ARTEMIS
Advanced Reactive Threat Elimination and Monitoring Integrated System

Computer Security Incident Handling Guide

Inspired by the recommendations of the National Institute of Standards and Technology

Sarang Shigwan
Atharva Kanawade
Praful Jadhao

Table of Contents

Executive Summary

This document provides guidelines for mitigating risks from computer security incidents. It assists organizations in responding to incidents effectively and efficiently, including establishing an incident response program, and detecting, analyzing, prioritizing, and handling incidents.

Introduction

1.1 Context

Cyber security relates to the confidentiality, availability and integrity of information and data that is processed, stored and communicated by electronic or similar means, and protecting it and associated systems from external or internal threat.

It is commonly recognized that cyber security involves the protection of critical information and ICT infrastructure, including supervisory control and data acquisition (SCADA) systems and industrial control systems (ICS), through the alignment of people, processes and tools.

This document supports organization in managing contemporary cyber threats and incidents. The application of this document will support organization in reducing the scope, impact and severity of cyber incidents.

1.2 Purpose and Scope

This publication seeks to assist the organization in mitigating the risks from computer security incidents by providing practical guidelines on responding to incidents effectively and efficiently. It includes guidelines on establishing an effective incident response program, but the primary focus of the document is detecting, analyzing, prioritizing, and handling incidents.

1.3 Authority

This guideline has been prepared for use by XYZ agencies. It may be used by non-governmental organizations or businesses on a voluntary basis and is a subject to copyright. Not even the makers of this document can access any confidential information filled in the appendices.

1.4 Audience

This document has been created for computer security incident response teams (CSIRTs), system and network administrators, security staff, technical support staff, chief information security officers (CISOs), chief information officers (CIOs), computer security program managers, and others who are responsible for preparing for, or responding to security incidents of the organization.

1.5 Compliance Requirements (Auto-generated)

Organizing a Computer Security Incident Response Capability

Organizing an effective computer security incident response capability (CSIRC) involves several major decisions and actions. One of the first considerations should be to create an organization-specific definition of the term “incident” so that the scope of the term is clear.

The organization should decide what services the incident response team should provide, consider which team structures and models can provide those services, and select and implement one or more incident response teams. Incident response plan, policy, and procedure creation is an important part of establishing a team, so that incident response is performed effectively, efficiently, and consistently, and so that the team is empowered to do what needs to be done.

This section provides guidelines for establishing incident response capabilities, and advice on maintaining and enhancing existing capabilities.

2.1 What is a computer security incident?

A computer security incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.

Examples of incidents are:

- An attacker commands a botnet to send high volumes of connection requests to a web server, causing it to crash.
- Users are tricked into opening a “quarterly report” sent via email that is actually malware.
- An attacker obtains sensitive data and threatens that the details will be released publicly.
- A user provides or exposes sensitive information to others through peer-to-peer file sharing services.

2.2 Need for Incident Response

The organization has a fully staffed internal CSIRT and SOC to ensure 24/7 incident detection and response capabilities.

Attacks frequently compromise personal and business data. Incident response supports responding to incidents systematically, minimizing loss or theft of information and disruption of services.

2.3 Incident Response Team Structure

An incident response team should be available for anyone who discovers or suspects an incident. The team handles the incident, analyzes the data, determines the impact, and acts to limit the damage and restore normal services. The team's success depends on the participation and cooperation of individuals throughout the organization.

The organization has a fully staffed internal CSIRT and SOC to ensure 24/7 incident detection and response capabilities.

2.3.1 Team Models

Possible structures for an incident response team include:

- Central Incident Response Team: A single team handles incidents throughout the organization.
- Distributed Incident Response Teams: Multiple teams, each responsible for a segment of the organization.
- Coordinating Team: An incident response team provides advice to other teams without having authority over those teams

Incident response teams can also use any of three staffing models:

- Employees: The organization performs all of its incident response work.
- Partially Outsourced: The organization outsources portions of its incident response work.
- Fully Outsourced: The organization completely outsources its incident response work.

2.3.2 Team Model Selection

When selecting appropriate structure and staffing models, organizations should consider factors such as:

- The Need for 24/7 Availability.
- Full-Time Versus Part-Time Team Members.

