**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:**  Tuesday 9:00 am | **Entry:**  Entry 1 |
| Description | Phishing email sent to numerous employees contained malicious attachment downloading ransomware and encrypted the organizations computer files. The ransom note stated they are demanding a large sum of money in order to unencrypt the files. Primary care services are provided by the company and due to not being able to access medical records and other documents business operations were unable to be completed. |
| Tool(s) used | None. |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? A group of unorganized unethical hackers * **What** happened? Phishing email encrypted business files and money is being demanded to unlock them. (ransomware) * **When** did the incident occur? 9:00 am Tuesday morning. * **Where** did the incident happen? U.S. healthcare clinic * **Why** did the incident happen? Phishing email with malicious attachment was opened by one or more employees of the company. |
| Additional notes | Team members may need to be trained to spot phishing emails going forward. Should the company pay the ransomware sum to decrypt files? |

|  |  |
| --- | --- |
| **Date:**  Wednesday 7/20/22 9:30:14 am | **Entry:**  Entry 2 |
| Description | A phishing email was sent to an HR employee expressing interest for a engineer role posted on our website. Attached to the email is a document for a “cover letter and resume” that is password protected. Password was given in the email and once opened downloaded a malicious file. |
| Tool(s) used | None. |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? Threat actor/hacker * **What** happened? Phishing email was opened downloading a malicious file. * **When** did the incident occur? 9:30 am Wednesday morning. * **Where** did the incident happen? Inergy * **Why** did the incident happen? Phishing email opened by an HR employee. |
| Additional notes | Employees of company could use more training on phishing. Password protected documents should be a red flag going forward. Link is verified malicious. Escalating event. |

|  |  |
| --- | --- |
| **Date:**  12/28/22 7:20 pm. | **Entry:**  Entry 3 |
| Description | A threat actor was able to exploit a vulnerability in the e-commerce web application using a forced browsing attack which allowed him access to customer transaction data. They were able to see purchase confirmation pages and the threat actor collected and exfiltrated this PII. After exfiltrating the data, he emailed an employee requesting $50,000 in exchange for not releasing this data to the public. |
| Tool(s) used | None. |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? Hacker. * **What** happened? Exploited a vulnerability in our web application that gave access to customer’s PII then requested money in exchange for not releasing this data. * **When** did the incident occur? 12/22/22 was time of first email that employee believed to be fake. 12/28/22 was second email with proof of stolen PII. * **Where** did the incident happen? E-commerce web based application * **Why** did the incident happen? A vulnerability was exploited that was overlooked by the security team. |
| Additional notes | Need to make sure we do more routine vulnerability scans and pen testing. Need to make sure employees escalate these type of emails the first time they are received so they can be investigated instead of deleting them. |