BAB XI

KEJAHATAN KOMPUTER

&

KEAMANAN KOMPUTER

KEJAHATAN KOMPUTER

David I. Bainbridge dalam bukunya Komputer dan Hukum membagi beberapa macam kejahatan dengan menggunakan sarana computer :

- **Memasukkan instruksi yang tidak sah,** yaitu seseorang memasukkan instruksi secara tidak sah sehingga menyebabkan sistem komputer melakukan transfer uang dari satu rekening ke rekening lain, tindakan ini dapat dilakukan oleh orang dalam atau dari luar bank yang berhasil memperoleh akses kepada sistem komputer tanpa ijin.
- **Perubahan data input,** yaitu data yang secara sah dimasukkan kedalam komputer dengan sengaja diubah. Cara ini adalah suatu hal yang paling lazim digunakan karena mudah dilakukan dan sulit dilacak kecuali dengan pemeriksaan berkala.

- **Perusakan data,** hal ini terjadi terutama pada data output, misalnya laporan dalam bentuk hasil cetak komputer dirobek, tidak dicetak atau hasilnya diubah.
- **Komputer sebagai pembantu kejahatan,** misalnya seseorang dengan menggunakan komputer menelusuri rekening seseorang yang tidak aktif, kemudian melakukan penarikan dana dari rekening tersebut.
- **Akses tidak sah terhadap sistem komputer atau yang dikenal dengan hacking.** Tindakan hacking ini berkaitan dengan ketentuan rahasia bank, karena seseorang memiliki akses yang tidak sah terhadap sistem komputer bank, sudah tentu mengetahui catatan tentang keadaan keuangan nasabah dan hal-hal lain yang harus dirahasiakan menurut kelajiman dunia perbankan.

Klasifikasi Kejahatan Komputer

- Fraud by computer manipulation
- Computer espionage and software theft
- Computer sabotage
- Theft or service
- Unauthorized access to data processing system
- Traditional business offences assisted by data processing.

Pembatasan

- Kejahatan yang memanfaatkan kemampuan komputer dalam memproses data dan kemudian memanipulasi data tersebut dengan akibat timbulnya kerugian bagi pihak lain
- Kejahatan yang dilakukan dengan cara memasuki system komputer orang lain, baik komputer pribadi ataupun komputer yang terhubung ke dalam satu jaringan komputer tanpa ijin.

Contoh Kejahatan

- Memasuki jaringan komputer orang lain tanpa ijin, misalnya melalui internet (hacking)
- Menyadap transmisi data orang lain, misalnya surat elektronik (e-mail).
- Memanipulasi data seseorang, misalnya kartu kredit seseorang dan kemudian menggunakan informasi kartu kredit tersebut untuk berbelanja di internet.
- Memanipulasi data dengan cara menyiapkan perintah yang tidak dikehendaki kedalam program komputer.
- Memalsukan surat dengan cara mendesain surat palsu menggunakan perangkat komputer. Mengubah data yang tersimpan dalam komputer.

Program Perusak / Pengganggu

- Virus
- Malware
- Botnet
- DoS Attack
- Back Doors
- Spoofing

Metode untuk melakukan kejahatan komputer

- **Penipuan data** → merupakan metode yang paling sederhan, aman dan lazim digunakan. Metode ini menyangkut pengubahan data sebelum atau selama proses pemasukan ke komputer. Perubahan ini dapat dilakukan oleh seseorang yang berkepentingan atau memiliki akses ke proses komputer. Kasus yang pernah terungkap yang menggunakan metode ini adalah pada salah satu perusahaan kereta api di Amerika. Petugas pencatat gaji menginput waktu lembur pegawai lain dengan menggunakan nomer karyawannya. Akibatnya penghsialannya meningkat ribuan dollar dalam setahun.
- **Trojan horse** → merupakan penempatan kode program secara tersembunyi pada suat program komputer. Metode ini paling lazim digunakan untuk sabotase. Trojan horse yang terkenal yaitu program machintosh yang disebut sexy lady. Program ini pada layar komputer menampilkan gambar-gambar erotis. Sepertinya tidak berbahaya, namun pada kenyataannya program tersebut merusak data pada komputer. Serupa dengan Trojan horse adalah program virus.

- **Teknik solami →** merupakan metode pengambilan sebagain kecil tanpa terlihat secara keseluruhan. Sebagai contoh adalah sistem tabungan di bank untuk mengurangi secara acak beberapa ratus rekening sejumlah 25 rupiah kemudian mentransfernya secara sah melalui metode normal. Biasanya metode ini diterapkan untuk perhitungan bunga dengan cara pembulatan ke bawah. Misalnya nilai bunga 175 rupiah akan dicatat 150 rupiah. Selisih 25 rupiah inilah yang akan ditransfer kerekening tertentu. Kecil memang tetapi bila jumlah rekaningnya banyak dan dilakukan beberapa tahun maka nilainya akan besar.

