Incident Response Process Guidelines - For Information Security Management

[1]S. P. DATTA, [2]PRANAB BANERJEE

[1]Prof., Eastern Institute Of Management, Kalyani University, Kolkata, India-700071

[2]Prof., Dept. of Electronics & Telecommunication Engineering, Kolkata, India-700032

E-mail: sp_datta2000@yahoo.co.in, pkbeceju65@gmail.com

ABSTRACT

Attacks on information systems and networks have become more numerous, sophisticated, and severe in recent years. New types of security-related incidents emerge more frequently. While preventing such attacks would be the ideal course of action for organizations, not all information system security incidents can be prevented. Every organization that depends on information systems and networks to carry out its mission should identify and assess the risks to its systems and its information and reduce those risks to an acceptable level [1], [2]. An important component of this risk management process is the trending analysis of past computer security incidents and identifying effective ways to deal with them. An incident response capability is therefore necessary for rapidly detecting incidents, minimizing loss or destruction, mitigating the weakness that were exploited, and restoring the information system. A well-defined incident response capability helps the organization detect incidents rapidly, minimize loss and destruction, identify weaknesses, and restore information technology (IT) operations rapidly.

Because performing incident response effectively is a complex undertaking, establishing a successful incident response capability requires substantial planning and resources. Continuous monitoring of threats through intrusion detection and prevention systems (IDPS) is essential. Establishing clear procedures for assessing the current and potential business impact of incidents is critical, as it is implanting effective methods of collecting, analyzing, and reporting data. Building relationships and establishing suitable means of communication with other internal groups (human resources, legal, etc.) and with external groups like (FISMA, OMB 79, CERT/CC, etc.) are also vital. National Institute of Standards and Technology (NIST) Special Publication (SP 800-61), *Computer Security Incident Handling Guide*, details a four-phase incident response process.

This article seeks to assist organizations in mitigating the risks from computer security incidents by providing practical guidelines on responding to security incidents effectively and efficiently. It includes guidelines on establishing an effective incident response program. Primarily focus has been put in detecting, analyzing, prioritizing and handling incidents. Organizations' agencies CERTS (Computer Security Response Teams) are encouraged to tailor the suggested guidelines to meet their specific security and mission requirements.

1. INTRODUCTION

Overall incident response process life-cycle is segregated into four phases – preparation, detection and analysis, containment/eradication/recovery, and post incident activity[3]. This primarily encompasses the following items:

Organizing a computer security incident response capability;
Handling incidents from initial preparation through the post-incident lessons learned phase;
Handling specific types of incidents
- Denial of Service (DOS)
- Malicious codes

- Unauthorized access
- Inappropriate usage
- Multiple components.

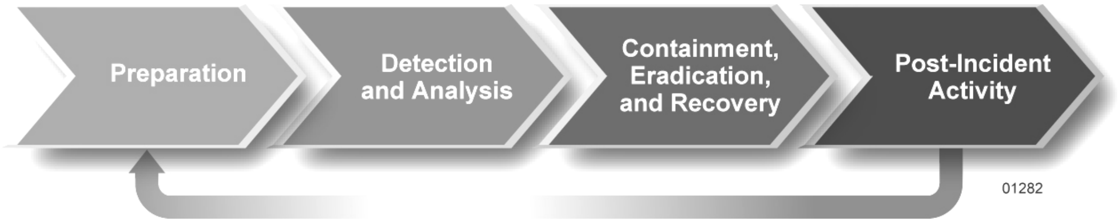

Figure 1. Incident Response Life Cycle

Figure 1 illustrates the incident response life cycle. The initial phase of incident response process involves establishing and training an incident response team, and acquiring the necessary tools and resources. During preparation, the organization also attempts to limit the number of incidents that will occur by selecting and implementing a set of controls based on the result of risk assessments. However, residual risk will inevitably persist after controls are implemented. Detection of security breaches is thus necessary to alert the organization whenever the incident occur. In keeping with the severity of the incident, the organization can act to mitigate the impact of the incident by containing it and ultimately recovering from it. After the incident is adequately handled, the organization issues a report that details the cause and cost of the incident and the steps the organization should take to prevent future incidents.

