Kejahatan Komputer

Pengertian Kejahatan Komputer menurut OECD yang didefinisikan dalam kerangka computer abuse yakni, ‘Any illegal, unethical or unauthorized behavior involving authomatic data processing and/or transmissing of data’, terjemahan bebasnya adalah sebagai berikut ‘Setiap perilaku yang melanggar /melawan hukum, etika atau tanpa kewenangan yang menyangkut pemrosesan data dan/atau pengiriman data’

Computer abuse merupakan tindakan sengaja dengan melibatkan komputer dimana satu pelaku kejahatan atau lebih dapat memperoleh keuntungan atau korban (satu atau lebih) dapat menderita kerugian. Computer crime merupakan tindakan melanggar hukum di mana pengetahuan tentang komputer sangat penting agar pelaksanaannya berjalan dengan baik.

Computer related crime adalah kejahatan yang berkaitan dengan komputer tidak terbatas pada kejahatan bisnis, kerah putih atau ekonomi. Kejahatan itu mencakup kejahatan yang menghancurkan komputer atau isinya atau membahayakan kehidupan dan kesejahteraan manusia karena semua tergantung apakah komputer dapat bekerja dengan benar atau tidak.

Pengaruh Komputer Pada Masyarakat

Aplikasi sosial dari komputer termasuk menggunakan komputer dalam memecahkan masalah sosial seperti masalah kejahatan. Dampak sosial ekonomi dari komputer memberikan pengaruh dari masyarakat termasuk dari penggunakan komputer. Contoh komputerisasi proses produksi memiliki dampak negatif seperti berkurangnya lahan kerja bagi manusia. Hal ini disebabkan karena pekerjaan yang biasa dilakukan oleh manusia sekarang dilakukan oleh komputer. Dampak positifnya yaitu konsumen diuntungkan dengan hasil produk yang berkualitas dan memiliki harga yang lebih murah.

Aplikasi komputer didalam masyarakat

Komputer memiliki banyak dampak yang menguntungkan dalam masyarakat ketika digunakan untuk menyelesaikan masalah kemanusiaan dan sosial. Aplikasi sosial yang dapat digunakan dalam komputer seperti diagnosa kedokteran, CAT, rencana program pemerintahan, kontrol kualitas dan pelaksanaan undang-undang. Komputer bisa

digunakan untuk mengontrol kejahatan melalui bermacam-macam pelaksanaan undang-undang atau hokum yang mengizinkan penegak hokum untuk mengidentifikasi dan bertindak cepatuntuk bukti dari kejahatan. Komputer juga digunakan untuk memantau tingkat polusi udara dan air.

Contoh – contoh kejahatan computer :

1. Pencurian uang
2. Virus computer
3. Layanan pencurian
4. Pencurian data dalam program
5. Memperbanyak program
6. Mengubah data
7. Pengrusakan program
8. Pengrusakan data

Metode Kejahatan Komputer :

Banyak metode yang digunakan untuk melakukan kejahatan komputer. Metode-metode itu antara lain penipuan data, trojan horse, teknik salami, logic bomb dan kebocoran data. Penipuan data merupakan metode yang paling sederhana, aman dan lazim digunakan. Metode ini menyangkut pengubahan data sebelum atau selama proses pemasukan ke komputer.

Jenis Kejahatan Komputer :

- **Hacker**

Hacker adalah sebutan untuk orang atau sekelompok orang yang memberikan sumbangan bermanfaat untuk dunia jaringan dan sistem operasi, membuat program bantuan untuk dunia jaringan dan komputer.Hacker juga bisa di kategorikan perkerjaan yang dilakukan untuk mencari kelemahan suatu system dan memberikan ide atau pendapat yang bisa memperbaiki kelemahan system yang di temukannya.

Hirarki / Tingkatan Hacker

Ternyata Hacker juga mempunyai tingkatan-tingkatan, tiap tingkatan di bedakan dengan kemampuan dan ilmu yang dimiliki sang hacker :

1.Elite

Ciri-ciri : mengerti sistem operasi luar dalam, sanggup mengkonfigurasi & menyambungkan jaringan secara global, melakukan pemrograman setiap harinya, effisien & trampil, menggunakan pengetahuannya dengan tepat, tidak menghancurkan data-data, dan selalu mengikuti peraturan yang ada. Tingkat Elite ini sering disebut sebagai ‘suhu’.

