**Incident handler's journal Entry 4**

**Instructions**

You recently joined the security team as a level-one security operation center (SOC) analyst at a mid-sized retail company. Along with its physical store locations, your company also conducts operations in e-commerce, which account for 80% of its sales.

You are spending your first week of training becoming familiar with the company's security processes and procedures. Recently, the company experienced a major security incident involving a data breach of over one million users. Because this was a recent and major security incident, your team is working to prevent incidents like this from happening again. This breach happened before you began working at the company. You have been asked to review the final report. To gain an understanding of the incident's life cycle, your goals for your review are as follows:

* Goal 1: Identify exactly what happened.
* Goal 2: Identify when it happened.
* Goal 3: Identify the response actions that the company took.
* Goal 4: Identify future recommendations.

|  |  |
| --- | --- |
| **Date:**  10/21/2023 | **Entry:**  Entry 4 |
| Description | Review a final report |
| Tool(s) used | Final Report |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? An unidentified attacker exploited a vulnerability in the e-commerce web application. * **What** happened? The attacker gained unauthorized access to customer transaction data by modifying the order number included in the URL string of a purchase confirmation page. * **When** did the incident occur? The initial attack occurred on December 22, 2022. The security team was notified on December 28, 2022. * **Where** did the incident happen? The incident happened because of a vulnerability in the e-commerce web application that allowed for forced browsing attacks. * **Why** did the incident happen? The incident happened because of a vulnerability in the e-commerce web application that allowed for forced browsing attacks. |
| Additional notes | How was the attacker able to identify the vulnerability in the web application?  Were there any other security controls in place that could have prevented this incident?  What steps is the organization taking to ensure that this type of incident does not happen again? |

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

The incident involved a forced browsing attack that allowed the attacker to access customer transaction data by modifying the order number included in the URL string of a purchase confirmation page.

The attacker collected and exfiltrated customer purchase confirmation pages, exposing customer data.

Approximately 50,000 customer records were affected.

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

The initial attack occurred on December 22, 2022, when the employee received an email from the attacker claiming to have stolen customer data.

The attacker sent a second email on December 28, 2022, with a sample of the stolen data and an increased payment demand.

The security team was notified on December 28, 2022, and began their investigation.

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

The security team investigated the incident and determined the root cause.

The company collaborated with the public relations department to disclose the data breach to its customers.

The company offered free identity protection services to customers affected by the incident.

**Goal 4: Identify future recommendations.**

Perform routine vulnerability scans and penetration testing.

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.