Nama : Wawan Tofik

Nim : 1310651045

Kelas : A

Akses kontrol

Akses kontrol pintu adalah sebuah sistem yang dapat atau untuk membatasi pengguna untuk mengakses suatu ruangan dengan menempatkan sistem perangkat kontrol pada pintu. Dalam Akses kontrol pintu, kontrol akses merujuk pada praktek membatasi pintu masuk ke properti, bangunan, atau ruang untuk orang yang berwenang.

Akses kontrol ini dapat dilakukan oleh personil seperti penjaga perbatasan, penjaga pintu, pemeriksa tiket, dll, atau dengan perangkat seperti sebuah kunci (Lock). Namun ketika akses kontrol berupa seorang penjaga atau kunci manual mempunyai banyak keterbatasan, kontrol akses elektronik menggunakan sistem komputerisasi atau mirokontroler memecahkan keterbatasan tersebut. Sistem akses kontrol pintu secara sederhana dipadukan dengan kunci (lock) saat ini telah dikembangkan seperti dipadu dengan sistem kartu (card) misalnya RF ID (Magnetic Card), Smart Card atau kartu lainnya atau yang lebih mutahir dan lebih tinggi tingkat keamanannya seperti sistem biometrik seperti sidik jari (fingerprint), muka (face) tau dengan retina.

Tujuan dari kontrol akses adalah untuk memungkinkan pengguna yang berwenang mengakses data yang sesuai dan menolak akses ke pengguna yang tidak sah. Kontrol akses melindungi Kerahasiaan, integritas, dan ketersediaan Kerahasiaan.

Identitas dan otentikasi

Identitas adalah klaim misalkan jika nama Anda adalah "Orang X," Anda mengidentifikasi diri dengan mengatakan "Saya Orang X. "Identitas saja lemah karena tidak ada bukti. Anda juga dapat engidentifikasi diri dengan mengatakan "Saya Orang Y." Membuktikan klaim identitas disebut otentikasi: Anda mengotentikasi klaim identitas, biasanya dengan menyediakan informasi atau sebuah benda yang hanya Anda dimiliki, seperti password atau paspor Anda.

Otorisasi menjelaskan tindakan yang dapat melakukan pada sistem setelah system mengidentifikasi dan dikonfirmasi. Tindakan mungkin termasuk membaca, menulis, atau file eksekusi dalam program.

Akuntabilitas

Akuntabilitas adalah penanggung jawab atas semua apa yang disediakan. Hal ini biasanya dicapai dengan login dan menganalisis data audit. Dengan akuntabilitas membantu menjaga akses Untuk beberapa pengguna.

Subyek dan obyek

Sebuah subjek merupakan entitas yang aktif pada sistem informasi. Sebuah objek bisa dikatakan data pasif dalam sistem. Objek didapatkan dari database ke file atau teks. Hal penting untuk diingat tentang obyek adalah data pasif dalam sistem. Mereka tidak memanipulasi yang lainnya.

Pertahanan berlapis

pertahanan berlapis berlaku pada beberapa sistem untuk melindungi aset. Setiap keamanan tunggal control mungkin akan mendapatkan permasalahan namun dengan adanya pertahanan berlapis akan meningkatkan kerahasiaan, integritas, dan ketersediaan data.

Kontrol akses discretionary

Discretionary Access Control (DAC) memberikan kontrol penuh dari hal - hal yang mereka miliki yang telah diberi hak akses seperti halnya halaman admin pada sebuah website. Admin akan mempunyai control penuh terhadap website tersebut. Sehingga admin bisa mengupdate, menambah, menghapus, dan menambah data.

Kontrol akses nondiscretionary

RBAC adalah jenis kontrol akses nondiscretionary karena pengguna tidak memiliki kebijaksanaan mengenai akun akses yang lain namun hanya diizinkan untuk mengakses dan tidak mampu untuk mentransfer objek lainnya. Contoh dari perangkat kontrol akses berbasis aturan seperti proxy firewall yang memungkinkan pengguna untuk searching di Web dengan konten yang disetujui yang telah ditetapkan. Situs lain dilarang dan aturan ini diberlakukan di seluruh semua dikonfirmasi pengguna.

