INTERCLASSE
WELLITON SOUSA DA CUNHA

SEGURANÇA EM BANCO DE DADOS: MÉTODOS DE PREVENÇÃO CONTRA POSSÍVEIS FALHAS E ATAQUES.

IMPERATRIZ – MA
2018

INTERCLASSE
WELLITON SOUSA DA CUNHA

SEGURANÇA EM BANCO DE DADOS: MÉTODOS DE PREVENÇÃO CONTRA POSSÍVEIS FALHAS E ATAQUES.

Trabalho de Conclusão de Curso – Artigo Cientifico, apresentado ao núcleo de Trabalhos de Conclusão de Curso do Curso de Pós-Graduação Lato Senso do Curso de Especialização em Banco de Dados, como requisito obrigatório para obtenção do grau de especialista.

IMPERATRIZ – MA
2018

SEGURANÇA EM BANCO DE DADOS: MÉTODOS DE PREVENÇÃO CONTRA POSSÍVEIS FALHAS E ATAQUES.

WELLITON SOUSA DA CUNHA.

RESUMO

Informação é o bem mais precioso para uma empresa, contudo, muitos dos empresários não dão a total importância que a merece, assim muitos dos dados estão sem segurança, podendo ocorrer perdas gravíssimas para as empresas, sem nenhuma política de segurança para recuperar ou assegurar que essas informações não serão extraviadas. Com isso, abre-se um desafio enorme para o especialista em banco de dados, manter essas informações, ter a total segurança que esses dados não serão perdidos ou roubados. O estudo demonstra quais os principais ataques não autorizados e maneiras para se proteger, tendo como base os três pilares da segurança da informação: Confidencialidade, Integridade, Disponibilidade.

Palavras Chaves: **Segurança da Informação**. **Política de Segurança. Confidencialidade**. **Integridade. Disponibilidade**.

1. INTRODUÇÃO

Segurança da informação é um dos temas mais importantes para uma organização, seja ela empresarial ou não, isso se deu pelo fato de recentemente muitas empresas terem seus dados roubados por crackers, que transformaram essas falhas em oportunidades ilegais para cometerem crimes virtuais. A informação para ser armazenado, precisa ter uma estrutura que garantam que esses dados serão mantidos e recuperados no momento certo pela pessoa autorizada, sem compromete-la. Os especialistas em segurança da informação estão tendo uma nova perspectiva para as empresas, devido as grandes perdas de dados que ocorreram nos últimos anos. Com isso, os profissionais desta área precisam estar atentos aos três pilares que sustentam a tecnologia da informação e moderar a ocorrências desses cenários, e agir de forma concisa contra invasões não autorizados.

Nesse seguimento de banco de dados existem vários *SGDBs*[1], métodos injection que o profissional especialista precisa saber, está a todo momento pesquisando, obtendo informações sobre temas novos envolvendo essas características, e criando possibilidades para tornar o ambiente coorporativo mais seguro, não é uma tarefa fácil, pois a tecnologia evolui de forma rápida, os crackers estão a todo momento criando novos métodos, e os especialistas precisam montar estratégias, políticas de segurança, ferramentas capazes de proteger as informações de pessoas não autorizadas.

Esse artigo tem como objetivos esclarecer algumas perguntas, como por exemplo: como proteger seus dados a partir dos três pilares da segurança da informação? Quais as principais causas de ataques em banco de dados?

Em pleno século XXI, as empresas, instituições, escolas, faculdades, bancos, todo e qualquer empreendimento seja de grande porte ou não, tem um banco de dados, seja qual forma de armazenamento for, contendo ali informações importantes, que muitos deles se forem perdidas pode causar o fim, por isso abre-se um tema para ser estudado, visando destacar as melhores práticas para proteger suas informações, criando políticas de segurança da informação que garantam que os processos internos fluam corretamente.

METODOLOGIA

Este artigo foi desenvolvido mediante uma abordagem metodológica da pesquisa bibliográfica, foi elaborado uma análise de fontes secundárias, com objetivo de reunir e analisar as informações e dados que serviram como base para construção da investigação do tema proposto.

[1]Sistema Gerenciador de Banco de Dados.

