INTERNATIONAL INTEGRALIZE SCIENTIFIC

ed.33
MARÇO/2024

INTERNATIONAL INTEGRALIZE SCIENTIFIC ISSN/2675-520

INTERNATIONAL INTEGRALIZE SCIENTIFIC

ed.33
MARÇO/2024

INTERNATIONAL INTEGRALIZE SCIENTIFIC ISSN/2675-520

INTERNATIONAL
INTEGRALIZE
SCIENTIFIC

Dados Internacionais de Catalogação na Publicação (CIP)

Biblioteca da EDITORA INTEGRALIZE, (SC) Brasil

International Integralize Scientific. 33ª ed. Março/2024. Florianópolis - SC

Periodicidade Mensal
Texto predominantemente em português, parcialmente em inglês e espanhol

ISSN/2675-5203

1 - Ciências da Administração

2 - Ciências Biológicas

3 - Ciências da Saúde

4 - Ciências Exatas e da Terra

5 - Ciências Humanas/ Educação

6 - Ciências Sociais Aplicadas

7 - Linguística, Letras e Arte

8 – Ciências Jurídicas

9 – Tecnologia

10 – Ciências da Religião /Teologia

INTERNATIONAL INTEGRALIZE SCIENTIFIC ISSN/2675-520

INTERNATIONAL
INTEGRALIZE
SCIENTIFIC

Dados Internacionais de
Catalogação na Publicação (CIP)
Biblioteca da Editora Integralize - SC – Brasil

Revista Científica da EDITORA INTEGRALIZE- 33ª ed. Março/2024
Florianópolis-SC

PERIODICIDADE MENSAL
Texto predominantemente em Português,
parcialmente em inglês e espanhol.
ISSN/2675-5203

1. Ciências da Administração
2. Ciências Biológicas
3. Ciências da Saúde
4. Ciências Exatas e da Terra
5. Ciências Humanas / Educação
6. Ciências Sociais Aplicadas
7. Ciências Jurídicas
8. Linguística, Letras e Arte
9. Tecnologia
10. Ciências da Religião / Teologia

INTERNATIONAL INTEGRALIZE SCIENTIFIC **ISSN/2675-520**

INTERNATIONAL INTEGRALIZE SCIENTIFIC

EXPEDIENTE

INTERNATIONAL INTEGRALIZE SCIENTIFIC
ISSN/2675-5203
É uma publicação mensal, editada pela
EDITORA NTEGRALIZE | Florianópolis - SC

Florianópolis-SC
Rodovia SC 401, Bairro Saco Grande, CEP 88032-005.
Contato: (48) 99175-3510
https://www.integralize.online

INTERNATIONAL INTEGRALIZE SCIENTIFIC **ISSN/2675-520**

INTERNATIONAL INTEGRALIZE SCIENTIFIC
ISSN / 2675-5203

É uma publicação mensal editada pela
EDITORA INTEGRALIZE.
Florianópolis – SC
Rodovia SC 401, 4150, bairro Saco Grande, CEP 88032-005
Contato (48) 4042 1042
https://www.integralize.online/acervodigital

EDITORA-CHEFE
Dra. Vanessa Sales

INTERNATIONAL INTEGRALIZE SCIENTIFIC **ISSN/2675-520**

INTERNATIONAL
INTEGRALIZE
SCIENTIFIC

TECNOLOGIA

TECHNOLOGY

INTERNATIONAL INTEGRALIZE SCIENTIFIC ISSN/2675-520

TECNOLOGIA

Autor: **Geraldo Lúcio Germano de Sousa**
Contato: ikarus25@gmail.com
DATABASE SECURITY ATTACK TECHNIQUES
TÉCNICAS DE ATAQUE A LA SEGURIDAD DE LAS BASES DE DATOS

TÉCNICAS DE ATAQUE À SEGURANÇA EM BANCO DE DADOS

DATABASE SECURITY ATTACK TECHNIQUES

TÉCNICAS DE ATAQUE A LA SEGURIDAD DE LAS BASES DE DATOS

Geraldo Lúcio Germano de Sousa
ikarus25@gmail.com

SOUSA, Geraldo Lúcio Germano de. **Técnicas de ataque à segurança em banco de dados.** Revista International Integralize Scientific, Ed. n.33, p. 08 – 17, março/2024. ISSN/2675 – 5203.

