Module-5

Incident Response

Incident Response Process

- Step 1: identification
- Step 2: incident recording
- Step 3: initial response
- Step 4: communicating the incident
- Step 5: containment
- Step 6: formulating a response strategy
- Step 7: incident classification
- Step 8: incident investigation

Step 9: Data collection

Step 10: Forensic analysis

Step 11: Evidence protection

Step 12: Notify external agencies

Step 13: Eradication

Step 14: Systems recovery

Step 15: Incident documentation

Audio and video documentation

strategies

Step 1: Identification

- **Obtaining and validating information related to information security issues**
  - In incident handling, detection may be the most difficult task. Incident response teams in an organization are equipped to handle security incidents using well-defined response strategies beginning with information gathering.
  - Preparing a list most common attack vectors such as **external/removable media, web, email, impersonation, improper use by authorized users etc.** can narrow down to the most competent incident handling procedure.
  - Therefore, it is important to validate each incident using defined standard procedures and document each step taken accurately.

Step 1: Identification

- **Common issues and incidents of information security that may require action and whom to report**
  - An indicator may not always translate into a security incident given the possibility of technical faults due to human error in cases such as server crash or modification of critical files.
  - Determining whether a particular event is actually an incident is sometimes a matter of judgment.
  - It may be necessary to collaborate with other technical and information security personnel to make a decision.
  - Therefore, incident handlers need to report the matter to highly experienced and proficient staff members who can analyse the precursors and indicators effectively and take appropriate actions.

Step 1: Identification

Mentioned below are some of the means to conduct initial analysis for validation

- **Profiling networks and systems**
  - in order to measure the characteristics of expected activity so that changes to it can be more easily identified and used one of the several detection and analysis techniques.
- **Studying networks, systems and applications**
  - to understand what their normal behavior is so that abnormal behavior can be recognized more easily.
- **Creating and implementing a log retention**
  - policy that specifies how long log data should be maintained may be extremely helpful in analysis because older log entries may show reconnaissance activity or previous instances of similar attacks.

Step 1: Identification

Mentioned below are some of the means to conduct initial analysis for validation

- **Correlating events using evidence of an incident**
  - captured in several logs such wherein each may contain different types of data — a firewall log may have the source IP address that was used, whereas an application log may contain a username.
- **Synchronizing hosts clock using protocols**
  - such as the network time protocol (NTP) to record time of attack.
- **Maintain and use a knowledge base of information**
  - that handlers need for referencing quickly during incident analysis.
- **Use internet search engines for research**
  - to help analysts find information on unusual activity.
- **Run packet sniffers to collect additional data**
  - to record traffic that matches specified criteria should keep the volume of data manageable and minimize the inadvertent capture of other Information.
- **Filter the data to segregate**
  - categories of indicators that tend to be insignificant.

Step 2: Incident recording

- Any occurrences of incident must be recorded and the incident response team should update the status of incidents along with other pertinent information.
- Observations and facts of the incident may be stored in any of the following sources such as logbook, laptops, audio recorders and digital cameras etc.

Incident record samples and template

- Documenting system events, conversations and observed changes in files can lead to a more efficient, more systematic and error-free handling of the problem.
- Using an application or a database, such as an issue tracking system helps ensure that incidents are handled and resolved in a timely manner.

Step 2: Incident recording

The following useful information are to be included in an incident record template:

- Current status of the incident as new, in progress, forwarded for investigation, resolved etc.
- Summary of the incident
- Indicators related to the incident
- Other incidents related to this incident
- Actions taken by all incident handlers on this incident
- Chain of custody, if applicable
- Impact assessments related to the incident
- Contact information for other involved parties (system owners, system administrators etc.)
- List of evidence gathered during the incident investigation
- Comments from incident handlers
- Next steps to be taken (rebuild the host, upgrade an application etc.)

Step 3: Initial response

- Commence initial response to an incident based on the type of incident, the criticality of the resources and data that are affected, the severity of the incident, existing service level agreements (SLA) for affected resources, the time and day of the week, and other incidents that the team is handling.
- Generally, the highest priority is handling incidents that are likely to cause the most damage to the organization or to other organizations.

Step 4: Communicating the incident

- The incident should be communicated in appropriate procedures through the organization’s points of contact (POC) for reporting incidents internally.
- Therefore, it is important for an organization to structure their incident response capability so that all incidents are reported directly to the incident response team, whereas others will use existing support

Step 4: Communicating the incident

- **Assigning and escalating information on information security incidents**
- Organizations should also establish an escalation process for those instances when the team does not respond to an incident within the designated time.
- This can happen for many reasons. For example, cell phones may fail or people may have personal emergencies.
- The escalation process should state how long a person should wait for a response and what to do if no response occurs.
- On failure to respond within a stipulated time, then the incident should be escalated again to a higher level of management. This process should be repeated until the incident is successfully handled.

Step 5: Containment

Containment and quarantine

- Containment is important before an incident overwhelms resources or increases damage.
- Most incidents require containment so that is an important consideration early in the course of handling each incident.
- Containment provides time for developing a tailored remediation strategy.
- An essential part of containment is decision-making where the situation may demand immediate action such as shut down a system, disconnect it from a network and disable certain functions.

Step 5: Containment

Various containment strategies may be considered in the following ways:

- ❖ Potential damage to and theft of resources
- ❖ Need for evidence preservation
- ❖ Service availability (network connectivity, services provided to external parties etc.)
- ❖ Time and resources needed to implement the strategy
- ❖ Effectiveness of the strategy (partial containment, full containment etc.)
- ❖ Duration of the solution (emergency workaround to be removed in four hours, temporary workaround to be removed in two weeks, permanent solution etc.)