2. BANCO DE DADOS

(OLIVEIRA, 2012) Destaca em um conjunto coerente e lógico de dados relacionados que representa aspectos do mundo real, que podem ser mantidos ou recuperados para atender requisitos solicitados.

Os bancos de dados são de grande importância para as empresas, pois neles são armazenados vários tipos de informações, como: números, textos, imagens, entre outros. As informações que estão contidas no banco são refletidas nas situações que acontecem no mundo real e vise vessa.

Segundo (NAVATHE, 2005) os bancos de dados são divididos basicamente em duas categorias: relacionais e não relacionais. Os relacionais são fundamentais nos paradigmas de orientação a conjuntos, também chamado de tabelas, que podem ser compostas de linhas e colunas. Sua linguagem é SQL (Structured Query Language) ou linguagem de pesquisa estruturada. Já os não relacionais foram criadas nas situações que os banco de dados relacionais não atendem de forma satisfatória, como por exemplo: trabalhar com dados mistos, imagens e tabelas ou trabalhar com uma quantidade de dados enormes sem perder a performance da aplicação. Com isso surge os bancos de dados chamados NoSQL (Not Only SQL).

1.1. SQL

(OLIVEIRA, 2012) define em um conjunto de comandos para manipulação de banco de dados utilizado com um objetivo de estruturar a arquitetura do banco ou incluir, excluir, modificar e pesquisar informação que possa estar contida nela.

A linguagem SQL não é uma linguagem de programação autônoma, logo quando se desenvolver uma aplicação, necessita-se de uma linguagem de programação, seja ela: Java, C, Python, C#, entre outras. Para embutir comandos SQL e depois manipula-los.

A linguagem SQL é dividida em algumas categorias que podem ser facilmente manipulados por intermédio de alguns comandos, que são classificadas como:

- DDL – Linguagem de Definição de Dados, permite criar, excluir e alterar tabelas, índices etc.
- DML – Linguagem de Manipulação de Dados, permite a manipulação de dados, como: inserir, deletar e atualizar.
- DQL – Linguagem de Pesquisa de Dados, permite obter informações a partir de uma busca.
- DCL – Linguagem de Controle de Dados, controla a segurança interna do banco de dados, como: criar usuários, estabelecer permissões, criptografia de dados.

1.2. GERENCIADOR DE BANCO DE DADOS

Segundo (MIYAGUSKU, 2008), são aplicativos com recursos e funcionalidades capazes de organizar, gerenciar todos os elementos dos bancos de dados, como: criar a estrutura do banco, armazenas as informações, consultas, entre outros. Utilizando a linguagem SQL para manipulação dos elementos.

DBMS (Database Management System), também conhecido no português como SGDB (Sistema Gerenciador de Banco de Dados), destaque-se por terem suas características em:

- *Controle de Redundância:* Estabelecendo assim um modelo para controlar os elementos repetidos, mantendo o mínimo possível de redundância para conter a estabilidade do modelo.
- *Compartilhamento de dados:* Os dados devem estar disponíveis para os usuários a quem a política de segurança assegurar.
- *Controle de Acesso:* É o monitoramento de quem pode realizar funções no banco de dados.
- *Esquematização:* Os elementos do banco de dados devem estar na mesma estrutura do banco para garantir o entendimento da aplicação e do modelo.
- *Backup:* É uma cópia de segurança que aplicação deve disponibilizar rotinas especifica ou não para realizar a cópia de segurança dos dados armazenados.

A segurança é um fator primordial e faz a maior diferença em escolher um SGDB para manipular os dados. A linguagem SQL para acesso e manipulação dos dados na maioria das vezes é a mesma, agora no controle de acesso as informações, podem ser diferentes de uma aplicação para outra. Os gerenciadores de banco de dados precisam estabelecer estratégias para prever o controle de acesso de forma íntegra e rápida sem que as informações sejam perdidas.

