FACULDADE DE ADMINISTRAÇÃO E NEGÓCIOS DE SERGIPE – FANESE

CURSO DE PÓS GRADUAÇÃO EM BANCO DE DADOS

ÂNGELO CÉSAR SANTOS DE CARVALHO

SEGURANÇA EM BANCO DE DADOS

Aracaju – SE

2016.1

ÂNGELO CÉSAR SANTOS DE CARVALHO

SEGURANÇA EM BANCO DE DADOS

Trabalho de Conclusão de Curso apresentado ao Núcleo de Pós-Graduação e Extensão – NPGE, da Faculdade de Administração de Negócios de Sergipe – FANESE, como requisito para a obtenção do título de Especialista em Banco de Dados.

_____

Nome completo do Avaliador

_____

Nome completo do Coordenador de Curso

_____

Nome completo do Aluno

Aprovado (a) com média: _____

Aracaju (SE), ____ de _____ de 2016.

SEGURANÇA EM BANCO DE DADOS

Ângelo César Santos de Carvalho

RESUMO

Este artigo apresenta uma visão geral sobre introdução a segurança em bancos de dados, adotando políticas, tecnologias e as melhores práticas que o administrador de banco de dados deve implementar para garantir um ambiente seguro. Para a efetivação da pesquisa científica utilizou-se de pesquisa qualitativa e bibliográfica para demonstrar a importância do tema. Constatamos que diariamente, são armazenadas e processados centenas de terabytes de informações em empresas de diversos segmentos do mercado corporativo, para garantir a disponibilidade, confiabilidade e segurança de tais informações, se faz necessário a utilização de um ou mais SGBDs. O papel do DBA é garantir que essas informações estejam seguras, integras e disponível o maior tempo possível, diante de tal responsabilidade, se faz necessário aplicar políticas e tecnologias de segurança garantindo a confidencialidade, integridade e disponibilidade de todos os bancos de dados da empresa.

Palavras-chave:

SGBD; DBA; Segurança.

1. INTRODUÇÃO

Em um mundo globalizado e competitivo, a tecnologia da informação tem proporcionado novos horizontes de trabalho, sendo um grande diferencial de competitividade, traçando estratégias visando a lucratividade e evitando perdas financeiras nas empresas.

Atualmente a tecnologia da informação pode ser encontrada nos mais diversos segmentos empresariais, desde empresas de pequeno porte até empresas multinacionais, sendo presente nas mais diversas formas como, computadores, sistemas, antivírus, firewall, banco de dados dentre outros ativos.

Os servidores de banco de dados são responsaveis pelo armazenamento e distribuição de informações em todos os sistemas informatizados, dos quais devem ser protegidos de roubos, desvios, exposições e perdas de informações.

O profissional de administração de banco de dados tem a obrigação de conhecer tecnicas, processos e melhores praticas em seguraça de banco de dados sob sua responsabilidade.

Este artigo apresenta uma visão geral sobre introdução a segurança em bancos de dados, adotando políticas, tecnologias e as melhores práticas que o administrador de banco de dados deve implementar para garantir um ambiente seguro.

Os procedimentos adotados neste artigo foram pesquisas na Internet relacionadas à segurança em servidores de banco de dados.

2 DESENVOLVIMENTO

2.1 Fundamentação Teórica

Segundo Elmasri e Navathe (2005), um SGBD é uma colecção de programas que permitem a criação, manipulação e manutenção de uma base de dados – BD. Ou seja, um SGBD é um software de propósito geral que facilita os processos de definição, construção, manipulação e partilha de bases de dados entre vários usuários e aplicações.

Seu principal objetivo é retirar da aplicação cliente a responsabilidade de gerenciar o acesso, a manipulação e a organização dos dados. O SGBD disponibiliza uma interface para que seus clientes possam incluir, alterar ou consultar dados previamente armazenados.

Em bancos de dados relacionais, a interface é constituída pelas APIs (*Application Programming Interface*) ou drivers do SGBD, que executam comandos na linguagem Structured Query Language.

Segundo DATE (2003, p. 10), Um banco de dados é uma coleção de dados persistentes, usada pelos sistemas de aplicação de uma determinada empresa.
São coleções organizadas de dados que se relacionam de forma a criar algum sentido (infomação) e dar mais eficiencia durante a pesquisa ou estudo.

