Can M'sia handle cyber attacks?

Free Malaysia Today
10 April 2014
Oleh P Ramani

PETALING JAYA: In an age of technology and cyberspace, netizens are hooked on search engines like Google, social media like Facebook, Twitter and mobile applications like WhatsApp and Viber. But there is a dark side to all these technological advancements.

We have been hearing of technical jargons like web defacement, phishing attacks, denial-of-services (DDOS) and system intrusion attempts, which makes little or no sense to the common man.

Let's take DDOS as an example. It has been used extensively by hackers since the mid-1980s to block access to a site or sites by legitimate users, rendering the site or even network inaccessible.

This can be achieved through any number of methods, including the relentless transmission of irrelevant information to tie up a server so that legitimate requests for information remain unanswered.

Hackers can also use these cyber attacks to obstruct the transmission of routing information, as a result, requests never reach their destination.

Alternatively, computer hackers could also use cyber attacks to obstruct communication between two servers or networks so that information cannot be sent or received by either party.

The hackers' motives are often based on political agendas, organised crimes or just for mere thrill of it to test their skills.

The Estonian 2007 cyber attack was an eye-opener to all international cyber security professionals, to take serious measures on cyber security readiness.

In that case, a large group of hackers carried out a series of cyber attacks lasting for two weeks swamping websites of Estonian organisations including the Estonia parliament, banks, ministries, newspapers and broadcasters.

Literally, the whole network and computer systems of Estonia was destroyed by the hackers for almost two weeks.

These also led to the infamous birth of the DDOS attacks that are widely used by hackers to deny fetching services from a website.

Looming threat

In the past five years, Malaysia has experienced several cyber attacks from local as well as foreign hackers. In 2009, a group of hackers disrupted nearly 41 Malaysian government portals.

Imagine if Tenaga Nasional Berhad (TNB) systems and networks were attacked using DDOS method. We could end up with no electricity for hours or even longer if there is a system shut down.

As a consequence, there can be a chain reaction down to other sectors, like the traffic and banking system. We may face a collapsed system and the repercussions can be unimaginable.

Several years back in the US and Europe, there were hackers who tried to slow down the satellite system but the attempt failed and systems were restored immediately.

There have been incidents where fake accounts on Facebook were apparently 'untraceable' by Malaysian Communications and Multimedia Commission (MCMC) officials.

This brings us to asking ourselves a critical question – are we prepared to face such hacking on our systems, be it defense, satellite or others?

Holistic approach

Currently the Malaysian government adopts a holistic approach across all government agencies, industries and societies to ensure the nation's readiness against any medium to large scale cyber attacks.

The Ministry of Science, Technology and Innovation (Mosti) developed the 'National Cyber Security Policy' (NCSP) in 2005 and implemented it in 2006 to strengthen the nation's cyberspace security.

The national policy focuses on enhancing the resiliency of Critical National Information Infrastructure (CNII) against cyber threats. It also addresses the national and regional benefits of the digital economy.

CNII is defined as assets in real and virtual worlds and systems that are vital to the nation. The destruction of it would have a devastating impact.

Over the past five years, the National Security Council (NSC) under the Prime Minister's department has been organising a yearly National Cyber Crisis Exercise known as X-MAYA.

This exercise is to address the emerging issue of cyber threats which poses serious challenges to the economic well being and security of the nation.

This annual exercise aims to test the effectiveness of the procedures that have been developed under the Malaysian National Cyber Crisis Management Plan and to assess the readiness and preparedness of critical national infrastructure agencies against cyber attacks.

In the exercise those under the CNII – namely health, water, banking and finance, information and communications, energy, transport, defense and security, government, food and agriculture and emergency services will be involved.

National policy

Last November, Deputy Prime Minister Muhyiddin Yassin launched a national policy document,

'National Security Council's Directive No 24: Policy and Mechanism of the National Cyber Crisis Management'.

This executive directive outlines Malaysia's strategy for cyber crisis mitigation and response through public and private collaboration and coordination. The roles and responsibilities of all CNII agencies are clearly defined in this document.

There are six main principles under this directive namely National Cyber Crisis Management Structure; National Cyber Threat Level; Computer Emergency Response Team (CERT); Cyber Security Protection Mechanism; Response, Communication and Coordination procedure and Readiness Programme.

By having this sort of annual practice, the level of cyber preparedness among CNII sectors are said to have improved as more organisations came to realise the importance of having a proper internal mechanism and procedure in managing cyber security incidents.

Although the policies and expertise are in place, the collaborative efforts and true commitment from the police, Attorney-General Chambers (AGC) and technical entities like CyberSecurity Malaysia (CSM) and MCMC are required to ensure that cyber threats are managed effectively

Source: http://www.freemalaysiatoday.com/category/nation/2014/04/10/can-msia-handle-cyber-attacks/