Stateline

Florida Hack Exposes Danger to Water Systems

STATELINE ARTICLE

March 10, 2021

By: Jenni Bergal

A city worker washes down a street after repairs to a water line in Sacramento, California. Cybersecurity experts say water systems need to be vigilant to protect against hackers.

Rich Pedroncelli / The Associated Press

A renegade mouse cursor signaled the danger at the water treatment plant in Oldsmar, Florida.

On Feb. 5, a plant operator for the city of about 15,000 on Florida's west coast saw his cursor being moved around on his computer screen, opening various software functions that control the water being treated. The intruder boosted the level of sodium hydroxide—or lye—in the water supply to 100 times higher than normal.

Sodium hydroxide, the main ingredient in liquid drain cleaners, is used to control water acidity and remove metals from drinking water in treatment plants. Lye poisoning can cause burns, vomiting, severe pain and bleeding.

After the hacker exited the computer, the operator immediately reduced the sodium hydroxide back to its normal level and then notified his supervisor, Pinellas County Sheriff Bob Gualtieri said at a news conference a few days later. Even if it hadn't been quickly reversed, the system has safeguards and the water would have been checked before it was released, so the public was never at risk, he added.

Nevertheless, the Oldsmar breach alarmed state and local officials around the country.

"Officials I've contacted are nervous. There is great concern," said Alan Shark, executive director of the Public Technology Institute, a Washington, D.C.-based nonprofit that provides training and other support to local government information technology executives.

Some states responded to the attack by issuing alerts to water systems. Some also decided to provide additional training and focus more on cybersecurity during their water plant inspections. But many local governments that run water systems lack the money or the personnel to strengthen cybersecurity.

In Wisconsin, state officials sent cybersecurity advisories to all 611 community water systems after the Florida breach, said Miranda Mello, a senior water supply engineer at the Department of Natural Resources.

"This incident is opening a lot of people's eyes because public health is connected to systems that have cybersecurity vulnerabilities," she said.

The state doesn't have a comprehensive way to track the cybersecurity measures that water systems have in place, she said. But it does ask about their security and emergency response systems when staffers inspect utilities every three years.

Because of the Oldsmar attack, Mello said, the state plans to incorporate more questions specifically about cybersecurity during its inspections.

In Massachusetts, the state Department of Environmental Protection issued an advisory to public water suppliers after the Florida attack, warning utilities to be "on heightened alert" for any unusual activity and remain vigilant by evaluating system security.

The agency also is planning additional training for state and water utilities' staff, spokesperson Edmund Coletta said in an email, and is reviewing all regulations and policies.

In New Jersey, cybersecurity officials also sent out a series of alerts after the Oldsmar breach.

“Changing the chemical equation and compounds to treat the water is shocking on the surface, but there’s been a concern about this for a long time,” Jared Maples, director of the state Office of Homeland Security and Preparedness, said in an interview with *Stateline*.

Officials need to be concerned not just about cybercriminals or terrorists trying to target the water supply, he said, but also about threats from insiders, such as disgruntled employees.

While water plants have fail-safes to prevent hackers from compromising drinking water that gets to the public, Maples said, they still have to be on their guard because there’s “no such thing as 100% safe in this game.”

“Our goal is to continually try to stay ahead of them, to make our system stronger and better,” he said. “It’s a constant cat and mouse [game] that we play.”

About 52,000 community water systems operate in the United States, providing water to more than 286 million people year round. Most systems are run by local governments; many are very small.

Small water utilities often don’t have their own IT or cybersecurity staff. They typically are part of city or county governments, but those too may not have the staff or resources to ensure that cybersecurity is strong.

“Sophisticated hackers could take advantage of weaknesses in the system and affect water quality or distribution,” said Michael Arceneaux, managing director of the Water Information Sharing and Analysis Center, a Washington, D.C.-based group that helps water utilities strengthen their physical and cybersecurity. “It could become a public health issue.”

Water utilities that don’t have the resources need technical training and help setting up secure systems, selecting software and hardware, and operating the technology, he added.

Oldsmar Breach

The Pinellas County Sheriff’s Office, FBI and Secret Service are investigating the Oldsmar incident. Investigators haven’t identified a suspect and don’t know whether the attack originated in the U.S. or why Oldsmar was targeted.

“The important thing is to put everybody on notice ... these kind of bad actors are out there,” Oldsmar Mayor Eric Seidel said at the news conference. “It’s happening. So really take a hard look at what you have in place.”

Oldsmar officials said they disabled the program that allowed the intrusion and will make security upgrades.

In response to the Oldsmar incident, four agencies including the FBI, EPA and a federally funded group that tracks cybersecurity issues for states and local governments released a joint advisory warning that "corrupt insiders and outside cyber actors" were using desktop sharing software to victimize targets, including those in the critical infrastructure sector.

