**Phishing** is a type of cyber-attack in which adversaries deceive individuals into disclosing private, financial, and sensitive information. This technique has widespread exposure through emails, messages, and phone calls. We can prevent this adverbial attack by following ways:

IMPACT

• Financial Loss: Victims may incur financial losses and have their personal details compromised, leading to identity theft or unauthorized transactions.

• Data Breaches : Phishing can expose sensitive information, allowing attackers to initiate other cyberattacks like malware infections or ransomware.

• Reputation: Companies can suffer a loss of customer trust and damage to their reputation due to compromised security.

• Operational Disruptions: Phishing attacks can disrupt business operations and lead to legal consequences, especially if customer data is exposed or compliance regulations are breached.

MITIGATION

• Encrypt All Data

Customer data should always be encrypted when stored on servers. Plain text storage, especially of usernames and passwords, should be avoided.

• Data Masking

Data masking should be applied to information that is not necessary for specific roles. For example, IT staff should only see the last four digits of Social Security Numbers when relevant.

• Deploy an Email Filtering Platform

Implement a filtering system that scans emails for content, attachments, senders, and checks the legitimacy of websites. This platform should also conduct regular campaigns to educate users about phishing tactics.

• URL inspection

Examining the url is a critical step in preventing phishing attacks, as attackers often create fake websites that closely mimic legitimate ones to steal sensitive information.

**Ransomware** is a type of cyber-attack in which adversaries encrypt data and demand a financial payment to restore access. This attack vector is on the rise, particularly in the banking sector, where threats such as Distributed Denial of Service (DDoS) attacks, compromised credentials, spoofing, and phishing is increasingly common. Below is a cybersecurity strategy for ‘SafeBank Corp’. aimed at mitigating risks associated with ransomware attacks.

IMPACT

• Business Disruption: Ransomware locks important data, causing major delays and preventing access to key systems or services.

• Financial Loss: Costs include paying the ransom, recovering data, and lost work time, all of which can harm the company financially.

• Reputation Damage: The attack can damage the company’s reputation, leading to a loss of customer trust and confidence.

MITIGATION

• Periodic Testing: Implement regular testing and tabletop exercises with stakeholders to prepare for potential ransomware incidents.

• Advanced Technologies: Utilize artificial intelligence (AI) and machine learning (ML) to enhance ransomware detection and secure the infrastructure.

• Multi-Factor Authentication (MFA): Implement MFA to add an additional layer of security beyond traditional password protection.

• Least privilege: Making sure the access to data is only allowed to perform the necessary duties.

**Insider threat** is a security danger that arises from within an organization, usually involving individuals who have permitted access to the company’s systems, information, or networks. These insiders may include employees, contractors, business associates, or anyone with internal knowledge and access to the organization’s infrastructure.

An insider threat happens when these individuals abuse their access, either on purpose or by mistake, to damage the organization’s resources, systems, or data.

IMPACT

• Trust Issues: Insider threats can create a culture of mistrust among employees, damaging morale and creating a sense of insecurity within the organization. It can also lead to increased surveillance and monitoring, which may further affect employee satisfaction.

• Compliance Risks: Insider threats can expose the organization to legal liabilities, especially if sensitive customer or employee data is compromised. This can lead to lawsuits, fines, or regulatory penalties.

• Competitive disadvantage: If sensitive business information or intellectual property is stolen, it can lead to the loss of a competitive edge, harming the organization’s position in the market.

MITIGATION

• Limit Access to What’s Needed: Give employees access only to the information and systems they need for their job to reduce misuse.

• Monitor Leaving Employees: Remove access and secure company information when employees leave to stop potential data theft or damage.

• Encourage Reporting: Set up a way for employees to report suspicious behavior or potential threats anonymously.

• Use Data Protection Tools: Install software that prevents sensitive data from being shared or moved without permission.

**Implement a Phishing Simulation**

|  |  |  |  |
| --- | --- | --- | --- |
| Phishing Campaign | Number of Emails Sent | Number of Clicks Received | Employee Actions |
| Campaign 1 | 200 | 45 | 30 Reported the Email, 15 Ignored |
| Campaign 2 | 150 | 25 | 20 Reported the Email, 5 Clicked the Link |
| Campaign 3 | 180 | 60 | 50 Reported the Email, 10 Clicked the Link |
| Campaign 4 | 220 | 55 | 40 Reported the Email, 15 Ignored |

The above table helps track how employees respond to phishing emails, showing how many clicked the links and what actions they took (e.g., reporting or ignoring). It helps measure the effectiveness of security training, identify weak areas, and improve response times, ultimately strengthening the organization’s defenses against phishing attacks.

**Summary**

The stages outlined are for a Phishing Incident Response Process. These stages describe how employees should recognize, report, and handle phishing threats, along with how IT support should respond to ensure the company's security is protected. The stages are:

*Detection* – Identifying phishing emails by recognizing warning signs.

*Immediate* Action – Taking steps to avoid interacting with the suspicious email.

*Reporting* – Reporting the phishing attempt to IT support.

*IT Response* – IT investigates the phishing threat and taking necessary actions.

*Follow-Up* – Employees following up by deleting the email and monitoring accounts.

*Ongoing Awareness* – Continuous training and vigilance to prevent future phishing incidents.