Um dos principais sistemas de gerenciador de banco de dados hoje no mercado segundo a (RANKING, 2018)[2] podem ser destacados segundo as suas popularidades como:

1. Oracle
2. MySQL
3. Microsoft SQL Server
4. PostgreSQL
5. MongoDB
6. DB2
7. Redis
8. Elasticsearch
9. Microsoft Access
10. Cassandra
11. SQLite
12. Teradata

[2] É uma Base de Conhecimentos de Sistemas de Gerenciamento de Banco de Dados Relacional e NoSQL.

2. SEGURANÇA EM BANCO DE DADOS

Um dos fatores primordiais que fazem diferenciar um banco de dados para outro é a segurança, é como as informações serão disponibilizada, quem tem acesso para manipular os dados , cada banco de dados tem sua estrutura, cabe o especialista em banco de dados montar uma estratégia para monitorar essas transações, criar políticas de prevenção com o objetivo de proteger os dados de possíveis furtos ou perdas.

Falar em segurança da informação já vem na mente os princípios básicos que assegura os dados, ainda podem ser destacados como os três pilares da segurança da informação:

- **Confidencialidade**

  Garante que a informação seja acessível apenas pela pessoa autorizada. Dos três pilares esse pode ser o mais significante, muitas empresas investem caro para proteger suas informações de pessoas mal-intencionada, o proprietário intelectual da informação fará de tudo para que seus dados não cheguem na vitrine dos concorrentes coorporativos.

- **Integridade**

  Garante que a informação armazenada esteja correta, e que seja alterada somente pela pessoa autorizada. Nas empresas, as informações são recuperas e inserida a todo momento, tanto o emissor quanto o receptor da informação, precisam interpretar da mesma maneira, se essa informação não for recuperada de forma inteira, isso pode comprometer a integridade da informação, requerendo um custo para corrigir os dados adulterados, de tempo, mão de obra, que podem ser convertidos em dinheiro, causando prejuízos irreparáveis, muitas das vezes ocasionando o fim das empresa.

- **Disponibilidade**

  Garante que as informações sejam obtidas pelas pessoas autorizadas, ou seja, que esteja disponível sempre a quem o detém. Isso pode envolver o método de busca, que muitas das vezes podem demorar, assim surge formas para criar estratégias de busca que atendam de forma mais eficiente.

2.1. INTEGRIDADE REFERENCIAL

Segundo (OLIVEIRA, 2012) é um método utilizado para manter a consistência dos dados, prevenindo a entrada de valores duplicados ou até mesmo fazer referência a uma chave inválida para uma entidade. Na construção do banco de dados fica claro a necessidade de se ter

um relacionamento de chave estrangeira que tenha o mesmo valor na outra entidade relacionada para que aquela entidade seja válida, e as informações não perca sua integridade.

É comum na maioria dos bancos de dados relacional que ao fazer uma inclusão ou exclusão em uma entidade que tem uma chave estrangeira ligada a uma entidade com chave primária, o código referente a chave deverá ser igual senão deverá ser gerado uma mensagem de erro, garantindo assim a consistência dos dados.

Há uma ligação de dependência da chave estrangeira com a chave primária, pois se houver uma necessidade para alterar ou excluir um valor que esteja ligado a outra tabela, nesta deverá ser modificada na tabela dependente. Se fosse permitido teríamos uma informação inválida, ocorreria um erro ao procurar as informações relacionadas.

Ao escolher um banco de dados é importante que considere essas características pois nem todos os bancos de dados disponibilizam desse recurso chamado de *CONSTRAINT*, que poderá fazer com que o especialista em banco de dados traçasse outros métodos para manter a consistência dos dados.

Existem alguns bancos de dados que disponibilizam até mesmo controle de alteração e exclusão em massa, gerando as modificações em toda a estrutura do banco, isso muitas das vezes podem ser muito perigosos, pois não exibe nenhuma mensagem explicativa ao usuário.

Ao desenvolver um programa, muitos dos programadores não utilizam desses recursos dos bancos de dados, deixando apenas os programas tomarem essas decisões de exclusão ou alteração dos dados sem contar com os relacionamentos de chave primária com estrangeira em banco de dados, colocando em risco as informações importantes do sistema. Poderia até mesmo o programa restringir algum acesso, mas todo e qualquer banco de dados existem outros programas que consegue manipular as informações de forma fácil, abrindo portas para pessoas mal-intencionada acessar informações privadas.

