Tugas Kelompok Perancangan Sistem Keamanan Basis Data
Basis Data Pertemuan 13

Rabu, 29 Mei 2024

Nama Anggota:

- Irvan Nurfauzan Saputra (2022071031)
- Indah Hairunisah (2022071025)
- Fitriyana Nuril Khaqqi (2022071003)

Tugas:

Dari hasil mempelajari Studi Kasus Manajemen Sistem Keamanan Basis Data, buatlah rancangan dan implementasikan pola rancangan ini berupa Sistem Keamanan Basis Data yang diterapkan terhadap RDBMS yang telah dirancang dan diimplementasikan oleh masing-masing kelompok.

Jawab:

Pendahuluan

Dalam studi kasus manajemen sistem keamanan basis data, penting untuk merancang dan mengimplementasikan sistem keamanan yang melindungi integritas, kerahasiaan, dan ketersediaan data. Sistem keamanan ini harus diterapkan ke RDBMS yang telah dirancang dan diimplementasikan oleh masing-masing kelompok. Berdasarkan permasalahan dari Ibu Maya, kelompok kami memberikan terobosan solusi teknologi berupa aplikasi berbasis aplikasi mobile dengan nama "MyBalance" untuk membantu Ibu Maya mencapai keseimbangan yang diinginkannya dalam hidup. Dengan menggabungkan berbagai fitur yang menunjang kesehatan, komunikasi, dan pengembangan diri, aplikasi ini dapat membantu Ibu Maya menjadi ibu sekaligus pekerja profesional yang lebih bahagia dan sejahtera.

Tujuan

- Melindungi Data: Memastikan bahwa data yang disimpan dalam RDBMS tetap aman dari akses yang tidak sah.
- Menjaga Integritas: Menjamin bahwa data tidak diubah dengan cara yang tidak sah.
- Ketersediaan: Memastikan data tersedia bagi pengguna yang berwenang kapanpun diperlukan.

Otorisasi dan Autentikasi

Setiap pengguna akan memiliki akun yang unik dan terotentikasi sebelum mereka dapat mengakses aplikasi dan basis data. Kombinasi username dan password yang kompleks akan memberikan sistem autentikasi yang kuat.

Pengendalian Akses

Tingkat akses akan disesuaikan untuk setiap pengguna. Misalnya, pengguna dapat memiliki akses penuh untuk jadwal mereka sendiri, tetapi hanya akses baca untuk jadwal pengguna lain. Adapun dalam pengendalian akses terdapat dua poin penting untuk mengamankan basis data.

- Buat pengguna dan peran di RDBMS.
- Tentukan hak akses untuk setiap peran.

Enkripsi Data

Enkripsi melindungi data dari akses yang tidak sah dengan mengubah data menjadi format yang tidak dapat dibaca tanpa kunci enkripsi.

Pemantauan dan Audit

Administrator akan melakukan pemantauan dan audit yang memungkinkan pencatatan aktivitas pengguna dan perubahan data. Pemantauan dan audit ini akan membantu mengidentifikasi potensi ancaman keamanan dan memungkinkan adopsi tindakan pencegahan yang tepat.

Pemulihan Bencana

Buat rencana pemulihan bencana yang mencakup pencadangan data secara berkala dan pemulihan sistem dalam situasi darurat. Simpan salinan cadangan di lokasi yang aman dan lakukan pengujian pemulihan secara berkala untuk memastikan integritas data yang tersimpan.

1. Backup:

   Backup adalah proses pembuatan salinan data yang dapat digunakan untuk memulihkan data yang hilang atau rusak. Backup dapat dilakukan dalam berbagai format, seperti snapshot, dump file, atau salinan lengkap dari database.

   Jenis-Jenis Backup

- Full Backup: Salinan lengkap dari seluruh database. Biasanya dilakukan secara berkala.
- Incremental Backup: Mencakup hanya data yang berubah sejak backup terakhir. Lebih cepat dan lebih efisien dalam penggunaan ruang penyimpanan.
- Differential Backup: Mencakup data yang berubah sejak full backup terakhir. Lebih cepat daripada full backup, tetapi lebih lambat daripada incremental backup.

2. Restore

   Restore adalah proses mengembalikan data dari backup ke sistem basis data setelah terjadi kehilangan data atau kerusakan. Ini memungkinkan pemulihan operasi normal dengan data yang telah disimpan sebelumnya.

Kesimpulan

Implementasi sistem keamanan basis data yang mencakup kontrol akses, enkripsi, audit, dan monitoring serta backup dan restore sangat penting untuk melindungi data dari akses tidak sah, memastikan integritas data, dan memastikan ketersediaan data dalam keadaan darurat. Langkah-langkah ini harus diintegrasikan dengan kebijakan keamanan yang kuat dan dipantau secara terus-menerus untuk mengantisipasi dan merespons ancaman keamanan yang mungkin muncul.