Incident Response Report (Based on NIST SP 800-61)

Incident Name: Unauthorized Data Access – Financial Records Breach

Date:12, 2024

Incident Handler: [Lassana Bakayoko]

Location: [Charlotte, NC]

Executive Summary:

On June 12, 2024, at 7:30 p.m. ET, unauthorized access to the organization's financial records was detected. The attacker compromised a server containing sensitive financial information, including customer credit card numbers and billing addresses. Approximately 25,000 customer records were affected. This incident response report follows the NIST 800-61 guidelines and details the response, containment, eradication, and recovery measures taken.

Phases of Incident Response (NIST SP 800-61)

1-Preparation:

- **Security Controls**:

Prior to the incident, the organization had implemented essential controls, including network firewalls, antivirus software, and endpoint detection and response (EDR) tools.

- **Incident Response Team (IRT):**

A dedicated incident response team was established, including IT security staff, legal, and communications representatives. Each member was trained on their roles in handling incidents.

- **Response Plan:**

The organization followed an incident response plan based on NIST SP 800-61, which included predefined procedures for detecting, responding to, and recovering from security incidents.

2-Detection and Analysis:

-**Incident Detection**:

On June 14-, 2024, an alert was triggered by the Security Information and Event Management (SIEM) system, identifying suspicious access attempts to the financial records database from an unrecognized IP address.

- **Incident Analysis:**

The incident response team (IRT) immediately analyzed the logs from the SIEM system and found multiple failed login attempts followed by a successful breach of the financial database. The attacker utilized stolen credentials to bypass security measures.

- **Indicators of Compromise (IoCs):**

  - Unauthorized logins from an IP address outside of the normal geographic range.
  - Multiple failed login attempts followed by a successful access attempt.
  - Database queries extracting large amounts of financial data.

-**Impact Assessment**:

The attacker was able to access approximately 25,000 customer financial records, including credit card numbers, billing addresses, and transaction histories. The estimated financial impact is projected to be $150,000 due to breach notification costs, potential legal fees, and damage control measures.

- **Classification:**

The incident was classified as a High Severity due to the nature of the sensitive financial data involved and the scope of the breach.

3-Containment:

- Short-term Containment:

- The IRT immediately disabled the compromised account and blocked the attacker's IP address.

- The affected server was isolated from the network to prevent further unauthorized access.

- Firewall rules were updated to restrict access to the database server to internal IP addresses only.

- **Long-term Containment:**

 - Implemented multi-factor authentication (MFA) for all users accessing sensitive databases.

 - Encrypted all sensitive financial data at rest and in transit.

- Reviewed and updated all access control policies to ensure only authorized personnel have access to sensitive records.

4-Eradication:

Root Cause Analysis:

The root cause of the breach was determined to be the use of stolen credentials obtained via a phishing attack targeting one of the organization's finance department employees.

Remediation Actions:

- Phishing attack analysis was conducted, and the malicious emails were identified and removed from the email system.

 - Compromised accounts were reset, and affected systems were scanned for malware and unauthorized software.

 - A full audit of privileged accounts was performed, and unused or dormant accounts were disabled.

5-Recovery:

Restoration of Systems:

After ensuring that all systems were secure and no further unauthorized access was possible, the financial records server was restored from a secure backup. Access was gradually restored, prioritizing critical business functions.

Monitoring for Residual Activity:

Enhanced monitoring was implemented on the affected systems to detect any unusual activity or attempted breaches. Network traffic and database queries were continuously monitored to ensure no further exploitation occurred.

Verification of System Integrity:

Multiple scans were conducted to verify the integrity of the server, and no signs of lingering malicious activity were detected. The system was deemed secure after thorough verification.

6-Post-Incident Activity:

Lessons Learned:

The incident highlighted a gap in email security and employee awareness regarding phishing attacks. While technical controls were effective in detecting the breach, better user training could have prevented the compromise of credentials.

Improvements to Security Posture:

Enhanced Email Security: Deployed advanced email filtering solutions and implemented phishing detection tools.

User Awareness Training:

Conducted mandatory phishing awareness training for all employees, with regular phishing simulation exercises.

Policy Updates:

Revised access control policies to enforce the principle of least privilege, ensuring users have the minimum access required for their roles.

Incident Response Plan Review:

Updated the incident response plan to include more robust procedures for handling phishing attacks and credential theft.

Follow-Up Actions:

A follow-up security audit is scheduled to assess the implementation of these improvements and ensure ongoing compliance with security policies.

Conclusion:

The security breach was successfully contained, eradicated, and mitigated, following the NIST SP 800-61 guidelines. While the financial impact was significant, the swift response and remediation efforts helped minimize further damage and exposure. Enhanced security controls and training programs have been implemented to prevent similar incidents in the future.

Incident Status: Closed

Signed: Lassana Bakayoko

Title: Incident Handler

Date: 05-15- 2024

This report adheres to the NIST SP 800-61 guidelines and outlines a complete incident response cycle, from detection to post-incident activity, ensuring a thorough and professional approach to handling security incidents.