JURNAL DASI
Vol. 12 No. 1 MARET 2011
ISSN: 1411-3201

KEAMANAN USER DATABASE

M. Rudyanto Arief
STMIK AMIKOM Yogyakarta
rudy@amikom.ac.id

ABSTRAKSI

Informasi merupakan aset yang sangat berharga bagi sebuah organisasi. Kebanyakan organisasi menyimpan data dan informasi mereka didalam sebuah program basis data (database management system). Untuk menjamin bagaimana keamanan data didalam sebuah program basis data aman, maka banyak perusahaan (vendor) pembuat program basis data menerapkan fitur-fitur pengamanan yang relevan untuk program basis data mereka. Untuk memahami bagaimana cara kerja fitur-fitur pengamanan tersebut yang berbeda untuk masing-masing vendor maka diperlukan pemahaman konsep pengamanan didalam program basis data secara umum

Kata Kunci : *Privileges, user account, database object privileges, database, database system privileges, roles, profiles, minimum least privileges database, grant, revoke*, stmik amikom yogyakarta

LATAR BELAKANG

Basis data saat ini sudah mulai banyak diterapkan dalam bisnis, baik bisnis skala kecil maupun bisnis skala besar (enterprise). Hal ini disebabkan oleh meningkatnya kesadaran pelaku bisnis bahwa data bagi organisasi mereka merupakan aset yang harus dijaga dan dikelola dengan baik. Pertumbuhan yang cukup pesat didalam sebuah organisasi bisnis secara otomatis akan menambah jumlah data yang dikelola oleh organisasi tersebut, sehingga tidak mungkin lagi mengelola semua data-data tersebut dengan menggunakan cara-cara konvensional tanpa melibatkan sistem komputerisasi.

Semua sistem informasi yang digunakan oleh pelaku bisnis pasti bersifat dinamis dan itu artinya harus melibatkan komponen basis data didalamnya. Menyadari hal tersebut maka saat ini banyak vendor yang membuat aplikasi pengolah basis data/ database management system mulai berlomba untuk menawarkan fitur-fitur yang menarik bagi pelaku bisnis yang akan mengembangkan sistem informasi yang menggunakan aplikasi pengolah basis data didalamnya. Beberapa vendor/ perusahaan yang membuat aplikasi pengolah basis data atau biasa juga disebut database misalnya Oracle, Microsoft, IBM.

Saat ini pelaku bisnis diberikan banyak pilihan jenis database seperti apa yang akan mereka pilih dan gunakan yang mampu mengolah data-data didalam organisasi mereka. Pilihan tersebut mulai dari aplikasi database yang berbayar seperti Oracle, Microsoft SQL Server, IBM DB2 atau database yang bersifat gratis (open-source) seperti MySQL, PostGreSQL. Tentunya beberapa contoh yang disebutkan diatas adalah contoh database yang termasuk database server yang dapat menampung data dalam jumlah yang banyak serta memiliki kinerja yang dapat diandalkan untuk organisasi bisnis dengan jumlah data yang banyak serta menerapkan sistem berasitektur clinet-server didalam sistem informasinya.

Bagi perusahaan dalam memilih aplikasi database seperti apa yang cocok bagi perusahaan mereka tentunya banyak pertimbangan yang perlu diperhatikan. Pertimbangan tersebut diantaranya lebih banyak disebabkan oleh karena data-data yang dimiliki oleh perusahaan tersebut merupakan aset sehingga harus dapat dijamin kehandalan dari aplikasi database tersebut jika mengolah data-data dalam jumlah yang banyak. Selain faktor kehandalan, faktor yang lain yang sama pentingnya untuk diperhatikan adalah mengenai keamanan/ security yang berkaitan dengan pengelolaan data dan user didalam aplikasi database tersebut. Metode pengamanan yang tepat dapat menjadikan data didalam sebuah aplikasi database menjadi aman.

