Cybersecurity cases rise by 82.5%

FOCUS

Sunday, 12 Apr 2020

By YUEN MEIKENG

MORE people are online now – be it for business, education, entertainment, socialising or working from home due to the movement control order (MCO).

But the higher usage of technology also means bigger risks of running into cyberthreats.

About 352 accounts on the video conferencing app Zoom were compromised on Wednesday, including a healthcare provider in the US and seven educational institutions.

There has yet to be any report on hacked Zoom accounts from Malaysia.

But over here, cybersecurity cases have spiked by a whopping 82.5% during the MCO so far compared to the same time last year.

A total of 838 incidents were reported to CyberSecurity Malaysia between the start of the MCO on March 18 and April 7.

Of this total, 18% or 152 cases involved local companies, while the rest were home users and others. It is a jump from the 459 cases reported in the same period last year, based on data made available to Sunday Star by the agency’s emergency response centre, Cyber999.

Most cases during the MCO have involved fraud, intrusion and cyberharassment.

“The recent incidents are due to the increased use of technologies during this time.

“Many are on the Internet, social media platforms, using online meeting applications either for leisure, education, business activities, banking, online purchasing and so on,” says CyberSecurity Malaysia chief executive officer Datuk Dr Amirudin Abdul Wahab.

Examples of fraud cases online include scams, phishing or social engineering tactics to deceive victims and obtain sensitive information from them.

Intrusion includes hacking or data breach attempts, while cyberharassment includes cyberstalking.

During these times, cybersecurity is of even more importance, Dr Amirudin highlights, as the environment is just right for cyber criminals to strike.

“Ultimately, hackers want to profit from the Covid-19 pandemic.

“This includes virus-themed social engineering attempts, the sale of counterfeit medical masks and the spread of misinformation or fake news,” he says.

Such cybecriminals or scammers are quick in spotting a chance to make a profit, especially when most users are concerned with ongoing global events.

“Those who are required to use the Internet to perform their tasks are vulnerable to several cyberattacks.

“This includes phishing emails using Covid-19 themes to trap its audience, malware attacks such as ransomware and fake news via multiple sources such as email, compromised unrecognised websites and many others,” Dr Amirudin says.

At the same time, organisations are also being targeted for larger-scale attacks such as distributed denial of service (DDOS) whereby the attacker seeks to make services or resources unavailable to its intended users.

Other threats faced by organisations are spam, spear-phishing emails targeting individuals within the organisation to obtain data or to interrupt the organisation’s system.

“IT is a must for an organisation’s IT security team to be proactive during this period, and perform close monitoring of telecommunication networks.

“They should pay attention to abnormal internal activities and traffic, any suspicious access requests and loads of external traffic,” Dr Amirudin adds.

Some members from the Malaysian Employers Federation (MEF) have also raised concerns and complaints about cybersecurity issues during the MCO.

It’s also a struggle to order new systems because suppliers face challenges to deliver products, says MEF executive director Datuk Shamsuddin Barden.

“For example, when companies purchase new laptops, it cannot be delivered on time.

“And when you need technical support, it is tough to get a person to come on site as they cannot breach the MCO and face being fined. But we don’t blame them due to the circumstances,” he says.

Shamsuddin says employers are bracing for possibilities of cyberattacks since hackers are more active at times like these.

“As companies open up our eyes, we need to be more prepared to assist employees in setting up home offices so that we can address cybersecurity, especially when it involves company data and confidential information,” he adds. For now though, Shamsuddin advises employers to use trusted platforms for work and review issues to improve safety measures.

“The MCO came as a sudden development for us and we were ill-prepared for it in allowing individuals to work from home.

“Most use personal devices to perform duties. Such laptops and computers are not like office equipment, which have safeguards in place,” he points out.

In the incident involving the Zoom app, it was reported that hackers posted sensitive information like passwords on the Dark Web from the compromised accounts.

“During the MCO, no incidents related to the Zoom case were reported to Cyber999,” Dr Amirudin says.

Nonetheless, CyberSecurity Malaysia through its Malaysia Computer Emergency Response Team (MyCERT) issued an advisory as a guideline on the best practices in using such teleconferencing apps.

“We will continue monitoring the situation and Internet users are encouraged to report any threats related to cybersecurity to our Cyber999 centre. We will keep providing technical support and assistance to organisations,” he assures.

Under its outreach programme called CyberSAFE, or Cyber Security Awareness for Everyone, the agency spreads information to increase public awareness and knowledge on cybersafety and ways to mitigate online threats.

During the MCO, it has published regular cybersafety messages in the form of infographics on issues such as online shopping, password security, fake news, online safety for youth and kids and online games.

To report cybersecurity incidents, contact Cyber999 through its emergency hotline at 1300 882 999 (9.00am to 9.00pm) or its mobile number 019-266 5850 (24-hour helpline).

For more information, log on to mycert.org.my.