Security Incident Response Plan

SUNY Broome

Version 1.0

July 23, 2014

1.0 Introduction

This document describes the plan and steps to be taken in response to an IT security incident.

The person who discovers the security incident will call the Information Technology office at 607-778-5011. If the IT department office personnel does not answer, then the person discovering the security incident should call the public safety department at 607-778-5083.

Sources requiring contact information may be:

a) A staff member
b) Intrusion detection monitoring personnel
c) A system administrator
d) A firewall administrator
e) A business partner
f) A manager
g) The security department or a security person.
h) An outside source
i) Students

2.0 Procedure

1) The IT or Public Safety Office will refer to the emergency contact list or effected department contact list and call the designated numbers in order on the list. The office will log:
    j) The name of the caller.
    k) Time of the call.
    l) Contact information about the caller.
    m) The nature of the security incident.
    n) What equipment or persons were involved?
    o) Location of equipment or persons involved.
    p) How the security incident was detected.
    q) When the event was first noticed that supported the idea that the security incident occurred.

2) The IT staff member or affected department staff member who receives the call (or discovered the security incident) will refer to their contact list for both management personnel to be contacted and security incident response members to be contacted. The staff member will call those designated on the list. The staff member will contact the security incident response manager using both email and phone messages while being sure other appropriate and backup personnel and designated managers are contacted. The staff member will log the information received in the same format as the grounds security office in the previous step. The staff member could possibly add the following:
    a) Is the equipment affected business critical?
    b) What is the severity of the potential impact?
    c) Name of system being targeted, along with operating system, IP address, and location.
    d) IP address and any information about the origin of the attack.

3) Contacted members of the response team will meet or discuss the situation over the telephone and determine a response strategy.
    a) Is the security incident real or perceived?
    b) Is the security incident still in progress?
    c) What data or property is threatened and how critical is it?
    d) What is the impact on the business should the attack succeed? Minimal, serious, or critical?
    e) What system or systems are targeted, where are they located physically and on the network?
    f) Is the security incident inside the trusted network?
    g) Is the response urgent?
    h) Can the security incident be quickly contained?
    i) Will the response alert the attacker and do we care?
    j) What type of security incident is this? Example: virus, worm, intrusion, abuse, damage.

4) A security incident ticket will be created. The security incident will be categorized into the highest applicable level of one of the following categories:
    a) Category one - A threat to public safety or life.
    b) Category two - A threat to sensitive data
    c) Category three - A threat to computer systems
    d) Category four - A disruption of services

5) Team members will establish and follow one of the following procedures basing their response on the security incident assessment:
    a) Worm response procedure
    b) Virus response procedure
    c) System failure procedure
    d) Active intrusion response procedure - Is critical data at risk?
    e) Inactive Intrusion response procedure
    f) System abuse procedure
    g) Property theft response procedure
    h) Website denial of service response procedure
    i) Database or file denial of service response procedure
    j) Spyware response procedure.

    The team may create additional procedures which are not foreseen in this document. If there is no applicable procedure in place, the team must document what was done and later establish a procedure for the security incident.

6) Team members will use forensic techniques, including reviewing system logs, looking for gaps in logs, reviewing intrusion detection logs, and interviewing witnesses and the security incident victim to determine how the security incident was caused. Only authorized personnel should be performing interviews or examining evidence, and the authorized personnel may vary by situation and the organization.

7) Team members will recommend changes to prevent the occurrence from happening again or infecting other systems.

8) Upon management approval, the changes will be implemented.

9) Team members will restore the affected system(s) to the uninfected state. They may do any or more of the following:

a) Re-install the affected system(s) from scratch and restore data from backups if necessary. Preserve evidence before doing this.
b) Make users change passwords if passwords may have been sniffed.
c) Be sure the system has been hardened by turning off or uninstalling unused services.
d) Be sure the system is fully patched.
e) Be sure real time virus protection and intrusion detection is running.
f) Be sure the system is logging the correct events and to the proper level.

10) Documentation—the following shall be documented:

a) How the security incident was discovered.
b) The category of the security incident.
c) How the security incident occurred, whether through email, firewall, etc.
d) Where the attack came from, such as IP addresses and other related information about the attacker.
e) What the response plan was.
f) What was done in response?
g) Whether the response was effective.

11) Evidence Preservation—make copies of logs, email, and other communication. Keep lists of witnesses. Keep evidence as long as necessary to complete prosecution and beyond in case of an appeal.

12) Notify proper external agencies—notify the police and other appropriate agencies if prosecution of the intruder is possible. List the agencies and contact numbers here.

13) Assess damage and cost—assess the damage to the organization and estimate both the damage cost and the cost of the containment efforts.

14) Review response and update policies—plan and take preventative steps so the intrusion can't happen again.

a) Consider whether an additional policy could have prevented the intrusion.

b) Consider whether a procedure or policy was not followed which allowed the intrusion, and then consider what could be changed to ensure that the procedure or policy is followed in the future.

c) Was the security incident response appropriate? How could it be improved?

d) Was every appropriate party informed in a timely manner?

e) Were the security incident-response procedures detailed and did they cover the entire situation? How can they be improved?

f) Have changes been made to prevent a re-infection? Have all systems been patched, systems locked down, passwords changed, anti-virus updated, email policies set, etc.?

g) Have changes been made to prevent a new and similar infection?

h) Should any security policies be updated?

i) What lessons have been learned from this experience?