KEAMANAN DATABASE DAN TEKNIK PEMULIHAN DATA

PERTEMUAN 13

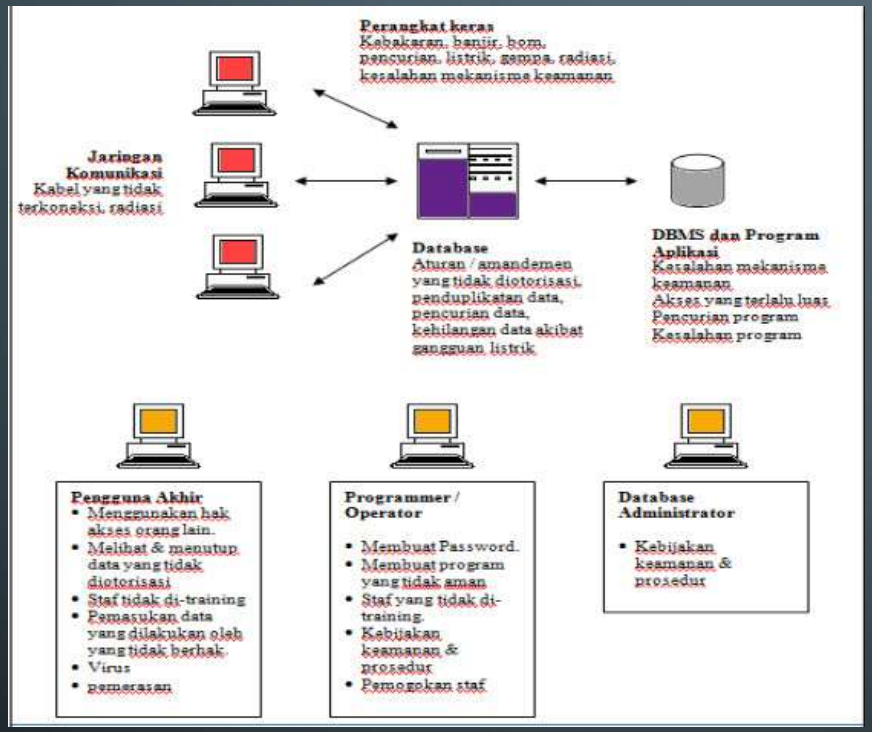
PENYERANGAN DATABASE

- Informasi sensitif yang tersimpan didalam database dapat terbuka (disclosed) bagi orang-orang yang tidak diizinkan (unauthorized)
- Informasi sensitif yang tersimpan didalam database dapat inaccessible bagi orang-orang yang diizinkan.

BAGAIMANA CARA MENJAGA KEAMANAN DATABASE ?

Penentuan perangkat lunak Data Base Server yang handal.

Pemberian otoritas kepada user mana saja yang berhak mengakses, serta memanipulasi data yang ada.



KONTROL AKSES TABLE

- Kontrol akses table merupakan hal tersulit. Pengamanan yang benar membutuhkan kolaborasi antara system Administrator dengan pengembang database, Pengamanan yang benar membutuhkan kolaborasi antara system Administrator dengan pengembang database

Ancaman Yang Mungkin Terjadi :

- Pengguna Akhir :
  - menggunakan hak akses orang lain
  - melihat dan menutup data yang tidak di otorisasi
  - staf tidak di training
  - pemasukan data yang dilakukan oleh yang tidak berhak
  - virus
  - pemerasan
- Programmer / Operator :
  - Membuat Password
  - Membuat program yang tidak aman
  - staf yang tidak di training
  - kebijakan kemanan dan prosedur
  - Pemogokan staff
- Database Administrator :
  - kebijakan keamanan dan prosedur

PENYALAHGUNAAN DATABASE

- Tidak Disengaja, jenisnya:
  - Kerusakan selama proses transaksi
  - Anomali yang disebabkan oleh akses database yang konkuren (bersaing)
  - Anomali yang disebabkan oleh pendistribusian data pada beberapa komputer
  - Logika error yang mengancam kemampuan transaksi untuk mempertahankan konsistensi database
- Disengaja, jenisnya
  - Pengambilan data/ pembacaan data oleh pihak yang tidak berwenang.
  - Pengubahan data oleh pihak yang tidak berwenang
  - Penghapusan data oleh pihak yang tidak berwenang

TINGKATAN PADA KEAMANAN DATABASE

- Fisikal lokasi-lokasi dimana terdapat sistem komputer haruslah aman secara fisik terhadap serangan perusak.
- Manusia wewenang pemakai harus dilakukan dengan berhati-hati untuk mengurangi kemungkinan adanya manipulasi oleh pemakai yang berwenang
- Sistem Operasi Kelemahan pada SO ini memungkinkan pengaksesan data oleh pihak tak berwenang, karena hampir seluruh jaringan sistem database menggunakan akses jarak jauh.
- Sistem Database Pengaturan hak pemakai yang baik.

