CYBER SECURITY AS A CENTRAL STRATEGY FOR SMART COMMUNITY

Amirudin Abdul Wahab
CyberSecurity Malaysia, amirudin@cybersecurity.my

ABSTRACT. The cyber threat landscape has evolved in fairly dramatic ways. Cyber threats come in various different forms both technical and content related threats. Emerging threats have become sophisticated and a lot more disastrous involving state actors, state-sponsored actors, international organized criminals and Internet hacker activist groups. Today's cyber threats pose challenges to the Government, organizations and individuals as there is already a trend of cyber-attacks on critical infrastructure. In recognition of the Internet connectivity and its borderless feature, smart community is not spared from cyber threats. Hence, those who are concerned with smart community security should explore an effective strategy to respond to cyber challenges in a holistic perspective. It should include the establishment of suitable cooperation amongst public and private sectors as well as cyber security professionals. It is expected that the demand for cyber security will grow in years to come as we continue to invest on Information Communication Technology and networks towards developing smart community.

Keywords: cyber threats, cyber-attacks, cyber security, cybercrimes, malicious codes, critical sectors, National Cyber Security Policy, cyber laws, cyber space

INTRODUCTION

Today's globalization has seen the increasing use of Information and Communication Technology (ICT) as a vital tool for development. A Nokia Siemens Network reported that by 2015, five billion people will be connected with a global community brought closer together with voice and, increasingly data communications. The East Asia region is becoming the most important political, economic, strategic and socially diverse and dynamic region. The major factor driving this change is the ability of the region to exploit ICT to both national and regional advantages. In this regard, Digital Age has provided unprecedented opportunities for Malaysia to utilise ICT and Internet to national advantage across the governments, industries and societies.

The widespread use of ICT and high Internet connectivity has introduced new cyber security challenges. The ubiquitous technology that permeates the daily lives of individuals, businesses and government is not without its challenges and downsides. The world has witnessed the development of cyber threats and how they are encroaching into every sphere of human activities. Increasing Malaysia's dependency on cyberspace has become a significant risk. Our cyber security landscape is worsened by the users' ignorance, technical incompetency, and ineffective cyber security measures by organizations. In view of this, the Government has already realized the importance of having a secure, resilient and trusted cyber

environment. Hence, in smart community that links people and communities together, the need for cyber security encompassing people, process and technology is rather critical and such need will continue to grow in many more years to come.

SMART COMMUNITY

Developing smart community is in line with the Digital Malaysia initiative that has been launched to begin the transformation into a digital economy with emphasis on innovation, creativity and productivity. The increase in communication networks and connectivity has multiplied the potential for knowledge sharing and wealth creation, as well as provided ample opportunities for enhancing prosperity among citizens and businesses. Smart community aims to make a conscious effort to use ICT to transform life and work of the people where the goal of such an effort is more than the mere deployment of technology. Rather it is about preparing one's community to meet the cyber security challenges of a globalized knowledge economy. In views of this, the Government and businesses will continue to invest heavily to protect ICT infrastructure as well as ensuring the safety and privacy of the people through the deliveries of state-of-the-art cyber security solutions. By incorporating cyber security as a central strategy, smart community will support Malaysia to achieve a truly digital nation, hence completing the National Transformation Agenda. In addition, the sustainability of smart community in today's globalized economy also relies on inter-agency cooperation and public-private partnership. In an interconnected environment, all systems are mutually affected. If a system is compromised, the impact will also spread throughout the other systems which are connected to it.

CYBER SECURITY– CYBERSECURITY MALAYSIA'S PERSPECTIVES

In Malaysia, the number of Internet users already surpassed 17.7 million people in 2012 and Nokia Siemens Network reported that by 2015, five billion people will be connected in a global community brought closer together by voice and, increasingly data communications. The East Asia region is becoming the most important political, economic, strategic and socially diverse and dynamic region. According to CyberSecurity Malaysia, an agency under the purview of the Ministry of Science, Technology and Innovation (MOSTI), there is an uphill trend in the number of cyber incidents being referred to the agency. The incidents have increased substantially from 8,090 in the year 2010 to 25,204 incidents in the year 2011 and 2012. As for 2013, there were 4486 incidents reported up to 31 May 2013. Cyber harassments, denials of service, fraud, intrusions and malicious codes are amongst the constantly reported incidents.

