8º FÓRUM ENSINO · PESQUISA EXTENSÃO · GESTÃO FEPEG
UNIVERSIDADE: SABERES E PRÁTICAS INOVADORAS
Trabalhos científicos · Apresentações artísticas e culturais · Debates · Minicursos e Palestras
REALIZAÇÃO: Unimontes
APOIO: FAPEMIG FADENOR
24 a 27 setembro
Campus Universitário Professor Darcy Ribeiro
www.fepeg.unimontes.br

Segurança em Banco de Dados: Uma visão geral sobre segurança e suas principais deficiências

Marcos Vinicius Soares Santos, Diorgenes Ferreira, Marcos Paulo Maia Rodrigues, Renato César Oliveira Moreira

INTRODUÇÃO

Atualmente, se trabalha com uma grande porção de dados e esses altamente relacionados com outras massas de dados ou aplicações diversas. Manter esses dados é uma tarefa complexa, tanto no ponto de vista de segurança, quanto mecanismos de recuperação de falhas, pois existem diversas técnicas ou problemas operacionais que são encontrados a cada dia para danificar, acessar informação ou qualquer tipo de ação não esperada em um banco de dados. Esse artigo tem o objetivo de demonstrar quais são os principais problemas de segurança atuais, e como ocorrem.

O banco de dados de uma empresa contém uma grande quantidade de dados e geralmente um grande número de usuários. A maioria destes usuários não tem a necessidade de acessar todos os dados. Assim, permitir o acesso irrestrito a todos os dados pode ser indesejável e o SGBD deve prover mecanismos para controlar este acesso.

Conceptualização

Segurança é a condição de estar sendo protegido contra o perigo ou a perda. Pode consistir em uma proteção física, social, espiritual, financeira, política, emocional, ocupacional, psicológica, educacional ou de outro tipo. Ou ainda, a ocorrência de falhas, danos, erros, acidentes ou algum outro evento que poderia ser considerado indesejado.

Segurança da informação está relacionada com a proteção existente ou necessária sobre dados que possuem valor para alguém ou para uma organização. Tal segurança não está restrita a sistemas computacionais, nem a informações eletrônicas ou qualquer outra forma mecânica de armazenamento.

Segundo ALBUQUERQUE (2002) e KRAUSE (1999) as principais propriedades que, atualmente, orientam a análise, o planejamento e a implementação da segurança para um determinado grupo de informações que se deseja proteger são:

- **Confidencialidade** – as informações só podem ser acessadas por pessoas autorizadas pelo seu proprietário;
- **Integridade** – as características originais da informação, estabelecidas pelo seu proprietário, devem ser mantidas; e
- **Disponibilidade** – a informação deve estar sempre disponível para os usuários autorizados pelo proprietário da informação.

Outros conceitos associados à segurança da informação são ameaça, vulnerabilidade e ataque que é uma ação executada por um intruso, que encontra uma vulnerabilidade para provocar a ocorrência de uma ameaça.

Ameaça

Ameaça em um sistema computacional é definida como qualquer ocorrência potencial que pode levar a um efeito indesejado nos recursos associados ao sistema. A Microsoft classifica essas ameaças em várias categorias importantes que são comumente conhecidas e facilmente lembradas pela sigla STRIDE [HERNAN (2006)], na qual cada letra representa as iniciais das seguintes ameaças:

- **Spoofing** (invasão disfarçada) – o spoofing ocorre quando um invasor (usuário ou sistema) se passa por um usuário legal do sistema;
- **Tampering** (adulteração) – a adulteração ocorre quando um invasor adultera o sistema;
- **Repudiation** (repúdio) – o repúdio ocorre quando não é capaz de provar o responsável por determinadas modificações no sistema;
- **Information disclousure** (revelação de informações) – a revelação de informação ocorre quando as informações de um usuário são visualizadas por um invasor;

- **Denial of Service** (negação de serviço) – um ataque de negação de serviço ocorre quando uma aplicação inunda o processamento ou a memória de um sistema pela grande injeção de mensagens; e
- **Elevation of privilege** (elevação de privilégios) – os ataques de elevação de privilégios são carregados quando um invasor for capaz de elevar ou ganhar privilégios adicionais aos normalmente concedidos.

