**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:**  Record the date of the journal entry. | **Entry:** 001  **Wednesday 17 May 2023** |
| Description | The health care clinic experienced a severe security incident that disrupted their business operations. The incident was caused by a targeted phishing email containing a malicious attachment, which led to the deployment of ransomware encrypting the clinic's computer files. An organized group of unethical hackers left a ransom note demanding a large sum of money in exchange for the decryption key. |
| Tool(s) used | Ransomware |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident?   An organized group of unethical hackers.   * **What** happened?   The hackers gained access through a phishing email, deployed ransomware, and encrypted the clinic's computer files.   * **When** did the incident occur?   On a Tuesday morning at approximately 9:00 a.m.   * **Where** did the incident happen?   At the U.S. health care clinic.   * **Why** did the incident happen?   The attackers targeted the clinic to gain financial advantage by encrypting their files and demanding a ransom. |
| Additional notes | It would be important for the clinic to immediately report the incident to the appropriate authorities and seek technical assistance to mitigate the impact. Measures should be taken to prevent future incidents, such as implementing strong email security practices, employee training on phishing awareness, and robust backup and recovery procedures. |

|  |  |
| --- | --- |
| **Date:**  Record the date of the journal entry. | **Entry:** 002  **Thursday 18 May 2023** |
| Description | An alert was received to the SOC at the financial services company which reported about a suspicious file downloaded from an employee’ computer.  As it happens very often the employee opened an email and downloaded the attachment and proceed to open it with a given password without realizing it had possibly downloaded malware. |
| Tool(s) used | Trojan |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident?   Likely organized group of unethical hackers.   * **What** happened?   Through a phishing email a possibly malicious payload was executed in the employee’s computer that cause an alert.   * **When** did the incident occur?   Not given   * **Where** did the incident happen?   At the financial services company.   * **Why** did the incident happen?   An employee perhaps inadvertently opened an email and download the malware that was contained in the attachment. |
| Additional notes | This type of attacks happened usually because of poor training in information security practices from employees as well as intentionally by disgruntled employees. |

|  |  |
| --- | --- |
| **Date:**  Record the date of the journal entry. | **Entry:** 003  **Friday 19 May 2023** |
| Description | An attachment has been verified as malicious which was downloaded by an employee at the financial security services company. It is time to follow the organization's process to complete the investigation and resolve the alert with tools such as the playbook. |
| Tool(s) used | Trojan |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident?   Likely organized group of unethical hackers experts in social engineering.   * **What** happened?   Through a phishing email a malicious payload was executed in the employee’s computer that cause an alert.   * **When** did the incident occur?   Not given date   * **Where** did the incident happen?   At the financial services company.   * **Why** did the incident happen?   An employee inadvertently opened an email and download the malware that was contained in the attachment. |
| Additional notes | Thanks to the playbook it makes it much easier and faster to respond to the incident in an organized manner. It is also useful to note that the playbook allows itself be updated and modified according to past experiences in order to optimize it. |

|  |  |
| --- | --- |
| **Date:**  Record the date of the journal entry. | **Entry:** 004  **Wednesday 20 May 2023** |
| Description | An unauthorized individual gained access to customer personal identifiable information (PII) and financial information of the mid-sized retail company. It caused some financial damage as well as a data leak of customers private information. |
| Tool(s) used | Insecure Direct Object Reference (IDOR) vulnerability(Web access control vulnerability) |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident?   A single unauthorized individual.   * **What** happened?   The unauthorized individual gained access to customer personal identifiable information (PII) and financial information. Approximately 50,000 customer records were affected.   * **When** did the incident occur?   On December 22, 2022, at approximately 3:13 p.m. PT, an employee received an initial email from the attacker. The incident escalated on December 28, 2022, when the same employee received a second email containing a sample of stolen customer data and an increased payment demand.   * **Where** did the incident happen?   At the computer systems and website of the mid-sized retail company.   * **Why** did the incident happen?   The attacker manage to vulnerability in the e-commerce web application, allowing the attacker to perform a forced browsing attack and access customer transaction data.. |
| Additional notes | - It was a goof thing that the incident was reported by the employee quickly.  - There was good coordination between the SOC and the public relation department.  - Offering identity protection services to the affected customers free of charge and notify them is better than stay silent. It also helps to safeguard the reputation of the company. |

**Goal 1: Identify exactly what happened.**

* Note that an unauthorized individual gained access to customer personal identifiable information (PII) and financial information.
* Approximately 50,000 customer records were affected.
* The incident was caused by a vulnerability in the e-commerce web application, allowing the attacker to perform a forced browsing attack and access customer transaction data.

**Goal 2: Identify when it happened.**

* On December 22, 2022, at approximately 3:13 p.m. PT, an employee received an initial email from the attacker.
* The incident escalated on December 28, 2022, when the same employee received a second email containing a sample of stolen customer data and an increased payment demand.

**Goal 3: Identify the response actions that the company took.**

* The employee who received the second email promptly notified the security team, initiating the investigation.
* The security team analyzed the web application access logs to determine the extent of the data theft.
* The organization collaborated with the public relations department to disclose the data breach to customers.
* Identity protection services were offered to affected customers.

**Goal 4: Identify future recommendations.**

* Perform routine vulnerability scans and penetration testing to identify and address vulnerabilities proactively.
* Implement an “allow\_list” of URLs to restrict access to a specified set of URLs and automatically block requests outside of this range.
* Ensure that only authenticated users are authorized to access content, improving access control mechanisms.
* By reviewing the provided information, I can achieve the goal of understanding what happened, when it happened, the company's response actions, and future recommendations to prevent similar incidents in the future.