SECURITY

Cyber security awareness on the uptrend

By YVONNE TAN
yvonne@thestar.com.my

AMID the Covid-19 pandemic, fresh worries about cyber security are piling on even as more and more people go online for work and to do simple everyday things like banking and grocery shopping.

In fact, according to reports this week, Malaysia recently received warnings that government websites would be hacked amid claims that the security systems in the country were loose, and therefore vulnerable to hackers.

In the working world, with a sudden spike in people working remotely and accessing Virtual Private Networks or VPNs from anywhere and at anytime, the risks for external parties to gain access to private information has increased by leaps and bounds.

So, for cyber security companies, has the current situation translated into a blessing in disguise of sorts?

According to Bursa Malaysia-listed Systech Bhd chief executive officer Raymond Tan, businesses remained cautious at the start of the movement control order (MCO) which started last March.

"Most adopted a wait-and-see approach with regards to investment in all aspects of their businesses, including cyber security.

However, gradual pick-up started in June with many businesses beginning to adopt a digital presence amid the realisation of the importance of cyber security," Tan tells *StarBizWeek*.

Systech provides cyber security services to organisations, monitoring the traffic on networks of companies and raising red flags if it detects anything "suspicious".

In its recently concluded financial quarter, its cyber security business reflected a pick-up in demand although the software side of its business, registered a decline and helped pushed the company into the red.

Tan says the recent awareness about the importance of cyber security has been "catching up" in the past 6 months as organisations are struggling to stabilise their operations amid a spike in demand for remote working tools.

"Since mid-2020, our clients have started asking for enhancements in cyber security solutions and policies," Tan says.

According to him, over the same period, the company also witnessed a jump in "sophisticated and highly technical cyber-attack methods with malicious threat actors utilising creative techniques to attack or extract information from their targets."

"To counter-act this, our team further enhanced our proprietary analytical methodologies and techniques to increase our strategic foresight capabilities, enabling us to better advise our clients on the latest threats and the required steps to improve their security posture and capabilities," he adds.

Edward Law, chief executive officer of Securemetric Bhd tells StarBizWeek that Italy's Computer Emergency Response Team or CERT recently issued a warning about a new family of Android malware that abuses accessibility services in devices to hijack user credentials and record audio and videos.

Dubbed "Oscorp", the malware induces the user to install an accessibility service with which the attackers can read what is present and what is typed on the screen, Law says.

> ***"We are seeing a significant increase of smart phone users being attacked, commonly via malware."***
>
> *Edward Law*

"We are seeing a significant increase of smart phone users being attacked, commonly via malware. We can no longer defend ourselves via traditional antivirus or firewalls alone. We need to scale up protection to the mobile application level."

He says his company has a product called SecureMobileAppSheild, which is an in-app protection that can provide security for mobile apps.

"This product can help companies which hope to take a proactive approach to combat this new aggression."

Meanwhile, a recent article by KPMG posted on its website entitled : " The rise of ransomware during Covid-19" states that "criminal groups are increasingly switching to Covid-19 themed lures" with "evidence that remote working increases the risk of a successful ransomware attack significantly."

The global audit, tax and advisory group adds that this increase in risks is due to " a combination of weaker controls on home IT and a higher likelihood of users clicking on Covid-19 themed ransomware lure emails given levels of anxiety."

Systech's Tan says during these challenging times, as organisations become more reliant on the digital world, the company has been witnessing a sharp increase in cyber security attacks both locally and internationally, targeting both individuals and corporate companies.

"The very fact that these attacks have had a broad range of targets – from the less technologically savvy to highly secure & sophisticated organisations – has had a chilling effect on our outlook and perspectives," Tan says.

"The conventional assumption that having several firewalls and sufficient security solutions are adequate in fending off against attackers no longer remains true, as these malicious actors have increasingly employed new tactics to damage or steal critical information."

In Malaysia, some of the other public-listed companies that are involved in the provision of cyber security services include Excel Force MSC Bhd and N2N Connect Bhd.

According to a Globe Newswire article released this week, citing Prophecy Market Insights (PMI) as source, the global cyber security market accounted for US$161.2bil last year and is expected to total over US$ 350bil by 2029.

Quoting information from PMI, the article says the major players in cyber security market are focused on "product upgradation" and establishing partnerships in order to operate in emerging markets.

"The demand for real-time solutions and services to safeguard and maintain data, information, program, and networks is projected to boost the global cyber security market in the forecast period," it adds.

In Malaysia, some RM27mil was allocated under Budget 2021 to enhance the nation's cyber security environment.

Prime Minister Tan Sri Muhyiddin Yassin also recently launched the Malaysia Cyber Security Strategy (MCSS) 2020-2024 which comes with an allocation of some RM1.8bil.

The Prime Minister was quoted then as saying that cyber crime had increased during the Covid-19 pandemic and cyber security remains an integral part of national defence.

He was also quoted as saying that the National Cyber Control and Command Centre had identified and contained several attacks on selected entities during the first round of MCO which was implemented last March to curb the spread of Covid-19.