BAB I
PENDAHULUAN

I.1 Latar Belakang

Dalam mengoperasikan Sistem Informasi Komputer, faktor keamanan data merupakan hal penting yang perlu diperhatikan. Semua ancaman dapat terjadi kapan saja. Oleh karena itu, sebaiknya kita terlebih dahulu mencegah dan mendeteksi ancaman-ancaman terhadap sistem serta memperbaikinya jika ancaman tersebut telah merusak sistem kita. Melakukan kontrol akses pada sistem informasi dan jaringan yang terkait, merupakan hal penting untuk menjaga *confidentiality, integrity, authentication* dan *availability.*

Confidentiality atau kerahasiaan dapat diartikan sebagai perlindungan terhadap data dalam sistem informasi perusahaan, sehinggga data perusahaan tidak dapat diakses oleh orang yang tidak berhak. Banyak yang beranggapan bahwa tipe perlindungan seperti ini hanya penting untuk kalangan militer dan pemerintahan, karena mereka perlu merahasiakan rencana dan data yang penting. Akan tetapi kerahasian juga sangat penting bagi kalangan bisnis yang perlu melindungi rahasia dagang mereka dari kompetitor, atau untuk mencegah akses terhadap data yang dianggap sensitif oleh orang-orang yang tidak berhak. Isu seputar privasi yang semakin diperhatikan akhir-akhir ini, telah memaksa badan pemerintahan dan perusahaan swata sekalipun untuk menjaga kerahasiaan informasi secara lebih baik lagi, demi melindungi data pribadi yang disimpan dalam sistem informasi badan pemerintahaan atau perusahaan swasta tersebut.

Integrity atau integritas merupakan perlindungan terhadap sistem dari perubahan yang tidak terotorisasi, baik secara sengaja maupun secara tidak sengaja. Tantangan yang dihadapi setiap sistem keamanan informasi adalah

untuk memastikan bahwa data terpelihara dalam keadaan yang baik. Walau tidak dapat meningkatkan akurasi dari data yang dimasukkan kedalam sistem oleh pemakai. Inisiatif keamanan informasi memastikan bahwa setiap perubahan memang benar-benar dikehendaki dan dilakukan secara benar.

Elemen tambahan dari integritas adalah kebutuhan untuk melindungi proses atau program yang digunakan untuk memanipulasi data dari modifikasi yang tidak terotorisasi. Saat paling penting dalam pemrosesan data dari kalangan komersial dan pemerintahan adalah memastikan integritas data untuk mencegah penipuan (*fraud*) dan kesalahan (*error*).

Authentication atau otentikasi merupakan aspek yang berhubungan dengan metode atau cara untuk menyatakan bahwa informasi betul-betul asli, orang yang mengakses atau memberikan informasi adalah betul-betul orang yang dimaksud. Biasanya metode yang sangat kita kenal untuk terkoneksi dan masuk ke dalam sistem adalah dengan metode *password* di mana terdapat suatu karakter yang diberikan oleh pengguna ke *server* dan *server* mengenalinya sesuai dengan kebijakan (*policy)* yang ada. Saat ini dengan perkembangan teknologi informasi terdapat beberapa metode *authentication* atau otentikasi yang lebih canggih dan aman seperti menggunkan retina mata, pengenalan suara, dan telapak tangan pengguna.

Availability (ketersediaan) memastikan bahwa bagi pengguna (*user*) yang berhak memakai sistem, memiliki waktu dan akses yang bebas gangguan pada informasi dalam sistem. Informasi, sistem, dan sumberdaya harus tersedia untuk pengguna (*user*) pada waktu diperlukan sehingga produktifitas tidak terpengaruh. Kebanyakan informasi perlu dapat diakses dan tersedia bagi pengguna (*user*) saat diminta, sehingga mereka dapat menyelesaikan tugas-tugas dan memenuhi tanggung jawab pekerjaan mereka.

