CompTIA Security + 5.0 Risk Management

Filename: comptia-secplussy0501-5-4-incident_response_procedures
Title: Incident Response Procedures
Subtitle: CompTIA Security+ (SY0-501)

5.4 Incident Response Procedures

- 5.4 Given a scenario, follow incident response procedures.
    - Incident response plan
        - Documented incident types/category definitions
        - Roles and responsibilities
        - Reporting requirements/escalation
        - Cyber-incident response teams
        - Exercise
    - Incident response process
        - Preparation
            - We get the right people - ahead of the incident
                - Authority (managers, first reponders, law enforcement)
                - Determining *roles and responsibility*
                - *Cyber-incident response team*
                - Contact information
                - Esculation procedures
                - Team Sizing
                - Policy Enforcement
                - On-premise/ Off premise (third-party, cloud provider)
                - Implementation of an incident tracking process
                - *Training - Exercise*
            - We get the right tools - ahead of the incident
                - Policies, Software
            - We right processes in place - ahead of the incident
            - We train the staff(understand of individual roles) - ahead of the incident
            - Promotes awareness and preparedness - ahead of the incident
        - Identification
            - Question - Do we move forward in the incident response handling process or return to monitoring?
            - Determine - Has an incident happens or is an incident still ongoing?
            - Identify - Categorize the incident
                - High Impact, Medium Impact, Low Impact
            - Allocate - Helps to enusre resources are allocated appropriately and that the right team or teams are deployed
        - Containment
            - Quickly containing the incident event can drastically reduce the cost to the company
            - Is isolation of a system needed, firewalls, VLANs, closing a switch port
            - Implement esculation procedures where necessary
            - Is a forensics investigation going to be needed?
        - Eradication
            - Requires and understanding of the attack vector
            - Antimalware, formatting, patching, updates, imaging
        - Recovery
            - Bringing the production system back online
            - Ensure that the data is restore
            - Ensure that the system is fully restored
            - Monitoring the system for full functionality
            - Auditing the system's logs for analysis
        - Lessons learned
            - How can security be improved?
            - Is more training require?
            - Has compliance been met/retained?
            - Do we have enough people and are they the right people?
            - Was there any accidental collateral damage?