KEAMANAN SISTEM INFORMASI

Gentisya Tri Mardiani, S.Kom

Pendahuluan

- **Sistem Informasi**

  Ward, J. dan Peppard, J. (2003)

  "Information systems as the means by which people and organizations, utilizing technology, gather, process, store, use and disseminate information"

Sistem Informasi

- Sistem informasi sebagai sarana yang orang-orang dan organisasi, memanfaatkan teknologi, mengumpulkan, memproses, menyimpan, menggunakan dan menyebarkan informasi

- Kumpulan dari beberapa komponen yang saling terkait sehingga dapat menghasilkan suatu informasi tertentu.

Komponen SI

Hardware

Database

Software

Data/
Informasi

People

Procedure

Kemanan Informasi

- G. J. Simons,

  Keamanan informasi adalah 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.

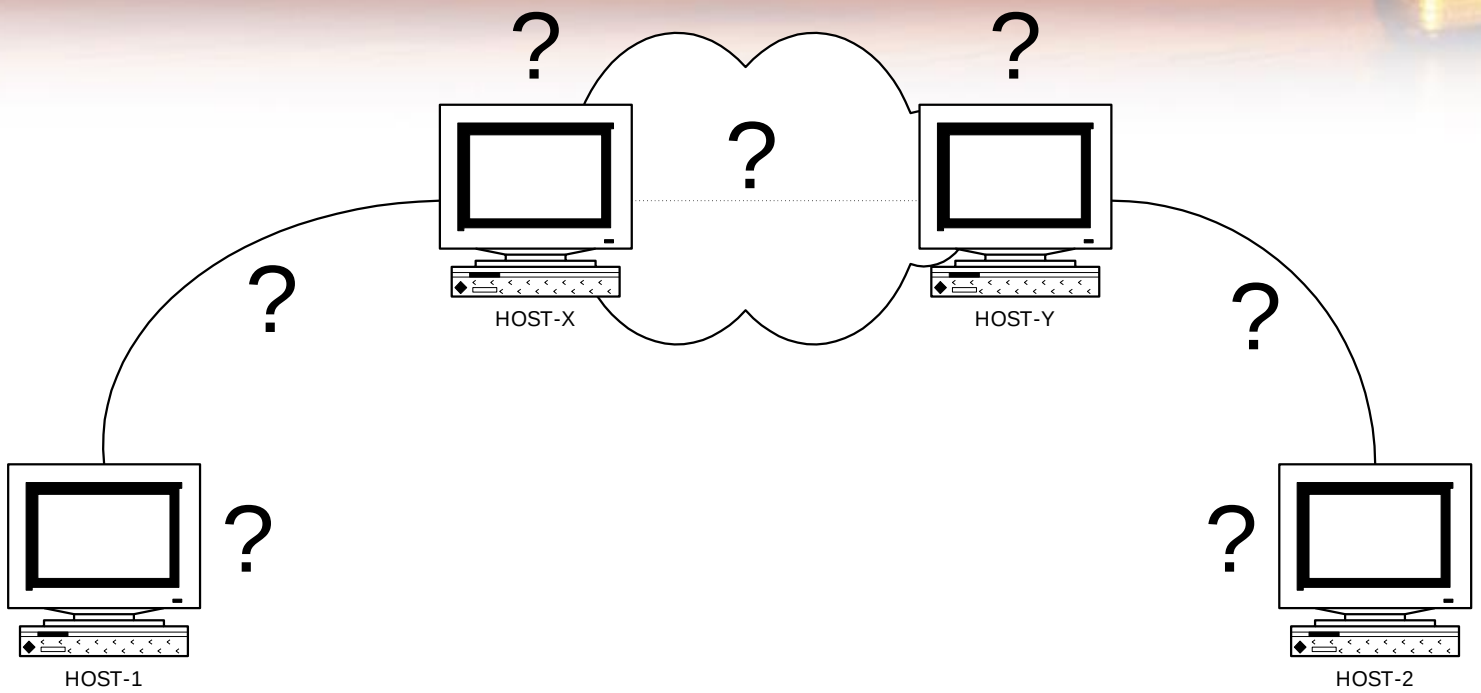
Kemanan Informasi

- Cara mengamankan, menjaga, menjamin sistem agar informasi dapat tersedia saat dibutuhkan.

Kemanan Informasi

- Sistem informasi: berbasis Internet
- Perlu ditinjau dan dimengerti hubungan komputer di jaringan
- Kemungkinan adanya resiko yang muncul atas sistem tersebut.