1.1. PREPARATION

Incident preparation involves not only establishing an incident response capability so that the organization is ready to respond to incidents but also preventing incidents by ensuring that systems, networks, and applications are afforded sufficient security. Incident prevention is now considered a fundamental component of incident response programs, also known as incident management programs, although the incident response team is not typically responsible for it. The incident response team's expertise should be used to establish recommendations for securing systems and preventing incidents, as much as possible. This phase provides basic advice on preparing to handle incidents and on preventing incidents.

1.1.1. PREPARING FOR INCIDENT RESPONSE

Organizing an effective incident response capability involves the participation of many people within the organization. Making the right planning and implementation decisions is key to establishing a successful incident response program. One of the first planning tasks should be to develop an organization-specific definition of the term "incident" so that the scope of the term is clear. Additional tasks that should be performed during the preparation phase include the following:

Create an Incident Response Policy. The policy should define what events are considered incidents, establish the organizational structure for incident response, define roles and responsibilities, and list the organization's incident reporting requirements.

Develop Incident Response and Reporting Procedures. Based on the incident response policy, standard operating procedures (SOPs) are a delineation of the specific technical processes, techniques, checklists, and forms used by the incident response team. SOPs should be comprehensive and detailed to ensure that the organization's priorities are properly reflected in response operations. In addition, following standardized response procedures is also an effective way to minimize errors. Prior to implementation, the organization should test incident response SOPs in order to validate their accuracy and usefulness. Once validated, the SOPs must be widely disseminated throughout the organization. Incidents occur in unpredictable ways; therefore, it is impractical to develop comprehensive procedures with step-by-step instructions for handling every incident. The best that the organization can do is to remain prepared to handle any type of incident, and more specifically, to handle common types of incidents.

Establish Guidelines for Communicating with External Parties. During the incident response process, the organization may need to communicate with outside parties, including other incident response teams, law enforcement, the media, vendors, and external victims. Because such communications often need to occur quickly, organizations should have predetermined communication guidelines so that only the appropriate information is shared with the right parties. However, if sensitive information is inappropriately released, it can lead to greater disruption and financial loss than the incident itself. Creating and maintaining a list of internal and external points of contacts (POC), along with backups for each contact, should assist in making communications among parties easier and faster.

Define Incident Response Team Services. Although the main focus of an incident response team is performing incident response, additional services an incident response team can provide to the organization include security advisory distribution, vulnerability assessment, intrusion detection, and education and awareness.

Adopt a Team Structure and Staffing Model. The organization should adopt the team structure and staffing model best suited to its needs. When contemplating the best team structure and staffing model, an organization need to consider several factors, such as size of the organization, the geographic diversity of major computing resources, the need for 24/7 availability, cost, and staff expertise.

Staff and Train the Incident Response Team. Members of the incident response team should have excellent technical and problem-solving skills because they are critical to the team's success. Excellent teamwork, organizational culture, communication ability, and speaking skills are important as well. Most incident response teams have a team manager and a deputy team manager who assumes authority in the absence of the team manager. In addition, some teams also have a technical lead who assumes oversight of and final responsibility for the quality of the technical work performed by the entire incident response team. Also, larger teams often assign an incident lead as the primary POC for handling a specific incident.

Organizations find difficulties to maintain situational awareness for handling large-scale incidents because of their complexity. Many people within the organization may play a role in the incident response, and the organization may need to communicate promptly and efficiently with various external groups. Collecting, organizing, and analyzing all the pieces of information so that the right decisions can be made and executed are not easy tasks. The key to maintaining situational awareness is to prepare the organization thoroughly to handle large-scale incidents. Two specific actions that support this matter are as follows:

Establish and Maintain Accurate Notification Mechanisms. Organizations should establish, document, maintain, and exercise on-hour and off-hour contact and notification mechanisms for various individuals and groups within the organization (e.g., chief information officer [CIO], head of information security, IT support, business continuity planning) and outside the organization (e.g., incident response organizations, counterparts at other organizations).

Set Written Guidelines for Prioritizing Incidents. Incident response teams should handle each incident with the appropriate priority, based on the criticality of the affected resources and the current and potential technical effect of the incident. For example, data destruction on a user workstation might result in a minor loss of productivity, whereas root compromise of a public Web server might result in a major loss of revenue, productivity, access to services, and reputation, as well as the release of confidential data (credit card numbers, social security numbers, etc.). Because incident responders normally work under stressful conditions ripe for human error, it is important to clearly define and articulate the incident handling priority process. The incident handling priority process should include a description of how the incident response team should react under various circumstances, as well as a service-level agreement (SLA) that documents appropriate actions and maximum response times. This prioritization should facilitate faster and more consistent decision making.

