
# Government Computer Security Incident Response Team

## BADAN PENGKAJIAN DAN PENERAPAN TEKNOLOGI

# PANDUAN PENANGANAN INSIDEN

# KEAMANAN DATABASE

*Diadopsi dari : SOP Incident Handling Database*
*Kementrian Komunikasi dan Informastika Republik Indonesia*

## BUKU PETUNJUK PELAKSANAAN

## BPPT CSIRT
## 2014

# DAFTAR ISI

# BAGIAN 1 : PENDAHULUAN

Operasional Penanganan Insiden terhadap Database adalah suatu usaha untuk melakukan langkah langkah penanganan baik preventive maupun reaktiv akan adanya berbagai hal yang menjadikan adanya kerusakan database yang dioperasikan. Hal ini mengingat data atau informasi yang ada di dalam database mempunyai value nilai yang amat berharga bagi organisasi.

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 mempengaruhi sistem

## 1.1 TUJUAN

Panduan ini dimaksudkan untuk membantu organisasi memahami tentang penanganan suatu insiden yang terjadi pada data-data yang dimiliki oleh organisasi. Penanganan insiden yang terjadi pada data-data organisasi, akan sangat bermanfaat untuk mengurangi resiko yang diakibatkannya. Resiko yang terjadi pada bocornya data-data penting / rahasia yang dimiliki oleh organisasi bisa jadi akan sangat membahayakan kelangsungan hidup organisasi tersebut, terutama apabila datatersebut jatuh kepada organisasi pesaingnya.

## 1.2 RUANG LINGKUP

Prosedur ini menetapkan suatu proses untuk penanganan insiden keamanan data/database di mana kerahasiaan, integritas atau ketersediaan telah atau mungkin dilanggar. Insiden pada keamanan data mungkin bisa disebabkan karena beberapa hal seperti, pencurian data, pembobolan data, dan pembuangan limbah dari data rahasia. Semua pelanggaran itu harus ditangani, dinilai, diselidiki dan dilaporkan sesuai dengan standar prosedur yang ada.

# BAGIAN 2 :
# PROSEDUR PENANGANAN INSIDEN TERHADAP DATABASE

Penanganan suatu insiden ditujukan utuk mencapai hal-hal sebagai berikut,

a. Mengumpulkan informasi sebanyak mungkin tentang sifat insiden;
b. Menghalangi atau mencegah eskalasi kerusakan yang disebabkan olehinsiden tersebut, jika mungkin;
c. Memperbaiki kerusakan yang disebabkan oleh insiden tersebut;
d. Mengumpulkan bukti insiden itu, yang sesuai;
e. Memulihkan layanan sesegera mungkin;
f. Mengambil langkah-langkah proaktif untuk mengurangi insiden masadepan

Supaya tujuan diatas dapat terlaksana dengan baik, maka perlu ditentukan tahap-tahap untuk melakukan penganan terhadap insiden yang terjadi. Tahap-tahaptersebut dapat digambarkan sebagai berikut,

**Tahap-tahap penanganan insiden**

## 2.1 Tahap Persiapan (Preparation)

Ini adalah tahap persiapan dimana kebijakan, prosedur, teknologi, dan sumber daya manusia harus disiapkan secara matang, dimana akan digunakan pada proses pencegahan dan penanganan terhadap insiden yang terjadi pada keamanan data / database. Dalam suatu organisasi / institusi, kemampuan melakukan respon yang cepat terhadap suatu insiden, merupakan persiapan yang mendasar bagi penanganan insiden yang terjadi pada data. Langkah-langkah yang harus diambilpada tahap ini adalah;

*Penyiapan Personil (orang)*

Meskipun memiliki kendali proses dan teknis yang kuat, keamanan dapat dikompromikan dengan memanfaatkan personil dan membuat mereka

melakukan tindakan yang sebaliknya tidak diizinkan. Tim penanganan insiden yang terampildan adanya matrik eskalasi merupakan komponen kunci dari startegi penangananyang efektif. Sebuah tim penanganan insiden yang baik adalah sumber daya sangat berharga ketika dibutuhkan untuk menangani situasi yang mungkin timbul karena adanya gangguan pada database. Sebagaimana personil adalah sumberdaya organisasi utama yang akhirnya bisa dirugikan oleh gangguan yang terjadi pada database organisasi, kesadaran akan keamanan merupakan salah satu dari isu-isu yang perlu terus menerus dipantau dan ditingkatkan untuk perlindungan yang tepat dari berbagai serangan.