Saat ini hampir semua vendor pembuat aplikasi database menawarkan berbagai macam mekanisme pengamanan didalam produk database yang mereka produksi. Hal inilah yang menjadi fokus dalam pembahasan karya ilmiah ini, yaitu bagaimana pengamanan user didalam aplikasi database.

Didalam sebuah aplikasi database terdapat user yang diberi wewenang untuk mengolah data-data dan obyek-obyek didalam database tersebut. User atau orang tersebut dapat berwujud orang/ personal atau dapat juga berwujud bagian/ divisi didalam sebuah organisasi, dan bahkan dapat berupa sebuah aplikasi komputer yang mengakses baik secara langsung maupun tidak langsung data-data atau obyek-obyek didalam database tersebut. User ini biasa juga disebut user account. Pengaturan user

 ISSN: 1411-3201

account untuk masing-masing aplikasi database tentu saja ada perbedaan tetapi kalau dilihat lagi secara detail ternyata perbedaan tersebut hanya sedikit saja sepanjang vendor yang membuat aplikasi database tersebut mengadopsi teori-teori dasar didalam basis data. Secara umum user account pasti memiliki: username yang unik, metode autentikasi, tablespace default, tablespace sementara/ temporary, user profile, pembatasan penggunaan sumber daya didalam komputer (consumer group), status usernya. Semua parameter didalam user account tersebut dikelola dan dibuat oleh user level tertinggi atau biasa disebut Database Administrator (DBA).

Pengelolaan keamanan user didalam basis data dapat diwujudkan melalui beberapa cara/ teknik. Masing-masing vendor biasanya menyediakan banyak alternatif tool yang dapat digunakan untuk membantu pekerjaan seorang DBA dalam mengelola user dan hak akses didalamnya. Tool yang paling dasar adalah dengan menggunakan SQL editor yang didalamnya dapat diketikkan perintah-perintah SQL (structured query language) dasar untuk mengelola user dan hak aksesnya. Perintah SQL tersebut adalah GRANT dan REVOKE yang termasuk dalam kategori SQL DCL (data control language). Selain itu vendor juga menyediakan tool pendukung berbasis GUI (graphical user interface) untuk pengelolaan user dan hak akses user. Berikut adalah contohnya:

Software DBMS	Tool SQL Editor	Tool berbasis GUI
MySQL	MySQL Command Prompt	PHPMyadmin MySQL-Front MySQL Query Browser
Oracle 10g	SQL Plus iSQL Plus	Enterprise Manager
SQL Server 2000	SQL Query Analyzer	Enterprise Manager

Username

Adalah nama user yang didaftarkan pada sebuah database yang sifatnya unik. Maksudnya tidak boleh ada username yang sama didalam satu database. Pada beberapa aplikasi database terdapat beberapa aturan main yang harus disepakati dalam pendaftaran username didalam database tersebut. Seperti lebar karakter maksimal untuk sebuah username ada yang maksimal 8 karakter dan ada juga yang sampai lebar karakternya 256 karakter. Penamaan username harus mengikuti kaidah tertentu seperti harus dimulai dengan huruf lalu kemudian boleh digabung dengan angka atau karakter khusus. Username merupakan salah satu langkah awal mekanisme pengamanan didalam aplikasi database dan disemua vendor yang membuat aplikasi database pasti memiliki fitur ini. Jika seorang user yang mencoba untuk login kedalam database tetapi user tersebut belum pernah didaftarkan didalam database, maka user tersebut tidak dapat login/ masuk kedalam aplikasi database tersebut. Username hanya dapat dibuat dan dikelola oleh user level tertinggi yaitu DBA.

Metode Autentikasi

Fitur ini juga terdapat di semua aplikasi database yang ada saat ini. Autentikasi adalah sebuah proses untuk melakukan verifikasi apakah user yang mencoba login kedalam database adalah user yang sah dan diberi ijin atau tidak. Salah satu metode autentifikasi yang paling dasar adalah password. Password biasanya digunakan bersama-sama dengan username untuk mengecek apakah user yang mencoba login pada saat itu adalah benar-benar user yang sah atau tidak. Beberapa vendor yang membuat aplikasi database menawarkan penggunaan enkripsi untuk mengamankan user password agar tidak mudah di jebol oleh pihak-pihak yang tidak bertanggung jawab.

