# AP 5 – IT Security

# AP Summary

This Action Plan applies to a cyber-attack on an IT intranet system. Examples of a cyber-attack include:

* Virus
* Denial of Service (DoS) including Smurf, ICMP, TCP SYN, UDP, TCP, Distributed Denial of Service, and various combinations
* Internet facing server attacks
* Unauthorized Network Intrusions / Unauthorized Access

## Prevent and prepare for attacks by:

* Updating all network documentation around the SCADA/DCS
* Documenting all network data flows to/from Intranet systems, SCADA/DCS and surrounding systems
* Identifying Zones of Vulnerability
* Identifying ramifications and feasibility of disconnecting networks, computers, and data flows
* Ensuring that sufficient monitoring and network control points (firewalls, IPS, etc.) are in place to both know what’s happening on your network and how to control it
* Characterizing network traffic so that anomalous behavior can be identified
* Becoming familiar with computer forensics tools and practices before being forced to learn them “under fire”
* Becoming familiar with host-based monitoring and intrusion detection, since most hacking over networks is now conducted via encrypted tunnels or data streams
* Ensuring that backup/restore procedures are up to date, as are the backups themselves

## Initiation and Notification

1. Initiate this AP if any of the following has occurred:

* More than one user reports unusual behavior of any IT system or software.
* Network intrusion detection indicates a violation.
* Unusual IT system activity is noted on holidays, evenings, or weekends.
* Unusual log file entries are noticed. Although expert intruders are good at covering their tracks, examples include numerous failed login attempts, and logins into dormant or default accounts (logins when not expected, logins to infrequently used accounts).
* Presence of new setuid or setgid files are discovered.
* Changes in system directories and files are noted.
* Unusual hidden files or ambiguous files, such as those from past incidents, are noticed. For example, /tmp/bob and /etc/inet/d (/tmp/…, /tmp/(space), /dev/\* saved as real files rather than device files.
* Missing files, altered files, or unknown users are found in password files.
* Users’ home pages are altered. These are usually the intentional target for visibility or other pages on the Web server.
* Accounting discrepancies are noticed.
* Suspicious probes and /or browsing is identified.
* Presence of cracking utilities is found, such as ‘Crack’.
* Unaccounted for changes in the DNS tables, router rules, or firewall rules are discovered.
* Unexplained elevation or use of privileges.

1. Notify the [WUERM] and Data (IT) Manager immediately upon discovery of the attack by whatever means of communication may be available. Notification numbers can be obtained from the Organization Contact List in the Appendices as well as from Section III.D of the ERP.

Contact others as appropriate, including:

* Internet Service Provider,
* Computer Equipment Vendor,
* Computer Emergency Response Team

### Equipment

This equipment is available to assist in the execution of this AP:

|  |  |
| --- | --- |
| Equipment | Location |
|  |  |
|  |  |

# Assess the Problem

The approach to addressing an incident can vary depending on the nature of the incident, so it is critical to be aware of the type of incident that has occurred BEFORE taking the following steps:

* 1. Take the customer information database, assuming it is a standard database, off the network, so that it is no longer accessible.
     + Modems should not be allowed on the database machine.
     + You might maintain critical customer information on your network. If a hacker steals, modifies, destroys, or even posts the information to the Internet, you may find yourself in court
  2. Isolate and Contain the Threat
     + In general, the intruder or the malicious code should be prevented from working through the network. Attempts to contain the threat should also consider every effort to minimize the impact to business operations. Prevent the use of your systems to launch attacks against other companies. Your computer may become one of hundreds of “soldier” machines rather than an “end target”.
  3. Document the event (See items 4 and 16)
     + Recording all the details may provide management with the information necessary to assess the break-in and could assist in the prosecution of specific individuals.
  4. Take a snapshot of the system to obtain forensic images and preserve original media. A snapshot is basically a photo of what a computer’s memory (primary storage, specific registers, etc.) contains at a specific point in time. It can be used to catch intruders by recording information that the hacker may erase before the attack is completed or repelled.
* Registers, peripheral memory, caches
* Memory (kernel and physical)
* Network state
* Running processes
* Hardware data residue, memory chips, and PDA-type systems
* Hard disks
* Disks and backup media
* CD-ROMs
* Printouts

Be prepared to revise the response plan as necessary based on new information. Flexibility is important. Be ready to change monitoring and defensive strategies during an incident as necessary to handle the distinctive circumstances of an individual attack.

# Isolate and Fix the Problem

1. Save the system state by backing up as much of the system as possible. This helps with further diagnosing the incident.
2. Alert others according to the response strategy including contacting a Computer Emergency Response Team. The Computer Emergency Response Team may know how to fix the flaw in the vendor’s software or hardware that allowed the intruder to access your network.
3. Determine if the system should be disconnected from the network. Users should still be able to use some local services. Be careful, the network might involve wireless local area networks. In these cases, it might be important to disable and/or remove the wireless access points from the internal network. Sometimes you may need to disconnect a system from the network to prevent further damage and limit the extent of the attack.
4. Determine if the system should be shut down entirely. This action might appear drastic but is sometimes advisable usually based on a decision to prevent further loss and/or disruption. Shut down or disconnect resources only when necessary.

# Monitor

1. Repair real-time scanning and detection to prevent further infection. This involves actively tracking traffic for unusual activity (for example, port scanning) or patterns of an attack stream of bits, bytes, or packets. Attackers sometimes use a “smoke screen”, an attack that attempts to divert attention from a stealthier network intrusion. It is therefore important not to focus all attention on an initial attack, but to continue diligently looking for other attacks.
2. Set up traps by learning the intruder’s identity or modus operandi (MO), the mechanism by which the perpetrator commits his or her crime. It is a learned behavior and can change over time. An MO can be considered a pattern, allowing for some variance. Examples of traps are honeypots, that is, computers designed to attract attackers to record their behavior and to gather evidence, but not meant for legitimate users.

# Recovery and Return to Safety

1. Change the filtering rules of firewalls and routers to exclude traffic from hosts that appear to be the source of an attack.
2. Disable known vulnerable services, such as file transfer or calendar services. This is effective when attackers exploit newly discovered service vulnerabilities.
3. Remove any hidden malicious programs or directories added by the intruder or deployed by the malicious code, up to and including a system-wide removal of all programs and files (i.e., format the disk and re-install). Recovery personnel need to balance the need recovery with the need to preserve evidence for prosecution.
4. Update virus signatures. Although it takes longer to update antivirus signatures to the desktop community, IT professionals can quickly update antivirus signatures at the gateway and perimeter to minimize the impact immediately.
5. Eliminate the vulnerability that allowed the exploit and ensure the system is restored with an optimal security configuration.
6. Complete a break-in report. Break-in reports provide an overall picture of the status of network security. Chronic, increasing break-in reports indicate need to update system security overall and help pinpoint weak points.
7. Based on experience, identify and document tools and techniques that would improve future incident responses. Thoroughly examine how well your procedures worked and decide whether you need to make changes for the future.

# Report of Findings

1. Turn over evidence to the proper authorities.

# AP 5 Revision Dates

* 10/01/2020