Water Sector Cybersecurity Incident Case Study

#002: Ransomware – 2021
IT, Lab Test Data Lost

INCIDENT OVERVIEW

A smaller wastewater utility experienced a limited ransomware incident that impacted part of their office network, but not their operations.

DESCRIPTION

Two of the four desktop office computers at one facility were infected with ransomware software that encrypted the files and made them unreadable. It was not clear how the ransomware made it onto the two systems or why it did not infect the other two computers at the facility. One of the two PCs had been left powered on and displayed blank icons when the user came to work in the morning. When the user went to shut it down in order to restart the system, the operating system said there was another user that might lose data if the shutdown was completed. The system was shut down and came back up but the files were not accessible. The ransomware actor gave the utility three days to pay, or the ransom amount would rise, and if they did not pay, the files would be sold on the dark web. No ransom was paid.

IMPACT

The files on the two computers were lost. One of the computers stored system test results, which were backup daily to an external hard drive. The connected external hard drive was also encrypted. There was an older external hard drive that some data could be restored from. The wastewater system operates manually, so there was no impact to operations and no SCADA system that could have been compromised. The utility does not do the billing for their service and no personal information was lost.

Water Sector Cybersecurity Incident Case Study

#002: Ransomware – 2021

IT, Lab Test Data Lost - CONT'D

RESPONSE

Town management was promptly notified of the incident. The IT contractor reloaded Windows 10 and restored the two impacted PCs within a day or two and added additional security measures. The state primacy agency was also told of the incident and shared the information with another state agency which in turn probably notified the FBI and DHS. There was no follow-up from either agency.

LESSONS LEARNED

Lessons learned from this incident, include:

- Disconnect the external backup hard drive each night to avoid infection of the backup.
- Be prepared to rebuild computers that are compromised.
- Rotate your backups so that your oldest extra backup is not too old.