2.Semi Elite

Ciri-ciri : lebih muda dari golongan elite, mempunyai kemampuan & pengetahuan luas tentang komputer, mengerti tentang sistem operasi (termasuk lubangnya), kemampuan programnya cukup untuk mengubah program eksploit.

3.Developed Kiddie

Ciri-ciri : umurnya masih muda (ABG) & masih sekolah, mereka membaca tentang metoda hacking & caranya di berbagai kesempatan, mencoba berbagai sistem sampai akhirnya berhasil & memproklamirkan kemenangan ke lainnya, umumnya masih menggunakan Grafik User Interface (GUI) & baru belajar basic dari UNIX tanpa mampu menemukan lubang kelemahan baru di sistem operasi.

4.Script Kiddie

Ciri-ciri : seperti developed kiddie dan juga seperti Lamers, mereka hanya mempunyai pengetahuan teknis networking yang sangat minimal, tidak lepas dari GUI, hacking dilakukan menggunakan trojan untuk menakuti & menyusahkan hidup sebagian pengguna Internet.

5.Lammer

Ciri-ciri : tidak mempunyai pengalaman & pengetahuan tapi ingin menjadi hacker sehingga lamer sering disebut sebagai ‘wanna-be’ hacker, penggunaan komputer mereka terutama untuk main game, IRC, tukar menukar software prirate, mencuri kartu kredit, melakukan hacking dengan menggunakan software trojan, nuke & DoS, suka menyombongkan diri melalui IRC channel, dan sebagainya.

- **Cracker**

Cracker adalah sebutan untuk orang yang mencari kelemahan system dan memasukinya untuk kepentingan pribadi dan mencari keuntungan dari system yang di masuki seperti: pencurian data, penghapusan, dan banyak yang lainnya.

Bagaimana cara cracker merusak ? Seorang cracker dapat melakukan penetrasi ke dalam sistem dan melakukan pengrusakan. Ada banyak cara yang biasanya digunakan untuk melakukan penetrasi antara lain : IP Spoofing (Pemalsuan alamat IP), FTP Attack dll. Pada umumnya, cara-cara tersebut bertujuan untuk membuat server dalam sebuah sistem menjadi sangat sibuk dan bekerja di atas batas kemampuannya sehingga sistem akan menjadi lemah dan mudah dicrack.

Dampak Aktifitas Cracker Terhadap e-Commerce

Perilaku cracker tersebut akan berdampak negatif bagi perkembangan e-commerce. Di satu sisi para pemiliki komoditi akan enggan mengaplikasikan e-commerce karena kuatir menjadi sasaran untuk dilumpuhkan, diganti tampilan situsnya atau data pelanggannya dicuri. Sedangkan bagi para konsumen akan dibayangi oleh ketakutan bahwa data pribadi mereka, termasuk nomor kartu kredit, akan dapat dibajak oleh cracker.

Pada survei yang dilakukan oleh America’s Federal Trade Commision (AFTC) seperti dikutip oleh majalah The Economist (edisi Mei 1999), 80 persen warga Amerika mencemaskan kemungkinan tersebarnya data pribadi dirinya di Internet. Sedangkan menurut survei yang dilakukan oleh PC Data Online pada tanggal 15 Februari 2000, dengan maraknya kasus kejahatan di Internet, 54 persen responden menyatakan bahwa dirinya akan mengubah kebiasaan kebiasaannya di Internet. 80 persen dari yang akan berubah tersebut menyatakan akan semakin jarang mengirim informasi kartu kredit melalui Internet.

