IT Security

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

Prepare for problems by:

- Updating all network documentation around the IT system
- Documenting all network data flows to/from Intranet systems 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 via encrypted tunnels or data streams.
- Ensuring that backup/restore procedures are up to date, as are the backups themselves

INITIATION AND NOTIFICATION

The individual that first notices or receives word of an attack should contact the Data (IT) manager and water utility manager immediately by whatever means of communication may be available.

Notification Procedures

Notify immediately upon discovery of the attack:

- Water Utility Manager,
- Data (IT) Manager
- Virginia Department of Health – Office of drinking Water

Others as appropriate (for example):

- Virginia State Police – Virginia Fusion Center
- Internet Service Provider
- Computer Equipment Vendor

Triggers

- More than one user reports unusual behavior of any IT system or software.
- Network intrusion detection indicates a violation.
- Noting unusual IT system activity on holidays, evenings, or weekends.
- Noticing unusual log file entries.
- Discover a presence of new setuid or setgid files.
- Changes in system directories and files are noted.
- Noticing unusual hidden files or ambiguous files, such as those from past incidents.
- Noticing unauthorized altering of users' home pages.
- Noticing accounting discrepancies.
- Identification of Suspicious probes and /or browsing.
- Finding presence of cracking utilities.
- Discovery of unaccounted for changes in the DNS tables, router rules, or firewall rules.

- Unexplained elevation or use of privileges.

Specific Activities

Complete the IT Incident Response and Reporting Checklist. Because the approach to addressing an incident can vary depending on the nature of the incident, it is critical to be aware of the type of incident that has occurred BEFORE taking action.

I. Assess the Problem

1. Protect Customer Information (Take the customer information database, assuming it is a standard database, off the network, so that it is no longer accessible). Note: Do not allow Modems on the database machine.

2. Isolate and Contain the Threat (Insert site-specific procedures consistent with your system architecture)

3. Document the event (See items 4 and 16)

4. Take a snapshot of the system – Obtain forensic images and preserve original media.

5. Registers, peripheral memory, caches

6. Memory (kernel and physical)

7. Network state

8. Running processes

9. Hardware data residue, memory chips, and PDA-type systems

10. Hard disks

11. Disks and backup media

12. CD-ROMs

13. Printouts

Note: 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.

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.

In general, prevent the intruder or the malicious code from working through the network. Attempts to contain the threat should also take into account 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".

Recording all of the details may provide management with the information necessary to assess the break-in and could assist in the prosecution of specific individuals.

A snapshot is 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..

II. <u>Isolate and Fix the Problem</u>

Alerting others in parallel with other steps. Your IT department may know how to fix the flaw in the vendor's software or hardware that allowed the intruder to access your 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.

This action might appear drastic; however, it is sometimes advisable to prevent further loss and/or disruption to the system. Shut down or disconnect resources only when necessary.

Steps for isolating and fixing the problem

1. Save the system state by backing up as much of the system as necessary.
2. Alert others according to the response strategy including contacting a Computer Emergency Response Team.
3. Determine if the system requires disconnection from the network.
4. Determine if the system requires shut down in its entirety.
5. Check for an NIPC water sector warnings (NIPC may contain additional protective actions to consider: http://www.NIPC.gov or https://www.infraguard.org for secure access infraguard members)

III. Monitoring

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.

This action involves learning the intruder's identity or modus operandi (MO). The MO is a mechanism by which the perpetrator commits his or her crime. It is a learned behavior and can change over time. A MO can be a pattern, allowing for some variance. Examples of traps are honeypots (that is, computers designed to attract attackers in order to record their behavior and to gather evidence, but not meant for legitimate users.).

1. Perform real-time scanning and detection to prevent further infection.
2. Set up traps.

IV. Recovery and Return to Safety

This action excludes traffic from hosts that appear to be the source of an attack.

Such as file transfer or calendar services. This action is effective when attackers exploit newly discovered service vulnerabilities. Need to balance the need recovery with the need to preserve evidence for prosecution.

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.

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. Thoroughly examine how well your procedures worked and decide whether you need to make changes for the future.

Steps for Recovery and Return to Safety:

1. Change the filtering rules of firewalls and routers
2. Disable known vulnerable services
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)
4. Update virus signatures

5. Eliminate the vulnerability that allowed the exploit and ensure system restoration with an optimal security configuration.
6. Complete a break-in report.
7. Based on experience, identify and document tools and techniques that would improve future incident responses.

V. Report of Findings

Turn over evidence to the proper authorities so that prosecution for the attack can occur.