

SEGURANÇA EM BANCO DE DADOS: CONCEITOS E APLICAÇÕES

Fábio Crepaldi MARTINS¹
Eli CANDIDO JUNIOR²

RESUMO: Um banco de dados deve ser seguro e confiável. Proteger e garantir a segurança de uma base de dados é umas das principais tarefas de um administrador de banco de dados (DBA). Esse artigo apresenta os principais conceitos referente a segurança e algumas soluções para possíveis problemas que possam ocorrer no dia-a-dia de quem atua nessa área de Tecnologia da Informação.

Palavras-chave: segurança em banco de dados; privilégios; backup.

1 INTRODUÇÃO

O artigo abordará segurança em banco de dados, informando os principais conceitos que envolvem o assunto. No texto será abordado alguns tipos de segurança que existem atualmente, e também uma solução para um problema corrente que são as injeções de SQL.

Relataremos o tema sobre contas de usuários, as concessões de privilégios e revogações dos mesmos, feitas pelo DBA (administrador de banco de dados) responsável por toda a segurança e confiabilidade do sistema de dados.

Haverá um tópico falando sobre o controle de acesso baseado em papéis e para sites e-commerce. A criptografia, uma boa alternativa para a proteção de dados e para a manutenção do sigilo da informação. E por fim, a importância de se fazer o backup do banco de dados.

¹Discente do 4º ano do curso de Bacharelado em Sistemas de Informação do Centro Universitário “Antônio Eufrásio de Toledo” de Presidente Prudente. fabiocrepaldi@toledoprudente.edu.br.

² Docente do curso de Sistemas de Informação do Centro Universitário “Antonio Eufrásio de Toledo” de Presidente Prudente. eli@toledoprudente.edu.br. Orientador do trabalho.

O principal objetivo deste artigo é abranger o conhecimento em segurança de banco de dados, um ponto de grande importância para qualquer empresa que deseja manter a integridade, a disponibilidade e a confidencialidade de seus dados, já que é o alicerce para crescer no mercado que está cada vez mais competitivo.

A escolha por esse tema foi justamente pela identificação com essa área relacionada a banco de dados, na qual desejo expandir meus conhecimentos.

Os procedimentos utilizados foram pesquisas realizadas em livros e internet, especificamente relacionadas à segurança, com a ajuda do meu orientador que me disponibilizou alguns materiais, além da orientação.

O artigo está dividido em seis (6) capítulos principais. O primeiro descreve o objetivo, os procedimentos e a estrutura do texto. Já os demais, relatam o assunto em si, informando os conceitos teóricos sobre o assunto e algumas práticas que podem ser adotadas pelos leitores interessados.

2 SEGURANÇA EM BANCO DE DADOS

Nos tópicos a seguir será relatado seguranças em banco de dados, que está dividido em um tópico principal e mais três (3) subtópicos.

2.1 Os princípios da segurança da informação

Abaixo segue os três (3) princípios da segurança da informação, explicando assim seus conceitos correspondentes.

2.1.1 Controle de redundância

A redundância é caracterizada por conter uma informação de forma duplicada. O controle de redundância por sua vez, não permite inserir dois registros com a mesma chave primária ou excluir algum registro que esteja relacionado com outras tabelas, para que assim não haja inconsistência de dados. Mas para isso, o SGBD (Sistema Gerenciador de Banco de Dados) deve oferecer este recurso.

2.1.2 Controle de concorrência

Quando transações SQL são executadas concorrentemente, ou seja, ao mesmo tempo, pode se haver uma violação na consistência da base de dados, mesmo que cada operação tenha sido feita individualmente correta.

Hoje, os sistemas desenvolvidos utilizam-se da multiprogramação “que permite a execução de transações visando o compartilhamento do processador” (AZEVEDO, CASTRO e SERRÃO, s.d., s.p.). Por isso, existe a necessidade de controlar a interação dessas transações, através do controle de concorrência, por meio de mecanismos especializados.

2.1.3 Restrições de integridade

As restrições de integridade servem exatamente para evitar danos acidentais em um Banco de Dados, garantindo assim que alterações realizadas por usuários autorizados não resultem na inconsistência de dados.