Kontrol akses terpusat

Kontrol akses terpusat berkonsentrasi kontrol akses di satu titik pusat saja untuk sistem atau organisasi. Dialihkan menggunakan database kontrol akses lokal, sistem mengotentikasi melalui server otentikasi pihak ketiga. Kontrol akses terpusat dapat digunakan untuk menyediakan Single Sign-On (SSO), dimana subjek dapat mengotentikasi sekali, dan kemudian mengakses beberapa sistem. Kontrol akses terpusat dapat terpusat menyediakan tiga "A" dari kontrol akses: Otentikasi, Otorisasi, dan Akuntabilitas. Contohnya seperti elearning universitas muhammadiyah jember yang hanya bisa diakses dari jaringan Lokal.

Daftar kontrol akses

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

Akses pengadaan siklus hidup

Setelah model kontrol akses yang tepat telah dipilih dan digunakan, akses penyediaan siklus hidup harus dijaga dan diamankan. Sementara banyak organisasi ikuti praktik terbaik untuk

mengeluarkan akses, banyak kekurangan proses formal untuk memastikan seumur hidup akses disimpan aman sebagai karyawan dan kontraktor bergerak dalam sebuah organisasi.

IBM menjelaskan aturan siklus hidup identitas berikut:

• Password untuk pemeriksaan kepatuhan kebijakan

• Memberitahu pengguna untuk mengubah password mereka sebelum berakhir

• Mengidentifikasi hidup perubahan siklus seperti rekening yang tidak aktif selama lebih dari 30 hari berturut-turut

• Mengidentifikasi akun baru yang belum digunakan selama lebih dari 10 hari setelah penciptaan mereka

• Mengidentifikasi akun yang calon untuk dihapus karena mereka telah ditangguhkan selama lebih dari 30 hari

• Ketika kontrak berakhir, mengidentifikasi semua account milik mitra bisnis atau karyawan kontraktor dan mencabut hak akses mereka "1 Hak pengguna, akses review, dan audit yang Akses agregasi terjadi sebagai pengguna individu memperoleh lebih banyak akses ke banyak sistem.

ACCESS CONTROL KATEGORI defensif

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:

• Pencegahan

• Detektif

• Corrective

• Pemulihan

• Pencegah

• Kompensasi

pencegah

Kontrol preventif mencegah tindakan yang belum terjadi. Ini berlaku pembatasan untuk apa Potensi pengguna, baik resmi atau tidak resmi. Contoh dari kontrol preventif administrasi adalah skrining obat pra kerja. Hal ini dirancang untuk mencegah organisasi dari mempekerjakan seorang karyawan yang menggunakan obat-obatan terlarang.

detektif

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

perbaikan

Kontrol pemulihan bekerja dengan "memperbaiki" sistem. korektif kontrol akses biasanya bekerja yang hubungan dengan kontrol akses detektif. Seperti Anti Virus perangkat lunak 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.

pemulihan

kontrol pemulihan mungkin perlu diulangi untuk mengembalikan fungsi dari sistem dan organisasi. Pemulihan berarti bahwa sistem harus pulih misalkan instal ulang OS Media atau gambar, data dikembalikan dari backup, dll

pencegah

pencegahan disini di contohkan seperti pencuri menghadapi dua bangunan, satu dengan anjing penjaga dan satu tanpa, lebih mungkin untuk menyerang anjing buildingwithout penjaga. Sebuah kebijakan yang membuat pengguna memahami bahwa mereka akan dipecat jika mereka tertangkap situs Web berselancar terlarang atau ilegal adalah pencegahan.

kompensasi

Sebuah kontrol kompensasi adalah kontrol keamanan tambahan dimasukkan ke dalam tempat untuk mengkompensasi kelemahan dalam kontrol lainnya.

METODE AUTHENTIKASI

Sebuah konsep kunci untuk melaksanakan jenis kontrol akses mengendalikan tepat otentikasi subyek dalam sistem IT. Seperti Subjek A pertama mengidentifikasi dirinya atau dirinya dan Identifikasi ini tidak bisa dipercaya. Subjek kemudian mengotentikasi dengan menyediakan jaminan bahwa identitas diklaim berlaku.

