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

Course Name: Policy Development in Information Assurance (IAP301)
Student Name: Nguyễn Trần Vinh – SE160258
Instructor Name: Mai Hoàng Đỉnh
Lab Due Date: 28/10/2023

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

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

The organization is committed to protecting its IT assets, systems, applications, data, and physical facilities from security breaches and other incidents that may compromise their confidentiality, integrity, availability, or reputation. The organization has established a Security or Computer Incident Response Team (CIRT) to deal with such incidents in a timely and effective manner. The CIRT is authorized and empowered to perform any actions necessary to contain, analyze, mitigate, and recover from an incident, as well as to preserve evidence and maintain the chain of custody for forensic purposes.

Purpose/Objectives

- Define the roles and responsibilities of the CIRT members and the scope of their authority during an incident
- Establish the procedures and guidelines for incident response activities and evidence collection
- Ensure compliance with GLBA and IT security best practices regarding employees, customers, and third parties
- Minimize the impact and damage of an incident on the organization’s business operations, reputation, and legal obligations

Scope

- All employees, contractors, consultants, vendors, and partners of the organization who have access to or use of the organization’s IT assets, systems, applications, data, or physical facilities
- All IT assets, systems, applications, data, or physical facilities owned, leased, operated, or controlled by the organization
- All incidents that affect or threaten the security, availability, or functionality of the organization’s IT assets, systems, applications, data, or physical facilities
- All seven domains of the organization’s IT infrastructure: user domain, workstation domain, LAN domain, LAN-to-WAN domain, WAN domain, remote access domain, and system/application domain
- Access any IT asset, system, application, data, or physical facility that is relevant to the incident investigation or resolution
- Disconnect or isolate any IT asset, system, application, data, or physical facility that is compromised or poses a risk to the organization
- Modify or delete any IT asset, system, application, data, or physical facility that is necessary to contain or mitigate the incident
- Request assistance or cooperation from any employee or third party that is involved in or affected by the incident
- Report any findings or recommendations to the appropriate management or authorities

Standards

- GLBA Section 501(b) - Safeguards Rule: requires financial institutions to protect the security and confidentiality of customer information
- NIST SP 800-61 - Computer Security Incident Handling Guide: provides best practices for incident response processes and procedures
- ISO/IEC 27035 - Information Security Incident Management: provides a structured approach for managing information security incidents

Procedures

- Preparation: The CIRT will prepare for potential incidents by developing and maintaining an incident response plan that defines the roles and responsibilities of the team members; identifies the tools and resources needed for incident detection, analysis, and resolution; establishes the communication channels and escalation procedures; and defines the criteria and thresholds for declaring an incident.
- Identification: The CIRT will identify an incident by monitoring and analyzing various sources of information such as logs, alerts, reports, complaints, or notifications from internal or external parties. The CIRT will verify the validity and severity of the incident and determine its scope and impact on the organization.
- Containment: The CIRT will contain an incident by isolating the affected IT assets, systems, applications, data, or physical facilities from the rest of the network or environment. The CIRT will also implement temporary countermeasures to prevent further damage or spread of the incident.
- Analysis: The CIRT will analyze an incident by collecting and examining relevant evidence such as files, memory dumps, network traffic, or logs. The CIRT will also perform root cause analysis to identify the source, vector, and motive of the incident.

- Eradication: The CIRT will eradicate an incident by removing any malicious code, backdoors, or unauthorized changes from the affected IT assets, systems, applications, data, or physical facilities. The CIRT will also restore any corrupted or lost data from backups or other sources.
- Recovery: The CIRT will recover from an incident by restoring the normal operations of the affected IT assets, systems, applications, data, or physical facilities. The CIRT will also verify that no residual effects or vulnerabilities remain after the incident resolution.

Guidelines

- Resistance or reluctance from employees or third parties to cooperate with the CIRT or grant them access or authority
- Conflicts or disputes between the CIRT and other departments or functions over the prioritization or resolution of incidents
- Legal or regulatory implications or obligations arising from the disclosure or handling of sensitive or confidential information
- Technical or operational difficulties or limitations in detecting, analyzing, or resolving incidents

PART B

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?

