KEAMANAN INFORMASI

UAS 2015/2016

{Arci Nur Rahman}

(1310652017)

ACCESS CONTROL

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

Sebelum kita bisa menjelaskan kontrol akses , kita harus mendefinisikan keamanan informasi landasan konsep .Konsep itu adalah:
Kerahasiaan , integritas , dan ketersediaan
1.Kerahasiaan
kerahasiaan berusaha untuk mencegah akses data yang tidak sah. Contoh,dari serangan kerahasiaan akan pencurian pribadi diidentifikasi
Informasi (PII) , seperti informasi kartu kredit.
2.Integritas
integritas berusaha untuk mencegah akses tulis yang tidak sah.
3.Ketersediaan
Ketersediaan memastikan bahwa informasi yang tersedia ada bila diperlukan.Sistem harus dapat digunakan (tersedia) untuk penggunaan bisnis normal. Contoh dari serangan terhadap ketersediaan akan menjadi (DoS) serangan Denial -of -Service , yang berusaha untuk menolak layanan (atau ketersediaan) dari sistem .

Jenis-jenis pengendalian dalam keamanan informasi
Sistem pengendalian keamanan komputer secara relatif akan menghambat/menghalangi produktifitas. Untuk itu penerapan keamanan harus selalu dikompromikan secara praktis baik sistem, operasional dan administratif dengan produktifitas organisasi.
A. Pengendalian secara fisik
Pencegahan dalam pengendalian secara fisik
Pencegahan yang dimaksud disini adalah usaha mencegah pihak-pihak yang tidak berhak agar tidak memasuki / menggunakan sumberdaya komputer dan juga melindunginya dari bahaya bencana alam. Hal-hal yang termasuk kategori pencegahan ini adalah :

1. – Back-up file/dokumentasi : yaitu untuk mencegah agar bila terjadi kecelakaan terhadap sistem komputer, file/dokumen penting tetap ada. Dokumen back-up ini sebaiknya disimpan ditempat yang berjauhan dan dengan perlakuan keamanan yang setara dengan dokumen aktifnya.
2. – Pemagaran : yaitu untuk membatasi agar hanya orang-orang yang berhak saja yang dapat memasuki sistem. Termasuk dalam sistem pemagaran adalah CCTV, alarm, anjing penjaga dan pagar.
3. – Penjaga keamanan : pada intinya hampir sama dengan pemagaran namun dengan keunggulan dapat melihat hal-hal yang berkenaan dengan bawaan personel yang akan memasuki area sistem. Agar lebih efektif perlu ditunjang dengan alat-alat elektronik seperti detektor.

B. Pengendalian secara teknis

Pengamanan secara teknis ini meliputi penggunaan penjaga keamanan, yang mana termasuk didalamnya adalah hardware komputer, sistem operasi dan software aplikasi, komunikasi serta peralatan lain yang berhubungan. Pengendalian teknis ini dikenal pula sebagai pengendalian logika.

1. Pencegahan dalam pengendalian secara teknis

Pencegahan secara teknis digunakan untuk mencegah pihak yang tidak berhak baik orang maupun program untuk mengakses sumber daya komputer. Yang termasuk jenis pencegahan ini adalah :

– Software Access Control : digunakan untuk mengendalikan pertukaran data dan program antar user. Biasanya diimplementasikan dalam bentuk daftar access control yang mendefinisikan hak akses setiap user.

– Software Antivirus : virus merupakan program yang mewabah dalam komputer serta dapat merusak sistem dan data yang pada akhirnya menghambat produktifitas. Virus baru bermunculan dengan cepat, sehingga pemasangan software antivirus yang selalu up-date dan selalu aktif dalam komputer merupakan suatu keharusan.

– Sistem pengendalian pustaka : mengharuskan semua perubahan program produksi diimplementasikan oleh personel pengendali pustaka ini, hal ini untuk menghindari pihak yang tidak berhak melakukan perubahan.

– Password : digunakan untuk membuktikan bahwa pengguna atau pemilik ID adalah orang yang memang memiliki hak akses tertentu terhadap sistem.

Sekarang kita telah meninjau konsep kontrol akses landasan , kita bisa mendiskusikan berbeda model kontrol akses : model utama adalah akses Discretionary Control (DAC) , Wajib Access Control (MAC) , dan akses nondiscretionary control .

Discretionary Access Control (DAC)
Discretionary Access Control (DAC) memberikan pelajaran kontrol penuh dari benda-benda yang mereka miliki telah diberi akses, termasuk berbagi objek dengan mata pelajaran lain . subyek diberdayakan dan mengendalikan data mereka . Sistem operasi standar UNIX dan Windows menggunakan DAC untuk sistem berkas : subjek dapat memberikan akses mata pelajaran lain untuk file mereka.

Akses wajib Control (MAC)
Akses wajib Control (MAC) adalah sistem - ditegakkan kontrol akses berdasarkan subjek clearance dan label objek. Subjek dan objek memiliki izin dan label , masing-masing, seperti rahasia , rahasia , dan rahasia . Sebuah subjek mungkin mengakses objek hanya jika izin subjek sama dengan atau lebih besar dari label objek . Subyek tidak dapat berbagi objek dengan mata pelajaran lain yang tidak memiliki izin yang tepat atau " menulis " objek untuk tingkat klasifikasi yang lebih rendah (seperti sejak rahasia untuk rahasia) . Sistem MAC biasanya berfokus pada melestarikan
kerahasiaan data .

Nondiscretionary access control
Nondiscretionary access control (RBAC) mendefinisikan bagaimana informasi diakses pada sistem berdasarkan peran subjek . Peran A bisa menjadi perawat , administrator cadangan,bantuan teknisi meja , dll Subyek dikelompokkan menjadi peran dan peran masing-masing didefinisikan memiliki
izin akses berdasarkan peran , bukan individu .

RBAC adalah jenis kontrol akses nondiscretionary karena pengguna tidak memiliki kebijaksanaan mengenai kelompok benda mereka diizinkan untuk mengakses dan tidak mampu untuk mentransfer objek untuk mata pelajaran lainnya.Kontrol akses tugas berbasis model kontrol akses nondiscretionary lain ,berkaitan dengan RBAC .