- Employee Morale.
- Cost.
- Staff Expertise.
- Current and Future Quality of Work.
- Division of Responsibilities.
- Sensitive Information Revealed to the Contractor.
- Lack of Organization-Specific Knowledge.
- Lack of Correlation.
- Handling Incidents at Multiple Locations.
- Maintaining Incident Response Skills In-House

2.3.3 Incident Response Personnel

A single employee, with one or more designated alternates, should be in charge of incident response. The managers typically perform a variety of tasks, including acting as a liaison with upper management and other teams and organizations, defusing crisis situations, and ensuring that the team has the necessary personnel, resources, and skills.

Team members should have excellent technical skills (e.g., system administration, network administration) and problem-solving skills. It is helpful to have some team members specialize in particular technical areas, such as network intrusion detection, malware analysis, or forensics.

Incident response team members should also have teamwork and communication skills.

2.3.4 Incident Response Team Services

The main focus of an incident response team is performing incident response. Other services a team might offer include:

- Intrusion Detection.
- Advisory Distribution.
- Education and Awareness.
- Information Sharing.

Handling an Incident

The incident response process has several phases: preparation, detection and analysis, containment, eradication and recovery, and post-incident activity.

Figure 3-1 illustrates the incident response life cycle.

3.1 Preparation

Incident response methodologies emphasize preparation—establishing an incident response capability and preventing incidents.

3.1.1 Preparing to Handle Incidents

Incident Handler Communications and Facilities:

- Contact information for team members.
- On-call information for other teams within the organization.
- Incident reporting mechanisms.
- Issue tracking system.
- Smartphones for off-hour support.
- Encryption software.
- War room for central communication and coordination.
- Secure storage facility.

Incident Analysis Hardware and Software:

- Digital forensic workstations and backup devices.
- Laptops.
- Spare workstations, servers, and networking equipment.
- Portable printer.
- Packet sniffers and protocol analyzers.
- Digital forensic software.
- Removable media.
- Evidence gathering accessories.

Incident Analysis Resources:

- Port lists.
- Documentation for OSs, applications, protocols, and intrusion detection and antivirus products.

- Network diagrams and lists of critical assets, such as database servers.
- Current baselines of expected network, system, and application activity.
- Cryptographic hashes of critical files.

3.1.2 Preventing Incidents

3.1.3 Containment Strategy (Auto-generated)

3.3 Threat-Specific Response (Auto-generated)

Keeping the number of incidents reasonably low is very important to protect the business processes of the organization. If security controls are insufficient, higher volumes of incidents may occur, overwhelming the incident response team.

Some of the main recommended practices for securing networks, systems, and applications:

- Risk Assessments.
- Host Security.
- Network Security.
- Malware Prevention.
- User Awareness and Training.

Detection and Analysis

3.2.1 Attack Vectors

Organizations should be generally prepared to handle any incident but should focus on being prepared to handle incidents that use common attack vectors. Common attack vectors include:

- External/Removable Media
- Attrition
- Web
- Email
- Impersonation
- Improper Usage
- Loss or Theft of Equipment
- Other

3.2.2 Signs of an Incident

For many organizations, the most challenging part of the incident response process is accurately detecting and assessing possible incidents.

Common indicators of an attack include:

- Web server log entries that show the usage of a vulnerability scanner
- An announcement of a new exploit
- A threat from a group stating that the group will attack the organization.

Examples of indicators are:

- A network intrusion detection sensor alerts.
- Antivirus software alerts.
- A system administrator sees a filename with unusual characters.
- A host records an auditing configuration change in its log.
- An application logs multiple failed login attempts.
- An email administrator sees a large number of bounced emails with suspicious content
- A network administrator notices an unusual deviation from typical network traffic flows.

3.2.3 Incident Analysis

Each indicator should be evaluated to determine if it is legitimate. The following are recommendations for making incident analysis easier and more effective:

- Profile Networks and Systems.
- Understand Normal Behaviors.
- Create a Log Retention Policy.

3.3 Threat-Specific Response (Auto-generated)

Coordination and Information Sharing

Coordination

The incident response team needs to coordinate its activities with other groups, both inside and outside the organization.Here are some of the parties within the organization with whom the incident response team may interact:

- Senior management
- Legal department
- Public relations
- Internal audit
- Physical security personnel
- Human resources

Information Sharing Techniques

Sharing incident-related information with other organizations can be beneficial. Common techniques include:

- Ad Hoc
- Partially Automated

Security Considerations

Organizations should consider the following security issues when sharing incident-related information:

- Granular Information Sharing
- Business Impact Information
- Technical Information