Tujuan kontrol akses lainnya adalah *reliability* dan *utilitas*. Tujuan-tujuan tersebut mengalir dari kebijakan keamanan suatu organisasi. Kebijakan ini merupakan pernyataan tingkat tinggi dari pihak manajemen berkaitan dengan

kontrol pada akses suatu informasi dan orang yang berhak menerima informasi tersebut.

Tiga hal lainnya yang patut dipertimbangkan untuk perencanaan dan implementasi mekanisme kontrol akses adalah ancaman pada sistem (*threats*), kerawanan sistem pada ancaman (*vulnerabilities*), dan resiko yang ditimbulkan oleh ancaman tersebut.

I.2 Rumusan Masalah

Saat ini kita berada pada era digital kemajuan komunikasi dan pertukaran informasi berlangsung dalam suatu jaringan yang kian hari semakin meluas. Di dalam sistem tersebut, pengguna *(use*r) saling berinteraksi melalui sebuah pengenal untuk merepresentasikan dirinya. Pengenal ini lazim disebut identitas *user*. Pengguna yang telah memiliki hak akses memiliki wewenang untuk mengolah data yang terdapat dalam sistem tersebut. Namun, kita perlu waspada dengan kemajuan teknologi yang begitu pesat. Banyak orang yang tidak bertanggung jawab menyalahgunakan kemajuan teknologi. Hal inilah yang perlu kita hindari, pentingnya kontrol akses dalam suatu sistem komputer dalam suatu organisasi untuk mengantisipasi penyusup-penyusup yang tidak bertanggung jawab serta ancaman baik itu ancaman *virus* maupun ancaman dari alam.

Oleh karena itu diperlukan suatu kebijakan dalam menerapkan keamanan teknologi informasi yang berfungsi menghindari berbagai ancaman yang dapat menggangu keutuhan suatu data di dalam suatu organisasi.

I.3 Tujuan Pembahasan

Adapun tujuan dari pembuatan tugas akhir ini adalah :

1. Menganalisis dan menentukan kebijakan penerapan keamanan teknologi informasi di dalam organisasi.
2. Menghindari hal-hal yang tidak diinginkan yang dapat merusak kerahasiaan, integritas dan ketersediaan data pada sistem komputer.
3. Mengimplementasikan model kontrol akses untuk menghindari ancaman-ancaman terhadap data di dalam suatu perusahaan.

I.4 Batasan Masalah

Mengingat pembahasan mengenai kontrol akses cukup luas maka penulis membatasi ruang lingkup tugas akhir ini dengan beberapa hal diantaranya :

1. Pemahaman kontrol akses dan metodologinya.
2. Analisis serta menjelaskan model-model kontrol akses.
3. Penerapan kebijakan kontrol akses terhadap dunia nyata.
4. Pengimplementasian model kontrol akses di dalam perusahaan.

I.5 Sistematika Pembahasan

Sistematika penulisan laporan tugas akhir ini dimaksudkan untuk mempermudah pembahasan dan memberikan gambaran yang jelas, sistematika penulisan laporan tersebut dijelaskan sebagai berikut :

BAB I PENDAHULUAN

Berisi penjelasan mengenai latar belakang, rumusan masalah, tujuan pembahasan, ruang lingkup kajian, sumber data, sistematika penulisan.

BAB II DASAR TEORI

Menguraikan pengertian serta konsep dasar akses kontrol suatu sistem komputer.

BAB III ANALISIS DAN PEMODELAN

Menguraikan analisis mengenai model-model kontrol akses yang akan digunakan secara lengkap.

BAB IV IMPLEMENTASI DAN PENGUJIAN

Menguraikan bagaimana menerapkan kebijakan keamanan teknologi informasi di dunia nyata serta implementasi model kontrol akses terhadap sistem komputer.

BAB V KESIMPULAN DAN SARAN

Pada bab kesimpulan dan saran mengemukakan kesimpulan yang dapat ditarik dari seluruh uraian dan saran yang diajukan.