2.2. SEGURANÇA DE ACESSO

Em banco de dados os administradores têm se preocupado com a criação e manutenção d**e** ambientes seguros, criando políticas de acesso, meios pelo qual a informação será acessada, privilégios, pois boa parte dos ataques, roubos de informação são ocasionado por brechas deixadas por empresas, ainda também tendo participação de funcionários que conhecem o ambiente, facilitando a entrada de pessoas não autorizadas.

Na prática, todos os controles de acesso direto ao sistema de informação, precisam levar em conta que todas as entradas ao ambiente tenham um roteiro pré-definido, para que a política de segurança assegure que somente a pessoa autorizada acesse as informações contida, isso não garante que os dados não serão roubados, mas identifica quem exatamente acessou.

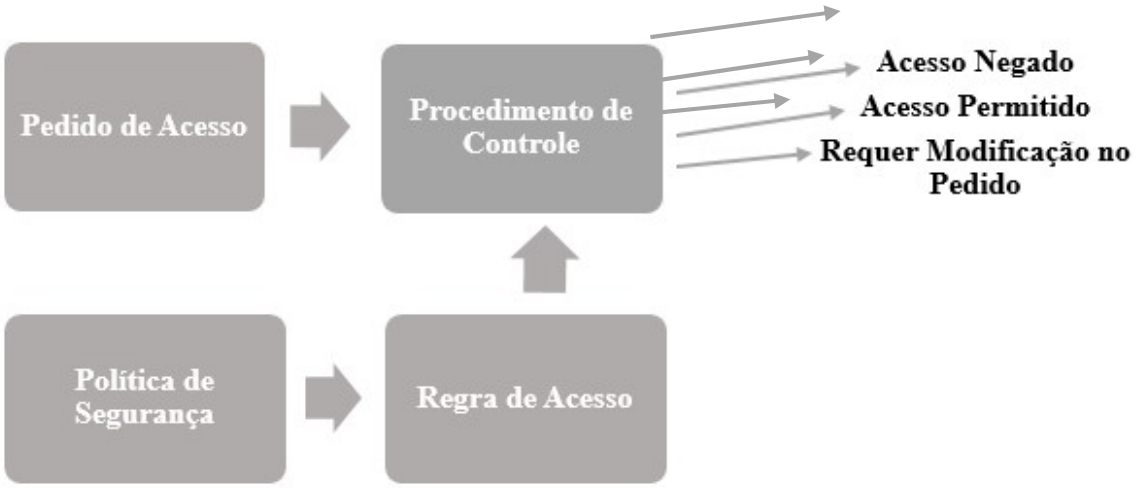

Figura 1 Representação de um Controle de Acesso.

Como mostra a figura 1 o controle de acesso pode ser dividido basicamente em dois componentes:

- Políticas de Segurança pode ser definida como modalidades de regras pré-definidas conforme as necessidades de segurança, com o objetivo de manter a confidencialidade.
- Procedimento de Controle é a interação entre os pedidos solicitados e as regras de acesso criado pelas políticas de segurança, nessa etapa é definida quem tem acesso permitido ou negado segundo seus privilégios armazenados.

Normalmente os controles de acesso são armazenados em uma tabela específica dos bancos de dados, chamadas de listas de controle de acesso (Access Control List, ACL), nelas estão contidos todos os privilégios que um usuário pode ter em um sistema. Essa tabela necessita ter uma atenção especial, pois se um usuário não autorizado conseguir acessar, pode alterar os privilégios ocasionando uma quebra de confidencialidade. Umas das formas para proteger a tabela contra possíveis alterações não autorizada é a criptografia de dados.

2.3. CRIPTOGRAFIA DE DADOS

Segundo (ELGSCREEN, 2018) criptografia de dados pode ser uma técnica ou estudo que tem como objetivo transformar uma informação em sua forma original para uma outra forma difícil de ser identificar. Ainda sobre criptografia de dados podem ser entendidas como um conjunto de informações que ao passar por um processo de codificação poderá ser lida apenas aquém tem a chave pra a decodificação.

