Materi 2

Keamanan Sistem Informasi

3 SKS | Semester 8 | S1 Sistem Informasi | UNIKOM | 2015
Nizar Rabbi Radliya | nizar.radliya@yahoo.com

Nama Mahasiswa	
NIM	
Kelas	

Kompetensi Dasar

Memahami konsep dasar keamanan sistem informasi.

Pokok Bahasan

Konsep Dasar Keamanan Sistem Informasi
1. Tujuan keamanan sistem informasi
2. Aset
3. Ancaman
4. Klasifikasi informasi

I. Tujuan Keamanan Sistem Informasi

Saat ini peran teknologi informasi pada sebuah perusahaan atau organisasi lainnya tidak lagi hanya sebatas penunjang/alat bantu proses bisnis perusahaan. Melainkan teknologi informasi sudah menjadi roda penggerak proses bisnis dalam bentuk implementasi sistem informasi pada perusahaan tersebut. Selain hal tersebut, informasi juga sudah menjadi aset penting perusahaan. Oleh sebab itu dibutuhkan keamanan yang bertujuan untuk menjamin keberlangsungan sistem informasi pada sebuah perusahaan serta menjamin integritas dan kerahasian informasi yang dihasilkan oleh sistem yang digunakan.

Jadi pada intinya keamanan sistem informasi bertujuan untuk menjamin keberlangsungan sistem informasi dengan memperhatikan beberapa aspek di bawah ini:

1. Integritas (*Integrity*)

Integritas adalah menyajikan informasi yang akurat, benar dan lengkap. Aspek ini sangat penting untuk menjamin kualitas informasi yang akan digunakan oleh para pengguna. Aspek ini bertujuan untuk:

a. Melindungi data dan program supaya tidak dirubah oleh pihak yang tidak berwenang.
b. Memberikan jaminan bahwa data dan informasi yang ada pada sistem informasi dapat dipercaya.

Contoh kasus yang berkaitan dengan integritas informasi adalah ketika ada pelanggan yang akan membeli barang pada sebuah situs online. Informasi yang ditampilkan pada situs tersebut menyatakan bahwa barang yang akan dibeli stoknya masih tersedia. Tetapi setelah melakukan pemesanan pihak administrator tidak menemukan barang yang dipesan karena stoknya sudah habis. Maka dari kejadian tersebut pihak pelanggan sudah dapat menilai integritas dari informasi yang ada pada sistem tersebut. Hal ini dapat memberikan kekecewaan pada pelanggan atau dapat menyebabkan perusahaan kehilangan pelanggan.

2. Kerahasisaan (*Confidentiality*)

Kerahasian adalah melindungi data dan informasi dari penggunaan yang tidak semestinya atau orang-orang yang tidak memiliki otoritas. Aspek ini bertujuan untuk:

a. Membatasi pengaksesan terhadap informasi sesuai tingkat kerahasiaannya.
b. Melindungi data dan informasi supaya tidak jatuh pada pihak yang tidak berwenang.

Sebagai contoh yang berkaitan dengan aspek ini adalah ketika jatuhnya informasi kepada kompetitor mengenai proses produksi dari produk unggulan perusahaan. Dari informasi tersebut maka pihak kompetitor dapat mengetahui cara menghasilkan produk yang sama dengan perusahaan tersebut atau bahkan dapat lebih baik.

3. Ketersediaan (*Availability*)

Ketersediaan adalah menjamin data dan informasi perusahaan tersedia bagi pihak-pihak yang memiliki otoritas untuk menggunakannya. Banyak faktor yang dapat mengganggu aspek ini, diantaranya:

a. Kerusakan hardware
b. Aktivitas user yang jahat (*malicious users*)
c. Penyusup dari luar yang mencoba mengahancurkan atau mencuri data perusahaan
d. Virus, dan sebagainya.

II. Informasi Sebagai Aset

Aset adalah harta atau sumber daya yang dimiliki oleh suatu perusahaan yang berfungsi dalam operasi perusahaan dan diharapkan dapat memberikan manfaat ekonomi di masa depan. Saat ini sudah banyak perusahaan yang menyatakan bahwa informasi termasuk kedalam aset organisasi yang sangat berharga dan penting seperti aset-aset lainnya seperti gedung, mesin-mesin, SDM, dan lain-lain.

