

Cyber security a must for telcos, banks
Free Malaysia Today
21 April 2014
By The Malaysian Reserve; John Gilbert

KUALA LUMPUR: Banks, telecommunications and government portals in Malaysia must ramp up efforts in adopting advance and effective cyber-defence capabilities to protect against espionage and fraud.

As cyber-criminals are using increasingly sophisticated threats that target specific computer systems in banks, financial institutions, telcos and other organisations, information technology and security professionals must be ready to face the constantly-evolving tactics and approaches used by criminal hackers.

“Companies and government departments form the critical part of the national infrastructure, typically the banks, financial institutions, telcos, resources and intelligence industry and these are critical infrastructure that need to be constantly protected from cyber attacks,” BAE Systems Applied Intelligence (M) Sdn Bhd MD for Asia Pacific and the Middle East Richard Watson told The Malaysian Reserve recently.

Global Economic Crime Survey 2014 conducted by Price Waterhouse Coopers showed that as cyber-crime operates largely unseen, organisations may not even realise they are being targeted until long after the damage is done.

This fact alone makes the many varieties of electronic fraud one of the most threatening types of economic crime and many entities may not have clear insight into whether their networks and the data contained therein have been breached, and they don't know what has been lost, or its value, the survey said.

“In Malaysia, we work closely with CyberSecurity Malaysia in raising awareness of cyber security and we have jointly done many different penetration testing of networks that are potentially exposed to attacks and we have done an assessment of the country's cyber networks using various different softwares,” Watson said.

CyberSecurity Malaysia is the national cyber security specialist agency under the Ministry of Science, Technology and Innovation.

The agency specialises in cyber security services in preventing or minimising disruptions to critical information infrastructure in order to protect the public, the economy, and government services, and also provides on-demand access to a wide variety of resources to maintain in-house security expertise, as well as access to advanced tools and education to assist in proactive or forensic investigations.

He explained that the old way of bank fraud would be filling up forms with false data and disappearing with large amounts of withdrawals. These days fraudsters use malwares to control the banking networks to divert money from the core system of the bank into other

accounts.

“From the attackers perspective, this is a lot lower in risk as they can do it anonymously, do it from abroad and not be in Malaysia and subject to Malaysian law and jurisdiction,” he said.

Watson said BAE Systems has also developed a product called Mobile Protect that can be deployed into the core telephone network and it can filter out viruses that attack mobile devices such as smartphones and tablets, enabling them to browse company data securely and at the same time be protected from attacks that steal sensitive data from these devices.

In March this year, BAE Systems and CyberSecurity Malaysia signed a memorandum of understanding to establish a general framework for potential future collaboration in cyber security.

Both parties have agreed that it is necessary to establish and strengthen cooperative efforts related to the development of capacity and capacity in information security and tap commercial opportunities in the provision of cyber security solutions in Malaysia.

Copyright © 2013 – Free Malaysia Today

Source: <http://www.freemalaysiatoday.com/category/business/2014/04/21/cyber-security-a-must-for-telcos-banks/>