TASK 2: CYBERSECURITY INCIDENT RESPONSE (Simulation)

Bryn Phoshoko 2/11/24 Intern Career

Task 2: Incident Response Simulation - Incident Report

Outline of Scenario:

An employee in Walkergenix company, let's call them Employee A, receives an urgent email purportedly from a high-ranking executive, requesting them to share their Office 365 login credentials due to a supposed IT emergency. Believing the message was legitimate, Employee A provides their credentials. The attacker gains access to Employee A's Office 365 account and begins sending phishing emails from their account to other employees, further compromising sensitive data.

1. Incident Overview:

- **Date and Time:** 11 February 2024
- **Incident Type:** Social Engineering Attack (Phishing)
- **Affected User:** Employee A
- **Attack Vector:** Email Spoofing and Social Engineering

2. Incident Detection:

Tools Used:

- Email monitoring tools.
- Simulated logs

Anomalies Detected:

- Unauthorized access to Employee A's Office 365 account
- Unusual outgoing email patterns
- Employee reports of suspicious emails

3. Roles within the Incident Response Team:

1. **Incident Coordinator:** John Moagi
2. **Security Analyst:** Bryn Phoshoko
3. **IT Administrator:** Juliet Smith
4. **Communication Coordinator:** Robert Makhubela

4. Response Plan Execution:

Incident Coordinator:

- Coordinated response efforts.
- Communicated with stakeholders.

Security Analyst:

- Investigated the compromised account.
- Analysed phishing emails for indicators of compromise.

IT Administrator:

- Disabled the compromised account.
- Assessed potential data breaches.
- Implemented security measures.

Communication Coordinator:

- Informed employees about the phishing threat.
- Educated them on identifying such attacks.
- Provided guidance on reporting suspicious activities.

5. Containment and Mitigation:

1. Disabled Employee A's compromised Office 365 account.
2. Analysed phishing emails to identify recipients and potential data breaches.
3. Implemented email filtering to block further phishing attempts.
4. Communicated with employees about the phishing threat and provided guidance.

6. Forensic Analysis:

Tasks:

- Collected and preserved evidence from Employee A's compromised Office 365 account.
- Analysed email logs and phishing emails to identify the attacker's methods and potential data breaches.
- Determined the root cause of the incident and identified vulnerabilities.

Tools:

- Forensic tools (email analysis software, log analysis tools, Office 365 audit logs).

7. Post-Incident Assessment:

Review and Identify Improvement Areas:

- Assessed the effectiveness of the incident response.
- Evaluated communication within the response team and with employees.
- Identified areas for improvement in employee training and awareness.
- Reviewed and updated security policies and procedures.

Lessons Learned:

- Documented strengths and weaknesses in the response.
- Captured lessons learned from the simulation.

8. Documentation and Presentation:

Documentation:

1. Detailed incident report.
2. Forensic analysis report.
3. Summary of lessons learned.
4. Recommendations for enhancing incident response capabilities and improving security awareness among employees.

Presentation:

- Delivered a presentation to key stakeholders, summarizing the incident, response, actions, and recommendations. Included visuals such as timelines, graphs, and key findings.

End of Incident Report.