# BAB I
# DASAR DASAR KEAMANAN KOMPUTER

## 1.1 Konsep Keamanan Komputer

Dalam dunia komunikasi data global dan perkembangan teknologi informasi yangsenantiasa berubah serta cepatnya perkembangan software, keamanan merupakan suatu isu yang sangat penting, baik itu keamanan fisik, keamanan data maupun keamanan aplikasi.Perlu kita sadari bahwa untuk mencapai suatu keamanan itu adalah suatu hal yang sangat mustahil, seperti yang ada dalam dunia nyata sekarang ini.Tidak ada satu daerah pun yang betul-betul aman kondisinya, walau penjaga keamanan telah ditempatkan di daerah tersebut, begitu juga dengan keamanan sistem komputer.Namun yang bisa kita lakukan adalah untuk mengurangi gangguan keamanan tersebut.

Sistem keamanan komputer bermanfaat menjaga suatu sistem komputer dari pengaksesan seseorang yang tidak berhak. Sistem keamanan komputer semakin dibutuhkan seiring dengan meningkatnya pengguna komputer saat ini. Selain itu makin meningkatnya para pengguna yang menghubungkan jaringan LANnya ke internet, namun tidak diimbangi dengan SDM yang dapat menjaga keamanan data dan infomasi yang dimiliki. Sehingga keamanan data yang ada menjadi terancam untuk diakses dari orang-orang yang tidak berhak. Keamanan komputer menjadi penting karena ini terkait dengan Privacy, Integrity, Autentication, Confidentiality dan Availability. Beberapa ancaman keamanan komputer adalah virus, worm, trojan, spam dan lain-lain. Masing-masingnya memiliki cara untuk mencuri data bahkan merusak sistem komputer yang ada. Ancaman bagi keamanan sistem komputer ini tidak bisa dihilangkan begitu saja, namun kita dapat meminimalisasi hal ini adalah dengan menggunakan software keamanan sistem antara lain antivirus, antispam dan sebagainya.

## 1.2 Pengertian Keamanan Komputer

Keamanan komputer adalah suatu cabang teknologi yang dikenal dengan nama keamananinformasi yang diterapkan pada komputer. Sasaran keamanan komputer antara lain adalah sebagai perlindungan informasi terhadap pencurian atau korupsi, atau pemeliharaan ketersediaan,seperti dijabarkan dalam kebijakan keamanan.

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.[1]

Menurut **Howard** (1997) 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. Keamanan dalam sistem komputer sangat berpengaruh terhadap beberapa faktor di bawah ini diantaranya adalah :

1. Social engineering
2. Security hole pada sistem operasi dan servis
3. Keamanan fisik

4. Serangan pada jaringan
5. DOS attack
6. Serangan via aplikasi berbasis web
7. Trojan, backdoor, rootkit, keylogger
8. Virus, worm
9. Anatomy of A Hack

Menurut **Wicak** dalam bukunya “mengamankan komputer dari Spywere: 2007” Keamanan dari data dan media serta teknik komunikasi (Communication security). Tipe keamanan jenis ini banyak menggunakan kelemahan yang ada pada perangkat lunak, baik perangkat lunak aplikasi ataupun perangkat lunak yang diugunakan dalammengelola sebuah database.[2]

Dalam keamanan sistem komputer yang perlu kita lakukan adalah untuk **mempersulit orang lain mengganggu sistem yang kita pakai,** baik menggunakan komputer yang sifatnya sendiri, jaringan local maupun jaringan global. Harus dipastikan system bisa berjalan dengan baik dan kondusif, selain itu program aplikasinya masih bisa dipakai tanpa ada masalah.