Answer:

- Preparation: This step involves developing and maintaining an incident response plan that defines the roles and responsibilities of the team members; identifies the tools and resources needed for incident detection, analysis, and resolution; establishes the communication channels and escalation procedures; and defines the criteria and thresholds for declaring an incident.
- Identification: This step involves monitoring and analyzing various sources of information such as logs, alerts, reports, complaints, or notifications from internal or external parties to identify an incident. This step also involves verifying the validity and severity of the incident and determining its scope and impact on the organization.
- Containment: This step involves isolating the affected IT assets, systems, applications, data, or physical facilities from the rest of the network or environment to contain an incident. This step also involves implementing temporary countermeasures to prevent further damage or spread of the incident.
- Analysis: This step involves collecting and examining relevant evidence such as files, memory dumps, network traffic, or logs to analyze an incident. This step also involves performing root cause analysis to identify the source, vector, and motive of the incident.
- Eradication: This step involves removing any malicious code, backdoors, or unauthorized changes from the affected IT assets, systems, applications, data, or physical facilities to eradicate an incident. This step also involves restoring any corrupted or lost data from backups or other sources.
- Recovery: This step involves restoring the normal operations of the affected IT assets, systems, applications, data, or physical facilities to recover from an incident. This step also involves verifying that no residual effects or vulnerabilities remain after the incident resolution.

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

Answer: Yes, an organization still needs an incident response team to handle forensics, even if it has no intention of prosecuting a perpetrator or attacker. Forensics is the process of collecting and analyzing evidence from a computer crime or security incident.

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

Answer: It is a good idea to include human resources on the Incident Response Management Team because:

- Provide guidance and support on the policies and procedures related to employee rights, responsibilities, and disciplinary actions in case of an incident
- Coordinate with the legal counsel and the public relations team on the communication and notification strategies for internal and external parties affected by or involved in an incident
- Assist with the training and awareness programs for employees on the security best practices and the incident response plan
- Help with the recruitment and retention of qualified and skilled incident response team members
- Contribute to the post-incident review and evaluation process and provide feedback and recommendations for improvement

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

Answer: It is a good idea to include legal or general counsel in on the Incident Response Management Team because:

- Advise on the legal and regulatory obligations and implications of an incident, such as reporting, notification, disclosure, evidence preservation, or litigation
- Review and approve the incident response plan and any policies, procedures, or contracts related to incident response
- Represent and defend the organization in any legal actions or disputes arising from or related to an incident
- Negotiate and coordinate with any external parties involved in or affected by an incident, such as law enforcement, regulators, customers, or vendors
- Assess and mitigate any legal risks or liabilities associated with an incident

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

Answer:

- Providing a structured and consistent approach for handling any security or other incidents that may occur
- Reducing the response time and the recovery time of an incident, thereby minimizing the impact and damage on the organization’s IT assets, systems, applications, data, or physical facilities
- Preserving and analyzing the evidence of an incident, thereby facilitating the identification and remediation of the root cause and the vulnerabilities that allowed the incident to happen
- Enhancing the organization’s security posture, policies, procedures, and practices by learning from the incident and implementing improvement actions
- Complying with the legal and regulatory obligations and expectations of the organization regarding incident reporting, notification, disclosure, or litigation
- Maintaining the organization’s reputation and credibility by demonstrating its commitment and capability to handle incidents effectively and professionally

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?

Answer: If you are reacting to a malicious software attack such as a virus and its spreading, you are attempting to minimize its spreading during the **containment** step in the incident response process. This step involves isolating the affected IT assets, systems, applications, data, or physical facilities from the rest of the network or environment to prevent further damage or spread of the incident. This step also involves implementing temporary countermeasures to stop or slow down the virus propagation.

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

Answer:

- Disconnect or shut down any non-essential IT assets, systems, applications, or data that are not required for the organization's core business functions or operations
- Backup any critical data or information that may be at risk of being corrupted, deleted, or stolen by the virus
- Implement or update the security controls and measures such as antivirus software, firewalls, encryption, or authentication on the remaining IT assets, systems, applications, or data
- Monitor and report any suspicious or anomalous activities or behaviors on the network or environment
- Contact and consult with the CIRT or other external experts for assistance or guidance

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?

Answer: Overall, whether or not a PC technician has full access and authority to seize and confiscate a vice president's laptop computer during a security incident is a complex question that depends on a number of factors. It is important for organizations to have clear policies and procedures in place that govern how security incidents should be handled. It is also important for organizations to train their employees on these policies and procedures.

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

Answer: The step in the incident response methodology where you should document the steps and procedures to replicate the solution is the **recovery** step. This step involves restoring the normal operations of the affected IT assets, systems, applications, data, or physical facilities to recover from an incident. This step also involves verifying that no residual effects or vulnerabilities remain after the incident resolution. By documenting the steps and procedures to replicate the solution, you can ensure that the solution is effective, consistent, and repeatable, and that you can apply it to any similar incidents in the future. Documenting the solution also helps with the post-incident review and evaluation process, where you can assess the performance and outcomes of the incident response team and identify any lessons learned or improvement actions.

