Prinsip Dasar 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 sistem komputer.

Terdapat 2 alasan mengapa keamanan komputer sangat penting yaitu:

- "Information-based society", yang menyebabkan informasi menjadi sangat penting dan menuntut kemampuan untuk mengakses dan menyediakan informasi secara cepat dan akurat menjadi 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).

Terjadinya kejahatan komputer pada zaman sekarang meningkat drastis dibandingkan beberapa tahun sebelumnya, disebabkan oleh :

- Aplikasi bisnis berbasis TI dan jaringan komputer meningkat seperti 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.

Menurut David Icove [John D. Howard, "An Analysis Of Security Incidents On The Internet 1989 - 1995," PhD thesis, Engineering and Public Policy, Carnegie Mellon University, 1997.] berdasarkan lubang keamanan, keamanan dapat
diklasifikasikan menjadi empat, yaitu :

- Keamanan yang bersifat fisik(physical security), termasuk akses orang ke gedung peralatan, media yang digunakan dll. Contoh:
- Wiretapping, berhubungan dengan akses ke media kabel dan kompouter secara langsung.
- Denial of Service, dilakukan dengan mematikan peralatan atau membanjiri saluran komunikasi dengan pesan-pesan dengan jumlah yang besar.
- Syn Flood Attack, dimana sistem(host) yang dituju dibanjiri dengan permintaan sehingga menjadi sibuk dan mengakibatkan komputer menjadi macet(hang), disebabkan resource komputer yang terbatas.
- Keamanan yang berhubungan dengan orang(personel), contoh:
- Identifikasi username dan password
- Profil resiko dari orang yang mempunyai akses
- Keamanan dari data dan media serta teknik komunikasi.
- Keamanan dalam operasi, adanya prosedur yang digunakan untuk mengatur dan mengelola sistem keamanan termasuk prosedur setelah serangan(*post attack recovery*)

Dalam keamanan komputer terdapat beberapa aspek penting yang harus diperhatikan antara lain:

1. Privacy / Confidentiality

- Defenisi : menjaga informasi dari orang yang tidak berhak mengakses.
- Privacy : lebih kearah data-data yang sifatnya privat , Contoh : e-mail seorang pemakai (user) tidak boleh dibaca oleh administrator.
- Confidentiality : berhubungan dengan data yang diberikan ke pihak lain untuk keperluan tertentu dan hanya diperbolehkan untuk keperluan tertentu tersebut.

- Contoh : data-data yang sifatnya pribadi (seperti nama, tempat tanggal lahir, social security number, agama, status perkawinan, penyakit yang pernah diderita, nomor kartu kredit, dan sebagainya) harus dapat diproteksi dalam penggunaan dan penyebarannya.
- Bentuk Serangan : usaha penyadapan (dengan program sniffer).
- Usaha-usaha yang dapat dilakukan untuk meningkatkan privacy dan confidentiality adalah dengan menggunakan teknologi kriptografi.

2. Integrity

- Defenisi : informasi tidak boleh diubah tanpa seijin pemilik informasi.
- Contoh : e-mail di intercept di tengah jalan, diubah isinya, kemudian diteruskan ke alamat yang dituju.
- Bentuk serangan : Adanya virus, trojan horse, atau pemakai lain yang mengubah informasi tanpa ijin, "man in the middle attack" dimana seseorang menempatkan diri di tengah pembicaraan dan menyamar sebagai orang lain.

3. Authentication

- Defenisi : metoda untuk menyatakan bahwa informasi betul-betul asli, atau orang yang mengakses atau memberikan informasi adalah betul-betul orang yang dimaksud.
- Dukungan :
- Adanya Tools membuktikan keaslian dokumen, dapat dilakukan dengan teknologi watermarking(untuk menjaga "intellectual property", yaitu dengan menandai dokumen atau hasil karya dengan "tanda tangan" pembuat) dan digital signature.
- Access control, yaitu berkaitan dengan pembatasan orang yang dapat mengakses informasi. User harus menggunakan password, biometric (ciri-ciri khas orang), dan sejenisnya.

4. Availability

- Defenisi : berhubungan dengan ketersediaan informasi ketika dibutuhkan.
- Contoh hambatan :
- "denial of service attack" (DoS attack), dimana server dikirimi permintaan (biasanya palsu) yang bertubi-tubi atau permintaan yang diluar perkiraan sehingga tidak dapat melayani permintaan lain atau bahkan sampai down, hang, crash.
- mailbomb, dimana seorang pemakai dikirimi e-mail bertubi-tubi (katakan ribuan e-mail) dengan ukuran yang besar sehingga sang pemakai tidak dapat membuka e-mailnya atau kesulitan mengakses e-mailnya.

5. Access Control

- Defenisi : cara pengaturan akses kepada informasi, berhubungan dengan masalah authentication dan juga privacy.
- Metode : menggunakan kombinasi userid/password atau dengan menggunakan mekanisme lain.

6. Non-repudiation

- Defenisi : Aspek ini menjaga agar seseorang tidak dapat menyangkal telah melakukan sebuah transaksi. Dukungan bagi electronic commerce.

Menurut William Stallings[William Stallings, "Network and Internetwork Security," Prentice Hall, 1995.]terdapat beberapa serangan yang umum terjadi pada aspek keamanan komputer antara lain:

- Interruption : Perangkat sistem menjadi rusak atau tidak tersedia, aspek keamanan yang ditujukan adalah ketersediaan(availability) sistem.
- Contoh: "Denial of Service Attack".
- Interception : Sistem diakses oleh orang yang tidak berhak.
- Contoh: Penyadapan / Wiretapping.
- Modification : Pihak yang tidak berhak berhasil mengakses dan mengubah data.
- Contoh: mengubah isi website dengan pesan-pesan yang merugikan pemilik website.
- Fabrication : Pihak yang tidak berwenang menyisipkan objek palsu kedalam sistem seolah-olah sebagai pihak yang berhak.
- Contoh: mengirimkan email palsu sebagai orang lain.