Kemanan Informasi



Hubungan komputer di Internet beserta titik-titik yang rawan

Security vs Convenience

- Kemudahan (kenyamanan) mengakses informasi berbanding terbalik dengan tingkat keamanan sistem informasi itu sendiri.
- Semakin tinggi tingkat keamanan, semakin sulit (tidak nyaman) untuk mengakses informasi.

Risiko Kemanan

1. Assets (aset):
   hardware, software, dokumentasi, data, komunikasi, lingkungan, manusia
2. Threats (ancaman):
   pemakai (users), teroris, kecelakaan, crackers, penjahat kriminal, bencana alam, intel, dsb.
3. Vulnerabilities (kelemahan):
   software/hardware bugs, unathorized users, print out, keteledoran, dsb.

Aspek Keamanan

Menurut S. Garfinkel, aspek keamanan meliputi:

- Confidentiality/ Privacy
- Integrity
- Availability
- Authentication

Confidentiality/ Privacy

- *Privacy* berhubungan dengan data yang pribadi sedangkan *confidentiality* biasanya berhubungan dengan data yang diberikan ke pihak lain untuk keperluan tertentu.
- Confidentiality menjamin perlindungan terhadap akses informasi.

Confidentiality/ Privacy

- Serangan terhadap aspek privacy misalnya adalah usaha untuk melakukan penyadapan (dengan program *sniffer).*

- Usaha yang dapat dilakukan untuk meningkatkan privacy dan confidentiality adalah dengan menggunakan teknologi kriptografi.

Integrity

- Integritas menjamin bahwa informasi tidak dapat diubah dan tetap konsisten.

- Serangan yang dapat terjadi berasal dari virus, trojan, atau user yang mengubah informasi tanpa izin.

Availability

- Ketersediaan menjamin kesiapan akses informasi.
- Sistem informasi yang diserang dapat menghambat atau meniadakan akses ke informasi.
- Contoh serangan yang sering disebut "*denial of service attack" (DoS attack),* dimana server dikirimi permintaan palsu yang bertubi-tubi sehingga tidak dapat melayani permintaan lain atau bahkan sampai *down, hang, crash.*

Authentication

- Autentikasi menjamin bahwa informasi yang diterima asli, atau orang yang mengakses atau memberikan informasi adalah pihak yang berhak.

- pengguna harus menunjukkan bukti bahwa memang dia adalah pengguna yang sah, misalnya dengan menggunakan password, biometric (ciri-ciri khas), dan sejenisnya.

Access Control

- Aspek ini berhubungan dengan cara pengaturan akses kepada informasi, berhubungan dengan masalah authentication dan privacy.

- Dilakukan dengan menggunakan kombinasi userid/password atau dengan menggunakan mekanisme lain.

Non-repudiation

- Aspek ini menjaga agar seseorang tidak dapat menyangkal telah melakukan sebuah transaksi.

- Penggunaan digital signature dan teknologi kriptografi secara umum dapat menjaga aspek ini.

Masalah Keamanan

- Beberapa web site Indonesia sudah dijebol dan daftarnya (beserta contoh halaman yang sudah dijebol) dapat dilihat di koleksi http://www.2600.com

- Meningkatnya kemampuan pemakai di bidang komputer sehingga mulai banyak pemakai yang mencoba-coba bermain atau membongkar sistem yang digunakannya.

Masalah Keamanan

Masalah Keamanan

- Kesulitan dari penegak hukum untuk mengejar kemajuan dunia komputer dan telekomunikasi yang sangat cepat.
- Semakin banyak perusahaan yang menghubungkan sistem informasinya dengan jaringan komputer global seperti Internet. Hal ini membuka akses dari seluruh dunia. Potensi sistem informasi yang dapat dijebol menjadi lebih besar.

Klasifikasi Kejahatan Komputer

1. **Keamanan yang bersifat fisik (*physical security)***
   - pencurian berkas
   - *wiretapping*
   - *denial of service*
   - *Syn Flood Attack*
2. **Keamanan yang berhubungan dengan orang (personel)**
   - social engineering

Klasifikasi Kejahatan Komputer

3. **Keamanan dari data dan media serta teknik komunikasi (*communications)***
   -virus atau *trojan*
4. **Keamanan dalam operasi**
   - prosedur yang digunakan untuk mengatur dan mengelola sistem keamanan

Peningkatan Kejahatan Komputer

- Jumlah pengguna semakin meningkat
- Aplikasi bisnis berbasis teknologi informasi semakin meningkat
- *Security awareness* masih rendah
- Penerapan *cyberlaw* masih lemah
- Jaringan publik semakin luas, tidak didukung dengan sistem pengamanan yang baik

See u next week

☺