Incident Response Case Study (SOC): Ransomware, Phishing, and Unauthorized Access

Simulated incidents documented using NIST incident response lifecycle.

1. **Overview**

   This document presents a simulated incident response case study involving multiple cybersecurity incidents, including ransomware, phishing, and unauthorized access. The incidents were analyzed and documented following the NIST Incident Response Lifecycle, including detection, analysis, containment, eradication, and recovery.

2. **Incident 1: Ransomware in Healthcare Clinic**

- Incident Phase:

  Detection and Analysis; Containment, Eradication, and Recovery

- Summary:

  A ransomware attack disrupted operations within a healthcare clinic after malicious phishing emails were sent to employees. Attackers gained unauthorized access to the internal network and encrypted critical systems, demanding a ransom for data recovery.

- Root Cause:

  The incident was caused by employees opening phishing email attachments that contained malicious content, exploiting human error and lack of email security awareness.

- Impact:

  Critical systems became unavailable, disrupting daily operations and risking exposure of sensitive healthcare data.

- Actions Taken / Response:

  The infected systems were isolated to prevent further spread. Recovery efforts focused on removing malicious components and restoring systems from backups.

- Recommended Controls:
  - Multi-factor authentication (MFA)
  - Regular offline backups
  - Employee phishing awareness training

3. **Incident 2: Phishing Email Alert and Escalation**

- Incident Phase:

  Detection and Analysis

- Summary:

  A phishing email containing a password-protected malicious attachment was delivered to an employee in the HR department, disguised as a legitimate job application.

- Root Cause:
  Social engineering techniques were used to trick the recipient into opening the attachment and entering the provided password.
- Impact:
  Potential malware execution on an internal endpoint and risk of unauthorized access.
- Actions Taken / Response:
  The alert was classified as medium severity and escalated to a Tier-2 SOC analyst for further investigation.
- Recommended Controls:
  - Advanced email filtering
  - Phishing simulations and training
  - Attachment sandboxing

4. Incident 3: Forced Browsing and Data Exposure

- Incident Phase:
  Detection and Analysis
- Summary:
  An attacker exploited a forced browsing vulnerability in an e-commerce application, gaining unauthorized access to customer transaction records.
- Root Cause:
  Insufficient access control allowed attackers to manipulate URL parameters to access restricted resources.
- Impact:
  Exposure of personal and financial information of approximately one million customers.
- Actions Taken / Response:
  The vulnerability was identified and addressed through access control enforcement and security review.
- Recommended Controls:
  - Input validation
  - Role-based access control
  - Regular vulnerability scanning

5. Supporting Activity: Network Traffic Capture with tcpdump

- Purpose:
  To observe and analyze network traffic during security investigations.
- Tool used:
  Tcpdump
- Description:

Network traffic was captured and inspected at the packet level to identify communication patterns and potential anomalies. This activity supports incident investigation by providing visibility into network behavior.

- Value to Incident Response:
  Packet-level analysis assists SOC analysts in validating suspicious activity and supporting incident triage.

6. **Key Mitigations and Recommendations**

- Implement multi-factor authentication (MFA) across all user accounts
- Conduct regular phishing awareness and simulation training
- Maintain offline and regularly tested backups
- Enforce least-privilege access controls
- Perform routine vulnerability scanning and monitoring

7. **Skills Demonstrated**

- Incident detection, analysis, and response documentation
- Alignment with the NIST Incident Response Lifecycle
- Phishing and ransomware incident investigation
- Risk identification and mitigation planning
- Network traffic analysis using tcpdump
- Security control recommendations and hardening strategies
- Clear technical documentation and reporting