saib

Cyber Security in Banks

9 July 2021

Contents

- Introduction
- Sample of Cyber Attack Scenarios
- Cyber Security Essentials

Introduction

Definitions

Cyber Attack:

A cyber attack is any attempt to gain unauthorized access to a computer, computing system or computer network with the intent to cause damage. Cyber attacks aim to disable, disrupt, destroy or control computer systems or to alter, block, delete, manipulate or steal the data held within these systems.

Cyber Attack Motives:

- **Financial gain**
- **Making a social/political point (Hactivism)**
- **Disruption and revenge**
- **Warfare (Government sponsored)**

Cyber Attacks

Cyber Attack Types:

- Insider Attackers
- Outsider Attackers (Targeted / Untargeted)

Cyber & Financial Sector:

- Financial sector suffers from cyber attacks 65% more than other sectors
- Annual cost of cyber attacks on financial sector may reach $370 Billions if it continues to spread as expected
- Banks are a primary target for attackers with financial gain motive
- Business need and customer demand for more online and mobile financial services are reflected on new services that increase the risk of cyber attacks

saib

- **Sample of Cyber Attack Scenarios**

Malware Attack:

Malicious software is used to attack information systems. Ransomware, spyware and Trojans are examples of malware. Depending on the type of malicious code, malware could be used by hackers to steal or secretly copy sensitive data, block access to files, disrupt system operations or make systems inoperable.

Phishing Attack:

Emails sent by attacker convincing the victim to perform a mistaken financial transaction or to open a malicious attachment or visit a malicious URL designed to steam sensitive information (i.e. user credentials)

DDOS Attack:

Distributed Denial of Service (DDOS) attack tries to bring the victim’s service down by sending large volumes of simultaneous data requests from multiple sources, thereby making the servers unable to handle any legitimate requests.

Man-in-the-Middle Attack:

Attacker gains access to the data traffic between two legitimate source and destination by secretly putting himself in between the two parties. If data is not encrypted, attacker can get sensitive data passing in this communication.

Vulnerability Exploit Attack:

Attacker scans target system looking for an open vulnerability and tries exploiting the same to gain privileged access to target system. If the vulnerability is not already known, the attack will be considered as zero-day exploit.

SQL Injection Attack:

Attacker inserts malicious code into servers through published web forms using the Structured Query Language programming language to get the server to reveal sensitive data.

- **Cyber Security Essentials**

Cyber Security Governance

- Cyber Security Organization
- Cyber Risk Management
- Cyber Security Regulatory Compliance
- Cyber Security Audit & Assessment
- Cyber Security Training & Awareness

Cyber Security Defense

IT Asset Management

Identity & Access Management

Network Security & Control

Encryption Management

Penetration Testing & Vulnerability Management

Cyber Security Monitoring & Incident Handling

Third Parties Cyber Security

Third Party Access Control

Contract Management & Service Level Agreements

Non-Disclosure Agreements

The Right to Audit & Third Party Reporting (e.g. ISAE 3402)

saib

Thank You