Viterbo University

PCI-DSS

Incident Response Plan

1.0 Overview

This incident response plan defines what constitutes a security incident and outlines the incident response phases. This incident response plan document discusses how information is passed to the appropriate personnel, assessment of the incident, minimizing damage and response strategy, documentation, and preservation of evidence. The incident response plan will define areas of responsibility and establish procedures for handing various security incidents. This document discusses the considerations required to build an incident response plan.

2.0 Purpose

This policy is designed to protect the organizational resources against intrusion.

3.0 Incident Response Goals

1. Verify that an incident occurred.
2. Maintain or Restore Business Continuity.
3. Reduce the incident impact.
4. Determine how the attack was done ir the incident happened.
5. Prevent future attacks or incidents.
6. Improve security and incident response.
7. Prosecute illegal activity.
8. Keep management informed of the situation and response.

4.0 Incident Definition

An incident is any one or more of the following:

1. Loss of information confidentiality (data theft)
2. Compromise of information integrity (damage to data or unauthorized modification).
3. Theft of physical IT asset including computers, storage devices, printers, etc.
4. Damage to physical IT assets including computers, storage devices, printers, etc.
5. Denial of service.
6. Misuse of services, information, or assets.
7. Infection of systems by unauthorized or hostile software.
8. An attempt at unauthorized access.
9. Unauthorized changes to organizational hardware, software, or configuration.
10. Reports of unusual system behavior.

11. Responses to intrusion detection alarms.

5.0 Incident Planning

In the incident response plan, do the following:

1. Define roles and responsibilities
2. Establish procedures detailing actions taken during the incident.
    1. Detail actions based on type of incident such as a virus, hacker intrusion, data theft, system destruction.
    2. Procedures should consider how critical the threatened system or data is.
    3. Consider whether the incident is ongoing or done.

6.0 Incident Response Life cycle

1. Incident Preparation
    1. Policies and Procedures
        1. Computer Security Policies - These involve many policies including password policies, intrusion detection, computer property control, data assessment, and others.
        2. Incident Response Procedures
        3. Backup and Recovery Procedures
    2. Implement policies with security tools including firewalls, intrusion detection systems, and other required items.
    3. Post warning banners against unauthorized use at system points of access.
    4. Establish Response Guidelines by considering and discussing possible scenarios.
    5. Train users about computer security and train IT staff in handling security situations and recognizing intrusions.
    6. Establish Contacts - Incident response team member contact information should be readily available. An emergency contact procedure should be established. There should be one contact list with names listed by contact priority.
    7. Test the process.
2. Discovery - Someone discovers something not right or suspicious. This may be from any of several sources:
    1. Helpdesk
    2. Intrusion detection system
    3. A system administrator
    4. A firewall administrator
    5. A business partner
    6. A monitoring team
    7. A manager
    8. The security department or a security person.
    9. An outside source.
3. Notification - The emergency contact procedure is used to contact the incident response team.

4. Analysis and Assessment - Many factors will determine the proper response including:
    1. Is the incident real or perceived?
    2. Is the incident still in progress?
    3. What data or property is threatened and how critical is it?
    4. What is the impact on the business should the attack succeed? Minimal, serious, or critical?
    5. What system or systems are targeted, where are they located physically and on the network?
    6. Is the incident inside the trusted network?
5. Response Strategy - Determine a response strategy.
    1. Is the response urgent?
    2. Can the incident be quickly contained?
    3. Will the response alert the attacker and do we care?
6. Containment - Take action to prevent further intrusion or damage and remove the cause of the problem. May need to:
    1. Disconnect the affected system(s)
    2. Change passwords.
    3. Block some ports or connections from some IP addresses.
7. Prevention of re-infection
    1. Determine how the intrusion happened - Determine the source of the intrusion whether it was email, inadequate training, attack through a port, attack through an unneeded service, and attack due to unpatched system or application.
    2. Take steps to prevent an immediate re-infection which may include one or more of:
        1. Close a port on a firewall
        2. Patch the affected system
        3. Shut down the infected system until it can be re-installed
        4. Re-install the infected system and restore data from backup. Be sure the backup was made before the infection.
        5. Change email settings to prevent a file attachment type from being allow through the email system.
        6. Plan for some user training.
        7. Disable unused services on the affected system.
8. Restore Affected Systems - Restore affected systems to their original state. Be sure to preserve evidence against the intruder by backing up logs or possibly the entire system. Depending on the situation, restoring the system could include one or more of the following
    1. Re-install the affected system(s) from scratch and restore data from backups if necessary. Be sure to preserve evidence against the intruder by backing up logs or possibly the entire system.
    2. Make users change passwords if passwords may have been sniffed.
    3. Be sure the system has been hardened by turning off or uninstalling unused services.
    4. Be sure the system is fully patched.

5. Be sure real time virus protection and intrusion detection is running.
6. Be sure the system is logging the correct items

9. Documentation - Document what was discovered about the incident including how it occurred, where the attack came from, the response, whether the response was effective.
10. Evidence Preservation - Make copies of logs, email, and other documentable communication. Keep lists of witnesses.
11. Notifying proper external agencies - Notify the police if prosecution of the intruder is possible.
12. Assess damage and cost - Assess the damage to the organization and estimate both the damage cost and the cost of the containment efforts.
13. Review response and update policies - Plan and take preventative steps so the intrusion can't happen again.
    1. Consider whether an additional policy could have prevented the intrusion.
    2. Consider whether a procedure or policy was not followed which allowed the intrusion, then consider what could be changed to be sure the procedure or policy is followed in the future.
    3. Was the incident response appropriate? How could it be improved?
    4. Was every appropriate party informed in a timely manner?
    5. Were the incident responses procedures detailed and cover the entire situation? How can they be improved?
    6. Have changes been made to prevent a re-infection of the current infection? Are all systems patched, systems locked down, passwords changed, anti-virus updated, email policies set, etc.?
    7. Have changes been made to prevent a new and similar infection?
    8. Should any security policies be updated?
    9. What lessons have been learned from this experience?