

Efektivitas Kontrol Akses Sistem Komputer di Dalam Organisasi

Anita Arianti

ABSTRAK

Bagi para profesional keamanan sistem teknologi informasi, perhatian harus diberikan pada kebutuhan akses kontrol dan metode-metode implementasinya untuk menjamin bahwa sistem memenuhi *availability* (ketersediaan), *confidentiality* (kerahasiaan), dan *integrity* (integritas). Dalam komputer jaringan, juga diperlukan pemahaman terhadap penggunaan akses kontrol pada arsitektur terdistribusi dan terpusat.

Mekanisme kontrol perlu ditempatkan untuk mendata siapa yang dapat mengakses data dan apa yang orang dapat lakukan terhadapnya saat pertama kali diakses. Aktivitas tersebut harus dikontrol, diaudit, dan dimonitor. Beberapa tipe informasi yang dipertimbangkan sebagai informasi rahasia adalah misalnya catatan kesehatan, informasi laporan keuangan, catatan kriminal, kode sumber program, perdagangan rahasia, dan rencana taktis militer. Sedangkan beberapa mekanisme yang memberikan kemampuan kerahasiaan sebagai contoh yaitu enkripsi, kontrol akses fisik dan logikal, protokol transmisi, tampilan database, dan alur trafik yang terkontrol.

Dengan mengkombinasikan sifat kontrol dan implementasinya diharapkan dapat mengefektifkan akses kontrol dalam suatu perusahaan melalui beberapa model dan metode yang diterapkan.

DAFTAR ISI

LEMBAR PENGESAHAN	i
LEMBAR PERNYATAAN PUBLIKASI LAPORAN PENELITIAN.....	ii
LEMBAR PERNYATAAN ORISINALITAS LAPORAN PENELITIAN	iii
KATA PENGANTAR	iv
ABSTRAK	vi
DAFTAR ISI	vi
DAFTAR GAMBAR	ix
DAFTAR TABEL	x

BAB I PENDAHULUAN

I.1 Latar Belakang	1
I.2 Rumusan Masalah.....	3
I.3 Tujuan Pembahasan	3
I.4 Batasan Masalah.....	4
I.5 Sistematika Pembahasan.....	4

BAB II LANDASAN TEORI

II.1 Pengertian Dasar Kontrol Akses.....	6
II.2 <i>Least Privilege</i>	8
II.3 Teknik-Teknik Kontrol Akses	8
II.3.1. Rancangan Kontrol Akses	9
II.3.1.1 <i>Mandatory Access Control</i>	9
II.3.1.2 <i>Discretionary Access Control</i>	10
II.3.1.3 <i>Nondiscretionary Access Control</i>	11
II.4 <i>Access Control Administration</i>	11
II.4.1 <i>Centralized Access Control</i>	11
II.4.2 <i>Decentralized Access Control</i>	12
II.5 <i>Accountability</i>	13
II.6 Metode Otentikasi dan Identifikasi	14
II.6.1 Metode Otentikasi	14
II.6.2 Metode Identifikasi	16
II.6.2.1 <i>Single Sign On</i>	16
II.6.2.2 <i>Kerberos</i>	17
II.7 Sumber Lubang Keamanan.....	17

BAB III ANALISIS DAN PEMODELAN

III.1 Analisis Metode Penyerangan Terhadap Kontrol Akses	20
III.2 Kepemilikan File dan Data	22
III.2.1 <i>Data Owner</i> (Pemilik Data).....	22
III.2.2 <i>Data Custodian</i> (Pemelihara Data).....	22
III.2.3 <i>Data User</i> (Pengguna Data).....	23
III.3 Model Kontrol Akses.....	23
III.3.1 <i>State Machine</i>	23

III.3.1.1 Model <i>Bell-LaPadula</i>	24
III.3.1.2 Model <i>Biba</i>	25
III.3.1.3 Model <i>Clark-Wilson</i>	26
III.3.1.4 Model <i>Noninterference</i>	26
BAB IV IMPLEMENTASI DAN PENGUJIAN	
IV.1 Profil Perusahaan	28
IV.2 Struktur Organisasi Perusahaan	29
IV.3 Aplikasi yang digunakan pada PT. Sumber Kerang Indah	31
IV.4 Kebijakan Keamanan Teknologi pada PT. Sumber Kerang Indah	34
IV.5 Kebijakan Penerapan Keamanan Teknologi Informasi	35
IV.6 Implementasi <i>The Clark-Wilson Integrity Model</i>	40
BAB V KESIMPULAN DAN SARAN	
V.1 Kesimpulan	47
V.2 Saran	48
DAFTAR PUSTAKA	49
RIWAYAT HIDUP PENULIS	

DAFTAR GAMBAR

Gambar 1. <i>Biometric</i>	16
Gambar 2. <i>State Machine</i> sederhana	24
Gambar 3. Struktur Organisasi PT. Sumber Kerang Indah.....	30
Gambar 4. Aplikasi SKIK (Penjualan LPG)	32
Gambar 5. Aplikasi SKIP (Penjualan Pelumas)	33
Gambar 6. Aplikasi SKIT (Transportir BBM)	34

DAFTAR TABEL

Table I. Kategori Kontrol Umum.....	6
Tabel II. <i>Military Classifies Document</i>	9
Tabel III. Klasifikasi Data Komersil.....	10
Tabel IV. Tipe Otentikasi.....	14
Tabel V. Properti <i>Bell-LaPadula</i>	25
Tabel VI Properti <i>Biba</i>	25
Tabel VII. Interpretasi <i>Window Server 2008</i> pada Model <i>Clark – Wilson</i>	44
Tabel VII. Interpretasi <i>Redhat</i> pada Model <i>Clark – Wilson</i>	46