Noor Mohamad Shakil Hameed

HARIAN METRO

Waspada jenayah siber

Perkembangan pesat dunia teknologi maklumat dan komunikasi bukan saja menyumbang kepada pelbagai kebaikan dan kemudahan, tetapi turut mencetuskan cabaran untuk kita berhadapan dengan ancaman dan jenayah siber.

Statistik lebih daripada 10,000 serangan keselamatan siber terhadap syarikat dan individu yang direkodkan di seluruh negara tahun lalu sewajarnya membuka mata semua pihak terhadap cabaran dan keperluan untuk menangani ancaman siber.

Kebergantungan kepada Internet dan teknologi tanpa wayar menyebabkan penjenayah siber cuba mengambil kesempatan. Baik individu mahupun organisasi sering menjadi kelompok sasaran mudah penjenayah itu yang menunggu peluang untuk bertindak. Ironinya kelicikan penjenayah siber boleh menyebabkan kita tidak sedar sedang diancam atau sudah menjadi mangsa jenayah siber.

Begitulah hebatnya strategi penjenayah siber yang dapat melakukan jenayah dari mana sekalipun asalkan ada kemudahan Internet dan kepakaran. Menyedari pihak berkuasa rancak memerangi pelbagai jenayah, penjenayah tegar ini mula beralih kepada jenayah terancang menggunakan platform siber dan maya.

Dengan kepakaran yang dimiliki penjenayah siber mampu melakukan pelbagai aktiviti sabotaj kepada individu mahupun organisasi seperti aktiviti penyebaran spam, menceroboh e-mel, menyalin fail serta mencuri maklumat peribadi. Lebih membimbangkan apabila penjenayah siber mampu melumpuhkan sistem sesebuah organisasi termasuk jabatan kerajaan seperti melumpuhkan sistem pengurusan maklumat atau data serta sistem perbankan.

Secara umumnya, ancaman siber adalah serangan yang dilancarkan secara maya terhadap infrastruktur dan aplikasi komunikasi fizikal dan tanpa wayar. Ancaman siber ini boleh dibahagikan kepada beberapa kategori antaranya pencerobohan iaitu menceroboh sistem dan aplikasi komputer tanpa kebenaran dan berupaya mengubah kandungan sistem itu.

Penipuan atau *fraud* pula merujuk kepada skim penipuan yang menggunakan satu atau lebih komponen Internet dan telekomunikasi seperti ruangan chat, e-mel, laman web dan khidmat pesanan ringkas (SMS) untuk mewujudkan ruangan pembujukan dan transaksi wang yang kelihatan seperti badan kewangan atau syarikat yang beroperasi secara sahih.

Gangguan pula melibatkan penghantaran mesej, gambar dan video berunsur fitnah, lucah, gangguan dan ancaman kepada pengguna lain. Ancaman pencerobohan pula merangkumi serangan ke atas sistem dan aplikasi komputer agensi tertentu dengan tujuan melumpuhkan operasi sistem agensi berkenaan. Kod berbahaya (*Malicious code*) adalah perisian atau skrip komputer yang diprogramkan untuk menceroboh komputer dan merosakkan sistem.

Manakala, gangguan perkhidmatan pula merujuk kepada serangan ke atas sesuatu sistem atau aplikasi komputer yahg boleh menyebabkan pengguna tidak dapat mencapai dan menggunakan sistem atau aplikasi berkenaan.

Di negara kita khususnya ada kira-kira lima jenis jenayah siber atau penipuan dalam talian yang popular iaitu seperti penipuan phising e-mel. Penipuan phising berdasarkan kepada komunikasi yang dilakukan melalui e-mel atau media sosial. Penjenayah siber akan menghantar e-mel dan cuba menipu kita untuk memberi butiran log masuk ke akaun bank, rangkaian sosial dan juga butiran perbadi yang bernilai.

Dalam e-mel itu, penjenayah akan memberikan pautan *(link)* di mana apabila kita akses lama web tersebut ia kelihatan seperti laman web yang sebenar dan meyakinkan tetapi sebenarnya ia dikawal pihak penjenayah siber. Kedua penipuan *money laundering* yang cukup popular dewasa ini. Penipuan bermula dengan mesej berbaur emosi seperti e-mel yang dihantar individu yang kononnya kaya raya dan memerlukan bantuan kita untuk mengeluarkan sejumlah wang dari bank.

Akhirnya kita terpedaya dan memindahkan sejumlah wang yang besar kepada penjenayah. Antara penipuan lain ialah penipuan loteri, penipuan pinjaman bank atau kad kredit terjamin serta penipuan skim cepat kaya.

Justeru, semua pihak perlu sentiasa berhati-hati dan bersedia untuk menangani cabaran dan ancaman siber ini. Kita perlu bertindak segera dan proaktif sebelum penjenayah bertindak. Ia penting demi menjaga keselamatan negara dan rakyat agar ia terus kekal terjamin. Kini, kita boleh merumuskan tahap kesedaran dan pemahaman masyarakat terhadap jenis ancaman siber serta kesannya kepada diri dan negara boleh dikatakan masih rendah, malah boleh dikatakan masih ramai yang langsung tidak ambil tahu dan mempedulikan ancaman siber.

Persoalannya, apakah kita sanggup berputih mata apabila mula menyedari menjadi mangsa jenayah siber. Oleh itu, sebelum semuanya terlambat elok kita berhati-hati dengan memahami secara terperinci ancaman siber.

Di samping meningkatkan tahap kesedaran, antara langkah lain yang wajar diambil untuk menangani masalah jenayah siber ialah kerajaan perlu terus secara aktif menjalinkan kerjasama strategik dengan negara luar. Ia dilihat mampu mempertingkatkan keupayaan bagi menghadapi serangan siber. Hubungan diplomatik yang baik pula wajar digunakan untuk menjalinkan kerjasama dalam konteks berkongsi maklumat dan keselamatan komputer serta kita juga boleh mendapatkan bantuan kepakaran dari negara terbabit.

Kerajaan juga perlu segera melatih lebih ramai anggota keselamatan bagi meningkatkan kemahiran dalam bidang forensik komputer. Kerjasama strategik antara kerajaan dengan pihak swasta serta pengguna komputer pula membolehkan langkah keselamatan dapat dimantapkan lagi termasuk berkongsi masalah pencerobohan dan penggodaman sekali gus memberikan pelbagai cadangan kepada pihak kerajaan.

Kesimpulan, sebagai langkah penguatkuasaan, hukuman terhadap kesalahan jenayah siber sedia ada juga wajar disemak semula supaya ia mampu mendatangkan ketakutan dalam kalangan penjenayah siber. Marilah kita membina benteng keselamatan yang sewajarnya supaya tidak terus menjadi mangsa jenayah siber.

Penulis Timbalan Pengarah Pejabat Strategi Korporat dan Komunikasi Universiti Putra Malaysia

Dialog Kotaraya

Oleh Juragan