Pengantar Keamanan Sistem Informasi

Keamanan Sistem

1. Pentingnya Keamanan Sistem
2. Tantangan Keamanan Sistem
3. Pengelolaan Keamanan Sistem
4. Penyebab Peningkatan Masalah Keamanan Sistem
5. Klasifikasi Keamanan Sistem
6. Aspek-aspek Keamanan Sistem
7. Serangan Terhadap Keamanan Sistem

Pentingnya Keamanan Sistem

- Latar belakang :

Keinginan memberikan informasi secara cepat dan akurat melalui media komputer

- Cara :

Menggunakan jaringan komputer global

- Tantangan :

Bagaimana kita dapat mencegah (atau minimalnya mendeteksi) penipuan / kecurangan di sebuah sistem

Tantangan Keamanan Sistem

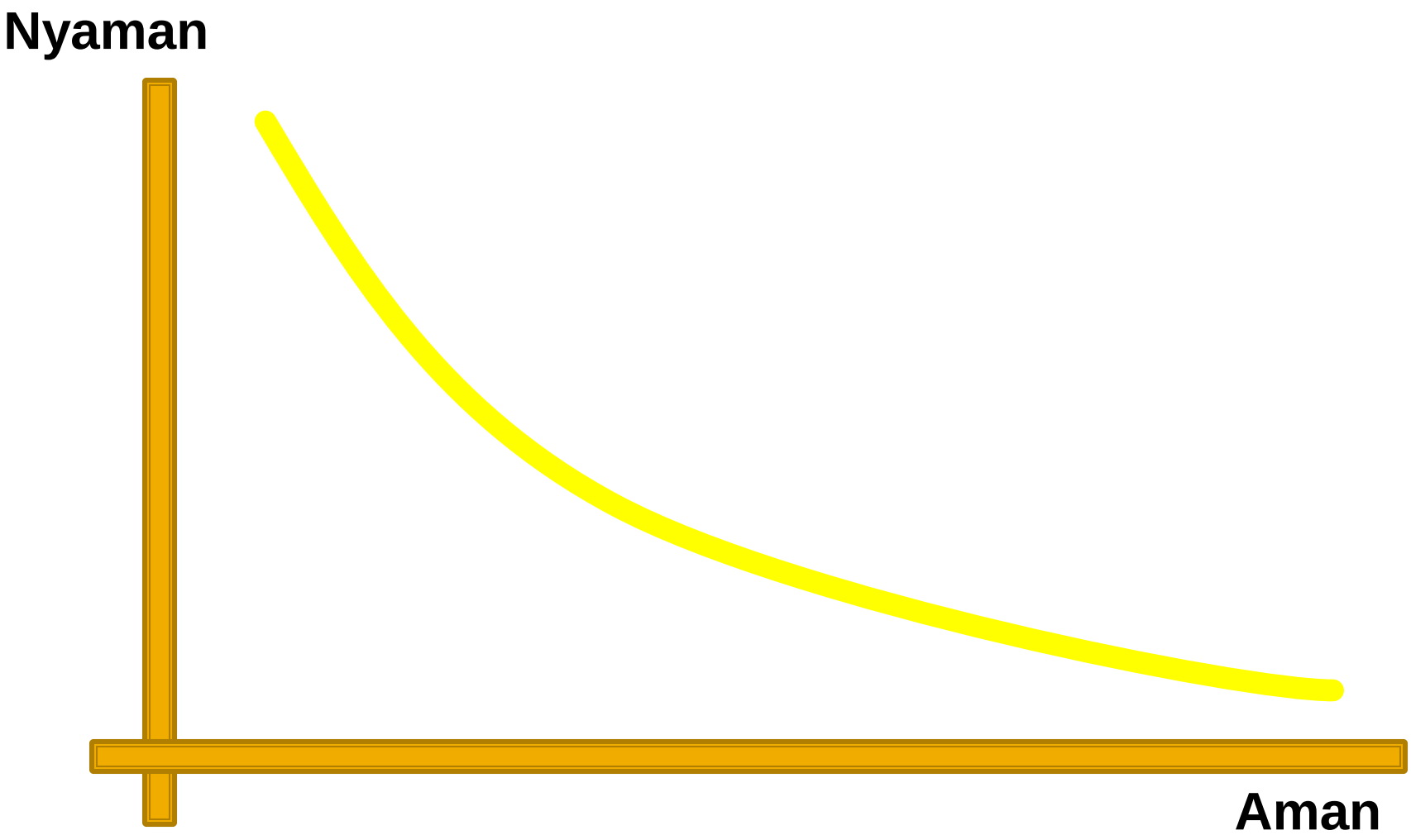
- Ketidakpedulian manajemen perusahaan
  - Lebih mementingkan *reducing cost*
- Tidak adanya perencanaan awal
  - Kebutuhan *budget* yang besar secara tiba-tiba
- Keuntungan tak terlihat
  - Keuntungan yang tidak bisa diukur dengan uang (intangible)
- Mengurangi kenyamanan
  - *Comfort or Secure ?*

