12.2.5 Incident Response Facts

A *security incident* is an event or series of events that result from a security policy violation and has adverse effects on a company's ability to proceed with business. *Incident response* is the actions taken to deal with an incident during and after the incident. Prior planning helps people know what to do when a security incident occurs. Incident response plans should:

- Define what is considered an incident.
- Identify who should respond to the incident. This person is designated as the *first responder*.
- Describe what action should be taken when an incident is detected.
- Provide a detailed outline of steps to take to handle an incident both efficiently and effectively while mitigating its effects.
- Explain how and to whom an incident should be reported.
- Explain when management should be notified of the incident and also outline ways to ensure that management is well-informed.
- Be legally reviewed and approved.
- Be fully supported by senior management and administration with appropriate funding and resources, such as camera equipment, forensic equipment, redundant storage, standby systems, and backup services.

All company leaders should be familiar with the incident response plan. At least one member of every department should be trained to recognize abnormal activities, suspicious behavior, unauthorized code activity, and irregular patterns in employee conduct. In addition, employees should be trained to report security incidents or suspicious activity immediately to the proper company staff members or directly to the first responder.

How to Respond to an Incident

When an an employee discovers an incident, he or she should take the following actions:

1. Recognize and declare the event.
2. Preserve any evidence that may be used in an investigation.
3. Contact the first responder.

In some organizations, the first responder may be a computer incident response team (CIRT), a group of in-house experts that are trained to quickly respond to a crisis computer event. A CIRT should have representation from any department that may be affected by an incident (representation from the human resources and legal departments should always be included). A CIRT should also consist of members with computer network skills, evidence handling training, and forensic skills.

Responding to a security incident is similar to responding to any other type of incident.

- Short-term (triage) actions focus on stopping the attack, mitigating its effects, and restoring basic functionality.
- Mid-term (action/reaction) actions focus on restoring operations to a normal state.
- Long-term (follow up) actions include implementing additional countermeasures and processes to reduce the likelihood of a future attack.

The first responder:

- May be a dedicated member of the security response team.
- Has the following goals:
  - Contain the damage (or incident) as much as possible.
  - Do not damage any evidence.
- Initiates an escalation procedure to ensure that the right people are informed and the right people are brought on the incident site.
- Initiates the documentation of the incident. This includes:
  - Taking photos of the scene.
  - Documenting what is on the computer screen.

Incident response should involve:

- Identifying and containing the problem.
- Investigating how the problem occurred and implementing forensics to preserve evidence that may be used in a criminal investigation.
- Removing and eradicating the cause of the incident.
- Recovering and repairing any damages.
- Documenting the incident and implementing countermeasures and processes to reduce the likelihood of a future attack.

The first step in responding to an incident is stopping the attack and containing or limiting the damage. For example, if the attack involves a computer system attached to the network, the first step might be to disconnect the system from the network. Although you want to preserve as much information as possible to assist in later investigations, it might be better to stop the attack, even if doing so alerts the attacker or results in the loss of evidence regarding the attack. In the case of a virus, isolate any systems that may be able to spread the virus to additional systems.

How to Collect and Analyze Evidence

There are several procedures you should follow while collecting and analyzing computer evidence.

- Before you touch the computer, document and photograph the entire scene of the crime, including the current state of the computer screen. It is better to use a film camera than a digital camera to avoid charges that an image was digitally altered.
- Do not turn off the computer until the necessary evidence is collected.
  - The computer might lose some data when it is turned off.
    - *Volatile* data is any data that is stored in memory that will be lost when the computer is powered off or loses power. Follow the order of volatility when you collect data.
    - *Persistent* data resides on the system's hard drives, USB drives, optical media, and other external hard drives.
  - If it is necessary to isolate a system to stop or prevent future attacks, disconnect the system from the network rather than shutting it down (if possible). In some situations, you may be able to connect the system to a quarantine network to perform a forensic investigation.

    Although you want to preserve as much information as possible to assist in later investigations, turning off the system might be the only practical method to prevent further damage and should be done if necessary, even if it results in the loss of potential evidence. In the case of a virus, isolate any systems that may be able to spread the virus to additional systems.

- Assess the situation to determine whether you have the expertise to conduct further investigations or whether you need to call in additional help.
- Save the contents of memory by taking one of the following actions:
  - Save and extract the page file.
  - Do a complete memory dump to save the contents of physical RAM. You will lose the page file, but the physical memory will be preserved.
- Clone or image hard disks.
  - To protect or ensure the integrity of collected digital evidence, create a checksum using a bit-level hashing algorithm. In the future, the same hashing algorithm can be used to create another checksum. If the two checksums are identical, this proves that the media was not altered (and that the copy is an exact copy of the original).
- In addition to looking for obvious evidence on computer systems (such as saved files), use special forensic tools to check for deleted files, files hidden in slack (empty) space, or data hidden in normal files through steganography.
- For some investigations, you might need to review archived log files or data in backups to look for additional evidence. Be sure to design your backup strategy with not only recovery but also investigation and preserving evidence in mind.
- Sometimes evidence is found on a corporate system that is not otherwise violated. This is known as *co-mingling*. Evidential data should be extracted from the corporate system with great care to maintain its integrity and the safety of the corporate system.
- Track man hours and expenses for each incident. This may be necessary to calculate a total damage estimation and, possibly, restitution.
- You may need to capture and analyze network traffic to understand the incident. This may include:
  1. Identifying suspicious network sessions and packets
  2. Replaying or reconstructing sessions and packets
  3. Interpreting the results
- The *time offset* is the difference in system time that the machines use compared to the actual time. You should record the time offset for each machine involved in the incident to ensure accurate and sequential date and time stamps for collected data.
- Utilities available to help in the analysis of the evidence include:
  - SANS Investigative Forensics Toolkit
  - EnCase
  - FTK
  - The Coroner's Toolkit
  - COFEE
- Repair any damage created by the incident and restore services only after the above procedures are complete.

When the analysis is complete, you must report the findings. The report should be well written, possibly with the assistance of an attorney. Specifically, the report must be self-contained and describe the incident, the response, and the findings. Be sure to include a section relating the lessons learned from the incident and how they should influence your organization's security posture. You should also include the hours and expenses involved in responding to the incident.
