Cybercrime

Hari Murti
Fakultas Teknologi Informasi, Universitas Stikubank Semarang
e-mail : harimurti@unisbank.ac.id

ABSTRAK: Cybercrime / kejahatan dunia maya adalah istilah umum untuk menggambarkan tindakan yang dilakukan oleh seseorang atau sekelompok orang yang ahli dalam bidang komputer / informatika merugikan orang atau sekelompok orang yang lain. Tindakan yang digolongkan terhadap cybercrime / kejahatan dunia maya adalah DoS, Hacking, menyebarkan / membuat virus, pencurian identitas dan lainnya. Dimana tindakan-tindakan tersebut memiliki pengaruh kerugian dan cara yang berbeda-beda bila seseorang ataupun sekelompok orang mengalami hal tersebut. Dan tindakan tersebut pada beberapa negara telah dapat diberikan hukumannya karena telah ada perundang-undangan yang mengatur mengenai cybercrime.

Kata kunci : cybercrime, dos, hacking, fraud, carding

PENDAHULUAN

Saat mendengar kata cybercrime, bisa jadi dalam pikiran kita terbayang sebuah tindak kejahatan yang menggunakan alat-alat yang canggih dimana si pelaku kejahatan adalah seseorang atau sekelompok orang yang ahli dalam bidang komputer atau informatika yang memanfaatkan keahliannya untuk hal-hal yang buruk yang merugikan banyak orang. Bayangan ini biasanya didapat dari film-film Hollywood yang cukup populer di seluruh dunia, yang menampilkan kecanggihan teknologi yang digunakan dan kecerdikan si pelaku.

Apakah memang seperti itukah cybercrime ? Atau yang terjadi adalah sebaliknya ? Dimana pelaku kejahatan adalah seseorang yang normal / biasa, tidak begitu ahli dalam bidang komputer / informatika tetapi dapat memanfaatkan kelemahan-kelemahan yang muncul atau timbul karena kesalahan dari pembuat keputusan untuk memanfaatkan teknologi informasi dalam organisasinya ?

Untuk lebih jelasnya, ada baiknya memahami terlebih dahulu pengertian dari cybercrime yang sebetulnya. Cybercrime adalah sebuah istilah yang digunakan secara luas untuk menggambarkan tindakan kejahatan yang menggunakan media komputer ataupun internet. Dan tindakan-tindakan kejahatan tersebut pada beberapa negara di dunia dapat dikenai hukuman, sedangkan di negara-negara lainnya masih terjadi perdebatan tentang bagaimana bentuk dan status hukumnya. (http://en.wikipedia.org/wiki/Cybercrime) Dari pengertian tersebut, dapat diambil kesimpulan bahwa cybercrime adalah sebuah tindakan yang memanfaatkan komputer atau internet sebagai alat bantu ataupun sebagai sasaran kejahatan.

Kemudian tindakan-tindakan apa saja yang termasuk dalam cybercrime ? Jika pengertian mengenai cybercrime seperti pada alinea diatas.

Tindakan yang dapat digolongkan menjadi tindakan kejahatan dunia maya / cybercrime adalah :

1. Melakukan Denial of Service Attack / DoS Attack
2. Hacking
3. Menulis dan menyebarluaskan virus / trojan
4. Cyberterrorism
5. Information warefare / Perang Informasi
6. Cyberstalking dan online harassment

7. Fraud dan Pencurian Identitas / phising (termasuk carding dan spoofing)

Berikut ini adalah penjelasan secara singkat untuk masing-masing tindakan yang dapat digolongkan menjadi tindakan cybercrime.

Denial of Service Attack / DoS Attack

Adalah sebuah serangan ke sebuah sistem komputer atau jaringan yang menyebabkan jaringan atau sistem tersebut tidak lagi dapat memberikan pelayanan (email, web, ftp, dns, dll) kepada user. Umumnya DoS dilakukan dengan cara menghabiskan bandwith yang tersedia di jaringan atau dengan memberikan permintaan palsu kepada sistem secara bertubi-tubi sehingga sistem akan mengalami overloading.

