KEAMANAN BASIS DATA PADA SISTEM INFORMASI DI ERA GLOBALISASI

Juwardi wafdan[1]
[1]Sistem informasi, fakultas teknik dan ilmu komputer, Universitas islam indragiri,
Email: *juwardiwafdan@gmail.com*[1]

ABSTRAK

Perkembangan teknologi teknologi informasi dan komunikasi memberikan dampak yang sangat besar pada hamper semua institusi, baik swasta maupun pemerintah . Salah satu dampak nya adalah penggunaan sistem informasi untuk membantu pekerjaan operasional dan yang paling penting adalah untuk menghasilkan informasi yang di gunakan oleh berbagai level manajemen. Implementasi database sudah lama menjadi bagian dari sistem informasi dalam menjalankan bisnis, dengan tujuan membantu orang dan organisasi menelusuri hal hal tertentu. Hal ini menunjukan bahwa database memiliki peran penting dalam organisasi sehingga sangat perlu di perhatikan dari sisi kemanannya.

Ancaman pada database dapat berdampa pada penanggulanga terhadap ancaman kemanan basis data dalam lingkunga multi user dapat di kelompokan pada 2 hal utama, yaitu control secara fisik sistem komputernya dan prosedur administrasinya. Apabila terjadi insiden terhadap sistem informasi, terutama yang berkaitan dengan kemanan basis data , maka perlu d lakukan tahap tahap penanganan meliputi : tahap persiapan (preparation) , identifikasi (containment), pemeberantasan , pemulihan,tindak lanjut.

Kata Kunci: basis data , keamanan basis data, penanggulangan ancaman keaman basis data

ABSTRACT

The development of information and communication technology has had a huge impact on inhibiting all institutions, both private and government. One of the impacts is the use of systems to assist work operations and the most important is to produce information that is used by various levels of management information. Database implementation has long been part of information systems in running a business, with the aim of helping people and organizations track certain things. This shows that databases have an important role in organizations so they really need to pay attention to their security .Threats to databases can have an impact on overcoming database security threats in a multi-user environment and can be grouped into 2 main things, namely physical control of the computer system and administrative procedures. If an incident occurs to the information system, especially those related to basic data security, it is necessary to carry out handling stages including: preparation, identification (containment), eradication, recovery, and follow-up stages.

Keywords: database, Database security, Countermeasures on database security Threats.

1 PENDAHULUAN

Saat ini , dapat di katakan hampir semua institusi swasta, pemerinth ataupun perusahaan telah menggunakan sistem informasiuntuk dapat menghasilkan informasi yang digunakan oleh berbagai level manjemen. Berbagai istilh, seperti data, data base, informasi dan sisteminformasi muncul. Aplikasi dalam organisasi, aplikasi client – server, aplikasi e-commerce, aplikasi e-bussines merupakan fungsi utama dari basis data. Tujuan basis data adalah membantu orang dan organisasi menelusurui hal hal tertentu.

Database (an khususnya SQL) telah lama menjadi bagian integral dari sistem dalam menjalankan bisnis,baik dalam bentuk awalnya, yaitu *file database* biasa maupun dalam bentuk sekarng ini, yaitu database yang berorentasi pada tingkt lanjut. Kebutuhan atas penyimpanan dan

pengaksesan informasi secara cepat menjadi hal hal yang mendesak bagi tip bisnis atau aplikasi, begitu pula *web* . aplikasi aplikasi *web* sekarang ini berpasangan dengan database. Database di pakai untuk beragam kegunaan mulai dari menyimpan nama nama *user* dan *password password* untuk akses resmi, sampai untuk menyimpan alamat alamat *e-mail user* , dan kartu kredit untuk mempermudah pengiriman produk dan pembayarannya. Oleh karena itu, pemahaman menyeluruh mengenai keamanan *web* harus mencakup juga lapisan databasenya dan terpnting memahami juga bagaimana penyusup berusaha memasuki aplikasi untuk memperoleh akses ke bagian bagian datanya.

