Project Report: Investigation of a Data Breach ABC Secure Bank

Submitted by

Archit Yadav

CYBER SECURITY INTERNSHIP AT

EXTION INFOTECH

2024

Table of Contents

About Me

My name is Archit Yadav. I am currently pursuing a Bachelor of Technology [B.Tech] in Electronics and Communication Engineering at Pranveer Singh Institute of Technology. During my academic journey, I have developed a strong foundation in programming languages such as C++ and Python and excelled in core subjects related to my field. I hold a design patent for a project based on Free Space Optics (FSO) and won a cash prize of ₹10,000 at my college's Tech-Xpo event. Additionally, I have completed research in wireless communication on the topic "Asymptotic Analysis of Kappa-Mu Shadowed Model with Application to Error Probability," verified through MATLAB simulations, and the research will be published soon.

I am also deeply passionate about Ethical Hacking and Cybersecurity. My interest began in class 10, where I started exploring tools like Kali Linux and Termux on mobile devices.

How to Reach me:-

Linkden:- https://www.linkedin.com/in/archit-yadav-42491321a

Gmail:- archityadav0007@gmail.com

Instagram:- https://www.instagram.com/yaduvanshi_archit

Leetcode:- **https://leetcode.com/u/ArchitYadav**

Objective

This report provides an in-depth investigation into a data breach incident that occurred at ABC Secure Bank, a well-regarded and trusted financial institution known for its robust security measures. The report comprehensively examines various aspects of the breach, including the specific methods used by the attackers to compromise the system, the overall extent of the damage inflicted on the bank's operations and reputation, and the steps taken to conduct a detailed forensic analysis. Additionally, it explores the data recovery efforts employed to restore lost or compromised information, the institution's adherence to regulatory compliance requirements, and the communication strategies implemented to address stakeholders and the public effectively during the crisis. Finally, the report evaluates the post-incident response and assessment processes to determine lessons learned and improvements needed in the bank’s cybersecurity defences. This case serves as an assessment of critical forensic and investigative skills essential for effectively managing and mitigating the consequences of a significant data breach.

Scenario Overview

Consider a situation where a data breach has occurred at a prominent and well-known website. The task at hand is to thoroughly investigate the breach, evaluate its impact, and determine the appropriate steps for resolution. Although the website's name is fictitious, this scenario is designed to challenge and assess investigative and forensic skills in managing such incidents.

Details of the Incident:

- Company Name: The affected organization is ABC Secure Bank, a prestigious and highly trusted financial institution known for its commitment to security and customer trust.
- Breach Discovery: The breach came to light during a routine security audit conducted as part of the organization's proactive measures. Preliminary findings indicate that sensitive customer data may have been compromised.
- Scope of the Breach: The breach potentially involves the exposure of critical customer information, including personal details such as names, account numbers, and transaction histories. This has raised significant concerns about data privacy and security.

The investigation aims to identify the root cause of the breach, assess the extent of the damage, and recommend strategies to mitigate further risks while ensuring compliance with regulatory standards.

Tasks and Findings

1. Incident Analysis

1.1 Overview of the Breach

ABC Secure Bank, a well-established and highly respected financial institution, recently experienced a substantial data breach that was uncovered during a routine security audit. The breach is believed to have exposed critical customer information, including personal details such as names, account numbers, and transaction histories. Due to the sensitive nature of the compromised data, the incident poses severe threats to customer privacy, the organization's reputation, and its compliance with legal and regulatory requirements.

1.2 Identification of the Breach

The breach was identified during a routine security audit, an essential element of ABC Secure Bank's comprehensive cybersecurity strategy. During the audit, anomalies in the access logs of customer databases were detected, suggesting unauthorized access to sensitive data. A subsequent detailed investigation revealed that the breach may have been ongoing for a prolonged period before detection, raising serious concerns about the effectiveness of the bank's monitoring and alerting systems.

