Keamanan dan Kerahasiaan Data

Keamanan dan Kerahasiaan Data

- Klasifikasi Kejahatan Komputer
- Aspek Dari Security
- Serangan Terhadap Keamanan Sistem
- Mendeteksi serangan
- Mencegah serangan
- Metoda Pengamanan

Taukah Anda?

- Menurut Anda, Apa yang dimaksud dengan keamanan!
- Menurut Anda, Apa bedanya keamanan dengan kenyamanan!
- Jelaskan maksud dari keamanan komputer!
- Menurut Anda, atas dasar apa kita harus melakukan atau menjaga keamanan komputer?
- Menurut Anda, bagaimana keamanan komputer telah dilakukan saat ini?
- “Untuk mendapatkan keamanan terkadang kita harus mengorbankan kenyamanan”. Jelaskan maksud dari kalimat tersebut!

Pengertian Keamanan 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.

Definisi Resiko

Success Factors of Risk Management

- Komitmen dari senior Management
- *Full Support* dan partisipasi dari tim IT
- Kehandalan *skills* dari tim risk *assessment*
- *Awareness* dan kerja sama dari user IT
- Proses monitoring yang bersifat *continual* dalam rangka memonitor resiko dan menurunkan resiko ke tingkat yang dapat diterima

Modal dasar

- Mengetahui Bahasa Pemrograman
- Menguasai pengetahuan perangkat keras dan perangkat lunak pengontrolnya (logika interfacing).
- Menguasai pengelolaan instalasi komputer.
- Menguasai dengan baik teori jaringan komputer ; protokol, infrastruktur, media komunikasi.
- Memahami cara kerja system operasi.
- Memiliki ‘pikiran jahat’ ;-p

Keamanan Komputer Mengapa dibutuhkan ?

- *"information-based society"*, menyebabkan nilai informasi menjadi sangat penting dan menuntut kemampuan untuk mengakses dan menyediakan informasi secara cepat dan akurat menjadi sangat esensial bagi sebuah organisasi,
- Infrastruktur Jaringan komputer, seperti LAN dan Internet, memungkinkan untuk menyediakan informasi secara cepat, sekaligus membuka potensi adanya lubang keamanan *(security hole)*

Kejahatan Komputer semakin meningkat karena :

- Aplikasi bisnis berbasis TI dan jaringan komputer meningkat : online banking, e-commerce, Electronic data Interchange (EDI).
- Desentralisasi server.
- Transisi dari single vendor ke multi vendor.
- Meningkatnya kemampuan pemakai (user).
- Kesulitan penegak hokum dan belum adanya ketentuan yang pasti.
- Semakin kompleksnya system yang digunakan, semakin besarnya source code program yang digunakan.
- Berhubungan dengan internet.

Klasifikasi Kejahatan Komputer

- **Keamanan yang bersifat fisik** (*physical security*): termasuk akses orang ke gedung, peralatan, dan media yang digunakan
- **Keamanan yang berhubungan dengan orang (*personel*)**: termasuk identifikasi, dan profil resiko dari orang yang mempunyai akses (pekerja).
- **Keamanan dari data dan media serta teknik komunikasi** (*communications*). Yang termasuk di dalam kelas ini adalah kelemahan dalamsoftware yang digunakan untuk mengelola data
- **Keamanan dalam operasi**: termasuk prosedur yang digunakan untuk mengatur dan mengelola sistem keamanan, dan juga termasuk prosedur setelah serangan (*post attack recovery*).

Aspek Dari Security

- *Confidentiality*
- *Integrity*
- *Availability*
- Ketiga di atas sering disingkat menjadi **CIA**
- Ada tambahkan lain
  - Non-repudiation
  - Authentication
  - Access Control
  - Accountability

Confidentiality / Privacy

- Kerahasiaan data. Data hanya boleh diakses oleh orang yang berwenang
  - Data-data pribadi
  - Data-data bisnis; daftar gaji, data nasabah
  - Sangat sensitif dalam e-commerce dan healthcare
- Serangan: penyadapan
  (teknis dengan sniffer / logger, man in the middle attack; non-teknis dengan social engineering)
- Proteksi: enkripsi

Integrity

- Informasi tidak boleh berubah (tampered, altered, modified) oleh pihak yang tidak berhak
- Serangan
  - Pengubahan data oleh orang yang tidak berhak, spoofing
  - Virus yang mengubah berkas
- Proteksi:
  - Message Authentication Code (MAC), digital signature / certificate, hash functions, logging

