ANCAMAN SIBER: MITOS ATAU REALITI?

Oleh
Pusat Keselamatan dan Tindakbalas Kecemasan ICT Kebangsaan (NISER)
Utusan Malaysia 15 Oktober 2003

PENGENALAN

Dominasi dan pertumbuhan pesat Teknologi Maklumat dan Komunikasi (ICT) telah menjadikan serangan siber satu bentuk senjata yang menarik dan berkesan untuk digunakan ke atas sesebuah negara.

Ini adalah kerana kosnya yang murah berbanding dengan kos yang diperlukan untuk pembangunan, penyelenggaraan serta penggunaan keupayaan ketenteraan yang canggih.

Hanya dengan usaha yang minima diperlukan untuk merekrut agen atau pengintip, mencipta maklumat palsu, memanipulasi maklumat atau melancarkan kod berbahaya (malicious code) ke atas sesebuah sistem maklumat yang dihubungkan melalui prasarana telekomunikasi yang dikongsi secara global.

KES-KES ANCAMAN SIBER

Sesetengah orang percaya bahawa ancaman siber hanyalah satu konsep sahaja, sementara ada yang berpendapat bahawa serangan siber adalah perkara yang sangat serius dan boleh dianggap sebagai ancaman kepada keselamatan negara.

Malah ada yang mengatakan bahawa satu Pelabuhan Harbour Elektronik sedang dicipta. Konsep ini dinamakan sedemikian sempena peristiwa serangan terhadap Pearl Harbour pada Perang Dunia Kedua.

Walaupun tidak ramai yang mengetahui kesannya, kisah-kisah kejayaan serangan siber yang telah berlaku boleh dijadikan sebagai teladan untuk kita mengambil langkah berjaga-jaga.

Banyak kisah serangan siber yang dilaporkan berlaku di luar Malaysia berikutan aktiviti penggodam. Contohnya pada tahun 1996, seorang penggodam komputer yang menggunakan nama sebagai “u4ea” telah dilaporkan memperolehi laluan kepada direktori utama dan memusnahkan struktur system fail di Universiti George Mason, Universiti Arkansas, satu laman web di Netherlands, dan kemungkinan beberapa laman web kepunyaan kerajaan Amerika Syarikat.

Dianggarkan bahawa “u4ea” telah berjaya memasuki lebih daripada 100 sistem yang berasingan.

Dalam satu kejadian yang lain, 13 pelayan asas yang menjadi tapak Sistem Nama Domain Internet telah diserang pada bulan Oktober 2002.

Para pakar ICT percaya bahawa serangan tersebut adalah cubaan untuk melumpuhkan Internet secara tersusun. Ada kemungkinan serangan tersebut diatur oleh pengganas atau perbuatan kerajaan tertentu bagi menguji senjata siber mereka, sama seperti keperluan untuk menguji bom nuklear di tengah lautan.

Kejadian terbaru gangguan bekalan elektrik utama yang melumpuhkan Bahagian timur-laut Amerika Syarikat dan Kanada pada lewat petang 14 August 2003 telah menimbulkan persoalan sama ada ia adalah hasil serangan siber.

Ramai yang berasa bimbang tentang keselamatan sistem kawalan tenaga di Amerika Syarikat, seperti sistem Kawalan Peyeliaan dan Perolehan Data (SCADA) yang semakin banyak digunakan secara online serta mempunyai akses kawalan jauh.

Keadaan ini menebabkan sistem tersebut boleh dipergunakan untuk serangan siber oleh mereka yanhg berniat jahat. Pihak Biro Penyiasatan Persekutuan (FBI) dan Jabatan Keselamatan Dalam Negeri Amerika Syarikat berkata bahawa gangguan tersebut berlaku disebabkan kejadian semulajadi dan bukanlah satu hasil keganasan.

Bagaimanapun, salah satu daripada unit Kumpulan Al-Qaeda, Briged Abu Fahes Al Masri telah mengaku bertanggungjawab melakukan gangguan tersebut, menurut satu kenyataan yang dilaporkan oleh sebuah akhbar Arab, *Dar Al Hayat*.

SERANGAN PRASARANA: KAJIAN KES DI MALAYSIA

Kod Merah *('Code Red')*
Pada bulan Jun hingga November 2001, masyarakat dunia termasuk di Malaysia telah terperangkap dengan serangan prasarana terbesar dalam sejarah Internet.

Cecacing Kod Merah memulakan serangan Penafian Perkhidmatan (DOS) dan akhirnya menghentikan semua aktiviti Internet. Varian Kod Merah ialah Code Red II, memasang laluan belakang ke dalam sistem yang dijangkiti. Keadan ini membolehkan sistem yang dijangkiti Kod Merah II dieksploitasi melalui akses kawalan jauh, seterusnya mengancam sistem tersebut.

