Nama : Dewi Ratnasari
Nim : 131065144
Kelas : B

Access Control

Salah satu bagian mendasar dalam Information System Security adalah Access Control. Menurut definisi dari CISSP (Certified Information System Security Profesional) , 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 mengakses 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.

Ada dua jenis integritas:

- integritas data
- integritas sistem

Identitas dan otentikasi
Identitas adalah klaim: jika nama Anda adalah "Orang X," Anda mengidentifikasi diri dengan mengatakan "Saya
Orang X. "Identitas saja lemah karena tidak ada bukti. Anda juga dapat mengidentifikasi diri dengan mengatakan "Saya Orang Y." Membuktikan klaim identitas disebut

authentica-tion: Anda mengotentikasi klaim identitas, biasanya dengan menyediakan sepotong informasi atau sebuah benda yang hanya Anda dimiliki, seperti password atau paspor Anda.

Otorisasi
Otorisasi menjelaskan tindakan yang dapat Anda lakukan pada sistem setelah Anda memiliki iDEN-tified dan dikonfirmasi. Tindakan mungkin termasuk membaca, menulis, atau file eksekusi atau program.

Akuntabilitas
Akuntabilitas memegang pengguna jawab atas tindakan mereka.

Nonrepudiation
berarti pengguna tidak dapat menyangkal (menolak) setelah dilakukan transaksi

Konsep Cornerstone Keamanan Informasi

Pertahanan-mendalam
Pertahanan di kedalaman
(Juga disebut pertahanan berlapis) berlaku beberapa perlindungan untuk melindungi aset. Setiap keamanan tunggal

Model Access Control

Sekarang kita telah meninjau konsep kontrol akses landasan, kita bisa mendiskusikan berbeda model kontrol akses: model utama adalah

- Discretionary Access Control
  (DAC) Memberikan pelajaran kontrol penuh dari benda-benda yang mereka miliki telah diberi akses ke, termasuk berbagi objek dengan mata pelajaran lain. Subyek diberdayakan dan mengendalikan data mereka. Sistem operasi standar UNIX dan Windows menggunakan DAC untuk sistem berkas
- Wajib Access Control
  (MAC) Adalah sistem kontrol akses ditegakkan berdasarkan sub izin ject dan label objek. S ubjects dan benda-benda memiliki izin dan label, masing-masing, seperti rahasia, rahasia, dan rahasia
- Peran Berbasis Access Control
  (RBAC) Mendefinisikan bagaimana informasi diakses pada sistem berdasarkan peran subjek. RBAC adalah jenis kontrol akses nondiscretionary karena pengguna tidak memilikikebijaksanaan mengenai kelompok benda mereka diizinkan untuk mengakses dan tidak mampu untuk mentransfer objek untuk mata pelajaran lainnya.

- Daftar kontrol akses
  (ACL) Digunakan di seluruh banyak kebijakan keamanan IT, prosedur-prosedur-, dan teknologi. Daftar kontrol akses adalah daftar objek.

IBM menjelaskan aturan siklus hidup identitas berikut:

- Password pemeriksaan kepatuhan kebijakan
- Memberitahukan pengguna untuk mengubah password mereka sebelum mereka berakhir
- Mengidentifikasi hidup perubahan siklus seperti rekening yang tidak aktif selama lebih dari 30 hariberturut-turut
- Mengidentifikasi akun baru yang belum digunakan selama lebih dari 10 hari setelah penciptaan mereka

Access Control Model
Mengidentifikasi akun yang kandidat untuk dihapus karena mereka telah
ditangguhkan selama lebih dari 30 hari
Remote Authentication Dial-In Service Pengguna
(RADIUS) Protokol adalah pihak ketiga
sistem otentikasi.

Sistem Terminal Access Controller Access Control
(TACACS) Adalah terpusat
sistem kontrol akses yang mengharuskan pengguna untuk mengirim ID dan statis (reusable) password untuk otentikasi. TACACS menggunakan port UDP 49 (dan mungkin juga menggunakan TCP).

PAP dan CHAP

Itu
Password Authentication Protocol
(PAP) Tidak aman: pengguna memasukkan password
dan itu dikirim melalui jaringan dalam bentuk teks. Ketika diterima oleh server PAP, itu adalah dikonfirmasi dan divalidasi. Mengendus jaringan dapat mengungkapkan plaintextn password Itu.

Tantangan-Handshake Authentication Protocol

(CHAP) Memberikan perlindungan
terhadap serangan pemutaran.Ini menggunakan lokasi yang menantang pengguna jarak jauh. Sebagai dinyatakan dalam RFC 1994, "CHAP tergantung pada 'rahasia' yang hanya diketahui authenticator dan peer. Rahasianya tidak dikirim melalui link.

ACCESS CONTROL KATEGORI defensif DAN JENIS

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:
    1. Pencegah
    2. Detektif
    3. Perbaikan
    4. Pemulihan
    5. Pencegah
    6. Kompensasi

FAKTA CEPAT
Jenis kontrol akses ini dapat jatuh ke dalam salah satu dari tiga kategori: administrasi, teknis, atau fisik.
1. Administratif
(Juga disebut directive) kontrol dilaksanakan dengan menciptakan dan mengikuti kebijakan organisasi, prosedur, atau peraturan. Pelatihan pengguna dan kesadaran juga jatuh ke dalam kategori ini.

2. Teknis kontrol
diimplementasikan menggunakan perangkat lunak, perangkat keras, atau firmware yang membatasi Akses logis pada sistem teknologi informasi. Contohnya termasuk firewall, router, dan enkripsi.

3.Fisik kontrol
diimplementasikan dengan perangkat fisik, seperti kunci, pagar, gerbang, dan penjaga keamanan.

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

- Contoh dari 7 Access Control Defensive Kategori dan Jenis
    - Kontrol pencegahan
    - Detektif
    - Kontrol Detektif
    - Kontrol korektif
    - kontrol pemulihan
    - Kontrol pencegah
    - Kompensasi

METODE AUTHENTIKASI
Sebuah konsep kunci untuk melaksanakan jenis kontrol akses mengendalikan tepat otentikasi subyek dalam sistem IT.