Tantangan Keamanan Sistem
Tangible vs Intangible

- Apakah keamanan adalah sesuatu yang tidak bisa diukur dengan uang ?
  Pertimbangkan kerugian yang terjadi jika :
  - Sistem tidak bekerja *(down)*
    - 1 X 24 Jam ? 7 hari ?
  - Ada kesalahan informasi
    - Informasi dirubah ?
  - Ada data yang hilang
    - Data pelanggan hilang ? Invoice hilang ?
  - Nama baik perusahaan
    - Web dirubah ?

Tantangan Keamanan Sistem

Keamanan vs Kenyamanan



Pengelolaan Keamanan Sistem

Menggunakan Risk Management System untuk pengelolaan Risk (resiko)

3 komponen yang memberikan kontribusi resiko :

1. Assets (aset)
2. Vulnerabilities (kelemahan)
3. Threats (ancaman)

Pengelolaan Keamanan Sistem

1. Assets (aset)

   (hardware, software, dokumentasi, data, komunikasi, lingkungan, manusia)

2. Threat (ancaman)

   (pemakai, teroris, kecelakaan, crackers, penjahat kriminal, nasib, intel luar negeri)

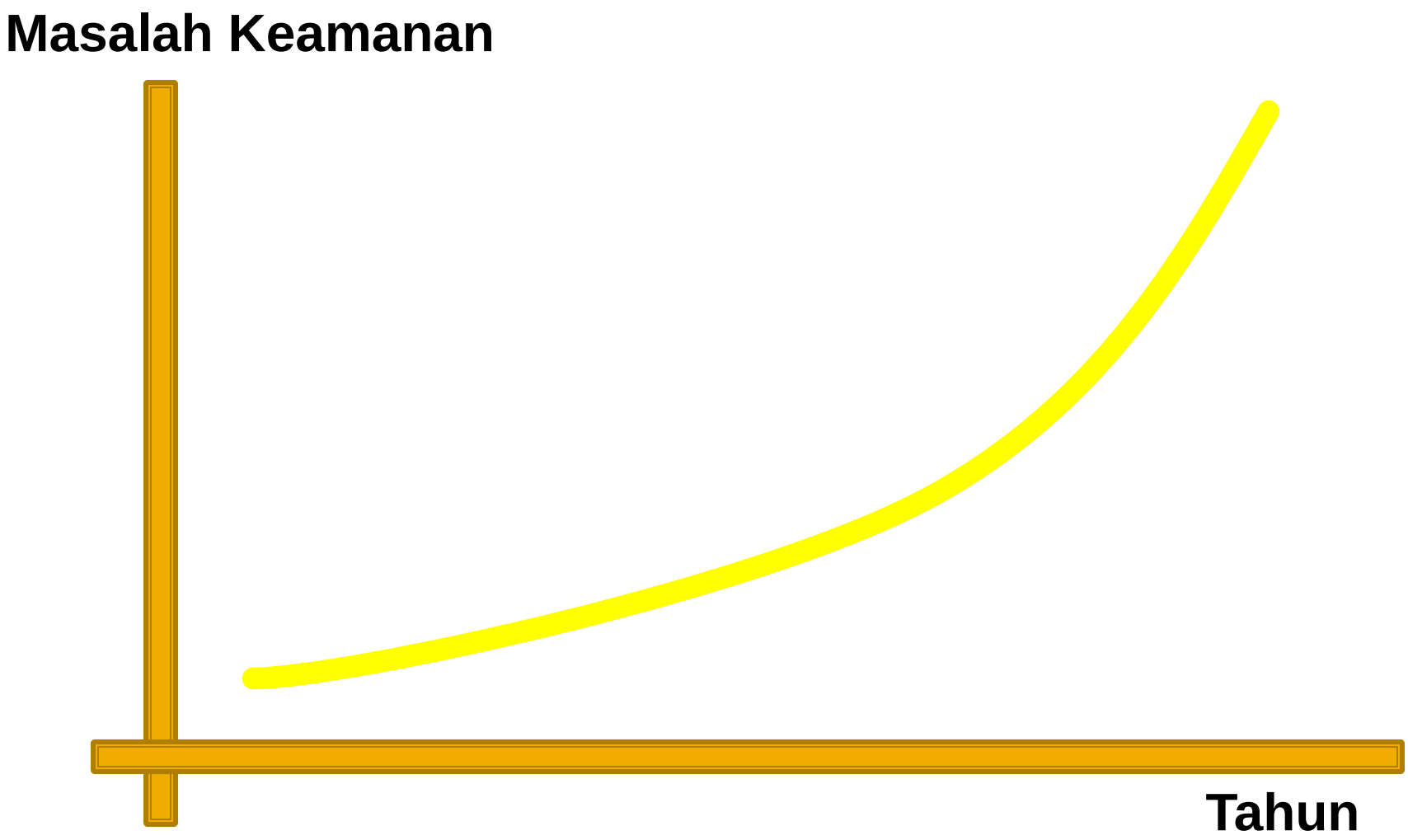
3. Vulnerabilities (kelemahan)