1 METODE PENELITIAN

Penelitian penelitian ini termasuk dalam jenis penelitian study literatur berbasis pengumpulan data. Populasi dalam penelitian ini adalah kumpulan dari berbagai buku dan jurnal. Penelitian menggunakan data sekunder sebagai sumber data yang di peroleh dari berbagai buku dan jurnal yang membahas tentang keamanan basis data pada sistem informasi.

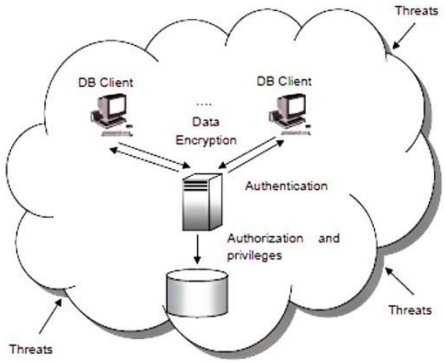
2 HASIL DAN PEMBAHASAN

a. Keamanan *Database*

Perkembangan organisasi perusahaan mempunyai dampak pada bertambahnya volume data yang harus di simpan mengenai segala aspek kegiatan operasionalny. Data data tersebut dapat di gunakan oleh organisasi untuk di jadikan dasar dalam pengambilan keputusan yang penting. Hal ini menunjukan bahwa data data tersebut penting bagi organisasi, sehingga perlu di perhatikan dari sisi keamanannya. Berdasarkan alasan ini pula, setiap personil dalam sebuah organisasi harus peka terhadap ancaman keamanan dan mengambil tindakan tindakan utnuk melindungi data pada organisasi mereka.

Masalah keamanan data sangatlah komplek. Seringkali masalah keamanan data dapat melibatkan aspek hukum, sosial atau etika, kebijakan yang berhubungan dengan pelaksana atau yang terkait dengan pengendalian peralatan secara fisik. Keamanan *database* berkaitan dengan perlindungan terhadapat *database* terhadap ancaman yang di sengaja atau tidak di sengaja, dengan menggunakan elemen kontrol peralatan komputasi atau yang tidak.

Analisis untuk kemanan *database* (basis data) tidak hanya cukup pada pelayanan yang di sediakan oleh DBMS, tetapi juga mencakup masalah masalah yang terkait dengan *database* dan keamanan lingkungannya. Pertimbangan keamanan tidak hanya berlaku untuk data yang terdapat dalam database saja, karena kesenjangan keamanan pada bagian lain dapat mempengaruhi sistem, Yang pada gilirannya dapat mempengaruhi keamanan *database*. Sehingga, dengan berpokus pada keaamanan *database* tidak akan menjamin bahwa *database* akan aman. Semua bagian dari sistem harus aman, antara lain : *database.* Jaringan, sistem operasi, bangunan di mana *database* berada secara fisik dan orang orang yang memiliki kesempatan untuk mengakses sistem.



Gambar 2. Keamanan *Database*
(Sharma, dkk :222:2010)

Ancaman terhadap database dapat mengakibatkan berkurang nya atau bahkan hilangnya tujuan dari keamanan database, yaitu menjamin : integrasi data, ketersediaan data, dan kerahasiaan data.

1) Hilangnya integritas, mengacu pada kebutuhan informasi yang di lindungi dari modifikasi yang tidak benar. Modifikasi data meliputi penciptaan, penyisipan, update, mengubah status data, dan penghapusan.

2) Kehilangan ketersediaan data mengacu pada penyediaan informasi untuk pengguna yang memiliki hak akses yang sah.

3) Kehilangan kerahasiaan. Kerahasiaan database mengacu pada perlindungan data dari pengungkapan yang tidak sah.

Menurut GCSIRT dan BPPT , penyebab adanya gangguan dari database bisa berasal dari dalam sistem komputer maupun dari manusia sebagai pengguna sistem komputer. Daro dalam sistem komputer yang di gunakan penyebabnya bisa berasal dari :

a. *Malware* yang menyerang sistem komputer.

