Cybersecurity: Incident Response Short

Student Guide

August 2017

Center for Development of Security Excellence

Contents

Lesson 1: Incident Response

Introduction

"By failing to prepare, you are preparing to fail." Benjamin Franklin

"The more you know about the past, the more prepared you are for the future." Theodore Roosevelt

"A man who does not plan long enough ahead will find trouble at his door." Confucius

"If you aim at nothing, you will hit it every time." Zig Ziglar

Preventing a cyberattack is usually less expensive and more effective than trying to respond to one after it has occurred. In 2016, 71% of companies were affected by a successful cybersecurity attack. Yet, only 46% have an incident response plan, and only 44% believe that they could detect a sophisticated attack.

With cyberattack attempts both increasing and sophisticating, chances are that some attempts will be successful—leading to downtime, disruption, loss or compromise of data, and cost. Building strong incident response capability, anchored on a comprehensive incident response plan, is the most effective way to address a successful cybersecurity attack.

This session covers how to respond successfully to cybersecurity attacks by developing incident response capability through policy, planning, and processes. Welcome to CDSE's Short on the importance of and approaches to building an effective response capability.

Incident Definition

An incident is an occurrence that:

- Actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or
- Constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

It is important to differentiate cybersecurity incidents from events:

- Incidents are cyber activities that deliberately or inadvertently threaten or negatively impact the confidentiality, integrity, or availability of a system and that are alerted and notified through proper channels.
- Events are changes to the normal behavior or environment, such as updates and installations.

Federal law requires federal agencies to report incidents to US CERT (US Computer Emergency Readiness Team). Data to be reported includes: the current level of impact on agency functions or services; the type of information lost, compromised, or corrupted; the scope of time and resources needed to recover from the incident; when the activity was first detected; the number of systems, records, and users impacted; the network location of the observed activity; and a point of contact.

In Category 1, or CAT 1 Unauthorized Access, an individual gains logical or physical access without permission to a federal agency network, system, application, data, or other resource.

Category 2, or CAT 2 Denial of Service, designates an attack that successfully prevents or impairs the normal authorized functionality of networks, systems or applications by exhausting resources. This activity includes being the victim or participating in the Denial of Service.

Category 3, or CAT 3 Malicious Code, applies to successful installation of malicious software (e.g., virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system or application. Agencies are NOT required to report malicious logic that has been successfully quarantined by antivirus software.

Category 4, or CAT 4 Improper Usage applies to incidents where a person violates acceptable computing use policies.

Category 5, or CAT 5 Scans/Probes/Attempted Access, includes any activity that seeks to access or identify a federal agency computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or denial of service.

Review Activity 1

Users are tricked into opening a “quarterly report” sent via email that is actually malware; running the tool has infected their computers and established connections with an external host.

Determine if this scenario is an incident or an event. Check your answer in the Answer Key at the end of this Student Guide.

- ○ *Incident*
- ○ *Event*

A firewall has blocked a connection attempt.

Determine if this scenario is an incident or an event. Check your answer in the Answer Key at the end of this Student Guide.

- ○ *Incident*
- ○ *Event*

A power failure has led to loss of data.

Determine if this scenario is an incident or an event. Check your answer in the Answer Key at the end of this Student Guide.

- ○ *Incident*
- ○ *Event*

A user provides or exposes sensitive information to others through peer-to-peer file sharing services.

Determine if this scenario is an incident or an event. Check your answer in the Answer Key at the end of this Student Guide.

- ○ *Incident*
- ○ *Event*

An attacker commands a botnet to send high volumes of connection requests to a web server, causing it to crash.

Determine if this scenario is an incident or an event. Check your answer in the Answer Key at the end of this Student Guide.

- ○ *Incident*
- ○ *Event*

Incident Response Capability Requirement

Before an incident occurs, it is important to develop comprehensive incident response capability. This advance preparation:

- Supports responding to incidents systematically,
- Helps personnel minimize loss or theft of information and/or disruption of service,
- Provides the ability to use information gained during incident handling to better prepare for handling future incidents,
- Deals properly with legal issues that may arise, and
- For federal departments and agencies, addresses the law, regulation, and policy directing a coordinated, effective defense against information security threats.

Requirements for incident response capability reside in various policies.

OMB Circular Number A-130, Appendix 3 was released in 2000. This policy directs federal agencies to ensure that there is a capability to provide help to users when a security incident occurs in the system and to share information concerning common vulnerabilities and threats.

This capability shall share information with other organizations and should assist the agency in pursuing appropriate legal action, consistent with Department of Justice guidance.

