SA operational technologies open to attack

Local organisations slow to mitigate risks facing Industrial Control System (ICS) /SCADA systems

South African operational Industrial Control System (ICS) /SCADA systems are becoming increasingly intelligent and connected, and therefore increasingly at risk of attack.

"While a major breach has not yet been reported in South Africa, it is only a matter of time before a mission critical ICS fails due to cyber attackers, malware, hacktivists or disgruntled employees, and organisations running mission-critical operational technologies (OT) start to realise they have to take network security and information security seriously in the OT environment too," says Mark Linnell, Major Account Manager at Fortinet.

Tommy Thompson, Lead Consultant OT CyberSecurity at nClose, says the South African market is not yet mature in terms of OT security, although some local attacks have already been documented.

"We have seen at least one targeted attack and one related to malware in South Africa. But local organisations tend to be reactive, so until there is a major breach, many will be slow to move to mitigate their OT risk," he says.

OTs in use across manufacturing, mining, oil and gas, utilities and retail are increasingly the targets of attack around the world, as competitors, criminals and hacktivists take advantage of vulnerabilities to shut down operations, slow production, or hold organisations to ransom.

This can result in financial losses, lost IP, reputational damage, and critical downtime that drives customers to competitors, or even results in organisational chaos, says Linnell. Attacks on public utilities, critical infrastructures, and interconnected services in smart cities could pose a range of risks to public safety.

In recent international attacks, Iranian hacktivists gained access to the control system for a dam in the suburbs of New York, hackers infiltrated a water utility's control system and changed the levels of chemicals being used to treat tap water, and a group of hackers took over computers at an electricity control center, plunging parts of the city of Kiev into darkness.

"Automated, intelligent systems are improving quality of life, but at the same time, attacks on these systems could seriously impact quality of life. It's a dark picture," says Linnell.

He cites Forrester's 2016 Industrial Control System Security Trends report sponsored by Fortinet, in which 78% of respondents stated that security attacks drove their SCADA/ICS security strategy, and 77% of organisations said their SCADA/ICS had experienced a security breach. Fallout from those breaches ranged from impacted ability to meet compliance standards to issues with maintaining functionality and employee safety.

Fortinet notes that securing ICS/SCADA systems can be complicated by legacy environments, environmental, geographic and regulatory issues. But these issues can be addressed by implementing ubiquitous security and posture control; using a tightly integrated solution in form factors that are designed for the extreme environments in which they must be deployed.

Thompson notes that SCADA environments are all very different: "A dairy's system vs a roads agency system, for example, differ considerably. To effectively mitigate risk, each organisation needs to analyse its risk, identify mission critical processes and OT systems and start segmenting like assets with a product like Fortinet."

"The Fortinet Security Fabric allows for IT and OT infrastructure managers to develop end-to-end security segmentation within and throughout the converging IT/OT—essentially a Zero Trust Model," says Linnell.

Fortinet's dedicated Security Solutions for ICS and SCADA deliver top-rated, industrial-control-specific protection from advanced threats, high levels of reliability and longer lifecycle appliances designed for harsh environments and compliance with FIPS 140-2 and Common Criteria EAL 4+.

With network security features such as application- and user-identity awareness, content security with integrated intrusion prevention, antivirus, and web filtering, SSL encryption/decryption and advanced threat detection and remediation, Fortinet secures east-west traffic in the often-neglected

OT environment. With FortiManager and FortiAnalyzer consolidated through a FortiGate, the enterprise is assured of centralised configuration with reporting, visibility, and event logging to create a comprehensive, real-time network monitoring and control centre, while FortiGate Rugged next generation firewalls are built to withstand extreme temperatures, harsh climates, and hazardous locations.