CYBER REPORT

America’s drinking water is facing attack, with links back to China, Russia and Iran

PUBLISHED WED, JUN 26 2024•11:16 AM EDT UPDATED 4 HOURS AGO

Trevor Laurence Jockims

KEY POINTS

Cyberattacks on the country’s water systems could damage infrastructure, disrupt the availability or flow of water, and alter chemical levels, contaminating public drinking water supply.

A recent string of attacks on water utilities included systems in Kansas, Texas and Pennsylvania.

Taking out critical national infrastructure has become a top priority for foreign-linked cybercriminals. “All drinking water and wastewater systems are at risk — large and small, urban and rural,” an EPA spokesman said.

Houston Chronicle/hearst Newspapers Via Getty Images | Hearst Newspapers | Getty Images

The city of Wichita, Kansas, recently had an experience that's become all too common — its water system was hacked. The cyberattack, which targeted water metering, billing and payment processing, followed the targeting of water utilities across the U.S. in recent years.

In going after America's water, hackers aren't doing anything special. Despite rising fears of AI use in cyber threats, the go-to criminal way into systems remains preying on human foibles, be it via phishing, social engineering, or a system still running on a default password — "old school" cyberattacks, according to Ryan Witt, vice president of cybersecurity firm Proofpoint.

The rising cybercrime wave targeting key infrastructure led the Environmental Protection Agency to issue an enforcement alert warning that 70% of water systems it inspected do not fully comply with requirements in the Safe Drinking Water Act. Without quantifying an exact number, the EPA said some have "alarming cybersecurity vulnerabilities" — default passwords that have not been updated, vulnerable single login setups and former employees who retained systems access.

While the methods may be simple, an attack last year by an Iranian-backed activist group against 12 water utilities in the U.S. reinforced how purposeful "an attacker's mindset" can be,

In February, the FBI warned Congress that Chinese hackers have burrowed deep into the United States' cyber infrastructure in an attempt to cause damage, targeting water treatment plans, the electrical grid, transportation systems and other critical infrastructure. A Russian-linked hack in January of a water filtration plant in a small Texas town, Muleshoe — located near a U.S. Air Force base — caused a water tank to overflow. "Water is among the least mature in terms of security," Adam Isles, head of cybersecurity practice for Chertoff Group, recently told CNBC.

Psychological impact on the population is also a strategic aim, seen not only in targeting of water assets but the Colonial Pipeline hack that made national headlines in 2021, and in the words of the federal Cybersecurity and Infrastructure Security Agency, featured "snaking lines of cars at gas stations across the eastern seaboard and panicked Americans filling bags with fuel, fearful of not being able to get to work or get their kids to school."

Attacks on U.S. water utilities' IT systems can have a similar psychological impact, and even if the attacks don't directly interfere with the operations of the utility, still lessen public trust in water supply. No hack to date has shut off the water to a population, but that's the bigger worry, said Stuart Madnick, an MIT professor of engineering systems and co-founder of Cybersecurity at MIT Sloan.

VIDEO 03:24

Service hacking by China is meant to create 'panic and chaos', says Fmr. CISA Director Chris

Wichita's system, is minor in comparison to a successful attack on the OT (operating technology) that controls water plants. That is a massive risk, Madnick said, and the threat of it happening is not zero.

"We have demonstrated in our lab how operations, such as a water plant, could be shut down not just for hours or days, but for weeks. It is definitely technically possible," he said.

A recent letter sent by EPA Administrator Michael Regan and national security advisor Jake Sullivan to the nations' governors detailed the urgency of the threat. But Madnick is wary of the government's ability to act quickly or robustly enough to prevent such an occurrence. Budgets, outdated infrastructure, and reluctance to move on an issue that may seem both vital and daunting suggest that the fixes may indeed not come quickly enough. "It has not happened yet, and serious action to prevent 'likely' will not happen, until after it has happened," he said.

Outdated water utility technology

Like any modern system, water utilities rely on technology for monitoring, for operations, and for customer communication. The technology creates vulnerabilities — for providers and users — so the need for enhanced security measures is acute. "The community risk from cyberattacks includes an attacker gaining control of the operations of a system to damage infrastructure, disrupt the availability or flow of water, or altering the chemical levels, which could allow untreated wastewater to be discharged into a waterway or contaminate drinking water provided to a community," said an EPA spokesman.

Witt says there are some initial steps to take in improving the cyber hygiene of dated systems. "Improving password strength, reducing exposure to public-facing internet, and the need for cybersecurity awareness training," would go a long way to shoring up defenses, he said. Another potential fix is the deployment of what are called air-gapped systems that separate supervisory and control systems from other networks. Since the easiest way into these systems is to obtain credentials and then exploit the system, "A systems admin should not be able to access office systems such as email and be able to operate a control panel of a water system from the same laptop," Witt said.

For the most part, attacks that have occurred have been preventable, according to the EPA.

While it has not been a tool needed to date in these water utility attacks, AI is coming alongside [illegible] cyber efforts of geopolitical rivals. "Rapid advances in artificial intelligence are [illegible] threat actors more sophisticated tactics, techniques, and procedures to penetrate [illegible] technology that controls critical infrastructure facilities," the EPA spokesman said. "These attacks have been linked to a variety of types of malicious actors, including hackers [illegible] either of or in support of other nations who could use disruptions to U.S. critical [illegible] to their strategic advantage."

RELATED

New Apple iPhone app proves how hard it is to kill the online password

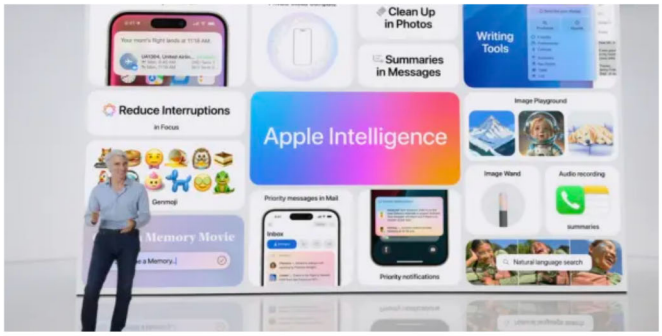
Microsoft employees' cybersecurity contributions will factor into their pay

Cyberattack shuts down car dealerships

Businesses need to be wary of cyber risks from vendors, says Fortalice Solutions CEO Theresa Payton

MORE IN CYBER REPORT

VIDEO 07:57



New Apple iPhone app proves just how hard it is to kill the online password

Michelle Castillo

Microsoft employees' cybersecurity contributions will factor into their pay

Jordan Novet

READ MORE

GET IN TOUCH

Advertise With Us

PLEASE CONTACT US

CNBC Newsletters

Sign up for free newsletters and get more CNBC delivered to your inbox

SIGN UP NOW

Get this delivered to your inbox, and more info about our products and services.