1. Kesadaran Keamanan :
   Kesadaran keamanan dapat dianggap sebagai yang paling penting dari semua langkah-langkah persiapan, yang dapat membantu dalam mengidentifikasidan mencegah sebagian besar masalah yang akan timbul. Hal ini mendidik pengguna tentang cara melindungi informasi, apa yang harus dilakukan dan apa yang tidak harus dilakukan, siapa yang harus dihubungi pada keadaan darurat dan bagaimana cara menganalisis jika mendapatkan kesulitan
2. Matrik ekskalasi penanganan insiden
   Setiap organisasi harus memiliki matrik eskalasi penanganan insiden yang secara jelas mendefinisikan siapa yang harus dihubungi dalam kasus insiden. Hal ini juga menunjukkan tingkat eskalasi untuk keterlibatan lebih jauh sesuai dengan kompleksitas atau dampak dari insiden.
3. Tim Terampil Penangan Insiden
   Sebuah tim penanganan insiden yang berpengetahuan dan terampil dapatmengurangi sebagian besar dampak terhadap bisnis. Tim penanganan insiden harus dimiliki pemahaman yang sangat baik dan tingkat keterampilan dalam berbagai teknologi yang digunakan oleh perusahaan. Karena banyak perusahaan memiliki kantor-kantor cabang yang berlokasi di wilayah geografis yang berbeda, tim komando pusat dan tim lokal/regional yangsesuai sangat direkomendasikan untuk dibentuk. Tim Perintah Pusat Tentu saja, harus memandu tim lokal dalam menangani insiden .Penyiapan dokumen-

dokumen yang dibutuhkan, yaitu

*Dokumen Kebijakan dan Prosedur*

Suatu dokumen kebijakan biasanya menguraikan persyaratan tertentu atau aturan yang harus dipenuhi. Suatu dokumen prosedur adalah dokumen yang memandu pengguna secara teknis dalam proses (langkah demi langkah) tentang cara untuk mencapai persyaratan yang telah ditetapkan dan diuraikan dalam dokumen kebijakan.

## 2.2 Tahap Identifikasi

Tahap ini adalah tahap di mana penelusuran terhadap insiden yang terjadi pada data/database organisasi mulai diidentifikasi. Penyebab terjadinya insiden harus dilakukan pada tahap ini. Penyebab adanya gangguan dari database bisa berasal dari dalam sistem komputer maupun dari manusia sebagai pengguna system komputer. Dari dalam sistem komputer yang digunakan, penyebabnya bias berasal dari

a. Malware yang menyerang sistem computer

   Malware yang menyerang pada sistem dan jaringan komputer bias menyebabkan juga terjadinya gangguan pada server database. Gangguan yang ditimbulkan bisa berupa terganggunya akses terhadap layanan data dan bahkan bisa merusak data-data pada komputer maupun server data base. Hal- hal berikut bisa menjadi ciri-ciri terjadinya gangguan akses terhadap database yang disebabkan oleh malware

   1. Antivirus tidak berfungsi seperti yang diharapkan
   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 database ditempatkan pada mesin khusus yang berupa server database. Untuk mengakses data-data dalam database, bisa dilakukan dengan menggunakan model client server. Pada model client server, peranan dari jaringan komputer sangatlah penting. Gangguan keamanan pada jaringan komputer bisa

mengakibatkan gangguan pada layanan database. Pengamatan pertama yang bisa dilihat pada gangguan adalah lamanya waktu yang dibutuhkan untuk mengakses server database, bahkan koneksi terhadap database bisa terputus.

