INCIDENT FINAL REPORT

Executive Summary:

On September 5, 2024, at 9:45 p.m. ET, the organization experienced a security breach where unauthorized access was gained to internal HR records, compromising personal identifiable information (PII) and salary data of employees. Approximately 45,000 employee records were affected. The financial impact of this incident is estimated to be $120,000 in direct costs, including mitigation efforts and potential legal expenses. The incident has since been closed, and a thorough investigation has been completed to determine the root cause and strengthen future defenses.

Timeline:

At around 2:00 p.m. ET on January 15, 2023, a manager received an email from an unknown external sender. The email claimed that internal employee data had been stolen and offered a sample of the stolen data as proof. The sender demanded $35,000 in cryptocurrency, threatening to release the full database if payment wasn’t made. The manager initially disregarded the email, assuming it was a phishing attempt.

On January 20, 2023, the same manager received another email from the same source, this time containing more sensitive employee records and increasing the ransom demand to $70,000. That day, the manager alerted the IT security team, who promptly initiated a formal investigation.

Between January 20 and January 25, 2023, the security team worked to determine how the breach occurred and the scale of the compromised data.

Investigation:

Upon receiving the alert, the security team began an on-site investigation. They quickly identified the root cause as a misconfigured internal server that exposed sensitive HR data to unauthorized users. A flaw in the server's access control mechanisms allowed the attacker to bypass standard security checks and access employee records by modifying the query parameters in the URL.

Once the vulnerability was confirmed, the security team reviewed the server logs and discovered that the attacker had accessed thousands of employee records over a two-week period, gathering sensitive HR data that was later used in the extortion attempt.

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 allow-listing 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.