OTORISASI

- Pemberian Wewenang atau hak istimewa (priviledge) untuk mengakses sistem atau obyek database
- Kendali otorisasi (=kontrol akses) dapat dibangun pada perangkat lunak dengan 2 fungsi :
  - Mengendalikan sistem atau obyek yang dapat diakses
  - Mengendalikan bagaimana pengguna menggunakannya
    - Sistem administrasi yang bertanggungjawab untuk memberikan hak akses dengan membuat account

TABLE VIEW

- Merupakan metode pembatasan bagi pengguna untuk mendapatkan model database yang sesuai dengan kebutuhan perorangan. Metode ini dapat menyembunyikan data yang tidak digunakan atau tidak perlu dilihat oleh pengguna pengguna.
- Contoh Pada Database Relasional, untuk pengamanan dilakukan beberapa level :
  - Relasi pengguna diperbolehkan atau tidak diperbolehkan mengakses langsung suatu relasi
  - View pengguna diperbolehkan atau tidak diperbolehkan mengakses data yang terdapat pada view
  - Read Authorization pengguna diperbolehkan membaca data, tetapi tidak dapat memodifikasi.
  - Insert Authorization pengguna diperbolehkan menambah data baru, tetapi tidak dapat memodifikasi data yang sudah ada.
  - Update Authorization pengguna diperbolehkan memodifikasi data, tetapi tidak dapat menghapus data.
  - Delete Authorization pengguna diperbolehkan menghapus data.

Untuk Modifikasi data terdapat otorisasi tambahan :

- Index Authorization : pengguna diperbolehkan membuat dan menghapus index data.
- Resource Authorization : pengguna diperbolehkan membuat relasi-relasi baru.
- Alteration Authorization : pengguna diperbolehkan menambah/menghapus atribut suatu relasi.
- Drop Authorization : pengguna diperbolehkan menghapus relasi yang sudah ada.

CONTOH PERINTAH MENGGUNAKAN SYNTAK SQL

Contoh perintah menggunakan SQL :

GRANT : memberikan wewenang kepada pemakai
Syntax : GRANT <priviledge list> ON <nama relasi/view> TO <pemakai>
Contoh :
GRANT SELECT ON S TO BUDI
GRANT SELECT,UPDATE (STATUS,KOTA) ON S TO ALI,BUDI

REVOKE : mencabut wewenang yang dimiliki oleh pemakai
Syntax : REVOKE <priviledge list> ON <nama relasi/view> FROM <pemakai>
Contoh :
REVOKE SELECT ON S FROM BUDI
REVOKE SELECT,UPDATE (STATUS,KOTA) ON S FROM ALI,BUDI

Priviledge list : READ, INSERT, DROP, DELETE, INDEX, ALTERATION, RESOURCE

BACKUP DATA DAN RECOVERY

- Backup : proses secara periodik untuk mebuat duplikat ari database dan melakukan logging file (atau program) ke media penyimpanan eksternal.
- Recovery : merupakan upaya uantuk mengembalikan basis data ke keadaan yang dianggap benar setelah terjadinya suatu kegagalan.

TEKNIK PEMULIHAN DATA

- Defered update / perubahan yang ditunda: perubahan pada DB tidak akan berlangsung sampai transaksi ada pada poin disetujui (COMMIT). Jika terjadi kegagalan maka tidak akan terjadi perubahan, tetapi diperlukan operasi redo untuk mencegah akibat dari kegagalan tersebut.
- Immediate Update / perubahan langsung: perubahan pada DB akan segera tanpa harus menunggu sebuah transaksi tersebut disetujui. Jika terjadi kegagalan diperlukan operasi UNDO untuk melihat apakah ada transaksi yang telah disetujui sebelum terjadi kegagalan.
- Shadow Paging: menggunakan page bayangan dimana pada prosesnya terdiri dari 2 tabel yang sama, yang satu menjadi tabel transaksi dan yang lain digunakan sebagai cadangan. Ketika transaksi mulai berlangsung kedua tabel ini sama dan selama berlangsung tabel transaksi yang menyimpan semua perubahan ke database, tabel bayangan akan digunakan jika terjadi kesalahan. Keuntungannya adalah tidak membutuhkan REDO atau UNDO, kelemahannya membuat terjadinya fragmentasi
  - Fragmentasi adalah sebuah proses pengambilan bagian naris atau kolom dari table table sebagai unit terkecil yang akan dikirimkan melalui jaringan komputer
  - Fragmentasi data adalah dimana proses basis data dipecah kedalam unit logic yagn disebut fragment yang kemudian akan disimpan dalam site yang berbeda

KESATUAN DATA DAN ENKRIPSI

- Enkripsi Keamanan Data Base merupakan salah satu hal penting yang berguna untuk menjamin kerahasian data dengan melakukan enkripsi pada data maka data yang tadinya dimengerti menjadi tidak dapat dimengerti
- Integritas : Metode Pemeriksaan dan validasi data (metode integrity constrain) yaitu berisi aturan aturan atau batasn batasan agar terlaksananya integritas data
- Konkuren : Mekanisme untuk menjamin bahwa transaksi yang konkuren pada database multi user tidak saling mengganggu operasinya masing masing . Adanya Penjadwalan prose yang kurang akurat (Time Stamping)