CYBERSECURITY

Countering attacks on energy networks

Increasing cyberattacks on energy infrastructure are the new realities to which companies must adapt. *Maria Kielmas* reports.

Stuxnet, Industroyer, WannaCry, Petya/NotPetya and Triton are just a few of the actors in what has become an everyday story of malware attacks on digital systems that control critical infrastructure. Targets have ranged from power generation to water treatment, communications, healthcare provision and manufacturing processes while experts report that the frequency of cyberattacks is growing at over 20% annually. Although these hacks caused major problems such as eight-hour long power cuts in 2016 in Ukraine, there has been no physical damage to date. The hackers using the Industroyer malware in Ukraine may have been information technology (IT) experts but apparently didn't understand the physical nature of power distribution and control systems.

Such a situation may not last, however. Michael Shalyt, CEO of Haifa, Israel-based cybersecurity company Aperio Systems, wonders what will happen when the hackers attack the physical infrastructure itself after discovering its vulnerabilities. He refers to the data that supports the decision-making process in, say, a power generation plant or oil refinery. Such data is transmitted through thousands of sensors in any one plant. If these become corrupted, there is a serious problem. 'Today we can use digital technology to blow things up,' he notes.

Although energy companies are increasingly aware of cyber risks they remain reluctant to discuss the issues (see **Box 1**) and to dedicate sufficient funds for its mitigation. 'US utilities are mandated by law to provide the most reliable power at the lowest cost,' says Justin Thibault, Senior Technical Leader at the Palo Alto, CA-based Electric Power Research Institute (EPRI). 'They have to weigh those investments carefully. They want to meet regulatory obligations as quickly and as affordably as possible for the benefit of the customer, but compliance alone does not always guarantee cybersecurity.'

Control systems

The control systems that operate physical processes in an energy or other industrial plant work within the operating technology (OT) environment where priorities are different from those of the standard IT systems. IT systems value confidentiality, integrity and availability, in that order. The loss of a bank's client information can be catastrophic but a 15-minute computer downtime is only inconvenient. OT systems' priorities are reliability, maintainability and availability. A 15-second production interruption could be disastrous.

Originally, the OT and IT systems were physically isolated from one another with internet access restricted to the IT side. But this isolation has largely been replaced by an IT/OT connection to enable remote control of numerous production locations and large networks including smart electricity meters. The result is an integrated system that ranges from supervisory control and data acquisition (SCADA) to large-scale industrial controls system (ICS) architecture. SCADA protocols control the interaction between various field systems such as the programmable logic controller (PLC) or remote terminal units (RTU). The whole integration process has spawned numerous cybersecurity risks, especially at the IT/OT connection, where the hackers may be hostile state-sponsored agents rather than lone wolves.

The last few decades of mergers, acquisitions and asset disposals in the energy sector have added to security problems. OT systems are built to last 20 to 30 years while IT systems are revamped every two years. The result is that a company has a lot of physical assets no one knows about, and you can't protect what you don't know. 'When we talk to utilities we often see a system in chaos,' says Andrew Ginter, Vice President of Industrial Security at Rosh Ha'yin, Israel-based Waterfall Security Solutions.

The first step is to organise the utility's assets into a defensive network architecture. The standard model is the Purdue model, a system of hierarchical functions of an industrial enterprise developed

Energy companies across the globe are facing increasingly sophisticasted cybersecurity risks

Photo: Bee Bright/Shutterstock

at Purdue University, Indiana. The model segments operations into different zones with physical operations at the bottom, the IT system at the top and control systems in the middle. Each zone or layer is separated by controlled conduits such as firewalls with user access control and intrusion detection.

Unidirectional gateway

Waterfall's solution is to place a unidirectional gateway at the IT/OT interface. This consists of a fibre-optic laser/transmitter that sends control system data to the IT system via a receiver/photocell module. The transmitter has no photocell so is physically not able to receive information in the opposite direction. Since all cyber-attacks are information, the blocking of all returning network information blocks all attacks from external networks. The gateway enables online, remote monitoring of important control system networks, without the risk of unauthorised control that comes with firewalls and other security software, Ginter explains. Unidirectional gateways are physical protection, not software. All software has bugs and some bugs are security vulnerabilities, meaning that all software can be hacked. Residual risks such as those due to software updates on USB Flash drives are typically dealt with using device control software and media cleansing stations.

