Cybersecurity Interns  
 InternCareers

Task Two: Incident Response Simulation

**Scenario Creation: Phishing Attack**  
  
An Account Payable (AP) Manager in a Company got an email from the Chief Financial Officer (CFO) to process payments to one of their trusted suppliers with different Bank details provided on the email. The CFO mentioned that he will be out of the office for a week, so he can’t regulate the transaction, but the transaction needs to happen by the end of business.  
The AP Manager did exactly what he was told. The following day the CFO showed up at work and found out about the previous day’s transaction with the trusted supplier, which he was not aware of.

Context: an attacker was performing a **phishing attempt**, email spoofing to be specific, by obtaining the CFO’s email account credentials and writing an email to the AP Manager to perform a certain transaction.  
Objective: the attackers aim was to **get an amount of money paid** to them through the performance of a transaction by the AP Manager, using their Bank account details provided on the email.  
Scope: in the email it was mentioned that the transaction needs to happen as soon as possible which is by the **end of business**.

**Incident Response Process**

* **Preparation:**

Write a procedure on how to respond phishing attacks.

Inform and train employees about phishing attacks and how to recognise them.

Set up the tools: TheHIVE for incident response and digital forensics, GRR Rapid Response for live remote forensics and incident management and Splunk for log management and real-time analysis.

* **Detection and Identification:**

Use Splunk to monitor email logs for any unusual patterns of activities.

Use email security tools to identify any potential phishing attacks.

* **Notification and communication:**

Use TheHIVE tool for incident response and implement a way on how the incident response team can communicate with each other when detection and response has happened.

* **Gather Information:**

Get details about the phishing email including senders email, any URL or document attachments, in which company the sender is writing from.

Use GRR Rapid Response for endpoint forensics to analyse affected systems.

* **Assessment:**

Determine if there was any sensitive information that was compromised.

* **Activation of Response Teams:**

Activate specific response teams and assign roles and responsibilities to team members using TheHIVE

* **Mitigation:**

GRR Rapid Response to investigate compromised computing devices.

Isolate affected systems to prevent further spread of the phishing attack.

* **Documentation:**

Keep records of the activities, the response, any compromises, findings and etc.

* **Legal and Regulatory Compliance:**

Involve legal practises within systems to ensure compliance with data protection.

Ensure that regulatory requirements are met by following the legal and regulatory obligations.

* **Continuous Monitoring:**

Use OSSEC tool to monitor email logs, network traffic, and computer devices for any signs of threats.

* **Post Incident Analysis:**

Review logs and mention points of improvement using Splunk tool.

Adjust security implementations with the lessons learnt.

**Enhancing incident response capabilities**

Prevention techniques that can be implemented to minimize phishing attacks withing organisations include:

1. Inform and train employees about phishing attacks on how to identify them and report them to the security team.
2. Use email filtering tools and security measures to verify the legitimacy of incoming emails.
3. Implement Multi-Factor Authentication (MFA) for extra layer of security.
4. Implement Security Information and Event Management (SIEM) solutions to detect and respond to security threats before they harm the organisation.
5. Activate Incident Response Teams.

By Amohelang Tsotetsi