13.2.3 Incident Response Facts

A *security incident* is an event or series of events that result from a security policy violation that has adverse effects on a company's ability to proceed with normal business. Security incidents include employee errors, unauthorized acts by employees, insider attacks, hacker attacks, malware attacks, and unethical gathering of competitive information.

This lesson covers the following topics:

- Incident response
- Damage containment
- Forensic investigation
- Notification

Incident Response

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, especially the *first responder*. The first responder:

- Is the first person on the scene after a security incident has occurred
- 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 that the right people are brought on the incident site
- Initiates the documentation of the incident

Incident response should involve:

- Identification and containment of the problem
- Investigation of how the problem occurred and the forensics to preserve evidence that may be used in a criminal investigation
- Removal and eradication of the cause of the incident
- Recovery and repair of any damages
- Documentation and report of the incident, and implementation of countermeasures and processes to reduce the likelihood of a future attack

Damage Containment

The first step in responding to an incident should be to take actions to stop the attack and contain the damage. For example, if the attack involves a computer system attached to the network, the first step might be to disconnect it 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.

Forensic Investigation

After containing a threat, forensic investigation can be performed on computer systems to gather evidence and identify the methods used in the attack. When working with computer systems, use special computer forensic tools to analyze the system. Investigations can be performed in the following ways:

- A *live analysis* examines an active (running) computer system to analyze the live network connection, memory contents, and running programs.
- A *dead analysis* examines data at rest, such as analyzing hard drive contents.

Follow these procedures when collecting and analyzing computer evidence:

- Before touching the computer, document and photograph the entire scene of the crime including the current state of the computer screen. A traditional camera is preferred over a digital camera to avoid allegations that an image was digitally altered.
- Do not turn off the computer until the necessary evidence has been collected.
  - Some data might be lost when the computer is turned off.
    - *Volatile* data is any data that is stored in memory, CPU registers, and CPU caches that will be lost when

        - the computer is powered off or loses power.
        - *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).
    - 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.
- Assess the situation to determine whether you have the expertise to conduct further investigations, or whether you need to call in additional help.
- Analyze data in order from most volatile to least volatile:
    1. CPU registers and caches
    2. RAM
    3. Virtual memory and temporary file systems
    4. Hard disk data
    5. Archived media (backups)
- 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. The page file will be lost but the physical memory will be preserved.
- Clone or image hard disks.
    - Never analyze the original data. Make several copies for analysis to preserve the original.
    - Archive the original system or data for later investigations and comparisons to your copy.
- 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 empty space, or data hidden in normal files.
- 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 preservation of evidence in mind.
- Track hours and expenses for each incident. This may be necessary to calculate a total damage estimation and possibly restitution.

Forensic investigation results can be used in a court of law if properly handled and documented. To ensure that evidence is admissible in court, you must be able to provide its *chain of custody*. The chain of custody:

- Documents the integrity of the evidence by providing a record of every person it has come in contact with and under what conditions. Without a chain of custody document, there is no way to prove who might have had access to the evidence, meaning that the evidence could have been altered after discovery. Failure to provide a valid chain of custody could make the evidence worthless in court.
- Should be started the moment evidence is discovered and should include what the evidence is, who found it, under what circumstances, the location of the evidence, the date and time of original discovery, how it was handled, and all precautionary actions that have been taken to ensure its integrity.
- Should be maintained throughout the evidence life cycle to document the people and procedures used at each stage.

Be aware that many organizations will intentionally not bring evidence to court to avoid the negative publicity that could be associated with a trial.

Notification

After you have analyzed the attack and gathered evidence, be aware that in some states you will be required to notify individuals if their personal information might have been compromised. For example, if an incident involves the exposure of credit card numbers, identifying information (such as Social Security numbers), or medical information, you might be legally obligated to notify potential victims and take measures to help protect their information from further attack.