Untuk melakukan DoS dapat dengan berbagai macam cara, tetapi secara garis besar dapat digolongkan menjadi 3 bagian, yaitu :

1. Menghabiskan sumber daya komputer/jaringan, seperti bandwith, disk space atau CPU time
2. Mengacaukan informasi konfigurasi jaringan seperti informasi routing
3. Mengacaukan secara fisik / hardware pada komponen jaringan

Hacking

Hacker adalah istilah yang digunakan untuk menggambarkan beberapa tipe kepandaian dalam komputer. Pada media massa dan anggapan orang banyak yang dipicu oleh tulisan-tulisan di media massa, istilah *hacker* sering diartikan sebagai kriminal komputer. Tetapi sesungguhnya yang terjadi adalah hacker berarti seorang programer yang pintar / cerdik dalam bidang pemrograman yang tidak ada kaitannya dengan bidang keamanan komputer. *Hacker* dapat juga berarti sebagai penghargaan kepada orang-orang yang memiliki kemampuan dan pengetahuan yang lebih dari rata-rata orang biasa di berbagai bidang komputer.

Hacking dapat diartikan sebagai tindakan dari seorang hacker yang sedang mencari kelemahan dari sebuah sistem komputer. Dimana hasilnya dapat berupa program kecil yang dapat digunakan untuk masuk ke dalam sistem komputer ataupun memanfaatkan sistem tersebut untuk suatu tujuan tertentu tanpa harus memiliki *user account*. Seorang *hacker* yang baik, jika menemukan hal-hal seperti itu akan memberitahu sistem administrator, bahwa sistem komputer yang dimasukinya telah terdapat kelemahan yang mungkin berbahaya bagi sistem komputer tersebut. Jika hasil dari hacking ini dimanfaatkan oleh orang yang tidak baik, maka tindakan tersebut digolongkan ke dalam cybercrime.

Menulis dan menyebarluaskan Virus / Trojan

Virus komputer adalah program komputer yang dapat menduplikasi diri dan penyebarannya dengan cara menginfeksi file program binari ataupun file dokumen. Dan jika file program binari ataupun file dokumen yang sudah mengandung virus dibuka atau dieksekusi, maka secara otomatis virus akan aktif di komputer yang membuka atau menjalankan program tersebut.

Untuk membuat viruspun sekarang sudah mudah, sebab sudah ada program-program yang dibuat dengan tujuan menghasilkan virus. Sebagai contoh adalah VBS Worm Generator, yang berarti seseorang tidak lagi harus bersusah-susah belajar pemrograman untuk membuat virus karena sudah tinggal menggunakan program yang menghasilkan virus.

Trojan adalah sebuah program yang seolah-olah merupakan program yang baik, tetapi memiliki kode-kode program yang berbahaya. Dan jika kode-kode program tersebut dijalankan dapat menyebabkan sistem komputer mengalami kerusakan atau membuat *back door* yang dapat dimanfaatkan oleh pihak yang mengirimkan trojan tersebut. Sehingga si pengirim trojan dapat masuk ke sistem komputer dan dapat melakukan apapun yang dia suka.

Nama *Trojan* ini diambil dari legenda yunani, kuda troya, dimana pada legenda tersebut prajurit yunani yang sedang berperang dengan troya membuat patung kuda besar yang dapat dimasuki tentara yunani dan kuda tersebut ditinggal begitu saja sehingga masyarakat troya menganggap bahwa pasukan yunani sudah mundur dan kalah. Kemudian patung kuda yang besar tersebut dimasukkan ke dalam kota, tetapi

tengah malam dimana para prajurit troya sedang tidur pasukan yunani keluar dari kuda tersebut dan langsung menyerang kota troya sehingga kalah.

