

Computer Security – Is Your Data & SCADA System Vulnerable?

January 31, 2002, MSNBC - “U.S. law enforcement and intelligence agencies have received indications that al-Qaida members have sought information on Supervisory Control And Data Acquisition (SCADA) systems available on multiple SCADA-related Web sites,” according to a Bulletin sent to the FBI by SecurityFocus.com .

IN THE BULLETIN, the FBI indicates members of al-Qaida have scoured the Web in search of methods for gaining control of water supply facilities and wastewater treatment plants through the computer networks used by U.S. utility companies.

Remote control of water or sewage plants is not merely a hypothetical concern. Two years ago, a frustrated computer hacker, seeking retribution for being fired, caused treatment plants in Queensland, Australia to overflow. The break-in caused millions of gallons of raw sewage to be dumped into creeks and parks on the Sunshine Coast, a popular tourist and holiday destination.

Network and infrastructure security has been a national concern for years. With the September 11 tragedy, there has been a heightened awareness to the possibility of future attacks. Increased automation and remote access have opened up our computer systems for potential cyber attacks, causing increased concern for the protection of our nation’s assets and public safety.

The Clinton administration issued Presidential Decision Directive (PDD) 63 in 1998. The PDD outlined the increased need for critical infrastructure protection, specifically listing groups essential to the economy and government. These groups include telecommunications, energy, banking and finance, transportation, water systems, and emergency services. These groups are known to be the most targeted sites for computer vandals and hackers.

In March of 2001, The Computer Security Institute (CSI) announced the results of its sixth annual “Computer Crime and Security Survey.” The survey was conducted with the participation of the San Francisco FBI Computer Intrusion Squad.

Based on responses from 538 computer security practitioners, the survey confirmed that the threat from computer crime and other information security breaches continues to rise and that the financial toll is mounting. Eighty-five percent of the respondents (primarily large corporations and government agencies) detected computer security breaches within the last twelve months. Sixty-four percent acknowledged financial losses due to computer breaches. Of those that quantified their financial losses, the total equated to nearly \$378 million.

The number of attacks through companies' Internet connections is also rising. The number of respondents attacked rose from 59% in the 2000 survey to 70% in 2001.

Utility companies such as electric, water, and wastewater treatment plants are more frequently utilizing automated systems such as SCADA systems. The flexibility that these systems provide for the users also increases the chances for cyber attacks from internal and external sources. In a 1997 report by the NSTAC on the electric power industry risk, "A knowledgeable intruder, aided by publicly available 'hacker' tools, could issue false commands to a utilities energy management system (EMS), opening and closing relays, shutting down lines, and causing voltage oscillations and, potentially, cascading outages." These same threats are possible for all unsecured public and private systems.

In an article on MSNBC.com dated January 14, 2002, the vulnerability of the nation's water supply was addressed. Included in this concern is the possibility of a cyber terrorist attack. "A single terrorist, or even a small group of terrorists could quite easily cripple an entire city by simply destroying equipment at the reservoir end of the pipeline, and even by poisoning the reservoir with concentrated toxins right where the water enters the pipeline," said James Atkinson, a counter-terrorism consultant and principle of the Gloucester, Mass.-based Granite Island Group. The EPA will spend \$90.3 million this fiscal year on water-security issues, as set out in emergency legislation passed last year. That compares with a scant \$2.5 million the agency spent on bio-terrorism efforts in the fiscal year that ended Oct. 2001.

Network and system administrators must remain up to date and system security must evolve along with the threats of offensive capabilities. Possible future attacks could bring about large financial losses as well as potentially severe damage to the national infrastructure affecting public safety and global markets. Proactive network defense and security management are imperative to prevent more serious attacks to infrastructure assets.

How can you protect your agency? Have a network security audit completed.

It's valuable to hire an outside party to perform your security analysis. A third party deals with network security issues on a daily basis and will not make assumptions about the existing security infrastructure. An internal networking or systems administrator may not have the tools or expert knowledge to recognize potential security leaks and gaps, or they may make incorrect assumptions about their own existing security.

An intrusion test and analysis will identify security weaknesses and strengths of your systems and networks as they appear from the inside and outside of your security perimeter.

Phone line scanning will identify undocumented and uncontrolled modems connecting you directly to the external telephone network. Phone and modem lines may represent security holes in your security perimeter.

Performing a hardware and software evaluation will not only provide you with an insurance list in case of physical theft or damage, but it will also provide you with a means to check for any updates imperative for continued security protection.

Checking your systems for access privileges will confirm who has access to your sensitive data. Many companies do not delete terminated employees from their privileges list, increasing the chances for

external hacking by an informed user. Sensitive information may also be accessed by unauthorized persons based upon the building of inappropriate trust relationships with insiders.

An information asset inventory may also be performed. The goal of this inventory is to identify and categorize relevant information resources so that you can make reasoned choices regarding the protection of your information.

If you have a Wireless Access Point attached to your network, you also need an audit performed for wireless security. Radio waves may be reaching far beyond the walls of your building. These same waves that make your office more convenient can also provide an intruder an easy way into your network without detection. Without encryption, user names and passwords, your IP and MAC addresses as well as your machine names are all visible to a packet sniffing program. If an intruder gains access to your network, they may be able to delete data, copy confidential data, originate attacks on other networks from your network, prevent access to your servers, or take over your machines to name a few.

A site survey should be done around your building. This will determine how far your access point's signal emits from your building. Keep in mind that your signals can travel thousands of feet.

You may also look into secure architecture services from a qualified information technologies specialist. These allow you to move to a more secure information systems environment through the proper design and implementation of effective network security architecture, closing your security gaps and leaks. This may involve adding new hardware or software, or simply updating the existing hardware and software already in place.

Once you've completed your security overhaul, you're still not done. You must remain constantly vigilant against future network attacks. This can be best achieved through a security maintenance plan and an ongoing relationship with an information technologies services company.

Sources:

Electric Power Information Assurance Risk Assessment Report. National Security Telecommunications Advisory Committee (NSTAC) <http://www.ncs.gov/nstac/nstac.htm>

CSI/FBI Computer Crime and Security Survey 2001. Computer Security Institute.
<http://www.gocsi.com/>

This CSRMA Bulletin was prepared with the assistance of Technology Development Associates, Inc. (www.tda-inc.com). They are a San Francisco company specializing in network and computer security. Should you have further questions on this issue, please contact Dana Yates at 415-252-2800 x225 or at dyates@tda-inc.com

Please Contact David Patzer, CSRMA Risk Control Advisor for more information on this and other loss control issues at 415.371.5430 or at dpatzer@rfdriver.com.