Materi 5

Keamanan Sistem Informasi

3 SKS | Semester 8 | S1 Sistem Informasi | UNIKOM | 2015
Nizar Rabbi Radliya | nizar.radliya@yahoo.com

Nama Mahasiswa	
NIM	
Kelas	

Kompetensi Dasar

Memahami kontrol logical security pada sistem informasi..

Pokok Bahasan

Manajemen Resiko Sistem Informasi
1. Tujuan *logical security*
2. Aplikasi *logical security*
3. Tanggungjawab pemberian kontrol

I. Tujuan *Logical Security*

Logical security merupakan jenis kontrol dalam sebuat sistem informasi yang berikaitan dengan aturan pengaksesan pengguna sesuai dengan wewenang yang diberikan/ditentukan dalam penggunaan data/informasi serta program-program sistem informasi. Maka dari itu logical security banyak berhubungan dengan *user-ID* untuk setiap pengguna sistem informasi.

Logical security bertujuan untuk:

1. Melindungi data/informasi yang tersimpan di dalam perangkat sistem informasi, dari perusakan atau penghancuran yang dilakukan baik disengaja maupun tidak disengaja.
2. Menghindari dan mendeteksi perubahan terhadap data/informasi yang dilakukan oleh pihak yang tidak berwenang, serta menjaga agar informasi tidak disebarkan kepada pihak yang tidak berwenang.

II. Aplikasi *Logical Security*

Terdapat beberapa pengaplikasian *logical security* terhadap sistem informasi yang pada umumnya aplikasi tersebut juga diimplementasikan ke dalam beberapa sistem aplikasi lainnya. Pengaplikasian tersebut diantaranya *user-ID, password, access level, closed menu*.

2.1. User-ID

Tujuan dari *user-ID* adalah untuk mengidentifikasi pengguna yang memiliki otoritas untuk mengakses sistem informasi. Sebelumnya sistem harus mendapatkan data semua *user-ID* yang akan disimpan pada basisdata sistem informasi. *User-ID* merupakan perisai pertama terhadap pengaksesan sistem. Setiap *user-ID* harus diidentifikasi oleh satu data yang bersifat unik (biasanya berupa kunci utama dalam sebuah basisdata). Beberapa data yang biasanya termasuk ke dalam *user-ID* diantaranya:

1. *Username*

   Username merupakan data yang menidentifikasi setiap pengguna. *Username* lebih baik bersifat unik untuk dapat mengidentifikasi setiap pengguna. *Username* dapat dibuat menggunakan kodifikasi. Sebagai contoh *username* dengan nilai BDGCSAP001 (BDG = Bandung, CS = *Customer Service*, AP = Agus Putra, 001 = Nomor urut apabila ada pengguna yang bekerja di bagian yang sama dan nama yang sama).

2. *Password*

   Password juga merupakan bagian dari data set *user-ID*. Tetapi dalam materi ini akan dibahas secara terpisah di sub bab berikutnya. *Password* merupakan kunci untuk masuk ke dalam sistem atau mendapatkan akses.

3. *Initial Menu*

   Initial menu merupakan informasi menu apa saja yang akan ditampilkan pada sebuah sistem informasi berkaitan dengan hak akses setiap pengguna. Sebagai contoh pada sistem informasi akademik, menu untuk bagian akademik dengan menu untuk guru harus berbeda. Daftar menu yang dapat ditampilkan untuk setiap jenik hak akses dapat disimpan dalam basis data atau juga dapat diseleksi langsung menggunakan kode program.

4. *Output Queue*

   Menentukan arah *output* dari setiap proses yang harus dikirimkan oleh sistem.

5. *Special Authorities*

   Apabila terdapat seorang pengguna yang diberikan wewenang tambahan untuk mengakses data atau proses, dapat didefinisikan di bagian *special authorities.*

6. *Password change date*

   Tanggal setiap ada perubahan password harus selalu terekam atau tersimpan.

