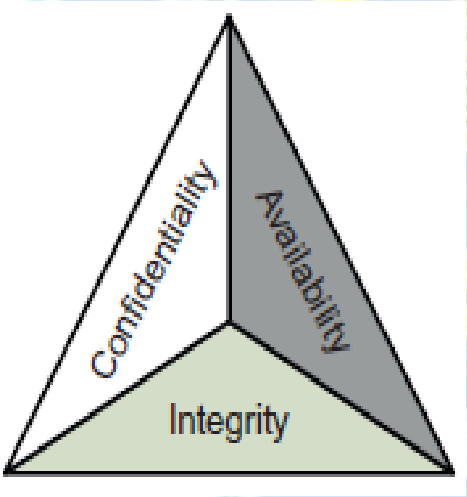
Rangkuman

Access Control Dalam Keamana Informasi

Nama : M. Hairul Umam / Nim : 1310651100 / Kelas : D

Salah satu bagian mendasar dalam Information System Security adalah Access Control. Menurut definisi dari ***CISSP (Certified Information System Security Profesional)*** Study Guide, Access Control didefinisikan sebagai suatu proses untuk mengatur / mengontrol siapa saja yang berhak mengakses suatu resource-rosource tertentu yang terdapat di dalam sebuah sistem. Di dalam proses ini akan diidentifikasi siapa yang sedang melakukan request untuk mengases suatu resource tertentu dan apakah orang tersebut memiliki hak akses (authorized) untuk mengakses resource tersebut. Access control memproteksi data terhadap unauthorize access atau akses yang dilakukan oleh orang yang memang tidak memiliki hak akses terhadap reource tersebut. Akses di sini bisa berupa melihat data (view) ataupun melakukan perubahan terhadapt suatu data (modify).



Dengan demikian Access Control mendukung terwujudnya :

1. Confidentiality

Memastikan data hanya bisa dilihat oleh orang yang memiliki hak akses untuk melihat data tersebut atau dikenal dengan istilah No Unauthorized Read.

2. Integrity

Memastikan data hanya bisa ditulisi dan diubah oleh orang yang memiliki hak akses untuk melakukan penulisan ataupun pengubahan terhadap data tersebut atau dikenal dengan istilah No Unauthorized Write.

Ketika membahas tentang Access Control, kita akan menemui dua entitas utama yang terlibat, yaitu:

1. Subject of the Access Control

Yang menjadi subject di sini adalah entitas yang mengajukan request / permintaan untuk melakukan akses ke data.

2. Object of the Access Control

Yang menjadi object di sini adalah entitas yang mengandung atau mengatur data. Atau dengan kata lain object adalah resource yang tersedia di dalam suatu system, nah dalam hal ini Access Control sendiri dapat dibagi menjadi 3, yaitu :

- ✓ ***Physical Access Control***

Physical Access Control ditujukan untuk membatasi akses secara fisik ke perangkat hardware yang membangun suatu system, Physical Access Control terbagi menjadi tiga bentuk, yaitu :

1. Perimiter Security adalah Perimiter Security bertujuan untuk membatasi akses masuk ke area atau lokasi di mana perangkat hardware berada. Contoh nyata dari penerapan Perimiter Security.

2. Cable Protection adalah Proteksi kabel dapat dilakukan melalui beberapa cara, yaitu shielding untuk meningkatkan ketahanan terhadap EMI (Electro Magnetic Interference), memilih jenis kabel yang tahan terhadap EMI seperti fiber optic, dan juga penggunaan conduit untuk memproteksi kabel dari gangguan kerusakan secara fisik seperti misalnya gigitan tikus.

3. Pembagian Area Kerja (separation of duties and work areas) adalah Pembagian area kerja secara fisik di antara karyawan ditujukan untuk meminimalisir terjadinya shoulder surfing. Yang dimaksud dengan istilah shoulder surfing adalah di mana seorang karyawan dapat melihat dan mengamati aktifitas yang dilakukan oleh karyawan lainnya dengan mengintip lewat balik bahu. Administrative Access Control.

- ✓ ***Administrative Access Control***

Ada 4 point utama yang terkandung dalam Administrative Access Control, yaitu:

1. Policies and Procedure

Di sini berbicara mengenai penyusunan aturan / kebijakan dan prosedur yang jelas berkaitan dengan akses terhadap resource-resource yang terdapat di dalam sistem. Dalam point ini peranan dan dukungan dari pimpinan dalam tataran eksekutif sangatlah penting sehingga kebijakan dan juga prosedur yang sudah disusun memiliki kekuatan (dan terkadang memang perlu agak dipaksakan) untuk bias diimplementasikan dan diikuti oleh semua karyawan yan terlibat di dalam sistem. Tanpa adanya dukungan dari pimpinan maka kebijakan dan prosedur yang sudah disusun menjadi powerless atau tak memiliki kekuatan apa-apa.

2. Hiring Pratices

Di sini berbicara mengenai mekanisme perekrutan karyawan baru. Dalam proses perekrutan, salah satu point yang perlu diperhatikan adalah tanggapan dan pendapat dari si calon karyawan tersebut berkenaan dengan kebijakan dan prosedur yang sudah disusun. Rekrutlah karyawan yang memang sejalan dan sependapat dengan kebijakan dan prosedur yang berlaku di perusahaan.

3. Security Awareness Training

Selain merekrut karyawan yang sependapat dengan kebijakan dan prosedur yang berlaku, perllu juga dilakukan pelatihan / training berkaitan dengan security awareness. Di sini setiap karyawan akan dijelaskan dan disadarkan betapa pentingnya aspek keamanan terhadap sistem. Diharapkan setelah mengikuti pelatihan ini setiap karyawan dapat mengikuti dan menjalankan setiap kebijakan dan prosedur yang berkaitan dengan keamanan sistem dengan penuh tanggung jawab karena telah menyadari betapa pentingnya aspek keamanan sistem yang terkandung di dalamnya.

4. Monitoring

Point terakhir adalah monitoring atau pengawasan terhadap kebijakan dan prosedur yang berlaku. Di sini akan dilakukan pemantauan apakah setiap prosedur sudah dilakukan dengan baik atau adakah pelanggaran-pelanggaran yang terjadi terhadap kebijakan dan prosedur yang berlaku. Tujuan utama dari point ini adalah memastikan setiap kebijakan dan prosedur yang berlaku berjalan dengan baik.

- ✓ ***Dan Logical Access Control.***

Logical Access Control akan berbicara mengenai hal-hal teknis yag diberlakukan untuk melakukan pengaturan / pengendalian akses terhadap resource-resource yang ada di dalam suatu sistem. Ada 3 point utama yang terkandung dalam Logical Access Control, yaitu:

1. Object Access Restriction

Point ini dimaksudkan untuk mengijinkan akses kepada authorized user. Hal ini bisa dilakukan dengan menggunakan Role Based Access Control di mana akan didefinisikan akses apa saja yang diijinkan kepada seorang atau sekumpulan karyawan berkaitan dengan jabatan dan wewenang yang dimilikinya.

2. Encryption

Melakukan penyandian data sehinga data hanya bisa dibaca oleh orang-orang yang memang memiliki hak akses.

3. Network Architecture / Segregation

Melakukan segmentasi pada infrastruktur jaringan komputer yang ada. Hal ini ditujukan untuk menghindari adanya aksi pencurian data yang dilakukan melalui infratruktur jaringan yang ada.