Investigation of a Data Breach

Date: June 10, 2024

Prepared by: Dinesh Kumar P

Table of Contents

1) Objective

2) Scenario Overview

3) Tasks and Findings

    3.1) Incident Analysis

    3.2) Forensic Analysis

    3.3) Data Recovery

    3.4) Regulatory Compliance

    3.5) Communication and Notification

    3.6) Post-Incident Review

4) Conclusion

Objective

The objective of this report is to investigate a data breach at ABC SecureBank, a fictional yet highly reputable financial institution. The investigation will cover how the breach occurred, the extent of the damage, forensic analysis, data recovery, regulatory compliance, communication strategies, and post-incident review. This scenario tests investigative and forensic skills in handling a data breach.

Scenario Overview

- **Company Name:** ABC SecureBank
- **Breach Discovery:** Discovered during a routine security audit
- **Scope of Breach:** Potential exposure of sensitive customer data, including names, account numbers, and transaction history

Tasks and Findings

1) Incident Analysis

Objective: Investigate how the breach occurred, determine the point of entry, the extent of the breach, and the timeframe during which it occurred.

Findings:

- **Point of Entry:** The breach was traced back to a phishing email that an employee unwittingly opened. This email contained a malicious link that installed malware on the employee's computer.

- **Extent of Breach:** The malware allowed attackers to gain access to the internal network. From there, they accessed a database containing customer account information.
- **Timeframe:** The breach was active for approximately two weeks before it was discovered during a routine security audit.

2) Forensic Analysis

Objective: Conduct digital forensics on the affected systems to identify any malware or suspicious activities. Collect evidence and logs.

Findings:

- **Malware Identified:** The malware identified was a Remote Access Trojan (RAT) known as "RAT-X". This RAT allowed the attackers to remotely control the infected computer and access the network.
- **Logs and Evidence:** Network logs showed unusual activity originating from the compromised employee's computer. Specifically, there were unauthorized database queries and data exfiltration attempts.
- **Additional Tools:** Attackers used legitimate administrative tools to move laterally within the network, making detection more difficult.

3) Data Recovery

Objective: Determine the type and quantity of customer data that was potentially exposed. Develop a strategy for data recovery and incident containment.

Findings:

- **Data Exposed:** Approximately 50,000 customer records, including names, account numbers, and transaction history, were potentially exposed.

- **Data Recovery Strategy:**
  - **Containment:** Isolate and remove the infected computer from the network.
  - **Backup Restoration:** Restore affected databases from backups taken before the breach.
  - **Enhanced Monitoring:** Implement enhanced network monitoring to detect any further suspicious activity.

4) Regulatory Compliance

Objective: Consider the legal and regulatory aspects of the data breach and ensure that the company complies with reporting requirements.

Findings:

- **Regulatory Requirements:** According to data protection regulations (e.g., GDPR, CCPA), the company must notify affected customers and regulatory bodies within a specified timeframe.

- **Compliance Steps:**
  - Notify relevant data protection authorities within 72 hours of breach discovery.
  - Inform affected customers about the breach, detailing the data compromised and steps taken to mitigate the impact.
  - Provide ongoing updates to regulatory bodies as new information becomes available.

5) Communication and Notification

Objective: Develop a communication plan for notifying affected customers, stakeholders, and regulatory bodies. Ensure that the communication is clear and in compliance with privacy laws.

Findings:

- **Communication Plan:**
  - **Customers:** Send notification emails and letters to affected customers. Include details about the breach, what information was exposed, and recommended actions (e.g., monitoring accounts for suspicious activity).
  - **Stakeholders:** Hold meetings with key stakeholders to explain the breach, its impact, and the steps being taken to address it.
  - **Regulatory Bodies:** Submit a detailed incident report to relevant authorities, including a timeline of the breach and remediation steps.

6) Post-Incident Review

Objective: After the breach has been contained and mitigated, conduct a thorough review to identify weaknesses in the security posture and provide recommendations for improving security.

Findings:

- **Security Weaknesses Identified:**
  - Lack of employee training on phishing threats.
  - Insufficient network segmentation, allowing attackers to move laterally.
  - Inadequate monitoring of network activity for suspicious behaviour.

- **Recommendations:**
  - **Training:** Implement regular cybersecurity training for all employees, focusing on phishing and social engineering threats.
  - **Network Segmentation:** Improve network segmentation to limit access to sensitive data.
  - **Monitoring:** Enhance network monitoring and implement intrusion detection systems (IDS) to identify and respond to suspicious activity more quickly.
  - **Regular Audits:** Conduct more frequent security audits and vulnerability assessments.

Conclusion

The investigation of the data breach at ABC SecureBank revealed significant vulnerabilities in the company's security posture. By following the outlined steps, including incident analysis, forensic investigation, data recovery, regulatory compliance, communication, and post-incident review, the company can address the breach effectively and strengthen its defences against future attacks. This comprehensive approach not only mitigates the current breach but also ensures long-term security improvements.