Case Study: Cyber Attack on a Financial Institution

Introduction

ABC Bank, a mid-sized financial institution, suffered a significant cybersecurity breach. Attackers exploited vulnerabilities in the bank's network, stealing customer data, including financial records, account credentials, and personal information. This case study will explore the types of security attacks ABC Bank encountered, the security services necessary to counteract them, and the mechanisms used for prevention and mitigation.

Security Attacks

The attackers used a combination of the following methods:

1. **Phishing Attack**
   - Attackers sent fraudulent emails to employees, posing as IT support. When employees clicked on links or provided sensitive information, attackers gained unauthorized access to internal systems.
2. **SQL Injection**
   - The attackers exploited weaknesses in the bank's website database by injecting malicious SQL code through input fields, gaining access to the database and extracting sensitive customer information.
3. **Denial of Service (DoS) Attack**
   - A separate attack flooded the bank's website and servers with traffic, leading to downtime and preventing customers from accessing online services. The DoS attack distracted the IT team while data exfiltration occurred.
4. **Man-in-the-Middle (MITM) Attack**
   - The attackers intercepted communications between the bank's web applications and its users, enabling them to eavesdrop on transactions and capture login credentials.

Security Services

To safeguard against these types of attacks, ABC Bank implemented the following security services:

1. **Authentication**
   - Ensures that only legitimate users can access the bank's systems, including strong user authentication and multi-factor authentication (MFA) for employees and customers.

2. **Confidentiality**
    - Protects sensitive data by encrypting all customer and transaction information, making it unreadable without proper decryption keys.
3. **Integrity**
    - Verifies that data has not been altered by unauthorized parties, utilizing hash functions and digital signatures to confirm data accuracy and authenticity.
4. **Non-repudiation**
    - Ensures that transaction details and actions are traceable, preventing either party (bank or customer) from denying their actions. This service is crucial for resolving disputes and tracking accountability.
5. **Access Control**
    - Restricts access to resources based on users' roles and responsibilities, limiting the potential for insider attacks or accidental breaches.

Security Mechanisms

To put these security services into action, the bank adopted several security mechanisms:

1. **Firewalls and Intrusion Detection Systems (IDS)**
    - Used to monitor incoming and outgoing traffic, blocking unauthorized access and identifying suspicious activities in real time.
2. **Encryption**
    - ABC Bank employed strong encryption (e.g., AES-256) for both data at rest and in transit to protect customer information. Public Key Infrastructure (PKI) and SSL/TLS were used to secure web transactions.
3. **Anti-Phishing Software and Training**
    - The bank implemented email filters to detect phishing attempts and conducted employee training on identifying phishing attacks.
4. **Database Security Measures**
    - To counter SQL injection attacks, the bank adopted prepared statements and parameterized queries, which prevent unauthorized database access.
5. **Incident Response Plan**
    - The bank set up an incident response plan, including regular backups, a disaster recovery strategy, and an established protocol for investigating breaches.
6. **VPN and Secure Socket Layer (SSL)/Transport Layer Security (TLS)**

- VPNs and SSL/TLS were used to secure data in transit, particularly for remote employees accessing the bank's network, to protect against MITM attacks.

7. **Access Control Lists (ACLs) and Role-Based Access Control (RBAC)**
   - Implemented to ensure that employees only have access to the data necessary for their roles, reducing the risk of internal attacks.

THANK YOU

By

2310030018-Balivada Sai Yashwant