Perbedaan Terminologi Hacker dan Cracker

Secara lebih spesifik hacker didefinisikan sebagai seseorang yang memiliki keinginan untuk melakukan eksplorasi dan penetrasi terhadap sebuah sistem operasi dan kode komputer pengaman lainnya, tetapi tidak melakukan tindakan pengrusakan apapun, tidak mencuri uang atau informasi. Sedangkan cracker adalah sisi gelap dari hacker dan

memiliki kertertarikan untuk mencuri informasi, melakukan berbagai macam kerusakan dan sesekali waktu juga melumpuhkan keseluruhan sistem komputer.

Perbedaan terminologi antar hacker dan cracker terkadang menjadi bias dan hilang sama sekali dalam perspektif media massa dan di masyarakat umum. Para cracker juga tidak jarang menyebut diri mereka sebagai hacker sehingga menyebabkan citra hacking menjadi buruk. (Richard Mansfield, Hacker Attack, 2000).

Tindakan penyusupan ke dalam suatu sistem komputer yang dilakukan oleh cracker tersebut dalam upaya mencuri data kartu kredit hingga mengganti tampilan suatu situs di Internet, disebut dengan istilah cracking. Hal tersebut menegaskan bahwa terminologi hacking sebenarnya adalah perilaku atau tindakan menerobos masuk sebuah sistem secara elektronis. Tidak lebih dari sekedar untuk mendapatkan akses sebuah sistem komputer dan membaca beberapa file di dalam sistem komputer tersebut, tanpa diikuti tindakan pencurian atau pengrusakan apapun.

Beberapa contoh tindakan cracker yang dianggap merugikan pengguna Internet lainnya antara lain adalah dilumpuhkannya beberapa saat situs Yahoo.com, eBay.com, Amazon.com, Buy.com, ZDNet.com, CNN.com, eTrade.com dam MSN.com karena serangan bertubi-tubi dari cracker dengan teknik Distributed Denial of Service (DDoS). Serangan yang dilancarkan pada bulan Februari 2000 tersebut sempat melambatkan trafik Internet dunia sebesar 26 persen.

- **Spammer**

Spammer adalah orang yang melakukan pengiriman informasi yang tidak pada tempatnya atau melanggar aturan hukum yang berlaku. Bukan hanya email. Kalau kita memposting pesan ke milis tapi tidak sesuai dengan topik pembicaraan, atau memposting iklan di situs iklan baris yang berulang-ulang dan tidak pada kategori yang benar, itu juga termasuk spam.

- **Virus komputer**

Virus komputer adalah sebuah program kecil yang bisa menggandakan dirinya sendiri dalam media penyimpanan suatu komputer. Formalnya adalah sebagai berikut: “A program that can infect other programs by modifying them to include a slighty altered

copy of itself. A virus can spread throughout a computer sistem or network using the authorization of every user using it to infect their programs. Every programs that gets infected can also act as a virus that infection grows (Fred Cohen).

Virus juga mampu, baik secara langsung ataupun tak langsung, menginfeksi, mengkopi maupun menyebarkan program file yang bisa dieksekusi maupun program yang ada di sektor dalam sebuah media penyimpanan (Hardisk, Disket, CD-R). Virus juga bisa menginfeksi file yang tidak bisa dieksekusi (file data) dengan menggunakan macros (program sederhana yang biasanya digunakan untuk melakukan suatu perintah). Intinya adalah kemampuan untuk menempel dan menulari suatu program.

Virus bukanlah sesuatu yang terjadi karena kecelakaan ataupun kelemahan perangkat komputer karena pada hakikatnya, semua virus merupakan hasil rancangan intelegensi manusia setelah melalui beberapa percobaan terlebih dahulu layaknya eksperimen-eksperimen ilmiah di dalam bidang-bidang lainnya.

Virus komputer, merupakan salah satu script code yang dapat mendatangkan kerugian bagi pihak yang perangkat teknologinya dijangkiti oleh virus ini. Sebagaimana virus dalam dunia kesehatan, virus ini pun seolah-olah mempunyai pengembangan biologis dengan cara meng-copy sendiri file yang dapat memperlambat kinerja komputer dalam memproses data atau informasi didalamnya, sehingga menimbulkan crash pada komputer tersebut dan beresiko kehilangan data yang telah dan sedang diproses.