Algoritma enkripsi yang digunakan biasanya bersifat satu arah (one-way hash) maksudnya setelah di enkripsi maka user password tersebut tidak dapat di dekripsi jika user passwordnya dilupakan dan hanya dapat di reset ulang user passwordnya. Algoritma enkripsi yang digunakan untuk masing-masing aplikasi database biasanya berbeda-beda tergantung kebijakan yang digunakan oleh masing-masing vendor yang membuat aplikasi database tersebut. Sebagai contoh, Oracle menggunakan algoritma enkripsi Data Encryption Standard (DES) untuk enkripsi pada user passwordnya untuk produk Oracle 10g dan Oracle 11g, Micorsoft menggunakan algoritma Advanced Encryption Standard (AES) untuk enkripsi pada user password mereka di hampir semua produknya seperti Microsoft Windows dan Microsoft SQL Server, MySQL menggunakan algoritma enkripsi Message Digest (MD5) untuk enkripsi user passwordnya.

Pada beberapa aplikasi database bahkan di tawarkan penggunaan metode autentikasi yang lebih aman lagi, seperti penggunaan metode autentikasi menggunakan token atau biometrik/

 ISSN: 1411-3201

DNA. Misalnya pada database Oracle 10g terdapat 3 (tiga) pilihan metode autentikasi yang dapat diterapkan pada user, yaitu password, external, global. Metode autentikasi external misalnya jika seorang user akan login ke database maka user tersebut tidak perlu memasukkan username dan password databasenya tapi database akan mengecek apakah user tersebut user yang sah atau tidak hanya berdasarkan username dan password yang di isikan ketika pertama kali login di sistem operasi (host credential).

Hak Akses/ Privileges

Ketika seorang user berhasil dibuat didalam sebuah database, biasanya user tersebut belum diberikan hak akses terlebih dahulu. Hak yang pertama kali diberikan pada seorang user ketika pertama kali dibuat adalah hak akses untuk login/ koneksi ke database. Dengan hak akses ini seorang user dapat melakukan login terlebih dahulu ke database walaupun user tersebut belum dapat melakukan pekerjaan lainnya sampai hak akses yang lain diberikan kepada user tersebut. Secara umum didalam database terdapat dua jenis hak akses, yaitu hak akses terhadap pengelolaan sistem datbase (system privileges) dan hak akses terhadap obyek database (object privileges). Perintah dasar SQL (structured query language) untuk pengelolaan hak akses adalah GRANT dan REVOKE. GRANT dan REVOKE termasuk dalam kategori bahasa SQL DCL (data control language). GRANT merupakan perintah yang digunakan untuk memberikan hak akses kepada user, sedangkan REVOKE adalah perintah yang digunakan untuk mengambil/ menhapus hak akses yang pernah diberikan kepada user tersebut sebelumnya. Pemberian hak akses (granting) ataupun penghapusan hak akses (revoking) terhadap seorang user tentunya sangat tergantung pada kebutuhan organisasi agar pemberian hak akses kepada seorang user tepat sasaran. Seorang DBA (database administrator) yang bertindak sebagai user tertinggi didalam database harus mengadopsi konsep minimum least privileges dalam mengatur hak akses user-user didalam databasenya. Minimum least privileges maksudnya adalah ketika seorang user dibuat didalam database maka secara default user tersebut belum diberikan hak akses dan hak aksesnya diberikan satu persatu oleh DBA sesuai dengan permintaan oleh user tersebut atau berdasarkan kebijakan yang telah diatur didalam organisasi.

