Cyber-Attackers Breach SCADA Network, Destroy Pump at Water Utility

By Fadelma Y. Rashid | Posted 2015-11-16

Hackers destroyed a pump used by a U.S. water utility after hacking the network of a SCADA vendor and stealing remote access login information.

Hackers breached the network at a water utility in Springfield, Ill. and destroyed a pump, according to a post on the Wired Threat Level blog.

Cyber-attackers gained remote access into the control systems used by the city water utility in Springfield, Ill. on Nov. 8, a security expert told Wired. A water district employee noticed the supervisor control and data acquisition (SCADA) systems used in the facility kept turning on and off, causing the attached water pump to burn out, according to the report.
Almost every SCADA performs well. They’re reliable and flexible, but often lack security.

The major challenge for governments is the inclusion of protection for these critical components in their cyber strategies.

There are many systems deployed with factory settings, pre-set standard configurations.

Attackers could target each of the components to compromise a controlled process.

For example, any supervisory system is usually a computer based on a commercial OS for which it’s possible to exploit known vulnerabilities or zero-day vulnerabilities.

SCADA systems could be infected exploiting attack vectors (e.g. USB sticks) or the network connections.
“... the awareness of cyber threats and the perception of the risks related to a cyber attack are high. Nearly 70% of respondents believe the threat to be high (53%) to severe (16%)”.

"SANS SCADA and Process Control Security Survey" The SANS Institute

SCADA Threats

A list of principal vulnerabilities that have been identified for control systems environments:

- Increased Exposure
- Interconnectivity
- Complexity
- Common Computing Technologies
- Increased Automation
FBI director James Comey said about cyberterrorism:

“There must be a collective effort by all governments to produce continuous report on the security status of critical infrastructures and related SCADA systems.”

“The security component must become part of the project of an industrial system. It must be considered a specific requirement. The overall security of critical infrastructures must be audited during the entire lifecycle of its components.”

“Recently the heads of the Federal Bureau of Investigation (FBI), DHS, and National Counterterrorism Center have declared cyber attacks are the most likely form of terrorism against the United States in the coming years.”

“That’s where the bad guys will go. There are no safe neighborhoods. All of us are neighbors [online].”
Management has a crucial role in security. Its primary task is to provide a strong commitment for the implementation of an efficient cyber strategy.

That includes:

- the assignment of cyber security roles, responsibilities, and authorities for personnel.
- A detailed security policy must be in place that describes how management defines roles and responsibilities.
- Each employee must be informed of all procedures adopted to keep architecture secure.
The goal of management is to:
- define a structured security program with mandated requirements to reach expectations
- provide personnel with formalized policies and procedures.
- Senior management must establish expectations for cyber security performance and hold individuals accountable for their performance.

Dr. Phyllis Scheck, Vice President and Chief Technology Officer, Global Public Sector, McAfee said:

"Achieving security by design is essential in securing critical infrastructure. Cybersecurity must be embedded in the systems and networks at the very beginning of the design process so that it becomes an integral part of the systems functioning."

All plants that host SCADA systems and networks must be assessed.

Due to the fact that SCADA systems are usually distributed over large distances in multiple locations with different physical security measures their protection must be carefully evaluated.
**SCADA Security - Physical**

Physical restrictions that could be applied to improve security to prevent incidents are:

- Restricted access to the site
- Restricted number of technicians responsible for maintenance
- No use of mobile support
- Segregated control network, no connection to other networks
- Each computer is locked in a restricted room or cabinet

**SCADA Security - Connectivity**

- Configure network appliances avoiding the use of default configurations
- Adopt firewalls, intrusion detection systems (IDSs), and other appropriate defense systems at each point of entry.
- Implementation of all security features proposed by SCADA vendors, in the form of updates or product patches
- Audit network connectivity and record the results clearly and accurately about every networked asset

**SCADA Security - Config. Mgmt.**

The NSA document titled “Securing SCADA and Control Systems (CS)” introduces the following suggestions for configuration management:

- Map out and document the entire CS network, including CS and infrastructure device configurations
- Prepare and configure new equipment off-line
- Sanitize old equipment before disposal
- Keep CS infrastructure security features current with device moves, additions, and decommissions
- Enable auditing features and periodically examine the resulting logs for signs of unusual activity
- Synchronize to a common time reference, so audit logs become more useful during incident response
- Develop a Disaster Recovery Plan (DRP) for the CS

---

8/27/2015
SCADA Security - Authentication

- Strong passwords must be implemented
- Identify and assess any source of information, including remote computer networks, phone lines, and fiber optics.
- Implement internal and external intrusion detection systems.
- Audit system logs

SCADA Security - Disaster Recovery

System backups are an essential to the rapid reconstruction of any network. Recovery plans usually include:

- Adoption of redundant hardware and fault tolerant systems
- Fallback mechanisms
- System backup procedure
- Routinely exercised disaster recovery
- Every change to the overall architecture triggers a review of the plan

SCADA Security - Disaster Recovery

Governments and private companies must be able to run simulations of attacks during exercises that have the intent of identifying potential attack scenarios and evaluating potential system vulnerabilities. The exercises must also consider the impact of accidental errors, and the effect of malicious insiders.
Questions?

Brad Schuette
IT Manager
City of Punta Gorda
bschuette@pgorda.us
(941) 575-3354