11. Incident Response

Digital Forensics and Cybercrime course

Prof. Zanero

Security Incident

“Any action that threatens one or more of the classic security services of confidentiality, integrity, availability, accountability, authenticity, and reliability in a system.”

Incident Response

Development of procedures to handle and respond to computer incidents

- Need to reflect the range of possible consequences of an incident on the organization.
- Allow for a suitable response.

Incident Response Capability Benefits

- Responding to incidents systematically so that the appropriate steps are taken.
- Helping personnel to recover quickly and efficiently minimizing loss or theft of information and disruption of services.
- Dealing properly with legal issues.
- Using information gained during incident handling
  - to better prepare for handling future incidents
  - to provide stronger protection for systems and data

Use Case:
Mass Email Worm Infection

Exploit unpatched vulnerabilities in desktop applications and then spread via e-mail.

The volume of traffic these can generate could be high enough to cripple both intranet and Internet Connections.

Obvious response: ...

Use Case:
Mass Email Worm Infection

Exploit unpatched vulnerabilities in desktop applications and then spread via e-mail.

The volume of traffic these can generate could be high enough to cripple both intranet and Internet Connections.

<u>Obvious response</u>:

- Disconnect the organization from the Internet
- Shut down the internal email system

Use Case:
Mass Email Worm Infection

- Serious impact the organization's processes

Need to find a trade-off between major loss of functionality against further significant systems compromise.

Use Case:
Mass Email Worm Infection

- Serious impact the organization's processes

Need to find a trade-off

A good incident response policy should:

- Indicate the action to take for an incident of this severity.
- Specify the personnel who have the responsibility to make decisions and detail how they can be quickly contacted.

Managing Security Incidents

Procedures and controls that address:

- Detecting potential security incidents.
- Sorting, categorizing, and prioritizing incoming incident reports.
- Identifying and responding to breaches in security.
- Documenting breaches in security for future reference.

Security Incident Terminology

- **Artifact**
  - Any file or object found on a system that might be involved in probing or attacking systems and networks or that is being used to defeat security measures.
- **Computer Security Incident Response Team (CSIRT)**
  - A capability set up for the purpose of assisting in responding to computer security–related Incidents that involve sites within a defined constituency, also called CERT, or with other acronyms

Computer Security Incident Response Team (CSIRT)

Responsible for:

1. Rapidly detecting incidents.
2. Minimizing loss and destruction.
3. Mitigating the weaknesses that were exploited.
4. Restoring computing services.

Security Incident Terminology

- **Constituency**
  - The group of users, sites, networks, or organizations served by the CSIRT.
- **Incident**
  - A violation or imminent threat of violation of computer security policies.
- **Triage**
  - The process of receiving, sorting, and prioritizing of information to facilitate its appropriate handling.
- **Vulnerability**

Detecting Incident

Security incidents may be detected by:

- **Users** who report a system malfunction or anomalous behavior or weaknesses of the system.
  - Staff should be encouraged to make such reports (training).
- **Automated tools** that analyze information gathered from the systems and connecting networks.

Automated tools for Incident Detection Categories

- **System integrity verification tools**:
  - Scan critical system files, directories, and services to ensure they have not been changed without proper authorization.
- **Log analysis tools**:
  - Analyze the information collected in audit logs using form of pattern recognition to identify potential security incidents.
- **Network and host intrusion detection systems (IDS)**:
  - Monitor and analyze network and host activity and usually compare this information with a collection of attack signatures to identify potential security incidents.
- **Intrusion prevention systems (IPS)**:
  - Augment an intrusion detection system with the ability to automatically block detected attacks.

Automated tools for Incident Detection Categories

- **Systen**
  - Scan cr
    have nc
- **Log an**
  - Analyze
    recogni
- **Networ**
  system
  - Monitor
    this info
    potentia
- **Intrusi**
  - Augmer
    block d

Automated Tools for Incident Detection

- The **effectiveness** depends on:
  - the accuracy of their configuration;
  - the correctness of the patterns and signatures used.

