Incident Response Handling

>

TROFI SECURITY®

INTELLIGENT INFORMATION SECURITY

Session Overview

- Basic Incidents
- Incident Response Methodology
- Incident Response Considerations

Definition of "Incident"

WHAT TO KNOW FIRST:

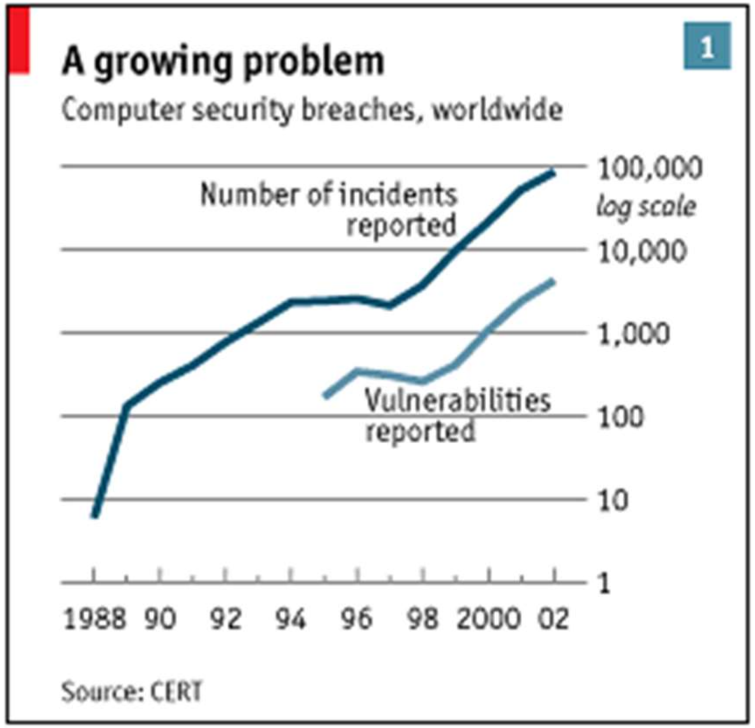
- An incident is an adverse event (or threat of an adverse event) in a computer system
- Adverse events include the following general categories:
  - Compromise of Confidentiality
  - Compromise of Integrity
  - Denial of Resources
  - Intrusions
  - Misuse
  - Damage
  - Hoaxes

What is Incident Handling?

INCIDENTS HAPPEN ALL AROUND US:

- Incident Handling is actions taken to protect and restore the normal operating condition of computers and the information stored in them when an adverse event occurs

The Number of Security-Related Incidents is Escalating



TROFI SECURITY®
INTELLIGENT INFORMATION SECURITY

Reasons For Incident Handling

INCENTIVES FOR EFFICIENT INCIDENT HANDLING:

- Economic
- Protecting Proprietary / Classified / Sensitive Information
- Operational / Business Continuity
- Public Relations
- Legal / Regulatory Compliance
- Safety

Management's Point of View

INCIDENT HANDLING FROM A MANAGER'S POINT OF VIEW:

- Issues:
  - It is often difficult to obtain the necessary resources
  - Incident response is often not done correctly, which can create obstacles for follow up analysis
- Solutions:
  - Careful planning and intelligent justification of incident handling capabilities is imperative

The Bottom Line

INFORMATION SECURITY RISKS CAUSE:

- Direct Financial Loss
- Unfavorable Media Exposure
- Outages and Disruption
- Fraud, Waste and Abuse
- Loss of Valuable Information
- Compromise of Proprietary / Sensitive / Classified Data and Information
- Lawsuits

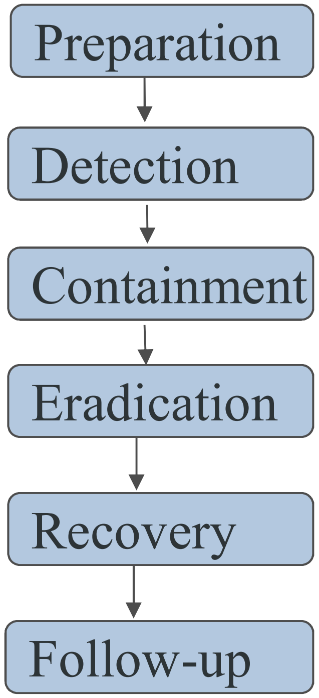
Incident Handling Methodology

WHY USE AN INCIDENT HANDLING METHODOLOGY?

