Slide 2

Oleh :

Agung Brastama Putra

Pembahasan

- Aspek-Aspek Keamanan
- Keamanan Fisik

Buku

- Salomon, David. 2010. Elements of Computer Security. Springer : Springer London Dordrecht Heidelberg New York.
- Christian W. Probst, Jeffrey Hunker, Dieter Gollmann, Matt Bishop. 2010. Insider Threats in Cyber Security. Springer : Springer London Dordrecht Heidelberg New York.

Aspek-Aspek Keamanan

- Masalah keamanan dari dalam atau internal amat sangat lebih berbahaya dibandingkan dengan ancaman dari luar.
- Karena orang dalam/internal mempunyai kemampuan mengakses “informasi” dari dari dalam tanpa tercurigai.

- Dalam sebuah penelitian insider didefinisikan sebagai seseorang dengan akses, hak istimewa atau pengetahuan tentang layanan sistem informasi.
- Contohnya :

- Penyalahgunaan Hak Akses
- Penggunaan komputer orang lain.
- Penggunaan ID orang lain.

Jadi orang dalam adalah

- Seseorang dengan sah meng-akses ke sumber daya.
- Seseorang yang sebagian atau sepenuhnya telah dipercaya.
- Individu yang telah atau memiliki hak akses ke sumber daya.

Ancaman Orang Dalam

- Pengguna sistem yang dapat menyalahgunakan hak istimewa
- Seorang individu dengan akses resmi yang mungkin mencoba atau yang dapat bantuan dari luar, dalam melakukan penghapusan atau sabotase terhadap aset kritis secara tidak sah.

Deteksi dan Mengurangi Ancaman

Detection

- Data berlebihan,
- Data tidak valid,
- Kehilangan data.

Mitigation

- Monitoring proses.
- Kebijakan jelas memainkan peran penting sehubungan dengan ancaman dari dalam, karena menentukan batas-batas antara boleh dan tidak boleh perilaku, baik pada tingkat teknis dan non-teknis.

- Hak Akses tiap orang, bagian dan jabatan untuk memasuki sebuah sistem.
- Diadakan Audit.

Faktor dan Kepatuhan Manusia

- Terdapat banyak kesalahan tentang asumsi Faktor dan Kepatuhan Manusia, antara lain

1. Ketika diadakan audit hanya berfokus untuk mencari-cari kesalahan dalam kebijakan.

2. Monitoring dilakukan secara kelompok tertentu atau individu-individu tertentu yang mempunyai tingkah yang berbeda, dan tidak keseluruhan.
3. Menanamkan budaya keamanan yang diinginkan oleh perusahaan.

Seharusnya....

1) kebijakan perlu dibuat lebih mudah dikelola, dan

2) diperlukan pengkajian ulang terhadap kebijakan-kebijakan yang berlebihan.

- Idealnya adalah kebijakan keamanan konsisten berkaitan dengan perilaku, dan sesuai dengan proses bisnis, dan nilai-nilai organisasi dan norma-norma.

Keamanan Fisik

- Lonjakan dalam listrik, sering disebabkan oleh petir, sehingga membuat komponen di komputer menjadi tidak stabil.
- Solusi : Menggunakan uninterruptible power Supply (UPS).

- Pertanyaanya bagiamana apabila power computer tiba-tiba mati????

- Banyak di perusahaan data dapat dihapus jika terutama jika data sensitif dicuri atau rusak. Kerusakan dapat disengaja, ditimbulkan oleh seorang kriminal atau karyawan puas, atau disebabkan oleh api, kegagalan daya atau rusaknya pendingin udara.

- Solusinya, kalau hal itu terjadi dalam rumah maka ditambahkan alarm dan untuk komputernya digunakan UPS.
- Solusi untuk perusahaan/Entitas komersial, dengan pengendalian akses, dioperasikan kartu kunci, kamera keamanan, dan sistem otomatis api (menggunakan gas bukannya air jika mungkin).

- Fasilitas yang menggunakan elektronik kunci dan kunci atau identifikasi fisik lainnya perangkat untuk membatasi akses ke daerah-daerah tertentu harus mempertimbangkan masalah berikut, dikenal sebagai piggybacking atau tailgating.

- Medan magnet. Hard disk adalah media penyimpanan. Data yang disimpan dalam titik-titik magnetik yang kecil pada disk dan itu sangat sensitif terhadap medan magnet.

- Keprihatinan terkait adalah listrik statis. Berjalan di atas karpet sering mengakibatkan listrik statis dikumpulkan di sepatu dan pakaian.
- Daya listrik habis ketika menyentuh sebuah konduktor dan dapat merusak peralatan listrik yang halus.
- Ruang komputer harus memiliki ubin lantai atau karpet setidaknya anti-statis

- Hard copy. Media telah telah menggembar-gemborkan the paperless office untuk beberapa dekade, tetapi kita masih menggunakan kertas.

- Memata-matai/Spyware. Spyware, ancaman penting, tetapi memata-matai juga dapat dilakukan dengan cara tradisional, oleh orang.
- Data integrity

DRP (Disaster Recovery Planning)

- Rencana pemulihan bencana adalah bagian penting dari setiap organisasi, apakah komersial, amal atau pemerintah.
- Rincian langkah-langkah yang diperlukan untuk cepat mengembalikan kemampuan teknis dan jasa setelah gangguan atau bencana.
- Ide dalam rencana tersebut adalah untuk meminimalkan dampak bencana di organisasi.
- DRP biasanya hanya disebut DRC (Disaster Recovery)