‘Companies should invest more in IT security’

Nora Jaswa
Free Malaysia Today July 17, 2017

Malaysia still lacks experts in the cyber security field, leaving it unprepared to face attacks when they occur.

KUALA LUMPUR: Malaysian companies should invest more in information technology (IT) security systems before cyber attacks happen, not after.

Crest, a UK-based not-for-profit accreditation body for the technical information security industry, said awareness of the importance of investing in IT security is still low in Malaysia compared with neighbouring Singapore.

Crest Malaysia chapter chairman Mohammed Fadzil Haron said Singapore had done much in terms of IT development, and that Malaysia should emulate it in developing its cyber security industry.

“In general, from what I’ve seen so far, companies are still not putting security at a level that would prevent cyber attacks from happening,” he told reporters.

He was speaking at the signing of a memorandum of understanding (MoU) between Crest and Persatuan Penguji Keselamatan Siber Kuala Lumpur (PPKS), which is also the Malaysian chapter of Crest, here today.

This was in response to reports that Malaysian companies are still complacent about investing in IT security.

“Some companies do invest, but only a handful. That’s why we need more experts in the cyber security field,” said Fadzil.

His response echoed previous concerns voiced by Communications and Multimedia Minister Salleh Said Keruak.

On his recent visit to Singapore, Salleh had expressed the desire for Malaysia to cooperate with its neighbour on cyber security initiatives.

Salleh said for Malaysia, the National Security Council (MKN) would be responsible for monitoring and taking appropriate action regarding cyber security.

Salleh also said he hoped the Cyber Security Bill would be tabled in Parliament as soon as possible, adding that Malaysia should have more experts in the field.

Concerns over cyber attacks have been raised in recent times, especially in response to the global WannaCry ransomware attack which began on May 12 and affected over 150 countries.

The malicious software worked by locking up files on a computer and encrypting them in a way that denies the owner access to them.

The programme then demanded payment through the Bitcoin digital payment system to make the files accessible again. However, security experts warned there was no guarantee that access would be granted after the payment was made.

More recently, on July 7, Nikkei Markets reported that authorities were investigating a suspected cyber attack which disrupted online stock trading at several local brokerages.

Dealers at the affected brokerages said the disruption, suspected to be a form of distributed denial of service or DDOS, took down some online trading platforms.

Fadzil said penetration testing had become widely accepted as one of the key elements to test a company's current defence mechanism.

He added that it is crucial for companies to have such tests to ensure their current system is up to date.

“Right now we have 45 companies that are accredited with us. Because of our rigorous examinations, we're aiming for another 10 companies by year-end.

“Not that much. But it's a start for the better,” he said.

The agreement, witnessed today by the Asian Institute of Chartered Bankers (AICB), will see the Crest Malaysia chapter aggressively promoting accreditation for cyber security services among companies in Malaysia, specifically on penetration testing and test stressing on IT security systems.