Gangguan lain 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 dilakukan dengan melakukan pemeriksaan pada log dari IDS tersebut. Disamping memasang IDS, tool lainnya yang bisa digunakan adalah snort, tcpdump, ettercap.

c. Kerentanan aplikasi database yang digunakan

Konfigurasi dan manajemen patch adalah pendekatan prinsip untuk memperbaiki kelemahan dari sistem basis data. Fitur-fitur default dari aplikasi pembangun database harus diubah. Identifikasi dapat dilakukan dengan melihat patch yang pernah dilakukan dan memeriksa fitur-fitur default dari sistem aplikasi database.

d. Kerentanan kode/program

Kerentanan kode-kode(program) yang digunakan untuk mengakses database, dapat dimanfaatkan oleh penyerang untuk menembus sistem keamanan dari database. Kode-kode itu meliputi kode-kode sql maupun kode-kode yang digunakan untuk membangun aplikasi dari sistem database. Pemeriksaan terhadap kode-kode itu bisa dilakukan untuk mengidentifikasi dari adanya gangguan keamanan pada database. Contoh dari serangan pada rentannya kode-kode adalah sql injection, buffer overflow, cross site scripting.

e. Kelalaian pengguna database

Apabila tidak ditemukannya adanya tanda-tanda bahwa penyebabnya berasal pada sistem komputer, maka identifikasi harus diarahkan kepada para pengguna sistem komputer. Beberapa perilaku dari pengguna komputer yang bisa membahayakan keamanan data,

1. Penggunaan password yang sembarangan

Kerahasiaan password yang tidak terjaga dengan baik, bias mengakibatkan password jatuh ke pihak yang tidak diinginkan. Akibatnya adalah pihak-pihak yang tidak memiliki akses ke dalam database dapat mengakses database tersebut. Dengan demikian maka pihak tersebut akan dengan mudah menguasai database.

2. Lupa melakukan log off dari sistem komputer
   Kealpaan dalam melakukan log off pada sistem komputer dapat dimanfaatkan oleh pihak lain untuk mengambil dan bahkan menghapus data-data penting yang terdapat pada sistem komputer. Identifikasi dari kasus ini bisa berupa ditolaknya akses ke dalam databse (record telah diubah atau dihapus), padahal tidak ditemukannya gejala malware, gangguan pada sistem jaringan komputer, dan kerentanan kode- kode sql dan program aplikasi database yang digunakan. Sedangkan pada kasus tercurinya database, identifikasi sulit dilakukan, karena dampak dari pencurian database tidak bisa dirasakan secara langsung. Pemilik data baru menyadari bahwa data-data telah tercuri apabila pihak pencuri telah melakukan ekspose terhadap data-data yang telah dicuri tersebut. Pada tahap identifikasi ini, disamping melakukan identifikasi untuk mengetahui penyebab terganggunya sistem database, juga dilakukan identifikasi terhadap penting atau tidaknya data/informasi yang telah mengalami gangguan. Hal itu dilakukan untuk melihat dampak yang diakibatkan oleh terganggunya data/informasi yang memiliki tingkat kerahasiaan tinggi.

## 2.3 Tahap Containment

Pada tahap ini akan dilakukan pencegahan lebih lanjut terhadap kerusakan atau kebocoran lebih lanjut dari data-data penting/rahasia dari organisasi. Apabila gangguan pada database disebabkan oleh adanya malware, maka dilakukan proses containment seperti pada prosedur penanganan insiden malware. Apabila gangguan pada

database disebabkan oleh adanya gangguan pada system jaringan, maka dilakukan proses containment seperti pada prosedur penagnanan insiden jaringan.

*Memblokir password yang digunakan untuk mengakses database*

Apabila penyebabnya berasal dari keteledoran dari para pengguna system komputer, terutama penggunaan password yang sembarangan, maka semua password-password tersebut harus diganti. Administrator sistem komputer harus memblokir semua password, dan memberikan password baru kepada para pengguna sistem.

*Melihat insiden yang pernah ada (Basis Pengetahuan).*

Langkah selanjutnya setelah mengidentifikasi gejala dasar malware adalah menelusuri dokumen untuk mencari pengetahuan yang berisi insiden yang pernah terjadi di masa lalu. Jika insiden tersebut merupakan pengulangan, maka prosedur yang diikuti sebelumnya harus dieksekusi dan dianalisis secara mendalam dari setiap langkah untuk mengidentifikasi penyebab terulangnya kejadian dan memastikan apakah Langkah-langkah tersebut cukup atau tidak. Jika belum, maka diperlukan perbaikan secara utuh pada prosedur.

