded a large sum of money in exchange for the decryption key. |
| Additional notes | We don’t know who opened the email? Will need to tighten our security controls and provide training on how to detect forged emails. The recommendation is to pay the ransom and retrieve the decryption key. We will then need to let the patients know about the data breach. |

|  |  |
| --- | --- |
| **Date:**  06-05-2025 | **Entry:**  2 |
| Description | A phishing email was opened and a malicious file was downloaded onto a computer |
| Tool(s) used | In this scenario I was in the position of a security analyst and I used VirusTotal which is an investigative tool that analyses a files hash code to check for viruses, worms or trojans.  This incident occurred in the detection and analysis phase. After the file was detected by the security systems in place I had to perform a deeper analysis to decide if this case should be escalated or not. |
| The 5 W's | Capture the 5 W's of an incident.   * **Who**: Unethical lone hacker * **What**: Phishing attack * **When**: Incident occurred at 10:30am on 29/04/2025 * **Where**: Financial services company. End device MAC address is 00:1A:2B:3C:4D:5E * **Why:** An employee, unbeknown to them downloaded a malicious file from an email that looked to be sent to them by a known and trusted source. |
| Additional notes | We need new security controls on verifying trusted email addresses.  Will the hacker try again? We will analyze the network traffic using a SIEM tool to find any other indications of compromise |

|  |  |
| --- | --- |
| **Date:**  15/05/2025 | **Entry:**  3 |
| Description | At 3:13 p.m., PT, on December 22, 2022 the organization received an email demanding money to not leak customers PII and financial records. 50,000 worth of crypto was the asking price |
| Tool(s) used |  |
| The 5 W's | Capture the 5 W's of an incident.   * **Who**: External unethical hacker * **What**: Sensitive data exfiltration. (Financial information, Credit Card details) * **When**: December 22, 2022 * **Where**: E-Commerce website, SO. CAL. * **Why**: There was a vulnerability in the e-commerce website in which the attacker exploited to gain access to otherwise restricted information. This vulnerability allowed the attacker to perform a forced browsing attack and access customer transaction data by modifying the order number included in the URL string of a purchase confirmation page. This vulnerability allowed the attacker to access customer purchase confirmation pages, exposing customer data, which the attacker then collected and exfiltrated. |
| Additional notes | Alt of money and public reputation was lost in the process, however, the organization used it as a massive learning curve in strengthening their security posture.  To prevent future recurrences, I have recommended the following actions: Perform routine vulnerability scans and penetration testing. Implement the following access control mechanisms: Implement allowlisting to allow access to a specified set of URLs and automatically block all requests outside of this URL range. Ensure that only authenticated users are authorized access to content. |

|  |  |
| --- | --- |
| **Date:**  Record the date of the journal entry. | **Entry:**  Record the journal entry number. |
| Description | Provide a brief description about the journal entry. |
| Tool(s) used | List any cybersecurity tools that were used. |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? * **What** happened? * **When** did the incident occur? * **Where** did the incident happen? * **Why** did the incident happen? |
| Additional notes | Include any additional thoughts, questions, or findings. |

|  |  |
| --- | --- |
| **Date:**  19/05/2025 | **Entry:**  4 |
| Description | Capturing my first packet |
| Tool(s) used | For this exercise I used tcpdump to capture and analyze network traffic. Tcpdump is a network protocol analyzer that’s accesses through the command line interface (CLI) . Similar to Wireshark, the value of tcpdump in cybersecurity is that it allows security analysts to capture, filter and analyze network traffic. |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** N/A * **What** N/A * **When** N/A * **Where** N/A * **Why** N/A |
| Additional notes | As I have previous experience using the CLI I had fun learning this new technology. I was able to try different options, capture logs and write them to files. I found that using tcpdump alongside Wireshark worked well for me. Capturing the logs on tcpdump, writing them to a pcap file and then opening this file on Wireshark to use its graphical user interface (GUI) to view and interact with the logs. |