   (software bugs, hardware bugs, radiasi, tapping, crosstalk, unauthorized users, hardcopy, keteledoran, cracker via telepon, storage media)

Pengelolaan Keamanan Sistem

- Usaha penanggulangan resiko (countermeasures) yang dapat dilakukan :
  - Mengurangi Ancaman (threat)
  - Mengurangi Kelemahan (vulnerabilities)
  - Mengurangi Dampak (impact)
  - Mendeteksi Kejadian (hostile event)
  - Proses pemulihan (recover)

Penyebab peningkatan masalah keamanan Sistem



Penyebab peningkatan masalah keamanan Sistem

- Aplikasi bisnis berbasis IT dan bersifat jaringan semakin meningkat
- Desentralisasi / distributed server
- Hardware dan software dari multi-vendor
- Kepandaian pemakai komputer meningkat
- Mudahnya diperoleh software untuk melakukan penyerangan
- Kesulitan dari penegak hukum
- Semakin kompleksnya sistem
- Semakin banyaknya perusahaan yang menghubungkan sistem informasinya dengan jaringan global

Penyebab peningkatan masalah keamanan Sistem

Sistem berbasis Internet semakin populer.

Alasan :

- Open platform
- Media yang ekonomis

Ancaman :

- Jaringan global
- Informasi melewati titik-titik yang berada di luar kontrol

Klasifikasi Keamanan

Klasifikasi berdasarkan lubang keamanan :

1. Keamanan fisik

   - Sobekan password / manual, penyadapan, DoS

2. Keamanan orang

   - Social Engineering

3. Keamanan data, media dan teknik komunikasi

   - Kelemahan Software

4. Keamanan operasi

   - Prosedur dan kebijakan

Aspek-Aspek Keamanan

6 Aspek Keamanan Komputer :

1. Privacy / Confidentiality
2. Integrity
3. Authentication
4. Availability
5. Access Control
6. Non-repudiation

Aspek-Aspek Keamanan

1. **Privacy / Confidentiality**

Usaha untuk menjaga informasi dari orang yang tidak berhak mengakses

Contoh ancaman :

- (Privacy) Email anggota tidak boleh dibaca oleh administrator server
- (Confidentiality) Data pelanggan sebuah ISP dijaga kerahasiaannya

Solusi :

- Kriptografi (enkripsi dan dekripsi)

Aspek-Aspek Keamanan

2. Integrity

Informasi tidak boleh diubah tanpa seijin pemilik informasi.

Contoh ancaman :

- Trojan, virus, man in the middle attack
- Pengubahan isi email

Solusi :

- Enkripsi
- Digital Signature

Aspek-Aspek Keamanan

3. Authentication

Metoda untuk menyatakan bahwa informasi betul-betul asli.

Contoh ancaman :

- Dokumen palsu, pengguna palsu

Solusi :

- Watermarking, digital signature
- Access Control (What you have/know/are ?)
- Digital certificate

Aspek-Aspek Keamanan

4. Availibility

Ketersediaan informasi ketika dibutuhkan.

Contoh ancaman :

- DoS
- Mailbomb

Solusi :

- Spam blocker
- Connection limit

Aspek-Aspek Keamanan

5. Access Control

Cara pengaturan akses kepada informasi

Contoh ancaman :

- Pengubahan data anggota oleh orang yang tidak berhak

Solusi :

- Membagi user dengan tingkatan (guest, operator, admin)

Aspek-Aspek Keamanan

6. Non-repudiation

Menjaga agar seseorang tidak dapat menyangkal telah melakukan sebuah transaksi.

