SOURCE: © SHUTTERSTOCK

Florida drinking water plant hack briefly raised sodium hydroxide levels 100-fold

BY TIM WOGAN | 11 FEBRUARY 2021

A hack targeting a US drinking water facility just outside Tampa, Florida increased the levels of sodium hydroxide more than a hundred-fold. The motive for and agents behind the attack, which was detected before the public was put in any danger, remain unknown, but it demonstrates the dangerous vulnerability of chemical plants and other critical infrastructure to cybersecurity breaches.

To most laboratory chemists, sodium hydroxide is to be treated with extreme caution: it is the principal component of most drain cleaners because of its ability to dissolve organic material, including the skin of any experimenter foolish enough to handle it without gloves. It might surprise some, therefore, to learn that minute amounts of sodium hydroxide are commonly added to drinking water. The reason is that, over time, acidic or even neutral water can leach toxic metals ions – predominantly lead – from pipes and solder that carry the water into and around buildings with old plumbing. Weakly alkaline water is less corrosive to metal, and as sodium hydroxide is such a strong alkali facilities need only

add tiny quantities to raise the pH to around 8.5 – something that has no ill effects on humans. One facility to do this is in Oldsmar – a Florida city of just over 15,000 people.

On 5 February, an operator at the Oldsmar water facility noticed that the cursor on his computer screen was moving without his intervention, and he reportedly assumed that his supervisor was working remotely using software called Teamviewer. When, however, his cursor began its unprompted wanderings again several hours later, he was alarmed to see the cursor reset the level of sodium hydroxide from its usual 100ppm to 11,100ppm – a level that 'would almost certainly have caused chemical burns', says Patrick Coyle, who, after spending 20 years in the chemical process industry, now writes the Chemical Facility Security News blog. In the event, however, the operator immediately intervened to reset the levels and reported the problem. Even if he had not, Mayor Eric Seidel said in a press conference, 'there's redundancies and alarms in this system that would have caught the change in the pH level anyhow', so there was no prospect of caustic drinking water reaching consumers.

Mystery attacker

Whether the attack was foreign or domestic remains unknown, but Sheriff Bob Gualtieri told the press that 'in order to get into the system, somebody had to use some pretty sophisticated methods'. Many cybersecurity experts, however, are skeptical. 'A sophisticated attacker would probably not have used this method of conducting an attack because it was so easily detected by an operator on the scene, who was able to take immediate action,' Coyle says. 'This sounds more like somebody who stumbled into a vulnerability and was seeing what they could do with it than, say, a nation state attack or something like that.'

Coyle doubts that a sophisticated attacker undertaking a concerted attempt to poison a city's water supply would use one of the approved additives such as sodium hydroxide. This is because of the safety monitoring protocols in place for these, although he acknowledges that 'the fact that this attack did occur, and was successful for a couple of minutes anyway, suggests that a more sophisticated attacker with knowledge of the system and knowledge of the controls for how that specific facility were laid out would have been able to not only increase the dosage of sodium hydroxide going into the water system, but would have been able to ensure that the reporting from the pH meters downstream would not have shown up in a manner that triggered an alert. This is the problem with allowing external access to an industrial control system.'

Coyle suspects that the vulnerabilities exposed by the Oldsmar plant hack are widespread. 'Particularly since the Covid-19 pandemic has made remote operation of all sorts of things more common, I believe that there would be a number of water systems – perhaps even some large ones – that have authorised unusual levels of external access because of operational needs,' he says.

The issue spreads well beyond the water industry into other areas of critical national infrastructure and certain precautions should be observed, says Coyle. 'An operational control system should be isolated from all other networks,' he says, 'but there are going to be various operational requirements for which facilities feel they need to provide access to that network from places outside… I can imagine instances where the plant manager gets a call in the middle of the night about an emergency at his facility and wants to see more details than he can get verbally from his operation team on site.'

Nevertheless, he says: ‘A sophisticated attacker who’s got lots of time and money and resources will be able to hack any system they want to. Anything that is made by man can be subverted by man.’