Para (MACEDO,2016), Os bancos de dados são utilizados para armazenar diversos tipos de informações, desde dados sobre uma conta de e-mail até dados importantes da Receita Federal. A segurança do banco de dados herda as mesmas dificuldades que a segurança da informação enfrenta, que é garantir a integridade, a disponibilidade e a confidencialidade. Um Sistema gerenciador de banco de dados deve fornecer mecanismos que auxiliem nesta tarefa.

A segurança da informação é a proteção da informação quanto a varios tipos de ameaças, de modo a garantir a continuidade do negocio, minimizar o risco para o negocio, maximizar o retorno sobre o investimento e as opotunidades de negocio (Dantas, 2011).

Para Elmasri e Navathe (2005), DBA, é o responsável máximo pela gestão de recursos de uma BD; é o responsável pela autorização do acesso à base, pela coordenação e monitorização de seu uso e por adquirir recursos de software e hardware, conforme necessário. Este é responsável também, por questões de segurança (brechas) ou tempo de resposta do sistema. Em grandes organizações, o DBA possui um staff de assistentes que o auxiliam no desempenho de suas funções.

Os dados compreendem a classe mais baixa da informação. A informação propriamente dita são os dados que passam por algum tipo de processamento para serem utilizados de uma forma inteligível.

O conhecimento é a informação cuja relevância, confiabilidade e importância foram avaliadas, e é obtido pela interpretação e integração de vários dados e informações para iniciar a construção de uma situação.

A inteligência é a informação com oportunidade, ou seja, é a parte do conhecimento que habilita a tomada das melhores decisões (Cardoso Júnior, 2005).

De acordo com (MACEDO,2016), os mecanismos de segurança referem-se às regras impostas pelo subsistema de segurança do SGBD, que verifica todas as solicitações de acesso, comparando-as com as restrições de segurança armazenadas no catálogo do sistema. Entretanto existem brechas no sistema e ameaças externas que podem resultar em um servidor de banco de dados comprometido ou na possibilidade de destruição ou no roubo de dados confidenciais.

3. SEGURANÇA DA INFORMAÇÃO NAS EMPRESAS

A segurança da informação vem crescendo e ganhando cada vez mais espaço e importância nas empresas.

O seu principal foco é na proteção de pessoas, ativos e informações sigilosas utilizadas como diferencial competitivo no mercado, desta forma as empresas estão investindo cada vez mais em tecnologia e políticas claras de segurança da informação independente do porte ou mercado de atuação.

3.1 O Valor da informação

No mundo globalizado as informações são muito importantes para as empresas, tendo um forte investimento em recursos para adquirir e transformar informações em informações estratégicas para a tomada de decisão.

A informação aliada às diversas tecnologias tornou-se o maior ativo das empresas, pois as empresas que possuem domínio sobre a gama de informações existentes, consequentemente possuem maior participação de mercado.

O mundo corporativo, não admite mais a ausência de sistemas ou ferramentas tecnológicas, e a empresa que deseja adquirir vantagem competitiva ou até mesmo permanecer no ambiente empresarial, deve buscar um aperfeiçoamento contínuo do seu negócio. Sistema “é um conjunto de partes e componentes, logicamente estruturados, com a finalidade de atender a um dado objetivo.” (CASSARRO, 1988, p. 27).

4. MECANISMOS DE SEGURANÇA

Neste tópico apresento as recomendações de segurança que podem ser encontradas.

4.1 Controle Físico - São barreiras que limitam o contato não autorizado direto a informação ou infraestrutura, como portas, trancas, sala confre, blindagem ou guardas.

4.2 Controle Lógico - São barreiras que impedem o acesso não autorizado a informação em ambientes controlados e monitorados, que podem ser digitais ou eletrônicos.

4.3 Criptografia - Conjunto de técnicas para esconder a informação de acesso não autorizado.

4.4 Assinatura Digital - Conjunto de dados criptografados, associados a um documento do qual possui a função de garantir a integridade e autenticidade do documento associado.

4.5 Integridade - Medida em que um serviço ou informação é genuíno, está protegido contra a personificação por intrusos.

5. PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO

5.1 Confidencialidade - Garante que apenas pessoas autorizadas tenham acesso as informações.

5.2 Integridade - Garantia que somente pessoas autorizadas possam alterar as informações.

5.3 Disponibilidade - Garantia de que serviços ou informações estejam acessíveis sempre que pessoas autorizadas necessitem.