### 1.3 Penyebab Meningkatnya Kejahatan Komputer

[3]Penyebab meningkatnya kejahatan komputer yaitu:

1. Meningkatnya aplikasi berbasis IT dan jaringan komputer, seperti : online banking, e-commerce, Electronic data Interchange (EDI).
2. Desentralisasi server sehingga lebih banyak system yang harus ditangani, sementara SDM terbatas. Seperti lemahnya keamanan ketika terjadi pemindahan data.
3. Transisi dari single vendor ke multi vendor, seperti: ada 2 server dalam 1 vendor.
4. Meningkatnya kemampuan pemakai (user).
5. Lemahnya hukum IT yaitu kesulitan penegak hukum dan belum adanya ketentuan yang pasti.
6. Kompleksitas sistem yang digunakan, seperti pada penginstallan aplikasi yang tidak kompleks/tidak selesai
7. Koneksi internet yang lemah tingkat security nya.
8. Banyaknya software yang pada awalnya digunakan untuk melakukan audit sebuah system dengan cara mencari kelemahan dan celah yang mungkin disalahgunakan untuk melakukan scanning system orang lain.
9. Banyaknya software-software untuk melakukan penyusupan yang tersedia di Internet dan bisa di download secara gratis.

[2]**Cybercrime** dapat didefinisikan sebagai perbuatan melanggar hukum yang dilakukan dengan menggunakan fasilitas internet dengan menggunakan teknologi komputer dan telekomunikasi.

### 1.4 Kebutuhan Keamanan Komputer

[4]Alasan kenapa keamanan komputer 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)

Ada beberapa hal penyebab keamanan komputer dibutuhkan, seperti:

1. Mengurangi resiko ancaman, hal ini biasa berlaku di institusi dan perusahaan swasta.
2. Melindungi system dari kerentanan, kerentanan akan menjadikan system berpotensi untuk memberikan akses yang tidak diizinkan bagi orang lain yang tidak berhak.
3. Melindungi system dari gangguan alam seperti petir dan lain-lainnya.

## 1.5 Klasifikasi Keamanan Komputer

[3]Klasifikasi keamanan menurut **John D. Howard, 1997** yaitu:

1. **Keamanan yang bersifat fisik (physical security):** termasuk akses orang ke gedung, peralatan, dan media yang digunakan.
   Contoh :
   a. Wiretapping atau hal-hal yang ber-hubungan dengan akses ke kabel atau komputer yang digunakan.
   b. Denial of service, dilakukan misalnya dengan mematikan peralatan atau membanjiri saluran komunikasi dengan pesan-pesan (yang dapat berisi apa saja karena yang diutamakan adalah banyaknya jumlah pesan).
   c. Syn Flood Attack, dimana sistem (host) yang dituju dibanjiri oleh permintaan sehingga dia menjadi ter-lalu sibuk dan bahkan dapat berakibat macetnya sistem (hang).
2. **Keamanan yang berhubungan dengan orang (personel)**, Contoh :
   a. Identifikasi user (username dan password)
   b. Profil resiko dari orang yang mempunyai akses (pemakai dan pengelola).
3. [5]**Keamanan dari data dan media serta teknik komunikasi (communications)**. yang termasuk di dalam kelas ini adalah kelemahan dalam software yang digunakan untuk mengelola data. Seorang kriminal dapat memasang virus atau trojan horse sehingga dapat mengumpulkan infor- masi (seperti password) yang semestinya tidak berhak diakses.
4. **Keamanan dalam operasi**: Adanya prosedur yang digunakan untuk mengatur dan mengelola sistem keamanan, dan juga ter-masuk prosedur setelah serangan (post attack recovery).

## 1.6 Karakterisitik Penyusup

[6]Macam – macam karakteristik penyusup, yaitu :

**a. The Curious (Si Ingin Tahu)**
Tipe penyusup ini pada dasarnya tertarik menemukan jenis sistem dan data yang digunakan.

**b. The Malicious (Si Perusak)**

Tipe penyusup ini ingin merusak system yang digunakan atau mengubah tampilan layar yang dibuat.