From 2002 and updated in 2014, the Federal Information Security Management Act, or FISMA, requires agencies to have procedures for detecting, reporting, and responding to security incidents and establishes a centralized Federal information security incident center, in part to: "Provide timely technical assistance to operators of agency information systems…including guidance on detecting and handling information security incidents, compile and analyze information about incidents that threaten information security, and inform operators of agency information systems about current and potential information security threats, and vulnerabilities."

The Federal Information Processing Standards, or FIPS, 200, *Minimum Security Requirements for Federal Information and Information Systems 5* from March 2006 specifies minimum security requirements for Federal information and information systems, including incident response. The specific requirements are defined in NIST Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*.

OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information, from* May 2007 provides guidance on reporting security incidents that involve PII.

Policy, Plan, and Process for Incident Capability

Each organization should define its own policy to govern its incident response and build its incident response capability. Most policies include several common elements such as:

- A statement of management commitment,
- The purpose and objectives of the policy,
- The scope of the policy,
- Definitions related to incidents and related terminology,
- Defined structure, roles, responsibilities, and levels of authority related to incident response,
- Prioritization or severity ratings,
- Performance measures, and
- Reporting and contact forms.

One of the critical elements of incident response capability is an incident response plan that outlines an approach for building the capability and preparing for effective response after a cyberattack occurs. A comprehensive incident response plan should include eight common elements:

- The Mission is a clear statement of purpose related to incident response capability.

- The Strategies and Goals section defines the overall aims and intended outcomes of the incident response capability.
- Senior Management Approval defines the required sign-offs and validation to an Incident Response Plan.
- The Approach section outlines the roles and personnel, critical processes, and required resources necessary to respond to incidents as they arise. This includes designation of an incident response team.
- The Communications portion defines how the designated incident response team will communicate with the rest of the organization and with other organizations and include an approach for notifying proper parties, internally and externally, about an incident.
- The Metrics section defines an approach for measuring the incident response capability and its effectiveness. These metrics should include key performance indicators that demonstrate the efficacy and effectiveness of incident response.
- A Roadmap section outlines a strategy for continuously developing and improving incident response and maturing it over time. This roadmap should address developing the skills of members of an incident response team to keep pace with changes and advances.
- The Fit and Alignment section designates how the Incident Response Plan aligns and integrates with the structure and practices of the organization.

Incident response processes should align with designated policies and plans. They should also delineate the procedures, protocols, and forms to be completed when an incident occurs. The Computer Security Incident Response Handling Guide, Recommendations of the National Institute of Standards and Technology, Special Publication 800-61, Revision 2, is available at the following link: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf. It contains helpful guidance for implementing effective incident response.

An effective incident response process addresses a comprehensive approach for handling an incident from the time of its identification and reporting through resolution. The trigger is the reporting of an incident. The designated incident response team should subsequently:

- Assess the incident,
- Contain it so that it does not continue to cause damage,
- Determine its severity,
- Preserve all evidence particularly about the origin,
- Initiate communications to notify other agencies,

- Recover any impacted data and information, and
- Assess the complete impact include cost and damages

Note that these steps may occur simultaneously and may require involving other parties. Going forward, any incident should include some reflection on lessons learned to update policies and training and improve the overall incident response capability.

Incident Scenario

Let's examine a sample incident and determine appropriate responses.

On a Tuesday night, a database administrator performs some off-hours maintenance on several production database servers. The administrator notices some unfamiliar and unusual directory names on one of the servers. After reviewing the directory listings and viewing some of the files, the administrator concludes that the server has been attacked.

Review Activity 2

What is the first activity the database administrator should perform in this situation?

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ Report the incident to US CERT.
- ○ Determine when the access started.
- ○ Report the incident internally to the incident response team.
- ○ Consult the lessons learned from previous incidents to determine the best approach.

What information should be reported to US CERT in this situation?

Select all that apply. Check your answers in the Answer Key at the end of this Student Guide.

- ☐ The current level of impact on agency functions or services.
- ☐ Lessons learned from previous incidents.
- ☐ The type of information lost, compromised, or corrupted.
- ☐ The scope of time and resources needed to recover from the incident.
- ☐ The name(s) of the individual(s) who first detected the incident.
- ☐ When the activity was first detected.
- ☐ The number of systems, records, and users impacted.
- ☐ The network location of the observed activity.
- ☐ A point of contact.

What work should the incident response team perform in this situation?

Select all that apply. Check your answers in the Answer Key at the end of this Student Guide.