- **Logic bomb** → merupakan program komputer untuk diaktifkan pada waktu tertentu. Logic bomb merupakan metode tertua yang digunakan untuk tujuan sabotase. Contoh kasus logic bomb ini adalah seperti yang dilakukan oleh Donald Burleson seorang programmer perusahaan asuransi di Amerika. Ia dipecat karena melakukan tindakan menyimpang. Dua hari kemudian sebuah logic bomb bekerja secara otomatis mengakibatkan kria-kira 160.000 catatan penting yang terdapat pada komputer perusahaan terhapus.
- **Kebocoran data** → merupakan metode pencurian atau pengambilan data secara tidak sah. Teknik yang digunakan mulai dari yang sederhana seperti mengambil data dengan media penyimpanan atau dengan teknik khusus seperti mencari kelemahan dalam sistem keamanan komputer baru mengambil data yang diperukan.

Sifat ancaman terhadap sistem informasi dapat berupa:

- **Ancaman Pasif** : ancaman ini biasanya disebabkan oleh bencana alam dan politik, contohnya : gempa bumi, banjir, perang dan lain-lain. Kesalahan manusia seperti, kesalahan memasukan atau menghapus data, dan kegagalan sistem seperti gangguan listrik.
- **Ancaman Aktif** : ancaman ini disebabkan oleh kecurangan dan kejahatan komputer, seperti: penyelewengan aktivitas, penyalahgunaan kartu kredit, sabotase, pengaksesan oleh orang yang tidak berhak. Selain itu juga karena program yang jahat/usil seperti, virus, worm, Trojan dan lainnya.

KEAMANAN KOMPUTER

Aspek Keamanan

Menurut dari Simson Garfinkel *"PGP : Pretty Good Privacy"*, O'Reilly & Associ-ates, Inc, 1995 bahwa keamanan komputer dapat dibedakan menjadi, antara lain :

- ✓ **Confidentiality (Kerahasiaan)**
- ✓ **Integrity**
- ✓ **Availability**
- ✓ **Non-repudiation**
- ✓ **Authentication**
- ✓ **Access Control**

Menurut David Icove, berdasarkan lubang keamanan, keamanan dapat diklasifikasikan menjadi empat :

- **Keamanan yang bersifat fisik (physical security)** : termasuk akses ke gedung, peralatan, dan media yang digunakan.
- **Keamanan yang berhubungan dengan orang (personel)**: termasuk identifikasi, dan profil resiko dari orang yang mempunyai akses (pekerja).
- **Keamanan dari data dan media serta teknik komunikasi**: yang termasuk dalam kelas ini adalah kelemahan dalam software yang digunakan untuk mengolah data.
- **Keamanan dalam operasi**, termasuk prosedur yang digunakan untuk mengatur dan mengelola sistem keamanan, dan juga prosedur setelah serangan.

Pentingnya Keamanan Sistem Komputer

- Untuk menghindari resiko penyusupan
- Mengurangi resiko ancaman
  - Ada beberapa macam penyusup yang bisa menyerang system yang dimiliki, antara lain :
    - **Ingin Tahu**, jenis penyusup ini pada dasarnya tertarik menemukan jenis system yang digunakan.
    - **Perusak**, jenis penyusup ini ingin merusak system yang digunakan atau mengubah tampilan layar yang dibuat.
    - **Menyusup untuk popularitas**, penyusup ini menggunakan system untuk mencapai popularitas dia sendiri, semakin tinggi system keamanan yang kita buat, semakin membuatnya penasaran. Jika dia berhasil masuk ke sistem kita maka ini menjadi sarana baginya untuk mempromosikan diri.
    - **Pesaing**, penyusup ini lebih tertarik pada data yang ada dalam system yang kita miliki, karena dia menganggap kita memiliki sesuatu yang dapat menguntungkannya secara finansial atau malah merugikannya (penyusup).

- Melindungi system dari kerentanan, kerentanan akan menjadikan system berpotensi untuk memberikan akses yang tidak diizinkan bagi orang lain yang tidak berhak
- Melindungi system dari gangguan alam seperti petir dan lain-lainnya

Terdapat 5 hirarki atau tingkatan hecker

- Elite
- Semi Elite
- Developed Kiddie
- Script Kiddie
- Lammer


THANK
YOU