Investigation of a Data Breach at ABC SecureBank

Cyber Security Internship Task 2 | Extion Infotech

Executive Summary

This report details the comprehensive investigation of a data breach discovered at ABC SecureBank, a highly reputable financial institution. The breach was identified during a routine security audit and potentially exposed sensitive customer data including names, account numbers, and transaction histories. This document outlines the investigative methodology, findings, remediation actions, and recommendations for preventing future incidents.

1. Incident Analysis

Point of Entry

After thorough investigation, the breach was determined to originate from a vulnerable web application server hosting the customer portal. The attackers exploited an unpatched SQL injection vulnerability in the login form, which allowed them to bypass authentication controls and gain unauthorized access to the backend database.

Timeline of Events

- **Day 1 (Initial Compromise)**: Attackers discovered and exploited the SQL injection vulnerability
- **Days 1-3**: Attackers established persistence by creating backdoor accounts and deploying web shells
- **Days 4-14**: Lateral movement occurred throughout the network, accessing multiple database servers
- **Days 15-30**: Data exfiltration occurred during low-traffic hours to avoid detection
- **Day 31**: Suspicious database query patterns triggered alerts during routine security audit
- **Day 32**: Incident response team initiated investigation

Attack Methods

The attackers used a multi-stage approach:

1. Initial exploitation via SQL injection
2. Privilege escalation to admin user by leveraging unsecured service accounts
3. Lateral movement through the network using stolen credentials
4. Data harvesting and exfiltration via encrypted channels to external servers

2. Forensic Analysis

Digital Evidence Collection

- Web server logs revealed suspicious query patterns containing SQL injection attempts
- Network traffic logs showed unusual outbound connections to unknown IP addresses
- Database audit logs indicated unauthorized queries executed outside normal business hours
- Memory dumps from compromised servers contained traces of malicious code

Malware Analysis

A custom data exfiltration tool was identified on the compromised servers with the following characteristics:

- Written in Python and compiled to an executable
- Used encrypted communications (TLS 1.3) to mask data transfer
- Implemented timing delays to evade detection
- Disguised itself as a legitimate system process ("svchost32.exe")

Log Analysis

Examination of system and application logs revealed:

- Failed login attempts from various IP addresses originating from Eastern Europe
- Successful privilege escalation events using compromised credentials
- Creation of unauthorized admin accounts
- Database queries extracting large volumes of customer data

3. Data Recovery & Breach Scope

Affected Systems

- Primary customer database server
- Web application servers (2)
- Internal authentication server
- Backup server (accessed but data not modified)

Compromised Data

Based on analysis of exfiltrated data packets and database query logs:

- Approximately 75,000 customer records were potentially exposed
- Exposed data includes:

    - Customer names, addresses, phone numbers
    - Account numbers and transaction histories
    - Partial credit card information (last 4 digits)
    - Account balances
- No passwords or complete payment card details were compromised

Recovery Actions

- Identified and preserved all affected data for forensic analysis
- Restored critical systems from clean backups predating the compromise
- Implemented database integrity checks to verify no data tampering occurred
- Established enhanced monitoring for any signs of compromised data being used

4. Regulatory Compliance

Applicable Regulations

- Financial Data Protection Act (FDPA)
- General Data Protection Regulation (GDPR) for European customers
- Payment Card Industry Data Security Standard (PCI DSS)
- State-specific data breach notification laws

Reporting Requirements

- Financial regulatory authorities: Report required within 72 hours of confirmation
- Affected individuals: Notification required within 30 days of discovery
- Law enforcement: Report filed with FBI Cyber Division and Internet Crime Complaint Center (IC3)
- Credit bureaus: Notification required due to potential identity theft risks

Documentation

- Detailed incident logs preserved in tamper-evident storage
- Chain of custody maintained for all digital evidence
- Comprehensive timeline of breach and response activities documented
- All communications with regulatory bodies archived for compliance verification

5. Communication & Notification Plan

Customer Communication Strategy

- Direct email notification to all affected customers
- Physical mail for customers with sensitive data exposure
- Dedicated secure website with incident information and FAQs
- 24/7 call center established for customer inquiries

Sample Customer Notification

```
IMPORTANT: Notice of Data Security Incident

Dear [Customer Name],

We are writing to inform you about a data security incident at ABC SecureBank that may have affected your personal information. On [Date], we discovered unauthorized access to certain systems containing customer information.

What information was involved?
The potentially affected information includes your name, account number, and transaction history from [date range]. Your password, full credit card details, and social security number were NOT compromised.

What we are doing:
We have secured our systems, engaged cybersecurity experts, and reported this incident to law enforcement and regulatory authorities. As a precaution, we are offering 24 months of free credit monitoring and identity protection services.

What you can do:
- Enroll in the complimentary credit monitoring service using code: [UNIQUE CODE]
- Monitor your account statements and credit reports for suspicious activity
- Change your online banking password and security questions

For more information:
Please visit www.abcsecurebank.com/securitynotice or call our dedicated assistance line at (800) XXX-XXXX.

We sincerely apologize for this incident and are committed to protecting your information.

Sincerely,
[CEO Name]
Chief Executive Officer
ABC SecureBank
```

Stakeholder Communications

- Board of Directors: Detailed briefing with financial and reputational impact assessment
- Employees: Security awareness training and communication guidelines
- Partners/Vendors: Notification for those with interconnected systems
- Media: Press release with transparent account of the incident and response

6. Post-Incident Review & Security Improvements

Root Cause Analysis

Primary security failures identified:

1. Inadequate web application security testing and patch management
2. Insufficient network segmentation allowing lateral movement
3. Weak monitoring systems that failed to detect unusual data access patterns
4. Overprivileged service accounts
5. Inadequate encryption of sensitive data at rest

Security Posture Improvements

Short-term Recommendations (0-30 days):

- Implement emergency patches for all identified vulnerabilities
- Reset all credentials and implement stronger password policies
- Deploy enhanced monitoring solutions focused on database activity
- Conduct targeted security awareness training
- Implement additional network segmentation

Medium-term Recommendations (1-3 months):

- Conduct comprehensive penetration testing of all public-facing applications
- Implement multi-factor authentication across all critical systems
- Review and revise access control policies based on principle of least privilege
- Enhance data loss prevention controls
- Improve encryption standards for data at rest and in transit

Long-term Recommendations (3-12 months):

- Implement a Zero Trust security architecture

- Establish a Security Operations Center (SOC) with 24/7 monitoring
- Develop an enhanced incident response plan with regular tabletop exercises
- Implement advanced threat detection capabilities with AI/ML components
- Conduct quarterly security assessments and annual red team exercises

7. Conclusion

The data breach at ABC SecureBank resulted from a combination of technical vulnerabilities and security process deficiencies. While the impact was significant, affecting approximately 75,000 customers, prompt detection and comprehensive response helped contain the incident and prevent more extensive damage. The lessons learned from this incident provide valuable insights for strengthening the organization's security posture and building resilience against future threats.

By implementing the recommended security improvements and maintaining heightened vigilance, ABC SecureBank can significantly reduce the risk of similar incidents and better protect customer data going forward.

Investigator Information

Investigator Name: Yug Moradiya
Investigation Date: 21st May,2025