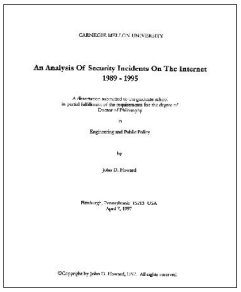
Keamanan Komputer (2)

Definisi **Keamanan Komputer**

- Menurut John D. Howard dalam Desertasinya *"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**."


CARNEGIE MELLON UNIVERSITY

An Analysis Of Security Incidents On The Internet 1989 - 1995

A dissertation submitted to Carnegie Mellon in partial fulfillment of the requirements for the degree of Doctor of Philosophy

in

Engineering and Public Policy

by

John D. Howard

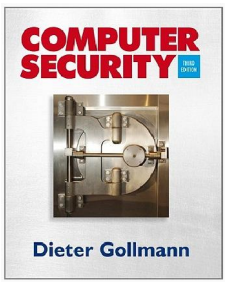
Pittsburgh, Pennsylvania, 15213 USA

April 7, 1997

©Copyright by John D. Howard, 1997. All rights reserved.

Definisi **Keamanan Komputer (2)**

- 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.**"



Kenapa Butuh **Keamanan Komputer ?**

- **"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**)

Aspek Keamanan Komputer

Privacy, Confidentiality, Integrity, Autentication dan Availability

Aspek Keamanan Komputer (1)

1. **Privacy,** adalah sesuatu yang bersifat rahasia(*private*). Intinya adalah pencegahan agar informasi tersebut tidak diakses oleh orang yang tidak berhak. Contohnya : email atau file-file lain yang tidak boleh dibaca orang lain meskipun oleh administrator. **Pencegahan** yang mungkin dilakukan adalah dengan menggunakan teknologi enksripsi, jadi hanya pemilik informasi yang dapat mengetahui informasi yang sesungguhnya.

Aspek Keamanan Komputer (2)

2. **Confidentiality,** merupakan data yang diberikan ke pihak lain **untuk tujuan khusus tetapi tetap dijaga penyebarannya**. *Confidentiality* akan terlihat apabila diminta untuk membuktikan kejahatan seseorang, apakah pemegang informasi akan memberikan infomasinya kepada orang yang memintanya atau menjaga clientnya.

Aspek Keamanan Komputer (3)

3. **Integrity,** penekanannya adalah sebuah informasi **tidak boleh diubah** kecuali oleh pemilik informasi. Contoh : Penyerangan Integritas ketika sebuah email dikirimkan ditengah jalan disadap dan diganti isinya, sehingga email yang sampai ketujuan sudah berubah.

Aspek Keamanan Komputer (4)

4. **Autentication,** ini akan dilakukan sewaktu user login dengan menggunakan nama **user dan passwordnya**, apakah cocok atau tidak, jika cocok diterima dan tidak akan ditolak. *Ini biasanya berhubungan dengan hak akses seseorang, apakah dia pengakses yang sah atau tidak.*

Aspek Keamanan Komputer (5)

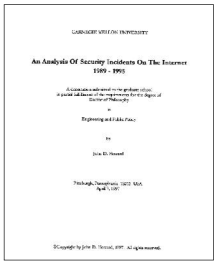
5. **Availability,** aspek ini berkaitan dengan apakah sebuah data tersedia saat dibutuhkan/diperlukan. Apabila sebuah data /informasi terlalu ketat pengamanannya akan menyulitkan dalam akses data tersebut.
Serangan yang sering dilakukan pada aspek ini adalah *denial of service (DoS),* yaitu penggagalan service sewaktu adanya permintaan data sehingga komputer tidak bisa melayaninya.
Contoh lain dari DoS ini adalah mengirimkan request yang berlebihan sehingga menyebabkan komputer tidak bisa lagi menampung beban tersebut dan akhirnya komputer down.

Kenapa Kejahatan Komputer **Meningkat?**

Kenapa Kejahatan Ada & Meningkat?

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

Klasifikasi Kejahatan Komputer?