*Melakukan backup semua data pada database*

Sebelum memasuki fase pemberantasan, semua data yang terdapat pada database yang ada diambil sebagai backup dan harus terus diisolasi dari backup lain yang mungkin telah terganggu keamanannya. Hal ini dilakukan untuk mengembalikan data yang hilang, setelah selesainya analisis.

*Memeriksa konfigurasi dan patch dari aplikasi database*

Konfigurasi default dari aplikasi database harus diubah, konfigurasi default merupakan salah satu kelemahan dari suatu aplikasi yang dapat dimanfaatkan untuk menyerang dan mengganggu fungsi normal dari suatu aplikasi.

*Memeriksa konfigurasi dan patch dari sistem operasi database server*

Kerentanan yang terdapat pada sistem operasi yang digunakan pada database server juga bisa digunakan oleh penyerang untuk mengganggu layanan data pada database server. Kerentanan itu harus diperiksa untuk memastikan keamanan dari sistem operasi yang digunakan.

*Memeriksa kode-kode program yang digunakan pada database*

Kode-kode program yang digunakan untuk mengakses dan memanipulasi data-data pada suatu data base harus memenuhi standar keamanan tertentu. Tidak amannya penggunaan kode-kode ini bisa dimanfaatkan oleh penyusup untuk masuk ke dalam database. Apabila seorang penyusup berhasil masuk ke dalam database dan mendapatkan hak akses penuh, maka penyusup dapat mencuri dan bahkan menghapus data-data penting dalam database.

*Melakukan investigasi terhadap personil*

Investigasi terhadap personil dilakukan untuk mengetahui seberapa besar tingkat keamanan terhadap hak akses ke dalam database yang dimiliki oleh para personil/karyawan. Bagaimana para karyawan dalam mengelolah kunci dan password yang telah dimilikinya harus mendapatkan perhatian. Penyusup ke dalam sistem database bisa memanfaatkan celah keamanan dari kerentanan pengelolahan hak akses para pengguna yang sah. Keteledoran dalam menyimpan password dapat menyebabkan password jatuh ke pihak-pihak yang tidak bertanggung jawab.

*Memeriksa penyandian yang digunakan pada data*

Supaya data-data yang tersimpan pada database memiliki keamanan yang relative tinggi, maka data-data tersebut harus disandikan (enkripsi). Data-data yang telah terenkripsi akan sulit diketahui arti sebenarnya dari data tersebut. Proses penyandian data dapat dilakukan pada data yang sedang dikirimkan pada jaringan, maupun data penting (memiliki tingkat kerahasiaan tinggi) yang tersimpan pada database.

*Memeriksa integritas database*

Memeriksa integritas data ditujukan untuk melihat tingkat keparahan dari kerusakan data yang diakibatkan oleh adanya gangguan pada sistem database.Informasi yang di simpan dalam basis data bisa berupa apa saja yang membuat keakuratan informasi dalam basis data itu perlu dipertanyakan. Untuk itulah integritas data dibutuhkan untuk menjaga keakuratan dan kebencxaran data.

Integritas data merupakan sebuah batasan atau syarat yang di peruntukan dalam basis data yang berfungsi dalam pembatasan data yang dapat simpan dalam basis data itu sendiri. Batasan itu menjaga

kerusakan terhadap database dengan memastikan bahwa perubahan tidak menyebabkan inkosistesi dari data. Integritas di sini mengacu pada konsistesi, akurasi dan keakuratan data yang disimpan dalam database.

## 2.4 Tahap Pemberantasan

Tahap ini merupakan tahapan untuk melakukan pemberantasan terhadap penyebab dari terjadinya insiden pada data/database. Pemberantasan yang dilakukan harus berdasarkan sumber dari serangan, yaitu

- Serangan malware, apabila terganggunya keamanan database disebabkan oleh malware, maka dilakukan prosedur pemberantasan malware (terdapat pada penanganan insiden malware)
- Serangan pada network, apabila terganggunya keamanan database disebabkan oleh adanya serangan pada jaringan, maka dilakukan prosedur pemberantasan gangguan pada jaringan (terdapat pada penanganan insiden jaringan).
- Memperbaharui kerentanan dari sistem operasi dari server database
- Memperbaharui kerentanan pada kode-kode pemrograman

