PENGAMANAN SISTEM KOMPUTER

Agenda

- Tujuan
- Pendahuluan
- Bagaimana Mengelola data dan Informasi
- Pengertian Pengamanan Komputer
- Keamanan Internet
- Kejahatan Internet

Tujuan

- Mahasiswa dapat memahami akan pentingnya konsep dasar pengamanan komputer
- Dapat melakukan usaha dan pencegahan dalam membangun sebuah sistem keamanan komputer
- Dapat merangcang sistem pengamanan komputer sesuai kebutuhan

- Kehadiran = 10%
- UTS = 30%
- Tugas = 30%
- UAS = 30%

SELAYANG PANDANG

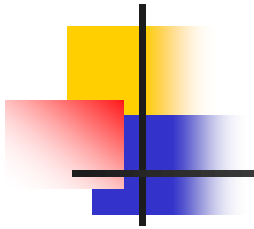
- **Keamanan informasi menjadi hal penting bagi:**
  1. Organisasi/Perusahaan penyedia jasa Teknologi Informasi (TI) maupun industri.
  2. Pengguna fasilitas TI dan menempatkannya sebagai infrastruktur kritikal (penting).

Pendahuluan

Masalah keamanan merupakan aspek penting untuk sebuah sistem informasi. Para pengelola dan pemilik informasi kadang kurang memperhatikan aspek keamanan. Seringkali masalah keamanan berada di urutan kedua, atau bahkan di urutan terakhir dalam daftar hal-hal yang dianggap penting.

Alasan Pentingnya pengamanan komputer:

- Informasi memiliki nilai yang sangat penting
- Kejahatan komputer tiap tahunnya meningkat.
- Menghindari resiko penyusupan
- Mengurangi resiko ancaman
  - Ingin Tahu
  - Ingin Merusak
  - Mencari populeritas
  - Persaingan
- Kontinuitas bisnis,
- Mengoptimalkan Return On Investment (ROI) dan mencari kesempatan bisnis.



Bagaimana Data atau Informasi dikelola

Pengertian Pengamanan Komputer

Menurut **John D. Howard** dalam bukunya "An Analysis of security incidents on the internet" menyatakan bahwa :

"Keamanan komputer adalah tindakan pencegahan dari serangan pengguna komputer atau pengakses jaringan yang tidak bertanggung jawab".

Menurut Gollmann pada tahun 1999 dalam bukunya "Computer Security" menyatakan bahwa :

"Keamanan komputer adalah berhubungan dengan pencegahan diri dan deteksi terhadap tindakan pengganggu yang tidak dikenali dalam system komputer".

Pengertian Pengamanan Komputer

- Keamanan Informasi adalah melindungi informasi dan sistem informasi dari akses yang tidak sah, penggunaan, pengungkapan, gangguan, modifikasi, teliti, inspeksi, merekam atau perusakan [Anderson, K. (October 12, 2006)]
- Keamanan informasi usaha memproteksi informasi dari ancaman yang luas untuk memastikan kelanjutan usaha, memperkecil rugi perusahaan dan memaksimalkan laba atas investasi dan kesempatan usaha

TUGAS KEAMANAN SISTEM INFORMASI

- Ketersediaan informasi yang diperlukan pada saat yang tepat, dengan isi informasi yang benar, penyajian informasi pada pihak yang berhak menjadi tugas dari keamanan sistem informasi.

- Manajemen Keamanan dalam suatu organisasi, memiliki tujuan untuk melindungi data organisasi dan menjaga nilai dari data atau infomasi perusahaan tersebut.

ELEMEN PENTING

- Elemen-elemen yang perlu dijaga dalam perlindungan data/informasi tersebut adalah:
  1. ***Confidentiality*** *(*Kerahasiaan data),
  2. ***Integrity*** *(*Integritas atau Keutuhan data*)* dan
  3. ***Availability*** *(*Ketersediaan) *data/informasi*.

KELEMAHAN KEAMANAN DALAM PERUSAHAAN

- Perusahaan/organisasi tidak mempuyai prosedur khusus yang ditetapkan untuk mengatasi kemungkinan ancaman-ancaman yang terjadi.
- Perusahaan belum memiliki metode dan cara untuk mengamankan sistem jaringan internal, eksternal dan telekomunikasi yang dimiliki

JENIS ANCAMAN PADA SISTEM INFORMASI

1. **Kehilangan data.**

   Kehilangan data ini dapat terjadi karena berbagai hal, mulai dari kerusakan data itu sendiri, kerusakan hardware, kesalahan pengguna, hal-hal ini dapat terjadi baik secara sengaja maupun tidak sengaja.

2. **Pemutusan akses**

   Pemutusan akses ini dapat terjadi pada akses telekomunikasi dan jaringan komputer ke luar.

3. **Pencurian Data**
4. **Pengubahan data**

REKOMENDASI PENCEGAHAN

1. Perlu adanya prosedur – prosedur Keamanan yang dilakukan oleh perusahaan.
2. Melakukan Penerapan pengawasan dan kontrol melalui (countermeasure):

   a. Pencegahan

   b. Deteksi

   c. Represif

   d. Evaluasi

Keamanan Internet

- Alasan Perusahaan menggunakan LAN & internet memungkinkan tersedia informasi secara cepat.
- Terhubungnya LAN/Komputer ke internet membuka potensi adanya lubang keamanan (security hole).
- Keamanan sistem informasi berbasis web tergantung desain keamanan sistem web.
- Arsitektur sistem web, terdiri dari : Server-client yang saling berhubungan.