Based on 2011 and 2012 statistics, fraud was the largest reported category of incidents with an average of 37.5% followed by intrusion, 32%. The figures in 2011 surpassed 2010 figures by 7,128 whereas, from January to September 2012 it has been 7905 incidents reported. Cyber harassments, denials of service, fraud, intrusions and malicious codes are amongst the constantly reported incidents. Whereas, malicious software (malware) is among the largest reported category of incidents. The rise of cyber incidents referred to CyberSecurity Malaysia also indicates that the users are now aware of potential dangers posed by cyber incidents and the need to report such incidents.

In view of this, it is foreseeable in the future that smart community will deal with cyber incidents in parallel with the rapid development of ICT systems together with increase of network connectivity and Internet users. Other than technical threats, the exploitation of ICT has introduced content-related threats. Such threats refer to any offensive and abusive contents such as hate speeches, radical and offensive statements, seditious and defamatory contents that can threaten national security and public safety. Cyber threats and their significant risks

on national security would remain as the major security concerns of smart community as in highly interconnected environment, smart community is not immune from cyber-attacks.

Cyber Crimes

In Malaysia, cybercrime hits 31,492 cases from 2010 to 2012 with an estimated loss of RM 241 million. Whereas in 2012 alone, Malaysian victims lost RM1.6 billion due to scam with 18,386 cases mainly involving love and parcel scam as well as phishing and hacking. At the international front, 2012 Norton Cyber Crime Report states that the scale of consumer cybercrime hits 556 million victims per year, more than the entire population of European Union equivalent to 1.5 million victims per day. Based on the report, 42% of direct financial loss comes from fraud, whereas theft and money loss contributes 17%. Cybercrimes will continue to grow and they can also spread throughout smart communities as long as criminals can have financial gains from the computer systems.

Act of Aggression and Hostile Activities In Cyber Space

The global community acknowledges the existence of hostile activities and act of aggression conducted by nation states, state-sponsored and non-state actors. Such activities can refer to anything from cyber espionage, malicious software (malware) infection and system intrusion to high-scale cyber-attacks conducted with technical complexity and sophistication. It is believed that such activities are committed with diverse political and economic motives to achieve cyber dominance. The explosion of Internet has also created the phenomenon towards "digital hacktivism". In 15-19 June 2010, Malaysia has witnessed cyber-attacks on her cyber space by a group of hacktivism known as "Anonymous". The attacks via codenamed "Operation Malaysia" have captured the headlines of mainstream media. During the 5-day period, 210 Malaysian websites were defaced by the "Anonymous" group. The group is regarded by experts as politically-motivated, high profile and sophisticated.

Sophistication of Malware

The world has seen how Stuxnet targeted the operations of industrial systems, specifically the ones that run nuclear facilities. Duqu was designed to gather intelligence data and to set a pre-cursor for a future attack. The world also witnessed the emergence of Flame, a sophisticated spyware believed to be part of a well-coordinated cyber espionage operation committed at a level of state. We have also seen Shamoon that stole information and took data from the targeted systems. One unusual characteristic, however, is that it could overwrite the master boot record (MBR) on infected machines, effectively rendering them useless. These malware are evolving and they provide an insight into the future state of the ever-changing cyber threat landscape. Protecting against such malware attacks also poses a key challenge to the smart community in the globalized digital economy.

Misuse of Social Media

The rise of social media shows that smart community has to do more to protect its residents. Internet users today are spending more time on social networks, hence exposing themselves to various risks posed by content-related threats. The misuse of Internet for sedition and defamatory contents can undermine the perception of the population transforming the moderates into radicals, and radicals to extremists. In Malaysia, it is estimated that 85% of the Malaysian online population are Facebook users which is about 13.5 million people, and we are ranked 18th in the world. Many of the actors in foiled plots have been discovered among others, to threaten national security and social harmony under the pretext of so-called freedom of speech. No doubt that social media is a powerful tool to promote peace and stability, while at the same time it can be also misused by irresponsible groups to undermine national security.