7. *Access Levels*

   Menentukan hak pengaksesan untuk setiap level pengguna yang berkaitan dengan data dan program (modul). Pembahasan lebih lengkap ada pada sub bab berikutnya.

2.2. Password

Password berkaitan dengan *user-ID,* untuk membuktikan bahwa pengguna memiliki wewenang untuk memaki dan masuk ke dalam sistem. Oleh karena itu setiap pengguna sebelum masuk ke dalam sistem informasi harus mengetik/memasukan *username* beserta *password*. Untuk menghindari percobaan pengaksesan oleh pengguna yang tidak memiliki wewenang, harus dikontrol dengan mengkombinasikan kontrol preventif dan pendeteksian. Hal tersebut dapat dilakukan dengan cara:

1. Ditentukan batasan kesalahan dalam memasukan *username* dan *password* (misalnya sebanyak 3 kali). Apabila sudah melebihi batas tersebut maka secara otomatis username yang berkaitan dinonaktifkan oleh sistem. Dapat juga dinonaktifkan terminal yang dipakai apabila tidak akan menggangu proses sistem informasi lainnya. Untuk fasilitas pengaktifan dapat diterapkan pada sistem administrator. Kontrol ini juga dapat memberikan informasi terhadap pemilik sistem bahwa adanya aktifitas percobaan pengaksesan sistem secara illegal.
2. Percobaan tersebut harus direkam di *log file.* Dimana nantinya secara berkala harus diaudit untuk menginvestigasi beberapa penyebabnya.

Sistem informasi yang baik akan merekam semua kegiatan pengguna (diwakili oleh *user-ID* setiap pengguna). Contohnya sistem akan merekam *user-ID* (beserta tanggal kejadian) yang melakukan perubahan dan penghapusan terhadap data. Pada tabel 1 di bawah ini terdapat beberapa saran untuk pengontrolan password.

Tabel 1. Pengontrolan *Password*

Ketentuan Kontrol	Penerapan Kontrol
Password harus terdiri dari panjang dan kombinasi karakter yang telah ditentukan. Contonya jumlah karakter minimal adalah 6 dan maksimal adalah 16, serta harus menggunakan kombinasi alfanumerik.	Pengentrolan dapat dilakukan oleh sistem.
Tidak diperbolehkan menggunakan nama pribadi, hobi, atau data-data pribadi lainnya yang mudah ditebak.	Pengentrolan dapat dilakukan oleh sistem dan peraturan perusahaan.
Setiap pengguna bertanggung jawab atas penggantian *password* pada fasilitas yang telah disediakan oleh sistem.	Pengentrolan dapat dilakukan oleh sistem dan peraturan perusahaan.

Pada jangka waktu tertentu *password* harus diganti, misalnya 3 bulan sekali. Sedangkan untuk sistem yang memiliki resiko tinggi *password* harus diganti lebih sering.	Pengentrolan dapat dilakukan oleh sistem.
Password tidak boleh ditampilkan di layar monitor atau dicetak.	Pengentrolan dapat dilakukan oleh sistem dan peraturan perusahaan.
Setiap *password* tidak boleh diberikan terhadap pengguna atau karyawan lain.	Pengentrolan dapat dilakukan oleh peraturan perusahaan.
Apabila karyawan meninggalkan perusahaan atau pindah ke unit kerja yang lain, maka *password* beserta *user-ID* harus segera dihapus atau diganti.	Pengentrolan dapat dilakukan oleh peraturan perusahaan.
Paling ideal apabila setiap individu memiliki satu *password* untuk semua aktivitas yang ia lakukan dengan sistem.	Pengentrolan dapat dilakukan oleh sistem.
Apabila karyawan absen untuk beberapa saat (cuti, mengikuti pelatihan, dan lain-lain), maka sebaiknya *user-ID* beserta *password* harus dinonaktifkan.	Pengentrolan dapat dilakukan oleh sistem dan peraturan perusahaan.
Untuk *password* yang sangat kritis (contoh password master administrator) harus dipersiapkan prosedur pengambilalihan (untuk kondisi darurat). Serta harus ada berita acara pengambilalihan password.	Pengentrolan dapat dilakukan oleh prosedur perusahaan.