Step 6: Formulating a response strategy

- An analysis of the recoverability from an incident determines the possible responses that the team may take when handling the incident.
- An incident with a high functional impact and low effort to recover from is an ideal candidate for immediate action from the team.
- In situations involving high end data infiltration and exposure of sensitive information the incident response team may formulate response by transferring the case to strategic level team. Each response strategy should be formulated

Step 6: Formulating a response strategy

- Based on business impact caused by the incident and the estimated efforts required to recover from the incident.
- Incident response policies should include provisions concerning incident reporting at a minimum, what must be reported to whom and at what times.
- Important information to be included are cio, head of information security, local information security officer, other incident response teams within the organization, external incident response teams (if appropriate), system owner, human resources (for cases involving employees, such as harassment through email), public affairs etc.

Step 7: Incident classification

Classifying and prioritizing information security incidents

- An incident may be broadly classified based on common attack vectors such as
  - External/ removable media;
  - Attrition;
  - Web;
  - Email;
  - Improper usage;
  - Loss or theft of equipment;
  - Miscellaneous.

Step 8: Incident investigation

- One of the key tasks of an incident response team is to receive information on possible incidents, investigate them, and take action to ensure that the damage caused by the incidents is minimized.
- **Following up an incident investigation**
  - In the course of the work, the team must adhere to the following procedures deemed
  - Receive initial investigation and data gathering from IT help desk members and escalate to high strategic level specialist if situation demands.
  - Use appropriate materials that may be needed during an investigation.

Step 9: Data collection

Chain of custody

- Evidences collected should be accounted for at all times whenever evidence is transferred from person to person, chain of custody forms should detail the transfer and include each party's signature.
- A detailed log should be kept for all evidence, including the following:
    - Identifying information (e.G. The location, serial number, model number, hostname, media access control (MAC) addresses and IP addresses of a computer).
    - Name, title, and phone number of each individual who collected or handled the evidence during the investigation.
    - Time and date (including time zone) of each occurrence of evidence handling.
    - Locations where the evidence was stored.

.

Step 10: Forensic analysis

- Incident handling requires some team members to be specialized in particular technical areas, such as network intrusion detection, malware analysis or forensics. Many incidents cause a dynamic chain of events to occur, an initial system snapshot may do more good in identifying the problem and its source than most other actions that can be taken at this stage.
- Therefore, it is appropriate to obtain snapshots through full forensic disk images, not file system backups. Disk images should be made to sanitized write-protectable or write-once media.

Step 10: Forensic analysis

- This process is superior to a file system backup for investigatory and evidentiary purposes. Imaging is also valuable in that it is much safer to analyse an image than it is to perform analysis on the original system because the analysis may inadvertently alter the original.
- Some of the useful resources in forensic aspects of incident analysis may include digital forensic workstations and/ or backup devices to create disk images, preserve log files, and save other relevant incident data

Step 11: Evidence protection

Importance of keeping evidence relating to information security incidents

- Collecting evidence from computing resources presents some challenges.
- It is generally desirable to acquire evidence from a system of interest as soon as one suspects that an incident may have occurred.
- Users and system administrators should be made aware of the steps that they should take to preserve evidence.
- In addition, evidence should be accounted for at all times whenever evidence is transferred from person to person, chain of custody forms should detail the transfer and include each party's signature and a registry or log be maintained location of the stored evidence.

Step 12: Notify external agencies

- An organization’s incident response team should plan its incident coordination with those parties before incidents occur to ensure that all parties know their roles and that effective line of communication are established.
- Some of the organizations’ external agencies may include other or external incident response teams, law enforcement agencies, internet service providers and constituents, law enforcements/ legal departments and customers or system owner etc.

Step 13: Eradication

- Eliminating components of the incident such as deleting malware and disabling breached user accounts as well as identifying and mitigating all vulnerabilities that were exploited follow next to successful containment and quarantine.
- During the process, it is important to identify all affected hosts within the organization so that they can be remediated.
- In some cases, eradication is either not necessary or is performed during recovery.

Step 14: Systems recovery

- In recovery, administrators restore systems to normal operation, confirm that the systems are functioning normally, and (if applicable) remediate vulnerabilities to prevent similar incidents.
- Recovery may involve such actions as restoring systems from clean back-ups, rebuilding systems from scratch, replacing compromised files with clean versions, installing patches, changing passwords and tightening network perimeter security (e.G. Firewall rulesets, boundary router access control lists etc.).
  - Higher levels of system logging or network monitoring are often part of the recovery process. Once a resource is successfully attacked, it is often attacked again or other resources within the organization are attacked in a similar manner.

Step 15: Incident documentation

- A logbook is an effective and simple medium for recording all facts regarding incidents. Documenting system events, conversations and observed changes in files can lead to a more efficient, more systematic and less error prone handling of the problem.
- Every step taken from the time the incident was detected to its final resolution should be documented and time-stamped.
- Every document regarding the incident should be dated and signed by the incident handler as such information can also be used as evidence in a court of law if legal prosecution is pursued.

Step 15: Incident documentation

- A logbook is an effective and simple medium for recording all facts regarding incidents. Documenting system events, conversations and observed changes in files can lead to a more efficient, more systematic and less error prone handling of the problem.
- Every step taken from the time the incident was detected to its final resolution should be documented and time-stamped.
- Every document regarding the incident should be dated and signed by the incident handler as such information can also be used as evidence in a court of law if legal prosecution is pursued.