Week-6

Asad Muhammad Channar

DHC-56

Security Incident Documentation:

- **Task:** Document the security incidents encountered during the mock drill in Week 5. Outline how they were handled and propose improvements to the incident response plan.
- **Goal:** Develop a comprehensive incident report and refine the response strategies for future incidents.

Security Incident Documentation Report

1. Overview of the Mock Drill and Incidents

This report documents the security incidents encountered during the mock drill conducted in Week 5. The objective of this drill was to test the effectiveness of the organization's incident response plan by simulating various security scenarios. The drill involved scenarios such as unauthorized access attempts, phishing attacks, and data exfiltration to assess team response times, coordination, and handling processes.

2. Incident Summary

The following incidents were simulated and documented during the drill:
- **Incident 1: Unauthorized Access Attempt**
  A simulated breach attempt by an unauthorized user within the internal network. This incident was intended to test access control measures and the response to lateral movement attempts.

- **Incident 2: Phishing Attack**
  A targeted phishing email was sent to multiple users to evaluate email security controls and user awareness.

- **Incident 3: Data Exfiltration Simulation**
  Simulated data extraction from sensitive folders to test data loss prevention (DLP) systems and alerting mechanisms.

3. Incident Handling and Response

Incident 1: Unauthorized Access Attempt

Upon detection of the unauthorized access attempt, the incident response team immediately activated network segmentation protocols to isolate the suspicious activity. Logs were reviewed to trace the access path, and the user account involved was temporarily disabled. The team then performed a forensic analysis to confirm if any data was compromised.

Resolution: The incident was contained, and no data was lost. All users were advised to update their credentials as a precaution.

Incident 2: Phishing Attack

A phishing email was detected by automated email security systems. It was flagged and isolated, preventing users from opening it. The incident response team ran an awareness campaign immediately after to educate users on identifying phishing attempts.

Resolution: The phishing email was successfully contained. No users interacted with the malicious content, highlighting the effectiveness of the awareness training and email filters.

Incident 3: Data Exfiltration Simulation

Simulated data exfiltration was detected through the organization's Data Loss Prevention (DLP) system. The incident response team was alerted to a possible data leak from secure folders. The team immediately stopped the data transfer and analyzed network traffic to ensure no sensitive information was removed.

Resolution: The simulation highlighted the DLP system's effectiveness, and no actual data was compromised. Follow-up analysis suggested areas for improvement in DLP configuration to reduce false positives.

4. Proposed Improvements to the Incident Response Plan

Based on the outcomes of the mock drill, the following improvements are proposed for the incident response plan:

- **Enhanced User Training**: Increase frequency of security awareness training to improve user vigilance.
- **Incident Response Drills**: Conduct regular drills to ensure all team members are proficient in handling security incidents and familiar with protocols.
- **Automated Alert Optimization**: Improve alert configurations in DLP systems to reduce false positives and focus on high-priority incidents.
- **Access Control Refinement**: Periodically review and update access controls to prevent unauthorized access attempts.

5. Conclusion and Next Steps

The mock drill provided valuable insights into the organization’s security preparedness. Each incident was handled effectively, but areas for improvement were identified. By refining the incident response plan with more rigorous training, optimized DLP alerts, and regular access control reviews, the organization can enhance its readiness for real-world threats.

Future steps involve periodic mock drills, integration of automated incident response tools, and continuous updates to incident response protocols.