LAB 4
Assessment Worksheet
Craft a Security or Computer Incident Response Policy – CIRT Response Team

Course:	**POLICY DEVELOPMENT IN INFORMATION ASSURANCE (IAP301)**
Semester:	**SP24**
Class:	**IA1702**
Name:	**Trần Minh Triết**
(roll numbers):	**SE172241**

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 email 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.

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

ABC Credit Union understands how crucial it is to respond to computer security events quickly and efficiently. The Computer Incident Response Team (CIRT) has full access and authorization to conduct digital forensics and uphold Chain of Custody for the containment of physical evidence in order to guarantee prompt resolution and mitigation of such situations.

Purpose/Objectives

This policy outlines the permissions and access that members of the ABC Credit Union Computer Incident Response Team are allowed to use in responding to computer security incidents. Preserving the integrity of both digital and physical evidence, minimizing the impact of security incidents, and ensuring prompt and effective reaction are the goals.

Scope

All members of the ABC Credit Union Computer Incident Response Team are subject to this policy, which describes their rights and obligations with regard to accessing and managing tangible and digital evidence when conducting investigations and resolving computer security problems.

Standard

The following actions are permitted for ABC Credit Union Computer Incident Response Team members:

1. Any devices, networks, or systems that might be connected to a security incident should be accessed and examined.
2. Gather, store, and evaluate digital evidence in compliance with legal standards and industry best practices.
3. Keep the Chain of Custody for any tangible evidence that is gathered throughout an investigation secure.
4. When it's required, work together with pertinent parties, such as IT personnel, legal advisors, and law enforcement organizations, to help with the investigation and settlement of security issues.

Procedures

1. The CIRT must be alerted as soon as a possible security incident is discovered.
The CIRT will evaluate the issue as soon as possible and take the required steps to contain and look into the event.
2. For the purpose of accessing and inspecting the systems, networks, and devices involved in the incident, members of the CIRT must adhere to established protocols.
3. For digital evidence to be admissible and of high integrity, it must be gathered with authorized instruments and methods.
4. Physical evidence must be gathered, appropriately documented, and securely stored in compliance with Chain of Custody protocols.
5. The CIRT is required to keep thorough records of every step taken during the investigation, including the processing and evaluation of the evidence.
6. The CIRT will deliver a thorough report detailing its findings, corrective measures, and suggestions for future prevention after the investigation is concluded.

Guidelines

1. The CIRT members will receive ongoing instruction and certification in incident response techniques and digital forensics.
2. Access to systems and sensitive data must be tightly supervised and provided only to those who have a legitimate need to know.
3. Any departure from the established protocols needs to be recorded and authorized by the relevant authorities.
4. To avoid unwanted access or tampering, all evidence and investigative materials must be treated with the highest confidentiality and maintained safely.
5. Every year, this policy will be reviewed and amended to reflect any changes in regulations, technology, or organizational needs.

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

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

The incident response approach consists of six steps: lessons learned, preparation, identification, containment, eradication, and recovery. Establishing policies, processes, and training is part of preparation. Finding and verifying an incident is a necessary step in identification. To stop more harm, impacted systems must be isolated as part of containment. Eradication is the process of eliminating the incident's source from the impacted systems. Recovery is the process of getting systems back to working normally. Analyzing the occurrence to enhance response in the future is part of the lessons gained.

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

Indeed, even in cases where a business chooses not to pursue attackers, having an incident response team in place is still essential. Understanding the attack's nature, locating weaknesses, and putting preventative measures in place are all made possible by forensics. Comprehensive documentation and analysis are also necessary for internal accountability, regulatory compliance, and insurance claims.

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

The incident response management team should include human resources as they can help in handling personnel concerns that arise from the occurrence. This entails keeping in touch with staff members, managing any legal or disciplinary proceedings, and making sure that HR rules and guidelines pertaining to data protection and worker welfare are followed both before and after the event.

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

To offer advice on legal ramifications and obligations, the Incident Response Management Team should include legal or general counsel. In order to reduce legal risks, they can evaluate regulatory requirements, offer guidance on potential liabilities, help preserve evidence for court cases, and organize contact with outside parties like law enforcement, regulators, and impacted parties.