Perangkaan Pasukan Tindakbalas Kecemasan Komputer Malaysia (MyCERT) menunjukkan bahawa cecacing ini telah menjangkiti 45,633 komputer pada bulan Ogos 2001, 27,705 komputer pada bulan September 2001 dan 195 komputer pada bulan Oktober 2001.

Nimda
Nimda adalah cecacing pertama yang mengubah dokumen web yang sedia ada dan beberapa fail boleh-lancar yang didapati di dalam sistem yang dijangkitinya. Salah satu keupayaan Nimda ialah menyerang komputer yang telah diancam oleh cecacing Kod Merah.
Perangkaan MyCERT menunjukkan Cecacing Nimda menjangkiti 9713 komputer pada bulan September 2001, 7654 komputer pada Oktober 2001 dan 462 komputer pada November 2001. Kos membaiki dijangka sebanyak RM22 juta dan jumlah ini tidak termasuk kos kehilangan peluang perniagaan.

Blaster
Blaster (dikenali juga sebagai 'Lovsan' dan 'Posa') adalah salah satu cecacing terkini yang telah menjangkiti komputer di seluruh dunia baru-baru ini. Cecacing ini ditemui pada hari Isnin, 11 Ogos 2003. Blaster mengeksploitasi kelemahan dalam perisian Windows NT, 2000 dan XP.

Menurut Pusat Koordinasi CERT di Universiti Carnegie Mellon, Amerika Syarikat, berkemungkinan sebanyak 1.4 juta komputer telah dijangkiti. Di Malaysia, MyCERT telah menganggarkan kira-kira 500 komputer telah dijangkiti dengan cecacing ini.

Nachi
Cecacing baru Nachi (dikenali juga sebagai 'Welchia' dan 'Blaster.D') telah menular dalam Internet sejak 19 Ogos 2003. Sambil membersihkan komputer yang dijangkiti Blaster, Nachi mencipta masalah baru dalam rangkaian komputer dengan mengimbas kelemahan sistem lain, yang mengakibatkan peningkatan kesesakan rangkaian. Adalah dilaporkan bahawa cecacing baru ini menyebabkan masalah rangkaian komputer kepada banyak organisasi di Malaysia. Anggaran kos untuk membasmi cecacing ini ialah sebanyak RM31 juta, dan ini tidak termasuk kos peluang dan produktiviti.

PENGAJARAN DARI KAJIAN KES

- **Memerlukan Kerjasama di Pelbagai Peringkat**

Kita tidak boleh menyelesaikan setiap serangan siber satu per satu secara individu tanpa mengutarakan kesan yang lebih besar. Untuk menangani ancaman siber secara berkesan, pendekatan yang terbaik adalah dengan mewujudkan penyelarasan, kerjasama serta komunikasi secara mendatar di antara semua agensi berkaitan. Semua pihak menghadapi ancaman siber yang sama dan kerjasama adalah satu aset yang amat penting. Cabaran utama ialah untuk bertindakbalas dengan pantas.

- **Memerlukan Kesungguhan dan Penyelarasan Yang Formal**

Kemusnahan dapat dihentikan dengan segera jika penyebaran maklumat dapat dilakukan dengan pantas. Kebanyakan organisasi lewat bertindakbalas atau tidak berupaya untuk bertindakbalas terhadap serangan siber kerana mereka tidak mempunyai maklumat yang tepat. Keadaan ini boleh dielakkan sekiranya terdapt hubungan yang formal di antara semua agensi terlibat.

- **Memerlukan Keseragaman Dalam Memahami Tahap Ancaman**

Kefahaman lazim mengenai tahap ancaman boleh dicapai dengan berkongsi maklumat menerusi persediaan katalog kelemahan, analisis impak dan sebagainya. Tahap ancaman perlu dikenalpasti secara terperinci supaya semua pihak mempunyai kefahaman yang sama. Jika tidak, perbezaan pendapat dan tafsiran akan timbul.

KESIMPULAN

Prasarana yang digunakan untuk menyalurkan maklumat turut sama memberikan peluang baru kepada para penjenayah, pengganas dan negara luar yang berniat jahat; yang berkemungkinan menjalankan kegiatan perisikan industri, menyebabkan prasarana kritikal tidaki operasi, atau melancarkan Peperangan Maklumat. Persoalannya bukanlah “adakah saya akan diserang?” sebaliknya “bilakah saya akan diserang?”. Serangan siber secara tersusun berkemingkinan besar akan berlaku adalah tidak diragukan. Oleh itu kita hendaklah berwaspada dan bersiapsiaga untuk menghadapi apa jua keadaan yang mendatang.