Keamanan Sistem Komputer

Definisi

- Tindakan pencegahan dari serangan pengguna komputer atau pengakses jaringan yang tidak bertanggung jawab.

- Perlindungan terhadap fasilitas komputer, kesalahan program dan data dari kerusakan oleh resiko lingkungan, kesalahan perangkat lunak, kesalahan manusia atau penyalahgunaan komputer.

Mengapa Perlu Dilakukan Keamanan Sistem Komputer?

- Melindungi sistem dari kerentanan, yakni dari akses liar dari pihak yang tidak diizinkan atau berhak.
- Mengurangi resiko ancaman, hal ini biasa berlaku di institusi dan perusahaan swasta.
- Menghindari resiko penyusupan, yaitu: membaca, menulis dan menjalankan program-program yang bisa mengganggu atau menghancurkan sistem.
- Adanya kejahatan komputer (Cybercrime)

Kejahatan komputer

- Meningkatnya pengguna komputer dan Internet.
- Desentralisasi server sehingga lebih banyak sistem yang harus ditangani, sementara SDM terbatas.
- Lemahnya hukum yang mengatur tentang kejahatan komputer.
- Semakin banyaknya perusahaan yang menghubungkan jaringan mereka ke Internet
- Banyaknya software yang mempunyai kelemahan.

Kelompok keamanan komputer

1. Keamanan Eksternal.

Berkaitan dengan fasilitas komputer dari penyusupan yang terjadi karena bencana alam, seperti kebakaran dan kebanjiran.

2. Keamanan Interface pemakai.

Keamanan yang berkaitan dengan identifikasi pemakai sebelum pemakai diizinkan mengakses program dan data yang disimpan.

3. Keamanan Internal.

Berkaitan dengan keamanan beragam kendali yang dibangun pada perangkat keras dan sistem operasi.

Aspek Keamanan Komputer

1. **Privacy/Confidentiality**

Aspek ini bermakna menjaga informasi dari orang yang tidak berhak mengakses, yang dimana lebih ke arah data-data yang bersifat privat (rahasia). Misalkan: email, nama, alamat dan sebagainya.

2. **Integrity.**

Informasi tidak boleh diubah tanpa seijin pemilik informasi.

Menjaga pada saat data ditransmisikan dari perubahan /modifikasi dari pihak lain.

Aspek Keamanan Komputer

3. Availability.

Ketersediaanya informasi atau sumber data yang diinginkan pada sebuah sistem pada saat dibutuhkan.

Aspek ini menjaga keamanan dari adanya serangan berupa penolakan akses terhadap data atau layanan dengan membuatnya tidak tersedia (data dihapus).

Aspek Keamanan Komputer

4. Authentication.

Metode untuk menyatakan bahwa informasi betul-betul asli atau orang yang mengakses atau memberikan informasi adalah betul-betul orang yang dimaksud.

Dapat berupa password, watermark, tanda tangan digital, biometrik, fingerprint dan sebagainya.

Jenis Ancaman

- **Interception**

Pihak yang tidak berizin mendapatkan akses untuk masuk ke dalam sistem.

- **Interruption**

Sistem komputer menjadi tidak tersedia atau tidak dapat bekerja.

- **Modification**

Pihak yang tidak berizin mengakses kedalam sistem dan mengubah (memodifikasi) data.

- **Fabrication**

Pihak yang tidak berizin memalsukan data.

Jenis Ancaman

- **Sabotage**

Melakukan kerusakan dan menghancurkan program/data.

- **Espionage**

Mengintai dan mengumpulkan data-data rahasia.

- **Malicious code**

Mengacu pada software yang mengganggu (virus).

- **Terrorism**

Mengancam pihak-pihak tertentu.

5 Langkah Keamanan Komputer

1. **Asset**

Menjaga tingkat privasi data dan menjamin keamanan data.

2. **Risk Analysis**

Mengidentifikasi segala resiko yang mungkin terjadi yang mengakibatkan kerusakan sistem.

3. **Protection**

Adanya regulasi yang menjamin sistem dari serangan.

4. **Tools**

Memanfaatkan peralatan-peralatan yang sesuai dan memiliki kekuatan keamanan.

5. **Priority**

Menganggap penting aspek keamanan.

Manajemen Keamanan Komputer

- Sistem komputer yang baik membutuhkan pengelolaan sistem keamanan dengan cara-cara yang tepat dan efektif.
- Manajemen keamanan mengelola 3 elemen penting:
  1. Sumber Daya Manusia (SDM)
  2. Teknologi
  3. Operasi

3 Elemen Manajemen: SDM

- Staff dan pegawai dari suatu organisasi yang memiliki sistem komputer harus:
  - Pemahaman terhadap berbagai jenis serangan.
  - Pemahaman tentang kebijakan jaminan dan prosedur.
  - Penetapan tugas dan tanggungjawab.
  - Mengikuti pelatihan keamanan sistem komputer.

3 Elemen Manajemen: Teknologi

- Teknologi yang digunakan harus:
  - Memiliki standar dalam keamanan sistem komputer.
  - Hardware dan Software yang baik.
  - Mengikuti keadaan dan situasi dari perkembangan komputer dan Teknologi Informasi.

3 Elemen Manajemen: Operasi

- Pemeliharaan kebijakan sistem keamanan agar tetap layak dan terbaharui.
- Memonitor dan menghadapi ancaman setiap saat.
- Merasakan Serangan, yakni: memberikan peringatan dan merespon dengan benar.

TERIMA KASIH