INVESTIGATION OF A DATA BREACH

EXTION INFOTECH PROJECT - II

BY

SELVA ARASU R

TABLE OF CONTENTS

PROJECT REPORT: INVESTIGATION OF A DATA BREACH AT ABC SECUREBANK

1. Executive Summary

ABC SecureBank, one of the leading financial institutions, has fallen prey to data breaches in which sensitive information of its customers, including the names, account numbers, and transaction history, was exposed, opening up possible avenues for exploitation. The incident came to light during a routine security audit, thus raising serious concerns regarding the integrity of the security infrastructure of the bank. The report includes detailed analyses of the incident analysis, forensic examination, data recovery, regulatory compliance, communication, and post-incident review in respect to the breach. This will be important in gaining an in-depth understanding of the breach and recommending ways to improve the cybersecurity posture for ABC SecureBank.

2. Incident Analysis

2.1. Breach Discovery

The event was discovered on August 5, 2024 as part of the routine security audit conducted by ABC SecureBank's IT department. In the process, unusual network activity was noted and unauthorized access to a critical database identified, whereupon an investigation was immediately launched.

2.2. Point of Entry

This is connected to victim employees described in the phishing attack because the analysts found that the hackers had probably accessed the system via a phishing attack of ABC employees. One e-mail had arrived for multiple employees with a malicious attachment of which one had opened. It led to unknowingly executing the attached malware. The host company's email server weakness was exploited, and the hackers got through to the internal network.

2.3. Extent of Breach

The breach exposed a part of the internal network of ABC SecureBank, which was the customer account management system. This allowed access and exfiltration of sensitive data, which included customers' names, account numbers, and transaction histories.

From preliminary estimates, the number of customers whose data had been compromised is approximately 150,000.

2.4. Timeframe of the Breach

This could have been a breach within a duration of three weeks, commencing on July 15, 2024 to August 5, 2024, when the incident detection happened in the course of an audit. To this regard, attackers were able to attain persistent access to the network that gave them the chance to collect data over some time.

3. Forensic Analysis

3.1. Digital Forensics on Affected Systems

A deep forensic analysis of the affected systems was conducted, which included the compromised email server, network devices, and customer account management system.

Among others, some of the key findings included:

- Identification of the malware variant responsible for a phishing attack; this was identified as a variant of the well-known banking Trojan, designed for credential stealing and data exfiltration.
- Proof of lateral movement within the network—the attackers accessed several systems using the compromised employee credentials.
- Log files demonstrating unauthorized access to data and its exfiltration attempts.

3.2. Collection of Evidence

Forensic investigators have collected a good deal of evidence, including:

- Email logs exhibiting delivery and opening of the phishing email
- Network traffic logs showing suspicious data transfer
- System logs from compromised servers showing unauthorized access and execution of commands
- Copies of malware for further analysis and attribution

3.3. Malware Analysis

The malware was reverse-engineered to know its capabilities and origin. It was determined that the malware had been designed for:

- Keystroke capturing and screenshots
- Extracting stored passwords from browsers and e-mail clients
- Setting up a C2 channel to remotely control infected systems
- Exfiltration of data using encrypted channels to avoid detection

4. Recovery of Compromised Data

4.1. Determination of Exposed Data

The forensic team identified the types of data that were potentially exposed:

- Customer names
- Account numbers
- Transaction histories
- Internal financial reports and financial analyses

Most of the data was exposed to in the customer account management system, which the attackers gained unauthorized access to.

4.2. Quantification of Exposed Data

This involved close to 150,000 customers whose data could have been exfiltrated. The exact quantity of data was not known since exfiltration was performed in an advanced manner by the hackers.

4.3. Data Recovery and Incident Containment Strategy

The following steps were taken to contain and recover from the incident:

- Immediate isolation of compromised systems from the network
- Restoring the affected systems from clean backups
- Deploy additional security measures; enhanced monitoring for further malicious activity
- Patch Management to close vulnerabilities that have exploited by malware.

4.4 Data Restoration Plan

In order to provide both integrity and availability of customer data, a data restoration plan was prepared as follows:

- Integrity of the backups is checked before restoration.
- Long-term scanning of the restored systems for malware or unauthorized modifications.
- Multi-factor authentication and other access controls that would prevent the unauthorized access in the future.