1.1.2. PREPARING TO COLLECT INCIDENT DATA

Organizations should be prepared to collect a set of objective and subjective data for each incident. Over time, the incident data collected by the organization can be used for many ends. For example, data on the total number of hours the incident response team has dedicated to incident response activities and its cost over a particular period of time, may be used to justify additional funding of the incident response team. A study of incident characteristics may reveal systemic security weaknesses and threats, changes in incident trends, or other data that can be used in support of the risk assessment process. Another good use of the data is measuring the success of the incident response team. If incident data is collected and stored properly, it should provide several measures of the success of the incident response team. Furthermore, organizations that are required to report incident information will need to collect the necessary data to meet their requirements.

In the process of preparing to collect incident data, organizations should focus on collecting data that is actionable. Absolute numbers are not informative—understanding how they represent threats to and vulnerabilities of the business processes of the organization is what matters. Organizations should decide what incident data to collect based on reporting requirements and on the expected return on investment from the data (e.g., identifying a new threat and mitigating the related vulnerabilities before they can be exploited).

1.1.3. PREVENTING INCIDENTS

Preventing problems is normally less costly and more effective than reacting to them after they occur. Thus, incident prevention is an important complement to an incident response capability. If security controls are insufficient, high volumes of incidents may occur, overwhelming the resources and capacity for response, which would result in delayed or incomplete recovery, possibly more extensive damage, and longer periods of service unavailability. Incident handling can be performed more effectively if organizations complement their incident response capability with adequate resources to actively maintain the security of networks, systems, and applications. This process is intended to reduce the frequency of incidents, thereby allowing the incident response team to focus on handling serious incidents. Examples of practices that help to prevent incidents are as follows:

- Having a patch management program to assist system administrators in identifying, acquiring, testing, and deploying patches that eliminate known vulnerabilities in system software and application software;

- Hardening all hosts appropriately to eliminate vulnerabilities and configuration weaknesses – adopting the principle of least privilege and elimination of default settings. Warning banners should be displayed whenever a user attempts to gain access to a secure resource. Host should have auditing enabled to log security-related events;

- Configuring the network perimeter to deny all activity that is not expressly permitted;
- Deploying necessary software (licensed) throughout the organization to detect and stop malicious code. Malicious code protection should be deployed at the host level, the application server level, and application client level;

- Making users aware of policies and procedures on the appropriate use of networks, systems, and applications. Improving user awareness regarding incident should reduce the frequency of incident, particularly those involving malicious codes and violations of acceptable use policies.

1.2. DETECTION AND ANALYSIS

Detection and analysis are, for many organizations, the most challenging aspects of the incident response process, in other words, accurately detecting and assessing possible incidents - determining whether an incident has occurred and, if so, the type, extent, and magnitude of the problem. Incidents can be detected through many different means, with varying levels of detail and fidelity. Automated detection capabilities include network-based and host-based intrusion detection and prevention systems (IDPSs), antivirus software, and log analyzers. Incidents may also be detected through manual means, such as user reports. Some incidents have overt signs that can be easily detected, whereas others are virtually undetectable without automation.

In a typical organization, the thousands or millions of possible signs of incidents that occur any given day are recorded mainly by computer security software. Signs of an incident fall into one of two categories: indications and precursors. A precursor is a sign that an incident may occur in the future. An indication is a sign that an incident may have occurred or may be occurring now. Some types of indications that exist are as follows:

- The network intrusion detection sensor alerts when a buffer overflow attempt occurs against an FTP server;
- The antivirus software alerts when it detects that a host is infected with a worm;
- The Web-server crashes;
- User complain of slow access to host on the internet;
- The system administrator sees a filename with unusual characters;
- The user calls the help desk to report a threatening e-mail message;
- The host records an auditing configuration change in its log;
- The application logs multiple failed login attempts from an unfamiliar remote system;
- The e-mail administrator sees a large number of bounced e-mails with suspicious contents;
- The network administrator notices an unusual deviation from typical network traffic.

One should not think of incident detection as being strictly reactive. In some cases, the organization may detect activities that are likely to precede an incident. For example, a network IDPS may record unusual port scan activity targeted at a group of hosts, which occur shortly before a DoS attack is launched against one of the same host. The intrusion detection alerts regarding the scanning activity serve as a precursor of the subsequent DoS incident. Other examples of precursor are:

- Web-server log entries that show the usage of a Web vulnerability scanner;
- An announcement of a new exploit that targets a vulnerability of the organization's mail server;
- A threat from a hacktivist group that the group will attack the organization.