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

Answer:

- Evaluate the effectiveness and efficiency of the incident response process and team
- Identify the strengths and weaknesses of the incident response plan and policies
- Learn from the incident and its root cause, impact, and resolution
- Implement improvement actions and recommendations for future incidents
- Document and share the lessons learned and best practices with relevant stakeholders

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

Answer:

- Provides a clear and consistent framework for the roles, responsibilities, and authority of the team members and other stakeholders involved in or affected by an incident
- Establishes the standards, procedures, and guidelines for the incident response process and activities, such as detection, analysis, containment, eradication, recovery, and post mortem review

- Ensures compliance with the legal and regulatory obligations and expectations of the organization regarding incident reporting, notification, disclosure, or litigation
- Enhances the organization's security posture, resilience, and readiness by defining the objectives and outcomes of the incident response plan and policies
- Minimizes the risks and liabilities associated with an incident by providing a structured and consistent approach for handling any security or other incidents that may occur

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

Answer:

- Provide clarity and consistency on the definitions, criteria, and thresholds for declaring an event or an incident, and the appropriate actions and responses for each
- Ensure that the CSIRT function is aligned with the organization's mission, vision, values, and goals, and supports its business objectives and strategies
- Establish the roles and responsibilities of the CSIRT members and other stakeholders involved in or affected by an event or an incident, and the scope of their authority and accountability
- Define the standards, procedures, and guidelines for the CSIRT function, such as incident response process, communication plan, escalation protocol, reporting format, evidence collection, post mortem review, etc.
- Ensure compliance with the legal and regulatory obligations and expectations of the organization regarding incident reporting, notification, disclosure, or litigation
- Enhance the organization's security posture, resilience, and readiness by providing a structured and consistent framework for managing and resolving events or incidents
- Minimize the risks and liabilities associated with events or incidents by providing a systematic and effective approach for handling any security or other issues that may occur

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

Answer:

- Identification: This step involves monitoring and analyzing various sources of information to identify an incident. This step may require collecting digital or forensic evidence from the affected IT assets, systems, applications, data, or physical facilities. The chain of custody should document when, where, how, and by whom the evidence was collected, and what tools or methods were used.
- Analysis: This step involves examining and investigating the collected evidence to determine the cause, scope, impact, and motive of the incident. The chain of custody should document what tools or methods were used to analyze the evidence, and what findings or conclusions were drawn from the analysis.
- Eradication: This step involves removing any malicious code, backdoors, or unauthorized changes from the affected IT assets, systems, applications, data, or physical facilities. The chain of custody should document what tools or methods were used to eradicate the incident, and what actions or changes were made to the evidence.
- Recovery: This step involves restoring the normal operations of the affected IT assets, systems, applications, data, or physical facilities. The chain of custody should document what tools or methods were used to recover from the incident, and what actions or changes were made to the evidence.

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

Answer:

- Enables the CSIRT to collect and aggregate log data from various sources, such as event logs, AppLocker logs, performance data, system center data, call detail records, quality of experience data, IIS Web Server logs, SQL Server logs, Syslog data, and security audit logs

- Allows the CSIRT to parse and normalize the log data into a unified format that can be easily read and analyzed
- Helps the CSIRT to detect and identify incidents by monitoring and analyzing the log data using rule-based, statistical, and machine learning methods
- Supports the CSIRT to contain and eradicate incidents by isolating or disconnecting the affected IT assets, systems, applications, data, or physical facilities based on the log data
- Assists the CSIRT to recover from incidents by restoring the normal operations of the affected IT assets, systems, applications, data, or physical facilities based on the log data
- Facilitates the CSIRT to preserve and analyze evidence by maintaining the chain of custody throughout the evidence collection process using the log data
- Enhances the CSIRT to comply with legal and regulatory obligations and expectations by providing a record of how the incident was obtained and processed using the log data
- Improves the CSIRT to learn from incidents and implement improvement actions by conducting a post mortem review using the log data

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

Answer:

- Enable the CSIRT to detect and identify incidents by monitoring and analyzing changes to critical files in the IT environment, such as operating system files, application software files, configuration files, or registry keys
- Alert the CSIRT to any unauthorized, suspicious, or malicious modifications to the files that may indicate an attack, such as file creation, deletion, alteration, or corruption
- Provide the CSIRT with valuable information and evidence about the cause, scope, impact, and motive of the incident, such as the source, vector, time, and nature of the file changes
- Support the CSIRT in complying with legal and regulatory obligations and expectations regarding incident reporting, notification, disclosure, or litigation, such as GLBA or PCI-DSS
- Enhance the CSIRT’s security posture, resilience, and readiness by providing a baseline for file integrity and a record of file changes