Outra utilização é assegurar que um valor que está em uma relação de um conjunto de atributos também esteja para certo conjunto de atributos em outra relação.

2.2 Tipos de segurança

A segurança em banco de dados refere-se a um assunto bem extenso, que envolve algumas questões:

- ❖ Questões legais e éticas referentes ao acesso a certas informações, em que são classificadas como privadas, e só podem ser acessadas por pessoas autorizadas.
- ❖ Questões do sistema, por exemplo, se as funções de segurança devem ser implementadas no nível de *hardware*, nível de sistema ou no nível de SGBD. Onde existem também classificações da importância dos dados - altamente secreto, secreto, não secreto.

Existem ameaças aos bancos de dados que resultam na perda dos seguintes itens: integridade, disponibilidade e confiabilidade.

No entendimento de Elmasri e Navathe (2006) a integridade do banco refere-se à exigência que a informação esteja assegurada de modificações impróprias, incluindo a criação, a inclusão, a alteração e a exclusão. Caso ocorra a perda da integridade dos dados e não for corrigida, podem causar imprecisão, acarretando em tomadas de decisões equivocadas.

A disponibilidade dos dados é essencial, pois se encarrega de tornar os objetos sempre disponíveis para o usuário ou para o *software* que tenha direito de acesso a eles.

Já a confiabilidade está ligada à proteção dos dados, algo importantíssimo, já que a exposição de certas informações pode ter como consequências o constrangimento dos envolvidos, a perda da confiança ou numa ação contra a instituição.

Neste contexto, para proteger o banco de dados contra essas ameaças, o SGBD deve oferecer mecanismos que restrinja certos usuários ou grupos de acessarem partes específicas de um banco de dados. Tudo isso é de grande importância quando se refere a um grande volume de dados acessados

por muitos usuários diferentes de uma organização. Atualmente são utilizados dois tipos de mecanismos de segurança, são eles:

- ❖ Mecanismos de acesso discricionário: utilizados para conceder privilégios a usuários (leitura, inclusão, exclusão e atualização).
- ❖ Mecanismos de acesso obrigatório: implementados para estabelecer níveis de acesso classificando os dados e os usuários, baseando-se no conceito de papéis e conforme as políticas de segurança da empresa.

2.3 A segurança e o DBA

O administrador de banco de dados (DBA) é a autoridade máxima, onde suas funções são incluir concessão de privilégios, classificação de usuários e dados de acordo com as políticas de acesso da empresa.

Também conhecido como superusuário, o DBA concede e revoga privilégios a usuários específicos e/ou a grupos de usuários, digitando comandos para as seguintes situações:

- ❖ Criação de contas: cria contas para novos usuários ou grupos para assim habilitar o acesso ao banco.
- ❖ Concessão de privilégios: é a ação em que se concedem novos privilégios a determinadas contas.
- ❖ Revogação de privilégios: consiste em cancelar certos privilégios antes concedidos a algumas contas.

Dessa forma, o DBA é o responsável por garantir que os dados estejam seguros de qualquer ameaça externa.

2.4 Contas de Usuário

As contas de usuário são criadas pelo DBA, para que uma pessoa ou grupo possa ter acesso ao banco de dados, mas só serão criadas caso seja

realmente necessário. Desta maneira, o usuário recebe um *log in* e senha que serão utilizadas para a realização do acesso.

Para se manter as informações dos usuários no banco de dados segundo Elmasri e Navathe (2006, p. 529):

Não há dificuldades em manter informações dos usuários do banco de dados e de suas contas e senhas por meio da criação de uma tabela ou um arquivo cifrado com os dois campos NumeroDeConta e Senha(...) Sempre que uma nova conta for criada, um novo registro é incluído na tabela. Quando uma conta for cancelada, o registro correspondente deve ser excluído da tabela.

O sistema também deve manter todas as operações realizadas pelo usuário desde a sua entrada (*log in*) até a sua saída (*log off*), mantendo assim todas as interações feitas durante a conexão.