Vulnerabilidade

Vulnerabilidade é uma característica do sistema que torna possível que uma ameaça potencial ocorra. Ou seja, uma vulnerabilidade permite que algo ruim aconteça. Algumas das vulnerabilidades mais comuns são descritas a seguir:

Atividade de usuário – os próprios usuários podem tornar o sistema vulnerável. Por exemplo, quando um usuário inadvertidamente tenta abrir um anexo de e-mail que possa conter um vírus;

Nomes de usuário e senhas fracos – nomes de usuário fracos, como "administrador", "gerente", e senhas fracas, como uma senha em branco ou "1234" (uma sequência);

Permissões excessivas – aos usuários frequentemente são concedidos mais permissões e privilégios do que são estritamente necessários. Permitindo que os usuários acidentalmente ou intencionalmente gerassem brechas na segurança;

Engano – os usuários podem ser iludidos em revelar informações privadas sobre eles mesmos. Por exemplo, um site disfarçado de um site de banco para capturar a senha da conta corrente do usuário;

Serviços e portas excessivos – na qual os serviços e portas que não são utilizados podem fornecer uma abertura para invasores; e

Ataques de injeção de SQL (SQL Injection) – esses ataques ocorrem quando uma pessoa mal intencionada usa as entradas de usuário injetando, ao invés do conteúdo requerido, instruções SQL para manipular o retorno das informações.

SQL Injection

SQL Injection é uma das principais ameaças que encontramos em relação a ataques em banco de dados, o termo é muito popular principalmente entre programadores.

O SQL Injection é um ataque que visa enviar comandos nocivos à base de dados através de campos de formulários ou através de URLs. Um ataque bem-sucedido pode, por exemplo, apagar uma tabela do banco, deletar todos os dados da tabela ou até adquirir senhas que estejam cadastradas.

Veja abaixo um exemplo de vulnerabilidade em um sistema de login:

```
$usuario = $_POST['usuario'];
$senha = $_POST['senha'];
$sql = "SELECT * FROM usuarios WHERE usuario = '".$usuario."' AND senha =
'".$senha."' ";
$processa = mysql_query($sql);
```

Neste exemplo as variáveis $usuario e $senha recebem conteúdo vindo diretamente de um formulário através do método POST. Imagine que o conteúdo da variável $senha seja "'or 1='1". Se nenhuma validação for realizada, o usuário mal-intencionado terá efetuado login no sistema sem ao menos ter especificado um cadastro válido, devido a uma falha gerada na instrução SQL.

Analisemos outro exemplo de vulnerabilidade. Muitos sites utilizam sistemas via Z

```
if (isset($_GET['pagina'])) {
// Pega o valor da variável $_GET['pagina']
$arquivo = $_GET['pagina'];
} else {
// Se não existir variável, define um valor padrão
$arquivo = 'home.php';
}
include ($arquivo); // Inclui o arquivo
```

E na URL do site você poderia ter:

http://www.seusite.com.br/?pagina=contato.php

Com isso o "invasor" pode, por exemplo, colocar um caminho de um script externo no lugar da variável:

http://www.seusite.com.br/?pagina=http://malicioso.com/apaga-banco.php

O seu site incluiria o arquivo normalmente e executaria tudo que existe dentro dele e seu banco poderia ser completamente zerado. Para esse tipo de coisa existe apenas uma solução, validação. A validação pode ser feita de várias maneiras, até mesmo com funções nativas da linguagem.

Segurança

Os dados armazenados em Bancos de Dados precisam ser protegidos contra acessos não-autorizados, destruição ou alteração intencional e introdução acidental de inconsistências.

Existem alguns aspectos a serem considerados sobre segurança:

- Aspectos legais, sociais e éticos (exemplo: a pessoa que faz a solicitação referente ao crédito de um cliente tem direito legal em relação à informação?)
- Controles físicos (a sala com os servidores deve ficar trancada ou protegida fisicamente de alguma outra maneira?)
- Questões políticas (como decidir quem tem acesso a que dentro do BD?)
- Problemas operacionais (na adoção de um sistema de senhas, como as senhas são mantidas?)
- Controle de hardware (existem chaves de proteção?)
- Segurança do sistema operacional (qual a política de armazenamento e estrutura de arquivos do sistema?)