- **Worm**

Sumber malapetaka lain yang mirip dengan virus, namun tidak bisa dikategorikan sebagai virus, adalah worm. Worm adalah program yang dapat menduplikasi diri tanpa menginfeksi program-program lainnya. Worm tidak memerlukan carrier, dalam hal ini program atau suatu dokumen. Worm biasa menyebar melalui pertukaran data antar hardisk, disket, maupun e-mail. Penyebaran melalui e-mail biasanya berupa sebuah attachment yang kecil. Pengguna yang tertarik akan menjalankan program tersebut. Selanjutnya, tanpa basa-basi, si program akan langsung melakukan aksinya. Worm akan menggandakan diri dengan mengirimkan file-nya secara otomatis melalui attachment ke setiap alamat yang ada dalam address book pada mail manager korban.

Umumnya worm tidak bersifat merusak, namun demikian selain mengakibatkan kejengkelan di pihak korban, serangan worm dapat sangat berbahaya bagi mailserver. Berjangkitnya worm menyebabkan beban kerja mailserver melonjak drastis hingga dapat mempengaruhi performanya. Dan tidak hanya untuk mailserver, bahkan komputer pribadi kita pun bisa dijadikan sasarannya. Hal ini terjadi karena worm mampu menduplikasikan dirinya sendiri di dalam memori komputer dalam jumlah yang sangat banyak. Sekarang bayangkan jika worm menduplikasi dirinya secara serentak, 'bakal lemot deh komputer'.
Worm umumnya berbentuk file executable (berekstensi .EXE datau .SCR), yang terlampir (attach) pada e-mail. Namun demikian, ada beberapa jenis worm yang berbentuk script yang ditulis dalam bahasa Visual Basic (VBScript). Sasaran serangan worm jenis ini terutama adalah perangkat lunak e-mail Microsoft Outlook Express, tapi bukan berarti aplikasi yang lain sudah pasti kebal dengan semua jenis worm.

- **Spyware**

Spyware adalah suatu aplikasi yang memungkinkan para pemasang iklan untuk mendapatkan informasi mengenai kebiasaan pengguna computer dimana spyware tersebut terpasang. Progam spyware ini sebenarnya bukanlah suatu virus. Anda tidak dapat menyebarkannya ke komputer yang lain. Tetapi spyware terkadang memiliki efek-efek lain yang tidak terduga.Anda bisa saja mendapatkan spyware ketika Anda mengakses suatu situs tertentu. Suatu pesan pop-up biasanya akan muncul dan menyuruh Anda untuk mendownload program yang "kelihatannya" Anda butuhkan, atau terkadang program spyware ini bisa secara otomatis terdownload tanpa Anda sadari. Spyware akan jalan di komputer Anda dan akan mencatat semua aktivitas Anda (misalnya mencatat situs apa saja yang Anda kunjungi) dan akan melaporkannya kepada pihak lain, dalam hal ini pihak pemasang iklan.
Efek lainnya adalah mengganti halaman home pada web browser Anda dengan suatu alamat situs tertentu atau bahkan juga ada yang memiliki efek untuk men-dial modem ke nomor 0900 (premium call). Aktivitas spyware ini jelas akan memakan resource pada komputer Anda dan dapat memperlambat performa dari komputer Anda.

Beberapa software anti-spyware saat ini sudah dapat mendeteksi adanya spyware pada komputer Anda dan bisa menghilangkannya secara otomatis. Contohnya adalah fitur anti-spyware pada aplikasi System Mechanic.

Jenis- jenis kejahatan perbankan yang berbasis it !

1. Skimmer (menangkap data di magnetic strip)

Skimming adalah penggunaan secara fisik reader sekunder untuk menangkap magnetic di belakang kartu kredit atau kartu debet. Skimmer dan keypad sekundernya digunakan untuk menangkap nomor account dan PIN ATM di box ATM. Sayangnya, ketika konsumen melakukan transaksi via ATM, konsumen tidak menyadari bahwa account-nya telah disadap. Kriminalitas ATM ini dimulai dengan menangkap nomor account ATM di slot ATM card pada umumnya, dan kemudian skimmer akan merekam informasi account dari ATM card.