5. Regulatory Compliance

5.1. Legal and Regulatory Requirements

Several legal and regulatory provisions would be applicable to ABC SecureBank on discovery of the breach:

- GDPR: ABC SecureBank should report the breach to the concerned DPA within 72 hours of its discovery since it is concerned with the possible exposure of EU customers' data.
- GLBA: ABC SecureBank being a financial institution was to adhere to the regulations created for protecting the information of customers, and also it should have reported the breaches with the FTC and other related agencies.
- State Breach Notification Laws: In light of this, ABC SecureBank shall respond to state breach notification laws and promptly notify the relevant customers.

5.2. Filing with Authorities

ABC SecureBank has written and filed all necessary reports with the appropriate authorities, including the following:

- A comprehensive incident report to the DPA by the provisions of GDPR.
- Informing the FTC as stipulated under GLBA.
- State-specific breach notification requirements.

5.3. Administrative Fines and Other Legal Implications

Non-compliance with these regulations will attract huge fines and other legal implications. ABC SecureBank has therefore taken all measures to make sure 100% compliance and avoid the associated legal risks.

6. Communication and Notification

6.1. Communication Plan

A communication plan was devised for the purpose of addressing the needs of the interested customers, stakeholders, and regulatory bodies. The plan comprises:

- Internal Information: The board of directors of the company and other executives are informed about the breach incident immediately, stating the nature of the breach and how it is to be addressed.
- External Information: by way of email, the website is updated with the relevant information and news releases issued clearly, proactively, and in a timely manner. The customers and the public are thus informed of the fact.

6.2 Customer Notification

ABC SecureBank e-mailed the following notification to the affected customers:

- Clearly, what had happened was explained.
- The kind of data that could have been exposed was specified.
- Measures the customers could take to protect themselves, such as checking their accounts for any suspicious activity and immediately reporting it
- Credit monitoring services offered by the bank

6.3. Communicating with Stakeholders

ABC SecureBank also contacted its stakeholders, which included shareholders and partners, to try and reassure them that measures were in place to fix the breach and to ensure that this would not happen again anytime soon.

6.4. Media and Public Relations

It published a news release to the public regarding the event and its measures to protect data security and transparency. Prepared for media enquiries and developed key messages for spokespeople.

7. Post-Incident Review

7.1. Security Posture Review

After the breach was contained, ABC SecureBank performed a thorough review of its security posture. Areas covered by this review included,

- Network Security: The segmentation of the network will be reviewed and enhanced; firewall configuration and intrusion detection and prevention systems will also be reviewed.
- Endpoint Security: Endpoint protection enhanced by threat detection, adequate software updating, and user training in phishing awareness in the field.
- Access Control: Stringent application of access controls, with the implementation of RBAC and mandatory MFA for all employees.
- Patch Management: Enhancement of the patch management process in the update timeline and in vulnerability management.

7.2 Incident Response Plan Update

It updated the incident response plan with lessons learned from the breach:

- Improved detection capabilities, response against phishing attacks.
- Closer coordination between IT, legal, and communications teams in case of an incident.
- Regular incident response drills and tabletop exercises on the training of behaviors to be expected in case of a potential future breach.

7.3. Recommendations for Security Improvement

The following, based on the findings, were recommended to improve ABC SecureBank's security:

- Employee Training and Awareness: Regular employee training in cybersecurity awareness, with particular focus on phishing prevention and best practices for handling sensitive information.
- Advanced Threat Detection: Implementation of advanced threat detection, including SIEM and EDR tools.
- Zero Trust: Implement a Zero Trust policy to lower the odds of unauthorized access.
- Third-party security testing: Involving third-party security experts for periodic evaluation and penetration testing.

7.4. Continuous Monitoring and Improvement

ABC SecureBank is committed to continuous monitoring and improving its measures taken in security by conducting regular audits, searching for vulnerabilities in the network, and updating the security protocols against the threats emerging.

8. Conclusion

The data breach at ABC SecureBank exposed several critical vulnerabilities in the company's security infrastructure. Although the immediate threat has been eliminated, this event will give the organization a chance to start being serious about its information security policies starting from the top. It is through investigations and forensic analysis, with corresponding recovery efforts and compliance with regulatory provisions, that have made the process of dealing with this breach possible. In reinforcing its readiness to further attacks, ABC SecureBank should implement the security enhancements suggested above to better shield sensitive customer data.

This report gives an elaborately detailed framework of the processes involved in investigating and responding to data breaches at a financial institution. It lays emphasis on an all-inclusive, coordinated approach toward cybersecurity.