6. SEGURANÇA EM BANCO DE DADOS

É papel do administrador de banco de dados implementar políticas de segurança no ambiente de banco de dados, desde que a gestão de TI e do negócio estejam em comum acordo com toda a documentação aprovada e assinada pela gerência.

De posse desde documento o administrador de banco de dados terá total liberdade para implementar e utilizar ferramentas que o auxiliam no controle, monitoramento e administração de segurança dos servidores de banco de dados.

6.1 Acessos ao servidor de banco de dados

Somente pessoas autorizadas devem ter acesso fisico ou logico ao ambiente de produção de banco de dados, com permissões restritivas de acordo com o nível e papel desempenhado dentro do setor de tecnologia da informação.

6.2 Permissões de usuários e aplicações

Para as aplicações é necessário o nível de permissão recomendada de acordo com cada senário, de forma geral as aplicações necessitam de permissões como, leitura, escrita e execução de determinados objetos como procedures, funções e etc.

As permissões a serem aplicadas para a equipe de profissionais de tecnologia da informação devem ser as mais restritivas possíveis de acordo com cada função desempenhada. Apenas profissionais que possuem a função de administrador do banco de dados devem ter permissões elevadas com acesso aos ambientes de banco de dados sem restrição.

Adotando a política de complexidade e tempo de vida das senhas, podemos melhorar a camada de segurança ao acessar o banco de dados com senhas complexas, tendo como parâmetro o tempo de vida da senha, forçando o usuário a trocar a senha em prazos de expiração determinados pelo profissional de segurança ou de administração de banco de dados.

Para o melhor mapeamento e distribuição de permissões, o administrador de banco de dados deve criar grupos de acordo com cada área e tipos de permissão, adicionando as permissões nos grupos e incluindo os usuários, evitando permissões excessivas e esquecidas.

6.3 Auditoria de banco de dados

Com o aumento e criticidade de informações, se faz necessário a auditoria do ambiente de banco de dados, para que o profissional de segurança ou administrador de banco de dados possa realizar o monitoramento e auditoria de informações que possam impactar e gerar prejuízos nas empresas.

De posse de tais informações é possível gerar relatórios de auditoria, indicando acessos, ou profissionais que realizaram mudanças nas informações sem o consentimento da gerência ou quando ocorreram erros operacionais para que os envolvidos possam ser punidos, e as correções possam ser aplicadas em tempo hábil minimizando o impacto e prejuízo a corporação.

Desta forma podemos garantir a segurança das informações armazenadas no banco de dados, além de realizar avaliações dos controles, processos e procedimentos adotados para a segurança de informações sensíveis para o negócio, um bom exemplo é a norma SOX, norma que visa garantir a criação de

mecanismos de auditoria e segurança confiáveis nas empresas, incluindo ainda regras e a criação de comitês encarregados de supervisionar as atividades e operações de riscos nas empresas.

No mercado existem diversas ferramentas que podem ser adquiridas para realizar a auditoria no ambiente de banco de dados, caso a empresa não possua recursos é papel do DBA dentro do possível, implementar políticas de seguraça utilizando recursos nativos do SGBD, como a implementação de triggers de auditoria, desta forma sendo possível mesmo com poucos recursos implementar a auditoria nos ambientes de banco de dados da empresa.

6.4 Auditoria de DDL

Auditoria que consisteste em auditar mudanças em objetos nos bancos de dados como, tabela, view, procedure, function. Atraves dessa auditoria podemos ter o historico de modificações executadas no ambiente de banco de dados, garantindo o controle de modificações e o versionamento de objetos alterados.

6.5 Auditoria de DML

Auditoria que mantem o historico de mudanças em informações que possuem maior valor para a empresa, atraves dela podemos ter o historico de ações e mudanças tendo diversos filtros e procedimentos visando garantir quadlidade, integridade e confidencialidade das informações.

6.6 Criptografia de banco de dados

Usando a tecnologia projetada para impedir acessos não autorizados a banco de dados locais ou em redes, temos a possibilidade de criptografar informações que são trafegadas na rede, dessa forma podemos evitar incidentes de segurança por individuos não autorizados que se utilizem de um sniffer de rede (técnica que consite em capturar pacotes de dados), dessa forma ele não consiguirá capturar os dados reais, apenas informações criptografadas garantindo a segurança e integridade das informações que trafegam na rede envolvendo servidores de banco de dados, usuários e servidores de aplicação.