System Privileges

Merupakan salah satu jenis hak akses yang dapat diberikan pada user didalam sebuah basis data. Hak akses ini membolehkan user untuk dapat melakukan aktivitas-aktivitas tertentu didalam sebuah basis data yang berkaitan dengan pengelolaan database secara keseluruhan.pemberian hak akses ini dapat dilakukan oleh seorang DBA/ Admin atau user lain yang memang memiliki hak akses untuk pemberian hak akses ini.

Pada semua jenis aplikasi pengolah basis data pasti memiliki jenis hak akses ini. Biasanya jenis hak akses user yang masuk kategori ini terdapat klausa "ANY" didalamnya. Contoh: CREATE ANY TABLE, ALTER ANY TABLE, DROP ANY TABLE. Maksud dari klausa "ANY" adalah hak akses tersebut dapat diterapkan pada seorang user yang dapat mengakses semua schema yang terdapat didalam basis data tersebut. Misal jika seorang user ingin diberikan hak akses agar dapat menghapus obyek tabel di semua schema walaupun bukan milik user tersebut maka hak akses yang dapat diberikan pada user tersebut adalah "DROP ANY TABLE".

Selain dari penambahan klausa "ANY" yang menyatakan bahwa hak akses tersebut dapat lintas schema, banyak juga hak akses yang termasuk kategori ini yang tidak terdapat klausa "ANY" didalamnya. Misal: CREATE SESSION (untuk dapat login/ koneksi ke basis data sesuai dengan autentikasinya), CREATE TABLE (membuat tabel di schema user tersebut), CREATE INDEX (membuat obyek index di schema user tersebut), DROP INDEX (menghapus obyek index).

Jika seorang user diberi hak akses sistem maka user tersebut dapat melakukan kegiatan pengelolaan database sesuai dengan hak akses tersebut. Jika seorang DBA ingin memberikan hak akses sistem kepada seorang user dimana user tersebut dapat juga memberikan hak akses sistemnya tersebut kepada user lainnya, maka user tersebut ketika diberikan hak akses ditambahkan klausa WITH ADMIN OPTION. WITH ADMIN OPTION adalah atribut tambahan yang harus diberikan pada hak akses sistem jika hak akses sistem tersebut akan diberikan pada user lain oleh user yang bersangkutan.

Object Privileges

Hak akses obyek adalah hak akses yang diberikan kepada seorang user agar user tersebut dapat mengelola obyek-obyek didalam database.

 ISSN: 1411-3201

Obyek-obyek didalam database jenisnya adalah obyek tabel, obyek view, obyek sequence, obyek stored procedure, obyek function, obyek package.

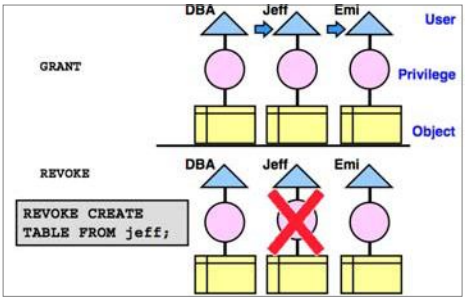
Seorang user secara default hanya dapat mengelola obyek-obyek database yang dibuat/ dimiliki oleh user tersebut saja. Agar user lain dapat mengelola obyek-obyek yang dibuat oleh user tersebut maka user yang lain tersebut harus diberikan hak akses obyek yang tepat untuk user tersebut. Berikut adalah contoh hak akses obyek: INSERT, UPDATE, DELETE, SELECT. Hak akses insert diberikan kepada user agar user dapat mengisikan data kedalam tabel. Hak akses UPDATE diberikan kepada user agar user dapat melakukan perubahan data pada sebuah tabel. Hak akses DELETE diberikan kepada user agar user dapat melakukan penghapusan data didalam tabel. Hak akses SELECT diberikan kepada user agar user dapat menampilkan data-data (retrieving data) dari sebuah tabel.

