Tingkat tahap keselamatan siber demi kestabilan negara

Anonymous Malaysia (Anonymous) memuat naik video di Facebook, antara lain memberi memberi amaran kepada Kerajaan Malaysia bahawa sistem keselamatan berada pada tahap lemah sehingga mengundang risiko penggodaman dan ancaman siber.

Walaupun amaran itu belum dapat dibukti kesahihannya, mesej disampaikan sepatutnya menjadi refleksi untuk menilai semula tahap keselamatan sistem kerajaan.

Infrastruktur Maklumat Kritikal Nasional (CNII) mengenal pasti beberapa sektor kritikal yang sewajarnya diberi perlindungan. Antaranya sektor pertahanan dan keselamatan negara; perbankan dan kewangan; maklumat dan komunikasi; tenaga; pengangkutan; air; perkhidmatan kesihatan; sektor kerajaan; perkhidmatan kecemasan serta makanan dan pertanian.

Semua infrastruktur maklumat kritikal ini – secara nyata atau maya – jika menjadi sasaran penjenayah siber, akan memberikan kesan amat buruk kepada negara.

Melihat statistik, sebanyak 50,789 insiden keselamatan siber membabitkan pelbagai sektor kerajaan dilaporkan antara 2012 sehingga 2016, diikuti 3,928 lagi pada 2017.

Pada awal Januari 2015 contohnya, data pelanggan Malaysian Airlines Bhd (Malaysia Airlines) dibocorkan secara dalam talian. Ia disebabkan tragedi malang menimpa negara pada 2014 susulan dua kejadian masing-masing membabitkan pesawat MH370 dan MH17.

Sekumpulan penjenayah siber membocorkan data pelanggan Malaysian Airlines dan menggodam laman web syarikat penerbangan itu dengan membuat provokasi '404 - Plane Not Found' dan 'ISIS WILL PREVAIL'.

Ia memberi persepsi buruk terhadap syarikat penerbangan sehingga menyebabkan kerugian berjuta-juta ringgit akibat kehilangan kepercayaan pelanggan.

Jika dihitung, sekurang-kurangnya 2,100 pelayan (server) digodam sepanjang 2016 dengan sebahagian besar milik agensi kerajaan, bank dan universiti. Maklumat diperoleh dijual kepada penjenayah siber.

Impaknya operasi terpaksa dihentikan, organisasi juga terpaksa memperuntukkan dana besar untuk memulihkan pelayar yang rosak akibat digodam.

Tahun 2017 mencatatkan kejadian kebocoran maklumat terbesar dalam sejarah negara apabila 46.2 juta maklumat peribadi pengguna telefon bimbit dibocorkan dalam talian ketika proses pemindahan data di syarikat telekomunikasi.

Data yang bocor disedari pengguna di Lowyat.net dan dipercayai dijual kepada pembeli yang berminat dalam bentuk bitcoin yang tidak diberitahu nilainya.

Kebocoran maklumat seperti alamat rumah, nombor kad pengenalan dan nombor SIM (Modul Pengenalpastian Pelanggan) yang terdedah merisikokan maklumat jatuh ke tangan penjenayah siber untuk pelbagai tujuan jenayah siber.

Pada masa sama, Kementerian Komunikasi dan Multimedia mendedahkan 81,309 rekod daripada Majlis Perubatan Malaysia, Persatuan Perubatan Malaysia (MMA) dan Persatuan Pergigian Malaysia (MDA) dibocorkan dan dijual dalam talian.

Ia menghakis kepercayaan masyarakat terhadap tadbir urus organisasi awam Malaysia untuk melindungi aset maklumat mereka.

Seterusnya, ketika kejohanan Sukan SEA pada 2017 di Kuala Lumpur, terdapat kesilapan dalam buku kecil cenderahati rasmi di mana bendera Indonesia secara tidak sengaja dicetak terbalik.

Akibatnya, sekumpulan penggodam Indonesia dikenali 'ExtremeCrew' melakukan serangan siber besar-besaran ke atas organisasi awam Malaysia. Sebanyak 40 laman web digodam, kebocoran maklumat sulit dan serangan Penolakan Layanan Secara Teragih (DDOS) dilaporkan ke atas organisasi awam Malaysia.

Pada masa sama, penularan virus WannaCry Ransomware berlaku besar-besaran seluruh dunia dan Malaysia tidak terkecuali.

Ransomware adalah sejenis perisian hasad yang menjangkiti platform pengkomputeran dan menyekat akses pengguna. Sistem dijangkiti dapat dibebaskan melalui pembayaran kepada penjenayah siber dalam bentuk bitcoin.

