datacentrix

eCentrix – September 2019

Becoming more cyber-savvy within the OT environment

Organisations running Operational Technology (OT), which according to Gartner can be described as “hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events in the enterprise”, have increasingly come under cyberattack, with malware sending shockwaves through these sectors, which include oil & gas, utilities, chemical manufacturing, waste management, mining and more.

So said Datacentrix security business unit manager, Wayne Olsen, who spoke at the company's recent Mining Indaba event, which took place event at Zebula Lodge in the Limpopo province.

“Back in 2010, the Stuxnet malicious computer worm was credited to have caused major damage to Iran's nuclear programme, with US and Israeli governments purportedly using stolen machine identities to infect Iranian nuclear centrifuges,” Olsen explained. “In October 2018, Gholamreza Jalali, head of Iran's civil defence agency, announced that the country had neutralised a new generation version of Stuxnet, which was more complex, and could be classed as a weaponised grade malware.”

In 2017, a type of malware discovered at a petrochemical plant in Saudi Arabia provided hackers with remote access to the plant's safety instrumented systems; essentially the final defence line against life-threatening disasters. Known as 'Triton', the malicious software targeted a safety controller module, triggering trips that brought the plant to a halt twice, and put lives at risk. On investigation, it was found that the hackers seem to have had access to the plant's IT network since 2014.

“We've also learned that Havex, a remote access trojan (RAT) discovered in 2013, was used as part of an espionage campaign targeting industrial control systems (ICS) across numerous industries, from industrial equipment providers, energy grid

> **“The cybercrime economy generates around 1.5 trillion dollars in profit per year, with ransomware attacks taking place every 15 minutes. We're seeing 1,000,000 new virus variants being created each day, with 24,000 of these being new mobile malware samples. Ninety-nine percent of computers are vulnerable to exploit kits, and a staggering 93 percent of companies have been successfully targeted in a cyberattack.**

Wayne Olsen, Datacentrix security business unit manager

operators, electricity generation organisations, and petroleum pipelines, to the pharmaceutical, defence and aviation sectors.

Linked to Russian Intelligence Services (RIS), the Havex malware is said to have impacted around 2,000 infrastructure sites, mostly within the US and Europe, and involved three stages of attack, the first being spear-phishing to infect computers and collect information. Havex' second stage was targeted users visiting legitimate websites, via watering hole attacks, where they were redirected to servers that infected software.

The third phase of an attack saw contamination via the download of genuine applications on vendor websites, with Havex then locating Supervisory Control and Data Acquisition (SCADA) or ICS devices on the network, and sending the data back to command and control servers.

“One point that is clear is that the motivation behind all of these cyberattacks is financial,” clarified Olsen. “The cybercrime economy generates around 1.5 trillion dollars in profit per year, with ransomware attacks taking place every 15 minutes. We're seeing 1,000,000 new virus variants being created each day, with 24,000 of these being new mobile malware samples. Ninety-nine percent of computers are vulnerable to exploit kits, and a staggering 93 percent of companies have been successfully targeted in a cyberattack.

“And with it taking up to 49 days for a breach discovery, it is no surprise that there is a huge demand for cybersecurity, and that we are seeing the industry grow in leaps and bounds, set to be worth $300 billion by 2020.”

Olsen explained that there are several main challenges faced by today's Chief Information Security Officer (CISO) when it comes to OT security. “Within the OT environment, standard IT security controls and technologies either don't translate or are prohibited due to the disruption they may cause to operational processes. In addition, OT devices are often plugged in straight out-of-the-box, using default passwords and with easily discoverable and exploitable default settings.

“Software and firmware may contain vulnerabilities, or were designed without modern security methodologies (encryption, data validation). Finally, patching often does not take place, as it can be disruptive to uptime, can void warranties, or cannot be done as the organisation is using legacy technology no longer supported by the vendor.”

The solution, said Olsen, is for companies to compare the aggregate access of the network to the access designed in security policies, analysing by Purdue model level, device type, and so on.

“It is also necessary to look closely at access end-to-end, in order to troubleshoot connectivity issues and protect critical assets, as well as to identify critical–risk exposed and exploited vulnerabilities to effectively plan patches or mitigation. Lastly, processes to maintain uptime must be automated to avoid costly or dangerous disruptions.”

However, he added, technology is not the only answer. “We've seen a 120 percent year-on-year increase in OT-specific vulnerabilities. The main sources of industrial control system (ICS) infection for last year were: the internet (20,6 percent); removable media (eight percent); and mail clients (four percent).

Therefore, it is critical that organisations making use of this type of technology must also look at the end users, and ensure that they receive the training needed to raise awareness of cyber threats, how they can infiltrate ICS technology, and how staff inadvertently play a role in this. Once employees and executives alike have a greater level of understanding on how to mitigate these threats, their behaviour will change, which should bring about a positive impact on security levels.”

For more information on the Mining Indaba, or to download Olsen's presentation, please visit https://www.datacentrix.co.za/miningindaba2019.html

Contact: Elzette du Preez, +27 87 741 5000, edupreez@datacentrix.co.za