Strategi Keselamatan Siber Malaysia – ke arah perkasakan upaya kriptografi negara

Oleh: Prof. Madya Dr. Muhammad Rezal bin Kamel Ariffin

Pengarah Institut Penyelidikan Matematik (INSPEM),

Universiti Putra Malaysia (UPM)

Bidang Kepakaran: Kriptografi Bermatematik

Nombor Telefon: 012-3766494

Emel: rezal@upm.edu.my

Strategi Keselamatan Siber Malaysia (MCSS) yang dilancarkan pada 12 Oktober 2020 oleh YAB Perdana Menteri Tan Sri Muhyiddin Yassin (ucapan dibaca dan majlis dilaksana oleh Menteri Komunikasi dan Multimedia Datuk Seri Saifuddin Abdullah) mempunyai 5 tonggak dan bernilai RM1.8 billion merupakan inisiatif terbesar negara untuk memastikan keselamatan siber negara sejak kedaulatan elektronik dijadikan teras dalam Agenda I.T Negara pada tahun 1996. MCSS adalah strategi yang dipertanggungjawabkan kepada Agensi Keselamatan Siber Negara (NACSA), Majlis Keselamatan Negara. MCSS akan dilaksana antara tahun 2020 hingga 2024.

Pada tahun-tahun yang lepas, dalam usaha mempertingkat kedaulatan elektronik negara, Malaysia telah merealisasikan Akta Tandatangan Digital (1997), Dasar Keselamatan Siber Negara (2006), Akta Perlindungan Data Peribadi (2010), Dasar Kriptografi Negara (2013) dan terkini MCSS (2020).

Dengan pelbagai usaha sejak 1996, Malaysia sepatutnya telah mempunyai upaya keselamatan maklumat yang mantap menjelang 2020. Namun, dengan hanya menggunakan enjin pencarian internet dengan kata kunci "*data breach Malaysia*", begitu banyak maklumat mudah diperolehi berkenaan kebocoron data milik rakyat Malaysia yang berada dalam keadaan boleh dibaca.

Kajian Microsoft dan Frost & Sullivan melalui laporan bertajuk "*Understanding the Cybersecurity Threat Landscape in Asia Pacific: Securing the Modern Enterprise in a Digital World*" pada tahun 2018, mendedahkan kerugian ekonomi di Malaysia berkaitan keselamatan siber boleh mencecah US$12.2 billion. Ini adalah 4 peratus daripada KDNK negara yang dianggarkan pada nilai US$296 billion.

Data breach yang merugikan berlaku kerana data yang disimpan dipengkalan data masih berada dalam keadaan boleh dibaca. Untuk mengatasi perkara ini kaedah kriptografi perlu dilaksanakan. Kriptografi merupakan kaedah yang berupaya menyulitkan maklumat yang hanya pemilik kunci sahaja boleh menyahsulit dan membaca maklumat tersebut.

Mengabaikan kriptografi akan menyebabkan data yang berjaya dicuri berada dalam bentuk yang boleh dibaca. Proses mencuri data dikenali sebagai "*hacking*", manakala proses menyahsulit data dicuri yang berada dalam keadaan sulit, dikenali sebagai "*cracking*".

Jika sistemkripto yang diguna adalah mantap, proses untuk memecahkan penyulitan tanpa kunci rahsia yang digunakan, merupakan proses yang tidak dapat dilakukan – walau dengan semua keupayaan pengkomputeran berprestasi tinggi sedia ada. Oleh itu, data yang berjaya dicuri tidak boleh dibaca dan tidak bermanfaat kepada pencuri data tersebut.

Kriptografi yang merupakan kaedah pertahanan terakhir keselamatan maklumat, perlulah menjadi salah satu keutamaan MCSS. Amat jelas bahawa tanpa hala tuju memperkasakan penggunaan kriptografi di Malaysia, usaha-usaha mempertingkatkan prasarana keselamatan maklumat negara akan kekurangan elemen kritikal dalam memastikan keselamatan maklumat.

Selain dari memastikan penyelidikan dan pembangunan (R&D) kriptografi tempatan diupayakan, MCSS juga perlu dengan jelas menggariskan tatacara mempertingkatkan keupayaan sumber manusia tempatan dalam bidang kriptografi. Oleh kerana kriptografi merupakan bidang ilmu yang merangkumi matematik, sains komputer dan kejuruteraan, maka tidak hairanlah bidang ini sering diketepikan, kerana untuk menggarap ilmunya merupakan suatu cabaran. Terkini, dengan munculnya teknologi komputer kuantum, kriptografi akan melibatkan juga bidang fizik kuantum.

Dalam menyedari hakikat ini, Institut Penyelidikan Matematik, Universiti Putra Malaysia (INSPEM, UPM) yang telah melaksanakan R&D dan pembangunan sumber manusia dalam bidang kriptografi sejak 2002 dan Persatuan Penyelidikan Kriptologi Malaysia (MSCR – tubuh 2007); berpendapat MCSS perlu dijadikan platform yang terbaik untuk memperkasa kriptografi di Malaysia. Justeru, salah satu indeks pencapaian utama (KPI) MCSS hendaklah berjaya memperlihatkan peningkatan R&D, sumber manusia dan penggunaan kriptografi yang betul dan meluas di Malaysia.