

Keamanan Sistem Informasi



TKB7351 - Keamanan Informasi & Jaringan
TKB7358 - Keamanan Sistem Informasi



Chalifa Chazar
<http://script.id>
chalifa.chazar@gmail.com

Last update : Juli 2017 | chalifa.chazar@gmail.com

“Prevention is better
than cure”

Keamanan Sistem Informasi

- Keamanan informasi adalah bagaimana kita dapat mencegah penipuan (*cheatting*), atau paling tidak mendeteksi adanya penipuan di sebuah sistem yang berbasis informasi (G. J. Simons)

Aspek Keamanan SI (Garfinkel)

- *Integrity*
- *Confidentiality*
- *Availability*
- *Authentication*

Integrity

- Aspek ini menekankan bahwa informasi tidak boleh diubah tanpa seijin pemilik informasi
- Permasalahan: trojan horse

Confidentiality

- Usaha untuk menjaga informasi dari orang yang tidak berhak mengakses
- Permasalahan: usaha melakukan penyadapan (dengan program *sniffer*)

Availability

- Berhubungan dengan ketersediaan informasi saat dibutuhkan
- Permasalahan: *denial of service attack*

Authentication

- Aspek ini berhubungan dengan metoda untuk menyatakan bahwa informasi betul-betul asli
- Permasalahan :
 - Watermarking & digital signature
 - Access control, membatasi orang yang mengakses informasi

Masalah yang dihadapi

- Seberapa jauh keamanan harus diterapkan?
- Berapa biaya yang harus dikeluarkan?
- Apakah dampak yang timbul dengan menerapkan ekstra keamanan dalam hal efisiensi dan fleksibilitas dari sistem komputer?

Strategi Keamanan SI

- Informasi dikatakan aset penting bagi keberhasilan perusahaan
- Melindungi teknologi (software&hardware) dari serangan dan ancaman
- Keamanan SI bukan sekedar masalah pengendalian dari sisi teknologi, tapi penerapan kebijakan dan standar yang baik untuk menentukan arah keamanan SI
- Bisnis elektronik membutuhkan kepercayaan bisnis
- Kebutuhan untuk *long term*

Kebijakan Keamanan SI

- Keamanan SI merupakan urusan dan tanggung jawab semua karyawan
- Penetapan pemilik sistem informasi
- Langkah keamanan harus sesuai dengan peraturan dan undang-undang
- Antisipasi terhadap kesalahan
- Pengaksesan ke dalam sistem harus berdasarkan kebutuhan fungsi
- Hanya data bisnis yang ditekuni perusahaan yang diperbolehkan untuk di proses di sistem komputer
- Pekerjaan yang dilakukan oleh pihak ketiga

- Pemisahan aktivitas antara pengembang sistem, pengoperasian sistem, dan pemakai akhir SI
- Implementasi sistem baru atau permintaan perubahan terhadap sistem yang sudah ada harus melalui pengontrolan yang ketat melalui prosedur sistem akseptasi dan permintaan perubahan
- Sistem yang dikembangkan harus sesuai dengan standar metode pengembangan sistem yang diemban oleh organisasi
- Pemakai bertanggung jawab penuh atas semua aktivitas yang dilakukan dengan memakai kode identitasnya (user ID)

</THANKS>

Chalifa Chazar

<http://script.id>

Email: chalifa.chazar@gmail.com