RESUMO

As técnicas de ataque a banco de dados estão cada vez mais sofisticadas. Por esse motivo a segurança dos dados é um tema grande relevância e complexidade por englobar questões políticas, nos níveis governamentais, legais, éticos bem como questões relacionadas ao sistema operacional entre outras.Nesse contexto, a presente pesquisa busca responder a seguinte questão problema: "Quais as técnicas deverão ser usadas pelo administrador de Banco de Dados para evitar possíveis ataques internos e externos?"O presente trabalho justifica-se pela necessidade de mostrar que o banco de dados é seguro e que existem várias formas para garantir a segurança dos mesmos. Foi realizada uma pesquisa bibliográfica, sendo utilizados alguns estudos científicos sobre o tema. Apresentou como objetivo geral descrever técnicas nos quais o Administrador de Banco de Dados deve se orientar para evitar ataques internos ou externos a um Sistema Gerenciador de Banco de Dados e como objetivos específicos analisar as estratégias e mecanismos que reduzam o acesso indiscriminado ao banco de dados, apresentar técnicas de ataque à segurança em banco de dados e verificar possibilidades para garantir a confidencialidade, a integridade e a disponibilidade do banco de dados. Conclui-se, portanto, que não existe um banco de dados 100% seguro. Algumas técnicas podem minimizar que o BD fique exposto a acessos não autorizados externamente e internamente.
Palavras-chave: Banco de Dados. SGDB. DBA. Técnicas de ataque.

SUMMARY

Database attack techniques are increasingly sophisticated. For this reason, data security is a highly relevant and complex topic as it encompasses political issues, at governmental, legal, ethical levels, as well as issues related to the operating system, among others. In this context, this research seeks to answer the following problem question: " What techniques should be used by the Database administrator to avoid possible internal and external attacks?" This work is justified by the need to show that the database is safe and that there are several ways to guarantee its security. A bibliographical research was carried out, using some scientific studies on the topic. Its general objective was to describe techniques in which the Database Administrator must orient itself to avoid internal or external attacks on a Database Management System and as specific objectives to analyze strategies and mechanisms that reduce indiscriminate access to the database, present database security attack techniques and verify possibilities to guarantee the confidentiality, integrity and availability of the database. It is therefore concluded that there is no 100% secure database. Some techniques can minimize the DB being exposed to unauthorized access externally and internally.
Keywords: Database. SGDB. DBA. Attack techniques.

RESUMEN

Las técnicas de ataque a bases de datos son cada vez más sofisticadas. Por esta razón, la seguridad de los datos es un tema de gran relevancia y complejidad ya que abarca cuestiones políticas, a nivel gubernamental, legal, ético, así como cuestiones relacionadas con el sistema operativo, entre otras. siguiente pregunta problema: "¿Qué técnicas debe utilizar el administrador de la Base de Datos para evitar posibles ataques internos y externos?" Este trabajo se justifica por la necesidad de demostrar que la base de datos es segura y que existen varias formas de garantizar su seguridad. Se realizó una investigación bibliográfica, utilizando algunos estudios científicos sobre el tema. Su objetivo general fue describir técnicas en las que debe orientarse el Administrador de Base de Datos para evitar ataques internos o externos a un Sistema Gestor de Bases de Datos y como objetivos específicos analizar estrategias y mecanismos que reduzcan el acceso indiscriminado a la base de datos, presentar técnicas de ataque a la seguridad de la base de datos y verificar posibilidades para garantizar la confidencialidad, integridad y disponibilidad de la base de datos. Se concluye por tanto que no existe una base de datos 100% segura. Algunas técnicas pueden minimizar la exposición de la base de datos a accesos no autorizados externa e internamente.
Palabras clave: Base de datos. SGDB. DBA. Técnicas de ataque.

INTRODUÇÃO

As técnicas de ataque a banco de dados estão cada vez mais sofisticadas. Por esse motivo, a segurança dos dados engloba questões políticas, nos níveis governamentais, legais, éticos, bem como questões relacionadas ao sistema operacional, entre outras. No ambiente de banco de dados, existem diferentes aplicações e usuários de uma organização referenciando a um único conjunto de dados através do Sistema de Gerenciamento de Banco de Dados (SGBD). Este fato faz com que a segurança se torne uma questão séria e importante (CASTANO, 1994).

