KERATAN AKHBAR

TARIKH	: 11 NOVEMBER 2022
AKHBAR	: THE EDGE MARKETS
MUKA SURAT	: https://www.theedgemarkets.com/article/securing-5g-and-ot-advancement-achieve-malaysias-ir40-digitalisation-goals

Securing 5G and OT advancement to achieve Malaysia's IR4.0 digitalisation goals

Organisations utilising digital solutions are moving faster and further than their peers in every aspect, from production efficiency and customisation, to delivering improvements in speed to market, service effectiveness, as well as new business-model creation.

According to the Ministry of Communications and Multimedia, major Malaysian States like Selangor, Penang and Sabah are set to deploy 5G technology by year-end. Furthermore, Malaysia’s MyDIGITAL blueprint and the National Policy on Industry 4.0 (Industry4wrd) also signal the government’s ambition to establish strategic partnership with smart manufacturing.

With the power to accelerate industrial transformation far beyond the capabilities offered by previous generations of broadband technology, 5G will enable Malaysian businesses to harness data-driven use cases, such as augmented reality-based maintenance, precise real-time asset tracking, mobile robots, and closed-loop process control.

However, Malaysia's industries will only realise the game-changing benefits of 5G — such as low latency and greater scalability — if networks and operational technology (OT) are secured.

Driving secure innovation in 5G environments

As a result of the convergence of OT and IT networks, the potential of cyber threats hitting critical infrastructure is increasing. The Malaysia Cyber Security Strategy 2022-2024 is recognition that proactive measures are essential to safeguarding critical infrastructure.

Internet of things (IoT), augmented reality (AR), virtual reality (VR) and artificial intelligence (AI) enabled by 5G that are emerging in various sectors will considerably expand the attack surface. With OT environment no longer 'air-gapped', organisations must learn how to mitigate 5G security risks by understanding and anticipating security gaps.

With the OT-IT convergence, traditional endpoint security solutions will be limited in their ability to adequately protect critical infrastructure, which rely heavily on legacy systems. On the other hand, a broad selection of point security solutions, while providing cover for each new risk exposure, only introduces complexity and leaves gaps in the organisational security posture.

Security in pre-5G industrial environments

Historically, security in OT environments was mostly implemented based on the Purdue model reference architecture, which outlines a hierarchical security model for key infrastructure layers used in industrial control systems (ICS) environments and the boundaries between them.

However, an ever-increasing amount of information now needs to pass between these zones thanks to the Internet of Things (IoT), Industrial IoT (IIoT) as well as wireless and cloud connectivity. Furthermore, the general rollout of 5G — by introducing a vast array of new connections, capabilities and services — essentially creates more attack vectors for cyber criminals to target, accelerating an issue which the original model did not anticipate.

Another aspect to consider for businesses in securing OT environments is how attackers' tactics are evolving. While it used to be that OT systems could only be targeted by highly specialised threat actors leveraging their knowledge of ICS and supervisory control and data acquisition (SCADA) systems, it is, in fact, no longer the domain of malicious actors with these specific, advanced capabilities. As the tools needed to execute such attacks are now available for purchase on the dark web, a broader set of far less technical attackers are now able to access the weapons to target organisations' OT systems.

With 5G-connected devices, platforms, and applications having the ability to send and receive data directly via flows that do not necessarily pass through the Purdue model-defined enforcement boundaries, it is crucial to put in place an additional security boundary at the 5G domain with the following high-level functionalities:

- OT/Industrial Internet of Things (IIoT) security visibility and control
- 5G network security
- Industrial applications security

Deploying 5G use cases in production will take time as devices, applications, 5G technology experience and know-how mature to become reliable enough for deployment. It is essential that alongside this evolution of 5G deployments in enterprise verticals that the appropriate security considerations are taken and implemented throughout the industrial environment, including the 5G network, services and overall use cases.

5G will undoubtedly play a leading role in driving innovation in Malaysia's industries, but local businesses can ill afford failing to implement a holistic security framework, as this places them at the mercy of costly stoppages to operations. More importantly, a failure to arm themselves with cutting edge security not only stops organisations from harnessing the full spectrum of business advantages from 5G, but also significantly increases the risks posed to lives.

Strengthening security to drive industrial 5G

The security of an industrial environment is only as strong as its weakest link. As Malaysia sets its sights on becoming a leader of 5G in Asia and boosts implementation in industrial environments, ensuring organisations' security can keep up with today’s complex and fast-evolving threat landscape is critical. As attack sequences get more complex and innovative, maintaining organisation-wide visibility and consistent policy enforcement is fundamental for impactful 5G adoption. This requires solutions that encapsulate IT, OT, IIoT, and 5G security with broad visibility and control. Through an integrated and unified platform, businesses can observe and act on threats across edges, clouds, endpoints and users to mitigate the consequences of leaks and breaches.

5G is said to be able to change the digital trajectory of the nation’s economy and enhance our capabilities in the Industrial Revolution 4.0. Official projections predict that 5G adoption — which the government has set itself a target of 90% coverage by the end of the decade — will increase the nation’s GDP by 5% or RM122 billion.

In tandem with this, technologies such as artificial intelligence and machine learning — are imperative. Such capabilities are crucial to ensuring businesses can adopt effective security strategies to add value to business operations while staying ahead of increasingly sophisticated threat actors. Deprived of that, 5G providers, industrial enterprises and systems integrators have little chance of securing critical traditional and 5G-enabled use cases over private, public, and hybrid 5G networks and services.

Dickson Woo is the country manager of Malaysia at Fortinet, a cybersecurity solutions provider.