KEAMANAN

Keamanan merupakan faktor penting yang perlu diperhatikan dalam pengoperasian sistem informasi. Keamanan dimaksudkan untuk mencegah ancaman dan gangguan terhadap sistem serta untuk mendeteksi dan memperbaiki akibat segala kerusakan sistem.

A. ANCAMAN TERHADAP SISTEM INFORMASI

Secara garis besar, ancaman terhadap sistem informasi terbagi dua :

1. **Ancaman Aktif**
   - Kejahatan terhadap komputer
   - Kecurangan

2. **Ancaman Pasif**
   - Kegagalan sistem
   - Kesalahan manusia
   - Bencana alam

Tabel 1. Ancaman terhadap sistem informasi

Macam Ancaman	Contoh
Bencana alam dan politik	• Gempa bumi, banjir, kebakaran, perang
Kesalahan manusia	• Kesalahan pemasukkan data • Kesalahan penghapusan data • Kesalahan operator (salah memberi label pada pita magnetik)
Kegagalan perangkat lunak dan perangkat keras	• Gangguan listrik • Kegagalan peralatan • Kegagalan fungsi perangkat lunak
Kecurangan dan kejahatan komputer	• Penyelewengan aktivitas • Penyalahgunaan kartu kredit • Sabotase • Pengaksesan oleh orang yang tidak berhak
Program yang jahat / usil	• Virus, cacing (*worm*), bom waktu, dll.

B. GANGGUAN-GANGGUAN TERHADAP SISTEM INFORMASI

Gangguan-gangguan terhadap sistem informasi dapat dilakukan secara :

1. **Tidak sengaja**
   Gangguan terhadap sistem informasi yang dilakukan secara tidak sengaja dapat terjadi karena :
   a) Kesalahan teknis (*technical errors*)
      - Kesalahan perangkat keras (*hardware problems*)
      - Kesalahan di dalam penulisan sintak perangkat lunak (*syntax errors*)
      - Kesalahan logika (*logical errors*)
   b) Gangguan lingkungan (*environmental hazards*)
      - Kegagalan arus listrik karena petir
   c) Kesalahan manusia (*human errors*)

2. **Sengaja**
   Kegiatan yang disengaja untuk menganggu sistem informasi termasuk dalam kategori :
   a) *Computer abuse* : adalah kegiatan sengaja yang merusak atau menggangu sistem informasi.
   b) *Computer crime* (*Computer fraud*) : adalah kegiatan *computer abuse* yang melanggar hukum, misalnya membobol sistem komputer.
   c) *Computer related crime* : adalah kegiatan menggunakan teknologi komputer untuk melakukan kejahatan, misalnya dengan menggunakan internet untuk membeli barang dengan menggunakan kartu kredit.

Cara Melakukan Gangguan-gangguan Sistem Informasi

Ada tiga cara untuk melakukan gangguan terhadap sistem informasi :
1. Data Tampering
2. Penyelewengan program
3. Penetrasi ke sistem informasi

➢ ***Data Tampering*** atau ***Data Diddling***
Data Tampering adalah merubah data sebelum, atau selama proses dan sesudah proses dari sistem informasi.

Data diubah sebelum diproses yaitu pada waktu data ditangkap di dokumen dasar atau pada saat diverifikasi sebelum dimasukkan ke sistem informasi.
Data diubah pada saat proses sistem informasi biasanya dilakukan pada saat dimasukkan ke dalam sistem informasi.
Data diubah setelah proses sistem informasi yaitu dengan mengganti nilai keluarannya. Data diubah dapat diganti, dihapus atau ditambah.

Kegiatan *data tampering* ini biasanya banyak dilakukan oleh orang dalam perusahaan itu sendiri.

➢ **Penyelewengan Program (*Programming Fraud*)**
Dengan cara ini, program komputer dimodifikasi untuk maksud kejahatan tertentu.

