SCADA Security

This Action Plan applies to a cyber-attack on a SCADA network system when the cyber intruder is:

- Conducting Denial of Service (DoS)
- Initiating SCADA/DCS command spoofing
- Attempting to take the SCADA/DCS system down
- Attempting to take control of or is in control of the system

Prepare for problems 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 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

SPECIFIC ACTIVITIES

I. Assess the Problem

An attack on SCADA system could occur in several different manners and it may be quite difficult to determine the specific mode of attack or objective of the SCADA threat.

Initial areas for investigation are:

- SCADA is not controlling plant parameters
- Complaints from customers
- Quality of water results
- Inadequate throughput

In a Denial of Service (DoS) attack, an intruder breaks into a number of computers and plants programs that lie dormant until activated by the attacker. The computers then send a steady stream of data packets to a targeted Web site in an attempt to crash a service (or server), overload network links, or disrupt other mission-critical resources. DoS attacks are powerful because they can occur simultaneously from hundreds of remotely controlled computers, thereby amplifying their reach. The objective of a DoS attack is to exhaust the resources of the target until the underlying network fails. The tools for DoS attacks are widely available and found at numerous hacker Web sites.

II. Isolate and Fix the Problem

Restricting access helps to preserve fingerprints for later prosecution (if physical access to systems is involved). These steps isolate the SCADA system from the outside world where the cyber-attack is originating. The SCADA system itself may be malfunctioning because of the attacks with equipment not operating as originally intended. Useful for later reference if the machine requires disassembly for examination.

Merely turning on a Windows computer changes time stamps and other important evidence, for example. Rebooting your computer may launch viruses or time bombs. Altering of access timestamps could occur.

Manual sampling may be necessary if computerized process are not functioning properly. A baseline analysis is important for determining if changes of an unknown nature occurred to the water supply. Contamination may pass through the system unnoticed if an insufficient number of sampling points is used or if misidentification of sampling points occurs.

Steps for isolating and fixing the problem

1. Restrict physical access to the area.
2. Physically unplug any phone lines that could dial in to the attacked computer.
3. Unplug the computer from the network.
4. Determine if the SCADA system needs to be isolated from process operations and needs to be completely off line.
5. Photograph the scene, including connections to any peripherals.
6. IF the computer is off, DO NOT turn it on (preferred method is to jumper system disk drive(s) as read only, and perform a post-mortem on a separate computer using suitable tools.)
7. IF the computer is on, DO NOT reboot it.
8. Avoid accessing any files on the compromised machine.
9. Increase sampling at or near system intakes – consider whether to isolate.
10. Preserve latest full battery background test at baseline.
11. Increase sampling efforts.
12. 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

With the SCADA system down, it may be easier for attackers to enter the site undetected.

1. Monitor unmanned components (storage tanks & pumping stations) – consider whether to isolate.

IV. Recovery and Return to Safety

Establish who within the Utility would comprise a Computer Emergency Response Teams. Their role is to:

- Preserve the evidence,
- Determine the extent of damage,
- Return the system to normal operation.
- The goal is for proper forensics to occur on these logs such that claims of tampering or altering of the logs cannot occur and prosecution can therefore take place.
- The goal is to preserve evidence for identifying and prosecuting the attacker utilizing assistance from the proper authorities in command (FBI, EPA, Virginia State Police, National Guard Cyber Brigade, etc.).

Steps for Recovery and Return to Safety:

1. Solicit the assistance of a Computer Emergency Response Team or Network Forensics Specialists.
2. OR with appropriate training, develop site-specific procedures to:
3. Retrieve logged data from the various equipment and server logs.
4. Collect adequate information (make image copies)
5. With law enforcement/FBI assistance, check for implanted backdoors and other malicious code (i.e., Trojan horse, or worm).
6. Install safeguards and patch to current levels.
7. Test security breach to ensure plugged (in a safe mode, in case the either the problem has not been fixed or some other attack was installed unbeknownst).
8. Assess / implement additional precautions for SCADA system.

Make sure not to return the system to operation prematurely as this may make the utility susceptible to specific attack via purposefully implanted attack pathways. Simply returning the system to operation may be insufficient and invite future attacks. Ensures attacker cannot use the same method to compromise SCADA system. Simply restoring from recent backup media may be insufficient to restore the system to a trusted state.

V. <u>Report of Findings</u>

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