Case Study:
The National Institute of Standards and Technology (NIST) Lifecycle - Review a Final Report

Scenario:

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.

INCIDENT FINAL REPORT

Executive summary

The organization experienced a security incident on December 28, 2022, at 7:20 p.m., PT, during which an individual was able to gain unauthorized access to customer personal identifiable information (PII) and financial information. Approximately 50,000 customer records were affected. The financial impact of the incident is estimated to be $100,000 in direct costs and potential loss of revenue. The incident is now closed and a thorough investigation has been conducted.

Timeline

At approximately 3:13 p.m., PT, on December 22, 2022, an employee received an email from an external email address. The email sender claimed that they had successfully stolen customer data. In exchange for not releasing the data to public forums, the sender requested a $25,000 cryptocurrency payment. The employee assumed the email was spam and deleted it.

On December 28, 2022, the same employee received another email from the same sender. This email included a sample of the stolen customer data and an increased payment demand of $50,000.

On the same day, the employee notified the security team, who began their investigation into the incident. Between December 28 and December 31, 2022, the security team concentrated on determining how the data was stolen and the extent of the theft.

Investigation

The security team received the alert and traveled on-site to begin the investigation.

The root cause of the incident was identified as a vulnerability in the e-commerce web application. 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.

After confirming the web application vulnerability, the security team analyzed the web application access logs. The logs indicated that the attacker accessed the information of thousands of purchase confirmation pages.

Response and remediation

The organization collaborated with the public relations department to disclose the data breach to its customers. Additionally, the organization offered free identity protection services to customers affected by the incident.

After the security team reviewed the associated web server logs, the cause of the attack was very clear. There was a single log source showing an exceptionally high volume of sequentially listed customer orders.

Recommendations

To prevent future recurrences, we are taking 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.