Teknik-teknik yang termasuk dalam kategori ini adalah :

- **Virus**
  Virus berupa penggalan kode yang dapat menggandakan dirinya sendiri, dengan cara menyalin kode dan menempelkan ke berkas program yang dapat dieksekusi. Selanjutnya, salinan virus ini akan menjadi aktif jika program yang terinfeksi dijalankan.

  Contoh virus jahat adalah CIH atau virus Chernobyl, yang melakukan penularan melalui e-mail.

- **Cacing (*Worm*)**
  Cacing adalah suatu program yang dapat menggandakan dirinya sendiri dengan cepat dan menulari komputer-komputer dalam jaringan.

  Contoh *worm* yang terkenal adalah yang diciptakan oleh Robert Morris pada tahun 1988. Program yang dibuatnya dapat menyusup ke jaringan yang menghubungkan Massachusets Institute of Technology, perusahaan RAND, Ames Research Center-nya NASA, dan sejumlah universitas di Amerika. *Worm* ini telah menyebar ke 6000 komputer sebelum akhirnya terdeteksi.

- ***Kuda Trojan (Trojan Horse)***
  Kuda Trojan adalah program komputer yang dirancang agar dapat digunakan untuk menyusup ke dalam sistem.

Sebagai contoh, *Trojan Horse* dapat menciptakan pemakai dengan wewenang supervisor atau superuser. Pemakai inilah yang nantinya dipakai untuk menyusup ke sistem. Contoh *Trojan Horse* yang terkenal adalah program pada Macintosh yang bernama Sexy Ladies HyperCard yang pada tahun 1988 membawa korban dengan janji menyajikan gambar-gambar erotis. Sekalipun janjinya dipenuhi, program ini juga menghapus data pada komputer-komputer yang memuatnya.

- ***Round down Technique***
  Teknik ini merupakan bagian program yang akan membulatkan nilai pecahan ke dalam nilai bulat dan mengumpulkan nilai-nilai pecahan yang dibulatkan tersebut.

  Bila diterapkan di bank misalnya, pemrogram dapat membulatkan ke bawah semua biaya bunga yang dibayarkan ke nasabah, dan memasukkan pecahan yang dibulatkan tersebut ke rekeningnya.

- ***Salami Slicing***
  Merupakan bagian program yang memotong sebagian kecil dari nilai transaksi yang besar dan menggumpulkan potongan-potongan ini dalam suatu periode tertentu.

  Misalnya suatu akuntan di suatu perusahaan di California menaikkan sedikit secara sistematik biaya-biaya produksi. Bagian-bagian yang dinaikkan ini kemudian dikumpulkan selama periode tertentu dan diambil oleh akuntan tersebut.

- ***Trapdoor***
  Adalah kemungkinan tindakan yang tak terantisipasi yang tertinggal dalam program karena ketidaksengajaan. Disebabkan sebuah program tidak terjamin bebas dari kesalahan, kesalahan yang terjadi dapat membuat pemakai yang tak berwenang dapat mengakses sistem dan melakukan hal-hal yang sebenarnya tidak boleh dan tidak dapat dilakukan.

- ***Super zapping***
  Adalah penggunaan tidak sah dari program utiliti Superzap yang dikembangkan oleh IBM untuk melewati beberapa pengendalian-pengendalian sistem yang kemudian melakukan kegiatan tidak legal.

- **Bom Logika atau Bom Waktu (*Logic bomb atau Time bomb*)**
  Bom logika atau bom waktu adalah suatu program yang beraksi karena dipicu oleh sesuatu kejadian atau setelah selang waktu berlalu.

  Program ini biasanya ditulis oleh orang dalam yang akan mengancam perusahaan atau membalas dendam kepada perusahaan karena sakit hati.

  Contoh kasus bom waktu terjadi di USPA, perusahaan asuransi di Forth Worth. Donal Burkson, seorang programmer pada perusahaan tersebut dipecat karena sesuatu hal. Dua hari kemudian, sebuah bom waktu mengaktifkan dirinya sendiri dan menghapus kira-kira 160.000 rekaman-rekaman penting pada komputer perusahaan tersebut.

