PERTEMUAN 8
DATABASE SECURITY

A. TUJUAN PEMBELAJARAN

Pada pertemuan ini akan dijelaskan mengenai keamanan dalam basis data. Setelah mempelajari materi ini mahasiswa diharapkan mampu untuk:

1. Mendefinisikan *database security*.
2. Memahami resiko pada *database security.*
3. Meningkatkan keamanan *database security*
4. Memahami *Data Base Management System* (DBMS)

B. URAIAN MATERI

1. Mendefinisikan Database Security

Database atau basis data adalah kumpulan data yang disimpan di komputer menggunakan aplikasi yang disebut sistem manajemen database. Data Base Management System (DBMS) adalah aplikasi yang memungkinkan orang lain mencari data yang disimpan untuk menemukan informasi tertentu. Tujuan dari DBMS adalah untuk memberikan pengguna sarana untuk memanipulasi, menganalisis, menyimpan, dan mengambil informasi.

Keamanan database adalah seperangkat prosedur, standar, kebijakan, dan alat yang digunakan untuk melindungi data dari pencurian, penyalahgunaan, dan gangguan, aktivitas, dan serangan yang tidak diinginkan. Keamanan database berkaitan dengan izin dan akses ke struktur data dan data yang terkandung di dalamnya. Alat yang digunakan untuk mengamankan database biasanya disertakan dan dikonfigurasi di dalam paket perangkat lunak database yang diinstal, tetapi kemampuan paket ini berbeda-beda menurut vendor (misalnya, Oracle, MySQL, Microsoft SQL Server).

Database security adalah mekanisme untuk melindungi database terhadap ancaman baik yang di sengaja maupun yang tidak di sengaja. Database security meliputi : Hardware, Software, Jaringan Internet, Database Server, dan Individual Person (user, proggrammer, administrator, operator dan outsider).

Risiko keamanan untuk sistem basis data meliputi, yaitu:

a. Aktivitas yang tidak sah atau tidak diinginkan atau penyalahgunaan oleh pengguna database resmi, administrator database, atau manajer jaringan / sistem, oleh pengguna atau peretas yang tidak sah (misalnya akses yang tidak tepat ke data sensitif, metadata atau fungsi dalam database, atau perubahan yang tidak pantas pada program database, struktur atau konfigurasi keamanan).
b. Infeksi malware yang menyebabkan terjadinya seperti akses tidak sah, kebocoran atau pengungkapan data pribadi atau hak milik, penghapusan atau kerusakan pada data atau program, gangguan atau penolakan akses resmi ke database, serangan pada sistem lain, dan kegagalan layanan database yang tidak terduga
c. Beban yang berlebih, kendala dalam kinerja, dan adanya masalah kapasitas yang mengakibatkan ketidakmampuan pengguna yang berwenang untuk menggunakan database sebagaimana dimaksud
d. Kerusakan fisik yang terjadi pada server database yang disebabkan oleh kebakaran atau banjir di ruang komputer, panas berlebih, petir, tumpahan cairan yang tidak disengaja, pelepasan muatan listrik statis, kerusakan elektronik / kegagalan peralatan, dan keusangan.
e. Cacat desain dan bug yang terjadi dalam pemrograman dalam database dan program serta sistem terkait, menciptakan berbagai kerentanan keamanan (misalnya eskalasi hak istimewa yang tidak sah), kehilangan dan kerusakan data, penurunan kinerja, dll.
f. Kerusakan dan kehilangan data yang disebabkan oleh masuknya data atau perintah yang tidak valid, kesalahan dalam proses database atau administrasi sistem, sabotase / kerusakan kriminal, dll.

2. Memahami Resiko pada Database Security

Keamanan database adalah suatu cara untuk melindungi database dari ancaman, baik dalam bentuk kesengajaan atau pun bukan. Ancaman adalah segala situasi atau kejadian baik secara sengaja maupun tidak yang bersifat merugikan dan memengaruhi sistem. Keamanan database tidak hanya berkenaan dengan data yang ada pada database saja, tetapi juga meliputi bagian lain dari sistem database, yang tentunya dapat memengaruhi database tersebut. Hal ini berarti keamanan database mencakup perangkat keras, perangkat lunak, dan data.