  Apabila ditemukan adanya kerentanan pada kode-kode pemrograman yang digunakan untuk mengakses database, maka segera perbaharui kode-kode program tersebut sesuai dengan standar keamanan yang telah ditetapkan oleh vendor/pembuat bahasa pemrograman. Contoh halaman web yang bias digunakan sebagai panduan untuk membuat kode/program dengan menggunakan php

  - ✓ https://www.owasp.org/index.php/PHP_Security_Cheat_Sheet
  - ✓ http://www.php.net/manual/en/security.php

- Memperbaharui konfigurasi dari aplikasi dengan mengubah semua konfigurasi default sesuai dengan yang disyaratkan oleh vendor pembuat suatu aplikasi. Dibawah ini adalah halaman web

yang berisi tentang konfigurasi yang aman dari aplikasi database

- ✓ http://www.symantec.com/connect/articles/securing-mysql-step-step
- ✓ https://www.owasp.org/index.php/OWASP_Backend_Security_Project_MySQL_Hardening
- ✓ http://dev.mysql.com/doc/refman/5.0/en/security.html

- Memperbaharui metode akses
  Apabila terdapat kerentanan terhadap metode akses terhadap suatu system atau database, maka segera perbaharui kerentanan tersebut. Tindakan ini bias sampai perubahan pada personil yang memiliki hak akses terhadap suatu sistem.
- Memperbaharui metode pengiriman data
  Data-data yang dikirimkan melewati media pada jaringan harus memiliki tingkat keamanan yang tinggi. Data-data yang disalurkan pada media harus disandikan agar tidak mudah dibaca oleh pihak-pihak yang melakukan pengintaian dan capture pada lalu lintas jaringan komputer. Hal ini terutama untuk data-data yang disalurkan dengan menggunakan media udara (wireless).

## 2.5 Tahap Pemulihan

Pemulihan merupakan tahap untuk mengembalikan seluruh sistem bekerja normal seperti semula. Pada insiden keamanan data/database, pemulihan dilakukan terhadap penyebab terjadinya kebocoran/kerusakan data/database. Langkah- langkah yang dilakukan adalah sebagai berikut

a. Apabila serangan berasal dari sistem jaringan, konfirmasikan bahwa serangan pada jaringan telah selesai dan layanan database bisa dilakukan kembali. Untuk melihat pulihnya jaringan bisa dilakukan dengan memanfaatkan perintah pada command prompt seperti ping, tracert, pathping.
b. Apabila serangan berasal dari adanya malware, maka konfirmasikan juga bahwa malware telah dibersihkan, dan

client dapat mengakses database pada server secara aman.

c. Validasi sistem

   Sistem yang telah pulih, harus divalidasi terhadap kesalahan atau kekurangan konfigurasi apapun. Jika ada kekurangan pada perangkat lunak atau data yang ditemukan, maka akan ditambahkan. Melakukan patching dan mengubah konfigurasi pada sistem database, apabila konfigurasi pada sistem database telah menjadi penyebab terjadinya insiden pada database, harus dilakukan. Sebuah tanda tangan dari pengguna dan pemilik system seharusnya diminta untuk mengkonfirmasikan pemulihan lengkap dan normal dari sistem .

d. Pemulihan Operasi

   Setelah validasi sistem pulih selesai, pemilik sistem memutuskan kapan untuk menempatkan sistem kembali online. Rekomendasi mengenai keamanan sistem dapat diberikan kepada pemilik sistem. Pemilik harus mengakui rekomendasi ini melalui memo yang telah ditandatangani. Rekomendasi berisi tentang penguatan pertahanan terhadap sistem dari database, misalnya mengharuskan dilakukannya enkripsi pada penyaluran data melalui jaringan, data-data penting yang tersimpan juga harus dienkripsi, dan bisa juga rekomendasi untuk mengganti kunci-kunci enkripsi yang ada

e. Pemulihan Database

   Apabila telah terjadi kerusakan pada database, maka database yang telah terganggu (rusak atau hilang) harus dipulihkan kembali dengan cara melakukan restore dari backup yang telah dilakukan.