Setiap user dapat mengelola obyek-obyek database yang dibuat oleh user tersebut saja. Agar seorang user dapat memberikan hak akses obyeknya kepada user lain maka user tersebut harus memiliki hak akses khusus. Pemberian hak akses tersebut hanya dapat diberikan oleh seorang DBA kepada seorang user atau dapat juga diberikan oleh seorang user yang memiliki hak akses DBA sehingga user tersebut walaupun bukan seorang admin tapi karena memiliki hak akses untuk memberikan hak akses kepada user maka dapat melakukan hal tersebut. Seorang user dapat memberikan hak akses obyeknya kepada user lain jika memiliki hak akses obyek dengan tambahan klausa WITH GRANT OPTION. Jika seorang user memiliki hak akses tambahan ini maka user tersebut dapat memberikan hak akses obyeknya yang sebelumnya di berikan oleh DBA kepadanya kepada user lain. Misalkan seorang user A diberikan hak akses agar dapat melihat isi tabel karyawan (SELECT karyawan) dengan tambahan WITH GRANT OPTION, maka user A selain dapat melihat isi data di tabel karyawan juga dapat memberikan hak akses SELECT karyawan kepada user lain misalkan user B. Berikut adalah contoh perintah pemberian hak akses tersebut kepada user A: GRANT SELECT ON A.karyawan TO A WITH GRANT OPTION. GRANT adalah perintah dasar SQL untuk memberikan hak akses, SELECT adalah jenis hak akses obyeknya, A.karyawan adalah tabel karyawan pada schema A, WITH GRANT OPTION artinya user A dapat memberikan hak akses tersebut kepada user lainnya.

Penghapusan Hak Akses (REVOKING PRIVILEGES)

Perintah revoke adalah perintah untuk menghapus hak akses seorang user jika sudah tidak digunakan lagi. Dalam menghapus hak akses user antara hak akses sistem (system privileges) dan hak akses obyek terdapat perbedaan. Pada penghapusan hak akses sistem tidak berlaku aturan cascading sedangkan pada penghapusan hak akses obyek berlaku aturan cascading. User yang memiliki hak akses untuk melakukan penghapusan hak akses adalah user yang levelnya DBA (database administrator) atau user lain yang memiliki hak akses khusus untuk menghapus hak akses.

Penghapusan Hak Akses Sistem



Gambar 1 Ilustrasi GRANT dan REVOKE hak akses sistem (system privileges) pada user dengan tambahan klausa WITH ADMIN OPTION

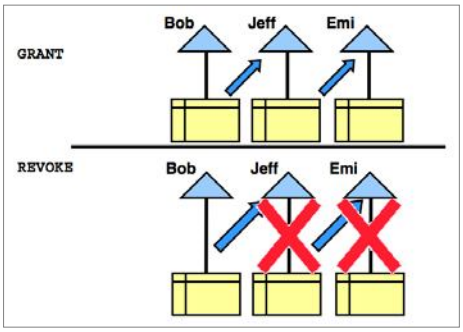
(sumber: materi Oracle Workshop 1, OCA WDP 1Z0-042)

Pada gambar 1 diatas, di ilustrasikan misalkan seorang DBA memberikan hak akses sistem (CREATE TABLE) pada user Jeff dengan tambahan WITH ADMIN OPTION. Karena user Jeff memiliki hak akses WITH ADMIN OPTION, maka Jeff memberikan hak aksesnya (CREATE TABLE) kepada user Emi sehingga Emi dapat juga membuat tabel karena mendapatkan hak akses tersebut dari user Jeff. Pada suatu waktu DBA menghapus hak akses CREATE TABLE yang sebelumnya diberikan pada user Jeff. Pada kondisi ini, user Jeff akan kehilangan hak akses CREATE TABLE tetapi hak akses CREATE TABLE yang dimiliki oleh user Emi tetap dapat digunakan oleh user Emi walaupun user Jeff sebagai pihak yang memberikan user tersebut telah hilang hak akses CREATE TABLE-nya. Inilah yang dimaksud

 ISSN: 1411-3201

tidak berlaku aturan cascading pada penghapusan hak akses sistem.