Malware yang menyerang pada sistem dan jaringan kompute bisa menyebabkan juga terjadinya gangguan pada *server* database. Gangguan yang di timbulkan bisa berupa terganggunya akses terhadap layanan data dan bahkan bisa merusak dat dat pada komputer maupun *server* database. Hal hal berikut ini bisa menjadi ciri ciri terjadinya gangguan akses terhadap database yang di sebabkan oleh *malware* , antara lain :

1) Anti virus tidak berfungsi seperti yang di harapkan
2) kegagalan membuka utilitas sistem pada sisi *client.*
` 3) lambatnya respon CPU.
4) sistem / aplikasi *crash.*

b. Gangguan sistem jaringan komputer.

Salah satu faktor penting dari keamanan database adalah ketersediaan dari database itu sendiri. Saat ini, hampir semua data base di tempatkan pada mesin khusus yang berupa *server* database. Untuk mengakses data data dalam database , bisa di lakukan dengan menggunakan model *client server,* peranan dari jaringan komputer sangat lah penting. Ganguan keamanan pada jaringan komputer bisa mengakibat kan gangguan pada layanan

database. Pengamatan pertama yang bisa di lihat pada gangguan adalah lamanya waktu yang di btuhkan untuk mengakses *server* database, bahkan koneksi terhadap data base bisa terputus. Gangguan lainnya pada sistem jaringan adalah terdapatnya proses pemindaian dan *capture* data pada yang keluar masuk pada *server* database. Proses ini bisa terdeteksi dengan menggunakan tool IDS berbasis *host* pada *server*, maupun IDS berbasis jaringan. Identifikasi bisa di lakukan dengan melakukan pemerksaan pada log dari IDS tersebut. Disamping memasang IDS, tool lainnya yang bisa di gunakan adalah *snort,TCPdump, etercap.*

c. kerentanan aplikasi database yang di gunakan .

konfigurasi dan manajemen *patch* adalah pendekatan prinsip untuk memperbaiki kelemahan dari sistem basis data. Fitur fitur default dari aplikasi pembangun data base harus di ubah. Identifikasi dapat di lakukan dengan melhat *patch* yang pernah di lakukan dan memeriksa fitur fitur default dari sistem aplikasi database.

d. kerentetan kode / program

kerentetan kode kode (program) yang di gunakan untuk mengakses database, dapat di manfaatkan oleh penyerang untuk menembus sistem keamanan dari data base. Kode kode itu meliputi kode kode SQL maupun kode kode yang di gunakan untuk membangun aplikasi dari sistem database. Pemeriksaan terhadap kode kode itu bisa di lakukan untuk mengidentifikasi dari adanyagangguan keamanan pada database. Contoh dari serangan pada rentannya kode kode adalah SQL *injection, buffer oferlow, cross site scrifting.*

e. kelainan penggunaan database.

Apabila tidak di temukannya adanya tanda tanda bahwa penyebabnya berasal pada sistem komputer, maka identifikasi harus di arahkan kepada para pengguna sistem komputer. Be Berapa prilaku dari pengguna komputer yang bisa di membahayakan keamanan data antara lain:

1) penggunaan password yang sembarangan
2) lupa melakukan *log off* dari sistem komputer

b. Metode penaggulangan terhadap ancaman dalam keamanan basis data

menurut connolly dan begg, jenis penaggulangan terhadap ancaman keamanan database yang di gunkan pada lingkungan *multi user* dapat di fokus kanpada dua hal, yaitu kontrol secara fisik sistem komputernya dan prosedur administrasi.