f. Pemulihan terhadap metode akses

   Pemulihan terhadap metode akses dilakukan dengan mengganti password- password yang telah diblokir. Password-password baru tersebut harus diubah oleh para penggunanya dengan mengikuti mekanisme yang telah diberikan oleh administrator. Konfirmasi pengubahan password harus dilakukan oleh para pengguna.

g. Pemantauan Sistem

Akhirnya aktifitas penting pada tahap pemulihan adalah melakukan pemantauan secara cermat agar sistem database tidak terganggu kembali. Pemantauan ini dilakukan untuk melihat adanya

1. Infeksi dan penyebaran malware
2. Aktifitas gangguan pada jaringan (DOS, DDOS)
3. Aktifitas pemindaian dan capture pada lalu lintas jaringan
4. Aktifitas pada server database (memantau log)

## 2.6 Tahap Tindak Lanjut

Tahap ini adalah fase di mana semua dokumentasi kegiatan yang dilakukan dicatat sebagai referensi untuk dimasa mendatang. Fase ini dapat memberikan masukan kepada tahap persiapan untuk meningkatkan pertahanan. Tahap dimana semua tahap sebelumnya telah dilalui, tujuan dari tahap ini adalah untuk,

a. Pelaporan, membuat laporan mengenai langkah-langkah dan hasil yang telah didapatkan pada penanganan insiden yang telah dilakukan. mendokumentasikan dampak dan biaya dari terjadinya insiden serangan pada sistem database.
b. Pembelajaran, adalah langkah yang sangat penting yang sering diabaikan. Pelajaran harus dapat dipetik dari kegiatan sesegera mungkin setelah penanganan insiden usai. Semua keputusan dan langkah-langkah yang diambil sepanjang siklus penanganan insiden harus ditinjau. Semua prosedur harus ditinjau untuk melihat di mana perbaikan dapat dilakukan.Salah satu hal penting yang harus dilakukan setelah berhasil menangani sebuah insiden adalah memperbarui pengetahuan. Catatan tentang penambahan pengetahuan ini harus ditambahkan pada dokuman laporan dan direview oleh semua pihak yang telah berperan dalam penanganan insiden. Hal ini akan membantu dalam penanganan insiden serupa di masa depan dengan mudah, efisien, dan cepat

c. Peningkatan kepedulian terhadap keamanan jaringan, dengan melakukan review setelah setiap kejadian, akan memungkinkan bagi organisasi untuk melakukan perbaikan terus-menerus dan berpotensi pada pengurangan yang signifikan akibat dampak insiden.

d. Peningkatan pertahanan

   Setelah penanganan selesai, Root Cause Analysis digunakan untuk menguatkan berbagai kontrol keamanan yang terdapat dalam perusahaan. Tim teknis dapat dibuat peduli dan menyadari terjadinya gejala serangan pada sistem database yang sama, tim penanganan insiden dapat diberikan insiden serupa untuk melatih diri dan manajemen dapat memperkenalkan kontrol keamanan yang baru untuk mengurangi risiko di masa depan.

e. Memperbaharui segala standar dan prosedur

   Semua jalan masuknya penyusup ke dalam sistem database yang diidentifikasi harus tepat diblokir untuk mencegah serangan masuk ke dalam jaringan data dimasa depan. Hal ini dapat dilakukan dengan menambahkan aturan baru di perimeter dan perangkat penyaringan lainnya (seperti filter URL, filter email, IDS). Memungkinan pembaharuan pada dokumen-dokumen berikut:

   - Standard Operating Procedures
   - Prosedur Operasi Darurat
   - Disaster Recovery plan (DRP)

# LAMPIRAN A - Informatif

## KEAMANAN SISTEM DATABASE

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 mempengaruhi sistem, dan memiliki konsekuensi terhadap perusahaan/organisasi yang memiliki sistem database.

Keamanan database tidak hanya berkenaan dengan data yang ada pada database saja, tetapi juga meliputi bagian lain dari sistem database, yang tentunya dapat mempengaruhi database tersebut. Hal ini berarti keamanan database mencakup perangkat keras, perangkat lunak, orang 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 system database, oleh karena itu administrator harus mempunyai kemampuan dan pengetahuan yang cukup agar dapat mengatur suatu sistem database.

