Timothy Compston finds out why utility providers are switching on to emerging cyber security threat

POWER PLAY

It is all too easy to sit back and take the electricity that powers our day-to-day lives and the water we drink for granted, especially as we are in an era which is far removed from the days of "blackouts", "brownouts" and stand-pipes. But, while things may seem smooth on the surface, the reality is more turbulent behind the scenes. This type of critical national infrastructure is under threat like never before, most especially from cyber attack.

The cyber security deficit that is often flagged up for power and water plants in particular is certainly not helped by the fact that vital control systems may need to be kept up and running around-the-clock – over months or even years in some cases – with any unplanned downtime impacting, potentially, on millions of people. Sadly individuals, terrorist groups and most especially state actors are all thought to be plotting to hack into and take control of such systems with malicious intent. Here we weigh up the potential impact of such attacks, report on some near misses and seek advice on what needs to be done to shore up the defences of assets from power stations to the electricity grid itself.

In the US, a researcher at cyber security specialist Trend Micro recently claimed that a Chinese hacking group, referred to as "APT1" and allegedly linked to the Chinese army, was involved in the hacking of a "decoy" water plant. The regular drip, drip, drip, of similar stories serves to underline that it is not just disgruntled hackers sitting in their bedrooms or criminals intent on extortion who have critical national infrastructure in their sights. In fact, as we will see, a number of high profile incidents have all the hallmarks of state-sponsored cyber activity.

In the above case, a dummy control system was set-up by a Trend Micro researcher, Kyle Wilhoit, who told the Black Hat conference in Las Vegas about the attack which took place in December 2012. APT1 gained access to the system via a word document containing malicious software. The most surprising thing which came out of this, in Wilhoit's view, was the fact that that APT1 – otherwise known as the "Comment Crew" – would want to hack into a local water authority plant. But their behaviour made it pretty clear that this wasn't just an accident; the dummy control system was directly targeted by the hackers.

Perhaps one of the most high profile examples of a cyber attack in recent times, with hints of state involvement, relates to the use of Stuxnet malware. Designed to target industrial control systems, allegedly with the intention of disrupting Iran's nuclear facilities, Stuxnet first come to the world's attention back in 2010. This was followed, over the next two years, by hacks deploying a range of computer viruses, aimed at, among other things, the Bandar Abbas electricity supply company and the Kharg

Island oil terminal – essential to the country's oil exports. Not surprisingly, Iran put the source of these attacks down to the US and Israel, claims which of course neither country is likely to confirm.

One wider concern that comes out of all of this, which cyber security expert, Eugene Kaspersky brought highlighted in late 2013, is that although this sort of activity is engineered by governments and has a specific target such as Iran's nuclear centrifuges, once the genie is out of the bottle it can become a bit of a "boomerang". To make his point, Kaspersky revealed that he had heard that the Stuxnet virus had actually gone on to "badly infect" a Russian nuclear power plant, which wasn't the original intention of its creators.

"Unauthorised access to systems was nearly twice as prevalent in 2014 compared to 2013 among the top five industries targeted during cyber attacks"

Over in South Korea, it was reported last December that South Korea's nuclear plant operator KHNP was gearing-up to conduct cyber security drills at four of its facilities to assess its ability to withstand a cyber-attack. This well publicised move to shore-up KHNP's cyber defences followed on from the leaking online of designs of plant equipment and associated threats from an "anti-nuclear" hacker. Although at the time KHNP was keen to allay any fears, saying that the leak had not impacted on safe operation, such incidents must ring alarm bells for any nuclear plant operator; next time it might involve a group, or government, with more sinister motives than simply wanting to protect the environment.

EY's 2014 Global Information Survey highlighted a lack of resilience in relation to "operational technology [OT] systems" such as power generators. In particular, the authors of the report lament that securing OT systems is "not an easy task". The main issues, they assessed, centre around the complexities of OT environments, legacy systems, and cultural differences between OT and IT teams. The report also referred to the fact that, because it is relatively easy to access OT systems via IP-addresses, they tend to be firmly in the sights of cyber criminals. Citing examples of attacks across a range of sectors to underline the dangers, the report refers, for instance, to malware which "destroyed" the control systems of an unnamed nuclear power plant.

