Cyber Security Incident Resonse Team

Incident Response Process

- Preparation
  - An organization with a well-planned incident response procedure, a strong posture, and a knowledgable CISO > able to limit the following damages ==>
    - Quickly discovering the breach
    - Having an internal response team ready to take action
    - Quickly obtaining forensic data
    - Beginning an incident response plan
- Identification
  - The recognition of whether an event that occurs should be classified as an incident

    Once identified > Contact might be required to other groups of escalate the problem, if necessary
- Containment
  - Isolating the problem

    This phase might also include evidence gathering, and further investigation
- Eradication
  - Removal of the attack or threat
- Recovery
  - Retrive data, repair systems, re-enable servers and networks ==> Make the IT landscape 100% operational again
- Lessons Learned
  - Document the process and make any changes to procedures and processes that are necessary for the future.

    Damage and Loss should be calculated and the result shared with the accounting department of the organization

    The affected systems (also the dependant ones) should be monitored for any repercussions

Security Event vs Security Incident

- Security Event
  - Any event that could have potential InfoSec implications e.g. Organizations may witness thousands of identifiable security events daily
    - Example: SPAM Mail since it may contains a link to Malware/ CEO Fraud/ Spear Phising etc
- Security Incident
  - A Security Event that could potentially require an investigation from the CSIRT-Team

Incident Response

- A Set of procedures that an investigator follows when examining a Security Incident

Incident Management

- The monitoring and detection of Security Events on a Computer Network and the execution of proper responses to those security events

Asset Management

- An asset is any tangible or intangible thing or characteristic that has value to an organization.
  [ISO/IEC 27000:2014]

  Asset management > Create an inventory and manage the value of the assets based on Risk, Impact and ease of attack

Vulernerability Management

- Vulnerability management is the ongoing, regular process of identifying, assessing, reporting on, managing and remediating cyber vulnerabilities across endpoints, workloads, and systems.

  Typically, a security team will leverage a vulnerability management tool to detect vulnerabilities and utilize different processes to patch or remediate them.

Presented with xmind