Incident Final Report – Cybersecurity Portfolio Entry

Executive Summary

On **December 28, 2022, at 7:20 PM PT**, a security incident resulted in unauthorized access to **50,000 customer records**, exposing **personally identifiable information (PII) and financial data**. The estimated financial impact was **$100,000** in direct costs and potential revenue loss. A thorough investigation was conducted, and the incident is now closed.

Timeline of Events

- **December 22, 2022, 3:13 PM PT** – An employee received an extortion email claiming customer data had been stolen, demanding **$25,000** in cryptocurrency. The email was ignored as spam.
- **December 28, 2022** – The same sender emailed again, providing a sample of the stolen data and increasing the ransom to **$50,000**.

- **December 28, 2022** – The employee reported the email, prompting the **security team to initiate an investigation**.
- **December 28 - December 31, 2022** – The security team analyzed logs and identified the method of attack.

Investigation Findings

The root cause was a **forced browsing attack** on the company's **e-commerce web application**. The attacker manipulated **order numbers in URL strings** to gain access to customer transaction data, systematically retrieving thousands of purchase confirmation pages.

Incident Response and Remediation

- The organization **publicly disclosed** the data breach and provided **free identity protection services** to affected customers.
- Security logs confirmed an abnormal pattern of **sequential customer order access**, which pinpointed the attack method.

Recommendations for Future Prevention

- **Routine vulnerability scans and penetration testing** to identify potential weaknesses.
- **Access control enhancements:**
    - **Allowlisting** to restrict access to only authorized URLs.
    - **Authentication enforcement** to ensure that only verified users can access transaction data.