KEAMANAN SISTEM INFORMASI

Helmi Veris S, S.T, M.Kom

Definisi dari keamanan informasi menurut G. J. Simons

- Bagaimana kita dapat mencegah *penipuan (cheating)* atau, paling tidak, mendeteksi adanya penipuan di sebuah sistem yang berbasis informasi, dimana informasinya sendiri tidak memiliki arti fisik.
- Permasalahan pokok sebenarnya dalam hal keamanan sistem informasi terletak pada kelemahan dan ancaman atas sistem informasi yang pada gilirannya masalah tersebut akan berdampak kepada 7 hal yang utama dalam sistem informasi yaitu :

Hal yang utama dalam sistem informasi yaitu :

- Efektifitas
- Efisiensi
- Kerahaasiaan
- Integritas
- Keberadaan
- Kepatuhan
- Keandalan

Dasar-dasar dari keamanan informasi, meliputi:

1. Tujuan

- Menjaga keamanan sumber-sumber informasi , disebut dengan Manajemen Pengamanan Informasi *(information security management-ISM*)

- Memelihara fungsi-fungsi perusahaan setelah terjadi bencana atau pelanggaran keamanan, disebut dengan Manajemen Kelangsungan Bisnis (business continuity management-BCM).

2. *CIO (chief information officer)* akan menunjuk sekelompok khusus pegawai sebagai bagian keamanan sistem informasi perusahaan. (*corporate information systems security officer-CISSO)*, atau bagian penjamin informasi perusahaan (*corporate information assurance officer-CIAO).*

Adapun tujuan keamanan Informasi menurut Garfinkel, antara lain:

- **Kerahasiaan/*privacy***

Inti utama aspek *privacy* atau *confidentiality* adalah usaha untuk menjaga informasi dari orang yang tidak berhak mengakses. *Privacy* lebih kearah data-data yang sifatnya privat sedangkan *confidentiality* biasanya berhubungan dengan data yang diberikan ke pihak lain untuk keperluan tertentu (misalnya sebagai bagian dari pendaftaran sebuah servis) dan hanya diperbolehkan untuk keperluan tertentu tersebut.

- **Ketersediaan/ *availability***

Agar data dan informasi perusahaan tersedia bagi pihak-pihak yang memiliki otoritas untuk menggunakannya.

- **Integritas/ *integrity***

Aspek ini menekankan bahwa informasi tidak boleh diubah tanpa seijin pemilik informasi. Adanya virus, *trojan horse*, atau pemakai lain yang mengubah informasi tanpa ijin merupakan contoh masalah yang harus dihadapi. Sebuah *e-mail* dapat saja "ditangkap" di tengah jalan, diubah isinya kemudian diteruskan ke alamat yang dituju. Dengan kata lain, integritas dari informasi sudah tidak terjaga. Penggunaan *enkripsi* dan *digital signature*, misalnya, dapat mengatasi masalah ini.

- **Autentikasi/ *Authentication***

- Berhubungan dengan metoda untuk menyatakan bahwa informasi betul-betul asli, orang yang mengakses atau memberikan informasi adalah betul-betul orang yang dimaksud, atau *server* yang dihubungi adalah betul-betul *server* yang asli. *Authentication* biasanya diarahkan kepada orang (pengguna), namun tidak pernah ditujukan kepada *server* atau mesin.

- ***Access Control***

Berhubungan dengan cara pengaturan akses kepada informasi. Hal ini biasanya berhubungan dengan klasifikasi data (*public, private, confidential, top secret*) *user* (*guest, admin, top manager*) mekanisme *authentication* serta *privacy*.

- ***Non-repudiation***

Menjaga agar seseorang tidak dapat menyangkal telah melakukan sebuah transaksi.

Jumlah kejahatan komputer (computer crime), terutama yang berhubungan dengan sistem informasi akan terus meningkat dikarenakan beberapa hal:

- Aplikasi bisnis berbasis teknologi informasi dan jaringan komputer semakin meningkat.
- *Desentralisasi server* sehingga lebih banyak sistem yang harus ditangani dan membutuhkan lebih banyak operator dan administrator yang handal.
- Semakin kompleksnya sistem yang digunakan, seperti semakin besarnya program *(source code)* yang digunakan sehingga semakin besar *probabilitas* terjadinya lubang keamanan.
- Semakin banyak perusahaan yang menghubungkan sistem informasinya dengan jaringan komputer yang global seperti *internet*..