- They need to:
  - Be updated regularly.
  - Distinguish adequately between normal, legitimate behavior and anomalous attack behavior.

Automated Tools for Incident Detection key advantages

It is difficult for security administrators to keep pace with the rapid changes to the security risks to their systems and to respond in a timely manner.

- Can track changes in known attacks
- Help reduce the risks to the organization from delayed response

Automated Tools for Incident Deployment

Their deploy involves significant resources, both monetary and personnel time

- needs to be justified by the benefits gained in reducing risks.

The decision to deploy automated tools depends on:

- The organization's security goals and objectives.
- The specific needs identified in the risk assessment process.

Triage Function

***GOAL**: Ensure that all information destined for the incident handling service is channeled through a single focal point regardless of the method by which it arrives for appropriate redistribution and handling within the service.*

Triage Function

The triage function responds to incoming information:

1. It may need to request additional information in order to categorize the incident.
2. If the incident relates to a known vulnerability,
   a. it notifies the enterprise about it.
   b. shares information about how to fix or mitigate it.
3. It identifies the incident as either new or part of an ongoing incident and passes this information on to the incident handling response function in priority order.

Responding to Incidents

Once a potential incident is detected, there must be documented procedures to respond to it.

Response activities:

- Taking action to protect systems and networks affected or threatened by intruder activity.
- Providing solutions and mitigation strategies from relevant alerts.
- Looking for intruder activity on other parts of the network.
- Filtering network traffic.
- Rebuilding systems.
- Patching or repairing systems.
- Developing other response or workaround strategies.

Response Procedures

Response procedure must:

- Identify
  - The cause of the security incident (accidental/deliberate)
  - Typical categories of such incidents
  - The approach taken to respond to them
  - The management personnel responsible for making critical decisions and how to contact them.
  - The circumstances when security breaches should be reported to third parties.
- Describe the action taken to recover from the incident
  - minimizing the compromise or harm to the organization
- Gather the evidence of the incident.