Keamanan merupakan suatu proteksi terhadap pengrusakan data dan pemakaian data oleh pengguna yang tidak berhak. Sistem keamanan database adalah sistem, proses, dan prosedur yang melindungi database dari aktivitas yang sengaja maupun tidak disengaja. Sistem yang aman memastikan kerahasian data yang terdapat didalamnya. Beberapa aspek keamanan yaitu :

- □ Mambatasi akses ke data dan layanan
- □ Melakukan autentifikasi pada user
- □ Memonitor aktivitas-aktivitas yang mencurigakan

Keamanan database dapat dikelompokan sebagai berikut :

- □ Pencurian dan penipuan.

Pencurian dan penipuan database tidak hanya mempengaruhi lingkungan database tetapi juga seluruh perusahaan/organisasi. Keadaan ini dilakukan oleh orang, dimana seseorang ingin melakukan pencurian data atau manipulasi data, seperti saldo rekening, transaksi, transfer dan lain-lain. Untuk itu fokus harus dilakukan pada kekuatan sistem agar menghindari akses oleh orang yang tidak memiliki kewenangan.

- Hilangnya kerahasiaan dan privasi
  Suatu data dapat memiliki nilai kerahasiaan, karena data tersebut merupakan sumber daya yang strategis pada perusahaan, maka pada kasus ini data tersebut harus diamankan dengan memberikan hak akses pada orang tertentu saja.
- Hilangnya integritas
  Integritas ini berkaitan dengan akurasi dan kebenaran data dalam database, seperti data korup. Hal ini akan secara serius mempengaruhi proses bisnis perusahaan/organisasi.
- Hilangnya ketersediaan
  Hilangnya ketersediaan berarti data, sistem, keduanya tidak dapat diakses, layanan mati, yang tentunya secara serius sangat mempengaruhi perusahaan/organisasi. Saat ini banyak perusahaan yang membutuhkan kemampuan sistem yang aktif 7 x 24 , 7 hari 1 minggu.

Berdasarkan pengelompokan tersebut, tentunya banyak aspek yang harus kita perhatikan demi terciptanya keamanan database. Bisa saja seseorang mencuri komputer kita yang berisi data penting, mungkin juga karyawan yang diberi hak untuk mengakses data melakukan kejahatan dengan menjual informasi tersebut pada pihak lain demi kepentingan pribadi. Hal- hal tersebut memang termasuk kendala keamanan database yang harus mendapat perhatian, tetapi seorang administrator tidak dapat mengawasi kelemahan tersebut. Seorang administrator hanya fokus pada sistem database itu sendiri, dan hal inilah yang seharusnya menjadi perhatian juga dalam organisasi.

Tentunya perkembangan teknologi mengharuskan suatu perusahaan untuk mengimplementasikan sistem database yang bukan hanya aman tetapi juga mudah diakses dan handal, menyala 7x24 jam, 7 hari 1 minggu tanpa off.

Penyebaran informasi secara global sangat menguntungkan semua pihak. Dengan adanya Internet, komunikasi antar cabang, perusahaan, konsumen dan sebagainya semakin mudah. Pemberian informasi mengenai perusahaan kepada masyarakat melalui internet merupakan salah satu strategi komunikasi, marketing, public relation perusahaan tersebut, adanya transaksi on line yang meningkatkan gaya hidup masyarakat dan lain-lain. Semua itu tidak terlepas dari suatu perkembangan sistem database dan tentunya membuat keamanan menjadi rentan.

Sangatlah mudah dalam suatu lingkungan database diciptakan suasana yang menakutkan, tanpa kepastian dan keraguan. Sebagai seorang administrator sangat perlu memperhatikan kondisi tersebut. Tentukan resiko yang sebenarnya dan selidiki apa yang dapat dilakukan terhadap kondisi itu. Sebenarnya kebanyakan database terkonfigurasi dalam keadaan yang mudah ditembus, akan tetapi hal ini bukan berarti database tidak dapat dibuat aman sebagaimana mestinya.

Secara garis besar keamanan database dikategorikan sbb:

- Keamanan Server
  Perlindungan Server adalah suatu proses pembatasan akses yang sebenarnya pada database dalam server itu sendiri. Server sebagai tempat database harus benar-benar dijamin keamanannya.