Penghapusan Hak Akses Obyek



Gambar 2 Ilustrasi GRANT dan REVOKE hak akses obyek (object privileges) pada user dengan tambahan klausa WITH GRANT OPTION

(sumber: materi Oracle Workshop 1, OCA WDP 1Z0-042)

Pada gambar 2 diatas, di ilustrasikan seorang user Bob memberikan hak akses INSERT karyawan kepada user Jeff, sehingga user Jeff dapat melakukan pengisian (insert) data ke tabel karyawan. Pada saat memberikan hak akses tersebut user Bob juga menyertakan tambahan klausa WITH GRANT OPTION pada hak akses INSERT untuk user Jeff sehingga dengan tambahan klausa WITH GRANT OPTION user Jeff selain dapat mengisikan data ke tabel karyawan juga dapat memberikan hak akses INSERT karyawan kepada user lain. Pada kasus diatas, user Jeff memberikan juga hak akses INSERT karyawan pada user Emi sehingga user Emi dapat juga melakukan pengisian data ke tabel karyawan. Pada suatu saat user Bob mengambil lagi hak akses INSERT karyawan yang sebelumnya pernah diberikan kepada user Jeff. Ketika hal itu dilakukan maka pada saat itu hak akses INSERT karyawan yang dimiliki oleh user Jeff menjadi hilang/ tidak berlaku lagi dan pada saat itu juga semua user yang pernah diberikan hak akses INSERT karyawan oleh user Jeff juga serta merta ikut terhapus juga. Pada kasus diatas user Emi juga ikut tidak berlaku lagi hak akses INSERT karyawan-nya ketika user Jeff dihapus hak aksesnya. Inilah yang dimaksud konsep cascading berlaku ketika penghapusan hak akses (revoking) diterapkan pada hak akses obyek.

Roles

Roles merupakan sekumpulan hak akses yang dapat diterapkan pada user dengan hak akses yang sama levelnya. Dengan menggunakan roles maka pengaturan terhadap hak akses didalam database menjadi lebih mudah. Semua software DBMS yang ada saat ini menyediakan fasilitas/ fitur untuk pembuatan roles didalamnya. Berikut adalah keuntungan penggunaan roles didalam konteks mengelola hak akses user didalam database:

1. Roles dapat memudahkan pengelolaan terhadap hak akses yang terdapat didalam database untuk beberapa user yang sejenis dan satu level hak aksesnya baik itu hak akses sistem maupun hak akses obyek.
2. Roles dapat membantu DBA dalam mengatur hak akses semua user didalam database secara dinamis. Maksudnya jika ingin melakukan penambahan atau pengurangan hak akses user yang sudah di masukkan kedalam roles maka perubahan tersebut tidak perlu dilakukan terhadap masing-masing user yang tergabung didalam roles tersebut tetapi cukup perubahan dilakukan disisi roles maka otomatis semua user yang berasosiasi dengan roles tersebut akan mengalami perubahan hak akses juga.
3. Roles dapat di aktifkan dan di non aktifkan sementara waktu sehingga dengan konsep ini pengaturan hak akses untuk masing-masing user dapat dilakukan secara selektif. Pada beberapa software DBMS roles dapat diamankan dengan menerapkan metode autentikasi didalamnya seperti penggunaan password sehingga hanya user yang diberi hak saja yang dapat melakukan perubahan terhadap hak akses yang terdapat didalam roles tersebut.

