CYBERSECURITY

Tackling the operational technology challenge

Cyber-attack simulation, training and response is supported by IBM's X-force Cyber Tactical Operation Centre – an 18-wheeled truck that drives around the US, with one also based in Europe

Photo: IBM

Interconnection between IT and OT systems poses a major challenge for oil and gas sector cybersecurity. It's not simply about the vulnerability of legacy systems, but also the need to establish strong test, security training and hard copy back-up plans, reports *Brian Davis*.

Digitalisation of the oil and gas sector is spurring interconnection between information technology (IT) and operational technology (OT) globally. At the same time, it is increasing vulnerability to cyber-attack. Security experts like IBM note that IT security solutions aren't designed to address OT security challenges, and OT solutions that rely on technology alone aren't effective. It's important to have a well-designed OT security strategy with the right skill sets in place.

Notorious attacks such as the Shamoon malware variant discovered on the network of an Italian gas and contractor in December 2018, which destroyed files on about 10% of the company's servers, mostly in the Middle East (including Saudi Arabia) but also infecting sites in India, Italy and Scotland, as well as more recent ransomware attacks like Ekans ('Snake' spelt backwards), illustrate the serious nature of the threats.

OT is the backbone of the oil and gas sector, using computer hardware and software to monitor and control physical devices. Industrial control systems (ICS) play a vital part in OT environments to monitor and regulate processes like temperature, pressure and flow, and prevent hazardous conditions and breakdowns. Increasingly, organisations are incorporating more Industrial Internet of Things (IIoT) with smart sensors to share and analyse information from compressors, turbines and other equipment.

Interconnecting industrial systems to the IT network in industrial environments offers better control, management and visibility of industrial ecosystems. But it's a double-edged sword, as it increases the vulnerability to malicious cyber-attacks. What's more, many organisations simply aren't prepared for these new security challenges. IBM believes that cybersecurity implementation today with the convergence of OT/IT environments resembles IT cybersecurity 20 years ago.

OT environments face a number of cybersecurity challenges. A significant number of the legacy systems feature old, vulnerable software like Microsoft NT and DOS. There's a general lack of understanding of cybersecurity threats and potential impact. And often no strategy in place for mitigation.

'The big challenge for cybersecurity is the convergence of IT and OT,' says Andreas Wespi, Research Staff Member of the IBM Research Lab in Zurich. 'All these high profile attacks have essentially the same patterns. First there's penetration of the IT environment, where there's a connection between IT and OT, then the malware gets introduced into the OT environment.'

The big challenge is often the lack of patching and software updates because OT patches often require vendor approval or extensive testing before application. Patching is slow and creates downtime. Furthermore, there is a big concern that changing a running system could have many side effects.

Even password protection can be counterproductive for OT environments. For example, a password authentication policy that locks-out a user after several failed attempts could be disastrous in an emergency where an engineer has to resolve a problem in a critical system within seconds. 'Some of the network protocols may also lack encryption or authentication. Many oil and gas operators would like to remedy this problem, but industrial systems are costly and have to stay in place for a long time,' says Wespi.

Production environments are also hard to test. Although penetration (pen) testing is an important tool in IT security, it can pose a significant risk to ICS systems. As a result, pen testing must be used with caution or replaced with alternative testing methods or simulation, in an OT environment.

There is also concern that employees in industrial environments don't understand cybersecurity, and IT security specialists may not be experienced in the OT environment. Indeed, few risk mitigation techniques and tools are deployed in OT environments. However, when an IT/OT network gets hacked, and data and control systems are

compromised, there can be serious impact on production, safety and the environment, with potential deaths.

Sophisticated attacks on operational networks are on the rise. But IBM research shows 74% of organisations lack current OT risk assessment. While 78% don't have OT specific security policies. And 81% lack an OT specific security incident response plan.

Taking action

So what measures should be put in place?

'You have to understand the challenges you face before you can properly secure your OT environment. You have to spot the weaknesses and do a priority search,' advises Wespi.

Asset identification is one of the most basic elements of an IT security programme. Every ICS device and process must be identified; which systems are interconnected, and what security controls are in place. As well as which systems don't support modern security controls.

Next, you have to gain visibility. 'Once you know where the risks are, you have to understand what's happening there, what the components are and how they interact? Getting visibility is an important step from an operational and security perspective,' he says.

Then you have to think about mitigation. If you can't replace an outdated system today, what compensating measures could be deployed? For example, a legacy system may be vulnerable to attacks, but its data traffic can be monitored. So, the shortcomings of the legacy system can be compensated with enhanced monitoring technology.

