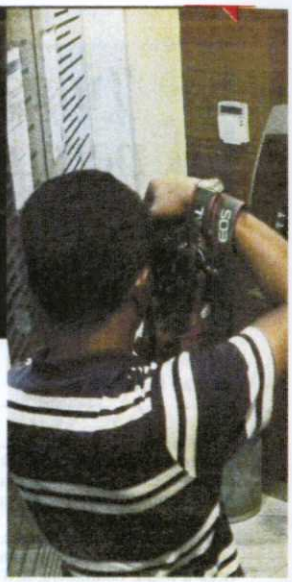
KERATAN AKHBAR-AKHBAR TEMPATAN
TARIKH: 05 OKTOBER 2014 (AHAD)

Bil	Tajuk	Akhbar
1.	Pengguna perlu ada kesedaran keselamatan siber	Berita Harian

KERATAN AKHBAR
BERITA HARIAN (RENCANA) : MUKA SURAT 28
TARIKH : 5 OKTOBER 2014 (AHAD)

Pengguna perlu ada kesedaran keselamatan siber

Kes penipuan atas talian, perbankan semakin serius



Wartawan: Revolusi kebebasan internet di seluruh dunia, termasuk Malaysia tidak boleh lari daripada kesan negatif kepada rakyat dan negara. Ia boleh digunakan untuk pelbagai tujuan termasuk jenayah, buli, penyalahgunaan kuasa dan pelbagai lagi. Apa penilaian dan komen CyberSecurity Malaysia mengenai perkembangan semasa yang berlaku sekarang?

Dr Amirudin: Internet kini adalah medium yang penting untuk rakyat Malaysia, termasuk berkongsi dan menyuarakan pandangan mereka mengenai pelbagai isu melalui laman media sosial. Mengikut Laporan Pencapaian Industri 2013, ada 19.2 juta pengguna dalam talian di Malaysia dan 15.6 juta daripadanya aktif dalam laman sosial Facebook. Namun, dalam kalangan pengguna internet ini, ada juga mereka yang menyalahgunakan kemudahan internet untuk perlakuan jenayah dan mengaut keuntungan secara haram.

Laman media sosial kini sering disalahgunakan untuk menyebarkan fitnah, hasutan, ugutan atau kandungan berbaur keagamaan dan perkauman serta provokasi yang boleh menggugat keharmonian dan keselamatan negara. Mereka didorong untuk melakukan perbuatan itu kerana menganggap alam siber selamat daripada dikesan oleh pihak berkuasa dan identiti mereka tidak boleh dicam atau dipalsukan. Kumpulan pelampau politik, agama dan kaum juga menggunakan internet untuk melancarkan propaganda dan menjalankan aktiviti mengikut agenda mereka sendiri.

Dalam hal ini, Malaysia sentiasa melindungi hak kebebasan bersuara oleh pengguna internet berdasarkan Artikel 10 - Perlembagaan Malaysia dan jaminan tiada tapisan terhadap Internet berdasarkan Jaminan Bilangan 7 Multimedia Super Corridor (MSC Bill of Guarantees No. 7). Namun, ia tidak bererti sesiapa saja boleh menyebarkan fitnah, hasutan dan provokasi dengan sewenang-wenangnya tanpa mengambil kira peraturan dan undang-undang di negara ini. Pengguna internet tertakluk kepada undang-undang negara antaranya termasuk Akta Komunikasi dan Multimedia 1998, Akta Jenayah Komputer 1997, Akta Perlindungan Data Peribadi 2010, Akta Hasutan 1948 dan Akta Fitnah 1957.

Semua negara terutama di Asia mempunyai kawalan undang-undang terhadap hak individu dan kebebasan bersuara agar ia seiringan dengan kepentingan keselamatan negara. Dalam hal ini, tiada kebebasan mutlak di alam siber kerana ia boleh disalahgunakan oleh pihak tertentu untuk menjejaskan keharmonian masyarakat berbilang bangsa dan agama di negara ini. Justeru, pengguna internet perlu mempunyai perlakuan yang beretika dan bertanggungjawab supaya tidak menimbulkan kekecohan dan huru-hara dalam kalangan rakyat yang boleh memberi kesan negatif kepada imej negara dan menjejaskan kesejahteraan awam dan keselamatan negara.