Not every attack can be detected through precursors. If precursors are detected, the organization may have an opportunity to prevent the incident (by altering its security posture through automated or manual means).

Automation is needed to perform an initial analysis of the detected data and select events of interest for human review. Event correlation software and centralized logging can be of great value in automating the analysis process. However, the effectiveness of the process depends on the quality of the data that goes into it. Organizations should establish logging standards and procedures to ensure that adequate information is collected by logs and security software and that the data is reviewed regularly. Proper and efficient reviews of incident-related data require people with extensive, specialized technical knowledge and experience.

When a potential incident is identified, the incident response team should work quickly to analyze and validate it, documenting each step taken. The team should rapidly perform an initial analysis to determine the incident's scope, attack methods, and targeted vulnerabilities. Performing the initial analysis and validation is challenging. The recommendations for making incident analysis easier and more effective are as below:

- Profile networks and systems;
- Understand normal behavior;
- Use centralized logging and establish a log retention policy;
- Perform event correlation;
- Keep all host clocks synchronized;
- Maintain and use a knowledge base of information;
- Use Internet search engines for research;
- Run Packet Sniffers to collect additional data;
- Consider filtering the data;
- Create a Diagnosis Matrix for less experienced staff as per Table 1;
- Seek assistance from others.

Organizations need to quantify the effect of its own incidents. To assign a severity rating for an incident, organizations should first determine the effect ratings and criticality ratings for the incident, based on Tables 2 and 3.

Table 1. Excerpt of a Sample Diagnosis Matrix

Symptom	Denial of Service	Malicious Code	Unauthorized Access	Inappropriate Usage
Files, critical, access attempts	Low	Medium	High	Low
Files, inappropriate content	Low	Medium	Low	High
Host crashes	Medium	Medium	Medium	Low
Port scans, incoming, unusual	High	Low	Medium	Low
Port scans, outgoing, unusual	Low	High	Medium	Low
Utilization, bandwidth, high	High	Medium	Low	Medium
Utilization, e-mail high	Medium	High	Medium	Medium

Table 2. Effect Rating Definitions

Value	Rating	Definition
0.00	None	No effect on a single agency, multiple agencies, critical infrastructure
0.10	Minimal	Negligible effect on a single agency
0.25	Low	Moderate effect on a single agency
0.50	Medium	Severe effect on single agency, negligible effect on multiple agencies or critical infrastructure
0.75	High	Moderate effect on multiple agencies or critical infrastructure
1.00	Critical	Severe effect on multiple agencies or critical infrastructure

Table 3. Criticality Rating Definitions

Value	Rating	Definition
0.10	Minimal	Non-critical system, systems, or infrastructure
0.25	Low	System or systems that support a single agency’s mission (DNS servers, domain controllers), but are not mission critical
0.50	Medium	System or systems that are mission critical to a single agency
0.75	High	System or systems that support multiple agencies or sectors of the critical infrastructures (root DNS servers)
1.00	Critical	System or systems that are mission critical to multiple agencies or critical infrastructure

This analysis should provide enough information for the team to prioritize subsequent activities, including the containment of the incident. When in doubt, incident handlers should assume the worst until additional analyses indicate otherwise. In addition to prioritization guidelines, organizations should also establish an escalation process for those instances when the incident response team fails to respond to an incident within the designated time.

The incident response team should maintain records about the status of incidents, along with other pertinent information. Using an application or database for this purpose is necessary to ensure that incidents are handled and resolved in a timely manner. The incident response team should safeguard this data and other data related to incidents because it often contains sensitive information concerning recent security breaches, exploited vulnerabilities, and users that may have performed inappropriate actions.

1.3. CONTAINMENT, ERADICATION AND RECOVERY

It is important to contain an incident before it spreads to avoid overwhelming resources and increasing damage caused by the incident. Most incidents require containment, so it is important to consider it early in the course of handling each incident. An essential part of containment is decision making, such as shutting down a system, disconnecting it from the network, or disabling certain system functions. Such decisions are much easier to make if strategies and procedures for containing the incident have been predetermined. Organizations should define acceptable risks in dealing with incidents and develop strategies accordingly.

