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: IAP301

Student Name: Nguyễn Quốc Vượng

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}

The Computer Incident Response Team (CIRT) at ABC Credit Union is granted full access and authority to perform forensics and maintain the Chain of Custody for physical evidence containment during security incidents or crises. This policy defines the roles, responsibilities, and authorization levels of CIRT members in handling and responding to security incidents

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.}

The purpose of this policy is to:
Establish the authority and responsibilities of the Computer Incident Response Team during security incidents or crises.
Define the access and authorization granted to CIRT members to perform forensic investigations and maintain the Chain of Custody for physical evidence containment.

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?}

This policy grants CIRT members at ABC Credit Union access to key IT areas, including networks, systems, data, and physical security, to conduct investigations, handle evidence, and coordinate incident response with internal and external teams.

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.}

This policy aligns with the hardware, software, and configuration standards established by ABC Credit Union. It complements the organization's existing security policies, incident response procedures, and incident management framework

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.}

The CIRT will follow a 6-step incident response approach: preparation, identification, containment, eradication, recovery, and lessons learned. Chain of custody requires documenting evidence, using tamper-proof packaging, tracking access, and thorough reporting

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.}

To implement this policy, train CIRT members in forensics and evidence handling , establish clear communication with stakeholders, regularly update the policy for new threats, and document any incident response challenges with solutions

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: IAP301

Student Name: Nguyễn Quốc Vượng

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?
   - Preparation: This involves establishing incident response policies, procedures, and plans, as well as identifying and training incident response team members.
   - Identification: This step involves detecting and determining the nature and scope of the incident.
   - Containment: This step involves containing the incident to prevent it from spreading further and causing additional damage or harm.
   - Eradication: This step involves removing the cause of the incident and restoring affected systems to their normal state
   - Recovery: This step involves restoring normal business operations and ensuring that systems and data are secure.
   - Lessons Learned: This step involves analyzing the incident to identify areas for improvement in incident response policies, procedures, and plans

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

   Forensics must be handled by the incident response team because it is all proof of a crimes

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

   - Help with legal and regulatory compliance: Many security incidents involve sensitive or confidential data, which can raise legal and regulatory compliance issues. HR can provide expertise on issues such as data privacy, confidentiality, and regulatory requirements, and help ensure that the organization remains in compliance with applicable laws and regulations.
   - Assist with employee support: Security incidents can be stressful and disruptive for employees. HR can provide support to affected employees, such as counseling services or other resources to help them cope with the incident.
   - Help with incident documentation: Documentation is an important part of incident response, and HR can assist with documenting the incident from an employee perspective. HR can help collect and document evidence, identify potential witnesses, and ensure that all documentation is accurate and complete

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

   - Legal expertise: Security incidents can have implications for legal issues, such as violations of data protection laws, breach of contractual requirements, or potential liability for damages. Legal counsel can provide expertise on incident-related legal issues, including regulatory requirements, contractual obligations and potential liability.
   - Risk management: Legal advisors can help IRMT assess the risks associated with incidents and provide guidance on how to mitigate those risks. This may include advice on how to minimize legal losses or reputational damage, or how to comply with legal or regulatory requirements

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

   Identify threats, develop incident response plans, assess and update, include legal or general counsel on the incident response team

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?
Classify and prioritize incidents

7. If you cannot cease the spreading, what should you do to protect your non-impacted mission-critical IT infrastructure assets?
Software Update, Device Shutdown (Turn off malware-infected devices to prevent spread), Network Separation (Separate infected computers from the rest of the network to prevent malware from spreading)

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?
- Subject to the policy set forth by the organization. If the policy allows a PC technician to have the authority to access and seize the vice president's laptop to gather evidence related to a security incident, then they have the authority to do so.
- In the opposite direction, if there is no policy to allow the above action, they do not have the right

9. Which step in the incident response methodology should you document the steps and procedures to replicate the solution?
Recovery & Note: Documenting these steps and processes makes it possible for an organization to effectively reuse solutions and reduce future problem resolution time

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

This is done so that the incident response team will be better prepared to respond quickly and effectively in the future if a situation similar to this one arise

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

Provide staff instructions on how to spot and handle computer security incidents. This makes it possible to guarantee that every employee is aware of how to act and react appropriately in the case of a security problem

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

Further information on how the company manages incidents would be included in a policy for the CSIRT team. Instead of naming individuals and their roles, the policy for the CSIRT team would be more inclusive and simpler to arrange. Although developing an incident policy could be useful, several policies would need to be developed because no two situations are exactly alike

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

Identification, containment, eradication, recovery

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

The CSIRT keeps track of all the incidents that happen on the computer system

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

File integrity monitoring tools can monitor and send alerts to the CSIRT team for immediate action before damaging systems and critical organization data