ABB – how to do cybersecurity on industrial systems

Industrial systems ("OT") cybersecurity requires a different approach to cybersecurity for the office – the dangers are greater, the threat is growing – but you can't lock the operators out of their systems. We interviewed ABB's head of cybersecurity in the UK

Industrial cybersecurity requires a different approach to office or IT cybersecurity.

The dangers are higher, with reports of attacks on safety equipment and ransomware finding its way onto offshore installations, so the hacking could cause a loss of life or disaster.

But at the same time, conventional approaches to cybersecurity, such as the "two failed password attempts and you're locked out" approach to preventing password guessing attacks, cannot be used, in case it leads to people not being able to operate systems when they need to.

Encryption, a common security measure in IT, is not necessarily appropriate for OT, because it can add latency – a control systems command to close a valve probably needs to be carried out immediately, not after a few seconds.

And conventional firewalls and virus detection systems are not designed to work with industrial protocols such as HART, IEC 60870-5-104, OPC or IEC 61850.

You can't just analyse the communicated data to detect threats, because a malicious command to shutdown plant equipment looks the same (in control system language) to a legitimate command.

The right approach to industrial cybersecurity can be described as all about understanding – knowing how your network can be breached, knowing what assets you have, knowing what data you are usually sending and who sends it, and what the normal pattern of communications looks like, says Ben Dickinson, recently appointed as head of ABB's team of industrial cybersecurity specialists in the UK.

Mr Dickinson previously worked at UK's National Cyber Security Centre (NCSC), part of GCHQ, and specialises in understanding unique challenges posted by securing Industrial Automation and Control Systems. ABB has recently expanded its cybersecurity team, adding another 20 roles.

Attacks on a petrochemical plant

Ben Dickinson, head of ABB's UK team of industrial cybersecurity specialists

In December 2017, the first publicly known cyber attack on a large safety system took place, on a (name undisclosed) petrochemical plant in the Middle East. It had the specific aim of disabling system safety functions, Mr Dickinson says, targeting Schnedier's "Triconex" safety systems. It reprogrammed the safety controller, trying to change safety limits in the system.

The attack was thwarted because some of the code it tried to run was defective, and caused the system to shut down. But whoever was behind it clearly knew what they were doing, and trying to create a catastrophic incident or harm to life, he says.

The attack was called Triton/TRISIS. The two names to the threat are due to two people discovering the attack at about the same time, and a protocol among cybersecurity experts that whoever discovered the attack getting naming rights, Mr Dickinson says.

What to be aware of

One of the first steps in doing cybersecurity on industrial systems is to understand how you are changing your vulnerability landscape when you digitise a system. For example if a retail petrol station installs tools to remotely monitor tank levels, the same system can be used to hack into the system and perhaps change the price it charges for fuel.

It helps if your systems are built as transparently and clearly as possible. Too many systems just end up with tons of data going through wires nobody understands, Mr Dickinson says. Cyber attacks often involve manipulation of data, so you need to understand your data in order to detect it.

The more sensors and data you have, the more complex your cybersecurity will be. Don't be impressed when companies tell you how much data their sensors generate a day – it is more important to know whether they are just collecting the data they need, and they understand it, Mr Dickinson says.

You need to make sure whoever implements the system knows how to implement it securely.

You need to be aware of whether your electronic devices are still supported by their manufacturer, issuing 'patches' if anyone discovers a vulnerability in their software. Otherwise, they need to be replaced, like with Windows XP computers. The idea of replacing equipment which seems to be working fine does not sit comfortably in the oil and gas industry, which is used to finding ways to extend the life of old products and systems.

Operational systems often use PC software (Windows) and so are vulnerable to the same threats, such as ransomware. But people trying to collect ransoms will often search for people they think will be most damaged by losing data, and so most willing to pay a ransom, Mr Dickinson says. They can see that if they can stop oil and gas operations, the company will pay a big price, so the oil and gas industry looks attractive to them.

Strategies for installing ransomware can include finding the name of a suitable target operations person on LinkedIn, guessing their e-mail address from company e-mail conventions, and sending a clever e-mail designed to get them to click on a link to install the ransom ware. "Humans are the weak link in your security system," he says.

Companies can do more to try to detect intrusions, rather than only being aware of attacks after they happen. Companies planning attacks can have communications on your system for a long time, so you can have time on your hands to carry out analysis.

Many organisations get a false sense of security from their antivirus, he said. But all antivirus can do is detect known malicious software. The best way to detect unknown malicious software is to look for unusual patterns in your communications, such as an unusual command, an unusual time of day, or a command sent by an unusual person.