NEW STRAITS TIMES

#TECH: Expect more cyber threats

By Izwan Ismail - January 25, 2023 @ 12:50pm

Metaverses will interact with other platforms via APIs, and these connections will be a target of attack.

ADVANCED technologies like 5G, Internet of Things (IoT), artificial intelligence (AI), Metaverse, cloud and many more undoubtedly bring a lot of benefits to businesses and consumers.

However, the adoption of these technologies also means businesses are exposed to cyber vulnerabilities.

According to Palo Alto Networks in its APAC Security Predictions 2023 report, hackers will always find loopholes in these technologies and take the opportunity to launch attacks.

The cybersecurity company has listed down five predictions for the year that it believes businesses and consumers should pay attention to.

5G VULNERABILITIES

The 5G connections in Asia Pacific are expected to reach 430 million in 2025, up from 200 million at end-2021, according to a recent report by the industry association GSMA.

Palo Alto Networks field chief security officer (Asia Pacific and Japan) Ian Lim said the threat from this could come in various ways.

"Modern 5G delivery infrastructures are built on cloud architectures. While cloud provides greater agility, scalability and performance, it also exposes the 5G core to cloud security vulnerabilities. Large-scale attacks could come from anywhere, even from within the operator's own network."

5G mobile networks also support the verticalisation of services across industries and the development of Industrial IoTs, smart factories and other new use cases. These unprecedented 5G innovations are prime targets for evolved ransomware attacks that could cause costly disruptions.

With the advent of 5G speeds and more edge devices in the mix, bad actors will have several entry points and tremendously high network speeds to launch cyber attacks.

DIGITISATION IN HEALTHCARE

Digitisation is enabling brand new capabilities for healthcare, such as virtual healthcare and remote diagnosis.

"The prevalence of legacy systems and sensitive data that is attractive to cyber criminals is making healthcare a soft target, and cyber threat actors will be focusing on it.

Ian Lim

"During the pandemic, technology was used extensively in the fight against Covid-19. We saw the growth of contact tracing applications, connected health scanners and telemedicine. Also proven during the pandemic was the fact that cyber attackers have no qualms about disrupting critical healthcare functions for illicit gain," Lim said.

The adoption of medical IoT is also trending up. However, a recent assessment from Palo Alto Networks revealed that an alarming 75 per cent of medical infusion pumps scanned had known security gaps that could be compromised by attackers.

It will not be enough to just secure the medical devices; the mass of patient data, as well as their digital health records, also need to be secured. In addition to stealing the data, attackers could encrypt it for ransomware and cause life-threatening issues at healthcare facilities.

CLOUD ATTACKS

As companies adopt cloud native architecture, they are also inherently consuming third-party code into their critical applications.

Log4J recently demonstrated how many organisations could be rendered vulnerable due to a piece of dependent code tucked deep into the software packaging process.

"We have also seen attackers targeting the volunteers who maintain these open source code constructs to infiltrate organisations through the package update processes. This issue falls under the cloud supply chain, and we will see more disruptions in the coming year(s) on this front due to cloud adoption trends," said Lim.

DATA SOVEREIGNTY

As the world becomes more reliant on data and digital information, the volume of regulations and legislation emanating from a desire to control and protect citizens, as well as ensure the continued availability of critical services, will increase. As a result, the conversations around data localisation and data sovereignty will likely intensify this year.

METAVERSE

With an estimated US$54 billion spent on virtual goods every year, Lim said, metaverse could open up a new playground for cybercriminals.

"The immersive nature of the metaverse will unlock new opportunities for businesses and consumers alike, as it allows buyers and sellers to connect in a new way. Companies will take advantage of mixed reality experiences to diversify their offerings and cater to the needs of consumers in the metaverse."

THREAT SCENARIO

Metaverse implementations can be attacked at four essential layers: platform, conduit, edge and users.

Platform — most metaverse platforms will be built on cloud architectures (public or private) and are susceptible to cloud-based attacks.

Conduit — metaverses will interact with other platforms via APIs (Application Programming Interface) and other bridging protocols which will be a target of attack. In particular are the conduits bridging cryptocurrencies between metaverses.

Edge — Consumers will require some kind of wearable hardware, such as smart glasses or headsets, to be fully immersed in the metaverse. These IoT devices will be vulnerable to endpoint attacks and may lead to data and privacy breaches.

Users — The expanded use cases for our digital identities will make them even more attractive for cyber criminals to exploit.