É de vital importancia a identificação e aplicação de politicas de segurança em dados sensiveis, dados sigiliosos que podem ser expostos e prejudiciais a empresa caso sejam acessados por pessoas não autorizadas.

7. PRINCIPAIS CAUSAS DE ATAQUES A BANCO DE DADOS

As principais causas de ataques a banco de dados entre 2013 e 2015 esta relacionado privilegios excessivos ou esquecidos, abuso de privilegio, SQL injectiom, malware, auditoria fraca, exposição a midia, exploração de vulnerabilidades, configurações default de banco de dados, dados sensiveis sem politicas de segurança e negação de serviço.

7.1 Privilegios excessivos ou esquecidos

São privelegios dados para resolver problemas pontuais ou privilegios que excedem as exigencias da função do trabalho executado pelo profissional, que não são revogadas apos a conclusão do trabalho, caindo no esquecimento.

Muitas vezes o profissional troca de area e por falta de politica ou mapeamento de segurança, ele continua com as permissões sensiveis sem que haja o bloqueio por mudança de area de atuação.

O exemplo claro é quando o funcionario sai de ferias ou é demitido e não efetuam o bloqueio de acesso aos recursos da empresa, deixando as permissões e o login com acesso aos sistemas e muitas vezes o acesso remoto, com tais privilegios o funcionario tendo uma indole ruim, podera roubar dados de alto valor ou provocar danos.

7.2 Abuso de privilegios

São operações que o usuario se utiliza das permissões para contornar bloqueios de segurança implementados nas aplicações ou serviços. Ao utilizar o sistema de recursos humanos o usuario so tera acesso ao seu salario, utilizando os prinvegios elevados ele ira ver todos os salarios da empresa ao fazer uma simples consulta no banco de dados do setor de recursos humanos, expondo os dados sensiveis de cada colaborador.

7.3 SQL Injection

São ataques de injeção de condigo mal intencionado, instruções SQL com campos de entrada em aplicações, que servem para conceder acessos sem restrinções ao banco de dados da corporação.

7.4 Malware

Softwares com função de infiltrar-se em um sistema ou uma rede de computadores com a função de causar danos ou roubar informações confidenciais.

7.5 Auditoria fraca, quando existir

Possue a função de gravar mudanças em informações sensiveis e que possuem grande valor a empresa, utilizando ferramentas e politicas para geração de historico das ações dos profissionais que possuem acessos ao banco de dados, gerando relatorios para tomada de decisão em caso de falhas de segurança ou em melhorias na segurança em banco de dados.

Muitas empresas não possuem auditoria, tendo consequencias drasticas quando são passiveis de invasão ou em incidentes, sem a possibilidade de identificar ou efetuar o devido rastreamento de informações que forem comprometidas ou acessadas por pessoas não autorizadas.

7.6 Exposição de Midia

Muitos backups são armazenados nos mais diversos tipos de midias, muitos profissionais não possuem a preocupação de criptografar os dados por medidas de segurança, caso essas midias caiam em mãos erradas, o individuo podera ter acesso da forma mais simples a todos os dados armazenados nessa midia, sem nenhum tipo de conhecimento tecnico.

7.7 Configurações fracas de banco de dados

É muito importante que os profissionais de administração de banco de dados, tenham a preocupação com a segurança, adotando boas praticas como mudar a porta de acesso ao SGBD, alterar a senha e usuarios administradores do banco de dados, atualizar as definições ou patchs de segurança no banco de

dados, evitando que as falhas conhecidas não sejam exploradas por pessoas não autorizadas ao ambiente de banco de dados.

7.8 Dados Sensiveis

São dados que devem ter políticas de segurança para o acesso ou alteração, o exemplo bem claro é o acesso a todos os cargos e salarios da empresa que o individio não autorizado podera visualizar.

7.9 Negação de serviço

São técnicas de sobrecarga a ativos, sistemas, serviços ou banco de dados, consiste em sobrecarregar recursos como, rede, processamento, ou consultas excessivas em banco de dados com a finalidade de sobrecarga ate que o servidor não consiga responder a grande quatidade de requisições e acabe travando.