Kecanggihan dan kemudahan teknologi terkini memudahkan urusan perbankan. Malah urusan berkenaan boleh dilakukan di mana saja tanpa mengira masa. Namun, wujud pihak tidak bertanggungjawab mencuri dan memindah wang orang lain melalui medium elektronik dan terbaharu negara dikejutkan dengan kes kecurian wang daripada 16 mesin pengeluaran wang automatik (ATM) di Johor, Selangor, Melaka dan Kuala Lumpur membabitkan kehilangan lebih RM3 juta. Pendedahan polis itu memang mengejutkan banyak pihak. Wartawan BH AHAD, MOHD AZIS NGAH dan ROHANIZA IDRIS mewawancara Ketua Pegawai Eksekutif, CyberSecurity Malaysia, Dr Amirudin Abdul Wahab dan Pengarah Eksekutif Persatuan Institusi Perbankan Islam Malaysia (AIBIM), Yusry Yusoff berhubung keselamatan siber serta kesan ancaman jenayah siber terhadap industri perbankan di negara ini.

S: Aplikasi yang banyak diguna pakai di Malaysia dan yang berisiko untuk mudah ditipu, disalah guna atau maklumat peribadi mudah diceroboh dan digunakan bagi tujuan tertentu. Bagaimana dengan modus operandi yang digunakan dan contoh kes secara am?

J: Antara aplikasi internet yang sering menjadi sasaran serangan penggodam ialah laman jual beli atas talian, permainan siber dan perbankan atas talian. Sebagai contoh, ada laman jual beli tertentu yang meminta pengguna memasukkan nombor kad kredit mereka dan maklumat peribadi yang mana laman ini adalah laman jual beli palsu. Maklumat tadi akan diambil oleh penjenayah siber untuk melakukan transaksi tanpa pengetahuan pengguna.

Ada laman yang memaparkan barang menarik contohnya telefon mudah alih, tablet dan aksesori wanita. Pengguna telah melakukan pembelian di laman berkenaan menggunakan kredit kad, tetapi selepas menunggu sekian lama, barang yang ditempah tidak tiba ke tangan pembeli. Rupa-rupanya laman itu telah mengambil duit bayaran pembeli tadi tanpa disedari. Oleh hal demikian, adalah penting untuk pengguna melakukan transaksi di laman yang dipercayai dan selamat untuk melakukan transaksi kewangan dan urusan jual beli.

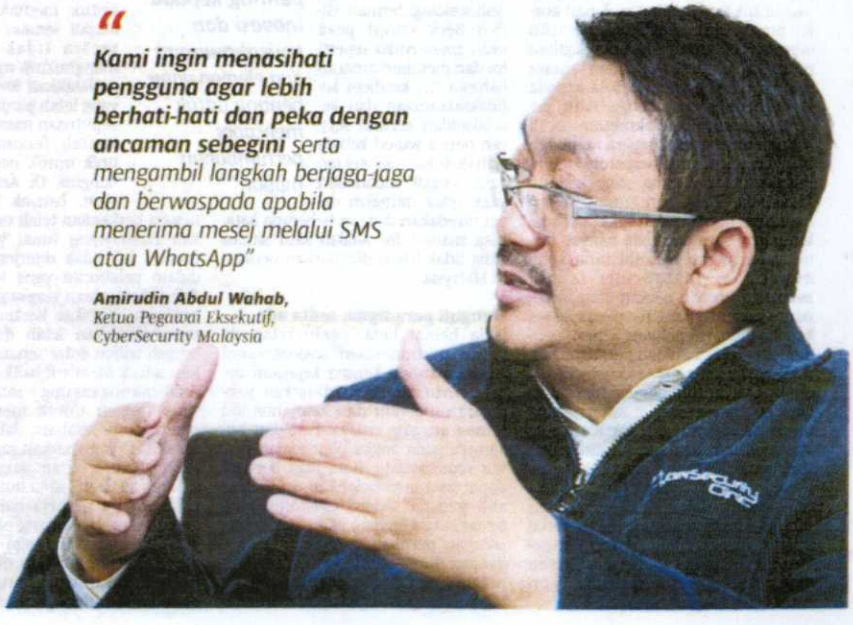
S: Kemudahan e-mel yang pernah dikatakan antara yang selamat juga kerap menjadi mangsa ceroboh atau e-mel palsu. Bagaimana pengguna boleh mengelak daripada terjebak daripada melayan sebarang e-mel yang meragukan dan tindakan susulan yang perlu dilakukan seperti kes, pengguna terpilih diumumkan memenangi hadiah secara rawak dan perlu mengikuti langkah tertentu sebelum boleh menuntut hadiah dan kes penjenayah memintas e-mel bank?