Contoh ancaman :

- Penyangkalan pesanan melalui email

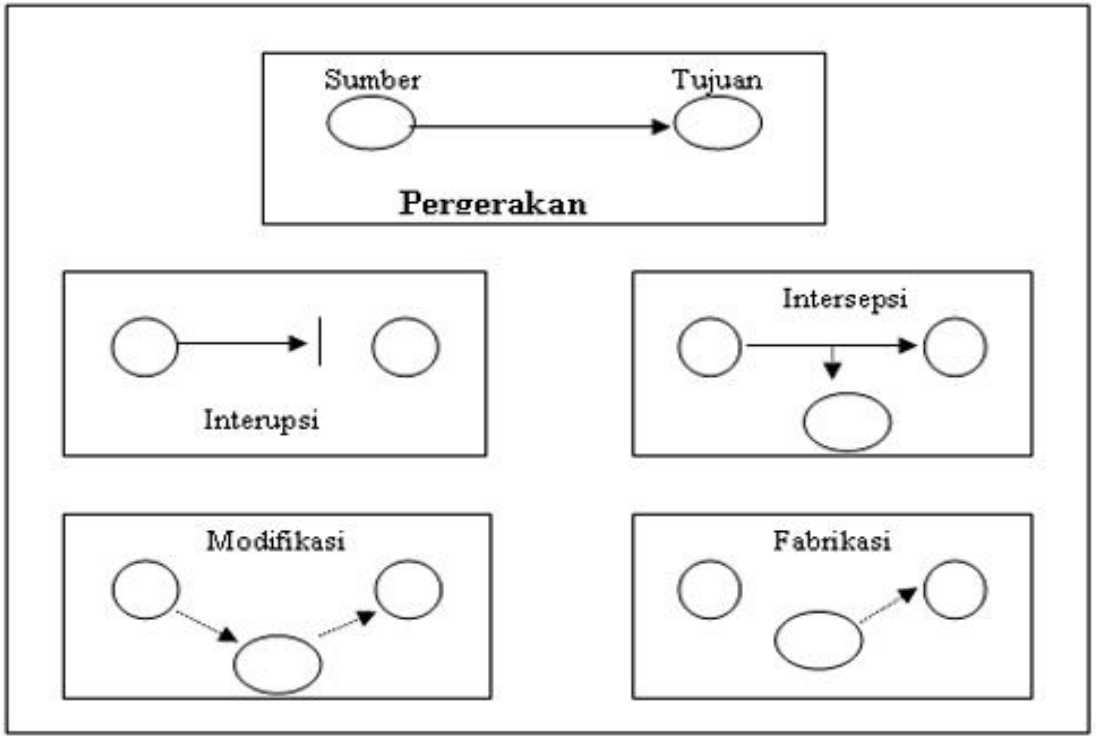
Solusi :

- Digital signature, certificate dan kriptografi

Serangan terhadap Keamanan

4 jenis serangan :

1. Interruption
2. Interception
3. Modification
4. Fabrication



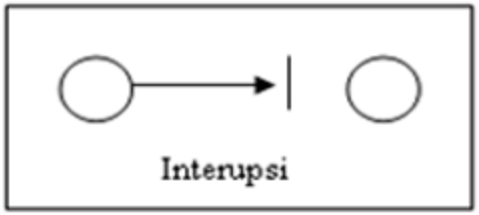
Serangan terhadap Keamanan

1. Interruption

Perangkat sistem menjadi rusak / tidak tersedia

Contoh :

- DoS attack



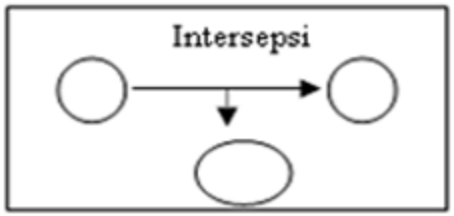
2. Interception

Pihak tak berwenang berhasil mengakses

aset/informasi

Contoh :

- Penyadapan



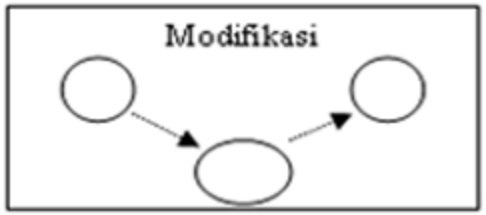
Serangan terhadap Keamanan

3. Modification

Pihak tak berwenang dapat mengubah aset

Contoh :

- Pengubahan isi website

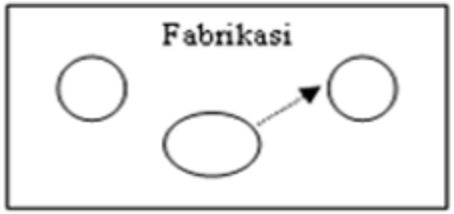


4. Fabrication

Pihak tak berwenang menyisipkan objek palsu ke dalam sistem

Contoh :

- Email palsu



Tugas (kerjakan 2 orang)

Carilah sebuah Sistem yang tersambung dengan jaringan internet, kemudian lakukan analisa mengenai 2 hal berikut :

1. Implementasi Aspek-aspek Keamanan pada sistem tersebut
2. Kemungkinan Serangan Terhadap Keamanan Sistem tersebut