Availability

- Informasi harus tersedia ketika dibutuhkan
- Serangan
  - Meniadakan layanan (Denial of Service / DoS attack) atau menghambat layanan (server dibuat lambat)
- Proteksi
  - Backup, redundancy, DRC, BCP, firewall

Non-repudiation

- Tidak dapat menyangkal (telah melakukan transaksi)
  - Menggunakan digital signature
  - Logging

Authentication

- Meyakinkan keaslian data, sumber data, orang yang mengakses data, server yang digunakan
  - what you have (identity card)
  - what you know (password, PIN)
  - what you are (biometric identity)
- Serangan: identitas palsu, terminal palsu, situs gadungan

Access Control

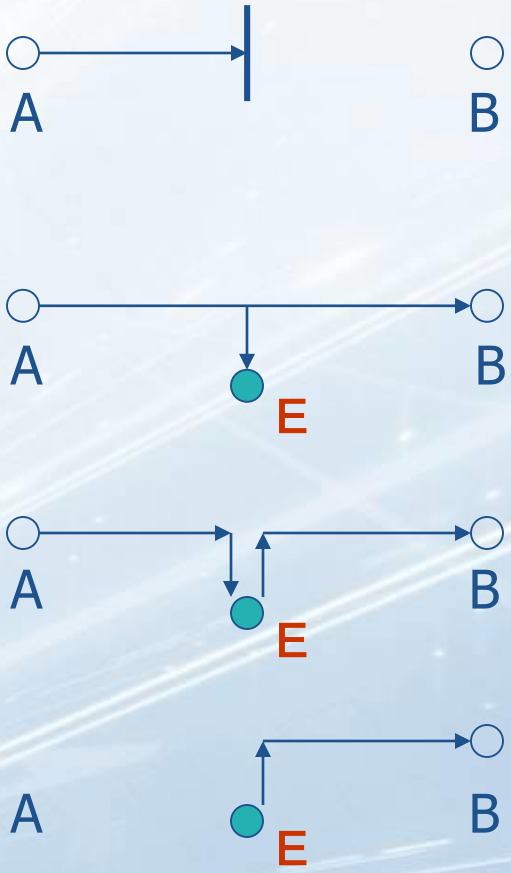
- Mekanisme untuk mengatur siapa boleh melakukan apa
  - Membutuhkan adanya klasifikasi data: *public, private, confidential, (top)secret*
  - Role-based access

Accountability

- Dapat dipertanggung-jawabkan
- Melalui mekanisme logging dan audit
- Adanya kebijakan dan prosedur (policy & procedures)

Serangan Terhadap Keamanan Sistem

- **Interruption**
  DoS attack, network flooding
- **Interception**
  Password sniffing
- **Modification**
  Virus, trojan horse
- **Fabrication**
  spoffed packets



Interupsi (Interuption)

- Interupsi adalah bentuk ancaman terhadap ketersediaan (availability), dimana data dirusak sehingga tidak dapat digunakan lagi. Perusakan dilakukan berupa :
- perusakan fisik
  - Perusakan harddisk
  - Media penyimpanan lainnya
  - Pemotongan kabel jaringan
- Perusakan nonfisik
  - Penghapusan suatu file-file tertentu dari sistem komputer

Intersepsi (Interception)

Intersepsi adalah bentuk ancaman terhadap kerahasiaan (secrecy), dimana pihak yang tidak berhak berhasil mendapat hak akses untuk membaca suatu data atau informasi dari suatu sistem komputer. Tindakan yang dilakukan melalui penyadapan data yang ditransmisikan lewat jalur publik atau umum yang dikenal dengan istilah writetapping dalam wired networking, yaitu jaringan yang menggunakan kabel sebagai media transmisi data.

Modifikasi (Modification)

Modifikasi adalah bentuk ancaman terhadap integritas (integrity), dimana pihak yang tidak berhak berhasil mendapat hak akses untuk mengubah suatu data atau informasi dari suatu sistem komputer. Data atau informasi yang diubah adalah record dari suatu tabel pada file database

Pabrikasi (Fabrication)

Pabrikasi adalah bentuk ancaman terhadap integritas. Tindakan yang dilakukan dengan meniru dan memasukkan suatu objek ke dalam sistem komputer. Objek yang dimasukkan berupa suatu file maupun record yang disisipkan pada suatu program aplikasi.

