Water utilities

Digital security: How safe are our water utilities?

Reports of cyber threats against utilities are on the increase. But what do the threats consist of, and how worried should we be?

Article by Görrel Espelund.

In recent years, cyber-attacks against critical infrastructure, such as water utilities, have been on the increase globally. However, growing awareness doesn't necessarily translate into the implementation of better security protocols and safer systems. And, in the developing world, water distributors also face a range of other challenges to maintaining safe water distribution.

When discussing cyber crimes, focus is often on security breaches in the private sector, especially retail and banking. But according to several studies conducted in the last few years, cyber attacks on vital infrastructure such as electrical grids and water distribution systems have escalated.

In a blog in *The Huffington Post Business*, Michael Deane, Executive Director of the National Association of Water Companies in the US explains how the evolution of computer-based management systems has, on the one hand, improved the reliability and quality of water services, but on the other has increased the possibility of targeted or accidental cyber events that could lead to disruption in the water supply.

He concludes: "In the drinking water and wastewater sectors, a cyber attack could hone in on four different threat vectors: chemical contamination, biological contamination, physical disruption and interference with the highly specialised computer systems controlling essential infrastructure known as Supervisory Control and Data Acquisition (SCADA) systems. A successful attack resulting in consequences in any of these areas could cause major damage, resulting in long periods of operational downtime, financial losses and most importantly, a threat to public safety."

According to Deane, the awareness of possible cyber attacks is steadily growing. Since 2013, November has been designated as "Critical Infrastructure Security and Resilience Month" with the aim of recognising the importance of protecting critical infrastructure in the US.

Even so, last year the US Department of Homeland Security received 159 reports involving "vulnerabilities in control systems components". Most of the vulnerabilities involved systems used in the energy sector, but water utilities and wastewater are also considered at high risk of cyber attacks, according to Water Online.

But cyber attack on vital infrastructure is not a phenomenon occurring in the US alone.

The Ponemon Institute, a research centre that specialises in data protection and information security policy, released a study in 2014 in which two thirds of 599 IT security executives in 13 different countries admitted to having had "at least one security compromise that led to the loss of confidential information or disruption of operations" in the previous year.

However, there is a large discrepancy between being aware of the risk and protecting the systems from it.

Dr Renier van Heerden, Principal Engineer and Researcher at the CSIR points out that because the risk of cyber attacks on a country's infrastructure is still considered fairly low, companies have yet to take the threat seriously enough to start investing in safer systems.

"Companies' main concern is uptime, to keep the systems running without disruption. To achieve this, they'd like robust and dependable systems. Unfortunately that runs contrary to security," he says.

The reason behind this is simple: if you add a layer of security to systems such as SCADA, used to control dams, power plants and water treatment facilities, it increases the risk of small configuration faults – which, in turn, can cause major problems or lead to down-time.

Firewalls and encryption, the most commonly used industrial cyber security programmes, are complex systems, and their configurations can be difficult to understand and verify.

"So we find that we have two competing mechanisms. Traditionally, because the world wasn't so interconnected, the openness and the robustness of the systems used to be more important than security. But with the technology changing and the world being more interconnected, security has become more important.

Companies – state-owned or private – look at the history when they make risk analyses. And up to now it hasn't been worth it to invest in that extra security measure. In my opinion, it's a mistake," van Heerden says.

The most infamous cyber attack on physical infrastructure in the world is the Stuxnet malware. It is believed to have been built jointly by the US and Israeli governments to sabotage Iran's nuclear programme in 2007/2008. It then accidently spread in 2010 and became widely known.

Malware such as Stuxnet, BlackEnergy and Havex are specifically designed to target industrial control systems – and attacks on vital industries and infrastructure are frequently reported in various Internet and computer magazines. However, when it comes to the developing world, things look a bit different.

Neil Macleod, former head of eThekwini Water and Sanitation who won the 2014 Stockholm Industry Water Award, points out that no matter how secure you try to make your system, it is only as good as your last password and the integrity of your staff.

"You have to be sure that you have a staff of happy workers and that they comply with the very rigorous security protocols in place. Compared to developed countries the issues are slightly different in the developing world. Richer countries have more computer-based solutions and therefore they are more vulnerable to these kinds of attacks. In developing countries we tend to have teams on every site."

"We do our work with limited computer-based systems, limited remote operations and a lot of on-site operations," says Macleod.

It is only large cities like Cape Town, Johannesburg and Durban that have started to move towards a computer-based management of operations, which also makes them more prone to cyber attacks. But Macleod is not worried.

"People can start hacking into the systems of the big cities and cause interruption to the service for a few hours before we notice what is going on. On the sewage side, there is a possibility that hackers could mess up the dosage [of chemicals] and then the river will be polluted, which is unacceptable, but recoverable. In the case of water purification plants, however, the impact could be more severe in terms of public health in that the water may not be safe to drink if the disinfection or coagulation processes are affected," says Macleod.

> *"The biggest problem for developing countries, where the level of IT and computer-based technology is pretty low, is not cyber attacks but poverty."*

Not even the department is safe

Earlier this year the Department of Water and Sanitation became the victim of a hacking sting. Hackers from the Anonymous collective broke into the official website of the department, breached the site's database, stole all its data and dumped it online. This included real names, emails and identification numbers of over 5 800 employees and collaborators. Even personal details such as phone numbers, addresses and passwords were revealed.

eThekwini Water and Sanitation received the Stockholm Industry Water Award as a recognition of its work to provide, within a few years, 1.3 million people in greater Durban (eThekwini) with piped water and 700 000 people with access to toilets.

"The biggest problem for developing countries, where the level of IT and computer-based technology is pretty low, is not cyber attacks but poverty. Poor people who try to tap into the water utilities illegally do most of the damage caused to our systems. Another big problem causing disruption is theft of the metals, valves or copper cables.

That is a constant scourge that we, and most developing countries, face. The people sell the goods to be able to buy bread, but the value of the metal is many times less than the cost of the repairs," concludes Macleod.

Article republished with the kind permission of the Stockholm International Water Institute (SIWI). Visit: http://www.siwi.org/publications/stockholm-water-front-no-1-2016/ to view the original article in the Waterfront magazine.