Pengurusan Risiko Siber

Teknologi telah memainkan peranan transformatif dalam penyediaan perkhidmatan kewangan dan pembayaran. Selain meningkatkan kecekapan proses, teknologi telah membuka saluran baharu dan berinovatif untuk institusi kewangan memberikan akses dan kemudahan yang lebih baik kepada pengguna. Teknologi juga telah membolehkan institusi kewangan menawarkan dan menguruskan secara berdaya maju rangkaian produk lebih meluas yang berdaya saing serta responsif kepada keperluan pengguna yang berbeza, melalui cara yang tidak mungkin dapat dilakukan sebelum ini. Pelanggan perniagaan dan runcit telah pun menggunakan kemajuan teknologi ini, seperti yang dibuktikan melalui peningkatan berterusan nilai urus niaga perdagangan dalam talian.

Walau bagaimanapun, kemajuan ini memberikan cabaran baharu terhadap pengurusan risiko oleh institusi kewangan. Dengan kebergantungan terhadap teknologi yang semakin meningkat, institusi kewangan menghadapi risiko baharu daripada tindakan berniat jahat oleh penjenayah dan pesalah laku lain. Tindakan ini boleh mengganggu penyediaan perkhidmatan dan juga menggugat kerahsiaan dan integriti data proprietari institusi kewangan serta data pelanggan mereka. Insiden sedemikian boleh menjejaskan reputasi sesebuah institusi kewangan dan boleh melemahkan keyakinan terhadap sistem kewangan.

Kerugian ekonomi global akibat jenayah siber dianggarkan sebanyak kira-kira USD375 bilion setahun[1]. Serangan siber biasanya bermotifkan keuntungan kewangan tetapi juga boleh didorong hasrat ingin menimbulkan gangguan atas tujuan sosial dan politik. Berikutan beberapa insiden keselamatan siber berprofil tinggi dalam sektor kewangan, pengurusan risiko siber telah menjadi perkara yang semakin penting pada peringkat global. Laporan[2] oleh Jawatankuasa Pembayaran dan Infrastruktur Pasaran Bank for International Settlements menekankan sifat risiko siber yang kompleks dan semakin pesat berubah, serta keutamaan yang semakin tinggi diberikan terhadap pengurusan risiko ini secara berkesan. Laporan itu juga mencadangkan pendekatan yang lebih bersepadu bagi mengukuhkan daya tahan siber, yang akan mengurangkan tempoh pemulihan jika berlaku serangan siber, dan pada masa yang sama membolehkan fungsi utama sistem kritikal terus beroperasi. Di Kesatuan Eropah, Jawatankuasa Bersama Lembaga Penyeliaan Eropah juga menggesa pihak berkuasa dan peserta pasaran kewangan supaya memastikan sumber dan perhatian yang mencukupi ditumpukan pada peningkatan daya tahan sistem kewangan terhadap risiko operasi berkaitan dengan IT dan siber.

Bentuk Ancaman Siber

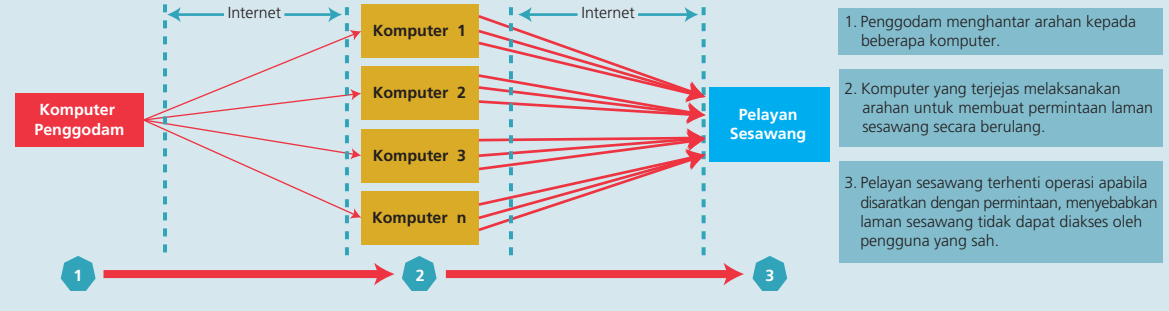
Serangan siber terhadap institusi kewangan kini semakin canggih dan boleh berlaku dalam pelbagai bentuk. Tiga ancaman yang biasa berlaku dalam sektor kewangan ialah:

Penafian Perkhidmatan Teragih (Distributed Denial of Service, DDoS) – Dalam serangan DDoS, sistem yang disasarkan akan terjejas akibat aliran trafik yang besar dihalakan untuk menyebabkannya terhenti daripada beroperasi, sekali gus menafikan akses oleh pengguna yang sah. Satu rangkaian komputer yang sudah dikompromi diarahkan membuat permintaan (seperti laman sesawang tertentu) daripada sistem tersebut secara serentak dan berulang (Rajah 1). Pakar menganggarkan bilangan serangan DDoS di seluruh dunia meningkat sebanyak 20% dalam tempoh dua tahun lepas, pada purata hampir 3,000 insiden sehari, dengan 43% daripadanya disasarkan kepada penyedia perkhidmatan kewangan[3]. Beberapa bank global telah mengalami serangan DDoS yang mengganggu akses pelanggan kepada portal perbankan Internet mereka selama beberapa jam atau sehingga beberapa hari pada satu-satu masa, lantas menghalang pelanggan menjalankan urus niaga dalam talian. Meskipun beberapa bank di Malaysia mengalami serangan DDoS pada tahun 2014, namun serangan ini tidak menyebabkan gangguan perkhidmatan yang ketara.

[1] Sumber: `Net losses: Estimating the global cost of cybercrime', laporan oleh Center for Strategic and International Studies.
[2] Sumber: `Cyber resilience in financial market infrastructures', November 2014.
[3] Sumber: Akamai, Arbor Networks.

Gambar Rajah 1

Serangan Penafian Perkhidmatan Teragih (DDoS) Terhadap Laman Sesawang

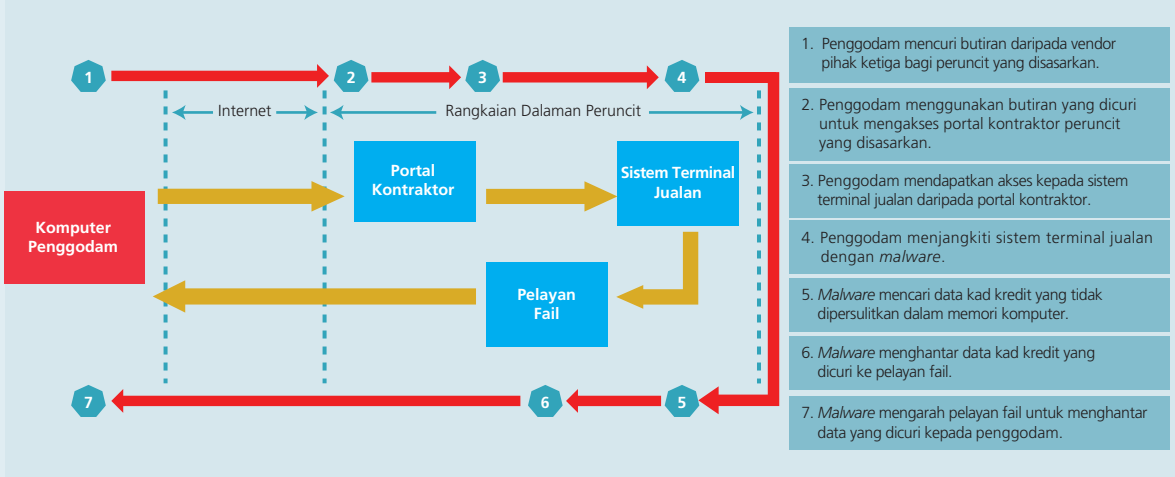


Sumber: Bank Negara Malaysia

Malware – Serangan *malware* melibatkan penggunaan perisian hasad (malicious software) untuk mengawal atau mengganggu operasi sistem atau peranti sasaran. *Malware* wujud dalam pelbagai bentuk, seperti virus dan cecacing, dan boleh menyebabkan kemudaratan melalui cara yang berbeza. Sejenis *malware* biasa dalam konteks perkhidmatan kewangan ialah penggunaan perisian intip yang dipasang pada mesin hos yang tidak dilindungi untuk mengumpul maklumat tentang pengguna, termasuk butiran akses perbankan Internet, nombor kad kredit, atau maklumat persendirian atau sensitif yang lain. Maklumat ini kemudiannya dihantar semula secara terselindung kepada penggodam untuk tujuan melakukan penipuan atau aktiviti haram yang lain (Rajah 2).