1.3 Initial Response

Immediately after discovering the breach, ABC Secure Bank activated its incident response plan to mitigate the impact of the attack. The bank assembled its incident response team, which swiftly worked to contain the breach and assess the extent of the damage. The team also began communicating with key stakeholders, including affected customers, regulatory authorities, and law enforcement agencies, to ensure transparency and compliance with reporting requirements.

1.4 Point of Entry

The investigation into the breach focused on identifying how the attackers gained access to the bank's network. Forensic analysis of firewall logs, Intrusion

Detection System (IDS) alerts, and server access logs revealed that the breach originated from a phishing attack targeting ABC Secure Bank employees. The phishing emails were skillfully designed to resemble legitimate communications from internal departments, persuading recipients to click on malicious links. These links redirected users to a compromised website that deployed malware onto their systems. The malware allowed attackers to gain remote access to the affected machines, escalate user privileges, and ultimately infiltrate the bank's internal network.

1.5 Attack Vector

Once inside ABC Secure Bank's internal network, the attackers exploited a vulnerability in the bank's web application. This vulnerability, caused by unpatched and outdated software, had a known fix available, but the necessary updates had not been implemented. The attackers employed SQL injection (SQLi) techniques to manipulate the application's database queries. By inserting malicious SQL commands into input fields, the attackers gained unauthorized access to sensitive customer data stored in the bank's databases.

1.6 Extent of the Breach

The forensic investigation determined that the attackers accessed multiple critical databases containing sensitive customer information. The compromised data included:

- Customer names
- Account numbers
- Transaction histories

The attackers remained undetected within the system for approximately three months, during which they systematically exfiltrated significant volumes of customer data. Evidence suggests that the stolen information was likely sold on dark web marketplaces or utilized for fraudulent purposes, exacerbating the impact of the breach on customers and the institution.

This breach underscores the critical need for rigorous cybersecurity practices, timely software updates, and robust employee training to mitigate the risk of future incidents.

2. Forensic Analysis

2.1 Overview

The primary objective of the forensic analysis was to systematically collect and analyze evidence related to the data breach. This included identifying any malware present on the affected systems, uncovering suspicious activities, and tracing the steps taken by the attackers.

2.2 Evidence Collection

To ensure the integrity and preservation of evidence, the forensic team began by creating forensic images of the compromised systems. These images served as exact replicas of the hard drives at the time of the breach, capturing all data, including deleted files and hidden information. Advanced forensic tools were then utilized to scrutinize the images, uncovering traces of the attackers' activities and identifying artifacts left behind.

2.3 Malware Analysis

A detailed analysis of the forensic images led to the identification of the malware used in the attack. The malware was a sophisticated Remote Access Trojan (RAT), designed to provide attackers with full remote control of the infected systems. This RAT was specifically engineered to bypass traditional antivirus detection mechanisms, making it exceptionally difficult to identify through routine security measures.

The investigation revealed that the RAT communicated with a command-and-control (C2) server located overseas. Through this C2 server, the attackers issued instructions to the compromised systems, enabling them to exfiltrate data, escalate user privileges, and move laterally within the bank's internal network.

2.4 Log Analysis

Log analysis played a pivotal role in reconstructing the sequence of events during the breach. The forensic team meticulously examined firewall logs, server access logs, and Intrusion Detection System (IDS) alerts. The key findings included:

- Initial Access: The attackers gained entry through a phishing email targeting employees of ABC Secure Bank.
- Lateral Movement: Once inside, the attackers used the compromised systems to navigate the internal network and elevate their privileges.
- Exploitation: A known vulnerability in the bank's web application was exploited to access the customer database.
- Data Exfiltration: Customer data was exfiltrated consistently over a span of three months.

Additionally, the logs revealed attempts by the attackers to conceal their actions by deleting specific log entries. Despite these efforts, the forensic team successfully recovered the deleted logs using specialized recovery tools, providing a more comprehensive picture of the breach.