2. Sniffer (menangkap paket data yang lalu lalang di jaringan komunikasi)

Sniffer adalah suatu aplikasi penyerang untuk melakukan pencurian ataupun penyadapan data. Data yang dimaksud tidak akan hilang secara fisik, namun akan disadap. Penyadapan ini sangat berbahaya, karena biasanya yang menjadi sasaran penyadapan ini adalah data-data penting seperti data pribadi (username, password, nomor authorisasi, dst). Hal ini dapat dicegah dengan cara terlebih dahulu melakukan enkripsi data sebelum data dikirimkan ke jaringan atau Internet, misalkan dengan menggunakan ssh atau secure shell yang berfungsi mengenkripsikan data dengan cara enkripsi 128 bit.

3. Keylogger (menangkap apa yang diketikkan di keyboard komputer)

Keylogger adalah suatu aplikasi atau software yang dapat mengunci tombol keyboard dengan menggunakan program logger tertentu. Sehingga, apapun yang diketikkan oleh user di layar monitor, dapat terekam. Artinya, meskipun saat mengetikkan password di kotak password yang tampil di monitor hanyalah ‘*****’ misalnya, namun isi password tersebut dapat terekam dan otomatis dapat terbaca. Hasil rekaman ini akan langsung tersimpan pada komputer dan dikirimkan melalui internet kepada si pencuri data tersebut. Bisa lewat e-mail, irc atau bahkan bisa diamati langsung secara realtime melalui web

4. Phishing (personal information fishing, dengan situs abal-abal, social engineering)

Phising , adalah tindakan memperoleh informasi pribadi seperti User ID, PIN, nomor rekening bank, nomor kartu kredit Anda secara tidak sah. Informasi ini kemudian akan dimanfaatkan oleh pihak penipu untuk mengakses rekening, melakukan penipuan kartu kredit atau memandu nasabah untuk melakukan transfer ke rekening tertentu dengan iming-iming hadiah.

Bagaimana phishing dilakukan?

Teknik umum yang sering digunakan oleh penipu adalah sebagai berikut:

Penggunaan alamat e-mail palsu dan grafik untuk menyesatkan Nasabah sehingga Nasabah terpancing menerima keabsahan e-mail atau web sites. Agar tampak meyakinkan, pelaku juga seringkali memanfaatkan logo atau merk dagang milik lembaga resmi, seperti; bank atau penerbit kartu kredit. Pemalsuan ini dilakukan untuk memancing korban menyerahkan data pribadi, seperti; password, PIN dan nomor kartu kredit

Membuat situs palsu yang sama persis dengan situs resmi.atau . pelaku phishing mengirimkan e-mail yang berisikan link ke situs palsu tersebut.

Membuat hyperlink ke web-site palsu atau menyediakan form isian yang ditempelkan pada e-mail yang dikirim.

5. Typo Site

Modus kejahatan typo site ini terbilang cukup unik dan seringkali tidak disadari oleh korbannya. Caranya, pelaku membuat situs yang memiliki nama yang hampir serupa dengan situs resmi lainnya. Misalnya saja, sebuah situs resmi yang memiliki alamat di http://anakku.com/ dibuat samarannya dengan alamat http://anaku.com/. Nyaris tak bisa dibedakan bukan?

Typo site dapat dengan mudah dibuat untuk domain .COM, .NET, .ORG, dan beberapa jenis domain lainnya. Setiap orang bisa menamakan situsnya tersebut dengan nama apa saja selama domain itu belum dimiliki orang lain. Dan kemudian si pembeli nama-nama domain yang mirip itu dapat membuat tampilan situsnya 100% mirip aslinya, sehingga seringkali orang yang salah ketik tidak menyadari bahwa ia sebenarnya berada di situs yang salah. Biasanya yang sering disalahgunakan adalah situs-situs dari bank resmi. Tujuannya tak lain adalah untuk menangkap user ID, password atau data-data pribadi lainnya. Data-data tersebut kemudian dimanfaatkan untuk melakukan transaksi illegal.