Uma meta básica é proteger o sistema contra usuários não autorizados que possam acessar dados. Logo, é necessária uma política de segurança para proteger a informação armazenada no Banco de Dados. Nessa política de segurança devemos ter um conjunto de leis, regras e práticas que regulamentam o fluxo e a proteção da informação.

Os mecanismos de segurança devem cuidar da prevenção e detecção de acessos impróprios. Uma boa prevenção e detecção requerem bons mecanismos de autenticação. Os mecanismos de segurança podem ser implementados de modo a evitar ataques ao banco de dados. Fornecer segurança num SGBD significa identificar as ameaças e escolher a política (OLSON and A., 1990) (BELL, 1975).

Nesse contexto, a presente pesquisa busca responder à seguinte questão-problema: "Quais as técnicas devem ser usadas pelo administrador de Banco de Dados para evitar possíveis ataques internos e externos?"

Como objetivo geral buscou descrever técnicas nos quais o Administrador de Banco de Dados deve se orientar para evitar ataques internos ou externos a um Sistema Gerenciador de Banco de Dados. E como objetivos específicos analisar as estratégias e mecanismos que reduzam o acesso indiscriminado ao banco de dados, apresentar técnicas de ataque à segurança em banco de dados e verificar possibilidades para garantir a confidencialidade, a integridade e a disponibilidade do banco de dados.

Com alto uso de tecnologias, surgem grandes necessidades nas empresas e com isso muitos dados são manipulados, seja de clientes, empresas e funcionários. Vários serviços como alteração, inclusão, exclusão de clientes entre outros processos que à primeira vista pode ser simples, pode se tornar um grande problema caso não aconteça um controle certo do banco de dados e o DBA pode facilitar esse processo. As empresas precisam acompanhar criticamente o processo de segurança do banco de dados. Um banco de dados precisa se manter seguro, ou seja, garantindo que as políticas de segurança sejam bem executadas. O presente trabalho justifica-se pela necessidade de mostrar que o banco de dados é seguro e que existem várias formas para garantir a segurança dos mesmos. Além disso , apresentar o papel do DBA nessa função.

Pensando nessa segurança, Elmasri e Navathe (2011) explicam que o SGDB apresenta diversas funções significativas e entre elas um sistema de segurança que age na proteção de dados contra possíveis acessos não autorizados. Sendo assim, esse tema se torna relevante para apresentar as possibilidades da segurança da informação.

O objeto de estudo da presente pesquisa são as técnicas de ataque à segurança em banco de dados. Foi realizada uma pesquisa bibliográfica, sendo utilizados alguns estudos científicos sobre o tema. Vergara (2005) classifica esse tipo de pesquisa como um estudo sistematizado desenvolvido com base em material publicado e acessível ao público em geral.

Por explorar um determinado tema com a finalidade de se conhecer melhor, pode-se dizer que apresentou uma abordagem de pesquisa qualitativa. Severino (2002) ressalta que uma

pesquisa qualitativa exige do pesquisador uma reflexão detalhista, onde se envolva com o objeto investigado. E complementando a visão desse autor, Minayo (2007) destaca que a pesquisa qualitativa precisa ser interpretada pelo pesquisador, através de influências como os textos que são lidos durante a pesquisa, valores que possui e experiências que já vivenciaram.

Quanto à natureza da pesquisa pode ser classificada como básica, pois foi realizada uma pesquisa investigativa sobre os princípios básicos e relevantes da segurança do banco de dados, podendo ser considerada também uma pesquisa teórica.

BANCO DE DADOS: CONCEITUAÇÃO

O banco de dados pode ser definido como um sistema computadorizado para manutenção de dados e registros. Sua funcionalidade permite o armazenamento de dados permitindo que os usuários busquem e atualizem os mesmos sempre que necessário. A tecnologia contribuiu muito para esse serviço porque antigamente tudo era manual e acarreta diversos problemas como demora em localizar determinada informação, assim como um volume muito grande de papel e pouca proteção dos dados (ELMASRI, 2007).

O sistema de banco de dados é composto por dados, software, hardware e usuários. Ele é integrado, apresentando a unificação de diferentes arquivos distintos e ao mesmo tempo é compartilhado, sendo acessado por todos os departamentos de uma empresa, tendo cada usuário acesso somente as informações pertinentes a seu setor de trabalho. Nesse contexto é importante destacar que segurança de dados não envolve somente danificação ou perda de dados, mas também acessos indevidos.