Semua ketentuan diatas dapat kita terapkan pada dokumen *job description* untuk setiap karyawan atau dapat juga dicantumkan ke dalam *manual book* sistem informasi.

2.3. Access Level

Setelah pengguna berhasil masuk ke dalam sistem dengan menggunakan user-ID dan passwordnya, maka sistem hanya akan menyediakan data dan informasi yang sesuai dengan level akses pengguna tersebut. Selain itu modul-modul yang digunakan juga sesuai dengan level akses. Oleh karena itu rincian tingkat pengaksesan harus diimplementasikan ke dalam sistem. Berikut beberapa level akses yang umum diterapkan, diantaranya:

1. *No Access*

   Tingkat pengaksesan ini berarti pengguna tidak diizinkan memakai program beserta datanya. Sebagai *default*, semua file dan program memiliki tingkat pengaksesan ini.

2. *Execute*

   Tingkat pengaksesan ini berlaku untuk program yang diizinkan untuk dijalankan oleh pengguna.

3. *Read Only*

Pengguna hanya diperbolehkan untuk menjalankan program yang diakses dengan membaca atau mencetak beberapa file yang berkaitan dengan program tersebut. Akan tetapi tidak diberikan akses untuk memodifikasi dan/atau menghapus data yang ada pada file tersebut.

4. *Modify/Update*

   Pengguna diberikan akses untuk memodifikasi data yang ada pada file.

5. *Delete*

   Pengguna diberikan akses untuk menghapus data yang ada pada file.

6. *Add/Write*

   Memungkinkan pengguna untuk menambahkan *record* ke dalam file.

7. *Owner*

   Memungkinkan pengguna memberikan hak pengaksesan terhadap file-file atau/dan menjalankan program-program tertentu kepada pengguna lain.

2.4. Closed Menu

Closed menu merupakan informasi menu apa saja yang akan ditampilkan pada sebuah sistem informasi berkaitan dengan hak akses setiap pengguna. Setiap pengguna akan diberikan menu program sesuai hak akses yang sudah ditentukan. Sebagai contoh pada sistem informasi akademik, menu untuk bagian akademik dengan menu untuk guru harus berbeda. Daftar menu yang dapat ditampilkan untuk setiap jenik hak akses dapat disimpan dalam basis data atau juga dapat diseleksi langsung menggunakan kode program.

III. Tanggungjawab Pemberian Kontrol

Tanggungjawab untuk pemberian kontrol terhadap tingkat pengaksesan untuk setiap pengguna biasanya dibebankan kepada *security administrator*. Jabatan tersebut memiliki wewenang untuk membuat, mengganti, dan menghapus *user-ID* beserta *password* dan tingkat pengaksesan. Pada tabel 2 di bawah ini terdapat beberapa contoh yang dapat dilakukan untuk memeriksa logical security.

Tabel 2. Hal-hal Yang Diperhatikan Dalam Memeriksa *Logical Security*

Aktivitas	Resiko
Tentukan apakah daftar *user accounts* yang berlaku sesuai dengan daftar karyawan perusahaan. Uji coba: Cocokan daftar *user accounts* yang berlaku saat ini dengan dartar karyawan yang masih bekerja di perusahaan.	*User* (pengguna) yang sudah tidak berwenang atau karyawan yang tidak bekerja lagi di perusahaan masih tetap bisa mengakses sistem informasi perusahaan.