J: Keselamatan siber tidak akan berjaya tanpa wujudnya kesedaran dalam kalangan pengguna internet itu sendiri. Penyebaran e-mel spam akan terus berlaku selagi masih ada pengguna yang 'klik' pada pautan yang dihantar melalui e-mel ataupun memberi reaksi kepada e-mel yang menjanjikan wang pulangan lumayan berbentuk loteri atau pelaburan. Sebagai pengguna, mereka harus sedar mengenai kewujudan jenayah siber. Mereka juga harus tahu bahawa tiada keuntungan atau kemenangan yang mudah akan datang sekelip mata melalui e-mel. Selain itu, pengguna juga harus mempunyai pengetahuan asas mengenai keselamatan siber untuk memeriksa sama ada aplikasi atau laman web yang mereka lawati itu selamat dan tulen (asli).

S: Kes siber kerap dilaporkan kepada CyberSecurity Malaysia. Adakah berlaku peningkatan kes dan tahap seriusnya kes. Statistik jika ada serta peruntukkan undang-undang berkaitan yang digunakan?

J: Kes atau insiden keselamatan siber

> "***Kami ingin menasihati pengguna agar lebih berhati-hati dan peka dengan ancaman sebegini*** *serta mengambil langkah berjaga-jaga dan berwaspada apabila menerima mesej melalui SMS atau WhatsApp"*
>
> ***Amirudin Abdul Wahab,***
> *Ketua Pegawai Eksekutif, CyberSecurity Malaysia*



SAMBUNGAN...
BERITA HARIAN (RENCANA) : MUKA SURAT 29
TARIKH : 5 OKTOBER 2014 (AHAD)

Anggota Polis Forensik membuat pemeriksaan ke atas ***mesin ATM yang di godam baru-baru ini.***

Maklumat pelanggan tak terancam walaupun ATM digodam

yang kerap dan yang paling banyak dilaporkan ke Pusat Bantuan Cyber999 kami adalah Penipuan (Fraud). Umumnya, ada peningkatan dalam kes penipuan atas talian dan ia serius kerana membabitkan kehilangan wang. Di bawah Penipuan atas talian (Fraud) ini ada banyak sub-kategori antaranya, penipuan pembelian barangan. Kes seperti ini tertakluk di bawah akta yang terdapat di Kementerian Perdagangan Dalam Negeri, Koperasi dan Kepenggunaan. Contoh sub-insiden lain ialah pelaburan tidak sah yang tertakluk kepada akta berkaitan yang boleh disabitkan sama ada di bawah Suruhanjaya Syarikat (SSM) atau Suruhanjaya Sekuriti. Mengikut statistik pada 2009 sebanyak 3,564 kes dilaporkan; 8,090 kes (2010); 15,218 (2011); 9,986 (2012); 10,636 (2013) dan sehingga September lalu (2014) 8,140 kes dilaporkan.

S: Adakah benar dakwaan pengguna yang melayari laman web mana-mana bank dan menjalankan urus niaga secara online atau dalam talian melalui telefon bimbit berisiko mendedahkan data peribadi mereka. Apa komen dan cadangan?

