Pengamanan Sistem

MARDAINIS

Beberapa pengertian tentang keamanan sistem informasi

1. John D. Howard mengatakan Computer Security is preventing attackers from achieving objectives through unauthorized access or unauthorized use of computers and networks.

2. G. J. Simons mengatakan bahwa keamanan sistem informasi adalah bagaimana sih kita dapat mencegah terjadinya suatu penipuan, paling tidak mendeteksi adanya penipuan dalam sebuah sistem yang berbasis informasi yang dimana informasi itu sendiri tidak mempunyai arti fisik.

3. Wikipedia menyimpulkan keamanan komputer sering sekali diistilahkan sebagai cabang dari teknologi komputer yang dipakai untuk komputer dan jaringan.

Tujuan dari keamanan sistem informasi

Keperluan adanya perkembangan keamanan sistem informasi tentunya mempunyai tujuan. Tujuannya adalah sebagai berikut :

- Penjaminan integritas informasi
- Pengamanan kerahasiaan data
- Pemastian kesiagaan sistem informasi
- Pemastian memenuhi peraturan, hukum, dan bakuan yang berlaku
- Kelemahan

Notifikasi

Notifikasi adalah pemberitahuan mengenai informasi atau pengumuman dari pihak tertentu kepada pihak yang dituju yang dilakukan melalui media seperti email, sms, maupun aplikasi chatting (line, whatsapp, bbm, wechat, dsb). Notifikasi sangat penting bagi penerima informasi, karena dengan notifikasi, informasi tersebut dapat langsung diketahui oleh penerima. Notifikasi diperlukan ketika informasi yang akan disampaikan kepada pihak terkait tidak memungkinkan untuk diberitahukan secara langsung atau tatap muka. Notifikasi memungkinkan keakuratan atau ketepatan informasi yang diberikan.

Keamanan Sistem Informasi

Keamanan sistem informasi mempunyai etika dalam SI dibahas pertama kalinya oleh Richard Mason, yaitu mencakup: Privasi, Akurasi, Properti dan Akses.

Privasi

Privesi disini menyangkut kepada setiap individu untuk dapat mempertahankan informasi pribadi dari pihak pengakses oleh orang lain yang sesungguhnya tidak diberikan izin untuk melakukan hal tersebut.

Kasus : Junk Mail (Manager pemasaran) menggantikan email bawahan dan data penjualan.

Akurasi

Akurasi terhadap informasi merupakan sebuah faktor yang harus dilengkapi oleh sebuah sistem informasi. Adanya ketidak akurasian setiap informasi dapat menimbulkan hal yang merugikan, mengganggu dan membahayakan.

Contoh Kasus :

Terhapusnya nomor keamanan sosial oleh seseorang yang bernama Edna Rismeller dan kasus kesalahan pendeteksi misil negara Amerika.

Properti

Properti disini maksudnya perlindungan terhadap hak sebuah properti yang dikenal dengan sebutan HAKI. Hak atas kekayaan intelektual ini biasanya diatur oleh hak cipta, paten dan sebuah rahasia perdagangan. Dengan adanya sebuah hak cipta yaitu setiap hak yang dijamin oleh adanya kekuatan hukum yang melarang menduplikasikan kekayaan intelektual tanpa adanya izin dari pemengangnya. Hak ini mudah sekali didapatkan dan diberi kepada pemengang selama masa hidup penciptanya ditambah 70 tahun. Hak paten termasuk bentuk perlindungan terhadap kekayaan intelektual yang sangat sulit sekali untuk didapatkan. Hukum paten disini dapet memberikan pelindungan selama 20 tahun.

Ada kaitannya dengan sebuah kekayaan intelektual, bayak sekali masalah yang belum dapat dipecahkan. Contohnya :

- Bagaimana sebuah informasi dapat dianggap sebagai properti ?

- Apa yang dapat membedakan antara satu produk dengan produk yang lainnya ?

- Akankah setiap pekerjaan yang dihasilkan dari komputer mempunyai manusia sebagai penciptanya ?

- Jika memang tidak, lalu hak properti yang seperti apa yang harus dilindungi ?

Akses

Difokuskan untuk masalah akses yaitu pada setiap penyediaan akses bagi seluruh kalangan. Sebuah teknologi informasi diharapkan untuk tidak menjadi sebuah penghalang dalam melalukan pengaksesan terhadap informasi untuk kelompok ataupun orang-orang tertentu. Tapi justru disini harus jadi pendukung pengaksesan bagi semua pihak.