Containment strategies vary based on the type of incident. For example, the overall strategy for containing an e-mail-borne virus infection is quite different from that of a network-based distributed denial of service attack. Organizations should create separate containment strategies for each major type of incident. The criteria for choosing the appropriate strategy should be documented clearly to facilitate quick and effective decision making. Examples of criteria include potential damage to and theft of resources, the need to preserve evidence, the effectiveness of the strategy, the time and resources needed to implement the strategy, and the duration of the solution.

In certain cases, some organizations delay the containment of an incident so that they can monitor the attacker's activity, usually to gather additional evidence. If an organization knows that a system has been compromised and allows the compromise to continue, it may be liable if the attacker uses the compromised system to attack other systems.

After an incident has been contained, eradication may be necessary to eliminate components of the incident, such as deleting malicious code and disabling breached user accounts. For some incidents, eradication is either unnecessary or is performed during recovery. In recovery, administrators restore systems to normal operation and (if applicable) harden systems to prevent similar incidents. Recovery may involve such actions as:

- Restoring systems from clean backups;
- Rebuilding systems from scratch;
- Replacing compromised files with clean versions;
- Installing patches;
- Changing passwords; and
- Tightening network perimeter security.

It is also often desirable to employ higher levels of system logging or network monitoring as 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.

1.4. POST-INCIDENT ACTIVITY

After a major incident has been handled, the organization should hold a lessons-learned meeting to review the effectiveness of the incident handling process and identify necessary improvements to existing security controls and practices. Lessons-learned meetings should also be held periodically for lesser incidents. Questions to be answered in the lessons learned meeting include:

- Exactly what happened, and at what time?
- How well did staff and management perform in dealing with the incident? Were the documentation procedures followed? Were they adequate?
- What information was needed sooner?
- Were any actions taken that might have inhibited recovery?
- What would the staff and management do differently the next time a similar incident occurs?
- What corrective actions can prevent similar incidents in future?
- What additional tools or resources are needed to detect, analyze, and mitigate future incidents?

The information accumulated from all lessons-learned meetings, as well as the data collected while handling each incident, should be used to identify systemic security weaknesses and deficiencies in policies and procedures. Follow-up reports generated for each resolved incident can be important for evidentiary purposes, used as a reference in handling future incidents, and used in training new incident response team members. An incident database, with detailed information on each incident that occurs, can be another valuable source of information for incident handlers.

2. CONCLUSION

The major steps to be performed in the initial handling of an incident (*categorized*) are:

- Determine whether an incident has occurred
  Analyze the precursors and indicators,
  Look for correlating information,
  Perform research (e.g., search engines, knowledge base),
  As soon as the handler believes an incident has occurred, start documenting the investigation and gathering evidence;

- Classify the incident using the categories presented (e.g., denial of service, malicious code, unauthorized access, inappropriate usage, multiple component);
- Follow the appropriate incident category checklist.

The items address only the detection and analysis of an incident; after that has been completed, incident responders should use checklists that are geared toward a particular type of incident. The steps followed for handling incidents (*uncategorized*) that do not fit into any of the aforesaid five categories are:

- Prioritize handling the incident based on the business impact

Identify which resources have been affected and forecast which resources will be affected,

Estimate the current and potential technical effect of the incident,

Find the appropriate cell in the prioritization matrix, based on the technical effect and affected resources;

- Report the incident to the appropriate internal personnel and external organizations;
- Acquire, preserve, secure, and document evidence;
- Contain the incident;
- Eradicate the incident

Identify and mitigate all vulnerabilities that were exploited,

Remove malicious code, inappropriate materials, etc.;

- Recover from the incident.

REFERENCES:

1. National Institute of Standards and Technology Special Publication 800-30, *Risk Management Guide for Information Technology Systems*, July 2002.

2. Federal Information Processing Standard 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.

3. National Institute of Standards and Technology Special Publication 800-61, *Computer Security Incident Handling Guide*, January 2003.

4. ISO/IEC International Standard ISO/IEC 17799, *Information Technology – Code of Practice for Information Security Management*, February 2001.

5. National Security Agency (UK), The NSA Security Manual.

6. Information System Security Association (USA), *Generally Accepted Information Security Principles, Version 3.0.*

7. Julia Allen, *The CERT Guide to System and Network Security Practice*, Addison Wesley, Boston.

8. Micky Krause and Harold Tripton, *Information Security Management Handbook*, Auerbach, Boca Raton, Fl.