TheStar

Companies on guard after falling victim to online attacks

By **YUEN MEIKENG**

Sunday, 19 Sep 2021

Employers to invest more in protecting and safeguarding their systems.

WITH cyber attacks on companies becoming more common, even the Malaysian Employers Federation (MEF) has not been spared.

MEF president Datuk Dr Syed Hussain Syed Husman says the organisation was hit with a ransomware attack in early July.

“It involved our accounting data, which was encrypted.

“Thankfully, our outsourced technical team managed to restore the server so that the downtime was only about three days,” he tells Sunday Star.

Later, the MEF was told by their accounting vendor that a few of their clients also encountered similar issues when accessing systems via a virtual private network (VPN).

Such a VPN is normally used by companies to enable employees to work remotely from home to access the company’s system away from the office.

“As more staff connect their own devices to the office network, such attacks are imminent.

“Some of the devices, especially employees’ personal IT devices, do not have proper security software,” says Syed Hussain.

He says that employers are aware of these issues that arise from remote working.

“Bosses are doing all they can to solve the issues which may be within their control.

“Issues like infrastructure of cables and telecommunication have to be addressed by the service providers,” he added.

Syed Hussain urges all employers to invest more in protecting and safeguarding their systems.

“Cybercrime is more rampant now, especially during the Covid-19 pandemic.

“The unauthorised access of government information, intellectual property, personal information, infrastructure and disruption highlights the urgent need to boost existing public and private digital security,” he says.

He points out that cybercrimes globally can potentially cost US$10.5tril (RM43.6tril) by 2025, based on projections.

“One of the major constraints faced by many employers is enough funding to beef up cybersecurity as employers have many other priorities during this challenging period.

“MEF hopes that the upcoming Budget 2022 will provide some incentives for employers to upgrade and strengthen cybersecurity,” Syed Hussain says.

SME Association of Malaysia vice-president CS Chin says many small and medium enterprises were affected by cyber attacks.

“We certainly have seen an increase in cyber threats.

“Cybersecurity is no longer an option when running a business but is a part of business costs and strategies,” he says, adding that this applies to small and large companies.

Chin, who is also National Tech Association of Malaysia (Pikom) adviser, says SMEs face two ongoing major threats, namely ransomware and botnet malware, which is a consistent trend worldwide.

Ransomware is a software that blocks you from accessing your data until you pay the cybercriminals. Botnet malware is a network of devices infected with malware like computer viruses and remotely controlled by a hacker.

Apart from that, cyber fraud continues to be a major concern for SMEs, with local businesses being targeted in phishing attacks, ie, a form of fraud where an attacker is disguised as a reputable entity or person in an email or other platforms.

One example Chin recalls is the case of a skincare distributor who transferred a payment of close to RM500,000 to a hacker account after their email was compromised.

“There are many such cases and the amount ranges from tens to hundred thousands. To SMEs, it’s a huge loss.

“However, most SMEs refuse to publicly admit that they have been compromised,” he says, adding that most cases are a result of the lack of emphasis on cybersecurity investment.

Chin highlights that companies must have a road map to deal with the ever-challenging cyberworld or face the risk of losses.

“They should invest at least 20% to 30% of their ICT (information and communications technology) budget to protect their systems.

“From what I understand, the willingness of SMEs to invest in protective measures is gradually improving, but it is by no means sufficient,” he says.

He advises organisations to keep updated backups of critical files offline and scan devices that are trying to access the network to guard against ransomware.

“However, beyond those steps, companies should also understand how ransomware works.

“With remote and hybrid work in place, phishing is the primary starting point for other forms of cybercrime like ransomware.

“Therefore, cybersecurity awareness and training should not be limited to IT teams and should be expanded to all employees,” Chin says.

He says bosses should invest in cybersecurity services or solutions that address the risks posed by employees working from home.

“Protecting their end point is the first thing to do.

“If this end is compromised, it will spread to the internal network and affect the server when they are back in the office,” Chin says.

Cybersecurity awareness training should also be implemented, as most breaches are due to human error and negligence.

“From the standpoint of the association, we strongly recommend that the government provide grants to encourage SMEs to be equipped with more cybersecurity protection,” he says.