INCIDENT FINAL REPORT

Executive Summary: On December 28, 2022, at 7:20 p.m. PT, the organization encountered a security incident wherein an unauthorized individual gained access to customer personal identifiable information (PII) and financial data. Approximately 50,000 customer records were compromised, resulting in an estimated financial impact of $100,000 in direct costs and potential revenue loss. The incident has been successfully resolved, concluding with a comprehensive investigation.

Timeline: Around 3:13 p.m. PT on December 22, 2022, an employee received an email from an external address claiming successful theft of customer data. The sender demanded a $25,000 cryptocurrency payment to prevent public disclosure, but the employee dismissed it as spam and deleted the email. On December 28, 2022, the same employee received a subsequent email from the same sender, presenting a sample of the stolen data and raising the payment demand to $50,000.

The employee promptly reported the incident to the security team, initiating an investigation between December 28 and December 31, 2022. The focus was on identifying the method of data theft and assessing the extent of the compromise.

Investigation: Upon receiving the alert, the security team conducted an on-site investigation. The root cause was identified as a vulnerability in the e-commerce web application, enabling a forced browsing attack. The attacker manipulated the order number in the URL string of a purchase confirmation page, accessing customer transaction data. This vulnerability allowed unauthorized access to customer purchase confirmation pages, leading to the exposure and exfiltration of customer data.

Web application access logs confirmed the attacker's access to thousands of purchase confirmation pages, substantiating the extent of the breach.

Response and Remediation: Collaborating with the public relations department, the organization disclosed the breach to customers and offered complimentary identity protection services to those affected. In-depth analysis of web server logs revealed a conspicuous single log source with an exceptionally high volume of sequentially listed customer orders, pinpointing the cause of the attack.

Recommendations: To avert future occurrences, the organization is implementing the following measures:

1. Conduct routine vulnerability scans and penetration testing.
2. Enforce access control mechanisms, including:
    - Implementation of allowlisting for specified URLs, automatically blocking requests outside this range.
    - Ensure that only authenticated users are authorized access to content.