Program Pengrusak

Bug

Kesalahan-kesalahan yang terdapat pada suatu program aplikasi yang terjadi secara tidak disengaja.

Bug dapat menyebabkan

- Sistem komputer hang
- Merusak media penyimpanan pada sistem komputer

Program Pengrusak

Chameleons

Program yang diselundupkan atau disisipkan ke dalam suatu sistem komputer dan berfungsi untuk mencuri data dari sistem komputer yang bersangkutan.

Sifatnya tidak merusak sistem komputer tetapi mendapatkan data dan berusaha untuk melakukan pengubahan data

Program Pengrusak

Logic Bomb

Bomb ditempatkan atau dikirimkan secara diam-diam pada suatu sistem komputer yang menjadi target dan akan meledak bila pemicunya diaktifkan.

Berdasarkan pemicu yang digunakan, logic bomb digolongkan menjadi

- Software bomb

Akan meledak jika dipicu oleh suatu software tertentu

- Logic bomb

Akan meledak jika memenuhi suatu kondisi tertentu

- Time bomb

Akan meledak pada waktu yang telah ditentukan

Program Pengrusak

- Trojan Horse

Prinsip kerja mirip seperti chameleons, bedanya trojan horse akan melakukan sabotase dan perusakan terhadap sistem komputer yang dijangkitinya

Program Pengrusak

- Virus

Awalnya merupakan suatu program yang dibuat hanya untuk menampilkan nama samaran serta beberapa baris kata dari pembuatnya sehingga tidak membahayakan komputer.

Perkembangannya, virus komputer mulai menggabungkan beberapa karakteristik dari beberapa program pengganggu dan perusak lainnya à merusak sistem komputer

Program Pengrusak

- Worm

Program pengganggu yang dapat memperbanyak diri dan akan selalu berusaha menyebarkan diri dari satu komputer ke komputer lain dalam suatu jaringan.Worm menjadikan ukuran suatu file menjadi membengkak dan dapat menguras kapasitas media penyimpanan

Mendeteksi serangan

- **Anomaly Detection (Penyimpangan)**
  mengidentifikasi perilaku tak lazim yang terjadi dalm Host atau Network.
- **Misuse Detection**
  Detektor melakukan analisis terhadap aktivitas sistem, mencari event atau set event yang cocok dengan pola Perilaku yang dikenali sebagai serangan.
- **Network Monitoring**
  (sistem pemantau jaringan) untuk mengatahui adanya lubang keamanan, Biasanya dipakai (SNMP)
- **Intrusion Detection System (IDS)**
  Penghambat atas semua serangan yg akan menggangu sebuah jarigan.

Mencegah serangan

- Desain Sistem
  - Desain sistem yg baik tidak meninggalkan lobang2 yg memungkinkan terjadinya penyusupan
- Aplikasi yang dipakai
  - Aplikasi yg dipakai sudah diperikasa dan apakah sudah dapat dipercaya.
- Manajemen
  - Pengolahan suatu sistem yg baik menurut standard operating procedure (SOP)

Prinsip merancang suatu sistem keamanan

- Dalam merancang suatu sistem keamanan, ada prinsip yang harus diperhatikan:
  - *LEAST PRIVILEGE*. SEMUA PROGRAM DAN USER DARI SISTEM HARUS BEROPERASI PADA LEVEL TERENDAH YG DIPERLUKAN UNTUK MENYELESAIKAN TUGASNYA.
  - *ECONOMY OF MECHANISMS*. MEKANISME KEAMANAN HARUS SEDERHANA, DAN MERUPAKAN BAGIAN YG TAK TERPISAHKAN DENGAN RANCANGAN SISTEM SECARA KESELURUHAN.
  - *ACCEPTABILITY.* SISTEM KEAMANAN MUDAH DIPERGUNAKAN OLEH USER.
  - *COMPLETE MEDIATION.* SETIAP AKSES HARUS DICEK KE DALAM INFORMASI KONTROL AKSES, TERMASUK PADA SAAT KONDISI TIDAK NORMAL SEPERTI PADA PEMELIHARAAN.
  - *OPEN DESIGN.* MEKANISME KEAMANAN DARI SISTEM HARUS DAPAT DISEBARLUASKAN SEHINGGA ADA UMPAN-BALIK YANG DAPAT DIMANFAATKAN UNTUK PERBAIKAN SISTEM KEAMANAN.