- Meningkatnya kemampuan pemakai di bidang komputer sehingga mulai banyak pemakai yang mencoba-coba bermain atau membongkar sistem yang digunakannya.
- Kesulitan dari penegak hukum untuk mengejar kemajuan dunia komputer dan telekomunikasi yang sangat cepat.

KELEMAHAN, ANCAMAN

- Cacat atau kelemahan dari suatu sistem yang mungkin timbul pada saat mendesain, menetapkan prosedur, mengimplementasikan maupun kelemahan atas sistem kontrol yang ada sehingga memicu tindakan pelanggaran oleh pelaku yang mencoba menyusup terhadap sistem tersebut.

Kelemahan tersebut dimanfaatkan oleh orang-orang yang tidak bertanggung jawab seperti gangguan /serangan:

- Untuk mendapatkan akses *(access attacks)*
- Berusaha mendapatkan akses ke berbagai sumber daya komputer atau data/informasi
- Untuk melakukan modifikasi *(modification attacks)*
- Didahului oleh usaha untuk mendapatkan akses, kemudian mengubah data/informasi secara tidak sah
- Untuk menghambat penyediaan layanan (*denial of service attacks)*
- Berusaha mencegah pemakai yang sah untuk mengakses sebuah sumber daya atau informasi Menghambat penyediaan layanan dengan cara mengganggu jaringan komputer

Beberapa cara dalam melakukan serangan, antara lain:

- 1. *Sniffing*→Memanfaatkan metode *broadcasting* dalam LAN, membengkokkan aturan *Ethernet,* membuat *network interface* bekerja dalam *mode promiscuousn*. Cara pencegahan dengan pendeteksian *sniffer (local & remote*) dan penggunaan *kriptografi*
- 2. *Spoofing*→Memperoleh akses dengan acara berpura-pura menjadi seseorang atau sesuatu yang memiliki hak akses yang *valid, Spoofer* mencoba mencari data dari *user* yang sah agar bisa masuk ke dalam sistem. Pada saat ini, penyerang sudah mendapatkan *username & password* yang sah untuk bisa masuk ke *server*

- 3. *Man-in-the-middle*→Membuat *client* dan *server* sama-sama mengira bahwa mereka berkomunikasi dengan pihak yang semestinya *(client* mengira sedang berhubungan dengan *server*, demikian pula sebaliknya)
- 4. Menebak *password*
  - Dilakukan secara sistematis dengan teknik *brute-force* atau *dictionary* (mencoba semua kemungkinan *password*)
  - Teknik *dictionary:* mencoba dengan koleksi kata-kata yang umum dipakai, atau yang memiliki relasi dengan *user* yang ditebak (tanggal lahir, nama anak, dan sebagainya)

Ancaman berasal dari luar perusahaan :

- Ancaman Alam
- Ancaman air, seperti : Banjir, Stunami, Intrusi air laut, kelembaban tinggi, badai, pencairan salju
- Ancaman Tanah, seperti : Longsor, Gempa bumi, gunung meletus
- Ancaman Alam lain, seperti : Kebakaran hutan, Petir, tornado, angin ribut
- Ancaman Manusia
- Ancaman Lingkungan

Menurut sifatnya :

1. Ancaman terhadap sistem informasi terdiri dari **ancaman aktif**.

   Ancaman aktif dapat berupa penyelewengan aktivitas, penyalahgunaan kartu kredit, kecurangan dan kejahatan komputer, pengaksesan oleh orang yang tidak berhak, *sabotase* maupun perogram yang jahil, contoh *virus,torjan,cacing,bom* waktu dan lain-lain.

2. Sedangkan **ancaman pasif** berupa kesalahan manusia, kegagalan sistem maupun bencana alam dan politik. Besar kecilnya suatu ancaman dari sumber ancaman yang teridentifikasi atau belum teridentifikasi dengan jelas tersebut, perlu di klasifikasikan secara matriks ancaman sehingga kemungkinan yang timbul dari ancaman tersebut dapat di minimalisir dengan pasti.