➢ **Penetrasi ke Sistem Informasi**

Yang termasuk dalam cara ini adalah :

- ***Piggybacking***
  Piggybacking adalah menyadap jalur telekomunikasi dan ikut masuk ke dalam sistem komputer bersama-sama dengan pemakai sistem komputer yang resmi

- ***Masquerading*** atau ***Impersonation***
  Masquerading atau Impersonation yaitu penetrasi ke sistem komputer dengan memakai identitas dan password dari orang lain yang sah. Identitas dan password ini biasanya diperoleh dari orang dalam.

- ***Scavenging***
  Scavenging yaitu penetrasi ke sistem komputer dengan memperoleh identitas dan password dari mencari di dokumen-dokumen perusahaan.

  Data identitas dan password diperoleh dari beberapa cara mulai dari mencari dokumen di tempat sampah sampai dengan mencarinya di memori-memori komputer.

- ***Eavesdropping***
  Eavesdropping adalah penyadapan informasi di jalur transmisi privat.

  Misalnya adalah yang dilakukan oleh Mark Koenig sebagai konsultan dari GTE. Dia menyadap informasi penting lewat telpon dari nsabah-nasabah Bank of America dan menggunakan informasi tersebut untuk membuat sebanyak 5500 kartu ATM palsu.

Selain cara di atas, metode yang umum digunakan oleh orang dalam melakukan penetrasi ke sistem informasi ada 6 macam ***(Bodnar dan Hopwood***,1993), yaitu :

1. **Pemanipulasian masukkan**
   Dalam banyak kecurangan terhadap komputer, pemanipulasian masukkan merupakan metode yang paling banyak digunakan, mengingat hal ini dapat dilakukan tanpa memerlukan ketrampilan teknis yang tinggi.

2. **Penggantian program**
   Pemanipulasian melalui program dapat dilakukan oleh para spesialis teknologi informasi.

3. **Penggantian berkas secara langsung**
   Pengubahan berkas secara langsung umum dilakukan oleh orang yang punya akses secara langsung terhadap basis data.

4. **Pencurian data**
   Pencurian data seringkali dilakukan oleh "orang dalam" untuk dijual.

   Salah satu kasus yang terjadi pada Encyclopedia Britanica Company. Perusahaan ini menuduh seorang pegawainya menjual daftar nasabah ke sebuah pengiklan *direct mail* seharga $3 juta.

5. **Sabotase**
   Sabotase dapat dilakukan dengan berbagai cara oleh ***Hacker*** atau ***Cracker***.

Hacker : para ahli komputer yang memiliki kekhususan dalam menjebol keamanan sistem komputer dengan tujuan publisitas

Cracker :penjebol sistem komputer yang bertujuan untuk melakukan pencurian atau merusak sistem.

Berbagai teknik yang digunakan untuk melakukan *hacking* :

- ***Denial of Service***
  Teknik ini dilaksanakan dengan cara membuat permintaan yang sangat banyak terhadap suatu situs, sehingga sistem menjadi macet dan kemudian dengan mencari kelemahan pada sistem, si pelaku melakukan serangan terhadap sistem.

- ***Sniffer***
  Teknik ini diimplementasikan dengan membuat program yang dapat melacak paket data seseorang ketika paket tersebut melintasi internet, menangkap password atau menangkap isinya.

- ***Spoofing***
  Melakukan pemalsuan alamat e-mail atau web dengan tujuan untuk menjebak pemakai agar memasukkan informasi yang penting seperti password atau nomor kartu kredit.

6. **Penyalahgunaan dan pencurian sumber daya komputasi**
   Merupakan bentuk pemanfaatan secara ilegal terhadap sumber daya komputasi oleh pegawai dalam rangka menjalankan bisnisnya sendiri.