



Universidade Federal do Ceará
Campus Crateús

Fundamentos de Banco de Dados

Aula 12 - Segurança em banco de dados



Professora Vitória Regina - vitoria@crateus.ufc.br



O que estudaremos?

- Aspectos Gerais de Segurança.
- Princípios da segurança da informação.



Aspectos Gerais de Segurança

- Porque devemos ter segurança em um Banco de Dados?
 - Possuir informação hoje é ganhar agilidade, competitividade, previsibilidade, dinamismo, portanto, possuir informação é o mesmo que possuir um diferencial, uma vantagem competitiva. Uma informação útil pode ser usada a favor ou contra você ou sua empresa.

Aspectos Gerais de Segurança

- Os princípios da segurança da informação são:
 - Confidencialidade;
 - Integridade;
 - Disponibilidade.

Aspectos Gerais de Segurança

- De acordo com SÊMOLA (2003, p.12), os principais motivos para se proteger uma informação são:
 - Seu valor;
 - Impacto de sua ausência;
 - Impacto resultante de seu uso por terceiros;
 - Importância de sua existência e a relação de dependência com a sua atividade, e
 - Informação deve ser protegida em todo o seu ciclo de vida, desde sua criação, manuseio, armazenamento transporte e descarte.

Aspectos Gerais de Segurança

- Controle de Redundância:
 - A redundância é caracterizada pela presença de um elemento de informação duplicado.
 - Sistemas de banco de dados devem ter capacidade de garantir que os dados não sejam redundantes.

Aspectos Gerais de Segurança

- Controle de Concorrência:
 - É um esquema usado para garantir que as transações são executadas de forma segura.
 - Uma das qualidades dos sistemas desenvolvidos é a multiprogramação que permite a execução de diversas transações visando o compartilhamento do processador. Nesse ambiente multiprogramado diversas transações podem executar concorrentemente. Por isso os sistemas precisam controlar a interação entre transações concorrentes com o objetivo de prevenir a violação da consistência do banco de dados.

Aspectos Gerais de Segurança

- Restrição de Integridade:
 - As restrições de integridade oferecem meios de assegurar que mudanças feitas no banco de dados por usuários autorizados não resultem em perda de consistência dos dados.
 - As restrições de integridade podem resguardar o banco de dados contra danos acidentais.

Aspectos Gerais de Segurança

- Restrição de Integridade:
 - A integridade referencial é usada para garantir que um valor que aparece em uma relação para um dado conjunto de atributos também apareça para um certo conjunto de atributos em outra relação.
 - No modelo Entidade – Relacionamento, o esquema do banco de dados relacional derivado de diagramas resulta em um conjunto de relacionamentos que possui regras de integridade referencial.

Aspectos Gerais de Segurança

- Evitar violação de consistência dos dados:
 - Para evitar a violação dos dados e garantir a consistência, confiabilidade, podemos adotar alguns mecanismos de segurança entre esses mecanismos podemos destacar:
 - **Mecanismos de controles físicos:** portas / trancas / paredes / blindagem /etc...
 - **Mecanismos de controles lógicos:** Mecanismos de criptografia/ Assinatura digital /Mecanismos de garantia da integridade da informação /Mecanismos de controle de acesso e etc...

Aspectos Gerais de Segurança

- Criptografia:
 - A Criptografia é a técnica pela qual a informação pode ser transformada da sua forma original para outra ilegível, de forma que possa ser conhecida apenas por seu destinatário, o que a torna difícil de ser lida por alguém não autorizado. Assim sendo, só o receptor da mensagem pode ler a informação com facilidade.

Aspectos Gerais de Segurança

- A criptografia tem quatro objetivos principais:
 - Confidencialidade da mensagem;
 - Integridade da mensagem;
 - Autenticação do remetente;
 - Não-repúdio ou irretratabilidade do emissor.

Aspectos Gerais de Segurança

- Criptografia:
 - Nem todos os sistemas ou algoritmos criptográficos são utilizados para atingir todos os objetivos listados acima.
 - Normalmente, existem algoritmos específicos para cada uma destas funções.
 - Mesmo em sistemas criptográficos bem concebidos, bem implementados e usados adequadamente, alguns dos objetivos acima não são práticos (ou mesmo desejáveis) em algumas circunstâncias.