2.5 Timeline of the Breach

The following timeline was established based on the forensic analysis:

- Day 1: Phishing emails were sent to employees of ABC Secure Bank.
- Day 2: An employee clicked on a malicious link, resulting in the installation of a Remote Access Trojan (RAT) on their system.
- Day 5: The attackers gained access to the internal network and escalated their privileges.
- Day 7: The attackers identified and exploited a vulnerability in the web application, granting them access to the database.
- Day 10 to Month 3: Customer data was systematically exfiltrated from the database over a three-month period.
- Month 4: The breach was finally detected during a routine security audit.

This timeline highlights the prolonged nature of the breach and underscores the critical need for enhanced monitoring and rapid response measures to mitigate such threats in the future.

3. Data Recovery

3.1 Overview

The data recovery phase aimed to assess the extent of the data exposure, identify the type and quantity of customer information compromised, and develop a comprehensive strategy to recover from the incident while containing its impact.

3.2 Identification of Exposed Data

Through forensic analysis, the investigation revealed the types of customer data compromised during the breach:

- **Customer Names**
- **Account Numbers**
- **Transaction Histories**

The scale of the exposure was significant, involving millions of customer records. The attackers focused on high-value data that could facilitate fraudulent activities such as identity theft, unauthorized transactions, and other financial crimes.

3.3 Data Recovery Strategy

The data recovery strategy addressed immediate containment, communication, customer support, and compliance with legal and regulatory requirements.

3.3.1 Containment

To halt the breach and minimize further damage, the following actions were taken:

- **Isolating Compromised Systems:** Disconnecting affected systems from the network to prevent further data exfiltration.

- **Patching Vulnerabilities:** Applying fixes to the exploited web application to close the attack vector.
- **Network Scanning:** Conducting thorough scans to detect and remove additional malware or suspicious activity.
- **Enhanced Security Measures:** Introducing multi-factor authentication (MFA) and advanced monitoring tools to prevent future incidents.

3.3.2 Communication

Clear and transparent communication was essential for managing the breach. ABC Secure Bank adopted the following measures:

- **Customer Notifications:** Informing affected customers about the breach, providing details on the compromised data, and offering guidance on protecting their accounts.
- **Law Enforcement Collaboration:** Engaging law enforcement agencies to assist in tracking down the attackers and investigating the breach.
- **Regulatory Reporting:** Coordinating with regulatory bodies to meet compliance obligations and avoid penalties.

3.3.3 Customer Support

To mitigate the impact on affected customers, the bank established a dedicated customer support team that provided:

- **Account Monitoring:** Assistance in monitoring customer accounts for unusual or suspicious activity.
- **Identity Theft Protection:** Services like credit monitoring, fraud alerts, and guidance on identity theft prevention.
- **Compensation:** Reimbursement for any unauthorized transactions resulting from the breach.

3.3.4 Legal and Regulatory Compliance

The breach raised potential legal and regulatory challenges. The recovery strategy included:

- **Legal Review:** Assessing liability and preparing for potential lawsuits.
- **Notification Laws Compliance:** Ensuring adherence to data breach notification requirements, such as GDPR and CCPA.
- **Regulatory Collaboration:** Working with legal counsel to prepare for investigations and potential penalties.

3.4 Long-Term Mitigation

To prevent future breaches, ABC Secure Bank developed a robust long-term mitigation plan, which included:

- **Employee Security Training:** Enhancing employee awareness to defend against phishing and social engineering attacks.
- **Frequent Security Audits:** Increasing the frequency and depth of security audits to identify vulnerabilities promptly.
- **Advanced Threat Detection Tools:** Deploying advanced technologies like Security Information and Event Management (SIEM) and Endpoint Detection and Response (EDR) to identify and mitigate threats in real time.
- **Third-Party Risk Management:** Strengthening policies to ensure that vendors and partners comply with the bank's security standards.
- **Data Encryption:** Expanding encryption for sensitive data, both at rest and in transit, to safeguard against unauthorized access.

By combining immediate containment measures with a strategic, long-term focus on cybersecurity improvements, ABC Secure Bank aimed to rebuild customer trust, comply with legal obligations, and fortify its defenses against future cyber threats.

