Phishing Incident Response Playbook

Purpose

The purpose of this playbook is to provide a structured and efficient response to phishing attacks, minimizing potential damage to systems, data, and reputation while safeguarding users.

Scope

This playbook applies to:

- Email systems, communication platforms, and cloud services.
- Employees, contractors, and stakeholders who interact with company systems.
- Scenarios involving phishing emails, messages, or fake websites attempting to steal credentials or deliver malware.

Assumptions:

- Employees have access to security awareness training.
- Tools like email filtering, endpoint detection, and incident tracking systems are operational.

Roles and Responsibilities

- **Incident Response Lead**: Coordinates the response effort and communicates updates to leadership.
- **IT Security Analyst**: Conducts technical analysis, isolates affected systems, and implements security measures.
- **System Administrator**: Supports containment and recovery efforts (e.g., email filtering, account restoration).
- **Legal and Compliance**: Ensures regulatory and reporting requirements are met.
- **Communication Team**: Manages internal and external communication.

Communication Protocols:

- Notify IT/Security teams immediately upon detection of a phishing incident.

- Use secure communication channels for sensitive updates.
- Alert all employees about confirmed phishing campaigns.

Detection and Analysis

Objective: Identify phishing attempts and assess the scope of the attack.

Actions:

1. **Identify Indicators of Compromise (IoCs)**:
    - Suspicious emails (e.g., unknown sender, misspellings, unexpected links).
    - Reports on unusual account activity.
2. **Analyze Phishing Email**:
    - Extract and examine headers, URLs, and attachments in a sandbox environment.
3. **Alert Monitoring**:
    - Check security tools for alerts (e.g., SIEM logs, endpoint detection).
4. **Determine the Impact**:
    - Identify users who clicked the link, submitted credentials, or downloaded files.
    - Determine if sensitive data was accessed or exfiltrated.

Tools and Resources:

- Email filtering systems.
- Sandboxing tools (e.g., Cuckoo Sandbox, VirusTotal).
- Log analysis tools (e.g., Splunk).

Containment

Objective: Limit the spread and impact of the phishing attack.

Actions:

1. Block malicious domains, URLs, and IPs on the firewall and email systems.

2. Disable affected user accounts immediately.
3. Isolate compromised devices from the network.
4. Warn employees via an internal alert:
    - Share IoCs (Indicators of Compromise) (e.g., email subject lines, domains).
    - Advice not to engage with similar emails.

Tools and Resources:

- Firewall and email security configurations.
- Endpoint isolation tools.

Eradication

Objective: Remove all traces of the phishing attack and prevent reoccurrence.

Actions:

1. Delete all instances of the phishing email from inboxes (automated or manual).
2. Remove malware or malicious files from affected systems.
3. Reset credentials for compromised accounts and enforce MFA.
4. Review and strengthen email filtering rules.

Tools and Resources:

- Antivirus and antimalware tools.
- Email server management tools.

Recovery

Objective: Restore normal operations and validate the security of systems.

Actions:

1. Restore any impacted systems or data from verified backups.
2. Validate the effectiveness of email filters and network controls.
3. Conduct security awareness refresher training for affected employees.

4. Monitor systems and accounts for signs of lingering threats.

Tools and Resources:

- Backup and recovery systems.
- Security monitoring tools.

Post-Incident Activity

Objective: Review the incident, document lessons learned and improve response strategies.

Actions:

1. Conduct a post-mortem meeting:
    - Review response actions and timelines.
    - Identify areas for improvement.
2. Update policies and training materials:
    - Incorporate lessons learned.
    - Enhance phishing simulations.
3. Submit reports to stakeholders:
    - Include findings, impact, and preventive measures.

Tools and Resources:

- Incident tracking system.
- Security awareness platforms.

Summary Checklist

- **Report phishing attempt. ( )**
- **Analyze email contents and IoCs. ( )**
- **Block and isolate malicious components. ( )**
- **Eradicate malware and reset compromised accounts. ( )**
- **Restore operations securely. ( )**
- **Review and update incident response measures. ( )**