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

By offering a methodical and well-coordinated approach to managing security issues, an incident response strategy and team assist in lowering risks to the company. Organizations may lessen the effects of accidents, cut down on downtime, prevent financial losses, protect their brand, and guarantee regulatory compliance by being well-prepared in advance. Furthermore, a responsive and well-trained incident response staff can assist find vulnerabilities and fix them early on, improving overall security posture and resilience.

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?

Minimizing the spreading of a malicious software attack, such as a virus, typically occurs during the containment phase of the incident response process. In this step, actions are taken to isolate affected systems or networks to prevent further propagation of the malware.

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

If the spreading of the malicious software attack cannot be ceased, protecting non-impacted mission-critical IT infrastructure assets becomes crucial. This involves implementing additional security measures such as network segmentation, deploying intrusion detection and prevention systems, and ensuring backups of critical data are intact to facilitate recovery.

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?
A PC technician does not typically have full authority to seize and confiscate a vice president's laptop computer during a security incident. Such actions should be conducted under the guidance and approval of the Incident Response Management Team, which may involve legal counsel and senior management. Unauthorized access to sensitive devices could lead to legal and privacy concerns.

9. Which step in the incident response methodology should you document the steps and procedures to replicate the solution?
Documenting the steps and procedures to replicate the solution should occur during the "lessons learned" phase of the incident response methodology. This step involves analyzing the incident response process, identifying areas for improvement, and documenting best practices and solutions to replicate in future incidents.

10. Why is a port mortem review of an incident the most important step in the incident response methodology?
The most crucial phase in the incident response process is the post-mortem review since it offers the chance to carry out a detailed investigation of the occurrence, pinpoint the underlying causes, evaluate the efficiency of the reaction mechanism, and put remedial measures in place to stop similar incidents from happening again. Organizations can continuously enhance their security posture and incident response skills by using this review to help them learn from past mistakes.

11. Why is a policy definition required for Computer Security Incident Response Team?
A policy definition is required for the Computer Security Incident Response Team (CSIRT) to establish clear guidelines, roles, and responsibilities for handling security incidents. It outlines the scope of the CSIRT's authority, procedures for reporting incidents, escalation processes, communication protocols, and compliance requirements. A well-defined policy ensures consistency, efficiency, and effectiveness in incident response efforts.

12. What is the purpose of having well documented policies as it relates to the CSIRT function and distinguishing events versus an incident?
Well-documented policies are essential for the CSIRT function as they provide clear guidelines for distinguishing events from incidents. Events are typically benign or routine activities that do not pose a significant threat to security, while incidents are events that have a negative impact on the confidentiality, integrity, or availability of information assets. By having well-defined policies, the CSIRT can quickly identify and prioritize incidents for timely and appropriate response, minimizing potential damage and disruption to the organization.

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

The four steps in the incident handling process that require adherence to the Daubert Standard for Chain-of-Custody evidence collection include identification, preservation, analysis, and documentation. The Daubert Standard ensures the integrity and admissibility of digital evidence in legal proceedings by establishing protocols for collecting, documenting, storing, and presenting evidence in a manner that maintains its authenticity and reliability.

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

Syslog and audit trail event correlation is a critical application and tool for CSIRT incident response handling because it allows for the centralized collection, aggregation, and analysis of log data from various sources such as network devices, servers, and applications. By correlating and analyzing syslog and audit trail events in real-time, CSIRT can detect suspicious activities, identify potential security incidents, and respond promptly to mitigate risks and minimize impact.

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

File Integrity Monitoring (FIM) alerts/alarms are a critical application and tool for CSIRT incident response identification because they provide continuous monitoring and detection of unauthorized changes to critical system files, configurations, and directories. FIM helps CSIRT identify potential security breaches, unauthorized access, or malware infections by alerting on changes that deviate from the expected baseline. Prompt detection of file integrity violations enables CSIRT to investigate and respond swiftly to mitigate the impact of security incidents and prevent further compromise of systems and data.