CYBERSECURITY RISKS AND RECOMMENDATION

MOHAMMAD FIRDHAUS BAHAROM [CAPSTONE PROJECT 2024]

Agenda

1. Introduction to Cybersecurity in Singapore’s Financial Sector
2. Case Study: 2024 Android Malware Scam Targeting Singapore Banks
3. Impact on Corporate Financial Security
4. Recurrent Phishing Attacks
5. At-Risk Critical Business Process: Financial Transactions
6. Risks in Data Storage
7. Encryption as a Primary Defense
8. Implementing a Comprehensive Cybersecurity Policy
9. Remediation through Account Lockdown and Credential Reset
10. Communication Plan for Security Incidents
11. Continuous Monitoring and Improvement

Introduction to Cybersecurity in Singapore’s Financial Sector

Cybersecurity Landscape
Singapore’s financial services sector is highly targeted due to its robust economy and technological advancement

Significance of Protection
The financial sector must prioritize cybersecurity to safeguard customer data and maintain trust

Regulatory Oversight
The Monetary Authority of Singapore (MAS) enforces strict cybersecurity regulations to ensure the resilience if financial institutions

Case Study: 2024 Android Malware Scam Targeting Singapore Banks

- **Incident Overview:** In early 2024, a phishing scam using Android malware targeted nearly 2000 Singaporeans, leading to losses exceeding S$34 million.
- **Attack Method:** Cybercriminals lured victims through fake investment ads on social media, leading to credential theft via fraudulent banking apps.
- **Impact:** The incident exposed vulnerabilities in legacy MFA systems, prompting calls for stronger security measures across the sector.

Impact on Corporate Financial Security

How the Phishing Scam Undermines a Company's Financial Cybersecurity

- **Financial Losses:** The incident demonstrates the vulnerability to significant financial loss through malware and phishing attacks threatening corporate financial security.
- **Brand Damage:** Breaches lead to loss of trust and reputational harm, further destabilizing the financial standing of the company.
- **Regulatory Penalties:** Non compliance with cybersecurity regulations could result in fines or sanctions, exacerbating financial damage.

Recurrent Phishing Attacks

The Growing Threat of Repeated Phishing Scams in Corporate Environments

Increased Phishing Sophistication

The success of the initial scam suggests attackers will likely continue and improve their tactics, making future attacks even harder to detect.

Expanded Attack Surface

The proliferation of mobile devices in corporate settings increases vulnerability, particularly with bring-your-own-device (BYOD) policies.

At-Risk Critical Business Process: Financial Transactions

Potential Targets in Corporate Financial Systems

Payment Processing Systems

These systems are attractive targets for cybercriminals aiming to redirect or steal funds.

Employee Payroll Data

Payroll systems contain both financial data and personally identifiable information, making them a high-value target.

Risks in Data Storage

Vulnerabilities in Storing Critical Financial Data and PII

- **Unencrypted Storage:** Storing sensitive information without encryption increases the risk of data breaches.
- **Inadequate Access Controls:** Insufficient access controls can lead to unauthorized data access and potential leaks.

Encryption as a Primary Defense

Protecting Financial Data and PII Through Advanced Encryption Techniques

- **Data Encryption:** Implementing encryption for data at rest and in transit to safeguard against unauthorized access.
- **Multi-Factor Authentication (MFA):** Using MFA for systems storing sensitive data adds an additional layer of security.

Implementing a Comprehensive Cybersecurity Policy

Policies to Safeguard Financial Data and PII in a Corporate Environment

- **Data Protection Policy:** Establish a policy requiring encryption, regular audits, and strict access controls for all critical data.
- **Incident Response Plan:** Develop a response plan to quickly address breaches, including procedures for containment, mitigation, and communication.

Remediation through Account Lockdown and Credential Reset

Immediate Steps to Contain and Mitigate Impact

- **Account Lockdown:** Immediately lock down affected accounts to prevent unauthorized access and further fraudulent transactions.
- **Credential Reset:** Enforce a mandatory reset of credentials for all affected users to ensure compromised credentials are no longer valid.

Communication Plan for Security Incidents

Effective Channels and Strategies for Crisis Communication

- **Internal Alerts via Email and SMS:** Trigger immediate notifications to employees via email and SMS to inform them of the breach and the necessary actions to take.

- **Public Disclosure Through Press Release:** Prepare a press release to inform customers and stakeholders, emphasizing the actions taken and offering guidance on protective measures.

Continuous Monitoring and Improvement

Key Takeaways and Next Steps

Continuous Monitoring and Improvement
Implement regular security audits and updates to fortify defenses against future attacks.

Employee Training
Conduct ongoing cybersecurity awareness training to empower employees against phishing and other cyber threats.