2.5 Injeção de SQL

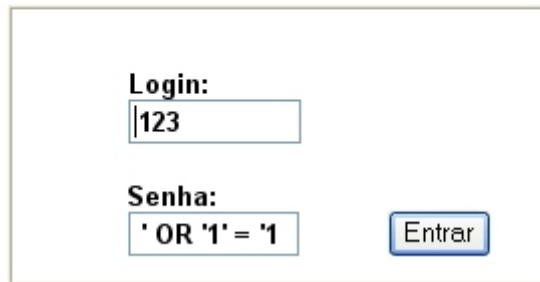
Em um sistema onde há o armazenamento das informações em um banco de dados e uma interação com o usuário via Web, existe a possibilidade da injeção de SQL (*SQL Injection*). Este ataque é basicamente a execução de comandos SQL, tanto DML (*select*, *insert*, *update* e *delete*) quanto DDL (*create*, *drop* e *alter*). Os autores FILHO, CAVALCANTI e FILHO (s.d.; s.p.) afirmam:

Estes comandos são executados através das entradas de formulários web, ou seja, no local destinado para digitação de informações pelo usuário, onde são passados comandos SQL, que por falhas nas aplicações acabam por resultar em alterações no banco de dados ou no acesso indevido à aplicação.

A figura a seguir mostra um exemplo prático de um tipo de ataque que pode ser feito por *hackers*.

Figura 1: Exemplo de injeção SQL.

Autenticação



The image shows a login form with two input fields and a button. The first field is labeled 'Login:' and contains the text '123'. The second field is labeled 'Senha:' and contains the SQL injection payload '' OR '1' = '1'. To the right of the password field is a button labeled 'Entrar'.

FONTE: (FILHO, CAVALCANTI e FILHO, s.d.; s.p.).

Um usuário comum normalmente iria digitar seu *login* e senha, o que faria com que a aplicação verificasse os mesmos na base de dados. Mas como podemos ver, foi digitado um comando SQL no campo senha, no que resulta na seguinte instrução:

```
SELECT * FROM tabela_usuarios WHERE login = '123' AND senha = ' ' OR '1' = '1'
```

Podemos observar que esta instrução independente do que for digitado no campo *login* e senha, a condição sempre será verdadeira, acarretando na entrada indesejada de um usuário que não contém permissão de acesso ao sistema.

Este fato pode ser algo muito perigoso em se tratando de vulnerabilidade dos dados, já que o usuário pode executar vários outros comandos, como de exclusão ou alteração de tabelas, podendo causar danos irreversíveis ao sistema, havendo assim uma inconsistência ou perda de dados valiosos.

2.5.1 Impossibilitando a injeção SQL

A melhor alternativa para impossibilitar a injeção SQL, é a validação de todas as entradas. Com este pensamento ou autores relatam que “Todos os valores originados da coleta de dados externos devem ser validados e tratados a

fim de impedir a execução de eventuais instruções destrutivas ou operações que não sejam as esperadas” (FILHO, CAVALCANTI e FILHO, s.d.; s.p.). Desta forma, tomando todas as medidas de precaução, dificilmente seu sistema sofrerá um ataque deste tipo.

3 PRIVILÉGIOS

Com o intuito de controlar a concessão e revogação dos privilégios, o SGBD por padrão atribui uma conta de proprietário, a conta que justamente estava sendo utilizada para a criação do novo SCHEMA de banco de dados. Dessa maneira, o proprietário recebe todos os privilégios sobre aquela relação.

Alguns comandos utilizados nas concessões segundo ROCHA (s.d; p. 3) são:

Para conceder privilégios a usuários e grupos, utiliza-se o comando GRANT. Qualquer privilégio concedido pelo comando GRANT é adicionado aos já concedidos, se existirem(...) A palavra chave PUBLIC indica que os privilégios devem ser concedidos para todos os usuários, inclusive aos que vierem a ser criados posteriormente(...) Se for especificado WITH GRANT OPTION quem receber o privilégio poderá, por sua vez, conceder o privilégio a terceiros.

Os privilégios concedidos ao um usuário ou a um grupo nada mais são que permissões de acesso a determinadas tabelas, podendo assim realizar vários tipos de permissões: “SELECT, INSERT, UPDATE, DELETE, RULE, REFERENCES, TRIGGER, CREATE, TEMPORARY, EXECUTE e USAGE” (ROCHA, s.d; p. 3).