Equipment performance patterns could also be analysed using artificial intelligence (AI) for security challenges. 'Due to the regularity of the control processes, the OT network traffic also shows a lot of regularity. AI can identify and describe the normal network behaviour. A deviation from the learned normal behaviour could indicate potential cyber-attack,' says Wespi.

But Wespi recognises: 'It's difficult to understand the inherent risks and mitigation measures required to isolate vulnerabilities that impact OT systems without complete system documentation and understanding. It is imperative to have OT professionals who understand the environment working together with IT security professionals.'

Considering that cyber-attacks can be disastrous for an OT environment, it requires a well-rehearsed plan for quick response and damage mitigation. This response plan must include clearly documented roles, responsibilities and action plans; the ability to pinpoint industrial processes and devices being attacked; log files that can be examined forensically; profile and log files of users that have access to OT devices; documentation of the data that could have been impacted; and disaster recovery plans and redundancies to restore critical assets and data.

Today there is a lot of interest in major oil and gas organisations to have integrated IT/OT security operations. But there is concern about the lack of skill sets. OT incident response is different from IT and a lot more complex. Companies like IBM help develop an incident response plan and 'playbooks', working with OT engineers, operators, vendors and contractors, providing forensic services, back-up and recovery solutions should an attack occur.

Cyber-attack simulation, training and response is supported by technologies to manage data risk, like IBM's X-force Cyber Tactical Operation Centre – an 18-wheeled truck that drives around the US, with one also based in Europe. An array of computer screens and desks is housed in the truck to simulate what happens when an organisation is hacked, for training and test purposes, for OT security personnel, engineers and operators.

Third-party integration

Rob Hayes, Director Lead for Industrial Cybersecurity at Deloitte, believes that 75% of cybersecurity incidents have been caused by third-party integration as organisations become more and more interconnected. He recognises that: 'The challenge is poor security, because many OT environments don't have the ability to limit the impact of attacks and patch. You can't have 100% security. The main issue is how to limit the blast zone. Often, there's poor system segregation and control, so most operations shut down.'

He continues: 'You have to accept there will be incidents and have to ensure that response and recovery plans are in place, with hardcopy artefacts, back-up directory and business process programmes to recover. Key business processes must be mapped. Keeping hardcopy is important as online back-ups are no use after a destructive cyber-attack event, when you want to get the business up and running again.'

The big challenge in the IT/OT environment is also accountability, as neither side wants to take responsibility for the other in the event of an incident.

Finally, there is a desperate shortage of people with the right skill sets for IT/OT cybersecurity. 'A mixed skill set is required, between IT and OT network specialists. We advise clients to increase cooperation across the sector in order to bring ageing OT systems to an acceptable risk level. We are building systems where the weakest link is on the technical/OT side,' comments Boye Tranum, Associate Director Cybersecurity at DNV-GL.

Tackling the cybersecurity threat still has a long way to go when it comes to the OT environments and advances in quantum computing, which need to be prepared for today. ●

Held to ransom

How serious are ransomware attacks for the oil and gas sector?

According to Moreno Carrullo, Founder and Chief Technology Officer of Nozomi Networks: 'Ransomware infiltrates IT and email systems, which adversaries use to pivot to OT systems. Therefore oil and gas companies need to protect the former systems to prevent ransomware impacting their OT systems later. A successful ransomware attack can be extremely debilitating, potentially costing millions of dollars in damages and downtime, and leaving victims with no other option than to meet the hacker's demands. In most cases we find oil and gas operators are taking the threat seriously and are working to ensure their security postures are strong and adapting to the ever-changing threat landscape.'

He suggests that when protecting against ransomware, operators should be particularly diligent when it comes to:

- Mail content scanning and filtering to thwart malicious campaigns.
- Security awareness among all employees to avoid falling victim to a phishing campaign.
- Applying a health check on network infrastructure, ensuring that correct network segregation and firewall policies are in place.
- Ensuring that all devices and services are patched and not vulnerable to known attacks.
- Implementing a back-up policy that supports quick access to impacted files.

It's important to have multiple controls in place to prevent and detect this threat. This includes continuous security awareness training for employees and personnel to help them better identify fake and malicious emails.

'In addition to SPAM filters and firewalls, we recommend the use of both anomaly detection technologies and traditional detection capabilities to provide additional context around suspicious actors related to known threats,' Carrullo notes. ●