**c. The High-Profile Intruder (Si Profil Tinggi)**
Tipe penyusup ini penyusup ini menggunakan system untuk mencapai popularitas dia sendiri, semakin tinggi system keamanan yang kita buat, semakin membuatnya penasaran. Jika dia berhasil masuk ke sistem kita maka ini menjadi sarana baginya untuk mempromosikan diri.

**d. The Competition (Si Pesaing)**
penyusup ini lebih tertarik pada data yang ada dalam system yang kita miliki, karena dia menganggap kita memiliki sesuatu yang dapat menguntungkannya secara finansial atau malah merugikannya (penyusup).

### 1.7 Fase Seorang Hacker

Istilah bagi hacker (penyusup) :

1. **Mundane**
   Tahu mengenai hacking tapi tidak mengetahui metode dan prosesnya.
2. **lamer (script kiddies)**
   Mencoba script2 yang pernah di buat oleh aktivis hacking, tapi tidak paham bagaimana cara membuatnya.
3. **Wannabe**
   Paham sedikit metode hacking, dan sudah mulai berhasil menerobos.
4. **larva (newbie)**
   Hacker pemula, teknik hacking mulai dikuasai dengan baik, sering bereksperimen.
5. **Wizard**
   Hacker yang membuat komunitas pembelajaran di antara mereka.
6. **Master of the master hacker**
   Lebih mengarah ke penciptaan tools-tools yang powerfull yang salah satunya dapat menunjang aktivitas hacking, namun lebih jadi tools pemrograman system yang umum.

### 1.8 Aspek Keamanan Komputer

[7]Menurut Garfinkel [Simson Garfinkel, "*PGP: Pretty Good Privacy,*" O'Reilly & Associ-ates, Inc., 1995.]

1. **Privacy / Confidentiality**
   a. Defenisi : menjaga informasi dari orang yang tidak berhak mengakses.
      **1) Privacy** : lebih kearah data-data yang sifatnya privat , Contoh : e-mail seorang pemakai (user) tidak boleh dibaca oleh administrator.
      **2) Confidentiality** : berhubungan dengan data yang diberikan ke pihak lain untuk keperluan tertentu dan hanya diperbolehkan untuk keperluan tertentu tersebut.
   b. 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.
   c. Bentuk Serangan : usaha penyadapan (dengan program sniffer).
   d. Usaha-usaha yang dapat dilakukan untuk meningkatkan privacy dan confidentiality adalah dengan menggunakan teknologi kriptografi.

2. **Integrity**
   a. Defenisi : informasi tidak boleh diubah tanpa seijin pemilik informasi.
   b. Contoh : e-mail di intercept di tengah jalan, diubah isinya, kemudian diteruskan ke alamat yang dituju.
   c. 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**
   a. Defenisi : metode untuk menyatakan bahwa informasi betul-betul asli, atau orang yang mengakses atau memberikan informasi adalah betul-betul orang yang dimaksud.
   b. Dukungan :
      1. 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.
      2. Access control, yaitu berkaitan dengan pembatasan orang yang dapat mengakses informasi. User harus menggunakan password, biometric (ciri-ciri khas orang), dan sejenisnya.

4. **Availability**
   a. Defenisi : berhubungan dengan ketersediaan informasi ketika dibutuhkan.
   b. Contoh hambatan :
      1) **“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.
      2) **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**
   a. Defenisi : cara pengaturan akses kepada informasi. berhubungan dengan masalahauthentication dan juga privacy
   b. Metode : menggunakan kombinasi userid/password atau denganmenggunakan mekanisme lain.

6. **Non-repudiation**
   a. Defenisi : Aspek iniberhubungan dengan si pengirim. Tujuannya agar seseorangtidak dapat mengelak bahwa dialah yang mengirim informasi tersebut.
   b. Contoh ancaman : Penyangkalan pesanan melalui email

c. Solusi : Digital signature, certificate dan kriptografi

**Soal**

1. Apa yang dimaksud dengan keamanan komputer?
2. Sebutkan 5 penyebab meningkatnya kejahatan komputer?