Segue abaixo exemplos de comandos na concessão de privilégios. Supondo que a CONTA1 deseja conceder a CONTA2 o privilégio de inserir dados na tabela USUARIO:

```
GRANT INSERT ON USUARIO TO CONTA2;
```


Para que a CONTA1 possa conceder privilégios a outras contas ela precisa necessariamente possuir o GRANT OPTION, o que lhe permiti realizar esse tipo de operação.

Agora imagine que CONTA1 deseja permitir a CONTA3 que recupere e atualize a tabela e que seja capaz de propagar o privilégio SELECT e UPDATE. Seria assim o comando:

```
GRANT SELECT, UPDATE ON PRODUTOS TO CONTA3 WITH  
GRANT OPTION;
```

Nos próximos tópicos serão abordados mais detalhes sobre o assunto, fornecendo mais alguns exemplos.

3.1 Privilégios usando Visões

As visões (*views*) é um ótimo mecanismo para se restringir a visualização de determinadas colunas, que supostamente contenham conteúdos sigilosos, por algum ou vários usuários.

Por exemplo, se o proprietário da relação quiser que determinado usuário só tenha acesso a apenas alguns campos de uma tabela, então a utilização neste caso, consiste na criação de uma visão que inclua somente aquelas tuplas (colunas).

3.2 Revogação de Privilégios

Em determinados momentos, é interessante conceder um privilégio a um usuário e posteriormente revogar o mesmo. Com este pensamento ELMASRI e NAVATHE (2006, p.531) exemplificam que:

O proprietário de uma relação pode querer conceder o privilégio SELECT a um usuário para uma tarefa específica e depois revogar aquele privilégio quando a tarefa estiver completada(...) Por isso, é necessário um mecanismo para a revogação de privilégios.

Na linguagem SQL o comando REVOKE serve para exatamente revogar privilégios. A seguir, veja um exemplo:

```
REVOKE SELECT ON PESSOAS FROM CONTA5;
```

Neste caso, o DBA revogou do usuário CONTA5 o privilégio SELECT sobre a tabela PESSOAS. Dessa maneira, este seu privilégio foi revogado.

5 CONTROLE DE FLUXO

O controle de fluxo controla o fluxo das informações entre objetos. Conforme afirmaram ELMASRI e NAVATHE (2006, p. 538), “os controles de fluxo verificam se informações contidas em alguns objetos não fluem explicita ou implicitamente para objetos de menor proteção”.

Uma política de fluxo mais simples utiliza-se de duas classificações para as informações: confidencial (C) e não confidencial (NC). Esse método na maioria das situações resolve o problema, por exemplo, de quando se contém dados dos clientes, onde alguns deles são de caráter sigiloso.

Segundo ELMASRI e NAVATHE (2006), as técnicas de controle de fluxo devem garantir que só fluxos autorizados, explícitos e implícitos, sejam executados.

5.1 Canais secretos

Um canal secreto seria a permissão de uma transação de dados que infrinja as regras de segurança. Então, ele permite que uma informação de nível alto passe para um nível mais baixo, de maneira ilegal.

Especialistas dizem que a melhor forma de se evitar essa prática é bloquear o acesso dos programadores a informações pessoais de clientes, como salário ou saldo bancário, por exemplo.

6 CRIPTOGRAFIA

A criptografia é uma das melhores soluções para se armazenar ou transferir dados, suponha que alguma informação caia em mãos erradas, se ela estiver cifrada, ou seja, que tenha sido usado um algoritmo de criptografia, a pessoa que a obteve terá dificuldades em conseguir encontrar o significado real, pois a criptografia mascara a informação trocando os caracteres por outros, disfarçando o sentido das palavras.

7 A IMPORTÂNCIA DE BACKUPS

O backup de dados é algo de extrema importância, até porque imagine o tamanho do transtorno caso uma empresa perca os seus dados, o que pode ocorrer por diversos motivos, queda de energia, vírus no servidor, falha humana, entre outros.