Keamanan merupakan faktor yang sangat penting yang harus Kamu perhatikan. Perhatikanlah sistem pengoprasian yang bertujuan untuk mencegah terjadinya ancaman terhadap sistem serta mendeteksi dan membetulkan semua kerusakan sistem.

Adanya ancaman terhadap sistem informasi dapat dibagi menjadi 2 macam. Yang pertama ancaman aktif dan yang kedua ancaman pasif. Ancaman aktif itu mencakup setiap kecurangan dan kejahatan kepada komputer. Sedangkan ancaman pasif yaitu ancaman yang mencakup kegagalan sistem, kesalahan manusia dan adanya bencana alam.

Metode yang biasanya digunakan oleh orang lain dalam melakukan penetrasi sistem yang berbasis komputer ada 6 macam. Yaitu sebagai berikut :

- Memanipulasi masukan
- Penggantian program
- Penggantian sebuah berkas secara langsung
- Pencurian data/sabotase
- Adanya penyalahgunaan
- Pencurian sumber daya komputasi

Cara yang digunakan untuk melakukan hacking sistem informasi

1. Denial of Service

Teknik danial of service ini dilaksanakan dengan cara membuat permintaan yang cukup banyak terhadap sebuah situs sehingga membuat macet dan setelah itu mencari kelemahan pada sistem si pelaku untuk melakukan serangan terhadap sistem.

2. Sniffer

Teknik sniffer ini di implementasikan dengan membuat suatu program yang dapat membantu melacak peket data seseorang ketika paket itu melintas di internet, bisa menangkap password dan menangkap isinya.

3. Spoofing

Teknik spoofing ini adalah melakukan pemalsuan email atau web untuk bertujuan menjebak pemakai agar memasukan info yang penting seperti nomor kartu kredit atau password.

Pengendalian sistem informasi

Demi menjaga sebuah keamanan sistem informasi, diperlukannya pengendalian terhadap sistem informasi kontrol yang mencakup kontrol administratif, kontrol pengembangan dan pemeliharaan sistem, kontrol operasi, proteksi terhadap pusat data secara fisik, kontrol perangkat keras, kontrol terhadap akses komputer, kontrol terhadap akses informasi, kontrol terhadap perlindungan terakhir dan kontrol aplikasi.

1. Kontrol administratif

Kontrol administratif disini mempublikasikan kebiakan kontrol yang bisa mengendalikan semua sistem informasi dapat dilakukan dengan jelas oleh semua pihak. Dalam hal ini yaitu dalam proses pengembangan sistem, prosedur saat melakukan backup, pemulihan data dan pengarsipan data. Dalam merekrut pegawai harus hati-hati, pembinaan dan adanya pelatihan yang diperlukan.

2. Kontrol operasi

Kontrol operasi ini mempunyai tujuan agar sistem beroprasi itu sesuai dengan yang diharapkan, termasuk dalam hal sebagai berikut :

- Pembatasan akses terhadap pusat data
- Kontrol terhadap personel pengoperasi
- Kontrol terhadap peralatan (terhadap kegagalan)
- Kontrol terhadap penyimpan arsip
- Pengendalian terhadap virus

3. Perlindungan fisik terhadap pusat data

Dari adanya faktor lingkungan yang menyangkut suhu, kebersihan, bahaya adanya banjir, kelembaban udara dan keamanan fisik ruangan perlu diperhatikan dengan seksama. Mengantisipasi jika kegagalan sumber daya listrik, biasanya itu digunakan UPS dan penyediaan generator.

4. Kontrol perangkat keras

Agar mengatisipasi adanya kegagalan sistem komputer, kadang organisasi menerapkan sistem komputer dengan berbasis fault-tolerant. Jadi toleransi terhadap adanya kegagalan pada penyimpanan eksternal bisa dilakukan melalui disk mirroring atau sis shadowing yang menggunakan teknik menulis semua data de 2 disk secara paralel.

5. Kontrol akses terhadap sistem komputer

Setiap kali pemakai sistem diberikan otoritasi yang berbeda-beda maka dari setiap pemakai itu dilengkapi dengan nama si pemakai dan password. Penggunaan teknologi yang canggih menggunakan sifat yang biologis manusia yang cenderung unik.


SCAN COMPLETE
PASSWORD PROTECT
1234
567
89
10
HACKING DETECTED
01010101110000101010101
01010101110000101010101

Selesai