J: Sekiranya telefon pengguna bebas daripada sebarang aplikasi yang mencurigakan dan laman web bank yang mereka layari adalah laman web yang asli, sudah pasti tidak akan timbul soal pendedahan data peribadi. Pihak bank khususnya sudah menjelaskan kepada pengguna dalam syarat langganan bahawa perlindungan data peribadi mereka adalah di bawah Akta Perlindungan Data Peribadi 2010 yang telah dikuatkuasakan mulai November 2013. Namun, pendedahan data peribadi mungkin boleh berlaku apabila pengguna itu sendiri melayari laman web mana-mana bank dan ketika menjalankan urus niaga secara dalam talian sekiranya pihak pengguna cuai dan mendedahkan maklumat peribadi mereka akibat daripada teknik 'social engineering' yang digunakan oleh pihak penjenayah siber. Penjenayah siber menggunakan pelbagai teknik antaranya melalui jangkitan virus yang dikenali sebagai Zeus. Virus ini mempunyai keupayaan untuk mencuri data, log masuk dan mengambil fail dari komputer yang dijangkiti.

Seperti insiden yang berlaku baru-baru ini, pihak MyCERT (satu daripada jabatan dalam CyberSecurity Malaysia) telah memberi peringatan kepada pengguna supaya berhati-hati mengenai ancaman virus Zeus yang digunakan oleh penjenayah siber untuk menjangkitkan komputer dengan memperdaya pengguna sebelum mengumpul nombor telefon pengguna. Penjenayah kemudiannya akan menghantar khidmat pesanan ringkas (SMS) yang mempunyai pautan untuk memuat turun sesuatu yang telah dipasangkan malware yang akan diserap ke dalam telefon bimbit pengguna.

Kami ingin menasihati pengguna agar lebih berhati-hati dan peka dengan ancaman sebegini serta mengambil langkah berjaga-jaga dan berwaspada apabila menerima mesej melalui SMS atau WhatsApp. Jika tidak pasti, hubungi pihak bank dan minta penjelasan sama ada mesej yang dihantar sah atau tidak.

Sekiranya pengguna menghadapi masalah pencerobohan ke atas sistem komputer, mereka boleh menghubungi CyberSecurity Malaysia melalui e-mel di cyber999@cybersecurity.my atau menghantar SMS ke 15888. Untuk pengguna telefon pintar, pastikan aplikasi yang dimuat turun adalah bebas daripada program jahat dan pastikan pembuat aplikasi tersebut adalah daripada sumber yang boleh dipercayai; jangan klik pada adware atau URL yang mencurigakan dihantar melalui SMS.

Oleh kerana URL pada laman mudah alih muncul berbeza daripada pelayar desktop, sila pastikan kesahihan URL berkenaan terlebih dahulu dan gunakan perisian antivirus yang dipercayai dan sentiasa mengemaskini perisian antivirus anda.

S: Berapa banyak kes yang diterima, disiasat dan diambil tindakan oleh Pusat Bantuan Cyber999?

J: Cyber999 adalah pusat tindak balas insiden keselamatan siber. Orang ramai dialu-alukan menghubungi Pusat Bantuan Cyber999 (cyber999@cybersecurity.my) untuk melaporkan kerunsingan yang disebabkan oleh kejadian di ruang siber yang mengancam keselamatan atau peribadi mereka. Pengendali insiden yang terlatih akan membantu pengadu menyelesaikan insiden. Pengendali insiden juga bekerjasama dengan jabatan yang berkaitan di CyberSecurity Malaysia atau organisasi lain seperti agensi penguatkuasaan undang-undang, badan-badan yang mengawal selia, dan pembekal perkhidmatan internet untuk membantu menyelesaikan masalah pengadu. Sehingga September lalu 55,634 kes dilaporkan dan semua kes disiasat dan diambil tindakan.

S: Perkembangan terkini mengenai ancaman virus jenis malware ke atas pengguna telefon mudah alih berasaskan android. Adakah jumlah kes serangan 'Trojan' jenis Carberp ini semakin meningkat dan bagaimana dengan tahap kawalan di Malaysia?