Agar memiliki suatu keamanan yang efektif dibutuhkan kontrol yang tepat. Seseorang yang mempunyai hak untuk mengontrol dan mengatur database biasanya disebut Administrator database. Seorang administratorlah yang memegang peranan penting pada suatu sistem database, oleh karena itu administrator harus mempunyai kemampuan dan pengetahuan yang cukup agar dapat mengatur suatu sistem database.

a. Tujuan Keamanan Database
   1) Secrecy/Confidentiality: Informasi tidak boleh diungkapkan kepada pengguna yang tidak sah. Sebagai contoh, Siswa seharusnya tidak diperbolehkan untuk memeriksa nilai siswa lainnya.·
   2) Integrity: Hanya pengguna berwenang yang diizinkan untuk memodifikasi data. Sebagai contoh, guru mata pelajaran lain mungkin diperbolehkan untuk melihat nilai, namun tidak diperbolehkan (jelas) untuk memodifikasi mereka.·
   3) Availability: Pengguna yang terdaftar tidak boleh ditolak akses. Sebagai contoh, seorang instruktur yang ingin mengubah kelas harus diizinkan untuk melakukannya encryptech-database-security
b. Ancaman Pada Database

   Ancaman terhadap database meliputi theft (pencurian) dan fraud (penipuan). Jika kedua ancaman tersebut terjadi pada sebuah perusahaan, maka perusahaan akan mengalami :

   1) Loss Of Confidentiality (Kehilangan kerahasiaan). Hilangnya kerahasiaan perusahaan akan menyebabkan hilangnya daya saing
   2) Loss of Privacy (Kehilangan Privacy), dapat menyebabkan tindakan illegal untuk melawan organisasi.
   3) Loss of Integrity (Kehilangan Integritas), menyebabkan data menjadi invalid atau rusak di dipertanyakan kejelasan sebuah data yang di kelola organisasi.
   4) Loss of Availibility (Kehilangan Ketersediaan), artinya data atau sistem tidak dapat diakses sehingga mempengaruhi kinerja finansial perusahaan.

Dengan adanya keamanan pada sebuah database, ancaman ancaman yang disebutkan bisa di minimalisir dan di antisipasi. Berikut ini tabel rincian kerugian yang di dapat jika terdapat ancaman pada database :

Tabel 8. Rincian Kerugian Database Security

Threat	Theft and Fraud	Loss of Confidentiality	Loss of Privacy	Loss of Integrity	Loss of Availibility
Using another persons access	✓	✓	✓		
Unauthorized amendment or copying of data	✓			✓	
Program Alteration	✓			✓	✓
Inadequate policies and procedures thet allow of mix of confidential and normal output	✓	✓	✓		
Wire Tapping	✓	✓	✓		
Illegal entry by hacker	✓	✓	✓		
Blackmail	✓	✓	✓		
Creating 'trapdoor' into system	✓	✓	✓		
Theft of data, programs, and equipment	✓	✓	✓		✓
Failure of security mechanism, giving greater access than normal		✓	✓	✓	
Staff shortages or strikes				✓	✓
Inadequite staff training		✓	✓	✓	✓
Viewing and disclosing unathorized data	✓	✓	✓		
Electronic interference and radiaton				✓	✓
Data Corruption owing to power loss or surge				✓	✓
Fire (Electrical fault, lightning strike, arson) flood, bomb				✓	✓
Physical damage to equipment				✓	✓
Breaking cables or disconnection of cables				✓	✓
Introduction of viruses				✓	✓

3. Meningkatkan Keamanan Pada Database Security

Secara garis besar keamanan database dikategorikan sebagai berikut:

a. Keamanan Server

Perlindungan Server adalah suatu proses pembatasan akses yang sebenarnya pada database dalam server itu sendiri. Menurut Blake Wiedman ini adalah suatu sisi keamanan yang sangat penting dan harus direncanakan secara hati-hati. Ide dasarnya adalah kita tidak dapat mengakses apa yang kita tidak dapat lihat. Database bukanlah suatu web server, koneksi yang tidak dikenali tidak akan diijinkan.

b. Trusted IP Access

Setiap server harus dapat mengkonfigurasikan alamat IP yang diperbolehkan mengakses dirinya. Anda tidak boleh mengijinkan semua orang

untuk mengakses server. Jika server melayani suatu web server maka hanya alamat web server itu saja yang dapat mengakses server database tersebut. Jika server database melayani jaringan internal maka hanya alamat jaringanlah yang boleh menghubungi server. Sangat perlu diperhatikan bahwa jangan pernah menggabungkan server database web dengan server database informasi internal perusahaan Anda, ini adalah suatu mental yang buruk untuk seorang admin. Trusted IP Access merupakan server database terbatas yang hanya akan memberi respon pada IP yang dikenali saja

c. Koneksi Database

Saat ini semakin banyaknya aplikasi dinamis menjadi sangat menggoda untuk melakukan akses yang cepat bahkan update yang langsung tanpa authentifikasi. Jangan pernah berpikir demikian, ini hanya untuk seorang pemalas. Jika Anda ingin mengijinkan pemakai dapat mengubah database melalui web page, pastikan Anda memvalidasi semua masukan untuk memastikan bahwa inputan benar, terjamin dan aman. Sebagai contoh, pastikan Anda menghilangkan semua code SQL agar tidak dapat dimasukan oleh user. Jika Anda seorang admin yang membutuhkan koneksi ODBC, pastikan koneksi yang digunakan unik.

d. Kontrol Akses Table

Kontrol akses table ini adalah salah satu bentuk keamanan database yang sering diabaikan, karena cukup sulit penerapannya. Penggunaan control akses table yang benar dibutuhkan kolaborasi antara sistem administrator dengan pengembang database. Hal inilah yang sulit dilakukan. Pemberian ijin user untuk mengakses informasi dapat membuat informasi terbuka kepada publik.