Tentukan dan periksa bahwa *user profile* yang terdaftar dapat mengidentifikasi nama pengguna. Uji coba: Cocokan daftar *user accounts* yang berlaku saat ini dengan dartar karyawan yang masih bekerja di perusahaan.	*User* (pengguna) yang tidak dikenal, tidak dapat mempertangjawabkan segala aktivitasnya di dalam sistem.
Tentukan apakah setiap pengguna hanya memiliki satu *user account*. Uji coba: Cocokan daftar *user accounts* yang berlaku saat ini dengan dartar karyawan yang masih bekerja di perusahaan.	Dengan memiliki *user accounts* lebih dari satu dapat menghambat *segregation of duties* yang diterapkan oleh perusahaan. Contohnya bagian penjualan dapat masuk ke menu bagian akuntansi.
Tentukan apakah user profile "*GUEST*" (tidak jelas siapa pemiliknya) yang diberikan oleh pengguna sudah dinon-aktifkan. Uji coba: cek melalui user manager apakah"*GUEST*" sudah dinon-aktifkan.	Apabila terjadi kerusakan atau pemanipulasian informasi, akan sulit untuk melacak pelakunya.
Tentukan apakah ketentuan *password* wajib diterapkan di *user profile*. Uji coba: cek apakah batas minimum dan maksimum panjang *password* sudah sesuai. Tidak dibenarkan untuk mengosongkan *password*.	Semua orang dapat masuk hanya menggunakan *user profile* yang sah.
Tentukan masa berlaku *password* sudah sesuai dengan rekomendasi perusahaan. Uji coba: cek di *account policy/active directory* penetapan "*maximum password age*"	Apabila *password* diketahui oleh orang lain tanpa sepengetahuan pemiliknya, maka orang yang tidak berwenang akan dapat mengakses sistem.
Tentukan apakah *password* dapat dengan mudah diterka. Uji coba: cek di *account policy/active directory* penetapan "*maximum password length*" dan apakah sistem memaksa untuk memakai *password* yang terdiri dari kombinasi *character* dan *alpha-numeric*.	Password akan mudah diterka oleh pengguna yang tidak berwenang.
Tentukan apakah *password* yang sama tidak dapat dipergunaan dalam kurun waktu 13 kali perubahan *password*. Uji coba: cek apakah "*password unique*" diisi dengan nilai 12 di *account policy/active directory*.	Mempergunakan password sebelumnya yang perna diketahui oleh orang lain.
Tentukan apakah fungsi *time-out* dipergunakan. Uji coba: Setelah *log-in* lalu diamkan *workstation* untuk beberapa saat tanpa aktivitas sampai pada batas *time-out* yang sudah ditentukan.	Pengaksesan oleh orang yang tidak berwenang ke dalam sistem, dikarenakan pengguna yang berwenang meningkalkan *workstation* untuk waktu yang cukup lama dengan tidak melakukan *log-off*.
Periksa bahwa setting *wokstation* tidak dapat diubah oleh *user*.	Keutuhan *workstation security* tidak dapat dijamin.
Periksa bahwa *workstation* hanya dapat digunakan pada hari kerja dan jam yang telah ditentukan.	Penyalahgunaan *user account* di luar jam kerja.

Uji coba: pergunakan *workstation* diluar jam kerja yang telah ditentukan.	
Periksa bahwa wewenang "*backup file and directories*" hanya diberikan kepada orang yang telah ditunjuk, misalnya administrator.	Kerahasiaan data perusahaan tidak dapat dijamin.

IV. Daftar Pustaka

[1] IBISA. 2011. Keamanan Sistem Informasi. Yogyakarta: Andi.
[2] Isa, I. 2012. Evaluasi Pengontrolan Sistem Informasi. Yogyakarta: Graha Ilmu.
[3] Laudon, K.C. & Laudon, J.P. 2005. Sistem Informasi Manajemen: Mengelola Perusahaan Digital, Edisi 8. Yogyakarta: Andi.
[4] Sarno, R. & Iffano, I. 2010. Sistem Manajemen Keamanan Informasi (Berbasis ISO 27001). Surabaya: ITS Press.

V. Materi Berikutnya

Pokok Bahasan	Physical Security
Sub Pokok Bahasan	1. Tujuan *physical security* 2. Kontrol *physical security*