J: Pada masa kini masalah malware yang membabitkan perbankan dalam talian atau online sangat berleluasa dan menyasarkan pengguna telefon pintar. Hal ini sangat mudah terjadinya penipuan secara 'mobile online' sekiranya pengguna tidak peka dengan kesedaran keselamatan internet. Dengan penggunaan malware sebagai ejen mendapatkan maklumat sensitif, pengguna sudah pastinya tidak sedar maklumat mereka telah dicuri. Trojan jenis Carberp tidak memberi ancaman besar di Malaysia setakat ini. Namun kemunculan malware seperti Zeus sesuatu yang perlu diberi perhatian memandangkan telah terjadi beberapa kes membabitkan membabitkan kehilangan wang pengguna.

Wartawan: Bagaimana AIBIM melihat isu menggodam mesin juruwang automatik (ATM) serta sistem perbankan internet yang menerima ancaman sejak kebelakangan ini?

J: Isu menggodam ATM adalah satu perbuatan jenayah yang amat serius. Ia menggugat operasi perbankan, menimbulkan keresahan pelanggan terhadap keselamatan wang mereka dan mengganggu perjalanan aktiviti ekonomi. Ia juga mendatang kesusahan kepada orang ramai dalam urusan kewangan mereka. Pihak AIBIM dan ahlinya akan bekerjasama dengan pihak berkuasa dalam membantu membanteras ancaman ini.

S: Apakah langkah keselamatan yang sudah diambil bagi menangani perkara ini?

J: Pihak bank bekerjasama dengan Polis Diraja Malaysia (PDRM) dan Bank Negara Malaysia (BNM) bagi meningkatkan langkah keselamatan. Selain menambahbaik sistem perisian ATM, pihak bank juga akan meningkatkan kawalan keselamatan di kawasan ATM melalui rondaan keselamatan dan pemantauan berterusan melalui CCTV. Keselamatan mesin ATM juga akan terus diperkukuhkan.

S: Adakah maklumat pelanggan terancam?

J: Maklumat pelanggan tidak terancam akibat penggodaman mesin ATM. Ia juga tidak mengganggu sistem teras perbankan. Namun, pihak bank akan terus mengambil langkah untuk mengukuhkan sistem bagi memastikan maklumat pelanggan tidak terancam.

> "***Pelanggan juga harus mengambil langkah berjaga-jaga**, terutama tidak mendedahkan maklumat perbankan seperti kata laluan"*
>
> ***Yusry Yusoff,***
> *Pengarah Eksekutif*
> *Persatuan Institusi*
> *Perbankan Islam Malaysia*

S: Bagaimana menangani isu keselamatan berkaitan keselamatan siber?

J: Pihak bank akan memantau aktiviti yang meragukan serta melakukan penambahbaikan sistem untuk mencegah daripada berulang kejadian yang sama. Namun, pelanggan juga harus mengambil langkah berjaga-jaga, terutama tidak mendedahkan maklumat perbankan seperti kata laluan. Mereka perlu mengelakkan daripada terperdaya dengan mesej yang meragukan dan perlu menghubungi pihak bank jika tidak pasti. Mereka juga disarankan untuk mendapatkan maklumat terkini dari laman sesawang pihak berkuasa seperti PDRM dan BNM.

S: Cabaran dan halangan menangani isu ini?

J: Isu berkaitan jenayah teknologi adalah sangat mencabar kerana kita tidak dapat jangkakan bila ia boleh berlaku. Bagi menangani cabaran ini, kita akan sentiasa mengambil langkah berjaga-jaga demi meningkatkan kepercayaan pelanggan terhadap sistem perbankan. Pihak AIBIM bersama-sama PDRM dan BNM akan terus memantau dan terus meningkatkan keselamatan perbankan dalam memastikan maklumat dan akaun pelanggan terus dilindungi daripada penjenayah siber. Kami juga akan terus mengadakan program kesedaran berkaitan isu ini.