MUBEEN GUL MALIK

DEP TASK 3

**Task 3**

**Developing Incident Response Plans**

**3.Key Steps:**

**1.Objective: Create a plan for responding to security incidents.**

**2.Description:Develop a structured approach for responding to**

**and managing security incidents. Ensure the plan minimizes**

**damage and facilitates quick recovery**

**Identifying potential security incidents and scenarios.**

**Defining roles and responsibilities for the response team.**

**Developing step-by-step response procedures.**

**Conducting training and simulation exercises.**

**Reviewing and updating the plan regularly.**

**Developing Incident Response Plans**

**Objective:**

* **Goal:** Create a comprehensive plan for effectively responding to security incidents.
* **Purpose:** Ensure the plan minimizes damage, manages the incident efficiently, and facilitates a swift recovery.

**Key Steps:**

1. **Identifying Potential Security Incidents and Scenarios**
   * **Assessment:** Identify and categorize possible security incidents, such as data breaches, malware infections, phishing attacks, insider threats, or DDoS attacks.
   * **Scenarios:** Develop specific scenarios for each type of incident, considering the impact on different parts of the organization.
   * **Prioritization:** Rank incidents based on their potential impact and likelihood of occurrence to focus on the most critical threats.
2. **Defining Roles and Responsibilities for the Response Team**
   * **Incident Response Team (IRT):** Form a team that includes key personnel such as IT security staff, legal advisors, PR, and HR.
   * **Role Definition:** Clearly outline the responsibilities of each team member, such as who will handle communications, who will investigate the breach, and who will coordinate recovery efforts.
   * **Escalation Paths:** Establish clear lines of communication and escalation procedures in case of an incident.
3. **Developing Step-by-Step Response Procedures**
   * **Incident Detection:** Outline how to detect and confirm an incident, including monitoring systems, alerts, and initial verification steps.
   * **Containment:** Detail how to contain the incident to prevent further damage, such as isolating affected systems.
   * **Eradication:** Provide steps to remove the cause of the incident, such as cleaning infected systems or closing security gaps.
   * **Recovery:** Develop procedures for restoring affected systems and services to normal operation.
   * **Communication:** Include guidelines for internal and external communications during and after the incident.
   * **Documentation:** Emphasize the importance of documenting every action taken during the response for post-incident analysis.
4. **Conducting Training and Simulation Exercises**
   * **Training:** Regularly train the response team on their roles, the tools they'll use, and the procedures they need to follow.
   * **Simulations:** Conduct tabletop exercises or full-scale simulations to test the response plan, identify weaknesses, and improve team coordination.
   * **Feedback Loop:** After each training session or simulation, review performance, gather feedback, and make necessary adjustments to the plan.
5. **Reviewing and Updating the Plan Regularly**
   * **Continuous Improvement:** Schedule regular reviews of the incident response plan to keep it up to date with new threats, technologies, and organizational changes.
   * **Lessons Learned:** After any real incident, conduct a post-mortem to learn from the experience and refine the plan.
   * **Stakeholder Involvement:** Ensure that all stakeholders are involved in the review process to maintain alignment and readiness.