Nama : Dewi Fatmawati

Nim : 1310651059

Kelas : D

Access Control

Pengertian Access Control

Access control secara umum dapat diimplementasikan dengan memberikan izin (permisi) dan hak terhadap objek secara spesifik. Izin diberikan terhadap objek untuk menentukan siapa saja yang dapat mengakses objek tersebut dan sebatas apa ia berhak mengaksesnya. Izin tersebut, dapat diaplikasikan oleh sistem atau pemilik objek tersebut (orang yang membuat objek). Jenis izin yang dapat diaplikasikan bergantung pada objek yang hendak diamankan. Access control dalam kenyataanya terkait dengan segala kejadian yang kita alami dalam kehidupan sehari-hari

Access Control. Menurut definisi dari CISSP (Certified Information System Security Profesional) Study Guide, Access Control merupakan sebagai suatu proses untuk mengatur / mengontrol siapa saja yang berhak mengakses suatu resource-rosource tertentu yang terdapat di dalam sebuah sistem.

Tujuan dari Acces Control adalah untuk memungkinkan pengguna yang berwenang mengakses data yang sesuaidan menolak akses ke pengguna yang tidak sah. Kontrol akses melindungi terhadap ancaman seperti akses yang tidak sah, modifikasi yang tidak pantas data, dan hilangnya .

Access Control System berfungsi untuk mengatur hak akses ke suatu area tertentu pada waktu tertentu atau dengan kata lain dapat juga berfungsi sebagai Alat yang membuka dan mengunci pintu secara otomatis sehingga orang tidak berkepentingan tidak dapat masuk. Terdapat 2 jenis access control system: standalone system dan network system (package). Kategori ini juga meliputi berbagai biometric system: mesin absensi sidik jari, fingerprint access control system. Juga terdapat berbagai aksesoris untuk Access Control System seperti kartu, exit button, dan lainnya.

Access Control mendukung terwujudnya hal- hal sebagai berikut

- Confidentiality
  Confidentality / Kerahasiaan dalam hal ini yaitu berusaha untuk mencegah pengungkapan yang tidak sah dari informasi itu. Dengan kata lain, kerahasiaan berusaha untuk mencegah akses yang tidak sah atau di kenal dengan istilah No.

Unauthorized Read. Contoh dari serangan kerahasiaan akan pencurian Secara pribadi yaitu seperti informasi kartu kredit.

- Integrity

  Integritas atau integritas adalah merupakan suatu usaha untuk mencegah modifikasi yang tidak sah dari informasi. Dengan kata lain, integritas berusaha untuk mencegah akses tulis tidak sah ke data.

Ada dua jenis integritas yaitu

a. Integritas data berusaha untuk melindungi informasi terhadap modifikasi yang tidak sah.
b. integritas sistem berusaha untuk melindungi sistem, seperti sistem operasi Windows server 2012, dari modifikasi yang tidak sah

Least Privilege

Least Privilege adalah memberikan hak akses yang memang dibutuhkan oleh subject yang bersangkutan untuk melakukan tugas-tugas yang memang menjadi bagian dari tanggung jawabnya. Yang perlu di perhatikan di sini adalah jangan pernah memberikan akses penuh (Full Access) terhadap semua resource yang tersedia di dalam sistem kepada subject. Berikan hak akses sesuai dengan yang dibutuhkannya. Tujuannya adalah meminimalisir terjadinya Authorization Creep atau suatu kejadian yang tidak disengaja di mana suatu subject diberi hak akses yang seharusnya tidak dia miliki.

Acces Ccontrol dapat di bagi menjadi 3 bagian yaitu

a. Physical Access Control

Physical Access Control ditujukan untuk membatasi akses secara fisik ke perangkat hardware yang membangun suatu sistem

b. Administrative Access Control

Administrative Access Control adaklah sekumpulan peraturan dan strategi untuk membatasi akses terhadap suatu resource tertentu dalam upaya pengaman terhadap sistem. Selain itu, Administrative Access Control juga berbicara mengenai mekanisme monitoring / pengawasan dan pendeteksian terhadap pelanggaran akses terhadap suatu resource.

c. 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 empat metode kontrol akses media yang digunakan dalam jaringan lokal, yaitu :

1) Carrier Sense Multiple Access with Collision Detection (CSMA/CD)

Metode ini digunakan dalam jaringan Ethernet half-duplex (jaringan Ethernet full-duplex menggunakan media yang beralih daripada menggunakan media bersama yang tidak memerlukan metode ini).

CSMA / CD adalah metode akses jaringan yang paling populer digunakan dalam jaringan lokal, jika dibandingkan dengan akses jaringan metode teknologi lainnya. CSMA / CD didefinisikan dalam spesifikasi IEEE 802.3 yang dirilis oleh Institute of Electrical and Electronics Engineers (IEEE).

2) Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)

Metode ini digunakan dalam teknologi jaringan AppleTalk dan beberapa bentuk jaringan nirkabel (wireless network), serta IEEE 802.11a, IEEE 802.11b dan IEEE 802.11g. Untuk AppleTalk, CSMA / CA didefinisikan dalam IEEE 802.3, sementara untuk jaringan nirkabel didefinisikan dalam IEEE 802.11.

3) Token Passing

Metode ini digunakan dalam teknologi jaringan Token Ring dan Fiber Distributed Data Interface (FDDI). Standar Token Ring didefinisikan dalam IEEE 802.5, sementara FDDI didefinisikan oleh American National Standards Institute (ANSI).

4) Demand priority

Digunakan dalam jaringan dengan teknologi 100VG-AnyLAN dan didefinisikan dalam standar IEEE 802,12.

Dalam implementasi jaringan, dukungan jaringan semacam network interface card, switch, atau router, metode kontrol akses diimplementasikan menggunakan algoritma MAC (MAC algoritma).

Perlu di ketahui di sini bahwa ada hal yang di anggap paling istimewa, Paling istimewa yang di maksud di sini berarti pengguna harus diberikan jumlah minimum akses (Otorisasi) diperlukan untuk melakukan pekerjaan mereka, tapi tidak lebih. Paling istimewa diterapkan untuk kelompok benda. Perlu tahu lebih rinci dari paling istimewa tersebut pengguna perlu mengetahui bahwa bagian tertentu dari informasi sebelum mengakses itu.

- **Subjects and objects**

SEBUAH subyek adalah entitas aktif pada sistem data. Sebagian contoh pelajaran melibatkan

orang mengakses file data. Namun, program komputer yang menjalankan adalah subyek

- **Defense-in-depth**

  Defense-in-depth yang (Juga disebut pertahanan berlapis) berlaku beberapa perlindungan (juga disebut kontrol tindakan yang diambil untuk mengurangi resiko) untuk melindungi aset. Setiap keamanan tunggal control mungkin gagal; dengan mengerahkan beberapa kontrol, Anda meningkatkan kerahasiaan, integritas, dan ketersediaan data Anda.

Kategori access control defensif dan typenya

Untuk memahami dan tepat menerapkan kontrol akses, pemahaman apa manfaat setiap kontrol dapat menambah keamanan sangat penting. Pada bagian ini, setiap jenis kontrol akses akan ditentukan atas dasar bagaimana menambah keamanan sistem. Ada enam jenis kontrol akses:

- Preventive

  Preventif mencegah tindakan dari terjadi. Ini berlaku pembatasan untuk apa Potensi pengguna, baik resmi atau tidak sah, dapat dilakukan.

- Detective

  Kontrol Detektif adalah kontrol yang siaga selama atau setelah serangan yang berhasil. Intrusi sistem deteksi sinyal setelah serangan sukses, kamera televisi sirkuit tertutup (CCTV) yang penjaga waspada terhadap penyusup, dan sistem bangunan alarm yang dipicu oleh penyusup merupakan contoh dari kontrol detektif.

- Corrective

  Kontrol korektif bekerja dengan "memperbaiki" sistem atau proses rusak. Koreksi yang kontrol akses tive biasanya bekerja bergandengan tangan dengan kontrol akses detektif. Anti- virus memiliki kedua komponen. Pertama, perangkat lunak antivirus menjalankan scan dan kegunaan file definisi untuk mendeteksi apakah ada software yang cocok daftar virus tersebut. Jika mendeteksi virus, kontrol korektif mengambil alih, menempatkan perangkat lunak yang mencurigakan di karantina, atau menghapusnya dari sistem.

- Recovery

  memungkin perlu diambil untuk mengembalikan fungsi dari sistem dan organisasi. Pemulihan berarti bahwa sistem harus pulih: diinstal ulang dari OS Media atau gambar, data dikembalikan dari backup, dll

- Deterrent

  mencegah pengguna dari melakukan tindakan pada sistem. Contohnya termasuk

  "Waspadalah terhadap anjing" tanda pencuri menghadapi dua bangunan, satu

dengan anjing penjaga dan satu dengan out, lebih mungkin untuk menyerang bangunan tanpa anjing penjaga. Denda besar untuk ngebut adalah pencegah untuk driver untuk tidak mempercepat. Sebuah kebijakan sanksi yang membuat pengguna memahami bahwa mereka akan dipecat jika mereka tertangkap situs Web berselancar terlarang atau ilegal adalah pencegahan.

- Compensating\
  control adalah kontrol keamanan tambahan dimasukkan ke dalam tempat untuk mengkompensasi kelemahan dalam kontrol lainnya.