Water Sector Cybersecurity Incident Case Study

#001: Ransomware – 2021

SCADA, Source Water Change and Grab Sample Increase

INCIDENT OVERVIEW

A small-size water utility experienced ransomware on a SCADA HMI computer that did not impact water service, but temporarily required a modification to normal operating procedures.

DESCRIPTION

On a Monday morning, the operator came to the water treatment plant and found that the dial-out alarm software on the SCADA computer would not save a change. The operator then noticed a ransomware note on the screen and restarted the computer. After the restart, the computer became unresponsive. The operator also noticed that the municipality's well was not operating as expected and thought there might have been a communications outage. The computer was infected with Lockussss ransomware. The adversary apparently used the utility's remote access application, "RD Client", to gain access sometime between Friday afternoon and Monday morning. There are four individuals authorized for remote access to the system. They all generally connect using their phones and one person also uses a personal laptop.

IMPACT

There was no impact to the delivery of safe drinking water. On the Monday morning of the incident, the water system demand was being met by ample storage in the elevated water tank. That morning the operator restarted the well system and its local disinfection process, which was not dependent on the infected SCADA computer. The SCADA computer is only used for running the treatment plant that processes surface water, which is considered a backup source. When the surface water turbidity is good enough, the treatment plant is operated on weekday days. During the two days that the SCADA computer was unavailable, automatic logging of water quality parameters could not take place, so the primary operator recorded manual sample readings of well water disinfection levels at set intervals for regulatory compliance. Some data was lost on the compromised SCADA computer, but it was not considered important.

Water Sector Cybersecurity Incident Case Study

#001: Ransomware – 2021

SCADA, Source Water Change and Grab Sample Increase - CONT'D

RESPONSE

When faced with the unresponsive SCADA HMI computer, the operator shut down the computer. The operator then disconnected the computer's communications link to the outside world at the advice of their IT contractor. The operator also contacted the state's environmental regulatory agency, local police, and a supervisor. The state's environmental regulatory agency in turn contacted the FBI and the local police contacted the State Police. The utility's IT contractor and SCADA vendor collaborated to restore the SCADA HMI computer within two days. No ransom was paid. After the event, another desktop computer and a laptop computer in the plant were scanned for viruses and none were found. The computers are not networked. The SCADA computer has a direct outside line. The other computers use wireless connections. Since the incident, the water utility has installed a more secure remote access method and is upgrading to Windows 10.

LESSONS LEARNED

Lessons learned from this incident, include:

- Keep the state environmental regulatory agency in the loop when there is a possible risk to water service.
- Use a secure remote access method.
- It is great to have a redundant water source, but if that is not possible have a manual means to operate your system.
- Emergency water interconnections with other communities is another excellent fallback.
- Limitations of SCADA software compatibility can slow down upgrades to new computer operating systems.