Beberapa organisasi awam Malaysia juga menjadi mangsa ancaman malware di mana sistem dijangkiti, menjangkiti pula sistem lain dalam rangkaian sama.

Sistem tidak dikemas kini akan rentan terhadap serangan malware, menyebabkan penjawat awam tidak dapat mengaksesnya memaksa sejumlah wang dibayar kepada penjenayah siber untuk dipulihkan.

Pada 2017 juga menyaksikan kempen pancingan data secara besar-besaran apabila orang ramai menerima panggilan daripada penjenayah siber yang menyamar sebagai penguat kuasa seperti Polis Diraja Malaysia (PDRM).

Melaluinya, maklumat mangsa dicuri dan tanpa disedari, wang dipindahkan secara haram ke dalam akaun penjenayah siber.

Pada awal 2018, negara sekali lagi dikejutkan kejadian kebocoran maklumat dalam talian membabitkan 200,000 maklumat peribadi penderma organ. Kebocoran maklumat penderma organ dipercayai dicuri daripada pangkalan data pusat dan mempunyai pelbagai maklumat seperti rekod pesakit, alamat, nombor kad pengenalan dan sebagainya.

Selain itu, portal Sistem Analisis Peperiksaan Sekolah (SAPS) Kementerian Pendidikan yang bertujuan menganalisis keputusan peperiksaan turut dilapor mengalami kelompongan terhadap keselamatan yang berpotensi mendedahkan lebih 10.3 juta maklumat peribadi pelajar dan ibu bapa.

Data itu membabitkan bilangan pelajar sekolah seperti nombor MyKad, nombor pengenalan ibu bapa, alamat dan status ibu bapa, seterusnya dapat memberikan akses ke seluruh unit keluarga.

Kebocoran maklumat ini disebabkan kelemahan sistem yang tidak menangani ciri keselamatan, di mana penggodam dapat mencuri maklumat dengan mudah.

Tahun 2019 pula menyaksikan 19,922 rekod radiologi pesakit seperti nama, tarikh lahir, tarikh pemeriksaan, skop penyiasatan, jenis prosedur pengimejan, doktor perawat, nama klinik serta foto imbasan X-ray, imbasan tomografi (CT) dan pengimejan resonans magnet (MRI) dilapor dapat diakses secara terbuka.

Maklumat sensitif pesakit ini, termasuk dalam 24 juta rekod pesakit seluruh dunia dibocorkan penjenayah siber.

November 2020 pula, MyCERT menerima beberapa laporan kejadian merujuk berita bahawa eksploitasi dalam talian berlaku untuk mencuri bukti kelayakan Rangkaian Peribadi Maya (VPN) daripada lebih 49,000 VPN SSL Fortinet yang rentan. Rangkaian Malaysia turut disenarai dan berpotensi menjadi sasaran.

Seterusnya, Jabatan Perlindungan Data Peribadi (JPDP) mengeluarkan kenyataan berkaitan penyalahgunaan data peribadi menerusi aplikasi mudah alih dilakukan penyedia pinjaman dalam talian tanpa lesen.

Kerosakan laman web secara besar-besaran juga membabitkan pelbagai laman web Malaysia dilaporkan. Sebilangan besar laman web yang rosak dibiarkan dengan mesej kebencian dan ketidakpuasan hati terhadap Malaysia.

Pada penghujung 2020, negara digemparkan dengan cubaan penggodaman rangkaian data Angkatan Tentera Malaysia (ATM). Dilaporkan kejadian ancaman keselamatan siber ini dikesan Bahagian Siber dan Elektromagnetik Pertahanan (BSEP) serta Pusat Operasi Pertahanan Siber (CDOC) ATM.

Melihat insiden keselamatan maklumat ini, adalah keutamaan bagi organisasi awam Malaysia untuk lebih fokus pada keselamatan maklumat, terutama dalam aspek sosial.

Dengan adanya amalan keselamatan maklumat dalam organisasi awam Malaysia, pekerja akan lebih berhati-hati dalam menangani teknologi keselamatan maklumat sehingga risiko insiden keselamatan maklumat dapat dikurangkan dan memberi kesan positif terhadap tahap keselamatan maklumat di negara ini secara kolektif.

Kerajaan Malaysia diseru melihat lebih teliti aspek keselamatan siber dengan meningkatkan dan memperkemas tahap keselamatan siber supaya insiden yang dapat menggugat kestabilan negara dapat dielakkan.

Penulis adalah *Pensyarah Fakulti Pengurusan Maklumat, Universiti Teknologi MARA (UiTM) Johor*