A criptografia de dados pode ser dividida em duas áreas de conhecimentos que envolve como a chave de segurança será usada.

- Simétrica é quando o emissor e o receptor têm a mesma chave de segurança que serve para codificar e traduzir a informação.
- Assimétrica há duas chaves, uma pública que server para criptografar os dados, e uma privada que é utilizada para decodificar as informações.

A criptografia de dados é importante pois ela tem como objetivo garantir a segurança a privacidade, evitando que a informação chegue em mãos errada. Com a criptografia você poderá proteger dados sigilosos armazenados na base de dados.

Em banco de dados a criptografia poderá ser usada em várias partes do banco, principalmente em áreas que fornece privilégios para os usuários e também locais como usuários e senha.

Segundo (WYKES, 2016), ao projetar um banco de dados é necessário analisar qual o tipo de criptografia que será utilizada para proteger suas informações, para cada situação é aconselhado uma forma de proteção, nesse contexto serão destacados os principais:

Funções de Hash criptográfico:

- MD5
- SHA-256
- SHA-1
- RIPEMD-160
- TIGER

Sistemas Free/Open Source:

- PGP
- GPG
- SSL
- IPSec /Free S/WAN

Algoritmos Assimétricos (Chave Pública):

- Curvas elípticas
- Diffie-Hellman
- DAS de curvas elípticas
- EI Gamal
- RSA

Algoritmos Simétricos:

- Máquina Enigma
- DES
- RC4
- RC5
- Blowfish
- IDEA
- AES
- RC6

2.4. SQL INJECTION

É um tipo de ameaça de segurança que se prevalecer-se de falhas em sistemas que se interatua com a base de dados SQL. A injeção de Sql acontece quando o invasor executa comandos SQL dentro de uma consulta por intermédio de uma aplicação.

Para ilustrar como é feito a inserção de SQL injection será implementado um código de linguagem de programação PHP junto com instruções SQL.

```
1  <?php
2
3    $usuario = $_POST['usuario'];
4    $senha = $_POST['senha'];
5
6    $query_string ="SELECT * FROM usuarios
7                    WHERE codigo = '{$usuario}' AND senha = '{$senha}'";
8
9  ?>
10
```

Figura 2 Código php de autenticação.

A figura 2 mostra uma estrutura básica onde na linha 3 e 4 destaca as variáveis usuario e senha que receberá um valor correspondente do tipo POST, nesse contexto a falha já é notória, pois não existe nenhum tipo de tratamento, claro que esse exemplo é apenas uma ilustração, mas serve para entendermos como funciona, o que uma estrutura mal projetada pode ocasionar em um sistema.

Em uma página de login e senha, com essa estrutura mostrada na figura 2, uma pessoa mal-intencionada com conhecimentos de comandos SQL pode facilmente mudar o resultado da busca, como por exemplo:

Figura 3 Tela de Login

Nesse exemplo foi possível entrar no sistema sem pelo menos fornecer o nome do usuario, apenas inserindo comando sql no campo senha. Analisando o código sql, o comando busca todos os usuarios cadastrados na base de dados, na primeira condição o campo "código" é condição de igualdade a "*vazio*", que nesse caso é uma coluna da tabela "*usuarios"* onde fica armazenado o nome de cada usuário cadastrado. Na segunda comparação do campo "*senha"* fica acrescentado mais uma condição "*or*", que nesse exato momento onde a invasão acontece, pois, essa condição e satisfeita.

Uma das políticas de proteção contra-ataques de injeção sql será feita no servidor de banco de dados, outras devem ser tratadas no código fonte da aplicação. Devem garantir as restrições de cada usuário, privilégios segundo suas funções que irá realizar no sistema.

Todos os valores que serão capturados externamente terão que ser validados e tratados afim de proteger eventuais inserções destrutivas que comprometam a integridade dos dados. Em vários banco de dados já contam com essas medidas de segurança que tratam essas inserções de forma efetiva, outro fator também importante a ser destacado é a forma como os bancos de dados exibi suas mensagens de erro, pois muitos deles mostram caminhos de diretórios do sistema de arquivos e informações a respeito do esquema de banco de dados, abrindo brechas para uma possível visão de monitoramento dos dados.