Gathering Evidence

This information is used to

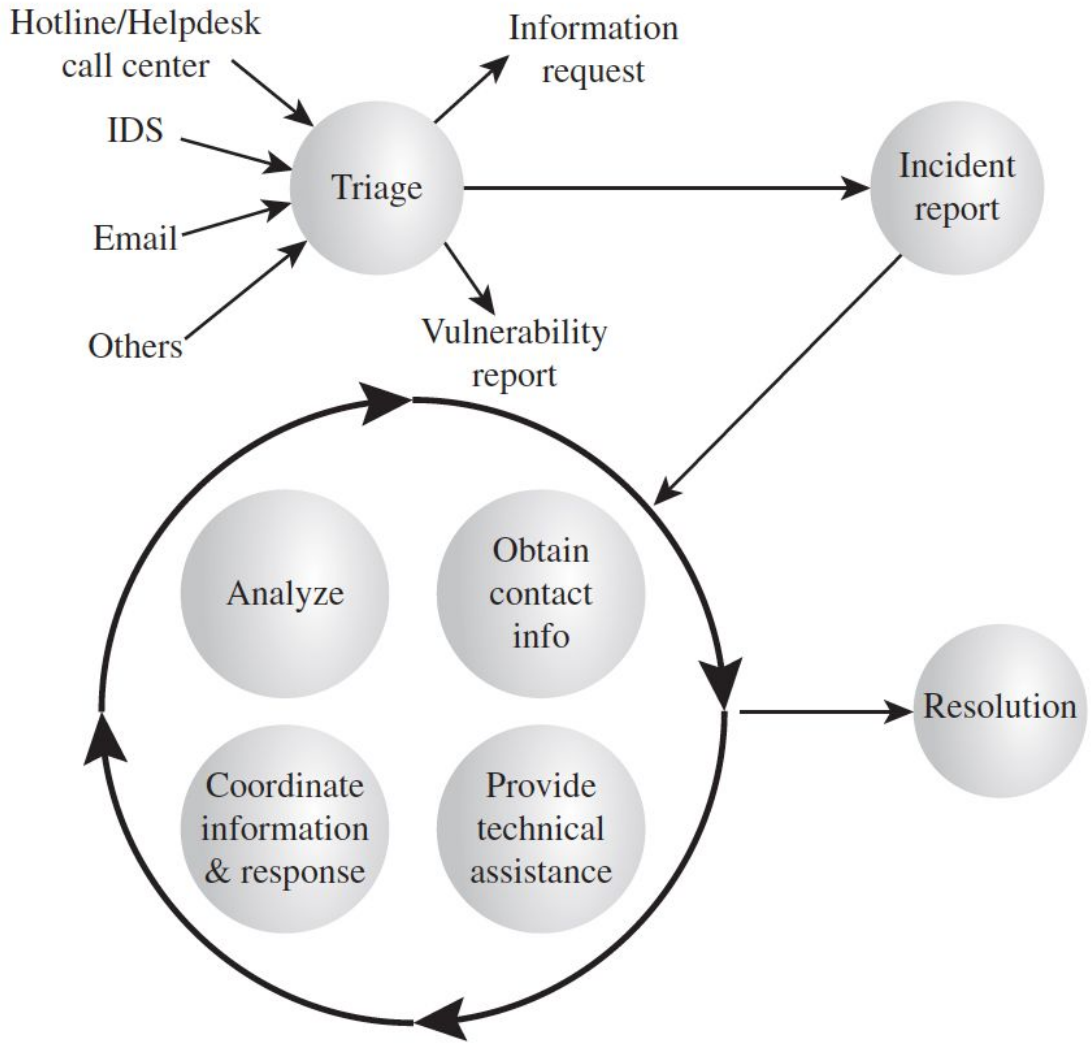
1. help recover from the incident
2. If the incident is reported to the police, then this evidence may also be needed for legal proceedings.

Responding to Incidents

A number of issues should be considered:

- How critical the system is to the organization's function.
- The current and potential technical effect of the incident in terms of how significantly the system has been compromised.

Incident Handling Life Cycle



The cyclic process of IT security management

- Identify what vulnerability led to its occurrence and how this might be addressed to prevent the incident in the future.
- Details of the incident and the response taken are recorded for future reference.
- The impact on the organization's systems and their risk profile must also be reconsidered as a result of the incident
  - A security incident reflects
    - a change in the risk profile of the organization
    - reviewing the risk assessment and controls

Information Flow for Incident Handling 1/3

Service Name	Information flow to incident handling	Information flow from incident handling
Announcements	Warning of current attack scenario	• Statistics or status report • New attack profiles to consider or research.
Vulnerability Handling	How to protect against exploitation of specific vulnerabilities	Possible existence of new vulnerabilities
Malware Handling	• Information on how to recognize use of specific malware • Information on malware impact/threat	• Statistics on identification of malware in incidents • New malware sample

Information Flow for Incident Handling 2/3

Service Name	Information flow to incident handling	Information flow from incident handling
Education/Training	None	Practical examples and motivation Knowledge
Intrusion Detection Services	New incident report	New attack profile to check for
Security Audit or Assessments	Notification of penetration test start and finish schedules	Common attack scenarios
Security Consulting	Information about common pitfalls and the magnitude of the threats	Practical examples/experiences

Information Flow for Incident Handling 3/3

Service Name	Information flow to incident handling	Information flow from incident handling
Risk Analysis	Information about common pitfalls and the magnitude of the threats	Statistics or scenarios of loss
Technology Watch	Warn of possible future attack scenarios Alert to new tool distribution	Statistics or status report New attack profiles to consider or research
Development of Security Tools	Availability of new tools for constituency use	Need for products Provide view of current practices