Profiles

Untuk membatasi penggunaan sumber daya (resources) didalam sistem database oleh masing-masing user maka database menawarkan konsep profiles. Profiles merupakan sebuah pengaturan yang tersimpan didalam database yang didalamnya berisikan pengaturan/ pembatasan mengenai penggunaan resources didalam sistem database oleh user dan juga pengaturan terhadap password user seperti panjang karakter password, masa kadaluarsa password, kompleksitas password, dan lain-lain. Pembatasan ini perlu dilakukan agar masing-masing user tidak menggunakan resources didalam sistem database diluar batas kewajaran. Dengan adanya pembatasan ini, maka masing-

 ISSN: 1411-3201

masing user hanya menggunakan resources didalam sistem database sesuai dengan pengaturan profiles yang memang telah di tentukan untuk user tersebut. Pembatasan didalam profiles meliputi penggunaan prosesor (CPU usage), penggunaan memory (memory usage), penggunaan jaringan (network usage), penggunaan harddisk (disk I/O).

Fitur keamanan tambahan

Selain beberapa aspek yang dibahas diatas, beberapa software database memiliki tambahan fitur keamanan yang ditambahkan oleh vendor pembuatnya sebagai salah satu nilai tambah/ keunggulan terhadap software database yang lain. Fitur penting yang berkaitan dengan keamanan user adalah fitur tambahan yang berkaitan dengan fitur keamanan pada password. Berikut adalah beberapa fitur tersebut:

1. Account locking, dengan adanya fitur ini maka user account dapat secara otomatis diblokir selama waktu tertentu jika user gagal mengautentikasi passwordnya untuk sekian kali percobaan (failed login attempts). Misalkan seorang user gagal memasukkan password yang benar selama 3 (tiga) kali berturut-turut maka user tersebut secara otomatis akan diblokir oleh database selama 24 jam atau sampai DBA membuka blokir user account tersebut di control panel DBA tersebut. Berapa kali kesempatan kegagalan melakukan login dapat di atur pada software databasenya. Kasus ini sering kali diterapkan di bank pada mesin ATM (automatic teller machine), yaitu jika seorang nasabah 3 kali gagal memasukkan nomor PIN (personal identification number) maka kartu ATM-nya langsung di blokir oleh mesin ATM dan di blokir oleh sistem database bank tersebut selama 24 jam atau selama petugas bank yang memiliki hak akses membuka blokir untuk nasabah tersebut. Pengaturan berapa lama user account tersebut di blokir dan kemudian aktif kembali setelah di blokir karena kesalahan melakukan login juga dapat di atur melalui software databasenya baik secara manual oleh DBA atau secara otomatis oleh databasenya (password lock time).
2. Password aging and expiration, fitur ini mengatur masa berlaku password yang dimiliki user dan setelah itu dianggap kadaluwarsa (expired) oleh database kecuali user tersebut mengganti passwordnya sebelum masa kadaluwarsa berakhir. Biasanya satuan waktunya adalah hari dan beberapa software database mengatur defaultnya adalah selama 30 hari. Setelah 30 hari maka user tersebut tidak dapat login ke database karena passwordnya sudah kadaluwarsa. Konsep ini dikenal juga dengan istilah password life time. Dengan penerapan fitur ini maka serangan terhadap sistem database yang dilakukan oleh seorang yang tidak berhak dapat di minimalisir. Jenis serangan yang sering dilakukan adalah dengan menggunakan teknik "password cracking program" yaitu menggunakan program aplikasi yang dapat melakukan penjebolan suatu password dengan menggunakan algoritma tertentu. Serangan seperti ini biasanya sukses dilakukan selama periode tertentu. Jika sebuah database menggunakan fitur password aging and expiration, maka seorang user yang mencoba menjebol password seorang user yang sah dengan menggunakan program yang dapat memecahkan password (password cracking program) akan mengalami kesulitan. Misalkan sebuah database menerapkan fitur pengamanan untuk kadaluwarsa password usernya 15 hari sekali dan pada saat itu juga ada seorang user yang mencoba menjebol password user didalam database tersebut dengan menggunakan teknik password cracking program dimana teknik ini akan berhasil menjebol password butuh waktu 20 hari maka sebelum user tersebut berhasil menjebol password user yang sah maka pada hari ke-15 user didalam sistem database tersebut sudah melakukan penggantian password berikutnya. Demikian seterusnya.
3. Password history, fitur ini biasanya terdapat di beberapa software database server untuk mengecek apakah password yang digunakan oleh user tersebut sebelumnya belum pernah digunakan oleh user tersebut. Tujuannya adalah agar user ketika mengganti password tidak boleh mengganti passwordnya dengan password yang sebelumnya pernah dibuat didalam database yang sama. Sehingga dengan cara ini tidak ada peluang bagi user untuk menggunakan passwordnya secara berulang-ulang. Daftar password yang pernah digunakan didalam sistem database tersebut akan di simpan dalam sebuah file didalam database dan kemudian isi file ini yang akan dibandingkan oleh database ketika ada user yang mencoba untuk membuat password baru. Jika password tersebut sudah terdapat didalam file password tersebut, maka user tersebut tidak di ijinkan untuk menggunakan

