INCIDENT FINAL REPORT

Executive summary

On December 28, 2022, at 7:20 p.m. PT, the organization encountered a security incident resulting in unauthorized access to customer personal identifiable information (PII) and financial data. Around 50,000 customer records were compromised. The incident has been resolved, following a comprehensive investigation. The estimated financial impact amounts to $100,000 in direct costs and potential revenue loss.

Timeline

Around 3:13 p.m., PT, on December 22, 2022, an employee received an email originating from an external address. The sender of the email asserted that they had successfully obtained customer data and proposed a ransom of $25,000 in cryptocurrency to prevent public disclosure. Regarding the email, the employee regarded it as spam and promptly deleted it.

Subsequently, on December 28, 2022, the same employee received another email from the identical sender, which contained a portion of the pilfered customer data. Moreover, the sender now demanded an escalated payment of $50,000.

On the very same day, the employee promptly reported the matter to the security team, initiating their investigation into the incident. From December 28 to December 31, 2022, the security team focused their efforts on determining the method of data theft and evaluating the magnitude of the breach.

Investigation

The security team was notified of an alert and promptly went on-site to initiate the investigation. Upon investigation, it was determined that the incident stemmed from a vulnerability in the e-commerce web application. This particular vulnerability enabled the attacker to carry out a forced browsing attack, gaining unauthorized access to customer transaction data by manipulating the order number within the URL of a purchase confirmation page. Exploiting this vulnerability, the attacker managed to retrieve and extract customer data by accessing their purchase confirmation pages.

Once the web application vulnerability was confirmed, the security team proceeded to examine the web application access logs. These logs revealed that the attacker had accessed the information contained in thousands of purchase confirmation pages.

Response and remediation

The organization partnered with the public relations department to inform its customers about the data breach. Furthermore, affected customers were provided with complimentary identity protection services by the organization.

Upon reviewing the web server logs, the security team easily determined the cause of the attack. A particular log source revealed an unusually high number of customer orders listed in sequential order.

Recommendations

In order to avoid future repetitions, we will undertake the following measures:

- Conduct regular vulnerability scans and penetration testing.
- Enforce the implementation of access control mechanisms as follows:
    - Incorporate allowlisting to permit access solely to a specified range of URLs, automatically blocking any requests beyond this defined range.

- Verify that access to content is granted only to authenticated users.