- Provides structure and organization
- Improves efficiency
- Facilitates understanding the process of responding
- Helps dealing with the unexpected

Incident Response Lifecycle

THE INCIDENT RESPONSE LIFECYCLE CONSISTS OF SIX STAGES:



Preparation

Detection

Containment

Eradication

Recovery

Follow-up

High Level Preparation

YOUR DIRECTION:

- Develop an incident response policy (see next slide)
- Create procedures for dealing with incidents as efficiently as possible
- Ensure that a suitable management infrastructure is in place
- Implement a reasonable set of defenses for systems that are to be used in responding to incidents

Preparation - 1

INCIDENT RESPONSE POLICY:

- Is the anchor of an entire incident response effort
- A suitable incident response policy should address/include
- Purpose and objectives
- Scope (to whom does the policy apply and when?)
- Events that are considered/not considered security-related incidents
- Acceptable risk limits
- Roles, responsibilities and authority of incident response effort
- Evaluation criteria
- Reporting requirements

Preparation - 2

HAVE POLICIES AND PROCEDURES REVIEWED BY LEGAL EXPERTS:

- Ensure that existing policies and procedures are current and appropriate--update and expand as necessary
- Have an objective evaluation of your incident response team’s charter, policy, procedures and accomplishments performed!
- Ensure that your team is especially well prepared to deal with incidents you are most likely to encounter
- Participate in FIRST (Forum of Incident Response and Security Teams)--FIRST works only if teams contribute

Preparation - 3

MANAGEMENT’S ROLE:

- Management's responsibilities include ensuring that:
  - Policy and procedures for incident handling are written, well-distributed, and followed
  - Each person who handles incidents is adequately trained
  - Appropriate tasks are assigned to each person who performs incident response duties
  - Each person involved in handling incidents make suitable progress
  - Resources are available to ensure that necessary software tools, hardware and technical personnel are available
  - Contact lists are created and updated
  - Provide Support to Enable Evidence Acquisition

Detection - 1

DETERMINE IF INCIDENT OCCURRED:

- Determine what the problem is and to assess its magnitude
- Major sources of information
- Log files
- Personal firewalls (e.g., Windows Firewall, BlackIce Defender)
- Firewall logs
- Intrusion detection systems (IDSs)
- Analyze all anomalies

Detection - 2

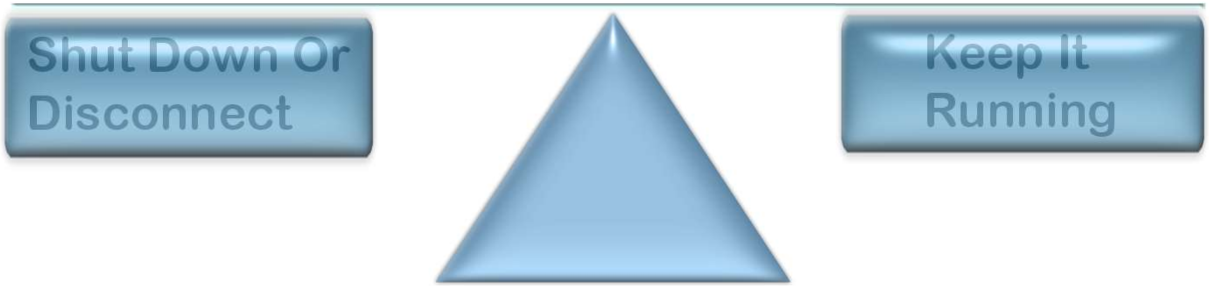
UPON INCIDENT IDENTIFICATION:

- If feasible, promptly obtain full backup and gather a copy of any compromised files/bogus code for analysis
  - In systems in which the likelihood that a security compromise has occurred
- Turn on or increase auditing
- Ensure that the system clock is set correctly
- Start documenting everything that happens
- Initiate notification process
  - Other members of incident response effort
  - Information security contact
  - Public relations office (if warranted by magnitude of incident)
  - Legal department (this is likely to be more appropriate than you might think!)

Containment - 1

DECISIONS AND GOALS:

- To keep incident from spreading
- Important decisions need to be made during this stage (shutting down, disconnecting from a network, monitoring, shunning, setting traps, disabling features, disabling accounts, etc.)



Containment - 2

ACTIVE CONTAINMENT:

- Some users may have to be advised of status of attacked system (avoid using e-mail during network intrusions!)
- Continue to log all activities
- Consider issuing “cease and desist” message
- Try to get users “out of the loop”
- Continue to keep your public relations and legal offices advised (if appropriate)--do not talk directly to the media
- Special considerations apply when proprietary, classified and/or sensitive systems are involved

Eradication

KEY STEPS:

- To eliminate cause of incident
- Be sure to save any copies of malicious programs before deleting them
- May require the use of eradication software
- Clean/reformat disks (if appropriate)
- Ensure that backups are clean
- Continue to document all activities
- Continue to keep your public relations and legal offices advised (if warranted)

