EXTION INFOTECH INTERNSHIP
PROJECT 2

DATA BREACH INVESTIGATION

Details :

Company Name: ABC SecureBank, a highly reputable financial institution. Breach Discovery: The breach was discovered during a routine security audit, and it appears that sensitive customer data may have been exposed. Scope of Breach: The breach involves potential exposure of customer account information, including names, account numbers, and transaction history.

TASK 1: Incident Analysis

The data breach might have occurred due to

1)Vulnerability exploitation

2)Social Engineering

3)Insider Threat

Vulnerability Exploitation : Vulnerability exploitation is a very harmful action, which can allow attackers to gain unauthorized access to the system, perform destructive actions or take over control of the system. For example, a loophole in the software used in a website can be exploited by an attacker to take over control of the website and steal important information such as personal orfinancial data from the user.

Social Engineering : In social Engineering the tricks are used to manipulate the employees to give away sensitive information related to their organisation.

Insider Threat: Insider threats are cybersecurity threats that originate with authorized users or employees who intentionally or accidentally misuse their legitimate access, or have their accounts hijacked by cybercriminals.

TASK 2 : FORENSIC ANALYSIS

System Image : create forensic images of affected systems to preserve the state of the system at the time of the breach. This ensures that the original data remains unaltered for analysis.

Network logs: collect network traffic logs, firewall logs, and IDS/IPS logs to trace the attacker's path and identify any malicious activities.

User activity Logs : Review user activity logs and access logs to identify any unauthorized or suspicious activities.

TASK 3: DATA RECOVERY

The type of data that was potentially exposed will be names ,account numbers , account balance of customers, transaction history, etc Secure physical areas potentially related to the breach. Mobilize your breach response team right away to prevent additional data loss. The exact steps to take depend on the nature of the breach and the structure of your business. Depending on the size and nature of the company, we may include forensics, legal, information security, information technology, operations, human resources, communications, investor relations, and management.

TASK 4 REGULATORY COMPLIANCE

For the ABC SecureBank breach involving the exposure of sensitive customer data, several regulatory requirements may apply, depending on the jurisdiction and industry-specific regulations. Here's a general approach to regulatory compliance and reporting requirements:

Identify applicable regulation

1)DATA PROTECTION LAW

Determine the relevant data protection and privacy laws applicable to the affected customers, such as the General Data Protection Regulation (GDPR) in the European Union, the California Consumer Privacy Act (CCPA) in California, or other regional data protection laws.

2)INDUSTRY REGULATION LAW

Consider industry-specific regulations and standards that may apply to financial institutions, such as the Payment Card Industry Data Security Standard (PCI DSS) for payment card data protection.

Notification and Reporting Obligations:

1)Regulatory Notifications:

Identify the regulatory bodies or authorities that must be notified of the breach, such as data protection authorities, financial regulatory agencies, or law enforcement agencies, within the stipulated timeframe prescribed by applicable laws.

2)Customer Notifications:

Comply with requirements to notify affected customers directly about the breach, including the nature of the data exposed, potential risks, protective measures, and contact information for inquiries or support.

TASK 5 COMMUNICATION AND NOTIFICATION :

It is necessary to develop a communication plan for notifying affected customer, stakeholders and regulatory bodies. Engage with key stakeholders, including customers, partners, investors, and regulators, to provide updates on the breach's resolution, compliance activities, and ongoing efforts to enhance cybersecurity resilience.

TASK 6 : POST-INCIDENT REVIEW

Potential Weaknesses

Inadequate Security Controls , Lack of Regular Security Audits,Insufficient Employee Training and Awareness,Ineffective Incident Response Plan,Data Protection and Privacy Measures:

Recommendations for ABC SecureBank:

1)Regular Vulnerability Assessments: Conduct regular vulnerability assessments and penetration testing to identify and address potential security weaknesses.

2)Enhanced Monitoring: Deploy advanced monitoring and intrusion detection systems to detect and respond to unauthorized activities promptly.

3)Data Encryption: Ensure sensitive data, both in transit and at rest, is encrypted to mitigate the risk of exposure in case of unauthorized access.