Uma das soluções é o uso de mídias ópticas (CD ou DVD) ou de um HD externo. Você pode criar rotinas diárias ou semanais, para a cópia de arquivos do seu servidor ou computador.

Existe outra bem utilizada que o uso de servidores espelhados, onde eles trabalham ao mesmo tempo. “Os HDs são configurados para serem “espelhos” um do outro, ou seja, os arquivos gerados no HD principal são automaticamente gravados nos demais HDs espelhados” (A IMPORTÂNCIA de backup, s.d; s.p.). Assim, se ocorrer do servidor principal falhar por algum motivo, o servidor secundário passa a ser o primário.

A alternativa mais recente é a utilização da computação nas nuvens, *cloud computing*, os arquivos ficam armazenados em servidores por todo o mundo, assim podem ser acessados de qualquer lugar que tenha Internet.

8 CONCLUSÃO

A área de banco de dados está sempre em alta, por ser a base de qualquer aplicação seja ela desktop ou web. A proteção dos dados de uma empresa é um assunto de grande importância, pois pode estar ali o diferencial para os concorrentes. Para vencer no mundo dos negócios é preciso ter a informação como estratégia de competitividade.

Assim, observamos que os dados são muito valiosos, por isso todas essas práticas são válidas, é que boa parte delas devem ser implementadas em um bom sistema de segurança de dados, para assim garantir a integridade, a disponibilidade e a confidencialidade de seus dados.

9 REFERÊNCIAS BIBLIOGRÁFICAS

A IMPORTÂNCIA de backup. s.d Disponível em: <<http://www.consuldatasistemas.com/novidades/a-importancia-do-backup>> acesso em: 15 abr. 2014.

AZEVEDO, Arthur Henrique; CASTRO, Edkarla Andrade de; SERRÃO, Paulo Roberto de Lima. **Segurança em banco de dados**, s.d. Disponível em: <<http://pt.slideshare.net/artinfo/segurana-em-banco-de-dados>> acesso em: 15 abr. 2014.

CRIOGRAFIA, s.d Disponível em: <<http://cartilha.cert.br/criptografia/>> acesso em: 16 abr. 2014.

ELMASRI, Ramez; NAVATHE, Shamkant B. **Sistemas de banco de dados**. 4 ed. São Paulo: Pearson Addison Wesley, 2006. 527p.

FILHO, Clóvis Luiz de Amorim; CAVALCANTI, Paulo Diego de Oliveira Bezerra e FILHO, Marcello Benigno de Barros Borges, **SQL Injection em ambientes Web**. Disponível em: < <http://www.devmedia.com.br/sql-injection-em-ambientes-web/9733#ixzz32CidD8Xc> > acesso em: 19 maio 2014.

HOTEK, Mike. **SQL Server 2008: passo a passo**. Porto Alegre: Bookman, 2010. 287 p.

MACÊDO, Diego. **Conceitos sobre Segurança em Banco de Dados**, 2011. Disponível em: <<http://www.diegomacedo.com.br/conceitos-sobre-seguranca-em-banco-de-dados/>> acesso em: 14 abr. 2014.

MEDEIROS, Marcelo. **Banco de dados para sistemas de informação**. Florianópolis: Visual Books, 2006. 116 p.

Ribeiro, Leandro, **A importância do Backup na administração de sistemas**. 2009. Disponível em: < <http://imasters.com.br/artigo/11174/linux/a-importancia-do-backup-na-administracao-de-sistemas/> > acesso em: 16 abr. 2014.

ROCHA, Luciano Roberto, **Concessão e revogação de Privilégios**. Disponível em: <[http://www.lrocha.com.br/arquivos/arquivos/BdWeb%20\(PostgreSQL\)/AULAS/bd_web_A9.pdf](http://www.lrocha.com.br/arquivos/arquivos/BdWeb%20(PostgreSQL)/AULAS/bd_web_A9.pdf)> acesso em: 15 abr. 2014.

VITOR, Joaquim & MORAES, Márcio Lucena & COSTA, Rafaello. **Visão geral de Segurança em Bancos de Dados**, s.d. Disponível em: <http://www.lyfreitas.com.br/ant/artigos_mba/artbancodedados.pdf> acesso em: 14 abr. 2014.