2.5. AUDITORIA EM BANCO DE DADOS

É uma ação dos administradores de banco de dados, muitas das vezes solicitados por empresas que estão preocupados em saber o que os usuários estão fazendo, é uma política de segurança, ocorre para fins de segurança, garantindo que os usuários não autorizados não estão acessando uma parte do banco de dados ou uma estrutura dos dados que não é permitida. A maioria das informações cruciais estão contidas no banco de dados, por isso se faz necessário ter um maior cuidado com essas informações, garantir que somente a pessoa autorizada vai ter acesso.

Segundo (PRISCILA, 2018), as empresas podem fazer auditorias em banco de dados segundo suas metodologias, basicamente são classificados em duas partes:

- Metodologia Tradicional
- Exclusão de Riscos

Metodologia tradicional é uma conferência feita por intermédio de uma lista contendo todas as informações referentes a política de banco de dados no que se diz respeito ao acesso dos usuários, permissões, autorizações, prevenindo a ocorrências de falhas.

O checklist é feito com forma a utilização do banco de dados, na conferência são elaboradas algumas perguntas que precisarão ser respondidas, como por exemplo: Existe procedimento de backup ou restore? As responsabilidades da administração de banco de dados estão documentadas? Existe algum tipo de controle sobre as mudanças ocorridas base de dados? O desempenho do banco de dados é analisado? O sistema é monitorado? Existe algum tipo de histórico armazenado para análise? Essas informações deverão ser analisadas para manter a segurança e a consistência dos dados.

Exclusão de riscos é a parte onde identifica os riscos que podem ocorrer em uma base de dados, com o objetivo de elimina-las ou diminuir seus riscos. Analise é feito em toda sua estrutura contida no banco, privilégios dos usuários, percorrer até onde um usuário pode chegar com essa permissão concedida, traçar rotas com perfis diferentes procurando falhas que possa ocorrer. Toda a análise feita precisa ser documentada e protegida em local seguro, disponível apenas a quem tem direito.

3. CONCLUSÃO

Pelo estudo realizado, vimos que a segurança em banco de dados é de total importância, pois nelas onde fica armazenada a maior parte das informações de uma empresa, e necessita ter um cuidado especial. Para manter um banco de dados seguro não é fácil, precisa criar uma rigorosa lista de métodos e práticas para manter a integridade das informações.

O conceito aprendido sobre banco de dados é padrão para todos, o que pode mudar são algumas estruturas dos sistemas gerenciador de banco de dados, contudo um fator comum entre todos é a segurança. Toda política de segurança em banco de dados precisa levar em conta os três pilares que sustentam a segurança da informação, confidencialidade, integridade e disponibilidade.

A vulnerabilidade de uma estrutura de banco de dados pode ser estudada em auditoria em banco de dados, nelas ficam claras as possíveis brechas que podem ter, logo após a identificação das falhas, vêm as medidas que poderão ser tomadas, sempre em pró de manter as informações seguras.

REFERÊNCIAS

ELGSCREEN. (01 de 09 de 2018). *O que é criptrografia de dados?* Fonte: ELGSCREEN: blog.elgscreen.com

MIYAGUSKU, R. (2008). *Curso Prático de SQL / Renata Miyagusku.* São Paulo: Digerati Books.

NAVATHE, R. E. (2005). *Sistemas de Banco de Dados.* São Paulo: Pearson Addison Wesley.

OLIVEIRA, C. H. (2012). *SQL Curso Prático.* São Paulo: Novatec Editora Ltda.

PRISCILA. (02 de 09 de 2018). *Auditoria em Bancos de Dados Relacionais* . Fonte: DEVMEDIA: https://www.devmedia.com.br/auditoria-em-bancos-de-dados-relacionais/16016

RANKING, D.-E. (25 de Agosto de 2018). *DB-Engines Ranking*. Fonte: DB-ENGINES: https://db-engines.com/en/ranking

WYKES, S. M. (2016). *Criptografia Essencial - a Jornada do Criptógrafo.* Rio de Janeiro: Elsevier Editora LTDA.