- ☐ Assess.
- ☐ Determine Impact.
- ☐ Contain.
- ☐ Establish Strategies and Goals.
- ☐ Update Policy and Training.
- ☐ Recover.
- ☐ Create a Roadmap.
- ☐ Determine Severity.
- ☐ Preserve Evidence.
- ☐ Initiate Communications.

How would the incident response team's activities change if this situation was determined to be an event rather than an incident?

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ No changes apply. All activities associated with incidents also apply to events.
- ○ No reporting to US CERT is required for events.
- ○ All activities would change.

Conclusion

In summary, it is not possible to predict and plan for every incident. Building an incident response capability is the best defense. Key elements to that capability include support, knowledge and skill, and a relevant plan.

Support: Be sure to secure leadership support for building the capability, in the beginning and ongoing, and keep all users updated.

Knowledge and Skill: Train for and practice how to respond to incidents:

- Simulate cyberattacks and conduct drills to test incident response capabilities.
- Conduct scenario-based training and technical skill building for members of an incident response team.
- Keep the incident response team current with changing cyberattack tactics and techniques.

- Facilitate after action reviews to discuss insights and lessons from incidents for leverage in future attacks.

Relevant Plan: Keep the incident response plan current by:

- Including specific guidelines for likely incident response scenarios,
- Defining a process for major decisions that may apply during an incident response, and
- Reviewing and updating the incident response plan to keep it current with changes in the organization and changing cyberattack tactics and techniques.

Congratulations! You have completed CDSE's Short on responding to cyber attacks by developing incident response capability.

Appendix A: Answer Key

Review Activities

Review Activity 1

Users are tricked into opening a “quarterly report” sent via email that is actually malware; running the tool has infected their computers and established connections with an external host.

Determine if this scenario is an incident or an event.

- ⦿ Incident
- ○ Event

***Feedback**: This situation is a cybersecurity incident due to the trickery.*

A firewall has blocked a connection attempt.

Determine if this scenario is an incident or an event.

- ○ Incident
- ⦿ Event

***Feedback:** In this case, the firewall functioned properly, and no data was threatened.*

A power failure has led to loss of data.

Determine if this scenario is an incident or an event.

- ○ Incident
- ⦿ Event

***Feedback:** While data was lost, it was not a violation of security policies or standard security practices.*

A user provides or exposes sensitive information to others through peer-to-peer file sharing services.

Determine if this scenario is an incident or an event.

- ⦿ Incident
- ○ Event

***Feedback**: The user’s actions threaten data security.*

An attacker commands a botnet to send high volumes of connection requests to a web server, causing it to crash.

Determine if this scenario is an incident or an event.

- ⦿ Incident
- ○ Event

***Feedback**: The attacker compromised the system.*

Review Activity 2

What is the first activity the database administrator should perform in this situation?

- ○ Report the incident to US CERT.
- ○ Determine when the access started.
- ⦿ Report the incident internally to the incident response team.
- ○ Consult the lessons learned from previous incidents to determine the best approach.

***Feedback:** The first response is to notify the internal incident response team to assess and contain the issue. The incident response team should subsequently notify US CERT, determine when the access started and other activities associated with responding to a specific incident, including documenting lessons learned.*

What information should be reported to US CERT in this situation?

- ☑ The current level of impact on agency functions or services.
- ☐ Lessons learned from previous incidents.
- ☑ The type of information lost, compromised, or corrupted.
- ☑ The scope of time and resources needed to recover from the incident.
- ☐ The name(s) of the individual(s) who first detected the incident.
- ☑ When the activity was first detected.
- ☑ The number of systems, records, and users impacted.
- ☑ The network location of the observed activity.
- ☑ A point of contact.

***Feedback:** The checked items should be reported to US CERT for any incident.*

What work should the incident response team perform in this situation?

- ☑ Assess.
- ☑ Determine Impact.
- ☑ Contain.

- ☐ Establish Strategies and Goals.
- ☑ Update Policy and Training.
- ☑ Recover.
- ☐ Create a Roadmap.
- ☑ Determine Severity.
- ☑ Preserve Evidence.
- ☑ Initiate Communications.

Feedback: *The checked items define sections of an effective incident response plan and should be performed by the incident response team.*

How would the incident response team's activities change if this situation was determined to be an event rather than an incident?

- ○ No changes apply. All activities associated with incidents also apply to events.
- ⦿ No reporting to US CERT is required for events.
- ○ All activities would change.

Feedback: *All activities for cyber incidents can apply to events. However, US CERT does not need to be notified of cyber events.*