Randy egan permana

1310652046

Teknik informatika/TI SORE

RESUME

Access Control

Kontrol akses memungkinkan perlindungan aset keamanan dengan membatasi akses ke sistem dan data dengan pengguna, aplikasi dan sistem lainnya. tapi tanpa diragukan lagi, penyewa kontrol akses suara adalah landasan dari setiap program keamanan informasi perusahaan.

Ada tiga kontrol akses yang harus dikelola: identitas, hak dan laporan. Ini sesuai dengan bidang otentikasi,. Identitas yang perlu dikelola termasuk nama pengguna, password, token keamanan dan faktor lain yang mengotentikasi pengguna. Misalnya, menetapkan atau mengatur ulang kata sandi pengguna adalah salah satu kontrol akses tugas manajemen yang sederhana.

Mengelola identitas telah menjadi dramatis lebih rumit seperti organisasi mengambil aplikasi yang lebih dan mendukung sumber daya tambahan komputasi atau penyimpanan. Hal ini telah menyebabkan pengenalan manajemen identitas (IDM) teknologi yang mengatur proliferasi account pengguna di bawah identitas dikelola tunggal. "Perusahaan yang bergerak ke model yang mana Anda mengelola identitas dan kemudian di bawah bahwa Anda memiliki login dan password,"

otentikasi membutuhkan pengujian subjek dengan beberapa semacam tantangan dan respon dimana subjek harus merespon dengan

pengetahuan jawaban yang luas. Subjek diberikan akses atas dasar sesuatu yang mereka tahu, seperti password atau PIN *(Personal Identification Number, password nomor-based).* Ini adalah bentuk paling mudah, dan sering lemah,

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 terhadap ancaman seperti akses yang tidak sah, modifikasi data yang tidak pantas, dan hilangnya kerahasiaan. otentikasiadalah biometrik, yang menggunakan karakteristik fisik sebagai sarana identifikasi atau otentikasi. Biometrics dapat digunakan untuk membentuk identitas atau untuk membuktikan klaim identitas. Sebagai contoh, sebuah Bandara sistem pengenalan wajah dapat digunakan untuk menentukan identitas teroris, dan pemindai sidik jari dapat digunakan untuk otentikasi identitas subjek (yang membuat klaim identitas dan kemudian gesekan atau jarinya untuk membuktikannya).

Sebuah konsep kunci untuk melaksanakan jenis kontrol akses yang mengendalikan tepat pada otentikasi subyek dalam sistem IT. Subjek A pertama mengidentifikasi dirinya atau orang lain; Identifikasi ini tidak bisa dipercaya. Subjek kemudian mengotentikasi dengan menyediakan jaminan bahwa identitas diklaim berlaku. Satu set credential adalah istilah yang digunakan untuk kombinasi keduanya identifikasi dan otentikasi pengguna.