Akses Control

Identity and authentication, authorization, and accountability

1.***Authentication*** adalah suatu proses dimana user diidentifikasi oleh server AAA sebelum user menggunakan jaringan. Pada proses ini, user meminta hak akses kepada NAS untuk menggunakan suatu jaringan. NAS kemudian menanyakan kepada server AAA apakah user yang bersangkutan berhak untuk menggunakan jaringan atau tidak.

Faktor-Faktor Autentikasi

Tiga jenis faktor autentikasi yang umum digunakan adalah:

a.Sesuatu yang diketahui oleh pengguna Contoh: *password*, *passphrase*, dan PIN (*Personal Identification Number*)
b.Sesuatu yang dimiliki oleh pengguna Contoh: *ID card*, kartu kredit, telepon seluler, dan perangkat token
c.Sesuatu yang 'ada' pada pengguna Contoh: sidik jari, DNA, suara, pola retina,
atau aspek biometrik lain.

Sedangkan, beberapa faktor autentikasi lain yang lebih jarang digunakan adalah:
a.Berbasis pengenalan (*recognition*) atau autentikasi cognometric, yaitu sesuatu yang dikenal oleh pengguna Contoh: Pengguna harus mengenali dari beberapa wajah yang dirahasiakan.
b.Berbasis *cybermetric*, yaitu sesuai yang ada pada komputer Contoh: Membatasi akses hanya dari komputer yang memiliki kombinasi unik hardware dan software tertentu.

c.Berbasis lokasi Contoh: Membatasi penggunaan ATM atau kartu kredit hanya pada cabang tertentu, membatasi login root hanya dari terminal tertentu.
d.Berbasis waktu Contoh: Membatasi penggunaan sebuah account hanya pada waktu tertentu, misalnya jam kerja.
e.Berbasis ukuran Contoh: Membatasi terjadinya transaksi hanya pada sejumlah tertentu saja.

2.***Authorization*** adalah pengalokasian layanan apa saja yang berhak diakses oleh user pada jaringan. Authorization dilakukan ketika user telah dinyatakan berhak untuk menggunakan jaringan.

3.***Accounting*** merupakan proses yang dilakukan oleh NAS dan AAA server yang mencatat semua aktivitas user dalam jaringan, seperti kapan user mulai menggunakan jaringan, kapan user mengakhiri koneksinya dengan jaringan, berapa lama user menggunakan jaringan, berapa banyak data yang diakses user dari jaringan, dan lain sebagainya. Informasi yang diperoleh dari proses accounting disimpan pada AAA server, dan dapat digunakan untuk berbagai keperluan seperti billing, auditing, atau manajemen jaringan.

Ada enam jenis kontrol akses:

- Pencegahan
- Detektif
- Corrective
- Pemulihan
- Pencegah
- Kompensasi

Sign-On tunggal (SSO) memungkinkan beberapa sistem untuk menggunakan server otentikasi pusat (AS). Hal ini memungkinkan pengguna untuk mengotentikasi sekali 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 faktor otentikasi multi-untuk alasan ini.

NIM:1310651072
Nama:Aditya Rizky P
Kelas E