Gambar Rajah 2

Serangan *Malware* Terhadap Peruncit



Sumber: Bank Negara Malaysia

Memancing data (Phishing) – *Phishing* merupakan kegiatan penipuan yang paling lazim. Ia merupakan kegiatan memancing data dengan menggunakan laman sesawang palsu untuk mendorong seseorang pengguna yang tidak menaruh syak wasangka (unsuspecting) supaya mendedahkan maklumat sensitif seperti butiran akses perbankan Internet dan kad kreditnya. Maklumat yang dicuri akan digunakan untuk melakukan pemindahan dana tanpa kebenaran atau melakukan penipuan yang lain.

Penjenayah boleh menggabungkan teknik yang berbeza untuk melancarkan serangan canggih terhadap sistem. Sebagai contoh, *malware* boleh digunakan untuk mengawal sebilangan besar komputer untuk menjalankan serangan DDoS. Serangan seperti itu akan kelihatan seolah-olah dilakukan dari pelbagai sumber yang tidak berkaitan, yang membuatkan usaha pertahanan lebih mencabar. Dengan menggabungkan teknik *malware* dan *phishing*, penjenayah boleh memintas Kod Kebenaran Transaksi (TAC) dan melakukan transaksi perbankan dalam talian secara haram tanpa pengetahuan mangsa.

Serangan siber juga telah dilakukan bersama-sama dengan kegiatan jenayah biasa yang lain. Pada tahun 2014, *malware* telah digunakan untuk mendapatkan akses tanpa kebenaran kepada 18 mesin teler automatik (ATM) dalam premis bank di Kuala Lumpur, Selangor, Johor dan Melaka. Dalam insiden ini, penjenayah menyasarkan beberapa ATM yang kurang dikawal dan yang beroperasi menggunakan model lama, lalu mendapatkan akses fizikal kepada komponen dalaman ATM dan kemudiannya memasukkan *malware* ke dalam sistem yang membolehkan ATM tersebut beroperasi. *Malware* ini telah direka khusus untuk mengeksploitasi kelemahan dalam sistem operasi ATM yang sudah lapuk. Ia seterusnya membolehkan penjenayah mengarahkan ATM supaya mengeluarkan wang tunai tanpa apa-apa kebenaran atau pengesahan. Meskipun bank-bank yang terlibat mengalami kerugian sebanyak RM3.4 juta, namun pelanggan tidak terjejas kerana pengeluaran tidak didebitkan daripada mana-mana akaun pelanggan. Bank-bank yang terjejas telah bertindak pantas dengan menaik taraf perkakasan dan perisian ATM ini dan ATM lain yang seumpamanya. Sejak itu, industri perbankan telah mengkaji semula dan melaksanakan amalan pengurusan risiko yang diperbaik serta pelbagai langkah keselamatan fizikal untuk melindungi ATM daripada ancaman seperti itu lagi.

Memandangkan serangan yang dilancarkan menggunakan teknik yang semakin canggih, usaha mengenal pasti dan menjangka ancaman siber dan membangunkan langkah tindak balas yang berkesan terus menjadi cabaran yang kritikal. Ada kalanya, sesebuah organisasi mungkin tidak menyedari bahawa ia menjadi sasaran serangan. Dalam insiden yang dikenali sebagai serangan `hari-sifar' (zero-day), penggodam mengeksploitasi kelemahan yang tidak diketahui oleh sasaran, sehinggakan sasaran tidak mempunyai masa atau peluang untuk menangani kelemahan tersebut. `Ancaman berterusan lanjutan' (advanced persistent threats) juga muncul sejak beberapa tahun kebelakangan ini yang mampu mengekalkan serangan siber secara berulang kali dalam tempoh yang panjang dan dapat disesuaikan dengan usaha untuk menentangnya.