Tipe 1 otentikasi ini membutuhkan pengujian subjek dengan beberapa semacam tantangan dan respon dimana subjek harus merespon dengan luas menjawab. Subjek iberikan akses atas dasar sesuatu yang mereka tahu, seperti password atau PIN (Personal dentification Number, password nomor-based). Ini adalah bentuk paling mudah, dan sering lemah, otentikasi. Contohnya password.

Tipe 2 otentikasi mengharuskan pengguna memiliki sesuatu,seperti token, yang membuktikan mereka adalah pengguna dikonfirmasi. Token adalah sebuah objek yang membantu membuktikan klaim identitas.

Tipe 3 otentikasi adalah biometrik yang menggunakan karakteristik fisik sebagai sarana identifikasi atau otentikasi. Biometrikdapat digunakan untuk membentuk identitas atau untuk otentikasi (membuktikan klaim identitas). Sebagai contoh, sebuah Bandara sistem pengenalan wajah dapat digunakan untuk menentukan identitas suatu diketahui teroris, dan pemindai sidik jari dapat digunakan untuk otentikasi identitas subjek (yang membuat klaim identitas dan kemudian gesekan atau jarinya untuk membuktikannya).

TECHNOLOGIES ACCESS CONTROL

Ada beberapa teknologi yang digunakan untuk pelaksanaan kontrol akses. Karena setiap teknologi disajikan, penting untuk mengidentifikasi apa yang unik tentang masing-masing solusi teknis.

Single sign-on Sign-On tunggal (SSO) memungkinkan beberapa sistem untuk menggunakan server otentikasi pusat . Hal ini memungkinkan pengguna untuk mengotentikasi hanya satu kali dan kemudian mengakses beberapa sistem yang berbeda.

Hal ini juga memungkinkan administrator keamanan untuk menambah, mengubah, atau mencabut hak pengguna pada satu sistem pusat. Kerugian utama untuk SSO itu memungkinkan penyerang untuk mendapatkan akses ke beberapa sumber setelah mengorbankan salah satu metode otentikasi, seperti password. SSO harus selalu digunakan dengan otentikasi multifaktor untuk alasan ini.

Manajemen identitas federasi

Federated Identity Management (FIdM) berlaku Single Sign-On pada lebih luas skala, mulai dari lintas organisasi untuk skala Internet. Kadang-kadang hanya disebut Identity Management (IDM). FIdM dapat menggunakan OpenID atau SAML (Security Association Markup Language). Menurut EDUCAUSE, "manajemen Identitas mengacu pada kebijakan, proses, dan teknologi yang membangun identitas pengguna dan menegakkan aturan tentang akses ke sumber daya digital. Dalam pengaturan kampus, banyak sistem-seperti informasi e-mail, belajar sistem manajemen, database perpustakaan, dan komputasi grid aplikasi, mengharuskan pengguna untuk mengotentikasi diri (biasanya dengan username dan password). Sebuah proses otorisasi kemudian menentukan sistem yang pengguna dikonfirmasi diizinkan untuk mengakses. Dengan sistem manajemen identitas perusahaan, daripada harus kredensial terpisah untuk masing-masing sistem, pengguna dapat menggunakan identitas digital tunggal untuk mengakses semua sumber daya yang pengguna berhak. Federasi izin manajemen identitas memperluas pendekatan ini di atas tingkat perusahaan, menciptakan otoritas terpercaya untuk identitas digital di beberapa organisasi. Dalam sistem federasi, yang berpartisipasi lembaga atribut identitas saham berdasarkan disepakati standar, memfasilitasi otentikasi dari anggota lain dari federasi dan memberikan akses yang sesuai untuk sumber daya online. Pendekatan ini arus akses ke aset digital sekaligus melindungi sumber daya terbatas. "8

Kerberos

Kerberos adalah layanan otentikasi pihak ketiga yang dapat digunakan untuk mendukung Single Sign-On

SESAME

SESAME adalah Sistem Eropa Aman untuk Aplikasi di lingkungan multivendor, sistem single sign-on yang mendukung lingkungan yang heterogen. SESAME dapat dianggap sebagai sekuel dari jenis untuk Kerberos,