Keamanan Sistem Informasi

TKB4364 - Keamanan Informasi & Jaringan

Nama |Chalifa Chazar
Modul | http://script.id
Email | chalifa.chazar@gmail.com

Last update : Januari 2022 | chalifa.chazar@gmail.com

“Prevention is better than cure”

Keamanan vs Kenyamanan

- Semakin tinggi tingkat keamanan semakin mahal biaya yang diperlukan
- Semakin tinggi tingkat keamanan semakin rendah tingkat kenyamanan
- Saat ini kita sudah berada pada "information-based society"
- Kemampuan dalam mengakses dan menyediakan informasi secara cepat dan akurat menjadi sangat esensial bagi sebuah organisasi (tidak hanya organisasi komersial, perguruan tinggi, pemerintahan, maupun individual)

Keamanan 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 Informasi

- **Integrity (Integritas)**
- **Confidentiality (Kerahasiaan)**
- **Availability (Ketersediaan)**
- **Authentication (Keaslian)**

Integrity

- Aspek ini menekankan bahwa informasi tidak boleh diubah tanpa seijin pemilik informasi

- Ancaman: Trojan horse, Man in the middle attack, dll
- Pencegahan: .....

Confidentiality

- Usaha untuk menjaga informasi dari orang yang tidak berhak mengakses
- Menurut ISO 17799, confidentiality adalah memastikan informasi hanya dapat diakses oleh orang yang berwenang atau orang yang memiliki otoritas

- Ancaman: usaha penyadapan (dengan menggunakan program sniffer)
- Pencegahan: ...

Availability

- Berhubungan dengan ketersedian informasi saat dibutuhkan
- Menurut ISO 17799, availability adalah kepastian tersedianya informasi pada saat yang dibutuhkan oleh orang yang berwenang untuk mengetahui dan mengakses data

- Ancaman: Distributed Denial of Service attack (DDoS Attack)
  - Ping of the Death
  - Syn flooding
  - Remote controled attack
- Pencegahan: ...

Authentication

- Aspek ini berhubungan dengan metoda untuk menyatakan bahwa informasi betul-betul asli

- Pencegahan:
  - 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?

Keamanan Informasi

- Informasi ialah aset yang sangat penting dalam suatu perusahaan, oleh karena itu, informasi harus dapat dilindungi
- Informasi bisa berbentuk dalam hardcopy, penyimpanan secara digital, visual (video, diagram), ditampilkan di website, verbal percakapan, panggilan telpon), dan sebagainya
- Informasi dapat dibuat, dimiliki, disimpan, diproses, dikirim, digunakan, dimodifikasi, dibagikan, dan dihapus
- Sedangkan, keamanan informasi adalah bagaimana cara membuat informasi yang bernilai terhindar dari bahaya
- Keamanan Informasi bukan sekedar masalah pengendalian dari sisi teknologi, tapi penerapan kebijakan dan standar yang baik untuk menentukan arah keamanan informasi
- Bisnis elektronik membutuhkan kepercayaan bisnis
- Keamanan Informasi merupakan kebutuhan untuk *long term*

Langkah-Langkah Keamanan Informasi

- Mengevaluasi ancaman terhadap informasi
- Memproteksi CIAA (Confidentiality, Integrity, Availability, Authentication)
- Menghindari, mencegah dan mendeteksi kejadian-kejadian yang tidak terduga
- Mengamankan orang, proses, dan teknologi tidak hanya pada IT saja

Dasar Manajemen Keamanan Informasi

Strategi dari keamanan informasi meliputi tujuh aspek kategori, yaitu :

1. **Physical security** yang membahas bagaimana pengamanan terhadap perangkat keras, perangkat lunak, dan data terhadap ancaman physical untuk mengurangi atau mencegah terganggunnya operasi, pelayanan, dan/atau hilangnya aset berharga.
2. **Communication security (COMSEC)** yang bertujuan untuk mengamankan media komunikasi beserta isinya, sehingga tidak terjadinya penyadapan atau modifikasi terhadap data.
3. **Computer security (COMPUSEC),** mencegah, mendeteksi, dan meminimalisir ancaman akibat dari pengguna yang tidak berwenang terhadap sistem komputer.
4. **Information security (INFOSEC)** adalah perlindungan informasi terhadap pengguna yang tidak berwenang, serta perlindungan perusakan, baik yang disengaja maupun yang tidak disengaja.
5. **System safety** didefinisikan sebagai penerapan teknik dan manajemen prinsip, kriteria, dan teknik untuk mengatasi risiko kecelakaan operasional, waktu, dan biaya, dari seluruh fase siklus sistem yang ada.
6. **System reliability** didefinisikan sebagai pengukuran akan perangkat lunak apakah menghasilkan keluaran yang akurat atau tidak dan konsisten secara berulangulang, baik dalam kondisi baik, sedang, atau buruk.

Kebijakan Keamanan Informasi

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

Kebijakan Keamanan Informasi

- Pemisahan aktivitas antara pengembang sistem, pengoperasian sistem, dan pemakai akhir sistem
- 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