Kontrol keamanan basis data berbasis komputer pada lingkungan *multi user* dapat di lakukan dengan beberapa cara, antara lain :

1. *Authorization*

Yaitu pemberian wewenang atau hak istimewa (*priviledge*) untuk mengakses sistem atau obyek data base. Kendali otorisasi dapat di bangun pada perangkat lunak dengan 2 fungsi, yaitu: mmengendalikan sistem atau obyek yang dapat di akses dan menegendalikan bagaimana pengguna menggunakannya. Dalam hal ini, seorang sistem administrasi yang bertanggung jawab untuk memberikan hak akses dengan membuat *account* pengguna.

2. *Acces controls*

Kontrol akses merupakan teknik keamanan yang di rancang untuk mengatur siapa atau jadi apa dan apa yang di lakukan pada pengguana sumber daya dalam lingkungan komputasi. Penggunaan kontrol akses yang benar membutuhkan kolaborasi antara sistem administrator dan pengembang database.

3. *views*

Merupakan metode pembatasan bagi pengguna untk mendapatkan model database yang sesuai dengan kebutuhn perorangan. Metode ini dapat menyembunyikan data todak di gunakan atau tidak perlu dilihat oleh pengguna.

4. *backup and recovery*

Backup alah peroses secara periodik untuk membuat duplikat dari data base dan melakukan *logging file* (atau program) kemediapenyimpanan external. Sedangkan *recovery* merupakan upaya untuk mengembalikan basis data ke keadaan yang di nggap benar setelah terjadinya suatu kegagalan. Terdapat 3 jenis pemulihan pada saat terjadi kegagalan, antara lain :

a) pemulihan terhadap kegagalan transaksi, yaitu kesatuan prosedur dalam program yang dapat mengubah atau memperbarui dapa pada sejumlah tabel.

b) pemulihan terhadap kegagalan media, yaitu pemulihan karena kegagalan mediadengan cara mengambil atau memuat kembali salinan basis data (*backup*).

C) pemulihan terhadap kegagaln sistem, yaitu pemulihan yang di lakukan karena adanya gangguan sistem, hang, listrik terputus aliran

5. *integrity*

Integritas juga memberikan kontribusi dalam menjaga keamanan database, guna menjaga data tetap valid, sehingga sistem informasi dapat memberikan informasi yang benar dan akurat.

6. *Encryption*

Untuk melakukan pencegahan terhadap kemungkinan ancaman dari luar (*eksternal*), maka di pandang perlu di lakukan *encode* terhadap data data yang bersifat senditif. Saat ini, beberapa DBMS telah menyediakan fasilitas untuk melakukan *encoding* (emkripsi). DBMS dapat mengakses data setelah di lakukan *decoding* terlbih dahulu terhadap data. Metode enkripsi dapat membantudalam keamanan data base, meskipun ada penurunan kinerja karena penambhan waktu yang di gunakan untuk memecahkan kode enkripsi.

7. *redundant Array of independent Disks (*RAID*) tecnology*

Perangkat keras yang bekerja pada DBMS hatus dapat berjalan dengan toleran, artinya DBMS harus terus beroperasi bahkan jika salah satu komponen *hardware* mengalami kegagalan. Kompnen *hardware* yang harus dapat berjalan dengan toleran antara lain *disk drive,* kontroler *disk,* CPU, pasokan listrik dan kipas pendingin. Diantara semua *hardware* tersebut, *disk drive* mempunyai tingkat kerentanan yang paling tinggi. Solusi untuk mengatasi hal tersebut adalah penggunaan *redundant Array of independent disks* (RAID) *tecnology* menggabungkan beberapa *hard disk* fisik ke dalam sebuah unit logis penyimpanan, dengan menggunakan perangkat lunak atau perangkat keras khusus.

C. Penanganan terhadap insiden dalam keamanan basis data

Penanganan suatu insiden di tujukan untuk mencapai hal hal ini sebagai berikut :

1) mengumpulkan informasi sebanyak mungkin tentang sifat insiden.
2) menghalangi atau mencegah eskalasi kerusakan yang di sebabkan oleh insiden tersebut, jika mungkin.
3) memperbaiki kerusakan yang di sebabkan oleh insiden tersebut.
4) mengumpulkan bukti insiden itu, yang sesuai.
5) memulihkan layanan sesegera mungkin.
6) mengambil langkah langkah proaktif untuk mengurangi insiden msa depan.

