Case Study

TOKIO MARINE
KILN

Cyber Business Interruption

Industrial Control System Security

At 8am, a plant operator at the Oldsmar water treatment facility in Pinellas County, Florida detected unauthorised remote access to a computer system he was monitoring. At 1.30pm someone gained access again, opening various software functions within the industrial control systems environment, including one that controls the amount of sodium hydroxide in the water supply.

Sodium Hydroxide (also known as caustic soda) is the main ingredient in drain cleaning fluid and is used to remove metals from potable water and regulate water acidity. The intruder altered the values in the system in an attempt to increase the level of sodium hydroxide from 100ppm to 11,100ppm. Thankfully the plant operator detected the change and reduced the levels back to the appropriate amount. At no time was there an adverse impact on the water supply.

cyber [ctrl]

Industrial Control System Security: What can be learned from the Oldsmar Intrusion?

TMK Cyber Underwriter Paul Gooch explains why the incident at the Oldsmar water treatment facility in Florida is a vivid reminder that industrial control systems are vulnerable to cyber-attacks – and what they can do to prepare.

What happened?

At 8am on Friday 5th February, a plant operator at the Oldsmar water treatment facility in Pinellas County, Florida detected unauthorised remote access to a computer system he was monitoring. At 1.30pm someone gained access again, opening various software functions within the industrial control systems environment, including one that controls the amount of sodium hydroxide in the water supply. Sodium Hydroxide (also known as caustic soda) is the main ingredient in drain cleaning fluid and is used to remove metals from potable water and regulate water acidity. The intruder altered the values in the system in an attempt to increase the level of sodium hydroxide from 100ppm to 11,100ppm. Thankfully the plant operator detected the change and reduced the levels back to the appropriate amount. At no time was there an adverse impact on the water supply.

How did this happen?

Full details of the attack methodology, including the sophistication of the techniques used, are not publicly known. At this stage we know that the intrusion was a result of unauthorised remote access. This is a common attack vector against industrial control systems due to the fact that maintenance and upgrades on such systems are often performed remotely rather than locally. So, when we refer to a 'cyber-attack', it could have been as easy as stealing an employee's username and password and using them to login via a legitimate remote access interface.

Has it happened before?

TMK has previously detailed the increasing prevalence of intrusions into industrial control systems (see blog here). Historically such attacks have been accepted as being theoretically possible, but not commonly carried out 'in the wild'. In 2017, researchers at Georgia State University developed malware that was capable of commanding industrial control systems at water facilities to shut valves, increase the amount of chlorine added to water, and display false readings. In May 2020, the head of Israel's National Cyber Directorate revealed that the country had thwarted a major cyber-attack against its critical water infrastructure, declaring that "If the bad guys had succeeded in their plot, we would now be facing, in the middle of the corona-crisis, very big damage to the civilian population and a lack of water and even worse than that."

What's the end goal of the attackers?

It should be reiterated that nothing is publicly known regarding the intentions of the intruder at the Oldsmar water treatment facility. Prior incidents at different facilities and threat intelligence from private and national cyber security organisations point to a wide variety of potential motives and threat actors. It could have been a 'bedroom enthusiast' looking to highlight deficiencies in industrial control system security more generally, as was the case with Dillon Beresford in 2011. It could have been a disgruntled ex-employee, similar to the Maroochy Swire attack in Australia in 2001. It could have been a criminal organisation looking for a way to gain an illicit financial benefit from such an attack, as we have seen with the huge increase in ransomware incidents in the past 18 months. It could also have been a terrorist group or nation-state, perhaps using the Oldsmar water treatment facility as a 'proving ground' for future, more widespread attacks on critical infrastructure. The focus on this event should be less on 'whodunnit' however, and more on how organisations can protect themselves from such intrusions, irrespective of who the threat actor is and what their motives might be.

How can organisations make themselves less vulnerable to attacks?

Strong industrial control system security controls form a core part of the insurance underwriting review process for TMK's critical infrastructure clients. TMK looks to partner with organisations that have implemented a robust security program, ideally based on industry best practices. With respect to water infrastructure specifically, an excellent free public resource is available from the US Water Information Sharing and Analysis Center (US Water ISAC). In 2019, it released its 15 Cybersecurity Fundamentals for Water and Wastewater Utilities. More generally, operators of critical infrastructure should disable remote access functionality on all assets except where absolutely necessary. Where remote access is deemed necessary, TMK would expect clients to take the following steps:

1. Ensure that there are no ICS assets directly connected to the internet – where internet connectivity is required, segregate ICS networks from the outside world using a Demilitarised Zone (DMZ) network architecture.
2. Limit the number of users who have remote access capabilities and the number of services and systems they have remote access to.
3. Use multifactor authentication – ensure that more than just a username and password are required to login.
4. Ensure remote access sessions are logged and monitored.

TMK looks to partner with organisations that have implemented a **robust security program,** ideally based on industry best practices

TOKIO MARINE
KILN

Tokio Marine Kiln
Tokio Marine Kiln is a trading name of Tokio Marine Kiln Insurance Limited (Registered Number 989421) and Tokio Marine Kiln Syndicates Limited (Registered Number 729671) which are authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority under Firm Reference Numbers: 202574 and 204909 respectively. The registered office of both companies is located at 20 Fenchurch Street, London EC3M 3BY. A member of the Association of British Insurers.

To Be a ***Good Company***