O mau uso do Banco de dados pode ser considerado como **intencional** ou **acidental**. A perda acidental pode resultar de:

- Quebras durante o processamento de transações;
- Anomalias causadas por acesso concorrente aos dados;
- Anomalias causadas por distribuição do banco de dados.

É mais fácil proteger o sistema contra perdas acidentais do que contra acessos maldosos ao Banco de dados. Entre as formas de acesso maldoso estão:

- Leitura não autorizada de dados (roubo de informações);
- Modificação não autorizada de dados;
- Destruição não autorizada de dados;
- Inserção não autorizada de dados.

A proteção do Banco de Dados contra acesso insidioso é impossível, mas o custo para o criminoso pode ser suficientemente alto para prevenir muitas, se não todas, tentativas de acesso ao Banco de Dados sem autorização.

A segurança de banco de dados, geralmente, diz respeito à segurança contra acessos maldosos, enquanto a integridade se refere ao fato de evitar a perda acidental da consistência. Com a finalidade de proteger o BD, medidas de segurança devem ser tomadas em diversos níveis:

- **Físico** – o sistema de computador deve ser fisicamente seguro contra entradas clandestinas de intrusos;
- **Humano** – os usuários devem ser cuidadosamente autorizados, para reduzir a chance de qualquer fornecimento de acesso a um intruso em troca de suborno ou favores;
- **Sistema operacional** – independente da segurança do SGBD, a debilidade na segurança do SO pode servir como um meio de acesso não-autorizado ao banco de dados;
- **Sistema de BD** – alguns usuários de sistemas de BD podem ter autorização de acesso somente a uma porção limitada do BD. Outros usuários podem estar habilitados a emitir consultas, mas podem ser proibidos de modificar dados;

Deve ser dedicado um esforço considerável para preservar a integridade e a segurança de um banco de dados. Os dados pertencentes a uma organização podem interessar a seus competidores, e a perda destes dados por fraude ou acidente pode representar prejuízo para uma organização.

CONCLUSÃO

Dados atualmente, na era do conhecimento, é valioso tanto para empresas quanto para pessoas comuns. A era do conhecimento persiste na informatização de dados que vão desde dados simples como nome, sexo, etc; à dados sigilosos como documentos pessoais, contas bancarias, etc.

Com essa massiva quantidade de dados espalhados e pela tecnologia atual, é impossível que algo seja 100% seguro. Esse artigo permitiu entender quais são os principais problemas de segurança e entender como funcionam, para que haja um esforço mínimo no desenvolvimento de aplicações com segurança.

REFERÊNCIAS

ROZA, Marcelo P. da. **Segurança em Banco de Dados**. Disponível em: <http://www.profs.iffca.edu.br/~mroza/Arquivos/bdii/segura/segurana_em_banco_de_dados.html>. Acesso em: 18 de agosto de 2014.

PHP BRASIL. **Anti SQL Injection**. Disponível em: <http://phpbrasil.com/artigo/3hsYE3jlum-K/anti-sql-injection>. Acesso em: 18 de agosto de 2014.

MICROSOFT. **Ameaças e Contramedidas de Segurança na Web**. Disponível em: < http://technet.microsoft.com/pt-br/library/dd569900.aspx>. Acesso em: 18 de agosto de 2014.

ALVES, René Araújo. **Um estudo sobre segurança em banco de dados móveis**. Recife, 2007. Disponível em: <http://www.cin.ufpe.br/~tg/2006-2/raa2.pdf>. Acesso em: 18 de agosto de 2014.

DANTAS, Felipe. **Segurança da Informação**. Disponível em: <http://www.cgu.gov.br/eventos/Ouvidoria_aperfeicoamento_RN/Arquivos/SegurancaInformacao_FelipeDantas.pdf>. Acesso em: 18 de agosto de 2014.