Florida water hack underscores cybersecurity threat to utilities

waterfm.com/florida-water-hack-underscores-cybersecurity-threat-to-utilities/

By WFM Staff February 12, 2021

Just days before Super Bowl LV kicked off in Tampa Bay, a water system in nearby Oldsmar, Florida, was the target of a cyber attack, renewing concerns around a major vulnerability for water utilities.

The hack briefly multiplied the amount of sodium hydroxide, or lye, used in the city's water treatment, by a factor of more than 100. Lye is an ingredient used in drain cleaners that is also used to control water acidity and remove metals from drinking water.

According to the Pinellas County Sheriff's Department, a plant operator noticed that someone remotely accessed a computer system that monitors and controls chemicals used to treat water as well as other functions. The computer system has a software program that allows authorized users to access it remotely. Then later in the day, a hacker again entered the system remotely and a plant operator observed the intruder opening various software functions that control the treatment of the water, police said.

One of the software functions the hacker took control of was one that regulates the level of lye, increasing the amount from about 100 parts per million to 11,100 parts per million, police said.

The utility stated that even if the pant operator had not noticed the change in levels, it still had other controls and alerts in place to protect any compromised drinking from going out to the public. So far no suspect has been identified and officials are unsure of whether the hack came from someone inside or outside of the United States.

The Wall Street Journal reported that the FBI and Secret Service are also involved in the investigation in addition to the Pinellas County Sheriff's Department.

AWWA CEO David LaFrance issued the following statement in response to the hack:

The Feb. 5 hacking incident on a Florida water utility is a jarring reminder that the threat of cyberattacks on critical water infrastructure is both real and serious. We live in a world where cyber intrusions are increasingly common in our personal and professional lives. Given the essential nature of water service, it's well known that water infrastructure – and water treatment plants of all sizes — are potential targets of people with bad intentions.

While the Florida incident is unsettling, there are some takeaways that should bring us confidence. First, while the hacker was able to gain access, it appears a vigilant water operator thwarted any potential harm. There's no clearer demonstration that water

professionals are essential workers, and the work they do each day protects us all.

Second, the incident makes clear to all water utilities and governing boards that they must take action to prevent or discourage similar attacks. The water sector has been actively addressing cybersecurity issues for many years. In fact, the 2018 America's Water Infrastructure Act requires utilities to complete a risk and resiliency assessment that must include cyber threats to enterprise systems and process control systems. This incident should underscore the urgency of that work.

Third, we are not powerless against cyber threats. There are resources available to help utilities of all sizes. AWWA's Water Sector Cybersecurity Risk Management Guidance and the accompanying assessment tool are free at awwa.org/cybersecurity, as is the Cybersecurity Risk & Responsibility in the Water Sector report and many other helpful eLearning opportunities and documents.

Federal agencies define cyberattacks as the top threat facing business and critical infrastructure. [The Feb. 5] incident demonstrates why. Let this incident be a constant reminder of the importance of round-the-clock cybersecurity vigilance in the days and decades ahead.

Of the top 20 issues facing the water industry, cybersecurity ranked 16th on AWWA's 2020 State of the Water Industry report. For more, an AWWA report detailing cybersecurity risks and best practices can be found here.

Tags: AWWA, cybersecurity