Supaya tujuan di atas dapat terlaksana dengan baik, maka perlu di tentukan tahap tahap untuk melakukan penangan terhadap insiden yang terjadi. Tahap tahap tersebut dapat di gambarkan sebagai berikut :

1) Tahap persiapan (*preparation*)

Langkah langkah yang harus di lakukan pada tahap ini aalah : penyiapan personil , dokumen kebijakan dan prosedur.

2) Tahap identifikasi

Tahap ini adalah tahap di mana penelusuran terhadap insiden yang terjadi pada data / database organisasi mulai diidentifikasi.

3) Tahap *Containment*

Tahap ini akan di lakukan pencegahan lebih lanjut terhadap kerusakan atau kebocoran lebih lanjut dari data data penting / rahasia dari organisasi.

4) tahap pemberntasan

Tahap ini merupakan tahapan unuk melakukan pemberantasan terhadap penyebab dari terjadinya insiden pada data / database.

5) tahapan pemulihan

Pemulihan merupakan tahap untuk mengembalikan seluruh sistem bekerja normal seperti semula.

6) tahapan tindak lanjut

Tahapan ini adalah fase di mana semua dokumentasi kegiatan yang di lakukan dicatat sebagai referensi untuk di maa mendatang. Fase ini dapat memberikan masukan kepada tahap persiapan untuk meningkatkan pertahanan.

3 KESIMPULAN

Basis data dalam sebuah perusahaan / organisasi mempunyai peran dan manfaat yang sangat besar sekali. Basis data dapat di gunakan sebagai dasar pada proses pengembalian keputusan yang penting. Peran dan manfaat yang sangat besar dari bisnis data juga harus di ikuti dengan keamanan terhadap basis data tersebut. Keamanan basis data harus mendapatkan perhatian khusus , karena saat basis data kehilangan integritas data, maka akan berdampak pada berkurangnya atau bahkan hilangnya tujuan dari keberadaan basis data itu sendiri.

REFERENSI

[1] Abdil kadir, 2014, *Pengenalan Sistem informasi ; Edisi revisi,*Andi offset,Yogyakarta.

[2] Connoly, Thomas & Begg, Carolyn, 2005, *Database system : A Practical Approach To Design, Implementation and Management 4th Edition,* Pearson Education, Publishing as Addison Wesle.

[3] Elmasri, Ramez; Navathe, shamkant, 2011, *fundamental of Database System 6th Edition,* pearson Education, Publishing Addison Wesley

[4] Government computer security insident response team (GCSIRT) dan BPPT & CSIRT, kemenkominfo republik indinesia.

[5] Hall, J. A, 2001, *Accounting informastion system, 3rd* Edition, south western college publishing.

[6] Hoffer, Jeffre A., Prescott, Mary B., McFadden, Fred R., 2005, *Modern database management,* new jersey: person education, inc

[7] Kroenke, David M., 2005, *dasar dasar desain, dan implementasi database processing, jilid 1,* penerbit erlangga.

[8] Laudon, Kenneth C. laundon, jane,P., 1998, *management information systems new approaches to organization & technology, new jersey :* prentice Hall, Inc.

[9] Raghu ramakrishnan, Johannes gehrke, 2010, *database management systems,second edition*_____

[10] Sharma N., perniu L., chong R., et.al 2010, *database fundamentals : ideal for application developers and administrators,* IBM Corporation , Canada.

[11] Turban, E; McLean, E;wetherbe, J., 1999, *information technology for management making connections ofr strategis advantage,2nd Edition,* John wiley & sons, Inc.

[12] Wilkinson, Joseph W., 1992, *Accounting and information system,* John Wiley & Sons, Inc.