Cara Menanggulangi Ancaman pada Database Security

Terdapat 2 faktor yang harus diperhatikan untuk menanggulangi ancaman-ancaman yang disebutkan. Yaitu faktor komputer-based control dan non-komputer-based control.

a. Computer Based Control

Computer-based control merupakan control yang dilakukan terhadap akses ke dalam database menggunakan komputer (multiuser environtment).

Biasanya dalam hal ini berkaitan langsung dengan authorization dan authentication yang diantaranya :

1) Password dan Account Number
2) Discretionary Access Controll
3) Mandatory Access Control

Selain authorization dan authentication, aspek seperti interface software yang mengakses database juga harus di lindungi seperti :

1) Memberikan enkripsi pada interface user application (Jika implementasi aplikasi dan database via internet (Public).
2) Selain enkripsi teknik implementasi yang digunakan menggunakan metode jaringan intranet, sistem jaringan yang menggunakan jaringan internet namun bersifat local access.
3) Memberikan firewall terhadap device baik yang mengakses maupun DBMS device

Otorisasi adalah pemberian wewenang atau hak istimewa yang memungkinkan subjek untuk memiliki akses yang sah ke sistem atau ke objek sistem. Otorisasi (authorization). Otorisasi dan tingkatan akses yang saling keterkaitan merupakan metode pembatasan bagi user sesuai kebutuhan user tersebut. Dengan memberikan pembatasan tingkatan akses pada tiap tiap user terkait dapat meminimalisir aspek bocornya privacy information. Contoh pemberian otorisasi dan tingkatan akses :

1) Read Authorization : User di perbolehkan membaca data tapi tidak dapat memodifikasi.
2) Insert Authorization : User di perbolehkan menambah data yang baru tapi tidak dapat menghapus data yang sudah ada.
3) Update Authorization : User diperbolehkan memodifikasi data yang sudah ada tapi tidak dapat menghapus data.
4) Delete Authorization : User di perbolehkan menghapus data.
5) Index Authorization : User diperbolehkan membuat dan menghapus index data.
6) Resource Authorization : User diperbolehkan membuat relasi-relasi baru.
7) Alteration Authorization : User di perbolehkan menambah/menghapus atribute suatu relasi.

8) Drop Authorization : User diperbolehkan menghapus relasi yang sudah ada.

4. Memahami Data Base Management System

Database Management Systems (DBMS) adalah aplikasi yang menyediakan pengguna sarana untuk memanipulasi, menganalisis, dan meminta data. Hampir semua DBMS yang ada saat ini dikembangkan untuk digunakan dengan database relasional. Aplikasi ini dikenal sebagai *Relational Database Management Systems* (RDBMSs).

Ada beberapa sistem manajemen basis data relasional yang ada saat ini, yaitu :

a. Oracle, adalah RDBMS yang dikembangkan oleh Oracle Corporation pada akhir 1970-an. Memegang 52% dari pasar DBMS pada tahun 2009, itu tetap menjadi salah satu server database paling populer. Oracle terkenal portabel, kemampuannya untuk berjalan di hampir semua sistem operasi, dan peran dominannya dalam menyediakan solusi yang diandalkan bisnis untuk mencapai kompetensi inti mereka. Database Oracle menawarkan sejumlah solusi penyimpanan, dan dapat ditemukan menjaga bisnis penting data seperti sumber daya manusia, penagihan, dan catatan keuangan di seluruh dunia.

b. Mysql, adalah RDBMS yang dikembangkan oleh Sun Microsystems. Menampilkan pertumbuhan yang luar biasa setiap tahun dan terkenal dengan kecepatannya, MySQL adalah server database open-source paling populer saat ini. Istilah open source mengacu pada perangkat lunak yang telah ditulis untuk didistribusikan untuk digunakan dan diunduh secara gratis. Selain biaya, aplikasi sumber terbuka memberikan keuntungan kustomisasi.

c. Microsoft SQL, Microsoft SQL sering disebut hanya sebagai SQL Server. SQL Server adalah RDBMS yang dikembangkan oleh Microsoft untuk menyediakan platform akses data yang cepat, aman, dan dapat diskalakan. Bahasa kueri utama SQL Server adalah T-SQL dan ANSI SQL. Skalabilitas arsitektur server SQL adalah fiturnya yang paling menarik, karena ia dikembangkan untuk berjalan secara merata di berbagai lingkungan. Dari database yang berjalan di komputer pribadi yang hanya melayani satu pengguna, ke database yang disimpan di sekumpulan server yang melayani beberapa ribu pengguna, SQL Server dapat memenuhi kebutuhan lingkungan Windows apa pun.

