What can we learn from the Oldsmar water supply hack?

Following the recent water supply hack in Florida, Phillip Corner, industrial systems cybersecurity expert at Cougar Automation, stresses the need for business decision makers and technical professionals in safety and security to work closely together to understand risk.

On Friday 5th February, a hacker used a common remote access application to take control of an employee's computer at the municipal water treatment plant in Oldsmar, Florida. During the cyberattack, which required little sophistication, the hacker changed the level of sodium hydroxide in the town's water supply from 100 parts per million to a dangerous 11,100 parts per million.

It is not yet clear what real risk this posed to the safety of the water supply, since well-designed systems would have multiple levels of checks for potentially dangerous chemical concentrations. Still, this kind of intrusion is a growing concern not just for water plants but all operators of critical infrastructure, many of whom are undergoing digital transformation and may have had to accelerate plans for remote access because of COVID-19.

Without effective cybersecurity measures, the same systems that allow engineers and contractors to remotely carry out routine adjustments and maintenance can also be exploited by hackers wishing to inflict harm.

The investment challenge

The municipal utility system in the USA, where each town or city has its own small water and electricity companies, means that providers may not have the resources to implement complex cybersecurity protection, leaving them especially vulnerable to attack. Although we have a different model in the UK, where larger private companies supply utilities regionally, British operators still face investment challenges.

Ofwat (The Water Services Regulation Authority) highly regulates what private water and sewerage companies in England and Wales can spend on improving their infrastructure. They are required to set out their budgets for improving quality, replacing outdated assets and implementing security measures as much as five years in advance. This is problematic given the risks of cybercrime are evolving much faster than the investment allocated to mitigate them.

Make do and mend

Moreover, a common factor across industry is that with a limited budget for modernisation, there may be little appetite for going back and investing in improvements to old systems if companies can make do a bit longer until a new system is installed. Our approach when working with customers on existing systems is to help them understand where the greatest risks are and suggest a package of improvements that will achieve the best cost-benefit ratio until it is time for replacement. If remote access is the biggest risk, for example, we can look at securing it with a cost-effective solution to reduce the risk in the meantime.

If it is not secure, it is not safe

Of course, cybersecurity should be an integral part of every new tender in the same way that safety is – not a bolt-on solution – and we are seeing this mindset shift across the industry. Nobody would dream of leaving safety risk assessment until the end of a project and the same is true for cybersecurity. The IEC 61511 safety standard for the process industries updated in 2016 essentially says that any system dealing with functional safety must include cybersecurity measures. The guiding principle is that if it is not secure, it is not safe. And since the NIS (Security of

Network & Information Systems) regulations came out in 2018, essential service operators, including utilities, are legally bound to consider cybersecurity. If an operator is hacked and someone gets hurt, the operator can be prosecuted under safety legislation.

Secure by design

In the case of the Oldsmar attack, many might wonder why it was possible for anyone – authorised or otherwise – to make such a drastic change to the level of a potentially dangerous chemical. Processes have diverse requirements so when designing systems for industrial processes, we work with the customer to identify their unique requirements and set reasonable limits for all eventualities to match the physical sizing of the plant.

It is also good systems integration practice to have other checks and balances in the background that alert to any anomalies. Lessons learned mean safety monitoring systems are continually improved and in many cases these systems are an ultimate failsafe for cyber incidents. However, we should not get to the stage where we are relying on safety measures to mitigate cybersecurity attacks. Safety and security professionals can work together to minimise vulnerability to targeted attacks as well as accidents.

The broader industrial risk

The Oldsmar incident was an intentional malicious action, although it is not yet clear if this was specifically targeted at the operator. However, all operators are at risk of untargeted or collateral disruption from ransomware. If an attacker can gain remote access like this they could also use ransomware for extortion, but ransomware need not be specifically targeted. Vulnerable Internet connected devices, infected portable computers, and USB flash drives can all result in infection.

Ransomware is one of the biggest risks in industry right now and for organised criminals today cybercrime is what narcotics were in the 1980s. This makes it vital for all businesses to take steps to protect their people, equipment, local environment, reputation and finances from harm – and at VINCI Energies we help our customers with the whole range of cyber risk controls.

Prev

Back to the list