Tindak Balas Industri Dan Pengawalseliaan Terhadap Ancaman Siber

Pada peringkat kebangsaan, inisiatif untuk menangani ancaman keselamatan siber di Malaysia dilaksanakan dan diselaraskan dengan agensi kerajaan lain sebagai sebahagian daripada Rangka Kerja Keselamatan Siber Negara. Di bawah rangka kerja nasional ini, Bank dan institusi kewangan yang dikawal selia dianggap sebagai Infrastruktur Maklumat Kritikal Kebangsaan (CNII), dan oleh itu tertakluk kepada perlindungan yang lebih ketat sebagai mengiktiraf peranan penting mereka kepada negara dan ekonomi. Beberapa inisiatif penting dilaksanakan untuk terus meningkatkan tahap kesediaan siber bagi CNII. Ini termasuk latihan siber tahunan yang menggunakan simulasi senario serangan siber untuk menguji keberkesanan program tindak balas oleh setiap CNII dan kesemua CNII secara kolektif terhadap serangan sistemik. Hasil daripada amalan ini kemudiannya digunakan untuk mengemas kini dan memperbaik tindakan dan strategi tindak balas. Beberapa institusi kewangan telah pun mengambil bahagian dalam latihan siber ini sejak tahun 2009 dan berjaya menamatkan latihan dengan memperlihatkan keberkesanan pelan tindak balas insiden masing-masing dalam mengurus senario serangan siber.

Pada peringkat industri, Pasukan Petugas Perbankan Internet (Pasukan Petugas) yang ditubuhkan oleh Bank dan industri perbankan telah menyokong tindak balas pengawalseliaan yang komprehensif terhadap ancaman keselamatan siber. Pasukan Petugas itu menyediakan forum bagi institusi kewangan berkongsi risikan dan membincangkan isu yang berkaitan dengan perbankan Internet, termasuk keselamatan siber. Melalui Pasukan Petugas ini dan platform yang lain, Bank dan industri

berbincang dan berinteraksi secara aktif dengan agensi kerajaan yang lain, termasuk Suruhanjaya Komunikasi dan Multimedia Malaysia, CyberSecurity Malaysia serta Polis Diraja Malaysia. Perbincangan dan interaksi ini membolehkan semua pihak berkepentingan, termasuk syarikat telekomunikasi dan penyedia perkhidmatan Internet, terus mendapat maklumat yang mencukupi tentang perkembangan ancaman terkini dan ancaman yang akan dihadapi oleh sektor kewangan, selain terus menggalakkan amalan terbaik industri berhubung dengan keselamatan perbankan Internet. Sebagai contoh, Pasukan Petugas ini telah memainkan peranan yang penting dalam mengurangkan ancaman penipuan berasaskan SMS yang tersebar luas beberapa tahun yang lalu. Pasukan Petugas ini berkongsi butiran teknikal dan maklumat tentang modus operandi kegiatan penipuan ini yang membolehkan kelemahan dalam proses sedia ada dikenal pasti dan ditangani, seperti menghendaki pelanggan perbankan Internet tertentu supaya mendaftar sendiri di cawangan. Langkah ini telah membawa kepada penurunan yang ketara dalam kejadian penipuan berasaskan SMS. Dalam kapasitinya sebagai pihak berkuasa berwibawa untuk menerima dan menganalisis maklumat tentang transaksi yang mencurigakan, Bank juga mengedarkan maklumat risikan kewangan berkaitan dengan individu yang disyaki memudahkan transaksi, serta pemegang akaun *mule*[4] (mule account holder), untuk menyokong siasatan oleh agensi penguatkuasaan undang-undang dan mengukuhkan usaha bersama dalam memerangi jenayah siber.

Pada peringkat institusi, institusi kewangan terus mempelbagaikan taktik pertahanan dan amalan keselamatan IT untuk menghalang dan bertahan daripada ancaman siber yang bakal dihadapi, termasuk:

- pembahagian zon rangkaian untuk mengawal akses pengguna dan mengehadkan penyebaran apa-apa ancaman yang menembusi rangkaian;
- melaksanakan kawalan tambahan dalam pelbagai lapisan infrastruktur rangkaian (defense-in-depth) supaya kegagalan pada satu langkah kawalan dapat ditampung oleh kawalan dalam lapisan yang lain;
- memasang alat keselamatan rangkaian yang sesuai seperti sistem pencegahan pencerobohan (IPS) dan penggunaan *firewall* yang berlapis-lapis, termasuk *web application firewall* (WAF) untuk menambah baik strategi menangani DDoS ;
- menjalankan penilaian keselamatan yang kerap dan rapi terhadap infrastruktur IT, termasuk ujian penembusan yang ketat. Skop ujian penembusan ini juga telah diperluas untuk melibatkan aplikasi berasaskan peranti mudah alih;
- memastikan pemantauan dan pengawasan keselamatan yang berterusan bagi membolehkan pengesanan awal terhadap pencerobohan; dan
- mewujudkan pasukan tindak balas kecemasan komputer untuk menambah baik masa tindak balas terhadap insiden siber.