8 BACKUP E RESTORE

Backup é um procedimento de segurança indispensável. É de vital importância para a recuperação de informações em caso de problemas lógicos ou físicos, desde que a política de backup seja bem planejada e estruturada.

É de vital importancia a adoção da política de restore aliada aà politica de backup, visto que desta forma podemos adotar políticas de segurança realizando verificações nas midias e testes de restore do ambiente de banco de dados, minimizando possíveis problemas que possam ocorrer quando realmenrte houver a necessidade da aplicação do restore no ambiente de banco de dados.

9 ALTA DISPONIBILIDADE

O principal objeto da alta disponibilidade é prover serviços ou soluções em banco de dados que possam ter acesso ininterruptos aos dados em caso de falhas, sejam falhas de rede, armazenamento ou banco de dados.

Existem soluções de diversos fabricantes que garantem a continuidade em caso de falhas nos ambientes de banco de dados, sejam soluções de espelhamento, cluster ativo-ativo ou cluster *failover*.

O papel do DBA é estudar e implementar a tecnologia que melhor se adapte ao cenária da empresa, visando a segurança do ambiente de banco de dados e a continuidade do negócio com o menor impacto possível.

10 CONSIDERAÇÕES FINAIS

Devido ao fato de existirem muitos sistemas legados com dados disponíveis em vários formatos, com novos tipos de dados constantemente surgindo, é bastante difícil se chegar a um padrão comum, apesar de existirem muitos esforços nesse sentido.

Mineração de dados geográficos é um tópico de estudo da área de Descoberta do Conhecimento (Knowledge Discovery) que ainda está começando.

A pesquisa nessa área tende a crescer, visto que cada vez mais cientistas estão dando especial atenção aos dados geográficos e, com isso, novas técnicas para explorar esses dados vem sendo desenvolvidas. Além disso, o crescimento do poder das plataformas computacionais contribui bastante para viabilizar a aplicação de novos métodos.

ABSTRACT

This article presents an overview of introduction to security databases , adopting policies, technologies and best practices that the database administrator must implement to ensure a safe environment. For the realization of scientific research used qualitative and literature to demonstrate the importance of the issue . We found that daily are stored and processed hundreds of terabytes of information in various segments of the corporate market companies , to ensure the availability , reliability and security of such information , if the use of one or more database management systems is necessary . The DBA role is to ensure that information is secure , undamaged and available as long as possible , before such responsibility, it is necessary to apply security policies and technologies ensuring the confidentiality , integrity and availability of all company databases.

Key words:

SGBD, DBA , security.

REFERÊNCIAS BIBLIOGRÁFICAS

EMASRI, Ramez, NAVATHE, Shamkant B. Sistema de Banco de Dados. Pearson Education do Brasil. São Paulo. 2005.

DATE, C. J.. INTRODUÇÃO A SISTEMAS DE BANCOS DE DADOS. 8. ed. Rio de Janeiro: Elsevier, 2003.

CASSARRO, Antônio Carlos, Sistemas de Informação para Tomada de Decisões. PIONEIRA,1988.

DANTAS, Marcus Leal Segurança da informação: uma abordagem focada em gestão de riscos. / Marcus Leal Dantas. – Olinda: Livro Rápido, 2011.

FERREIRA, Fernando Nicolau Freitas. Política de Segurança da Informação. Rio de Janeiro: Ciência Moderna Ltda., 2006.

http://intertemas.unitoledo.br/revista/index.php/ETIC/article/viewFile/4412/4172. Em 04/04/2016.

http://pt.slideshare.net/artinfo/segurana-em-banco-de-dados. Em 04/04/2016.

http://www.ibm.com/support/knowledgecenter/SSVRGU_8.5.3/com.ibm.designer.domino.main.doc/H_DATABASE_ENCRYPTION_OVERVIEW.html?lang=pt-br. Em 04/04/2016.

http://www.perallis.com/news/10-principais-causas-de-ataques-a-banco-de-dados. Em 03/05/2016.

https://pt.wikipedia.org/wiki/Lei_Sarbanes-Oxley. Em 04/04/2016.

https://pt.wikipedia.org/wiki/Seguran%C3%A7a_da_informa%C3%A7%C3%A3o. Em 04/04/2016.