- Trusted Ip Access
  Setiap server harus dapat mengkonfigurasikan alamat ip yang diperbolehkan mengakses dirinya. Sistem harus tidak mengijinkan semua orang untuk dapat mengakses server, sebagaimana tidak mengijinkan seseorang memasuki rumah tanpa ijin. 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 dianjurkan untuk tidak menggabungkan server web dengan server database

informasi internal perusahaan, ini adalah suatu cara yang buruk untuk seorang admin. Trusted Ip Acces merupakan server database terbatas yang hanya akan member respon pada alamat ip yang dikenali saja.

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

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

Pelanggaran keamanan mungkin terjadi karena seorang hacker yang mampu melewati langkah-langkah keamanan yang telah dibentuk. Ini mungkin juga dikenal sebagai suatu pelanggaran keamanan. Keamanan pelanggaran bisa terjadi bukan hanya karena hacker, tetapi juga karena kecerobohan. Ada undang-undang tentang pelanggaran keamanan yang menyatakan bahwa seseorang harus diberitahu ketika informasi vitalnya telah diganggu.
Ada banyak cara yang berbeda tentang bagaimana menangani pelanggaran keamanan ketika keamanan database telah dilanggar.
Database (dan khususnya SQL) telah lama menjadi bagian Integral dari

sistem dalam menjalankan bisnis, baik dalam bentuk awalnya, yaitu file database biasa maupun dalam bentuk sekarang ini,yaitu database yang berorientasi pada tingkat lanjut. Kebutuhan atas penyimpanan dan pengaksesan informasi secara cepat menjadi hal-hal yang mendesak bagi tiap bisnis atau aplikasi, begitu pula web.

Aplikasi-aplikasi web sekarang ini berpasangan dengan database. Database dipakai untuk beragam kegunaan mulai dari menyimpan nama-nama user dan password-pasword untuk akses resmi, sampai untuk menyimpan alamat-alamat email user, dan informasi kartu kredit untuk mempermudah pengiriman produk dan pembayarannya. Oleh karena itu, pemahaman menyeluruh mengenai keamanan web harus mencakup juga lapisan databasenya dan terpenting memahami juga bagaimana penyusup berusaha memasuki aplikasi untuk memperoleh akses ke bagian-bagian datanya.

Keamanan database merupakan satu dari sekian banyak metodologi yang sering diabaikan dan tidak dikembangkan untuk melengkapi dan memperketat kebijaksanaan atas keamanan database, beberapa cara dibawah ini berguna untuk pencegahan dalam tiap kelemahan.

1. Selalu mengupdate patch

   Baik untuk Microsoft maupun oracle, patch-patch dan beberapa perbaikan baru biasanya diedarkan secara regular. Memastikan untuk nengunduh dan menginstalnya segera setelah patch patch itu tersedia. Selalu menguji patch terlebih dahulu pada system mirror atau pada sistem yang tak menghasilkan produksi, tidak pada system yang sebenarnya,

2. Menerapkan aturan-aturan firewall yang ketat

   Memastikan memeriksa konfigurasi firewall dari waktu ke waktu dan selalu memblock port-port akses database seperti TCP dan UDP 1434 (MS SQL) dan TCP1521-1520 (Oracle).

3. Sanitasi/Penyaringan Input

   Direktorat Keamanan Informasi, Halaman 24/40Penyaringan harus dilakukan pada yang di terima dari user, data–data yang diterima harus diperiksa tipenya (integer, string, dan seterusnya) dan harus memotong karakter-karakter yang tidak diinginkan, misalnya meta karakter.

4. Membuang Stored Procedure

Stored Procedure adalah sebuah prosedur yang disimpan dalam suatu tabel database. Memastikan telah membuang semua stored procedure (termasuk extended stored procedure) dari keseluruhan database, termasuk master. Script-script yang kelihatannya tidak berbahaya ini bisa memberi bantuan dalam menumbangkan bahkan database yang paling aman sekalipun.

5. Enkripsi Session

   Jika server database terpisah dari Web server, memastikan untuk mengenkripsi session dengan beberapa cara, misalnya menggunakan IPSec built-in Pada Windows.

6. Sedikit Hak-hak khusus

   Memastikan untuk menerapkan sesedikit mungkin hak-hak akses untuk mengakses file-file database.