Aspek ancaman keamanan komputer atau keamanan sistem informasi

- *Interruption* →informasi dan data yang ada dalam sistem komputer dirusak, dihapus sehingga jika dibutuhkan, data atau informasi tersebut tidak ada lagi.
- I*nterception* →informasi yang ada disadap atau orang yang tidak berhak mendapatkan akses ke komputer dimana informasi tersebut disimpan.

- *Modifikas*i →orang yang tidak berhak berhasil menyadap lalu lintas informasi yang sedang dikirim dan diubah sesuai keinginan orang tersebut.
- *Fabrication*→ orang yang tidak berhak berhasil meniru suatu informasi yang ada sehingga orang yang menerima informasi tersebut menyangka informasi tersebut berasal dari orang yang dikehendaki oleh si penerima informasi tersebut.

Macam-macam resiko keamanan informasi dapat berupa:

- Pengungkapan dan pencurian
- Ketika database dan perpustakaan perangkat lunak dapat diakses oleh orang yang tidak berhak.
- Penggunaan secara tidak sah
- Terjadi ketika sumber daya perusahaan dapat digunakan oleh orang yang tidak berhak menggunakannya, biasa disebut hacker.

- Pengrusakan secara tidak sah dan penolakan pelayanan
- Penjahat komputer dapat masuk ke dalam jaringan komputer dari komputer yang berada jauh dari lokasi dan menyebabkan kerusakan fisik, seperti kerusakan pada layar monitor, kerusakan pada *disket*, kemacetan pada *printer*, dan tidak berfungsinya *keyboard*.

- Modifikasi secara tidak sah

  Perubahan dapat dibuat pada data-data perusahaan, informasi, dan perangkat lunak. Beberapa perubahan tidak dapat dikenali sehingga menyebabkan pengguna yang ada di output system menerima informasi yang salah dan membuat keputusan yang salah. Tipe modifikasi yang paling dikhawatirkan adalah modifikasi disebabkan oleh perangkat lunak yang menyebabkan kerusakan, biasanya dikelompokkan sebagai virus.

STRATEGI DAN LANGKAH PENGAMANAN

Strategi dan taktik keamanan sistem informasi yang dimaksud meliputi:

- Keamanan fisik
- Siapa saja memiliki hak akses ke sistem. Jika hal itu tidak diperhatikan, akan terjadi hal-hal yang tidak dikehendaki.
- Kunci Komputer
- Banyak *case PC* modern menyertakan atribut penguncian. Biasanya berupa soket pada bagian depan *case* yang memungkinkan kita memutar kunci yang disertakan ke posisi terkunci atau tidak.
- Keamanan BIOS
- Untuk mencegah orang lain me-reboot ulang komputer kita dan memanipulasi sisten komputer kita.
- Mendeteksi Gangguan Keamanan Fisik
- Pertama yang harus diperhatikan adalah pada saat komputer akan di-*reboot*.

Langkah keamanan sistem informasi

- Aset

Perlindungan aset merupakan hal yang penting dan merupakan langkah awal dari berbagai implementasi keamanan komputer.

- Analisis Resiko

Menyangkut identifikasi akan resiko yang mungkin terjadi, sebuah *even* yang potensial yang bisa mengakibatkan suatu sistem dirugikan.

- Perlindungan

Melindungi jaringan internet dengan pengaturan *Internet Firewall* yaitu suatu akses yang mengendalikan jaringan internet dan menempatkan *web dan FTP server* pada suatu *server* yang sudah dilindungi oleh *firewall*.

- Alat

Alat atau tool yang digunakan pada suatu komputer merupakan peran penting dalam hal keamanan karena tool yang digunakan harus benar-benar aman.

- Prioritas

Jika keamanan jaringan merupakan suatu prioritas, maka suatu organisasi harus membayar harga baik dari segi material maupun non material. Suatu jaringan komputer pada tahap awal harus diamankan dengan *firewall* atau lainnya yang mendukung suatu sistem keamanan.

Upaya melindungi sisstem informasi

- Pendekatan *preventif* yang bersifat mencegah dari kemungkinan terjadinya ancaman dan kelemahan
- Pendekatan *detective* yang bersifat mendeteksi dari adanya penyusupan dan proses yang mengubah sistem dari keadaan normal menjadi keadaan abnormal
- Pendekatan *Corrective* yang bersifat mengkoreksi keadaan sistem yang sudah tidak seimbang untuk dikembalikan dalam keadaan normal

TERIMA KASIH