Keberkesanan dan ketekalan amalan ini juga sering dikaji semula oleh juruaudit institusi kewangan, dan apa-apa kelemahan yang dikenal pasti segera diketengahkan untuk pembaikan. Namun, pengurusan yang wajar bagi risiko keselamatan siber sebenarnya merupakan tanggungjawab pada peringkat lembaga pengarah. Bank menghendaki lembaga pengarah institusi kewangan supaya memastikan keutamaan dan sumber yang cukup diperuntukkan kepada pengawasan dan pengurusan risiko ini. Sesetengah lembaga pengarah telah pun mencapai kemajuan dalam bidang ini seperti yang dibuktikan melalui perbincangan yang lebih mantap tentang strategi pengurusan risiko dan pemahaman yang lebih mendalam mengenai aspek keselamatan siber yang lebih teknikal.

Di pihak Bank, pelbagai garis panduan telah dikeluarkan untuk menetapkan piawaian minimum yang perlu dipatuhi oleh institusi kewangan dalam penyediaan perkhidmatan perbankan elektronik dan pengurusan sistem dan rangkaian IT. Dari semasa ke semasa, ini akan disokong oleh panduan tambahan yang diterbitkan oleh Bank untuk menghadapi ancaman tertentu, seperti keperluan terperinci untuk mengukuhkan kawalan keselamatan di kiosk perbankan Internet awam dan

[4] Pihak yang membenarkan akaun bank mereka digunakan oleh penjenayah untuk menyimpan atau memindahkan wang yang diperoleh secara tidak sah.

meningkatkan ketersediaan terhadap serangan DDoS. Bank kini sedang dalam proses mengkaji semula dan mengemas kini piawaian serta panduan pengawalseliaan yang sedia ada untuk terus memantapkan piawaian keselamatan IT di seluruh sektor kewangan, serta meningkatkan pertahanan dan tindak balas industri terhadap ancaman siber yang berubah-ubah. Objektif utama piawaian baharu yang akan dikeluarkan pada tahun 2015 adalah untuk:

- mengukuhkan tadbir urus bagi keselamatan siber dalam institusi kewangan;
- memastikan fokus strategik dan sumber yang mencukupi disalurkan oleh institusi kewangan kepada pengurusan risiko keselamatan siber;
- menyediakan panduan praktikal yang mencerminkan landskap teknologi dan model perniagaan yang berubah, dan cukup fleksibel untuk berhadapan dengan ancaman baharu;
- meningkatkan ketegasan penilaian institusi kewangan terhadap ancaman siber dan kualiti maklumat yang digunakan untuk memaklumkan penilaian tersebut;
- memperbaik pelan pemulihan dan luar jangka atau pengaturan kesinambungan perniagaan; dan
- menggalakkan penilaian wajar yang lebih mantap terhadap penyedia perkhidmatan pihak ketiga yang kritikal.

Bagi memastikan pengguna juga dapat melindungi diri daripada ancaman-ancaman siber ini, usaha juga telah dijalankan oleh Bank bersama-sama dengan industri, untuk menggalakkan kesedaran tentang amalan dalam talian yang selamat. Selain mengadakan program pendidikan pengguna secara berterusan, institusi kewangan juga telah meningkatkan usaha memberikan panduan keselamatan perbankan dalam talian di laman sesawang mereka.

Memandangkan kaedah dan alat keselamatan IT sedia ada sentiasa menghadapi ancaman baharu, sektor kewangan perlu terus berwaspada terhadap kelemahan yang mungkin wujud dalam sistem kritikalnya, dan terus mengemas kini pertahanannya serta memperkukuh strateginya untuk menangani dan mengurus risiko siber yang akan dihadapi. Ini termasuk meningkatkan keupayaan pengumpulan maklumat risikan dan juga menggunakan pendekatan yang lebih bersepadu dan terselaras dalam menangani ancaman siber.