Communication and Notification

Objective

Develop a comprehensive communication plan to inform affected customers, stakeholders, and regulatory bodies about the data breach, ensuring transparency, clarity, and adherence to applicable privacy laws.

Communication Plan

Customers

a. Notification Methods:
   Send notifications via email and physical letters to all affected customers.

b. Content of Communication:
   Provide a detailed explanation of the breach, including:

    a. A summary of the incident.

    b. Information about the data that was exposed.

    c. Recommended actions customers should take, such as monitoring their accounts, enabling fraud alerts, and securing their personal information.

Stakeholders

a. Engagement Strategy:
   Organize meetings with key stakeholders, including executives, board members, and major investors.

b. Discussion Points:

    a. Outline the breach's impact on the organization.

    b. Highlight the immediate actions taken to contain the breach.

    c. Present the long-term measures being implemented to prevent future incidents.

Regulatory Bodies

a. Compliance Reporting:
   Submit a detailed incident report to relevant regulatory authorities, ensuring full compliance with data breach notification laws.

b. Report Content:

    a. A comprehensive timeline of the breach.

    b. Steps taken to contain and remediate the incident.

    c. Measures implemented to strengthen security and prevent recurrence.

This communication plan aims to build trust with customers, maintain transparency with stakeholders, and ensure adherence to legal and regulatory requirements.

Post-Incident Review

Objective

Conduct a comprehensive review to identify security vulnerabilities and provide recommendations for strengthening defenses after the breach has been contained and mitigated.

Security Weaknesses Identified

1. **Insufficient Employee Training:** Employees lacked awareness and preparedness to recognize and respond to phishing attacks.
2. **Inadequate Network Segmentation:** Poor segmentation allowed attackers to move laterally across the network, increasing the extent of the breach.
3. **Limited Monitoring Capabilities:** Network activity was not adequately monitored, delaying the detection of suspicious behavior.

Recommendations for Enhancements

1. Employee Training

- Conduct regular, organization-wide cybersecurity training sessions.
- Focus training programs on recognizing phishing attempts and social engineering tactics.
- Simulate phishing exercises to assess and improve employee readiness.

2. Network Segmentation

- Strengthen network segmentation to limit access to sensitive systems and data.
- Establish strict access controls based on roles and responsibilities.
- Regularly review and update access permissions to ensure minimal privilege requirements.

3. Enhanced Monitoring

- Deploy advanced monitoring tools, such as Intrusion Detection Systems (IDS) and Security Information and Event Management (SIEM) solutions, to track and analyze network activity in real-time.
- Implement automated alerts for unusual or unauthorized activity to enable a rapid response.
- Establish a dedicated team to oversee continuous monitoring and threat detection.

4. Regular Audits

- Increase the frequency of security audits to proactively identify and address vulnerabilities.
- Conduct regular vulnerability assessments and penetration testing to evaluate system defenses.
- Incorporate third-party audits to ensure unbiased evaluation and industry-standard compliance.

By addressing these weaknesses and implementing the recommended measures, the organization can significantly improve its security posture and reduce the likelihood of future breaches.

Conclusion

The data breach at ABC Secure Bank underscores the critical need for a robust and comprehensive cybersecurity strategy. Such a strategy must integrate proactive incident response measures, detailed forensic analysis capabilities, and effective data recovery processes. This breach was initiated by a sophisticated phishing attack, which was further exacerbated by the exploitation of a known vulnerability in the bank's web application.

The forensic investigation revealed key details about the attackers' activities, enabling the organization to understand the scope of the breach and its impact. The data recovery plan prioritized immediate containment, transparent communication with stakeholders, and the development of long-term mitigation strategies to prevent future incidents.

This incident highlights several key lessons, including the importance of regular security audits, employee training to recognize and mitigate phishing threats, and the implementation of advanced threat detection technologies. By adopting these practices, ABC Secure Bank can strengthen its defenses, safeguard its customers' sensitive data, and uphold its reputation as a trusted and reliable financial institution.