List of Appendices

- Appendix A— Situation update (template)
- Appendix B— Resolution Action Plan (template)
- Appendix C— Evidence Register (template)
- Appendix D— Assets and Key Contacts (template)
- Appendix E— Glossary

Appendix A—Situation update (template)

Date/Time	Update	Submitted By
[Date/Time of update]	[Details of the situation update]	[Name of person submitting update]
[Date/Time of update]	[Details of the situation update]	[Name of person submitting update]
[Date/Time of update]	[Details of the situation update]	[Name of person submitting update]

Appendix B—Resolution Action Plan (template)

Step #	Action	Assigned To	Target Date/ Time	Completion Date/Time	Status
[Step Number]	[Description of action]	[Name of person assigned]	[Target date/ time]	[Completion date/time]	[Status of action]
[Step Number]	[Description of action]	[Name of person assigned]	[Target date/ time]	[Completion date/time]	[Status of action]
[Step Number]	[Description of action]	[Name of person assigned]	[Target date/ time]	[Completion date/time]	[Status of action]

Appendix C—Evidence Register (template)

Evidence ID	Item Description	Date/Time Collected	Collected By	Location	Chain of Custody
[Evidence ID]	[Description of evidence item]	[Date and time of collection]	[Name of collector]	[Location where evidence was collected]	[Record of evidence transfer and handling]
[Evidence ID]	[Description of evidence item]	[Date and time of collection]	[Name of collector]	[Location where evidence was collected]	[Record of evidence transfer and handling]
[Evidence ID]	[Description of evidence item]	[Date and time of collection]	[Name of collector]	[Location where evidence was collected]	[Record of evidence transfer and handling]

Appendix D—Assets and Key Contacts (template)

GENERATOR		SCADA PLC RTU		CLIENT ENVIRONMENT	
HARDWARE/ LOCATION	**FIXED/ PORTABLE, CAPACITY (KVA), FUEL TYPE/ CAPACITY**	**HARDWARE/ FIRMWARE/ LOGS & LOCATIONS**	**AUTHENTICATION METHODS & CONT**	**OS/LOGS & LOCATIONS**	**CLIEN HARD MANU MODE**
[GENERATOR HARDWARE/ LOCATION]	[FIXED OR PORTABLE, CAPACITY (KVA), FUEL TYPE / CAPACITY]	[SCADA PLC RTU HARDWARE / FIRMWARE / LOGS & LOCATIONS]	[AUTHENTICATION METHODS & CONT]	[CLIENT ENVIRONMENT OS / LOGS & LOCATIONS]	[CLIEN HARD MANU MODE
[GENERATOR HARDWARE/ LOCATION]	[FIXED OR PORTABLE, CAPACITY (KVA), FUEL TYPE/ CAPACITY]	[SCADA PLC RTU HARDWARE / FIRMWARE / LOGS & LOCATIONS]	[AUTHENTICATION METHODS & CONT]	[CLIENT ENVIRONMENT OS / LOGS & LOCATIONS]	[CLIEN HARD MANU MODE

DISASTER RECOVERY PLAN	
IDENTIFIED	**KEY CONTACTS**
[DISASTER RECOVERY PLAN IDENTIFIED]	[DISASTER RECOVERY PLAN KEY CONTACTS]

Appendix E—Glossary

Baselining: Monitoring resources to determine typical utilization patterns.

Computer Security Incident: A violation or imminent threat of violation of computer security policies.

Computer Security Incident Response Team (CSIRT): A capability set up for the purpose of assisting in responding to computer security-related incidents.

Event: Any observable occurrence in a network or system.

False Positive: An alert that incorrectly indicates that malicious activity is occurring.

Incident: A violation or imminent threat of violation of computer security policies.

Incident Handling: The mitigation of violations of security policies and recommended practices.

Indicator: A sign that an incident may have occurred or may be currently occurring.

Intrusion Detection and Prevention System (IDPS): Software that automates the process of monitoring events and analyzing them for signs of possible incidents.

Malware: A virus, worm, Trojan horse, or other code-based malicious entity that successfully infects a host.

Precursor: A sign that an attacker may be preparing to cause an incident.

Profiling: Measuring the characteristics of expected activity.

Signature: A recognizable, distinguishing pattern associated with an attack.

Social Engineering: An attempt to trick someone into revealing information that can be used to attack systems or networks.

Threat: The potential source of an adverse event.

Vulnerability: A weakness in a system, application, or network that is subject to exploitation or misuse.