 ISSN: 1411-3201

kembali password tersebut dan harus menggantinya dengan password yang benar-benar baru.

4. Password complexity verification, fitur ini juga terdapat di hampir semua software database server yang ada saat ini. Fungsinya adalah untuk mengecek apakah password yang dibuat oleh seorang user memenuhi kriteria password yang aman atau tidak. Hal ini dapat dilihat dari sisi kompleksitas password tersebut. Parameter yang di cek misalnya apakah panjang karakter sudah memenuhi minimal 8 karakter, apakah password berisikan kombinasi huruf besar, huruf kecil, angka, dan karakter khusus (simbol). Pada beberapa software database jika kriteria ini tidak terpenuhi maka sistem databasenya akan menolak pembuatan password tersebut, sementara pada software database lainnya tetap di ijinkan tetapi database tersebut akan menampilkan pesan peringatan bahwa password yang dibuat tidak memenuhi kriteria standar keamanan password didalam sistem database tersebut.

KESIMPULAN

Keamanan user merupakan salah satu bagian yang penting dalam sebuah sistem. Selama ini fokus pengamanan biasanya pada sisi jaringan komputer dan pada sisi program aplikasi client, sedangkan pengamanan user dari sisi software database tidak begitu menjadi perhatian. Padahal jika berbicara sebuah sistem informasi yang terintegrasi, maka keamanan sistem harus melihat sebuah aspek dari komponen-komponen yang terlibat didalam sistem informasi tersebut. Saat ini semua vendor pembuat software pengolah database, menawarkan mekanisme pengamanan yang cukup lengkap dan terintegrasi terhadap data dan user didalam sistem database tersebut. Tentunya semakin lengkap sistem pengamanan di sisi database maka akan semakin besar juga biaya investasi yang dikeluarkan oleh sebuah organisasi/ perusahaan dalam merencanakan pembelian software database yang sesuai dengan kebutuhan dan standar keamanan data/ user perusahaan tersebut. Untuk itu diperlukan pemahaman yang cukup komprehensif bagi seorang DBA dalam memilih software database apa yang akan di aplikasikan serta sistem pengamanan seperti apa yang perlu di aplikasikan yang sesuai dengan kebutuhan organisasi tersebut. Bagi perusahaan yang sangat mengutamakan data seperti di perbankan maka penerapan sistem keamanan di dalam databasenya tentu berbeda dengan perusahaan yang tidak memprioritaskan keamanan data didalam sistem databasenya. Untuk itu diperlukan kerjasama yang baik antara DBA dan pihak manajemen perusahaan untuk mewujudkan hal tersebut agar pemilihan software database dan penerapan standarisasi keamanan database betul-betul tepat dan sesuai dengan kebutuhan perusahaan.

DAFTAR PUSTAKA

Database System Concepts, Silberschatz. A, McGraw Hill, 2006

Pemrograman Basis Data menggunakan Transact-SQL dengan Microsoft SQL Server 2000, Arief Rudyanto. M, Penerbit Andi, 2005

Oracle Workshop 1, oracle Corp, oracle Corp, 2005

CompTIA Security+, Part 1 – security concepts., www.comptia.net