This growing complexity is something which Peter Jopling, deputy global leader of IBM Security's "Tiger Team", is also keen to address. "Most of these process control on SCADA (Supervisory Control and Data Acquisition) systems," he said. "These are relatively old and the technology was never envisaged to have layered security."

Jopling also highlighted an added complication: "The challenge now is that utilities want to take these systems 'online' so they can carry out checks and monitor them, and do process-orientated controls, as opposed to having to physically go to them," he said. "If I can access that particular device and appliance then what is to stop someone else being able to that?"

Jopling reiterated that any solution to this problem must accommodate the fact that many of these systems cannot be patched up from a security perspective because of their age – many date from a time before networking. "So how can we open up the infrastructure and then allow people to do what they need to do in a secure manner?" He suggests that one strategy is to create what he terms a "security bubble" around these devices to actively monitor what is going on. "You have got external people, contractors, coming in, and you also have issues in terms of employees, either deliberately or accidentally doing things while they are on the 'other side of the wire' in the secure zone," he said. "The risk is they accidentally mis-configure something or load software which may not have been fully tested. There are vulnerabilities there."

POWER PLAY

Powerful target: the impact of a successful cyber attack on utilities could be severe

He added that operators also need to be alert to the headaches thrown-up by portable media which can easily hide malware and when they are connected evade the security mechanisms around the perimeter.

Jopling highlighted an incident a few months earlier which, while not directly involving a power plant, brings into sharp focus just how much damage can be caused by hackers. "In Germany they allegedly had a malware attack on a blast furnace at a steel works," he said. "The end result was it being shut down. That may not seem too onerous, but actually when a blast furnace cools you effectively have to rebuild it because all the bricks start falling out."

Although other sectors ranked higher on the cyber attack scale in IBM's 2015 Cyber Security Intelligence Index, the fact that energy and utilities entered the top five last year is concerning. Another worrying development to come out of the Index is that unauthorised access to systems was nearly twice as prevalent in 2014 than in 2013 among the top five industries targeted during cyber security incidents.

So what is being done to redress the balance? In the US, for example, Presidential Executive Order 13636 – "Improving Critical Infrastructure Cybersecurity" – was a catalyst for NIST to come up with a voluntary framework for improvement. This has been well received by infrastructure operators on the frontline as well as overseas governments.

Matt Barrett, programme manager at NIST, explained further. He feels that the cyber security framework – which seeks to bring together the best of existing standards – is more powerful as a voluntary arrangement. "That keeps it within a security operation as a dynamic risk decision-making tool," he said. "The moment we make things mandatory, things like the cyber security framework get relegated under the legal structure and CFO of an organisation where they tend to be a little bit more risk averse and compliance orientated. So companies then look at what they have to do – usually the bare minimum – to satisfy any external auditors."

Barrett reported there has already been a great deal of international interest, including from the UK, in the framework which was released in February 2014. "I believe our country-count of the number of governments that have interacted with us now is 24," he said. "We certainly have been in dialogue with four out of the five Five Eyes [an intelligence-sharing arrangement between the US, Australia, Canada, New Zealand and the UK], 11 of the European Union nations, five nations in Asia and four in the Middle East." How nations want to fit the framework in with what they are doing does vary, however, as Barratt explained. "Some nations are saying this is great, the framework is going to be their framework, and others are saying they really like the principles," he said.

Ultimately, it is evident that the cyber threat to critical national infrastructure such as power stations is on the rise. Any initiatives which make things more difficult for the hackers, such as the creation of a framework such as that being delivered in the US, is therefore a step in the right direction, along with a greater appreciation of the sorts of vulnerabilities that are out there.

Timothy Compston is a journalist and PR professional who specialises in security issues. He studied International Relations and Strategic Studies at Lancaster University, is PR director of Compston PR and a previous chairman of both the National PR Committee and CCTV PR Committee of the British Security Industry Association (BSIA).