The agencies made a number of cybersecurity recommendations and advised organizations to upgrade their Windows operating systems.

They also cautioned that water utilities should install "independent cyber-physical safety systems" that would prevent dangerous conditions if the control system is compromised. That would let smaller systems that have limited cyber capability take steps that would prevent hackers from gaining control of a pump and raising the pH to hazardous levels, as happened in Oldsmar.

The Oldsmar breach has gotten attention in Congress as well.

Calling it a "serious security compromise," U.S. Sen. Mark Warner, the Virginia Democrat who chairs the Senate Intelligence Committee, has asked the FBI for a progress report on the criminal investigation and the EPA for a review of the plant's compliance with federal water security plans.

Shark, of the Public Technology Institute, said it's been hard for local governments to get the funding to beef up cybersecurity at water utilities.

"States have to step up, and they're going to need help from the feds to find ways to fortify this," he said. "There are a whole set of bad actors out there probing for weaknesses to bring certain facilities to their knees."

Sometimes they're able to break through.

In the past few years, water utility systems in Jacksonville, North Carolina, and Fort Collins, Colorado, have been victimized in ransomware attacks, according to a 2019 study in *Journal of Environmental Engineering*. Ransomware hijacks computer systems and holds them hostage until their victims pay a ransom or restore the system on their own.

The study noted that 25 U.S. water utilities had reported cybersecurity incidents in 2015 and that many cases either go undetected or are not disclosed.

Across the globe, hackers who've struck water utilities have ranged from curious amateurs to disgruntled former employees to cyberterrorists, the researchers found.

Remote Systems

In Oldsmar, before the breach, authorized users could use software to remotely monitor operations and check chemical levels to troubleshoot any problems. Many utilities use a similar system, which could become an entry point for hackers, cybersecurity experts say.

"Everything is getting automated these days. A lot of these utilities operate with razor-thin budgets and limited staffing. They'll set up systems where someone can access it from home," said Alex Hamerstone, risk management director at TrustedSec, a company based in a Cleveland suburb that does cybersecurity testing for water plants and other utilities.

If water utilities use passwords that aren't strong enough or terminate workers without changing their passwords, Hamerstone said, that can leave them vulnerable to hackers.

Cybercriminals can use phishing or other methods to try to get into email or billing systems at water utilities, just as they do with other government agencies, he said. But Oldsmar's breach was much more dangerous because it threatened lives, he added.

"Now, if you want to poison water, you can do it from the comfort of your home."

Mello, of Wisconsin's environmental agency, said water systems typically have multiple alarms that will alert an operator if there's an issue going on, and checks and balances to ensure the water quality is at the level that it should be.

But she cautioned that water plants' operating systems need to be up-to-date and staffers should be using strong passwords and multi-factor authentication, a method of confirming identity before someone logs in, usually by entering a randomized one-time password or number sent to a smartphone or email address.

In Manatee County, Florida, officials decided against using a remote system at their water plant, which serves more than 400,000 residents.

"Even if you've got firewalls and other security measures in place, it's still vulnerable. We want to eliminate that," said Manatee County Utilities spokesperson Amy Pilson.

The utility uses an older, closed system that has no remote access, Pilson said. While it is in the process of upgrading to a newer system with tighter security and more safeguards, it will allow managers or superintendents remote access to a dashboard only to look at readings and measurements; not to make changes.

Arceneaux, of the water utilities' security group, said since the COVID-19 pandemic began and more people have been working at home, his group has been recommending that utilities update software, provide training and assess what software and hardware they use—as well as vulnerabilities.

"It's really important that water boards and city councils and top managers take an interest in cybersecurity and provide the investments that are needed to prevent these types of attacks," Arceneaux said.

And water utility officials and others need to understand that it's not just something that can hit a small community, said Kevin Morley, federal relations manager at the American Water Works Association, a Denver-based group that represents water utilities and others in the field.

"This could happen to a large city as well," Morley said. "Water systems, large or small, need to be vigilant. It's a very real threat."

States, Cities Get $325B In Direct Aid From COVID-19 Package

Top State Stories 3/11

AUTHOR

Jenni Bergal
Staff Writer
Stateline

RELATED

Topics Business of Government, Energy and Environment, Homeland Security

Places Florida, New Jersey, Wisconsin

EXPLORE MORE FROM STATELINE

explore by place

explore by topic

About Stateline

Stateline provides daily reporting and analysis on trends in state policy.

ABOUT

Media Contact

Grace Jensen-Moran
Senior Associate, Communications
202.540.6804

Sign Up

Sign up for our daily update—original reporting on state policy, plus the day's five top reads from around the Web.

Email address SUBMIT