Cyberterrorism

Adalah kegiatan yang menggunakan jaringan komputer ataupun internet sebagai alat untuk melakukan terorisme. Dengan makin berkembangnya internet dan teknologi komputer sampai saat ini, maka perkembangan tersebut dapat dimanfaatkan untuk melancarkan aksi terorisme seperti menyebarkan virus / trojan yang berbahaya, melakukan DoS pada sistem tertentu sehingga macet, sabotase pada alat atau infrastruktur jaringan komputer dan data yang tersimpan di server tempat musuh dari teroris dan lainnya

Hal ini dapat menjadi ancaman serius jika tidak dimulai diantisipasi dari sekarang, karena dalam internet / jaringan komputer, tidaklah mudah untuk memonitor semua orang yang sedang beraktivitas di dalam jaringan tersebut.

Information warefare / Perang Informasi

Adalah perang yang menggunakan informasi sebagai salah satu target dan alat untuk melakukan penyerangan. Dalam perang informasi, dapat dilakukan penyebaran informasi / propaganda kepada musuh dimana informasi tersebut seakan-akan benar sehingga musuh percaya dan kemudian menyerah. Dimana informasi tersebut dapat berupa bantahan keadaan yang sesungguhnya sehingga menyebabkan orang-orang pengikut dari pihak musuh bingung mengenai informasi yang sebenarnya sehingga memudahkan mereka untuk diserang.

Perang informasi merupakan juga salah satu strategi untuk mengacaukan data dan sistem informasi musuh. Perang ini tidak terjadi di dunia nyata, tetapi terjadi di jaringan komputer ataupun jaringan informasi milik musuh. Perang informasi dapat menyebabkan keadaan yang berbahaya seperti salah jalur pada penerbangan ataupun kereta api sehingga menimbulkan banyak korban. Ataupun menimbulkan kekacauan pada bursa efek karena perubahan data transaksi secara drastis yang berarti ikut juga mengacaukan keadaan ekonomi dari musuh tersebut.

Cyberstalking dan Online Harassment

Stalking adalah gangguan (*harrasing*) terus menerus terhadap privasi seseorang yang dapat menyebabkan orang tersebut ketakutan dan terancam hidupnya. Gangguan ini dapat berbentuk informasi yang sifatnya pribadi dari orang yang diganggu yang dimanfaatkan untuk mendapatkan sesuatu atau karena alasan tertentu seperti sakit hati, dendam atau lainnya.

Biasanya yang menjadi sasaran tindak kejahatan ini adalah ex -suami/istri, ex-pacar, guru, dokter, selebritis, dan orang-orang yang bergerak di bidang sosial. Pada kasus-kasus yang ekstrim, stalking dapat berubah menjadi kekerasan dan bahkan dapat sampai menghilangkan nyawa seseorang atau menjadi pidana.

Fraud dan Pencurian Identitas / phising (Carding, Spoofing)

Dalam dunia komputer, *Phising* (carding, spoofing) merupakan tindakan untuk mengambil informasi berharga seperti password, nama user, nomor kartu kredit, tanggal kadaluarsa kartu kredit, alamat pemiliki dan lainnya oleh seseorang yang tidak berhak.

Salah satu cara yang sering digunakan adalah dengan menggunakan email, dimana melalui email dikirim informasi yang seolah-olah berasal dari pihak-pihak yang dapat dipercaya untuk memperoleh data-data dari target / korban. Karena, begitu korban percaya bahwa email tersebut seolah-olah berasal dari pihak yang dapat dipercaya, maka secara otomatis mereka akan memberikan data yang berharga ke pihak pengirim email. Bentuk email yang sering adalah seperti penawaran yang menggiurkan sehingga korban langsung percaya saat diminta untuk mengirimkan data yang berharga ataupun pengumuman bahwa sistem yang dipakai korban sedang kacau sehingga sang administrator membutuhkan data dari pelanggan sistem tersebut. Atau dapat juga melalui sebuah website yang namanya hampir mirip dengan web site yang sering dikunjungi oleh user sehingga orang-orang yang tidak

berkepentingan dapat dengan mudah memperoleh data berharga.

DAFTAR PUSTAKA

1. http://en.wikipedia.org/Cybercrime
2. http://www.klik-kanan.com/fokus/belajar_menjadi_hacker.shtml
3. http://www.klik-kanan.com/fokus/tutorial_cracking.shtml
4. http://www.klik-kanan.com/fokus/vbswm.shtml