Aspectos Gerais de Segurança

- Segurança de acesso:
 - A preocupação com a criação e manutenção de ambientes seguros têm sido tarefas cruciais de administradores de redes, de sistemas operacionais e de bancos de dados.
 - Pesquisas mostram que boa parte dos ataques, roubos de informações e acessos não-autorizados são feitos por pessoas que pertencem à organização alvo.

Aspectos Gerais de Segurança

- Segurança de acesso:
 - Quando um usuário se conecta ao banco de dados “sua identidade” é determinada pela máquina de onde ele conectou e o nome de usuário que ele especificou.
 - O sistema concede privilégios de acordo com sua identidade e com o que ele deseja fazer.
 - Assim é possível que usuários provenientes de diferentes lugares da internet possuam o mesmo nome de usuário e privilégios totalmente diferentes um do outro.

Aspectos Gerais de Segurança

- SQL injection:
 - A Injeção de SQL, mais conhecida através do termo americano SQL Injection, é um tipo de ameaça de segurança que se aproveita de falhas em sistemas que interagem com bases de dados via SQL.

Aspectos Gerais de Segurança

- Impossibilitando o uso de SQL Injection
 - Para que se esteja livre da utilização da SQL Injection, certas providências devem ser tomadas. Algumas das ações serão realizadas no servidor de banco de dados, outras devem ser garantidas pelo código fonte.
 - Deve-se tomar cuidado com a configuração do usuário que estabelece a conexão com o banco de dados.

Aspectos Gerais de Segurança

- SQL injection:
 - Uma dica importante é evitar a exibição das mensagens de erro em um servidor de aplicação em produção, pois geralmente nos erros ou alertas são exibidos caminhos de diretórios do sistema de arquivos e informações à respeito do esquema do banco de dados, podendo comprometer a segurança do sistema.

Aspectos Gerais de Segurança

- Segurança contra falhas (recovery):
 - A recuperação/tolerância a falhas tem por objetivo restaurar o BD para um estado de integridade, após a ocorrência de uma falha;
 - O mecanismos de recuperação baseia-se na utilização de formas de redundância que quase duplicam o BD, utilizando: Backup.

Aspectos Gerais de Segurança

- Backups do BD:
 - Os backups são cópias de segurança do BD, que são executados periodicamente e constituem um ponto de partida para a recuperação do BD após a ocorrência de uma falha, independentemente da sua gravidade.

Aspectos Gerais de Segurança

- Backups do BD:
 - Uma forma de minimizar esta situação é aumentando a periodicidade dos backups, o que é um processo pesado, consumidor de recursos e que pode obrigar a paradas dos sistemas.

Aspectos Gerais de Segurança

- Backups do BD:
 - Com isso se garante duas das características fundamentais das transações:
 - Atomicidade;
 - Persistência.

Aspectos Gerais de Segurança

- Tipo de Falhas:
 - Falha de disco;
 - Falha de sistema;
 - Falha de transação.

Aspectos Gerais de Segurança

- Auditoria em Banco de Dados:
 - É o conjunto de ações para verificar o que os usuários estão fazendo.
 - Muitas empresas fazem isso para os fins de segurança. Isso é para garantir que usuários não autorizados não estão acessando uma parte do banco de dados ou a estrutura principal que não é permitida.
 - A maioria das informações críticas de uma empresa, 90% ou mais, é mantida no banco de dados.

Aspectos Gerais de Segurança

- Segurança em Banco de dados Livres (Mysql):
 - O MySQL sem dúvida nenhuma, é o banco de dados open source mais conhecido do mercado e provavelmente o mais utilizado.
 - Ele é rápido, simples, funcional e hoje implementa recursos que o colocam próximo a grandes nomes como Oracle.
 - Até pouco tempo um recurso extremamente útil e que era fator que impedia utilização em várias empresas, é o suporte à transação.

Aspectos Gerais de Segurança

- Recomendações para um ambiente seguro:
 - Conceder apenas os privilégios necessários para cada usuário, nunca mais do que isso;
 - Não manter senhas em texto puro no banco de dados, em vez disso, utilizar alguma função de criptografia de via única, com SHA1 ou MD5;

Aspectos Gerais de Segurança

- Recomendações para um ambiente seguro:
 - Não escolher senhas que contenham palavras existentes em dicionários;
 - Utilizar um firewall;
 - Não confiar em nenhum dado inserido pelos usuários, muitos deles podem tentar atacar o sistema inserindo caracteres especiais nas entradas dos formulários contendo algum.



Aula 12 - Segurança em banco de dados



Dúvidas?
vitoria@crateus.ufc.br