CYBER SECURITY AS A CENTRAL STRATEGY TO SMART COMMUNITY

No doubt that the development of smart community plays an increasingly important role in Malaysia's digital progress as it is emphasizing on innovation, creativity and productivity that will help to enhance the nation's prosperity. It also reflects specifically our journey towards becoming an innovative digital economy in ways that will benefit the country and the citizens. Anyone responsible for the security of smart community's information systems has reason for concern as the community is exposed to various cyber threats. In view of this, the Government has already realized the importance of having a secure, resilient and trusted cyber environment.

National Cyber Security Policy

The Malaysian government has adopted the National Cyber Security Policy (NCSP) in 2006, a comprehensive cyber security approach namely to increase the resiliency of the Critical National Information Infrastructure (CNII). CNII is vital to the nation that its incapacity or destruction would have a devastating impact on national defense and security, national economic strength, national image, government's ability to function and public health and safety. Cyber security that ensures a secure, trusted and resilient ICT domain is a critical factor in safeguarding national security and prosperity. Collectively, such cyber security posture will promote productivity, national sustainability, social harmony and well-being, as well as wealth creation. To this end, innovation in both the technical and operational aspects plays a key role in the cyber security strategic approach, more so as the rapid pace of technological change requires that it always stays in lockstep with the evolution of emerging threats and challenges.

Innovative Cyber Security Programs

As a provider of specialized services for cyber security, CyberSecurity Malaysia has instituted a broad range of innovation-led programs and initiatives to help reduce the vulnerability of ICT systems and networks, nurture a culture of cyber security, and strengthen Malaysian self-reliance in cyberspace which are relevant and applicable for smart community. Cyber threats are revolutionary and our cyber security initiatives should be equally evolutionary and innovative in order to be relevant with the technology changes. These initiatives include policy research, technical research and development, public awareness and outreach, and facilities to provide advice, assistance, and expertise to individuals and businesses.

Cyber Security Through Public Private Partnership

The first priority for smart community is to implement an effective cyber security strategy and policies, and to extend all possible supports to the other entities in their legitimate requests for cyber security cooperation. In this case, no single entity can work alone and there is a need for public-private partnership. It can be done by bringing together various cyber security experts from the Government, industry, academia and individual experts to share, elaborate and debate various relevant cyber security issues and challenges, as well as to examine likely security risks in coming up with effective cyber security recommendations. Those who are responsible for ensuring the security of smart community are to further explore suitable collaborative efforts and to identify appropriate cooperative programs towards protecting our common interests in cyber security. As the way forward, we should continue the discussion on cyber security that will enable collective cooperation, the setting and measuring goals and action within those areas, and related priorities.

CONCLUSION

Cyber threats are growing in sophistication in parallel with ICT revolution and they would remain as security concerns to smart community and cyber security professionals in many more years to come. Malaysia, has already expressed great concern about the rise of cybercrimes and the trend cyber-attacks geared at attacking critical systems and their impacts on smart community. In view of this, the Government, industry, academia and individual experts via public-private partnership, should combine their ideas and work together in an innovative manner. Malaysia, as a nation should also adopt a more inclusive cyber security strategy and a holistic approach in protecting its cyber environment. Whilst at the same, as part of a global community, Malaysia should also aim to strengthen its international cooperation to respond to global cyber challenges in order to protect its regional and global common interests. With such a holistic approach, we hope to be able to operate within and benefit from the advantages of a secure, resilient and trusted smart environment.

REFERENCES

Ronald Byrne (2011). The Star News, *Hacker Group Tells Why It Wants to Attack Malaysian Gov. Portal*, 14 June 2011, http://thestar.com.my/news/story.asp.

BBC News Technology, Stuxnet 'Hit' Iran Nuclear Plans, 22 November 2010, http://www.bbc.co.uk/news/technology-11809827

Mathew J. Schwartz (2011). *Information Weekly Security*, 7 Facts On Duqu Malware Attacks, 16 November 2011, http://www.informationweek.com/security/attacks/.

Steve Evans (2012). *CBR Computer Business Review*, France Accuses US of Flame Malware Attack on Government Computers, 21 November 2012.

Jamal R. Nassar (2012). University Technology of Sydney – News Room, *The Arab Spring: Root Causes And Implications*, 2 July 2012, http://newsroom.uts.edu.au/events/2012/07/the-arab-spring-root-causes-and-implications.