Such software vulnerabilities were demonstrated in November 2017 when Triton malware was deployed to attack the safety system – in this case France-based Schneider Electric's Triconex products – of critical infrastructure in a Middle East state, possibly Saudi Arabia. The plant shut down and no harm was done.

Triton is comparable with Stuxnet, a US-developed (although unconfirmed) malware that between November 2009–January 2010 destroyed centrifuges in Iran's Natanz uranium enrichment plant by changing the plant's control system codes, and Industroyer that was used in Ukraine. The malware is designed to disable safety mechanisms in industrial control systems and has the capability to cause physical damage. It can communicate with the Triconex controllers and reprogram them with an attack payload. Stuxnet was uploaded into the Iranian system by an infected USB stick. The provenance of Triton remains unclear, although investigators suspect it was state-sponsored.

Process safety risks

The Energy Institute is conducting preliminary research into process safety risks caused by cyber threats. Headed by Lee Allford, EI Manager for Process Safety and Decommissioning, who has over 15 years' experience of managing process safety networks, the focus will be on incidents that have the potential to cause multiple fatalities and damage to assets and the environment rather than data security breaches.

Allford will be chairing the annual Hazardex conference in late February in Runcorn, Cheshire, and is on the technical committee for the Institute of Chemical Engineers Hazards28 conference in May in Edinburgh.

Allford contends that although there has been a plethora of information, possibly even overwhelming, from various government agencies about cybersecurity risks, industry response to date has been fairly muted. 'Industry appears to be digesting the implications of operational guidance published by the Health & Safety Executive in 2017 which will form the standard of its inspection for major hazard sites. Typically, process safety professionals have been at the forefront of understanding risks posed by major hazards, be they technological or natural. Combatting cyber threats represents an entirely new frontier for the process safety community.'

There is a similar reluctance to open up about cyber risks among US energy companies, notes EPRI's Jason Hollern, although the US nuclear sector is good at sharing information. Cyber specialists prefer personal contact, he adds, where the only worry is what one or both sides writes with a pen in a notebook. ●

Monitoring platforms

New York-based Indegy aims to counter such cyber risks through its platform that monitors what is happening in the ICS and gives alerts of any dangers. This is used where third parties work in a plant, explains Dana Tamir, Indegy Vice President for Market Strategy. People come to a site with their own laptops or other devices. You don't know if these contain malware but you cannot restrict their access as the company needs them to work, so the vulnerabilities exist. 'If you gain access to a network you can do whatever you want,' Tamir says.

Therefore the question is: 'If someone is in the network, what is he doing?' Indegy employs its platform at every site of a given plant. Its technology can plug into the network and monitor the traffic, but it is not intrusive as such traffic does not pass through the device.

A lie detector for machines

Nevertheless, any industrial system whose physical operations are monitored by thousands of sensors still needs to get this data out to a control room. Displays of parameters such as pressure or temperature on control room screens should be reliable, but a virus can also be created there. Unidirectional gateways or other one-way links between the IT and OT systems are fine in theory, says Shalyt, but do not always work in practice. 'You have to update software once in a while and you need to know what is going on.'

So, when Aperio starts a job the assumption is that the digital network is contaminated. The company has developed what Shalyt calls a 'lie detector for machines'. This technology scours the ICS to seek out any inconsistencies between the real time and historical performance of any sensing component. Any mismatch will trigger an alert. 'We don't focus on the SCADA network at all. We sit on top, we monitor and we have a nerve centre, a control room,' Shalyt explains. Any fake data that is detected can be reverted to its original value in real time.

It is important that energy companies adapt to new realities and go beyond the notion of 'I'm building a firewall and I'll be safe' paradigm, Shalyt says. Such are the challenges today in Portugal and other countries where there are tens of thousands of solar users connected to a central power grid. This grid can be easily destabilised with false data.

Nevertheless, getting back to basics on good practices and training programmes in companies is crucial, notes Jason Hollern, Principal Technical Leader at EPRI. 'You maintain cybersecurity as you keep up maintenance. Stay on top of the system and train the right staff before you become a hacking target.' ●