An Analysis Of Security Incidents On The Internet
1989 - 1995

Menurut John D. Howard, dalam bukunya *"An Analysis Of Security Incidents On The Internet 1989 - 1995,"* PhD thesis, Engineering and Public Policy, Carnegie Mellon University, 1997. Keamanan dapat diklasifikasikan menjadi 4 : ***physical security, personel, communications dan operasi***

Klasifikasi Kejahatan Komputer (1)

1. **Keamanan yang bersifat fisik *(physical security)* :** Pengaksesan orang ke gedung, peralatan, dan media yang digunakan.
   Wiretapping atau hal-hal yang ber-hubungan dengan akses ke kabel atau komputer yang digunakan juga dapat dimasukkan ke dalam kelas ini.
   Denial of service, misalnya dengan mematikan peralatan atau membanjiri saluran komunikasi dengan pesan-pesan (banyaknya jumlah pesan).
   Sync Flood Attack, dimana system yang dituju dibanjiri oleh permintaan sehingga dia menjadi ter-lalu sibuk dan bahkan dapat berakibat macetnya sistem (*hang*).
   Pencurian Komputer/laptop, Hilang data secara fisik. 15% perusahaan US pernah hilang laptop
   Memaatikan Listrik, Penyebab hilangnya data dan rusaknya sistem

Klasifikasi Kejahatan Komputer (2)

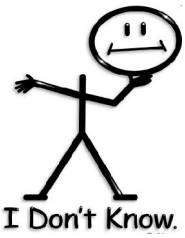
2. **Keamanan yang berhubungan dengan orang (personel).** Identifikasi user (username dan password), dan Profil resiko dari orang yang mempunyai akses (pemakai dan pengelola). Ada sebuah teknik yang dikenal dengan istilah **"social engineering"** yang sering digunakan oleh kriminal untuk berpura-pura sebagai orang yang berhak mengakses informasi.

Klasifikasi Kejahatan Komputer (3)

3. **Keamanan dari data dan media serta teknik komunikasi (*communications*).** Kelemahan dalam software yang digunakan untuk mengelola data. Seorang kriminal dapat memasang **virus** atau **Trojan horse** sehingga dapat mengumpulkan informasi (seperti password) yang semestinya **tidak berhak diakses.**

Klasifikasi Kejahatan Komputer (4)

4. **Keamanan dalam operasi**
   Adanya prosedur dan **kebijakan** yang digunakan untuk mengatur dan mengelola sistem keamanan, dan juga termasuk prosedur setelah serangan *(post attack recovery). Seringkali perusahaan tidak memiliki dokumen kebijakan dan prosedur.*



Sistem Keamanan Komputer

*Suatu sistem dengan tujuan untuk mengamankan komputer, data dan infrastruktur dari **serangan pihak luar**, baik berupa serangan virus, spyware, rootkit, trojan dan kejahatan lainnya*

Komponen Pengaman Sistem ?

1. **Anti virus.**
   *Anti-Virus sebuah software untuk membasmi berbagai macam virus. Harus pandai memilih Anti-Virus, meskipun banyak jenis dan nama, tentu Anti-Virus juga dapat kekurangan. Untuk itu usahakan Anti-Virus selalu **terupdate**.*

2. **Anti-Spyware.**
   *Karena memang sifat **spyware** dan virus ini berbeda, sehingga anti virus tidak bisa menangani spyware dengan baik. Seperti halnya anti virus, anti spyware juga haruslah terupdate tiap sa dan memiliki fasilitas real time protection. Apapun anti spywar yang anda pakai, sebaiknya memiliki fasilitas di atas.*

3. **Firewall.**
   *Firewall ini melindungi dari tangan- tangan jahil di **network** anda. Jadi jika komputer anda hanya single alone, dipakai di rumah, maka firewall bisa diabaikan. Untuk firewall, anda bisa memakai bawaan windows, atau jika anda ingin yang lebih fleksible dan aman, anda bisa menggunakan firewall lain.*