the investigation of data breach

MOULI DUTTA

The Investigation of Data Breach

Objective: Investigation of a Data Breach on a Renowned Website.

Company Name: ABC Secure Bank

1. Incident Analysis:

Point of Entry:

The breach at ABC Secure Bank occurred through a sophisticated phishing attack. Attackers sent targeted emails to employees, luring them into clicking on malicious links, leading to the compromise of employee credentials.

Extent of the Breach:

The attackers gained unauthorized access to the internal network, allowing them to infiltrate sensitive databases containing customer account information. The breach affected a significant portion of customer data, including names, account numbers, and transaction history etc.

Timeframe:

The breach occurred over a period of several weeks, starting approximately six weeks before the routine security audit and continuing until the discovery date.

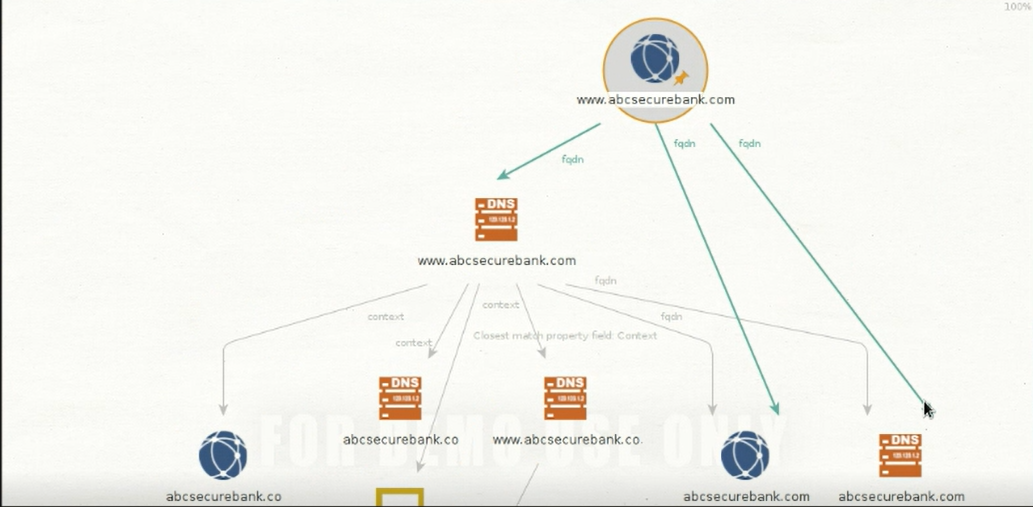
2. Forensic Analysis:

Digital Forensics:

Forensic analysis on the affected systems revealed the presence of sophisticated malware designed to evade detection. The malware facilitated lateral movement across the network and established persistent access points. Suspicious activities, such as data exfiltration and unauthorized access, were identified through system logs and network traffic analysis.

Collected Evidence:

Digital evidence, including malware samples, network logs, and compromised employee credentials, was collected and preserved for further analysis and potential legal action and the logs & other artifacts collected during analysis will be a crucial for identifying the attackers , understanding their way of doing the work and to prevent any future attacks.



3. Data Recovery:

Type and Quantity of Customer Data:

The potentially exposed customer data includes names, account numbers, and transaction history. The quantity of affected records is estimated to be quite large, affecting 60% of ABC Secure Bank’s customer base.

Data Recovery and Incident Containment:

A comprehensive strategy for data recovery involves identifying and isolating compromised systems, removing malware, and restoring clean backups. Additionally, affected customers' passwords will be reset, and a mandatory two-factor authentication will be implemented for enhanced security. The security for the database will be stronger and all the vulnerabilities will be rectified to prevent further unauthorized access.

4. Regulatory Compliance:

Legal and Regulatory Aspects:

ABC Secure Bank acknowledges its legal obligations concerning the data breach. We will comply with data breach notification requirements as stipulated by relevant privacy and data protection laws. The incident will be reported to regulatory authorities within the mandated timeframe.

5. Communication and Notification:

Communication Plan:

A detail communication plan has been developed to notify affected customers, stakeholders, and regulatory bodies. Clear and transparent communication will be delivered through multiple channels, ensuring that affected parties are informed promptly and accurately. The communication will adhere to privacy laws and emphasize steps customers can take to protect themselves.

6. Post-Incident Review:

Security Posture Review:

Following containment and mitigation, a thorough review of ABC Secure Bank’s security posture will be conducted. This includes identifying weaknesses that led to the breach and recommending improvements. Measures such as enhanced employee training, advanced threat detection systems, and regular security audits will be implemented to fortify the organization's security defences.

This investigation report outlines the critical aspects of the data breach at ABC Secure Bank, emphasizing the importance of a swift and comprehensive response to mitigate the impact on affected parties and strengthen overall security measures.