Laboratory #8

Lab #8: Craft a Security or Computer Incident Response Policy – CIRT Response Team

Learning Objectives and Outcomes

Upon completing this lab, students will be able to complete the following tasks:

- Define the purpose of a security or computer incident response team
- Identify the major elements of a security or computer incident response methodology
- Align the roles and responsibilities to elements of a CIRT response team
- Identify critical management, HR, Legal, IT, and information systems security personnel required for the CIRT response team
- Create a CIRT Response Policy Definition that defines the purpose and goal of the CIRT Response Team and the Authority Granted During an Incident

Required Setup and Tools

This is a paper-based lab. Internet access and the student's Microsoft Office applications are needed to perform this lab.

The following summarizes the setup, configuration, and equipment needed to perform Lab #8:

1. Standard onsite student workstation must have the following software applications loaded and Internet access to perform this lab:
    a. Microsoft Office 2007 or higher
    b. Adobe PDF reader
    c. Internet access

Recommended Procedures

Lab #8 – Student Steps

The following presents the steps needed to perform Lab #8 – Create a Security or Computer Incident Response Policy – CIRT Response Team:

1. Review the sample Incident Response Plan outline and discuss the overall purpose and scope of the plan
2. Discuss the goal and purpose of a Security or Computer Incident Response Plan

3. Review the policy definitions that are required with a Security or Computer Incident Response Plan using the sample outline
4. Discuss what organizations can do to mitigate the risks and threats by having a Security or Incident Response Plan and Team
5. Review the 6-step methodology for performing incident response
6. Review the Chain of Custody and integrity of physical evidence in a court of law

   Chain of Custody: The movement and location of physical evidence from the time it is obtained until the time it is presented in court.

7. Discuss the need for a Security or Computer Incident Response Team Policy Definition that addresses the delegation of authority to the CIRT response team members during an incident response emergency
8. Review how to perform Lab #8 – Create a Security or Computer Incident Response Policy – CIRT Response Team
9. Answer the Lab #8 – Assessment Questions & Answers

Deliverables

Upon completion of the Lab #8: Create a Security or Computer Incident Response Policy – CIRT Response Team, the students are required to provide the following deliverables as part of this lab:

1. Lab #8 – Assessment Worksheet – Create an Incident Response Team Policy Definition
2. Lab #8 – Assessment Questions & Answers

Evaluation Criteria and Rubrics

The following are the evaluation criteria and rubrics for Lab #8 that the students must perform:

1. Was the student able to define the purpose of a security or computer incident response team? – [**20%**]
2. Was the student able to identify the major elements of a security or computer incident response methodology? – [**20%**]
3. Was the student able to align the roles and responsibilities to elements of a CIRT response team? – [**20%**]

4. Was the student able to identify critical management, HR, Legal, IT, and information systems security personnel required for the CIRT response team? – [**20%**]
5. Was the student able to create a CIRT Response Policy Definition that defines the purpose and goal of the CIRT Response Team and the Authority Granted During an Incident? – [**20%**]

Lab #8 – Assessment Worksheet

Craft a Security or Computer Incident Response Policy – CIRT Response Team

Course Name: _____

Student Name: _____

Instructor Name: _____

Lab Due Date: _____

Overview

In this lab, you are to create an organization-wide policy defining and authorizing a Security or Computer Incident Response Team to have full access and authority to all IT systems, applications, data and physical IT assets when a security or other incident occurs. Here is your scenario:

- Regional ABC Credit union/bank with multiple branches and locations throughout the region
- Online banking and use of the Internet is a strength of your bank given limited human resources
- The customer service department is the most critical business function/operation for the organization
- The organization wants to be in compliance with GLBA and IT security best practices regarding employees
- The organization wants to monitor and control the use of the Internet by implementing content filtering
- The organization wants to eliminate personal use of organization owned IT assets and systems
- The organization wants to monitor and control the use of the e-mail system by implementing e-mail security controls
- The organization wants to create a Security or Computer Incident Response Team to deal with security breaches and other incidents if attacked providing full authority for the team to perform whatever activities are needed to maintain Chain of Custody in performing forensics and evidence collection
- The organization wants to implement this policy throughout the organization to provide full authority to the CIRT team members during crisis to all physical facilities, IT assets, IT systems, applications, and data owned by the organization

Instructions

Using Microsoft Word, create a Security or Computer Incident Response Policy granting team members full access and authority to perform forensics and to maintain Chain of Custody for physical evidence containment. Use the following policy template:

ABC Credit Union

Computer Incident Response Team – Access & Authorization Policy

Policy Statement

{Insert policy verbiage here}

Purpose/Objectives

{Insert purpose of the policy as well as the objectives – bulleted list of the policy definition
Define the Security Incident Response Team Members and the Authorization and Authority granted to them during a crisis or securing incident situation.}

Scope

{Define this policy's scope and whom it covers.

Which of the seven domains of a typical IT infrastructure are impacted?

What elements or IT assets or organization-owned assets are within the scope of this policy?

What access and authority are granted to the incident response team members that may be outside of standard protocol?}

Standards

{Does this policy point to any hardware, software, or configuration standards? If so, list them here and explain the relationship of this policy to these standards.}

Procedures

{Explain how you intend to implement this policy across the organization.

Also, define and incorporate the 6-step incident response approach here along with how the Chain of Custody must be maintained throughout any evidence collection process.}

Guidelines

{Explain any road blocks or implementation issues that you must address in this section and how you will overcome them per defined policy guidelines.}

Note: Your policy document must be no more than 3 pages long.

Lab #8 – Assessment Worksheet

Craft a Security or Computer Incident Response Policy – CIRT Response Team

Course Name: _____

Student Name: _____

Instructor Name: _____

Lab Due Date: _____

Overview

In this lab, you are to create an organization-wide policy defining and authorizing a Security or Computer Incident Response Team to have full access and authority to all IT systems, applications, data and physical IT assets when a security or other incident occurs. A review of the 6-step incident response methodology and an outline of a Security or Computer Incident Response Plan was presented. The students also learned about the Chain of Custody and what forensic procedures and protocols must be followed to allow physical evidence to be admissible in a court of law.

Lab Assessment Questions & Answers

1. What are the 6-steps in the incident response methodology?

2. If an organization has no intention of prosecuting a perpetrator or attacker, does it still need an incident response team to handle forensics?

3. Why is it a good idea to include human resources on the Incident Response Management Team?

4. Why is it a good idea to include legal or general counsel in on the Incident Response Management Team?

5. How does an incident response plan and team help reduce risks to the organization?

6. If you are reacting to a malicious software attack such as a virus and its spreading, during which step in the incident response process are you attempting to minimize its spreading?

7. If you cannot cease the spreading, what should you do to protect your non-impacted mission-critical IT infrastructure assets?

8. When a security incident has been declared, does a PC technician have full access and authority to seize and confiscate a vice president's laptop computer? Why or why not?

9. Which step in the incident response methodology should you document the steps and procedures to replicate the solution?

10. Why is a port mortem review of an incident the most important step in the incident response methodology?

11. Why is a policy definition required for Computer Security Incident Response Team?

12. What is the purpose of having well documented policies as it relates to the CSIRT function and distinguishing events versus an incident?

13. Which 4 steps in the incident handling process requires the Daubert Standard for Chain-of-Custody evidence collection?

14. Why is syslog and audit trail event correlation a critical application and tool for CSIRT incident response handling?

15. Why is File Integrity Monitoring alerts/alarms a critical application and tool for the CSIRT incident response identification?