Database Connection Manager

Manajer koneksi database melakukan apa yang tersirat dari namanya. Ia mengatur koneksi ke server MySQL. Lapisan manajemen koneksi sangat serbaguna, memungkinkan hampir semua klien untuk terhubung ke server MySQL. Aplikasi open-source yang dibangun untuk berjalan di hampir semua platform, MySQL telah menyediakan beberapa cara bagi klien untuk terhubung melalui lapisan manajemen koneksi. Pengembang dapat membuat klien dan antarmuka pemrograman aplikasi (API) di hampir semua bahasa pemrograman modern saat ini (misalnya, C, C ++, Perl, dan PHP), dan klien yang menggunakan Open Database Connectivity (ODBC), Java, dan .net disediakan dukungan melalui antarmuka MySQL.

Database Activity Monitoring (DAM)

Lapisan keamanan lain yang lebih canggih mencakup pemantauan aktivitas basis data waktu nyata, baik dengan menganalisis lalu lintas protokol (SQL) melalui jaringan, atau dengan mengamati aktivitas basis data lokal di setiap server menggunakan agen perangkat lunak, atau keduanya. Penggunaan agen atau native logging diperlukan untuk merekam aktivitas yang dijalankan di server database, yang biasanya mencakup aktivitas administrator database. Agen mengizinkan informasi ini ditangkap dengan cara yang tidak dapat dinonaktifkan oleh administrator database, yang memiliki kemampuan untuk menonaktifkan atau mengubah log audit asli.

Analisis dapat dilakukan untuk mengidentifikasi eksploitasi yang diketahui atau pelanggaran kebijakan, atau garis dasar dapat diambil seiring waktu untuk membangun pola normal yang digunakan untuk mendeteksi aktivitas anomali yang dapat menjadi indikasi intrusi. Sistem ini dapat menyediakan jejak audit database yang komprehensif selain mekanisme deteksi intrusi, dan beberapa sistem juga dapat memberikan perlindungan dengan menghentikan sesi pengguna dan / atau mengkarantina pengguna yang menunjukkan perilaku yang mencurigakan. Beberapa sistem dirancang untuk mendukung pemisahan tugas (SOD), yang merupakan persyaratan khas auditor. SOD mensyaratkan bahwa administrator database yang biasanya dipantau sebagai bagian dari DAM, tidak dapat menonaktifkan atau mengubah fungsionalitas DAM. Hal ini memerlukan jejak audit DAM untuk disimpan dengan aman di sistem terpisah yang tidak dikelola oleh grup administrasi database.

Program keamanan basis data yang baik mencakup tinjauan rutin hak istimewa yang diberikan ke akun pengguna dan akun yang digunakan oleh proses langsung. Untuk akun individu, sistem otentikasi dua faktor meningkatkan keamanan tetapi menambah kompleksitas dan biaya. Akun yang digunakan oleh proses otomatis memerlukan kontrol yang sesuai seputar penyimpanan kata sandi seperti enkripsi yang memadai dan kontrol akses untuk mengurangi risiko penyusupan.

Dalam hubungannya dengan program keamanan database yang baik, program pemulihan bencana yang sesuai dapat memastikan bahwa layanan tidak terganggu selama insiden keamanan, atau insiden apa pun yang mengakibatkan pemadaman lingkungan database utama. Contohnya adalah replikasi untuk database utama ke situs yang terletak di wilayah geografis yang berbeda.

Setelah insiden terjadi, forensik database dapat digunakan untuk menentukan ruang lingkup pelanggaran, dan untuk mengidentifikasi perubahan yang sesuai pada sistem dan proses.

C. SOAL LATIHAN/ TUGAS

1. Jelaskan definsi database security yang anda ketahui!
2. Sebutkan dan jelaskan resiko apa saya yang terdapat pada database security!
3. Sebutkan dan jelaskan system manajemen basis data!
4. Berikan kesimpulan yang anda ketahui dalam database security!
5. Adakah standart database security yang Anda ketahui?

D. REFERENSI

Basta Alfred,Ph.D.Zgola Melissa,M.A,M.S.I.S(2011). *Database Security*. Tersedia pada : http/z-lib.org/

Thuraisingham, Bhavani (2005). *Database and Applications Security Integrating Information Security and Data Management.* Tersedia pada : http/z-lib.org/

https://idwebhost.com/blog/tips-keren/panduan-lengkap-tentang-keamanan-database