EXTION INFOTECH PROJECT-2

August 10, 2024

INVESTIGATION OF A DATA BREACH

COMPLETE REPORT

PREPARED BY:
LOKESHWARAN R
CYBERSECURITY INTERN
EXTION INFOTECH

INVESTIGATION OF A DATA BREACH:

ABOUT THE COMPANY:

ABC SecureBank is a leading financial institution committed to delivering secure, innovative, and customer-centric banking solutions. Established in [Year of Establishment], we have grown to become a trusted partner for millions of customers, providing a wide range of financial services tailored to meet diverse needs. With a steadfast commitment to security and technological advancement, ABC SecureBank is dedicated to offering reliable and forward-thinking banking experiences.

BASIC INFO ABOUT THE BREACH

Date of Discovery: August 9, 2024

Breach Discovery Method: Routine Security Audit

THE STEP BY STEP INVESTIGATION OF A DATA BREACH IN A ESTEEMED COMPANY COMPRISES BELOW:

- INCIDENT ANALYSIS
- FORENSIC ANALYSIS
- DATA RECOVERY
- REGULATORY COMPLIANCE
- COMMUNICATION AND NOTIFICATION
- POST-INCIDENT REVIEW

1.INCIDENT ANALYSIS

OBJECTIVES:

The goal of this section is to understand how the data breach occurred, pinpoint the entry method, assess the extent of the damage, and establish the timeline of events.

FINDINGS:

- **Point of Entry**:
  - Compromised Workstation: The breach originated from an employee's workstation, which was infected via a phishing email. Phishing emails are designed to trick recipients into opening malicious attachments or clicking harmful links.
  - Exploitation of Vulnerability: The phishing email contained an attachment that exploited a known vulnerability in the email client software. This allowed the attackers to install Remote Access Tools (RATs) on the workstation. RATs are a type of malware that enables attackers to remotely control the infected system.
  - Unauthorized Network Access: With RATs installed, attackers gained unauthorized access to the internal network, bypassing the initial security measures in place.
- **Extent of the Breach**:
  - Data Compromised: The attackers navigated the network and accessed the customer database, which included sensitive information such as customer names, account numbers, and transaction histories.
  - Scale of Impact: The breach affected approximately 5 million customer records. This scale indicates a significant impact on customer privacy and potential financial risk.
- **Timeframe:**
  - Initial Compromise: The attackers first compromised the workstation on July 25, 2024.
  - Ongoing Access: They maintained access to the network and continued their activities until the breach was discovered on August 9, 2024. During this period, they intermittently exfiltrated data, employing encryption to obscure their activities and avoid detection.

2.FORENSIC ANALYSIS

OBJECTIVES:

This section focuses on conducting digital forensics to identify malware, detect suspicious activities, and gather evidence.

FINDINGS:

- **Malware Detection**:
  - Presence of RATs and Keyloggers: Forensic analysis found several RATs and keyloggers on the infected workstation. RATs allowed remote control of the system, while keyloggers captured keystrokes, potentially exposing sensitive data such as passwords.
- **Suspicious Activities**:
  - Database Access: Logs showed that attackers accessed the database server outside of regular business hours. They executed large queries and exported customer data, indicating a deliberate and extensive effort to gather information.
  - Data Exfiltration: Unusual outbound traffic patterns were detected, suggesting that the attackers were transferring large volumes of data to external servers. The use of encryption further masked their activities, making detection more challenging.
- **Evidence Collection**:
  - Logs and Network Traffic: Evidence includes logs from the compromised systems and network traffic records that trace data transfers to suspicious external IP addresses.
  - Malware Samples: Samples of the malware found on the infected systems are being analyzed to understand their operation and to enhance detection measures.

3.DATA RECOVERY

OBJECTIVES:

Determine the nature and volume of the exposed data and establish a strategy for data recovery and containment.

FINDINGS & ACTIONS:

- **Type and Quantity of Data:**
  - Data Exposed: The breach involved sensitive customer data such as names, account numbers, and transaction histories. Approximately 5 million records were compromised.
- **Data Recovery Strategy:**
  - Isolation: Compromised systems were disconnected from the network to prevent further data leakage and limit the attackers' access.
  - Restoration: Efforts are underway to restore affected systems using clean backups. This ensures that systems are returned to a secure state and that any changes made by the attackers are reversed.
  - Enhancements: Enhanced monitoring tools and scanning mechanisms have been implemented to detect and respond to any further unauthorized activities.
- **Incident Containment:**
  - New Security Measures: Multi-factor authentication (MFA) has been introduced to add an extra layer of security. Network segmentation has also been implemented to limit access and contain potential future breaches.

4.REGULATORY COMPLIANCE

OBJECTIVES:

Ensure that all legal and regulatory obligations related to the breach are addressed and met.

FINDINGS & ACTIONS:

- **Regulatory Requirements:**
  - Compliance: The breach falls under regulations such as GDPR and CCPA, which require specific actions for data breaches involving personal information.
  - Notification: Regulatory bodies must be informed within 72 hours of discovering the breach. This involves preparing a comprehensive report detailing the breach's nature and scope.
- **Actions Taken:**
  - Regulatory Notification: Authorities have been notified as required. This includes providing detailed information about the breach and the affected data.
  - Documentation: Detailed records are being prepared to facilitate regulatory review and to ensure transparency and compliance

5.COMMUNICATION AND NOTIFICATION

OBJECTIVES:

Create a communication strategy to inform affected customers, stakeholders, and the public about the breach.

FINDINGS & ACTIONS:

- **Communication Plan:**
  - Customer Notification: Affected customers will receive notifications via email and postal mail. These communications will detail the breach, the type of exposed data, protective measures they can take, and available support services.
  - Stakeholder Communication: Business partners, investors, and other stakeholders will be briefed on the breach and the steps taken to address it. This helps maintain trust and keeps key parties informed.
  - Public Statement: A public statement will be issued to address media inquiries and provide transparency regarding the breach and the response efforts.
- **Compliance:** All communications will be crafted to comply with privacy laws and best practices, ensuring clarity and accuracy to effectively manage the situation and minimize harm.

6.POST-INCIDENT REVIEW

OBJECTIVES:

Evaluate the security posture, identify weaknesses, and recommend improvements to enhance future security.

FINDINGS & RECOMMENDATIONS:

- **Review Summary:**
  - Identified Weaknesses: The breach highlighted several security weaknesses, including inadequate employee training on phishing, outdated software patches, and insufficient network segmentation.
- **Recommendations:**
  - Employee Training: Implement regular training programs to improve employee awareness and response to phishing attempts and other cyber threats.
  - Security Upgrades: Ensure that all software is regularly updated and patched to address known vulnerabilities.
  - Network Security: Enhance network segmentation and access controls to better contain and manage potential breaches.
- **Implementation Plan:**
  - Short-Term Actions: Address immediate vulnerabilities and conduct a comprehensive security audit to identify and fix any other issues.
  - Long-Term Strategy: Develop a robust cybersecurity strategy, including advanced threat detection and response mechanisms, to improve overall security and resilience.

CONCLUSION:

The data breach at ABC SecureBank was a serious incident with significant implications for customer privacy and security. The response involved a detailed investigation, forensic analysis, and compliance with regulatory requirements. Going forward, the focus will be on strengthening security measures, improving employee training, and implementing comprehensive incident response protocols to prevent future breaches and restore trust.