Recovery

BUSINESS RESUMPTION:

- To return system / network to mission status
- Follow technical procedures for system recovery
- Users may need to be given an "all clear" message
- Restore data (if appropriate)--may require deletion of all files and a full restore from a backup tape
- All passwords must be changed if there has been administrative level compromise
- Continue to log all activities
- If classified/sensitive/proprietary systems are involved, may require verification of integrity of data stored on systems

Follow-up

MAKE THINGS BETTER:

- Overall goal: to review and integrate information related to incident
- Although the most frequently neglected stage of the computer security process, this stage is potentially the most valuable to the computer security effort
- Perform postmortem analysis of incident
- Reevaluate/modify procedures on basis of "lessons learned“
- Assess time and resources used, and any damage incurred to create monetary cost estimates
- Prepare report(s)
- Support prosecution activity (if applicable)

Hints Moving Forward

HANDY HINTS FOR HANDLING INCIDENTS:

- Verify the incident, ruling out alternative explanations of what has happened
- Follow written procedures during incidents
- Ensure that you have backups very early during the course of an incident
- Coordinate and consult with other technical experts
- Keep management advised of status of incident and your efforts
- Log all activities

Legal Considerations - 1

INCIDENT RESPONSE HAS LEGAL IMPLICATION :

- National laws and directives
- EU directives
- State/province laws
- Civil liabilities
- Legally-advisable practices

Legal Considerations - 2

DOCUMENTATION AS A LEGAL FOUNDATION:

- Start gathering evidence early during an incident's onset
- Always consider the possibility of a coordinated effort with appropriate law enforcement agency
- Don't allow evidence to be contaminated in any way
- Ensure that all evidence is properly accounted for at all times
- Put one person in charge of gathering evidence
- In general, keep the number of people involved to a minimum
- Document virtually everything that you do

Legal Considerations - 3

KEEP GOOD RECORDS:

- Nature of analysis to be performed depends on type of incident than anything else
- Keyword searches are used more than any other type of search
- Some forensics analysis tools support searches using conditional logic
- Be sure to record the results of each search in a special logbook, PDA, voice recorder or incident case handling software programs

Incident Response Team - 1

WHY FORM AN INCIDENT RESPONSE TEAM?

- Information security incidents are becoming increasingly complex--incident handling experts are needed
- Efficiency
- Proactive element
- Agency or corporate requirements
- Liaison function
- May be given authority to engage in activities that a normal organization does not get

Incident Response Team - 2

MOCK INCIDENT RESPONSE EXERCISES:

- Basic notion: execute incident handling procedures by simulating a computer security incident and having employees respond
- Validation of procedures
- “Practice makes perfect”
- Enables you to gauge the magnitude and complexity of the process
- Exercise benefits are greatly increased if there is an external objective observer to identify issues

Incident Response Team - 3

MOCK INCIDENT HANDLING EXERCISES:

- Require development of a variety of incident scenarios
- Record critical data and evaluate
- Should be conducted at regular intervals
- Warning--Carefully plan any mock incident handling exercises to avoid disruption of operational environments

Management’s Responsibility

MANAGING AN INCIDENT PROPERLY IS KEY:

- Over time incident handling becomes a stressful, difficult activity
  - Convey a positive, supportive management style
  - Keep things organized as much as possible
  - Unless you see trouble, don’t constantly intervene in team members’ efforts
- Develop communication channels accordingly
- Take all feedback seriously

Matters That Managers Too Often Overlook - 1

THINGS CHANGE:

- Conducting regular follow-up activity
- Ensuring that the incident response effort is well-aligned with business drivers
- Ensuring that team members document their handling of incidents sufficiently

Matters That Managers Too Often Overlook - 2

KEEP EVERYONE IN THE LOOP THAT NEEDS TO KNOW:

- Initiating vertical communication
- Interdependencies with other organizations
  - Information security
  - IT and business units
  - Telecommunications
  - Public affairs
  - Legal
  - Human resources
  - Business continuity
  - Physical security
  - Others

Technical Considerations

REACT ACCORDINGLY:

- Some incidents occur in large servers with special complications
  - They cannot be taken off-line, OR
  - They have so much storage that it cannot be successfully imaged (or have RAID, so an image will be technically infeasible)
- The best option is still to perform some sort of backup, at least of the suspicious files and logs, then analyze them off-line
- A tape backup will not include all the information such as slack space data, but it may be the only alternative

Session Summary

KNOW WHAT TO DO:

- Computer forensics requires
  - The right hardware and software
  - A great amount of technical proficiency
- To be successful, an incident response effort needs to have a strong proactive element

Questions and Answers

TROFI SECURITY®
INTELLIGENT INFORMATION SECURITY