Cyber Protection of Critical Water Infrastructures at HaGihon - The Jerusalem Regional Water & Sewage Utility

Authors: Shai Shoval, CIO, HaGihon; Daniel Ehrenreich, SCCE

One of the most critical factors affecting the wellbeing of citizens is the orderly operation of potable water and sewage systems. HaGihon – The Jerusalem Regional Water & Sewage Utility is responsible for providing 24/7 potable water and sewage removal services for the one million residents of the greater Jerusalem region. People in this semi-arid region cannot survive more than several hours without these critical infrastructures. Cyber threats, whether intentional or not, have made cyber protection of the water & sewage infrastructures a first priority of the HaGihon management.

Overview

HaGihon Company Ltd ("HaGihon"), the Jerusalem Regional Water and Sewage utility, operates about 50 water and sewage facilities (reservoirs, pumping stations, lift stations, pressure modulators, quality monitoring etc.) in dispersed locations (www.hagihon.co.il). These installations utilize mostly wireless communications and are controlled by a Supervisory Control and Data Acquisition **(SCADA)** system.

Control system experts are well aware that there is no single measure that provides complete system cyber protection. In addition, the HaGihon SCADA engineers realized that the urban utility environment dictates operational continuity and preparedness for unexpected events, and the necessity to keep in mind future network expansion, all without incurring significant and costly changes. Their conclusion: gradual implementation of enhanced cyber defense security measures to the existing SCADA system by deploying only incremental upgrades and add-on solutions.

This Case Study paper highlights the cyber defense challenges addressed by HaGihon, which in our opinion present Best Practice guidelines for the successful deployment of an effective cyber defense for water and sewage systems.

SCADA System Risks

Securing SCADA systems always requires careful evaluation of the installed hardware, operating system, communication network and application software. Therefore, prior to defining the technical solution for an effective defense, it was important to compile and analyze the list of expected threats and associated risks to the HaGihon system.

The existing HaGihon SCADA consists of a single MS Windows™ based control center with a Disaster Recover **(DR)** computer, a variety of radio-based Remote Terminal Units **(RTUs),** Programmable Logic Controllers **(PLCs)** and an Operation Technology **(OT)** network combining physical and wireless media. In the past, control architectures focused on achieving operational reliability and safety while employing outdated hardware and operating system software. The Hagihon's SCADA, just as most systems installed globally, was inherently vulnerable to cyber threats.

The HaGihon experts began the process by identifying the potential risks related to sewage and water supply control that would result from hostile exploitation of the water SCADA system's cyber vulnerabilities:

a) Changing operating parameters - thus causing network disruption
b) Interfering with water quality monitoring and data – thus causing supply outage
c) Blocking information flow to the SCADA center – thus affecting optimization processes
d) Interfering with pressure control and leak detection systems - causing increased losses

Points of Penetration

A second stage to the HaGihon vulnerability analysis was identifying points of potential threat penetration. These include:

a) Unauthorized physical entry of people to remote sites

b) Irresponsible conduct by workers with access to these sites and to SCADA equipment.

It should be noted, that maintaining reliable communication between the SCADA control center and remote sites (RTUs, PLCs, etc.) is critical, however a short interruption shall not cause an outage, and only may degrade the operation efficiency. While the use of public networks, such as the Access Point Name **(APN)** gateway between a cellular mobile network and physical network is convenient and cost-effective, it certainly increases the risk of cyber-attack.

Securing the System

With a clear understanding of the relevant vulnerabilities, the potential threat penetration points, the realization that there isn't a single defense mechanism ("no silver bullet") that provides complete security to the entire system, HaGihon adopted a layered defense. Deployment of a layered defense is also a more challenging defense to overcome and initiates protection measures that prevent unauthorized access. Some of the following solutions are presently deployed, while others are presently being evaluated by HaGihon:

a) Deployment of physical security measures (camera, access control) to field sites and SCADA control center to prevent unauthorized access
b) Effective hardening (blocking/disabling) of all communication ports on SCADA control center computers, communication devices and field control units (BT, Wi-Fi Infra-Red, PCMCA, USB)
c) Strict adherence to company security policy as related to maintaining passwords, exclusive use of SCADA computers for the OT network related internal maintenance purposes, etc.
d) Deployment segregation and zoning of the network using advanced firewall devices. Secure connections using advanced - configurable switches provide enhanced security for each data port.
e) Controlling the access to RTUs and PLCs though a variety of authentication measures. These measures combine controlling the physical access to the remote site (gates) and accessing the control devices.
f) A stateful firewall is inspecting incoming and outgoing data and is well suited for control systems. It performs these inspections with short latency, ensuring that the control process is not impacted.
g) Deployment of “White Listing” procedures assures that no unauthorized application of software code can be installed on any of the SCADA related components.
h) Anomaly detection systems are beneficial for SCADA systems as they do not require upfront knowledge of the attack vector as there refer to a self-learning process as a baseline. The simple "data-crunching" method is ineffective, since the operating parameters are constantly changing.
i) Industrial Intrusion Detection Systems **(IIDS)** are capable detecting anomalous traffic and other irregular processes monitored in multiple locations in the SCADA architecture. It may help detection Denial of Service (**DOS** and Distributed DoS) type attacks.
j) Use of Unidirectional Security gateway for performing SCADA related processes, data collection and management report without actually accessing the database and risking the SCADA process.
k) Utilizing multiple types of wireless and physical communication technologies. When dealing with a wide-area SCADA data network, it is important to employ secured channels involving authentication and high class encryption, in order to minimize the risk of Man in the Middle **(MitM)** attacks.
l) Implementing System LOGs **(Syslog)** to gather events, which in turn are managed by the Security Operation Center **(SOC)** and can be used to generate security alerts.

Summary

Water and sewage utilities are considered critical infrastructures, as they directly affect the welfare and health of the general population. With the growth of cyber capabilities by attackers who are directed by countries and hostile organizations, the challenges of protecting these relatively outdated SCADA and vulnerable systems, have become more complex. Realizing the threats and at the same time the realities of financial limitations and constraints, the management of HaGihon has designed a layered approach combining a range of technical solutions – each targeting a separate segment of the SCADA vulnerabilities – and Best Practice methodologies, and is examining additional solutions for future security improvements.

@@@@@@