DATA BREACH INVESTIGATION REPORT FOR ABC SecureBank

Company: extion infotech investigator: aliyu egwa usman date:02/12/2024

CONTENTS:

- **EXECUTIVE SUMMARY**

1. OVERVIEW OF DATA BREACH

   {Scope and impact of the breach}: ABC SecureBankk data breach was a significant cybersecurity incident that exposed sensitive customer information such as social security numbers, account balances, transaction records and personal identifiable (PII). allowing the attackers to compromise sensitive customer data. The breach was initiated through a phishing attack that compromised employee credentials.

2. TIMELINE OF THE BREACH

   the breach was identified when unusual activity was detected in the system. In the process of investigation, it was discovered that the breach occurred one week to its detection. This was determined through a thorough investigation that included analyzing network traffic, system logs, and memory dumps. The breach and mitigation for further damage was initiated instantly as incident response protocol for which the ABC SecureBank used to contain.

- INCIDENT ANALYSIS

(FINDINGS)

CONCLUSION

The investigation on ABC SecureBank uncovered critical weaknesses on company`s security posture and highlighted several key findings and action taken such as:

- ⇨ Root cause
- ⇨ Extent of Breach
- ⇨ Response and Recovery
- ⇨ Regulatory Compliance
- ⇨ Security enhancement
- ⇨ Customer support

1. POINT OF ENTRY

ABC SecureBank data breach was identified as phishing attack. attackers sent deceptive emails to employee, tricking one of them into providing login credentials were then used to gain unauthorized access to the internal network, allowing the attackers to compromise sensitive customer data.

2. EXTENT OF THE BREACH

Attackers were able to gain access to the internal network and compromise sensitive data such account name, account numbers and transaction history.

- FORENSIC ANALYSIS

(FINDINGS}

1. MALWARE DISCOVERED

Malware discovered in ABC SecureBank is a sophisticated strain of malware designed to exfiltrate data and evade detection. This malware was identified during the forensic analysis of affected system and was found to be responsible for the unauthorized access and data theft. The malware discovered was a KEYLOGGERS that record keystroke to capture sensitive information like credit card details and REMOTE ACCESS TROJAN (RAT) to remote control over infected systems, allowing them to steal data and perform other malicious activities.

2. NETWORK LOGS AND EVIDENCE

Unusual network traffic: analysis of network traffic using tool like wireshark shows large data transfers and connection to unfamiliar IP addresses during the breach period.
Unauthorized access attempts: system logs analyzed with Splunk Enterprise indicated multiple unauthorized access attempts and unusual logins patterns from various IP addresses.
Malware activity: Memory analysis using volatility uncovered hidden processes and malware, which were later identified as sophisticated strains designed to exfiltrate data and evade detection.
Data exfiltration: Evidence of data being transferred to external servers was found, confirming the attacker intent to steal sensitive information.

3. ADDITIONAL TOOLS

Attackers use CREDENTIAL STUFFING tools to automate the process of trying stolen credentials on different systems to gain broader access and PHISHING KITS to create convincing fake emails and websites to trick employees into providing their login credentials.

- DATA RECOVERY

  (FINDINGS)

  1. DATA EXPOSED
     The data exposed in the ABC SecureBank includes sensitive customer information such as:
     -Social Security Numbers
     -Account balances
     -Transaction record
     -Personal identifiable information (PII), includes names, addresses, and phone numbers. This exposure put customers at risk of identity theft and financial fraud.

  2. DATA RECOVERY PROCESS
     -**System isolation:** the affected systems were isolated to prevent further unauthorized access.
     -**Data restoration:** restore affected data from backups taken before the breach occurrence.
     -**containment:** isolate and remove the infected systems from the network.

- REGULATORY COMPLIANCE

  (FINDINGS)
  =>The regulatory compliance and steps for ABC SecureBank following the data breach involve adhering to data protection laws and implementing measures to mitigate the impact of the breach.

  -**NOTIFICATION:** The company must notify affected customers and relevant authorities about the breach, as required by data protection regulations.
  -**Data protection laws:** compliance with local data protection laws, such as the Nigerian Data Protection Act 2023, which mandates organization to protect personal data report breaches.
  -**Transparency:** providing clear and timely communication to customers about the extent of the breach and the steps being taken to address it.

- COMMUNICATION AND NOTIFICATION PLAN

  (FINDINGS)

  1. IMMEDIATE NOTIFICATION
     informing affected customers and relevant authorities about the breach as soon as it is discovered.

  2. CLEAR AND TRANSPARENT COMMUNICATION
     Providing detailed information about the nature and extent of the breach, including what data was compromised and how it might affect customers.

  3. REGULAR UODATES
     Offering ongoing updates as the new information progresses and new information becomes available.

  4. CUSTOMER SUPPORT
     Establishing a dedicated support line for affected customers to address their concern and provide guidance on protecting their personal information.

- POST-INCIDENT REVIEW

  (FINDINGS)

  1. SECURITY WEAKNESSES IDENTIFIED
     -**Lack of employee training on phishing threats**.
     -**Lack of network segmentation.**
     -Lack of monitoring network for suspicious activity.
  2. RECOMMENDATIONS
     -**Network segmentation:** Enhance network segmentation to restrict access to sensitive information.
     -**Training/awareness:** implement regular cyber security training that focus on social engineering threat and phishing.
     -**Security enhancement:** Proposing enhancement to security measures, such as implementing stronger access control and regular audit.

Overall, the investigation concluded that while the breach was significant, ABC SecureBank took appropriate steps to address the issue, mitigate its impact, and prevent future occurrences.