Dari pernyataan di atas maka muncul konsekuensi berupa kewajiban untuk melindungi informasi dari berbagai ancaman. Kewajiban tersebut diimplementasikan

dalam bentuk pengaturan keamanan sistem informasi. Selain informasi, masih banyak yang dikategorikan sebagai aset dalam sebuah sistem informasi, diantaranya:

Aset	Contoh
Personel	Programmer, Sistem Analis, Operator, DBA, Spesialis Jaringan.
Hardware	CPU, Concentrator, Printer.
Aplication Software	Sistem Informasi Penjualan, Sistem Informasi Keuangan, DSS.
System Software	Operating System, DBMS.
Data	File Master, File Transaksi, Backup File.
Fasilitas	Ruang Server, Lab Komputer, Meja Komputer.

III. Ancaman

Ancaman adalah aksi yang terjadi baik dari dalam sistem maupun dari luar sistem yang dapat mengganggu keseimbangan sistem informasi. Ancaman ini dapat dikategorikan sebagai berikut:

1. Manusia

   Ancaman ini dapat berupa:

a. Hacking, cracking atau siapa saja yang mengakses sistem tanpa ijin baik dari pihak dalam maupun luar untuk melakukan pencurian atau perusakan.
b. Memasukan virus atau membangun malicious software.
c. Keterbatasan kemampuan pengguna dalam menggunakan dan memelihara sistem yang ada. Hal ini terjadi akibat kurangnya pelatihan atau kesadaran pengguna.

2. Hardware Failure

   Ancaman ini dapat berupa:

a. Kenaikan atau penurunan tegangan listrik dalam jangka waktu yang cukup lama.
b. Korsleting listrik yang dapat mengakibatkan terhentinya proses sistem atau kerusakan hardware.
c. Keborocan AC atau atap pada saat hujan yang membasahi perangkat keras sistem.

3. Software Failure

a. Kesalahan sistem operasi.
b. Kesalahan update program.
c. Uji coba program yang tidak memadai sehingga masih menyisakan kesalahan pada program yang sudah diimplementasikan.

4. Alam

Ancaman alam merupakan bencana alam seperti banjir, gempa bumi, kebakaran dan lain-lain.

IV. Klasifikasi Informasi

Seperti yang telah dibahas sebelumnya bahwa informasi merupakan aset perusahaan yang harus dilindungi dari ancaman penyalahgunaan. Informasi dalam bentuk hardcopy atau softcopy yang dihasilkan oleh sistem informasi dapat diklasifikasikan sebagai berikut:

1. Sangat Rahasia (*Top Secret*)

   Apabila informasi ini disebarkan maka akan berdampak sangat parah terhadap keuntungan berkompetisi dan strategi bisnis organisasi.

   Contoh: strategi bisnis, strategi marketing, proses produksi.

2. Konfidensial (*Confidential*)

   Apabila informasi ini disebarluaskan maka akn merugikan privasi perorangan dan merusak reputasi organisasi.

   Contoh: Keuntungan penjualan, gaji karyawan, data karyawan, data nasabah.

3. *Restricted*

   Informasi ini hanya ditujukan kepada orang-orang tertentu untuk menopang bisnis organisasi.

   Contoh: Strategi promosi, ketentuan perekrutan karyawan.

4. *Internal Use*

   Informasi ini hanya boleh digunakan oleh para pegawai untuk melaksanakan tugasnya.

   Contoh: buku panduang penggunaan program, prosedur sistem informasi, pengumuman mengenai organisasi.

5. *Public*

   Informasi ini dapat disebarluaskan kepada pihak luar atau umum melalui jalur yang resmi.

   Contoh: informasi di Web resmi, daftar produk atau jasa perusahaan, prosedur pembelian atau pemesanan.

V. Daftar Pustaka

[1] IBISA. 2011. Keamanan Sistem Informasi. Yogyakarta: Andi.
[2] Isa, I. 2012. Evaluasi Pengontrolan Sistem Informasi. Yogyakarta: Graha Ilmu.

[3] Laudon, K.C. & Laudon, J.P. 2005. Sistem Informasi Manajemen: Mengelola Perusahaan Digital, Edisi 8. Yogyakarta: Andi.
[4] Sarno, R. & Iffano, I. 2010. Sistem Manajemen Keamanan Informasi (Berbasis ISO 27001). Surabaya: ITS Press.

VI. Materi Berikutnya

Pokok Bahasan	Kebijakan dan Strategi Keamanan Sistem Informasi
Sub Pokok Bahasan	1. Kebijakan keamanan sistem informasi 2. ISO 17799 3. Dampak dari pemanfaatan komputer 4. Kebutuhan atas strategi keamanan sistem informasi