A parte lógica do banco de dados envolve os softwares que são utilizados para garantir a segurança ao acesso dos dados. Esses softwares são desenvolvidos por programadores e todas as solicitações ou atualizações necessárias são feitas pelo SGBD (Sistema Gerenciador de Banco de Dados). Elmasri e Navathe (2011) afirmam que,

> O mecanismo de segurança de um SGBD precisa incluir provisões para restringir o acesso ao sistema de banco de dados como um todo. Essa função, chamada de controle de acesso, é tratada criando-se contas do usuário e senhas para controlar o processo de login pelo SGBD (ELMASRI; NAVATHE, 2011, p.564).

Os usuários são responsáveis por alimentar o banco de dados, cadastrando, alterando ou excluindo os registros. Os usuários se dividem em programador, responsável em desenvolver os softwares para utilização do sistema, usuários finais, responsável por informar ao sistema os dados solicitados e os administradores de banco de dados conhecidos como DBA responsável pelo banco de dados. Silva e Rosa (2017) destacam que,

> O DBA é responsável pela segurança geral de um sistema de banco de dados. Ele é a autoridade máxima e utiliza uma conta conhecida como super usuário ou conta do sistema para desempenhar suas funções como, por exemplo, decidir os privilégios dos usuários (SILVA;ROSA, 2017, p.63).

Ou seja, é um profissional específico que comanda o banco de dados, decidindo quais

dados serão armazenados, formas e usuários para acesso e estabelecer critérios para a segurança de dados. “É imperativo que deva existir alguma pessoa que entenda esses dados e as necessidades da empresa com relação a esses dados, em um nível elevado de administração. O administrador de dados é essa pessoa” (DATE, 2003, p.15).

É importante destacar que os dados não pertencem ao DBA ou aos usuários e até mesmo do sistema, eles pertencem às organizações. E como as empresas fazem o compartilhamento de muitos dados e recursos computacionais é indispensável a presença desse profissional. Entre diversas funções atribuídas a esse cargo, destaca-se garantir a confidencialidade para segurança de dados.

ESTRATÉGIAS E MECANISMOS DE SEGURANÇA EM BANCO DE DADOS

O DBA (Database Administrator) tem a responsabilidade de definir estratégias e mecanismos para melhor acesso ao banco de dados, definindo inclusão ou concessão de privilégios a usuários que precisam utilizar o sistema e classificação de usuários e dados de acordo com as políticas da organização (ELMASRI, 2007).

Entre alguns recursos adotados pelo DBA podemos citar: autenticação de usuários e esquemas, autorização, auditoria, criptografia e visões. Para o usuário acessar o banco de dados ele será submetido a uma autenticação, que irá identificar se o usuário em questão está apto a entrar no Banco de Dados (BD) e quais recursos lhe serão concedidos. A autenticação para acessar ao BD será por meio de um *login* e senha respectivamente.

Um exemplo é o acesso ao cardápio de almoço diário de um restaurante. Se ocorrer que uma aplicação *web* acessa o banco de dados apresentando um conteúdo personalizado baseado no perfil do usuário, você precisa se certificar de que receberá o cardápio de almoço para seu escritório da filial em Houston, Texas, não o cardápio para o escritório da matriz de Buffalo, Nova York. (BRYLA BOB;LONEY KEVIN,2009).

Cada usuário ao BD terá um esquema associado. Um esquema é uma coleção lógica de objetos do BD como: tabelas, visões, sequências, sinônimos, índices, procedimentos, funções e etc.

A autorização para acessar e modificar o BD é concedida ao usuário pelo o DBA. Ela é maior que um simples acesso a tabelas ou relatórios, alguns usuários poderão ter o privilégio de criar ou excluir tabelas no esquema de qualquer outro usuário. Outro exemplo, seria a criação de uma política implementada por uma *Stored Procedure*(são um conjunto de comandos de SQL que restringe o acesso baseado no horário estipulado ou quais colunas serão acessadas.

A auditoria é um monitoramento que auxilia na investigação ao uso de uma BD, ela é um controle ao qual ficam registradas todas as alterações no BD. Ela não registra apenas *login* que ocorreram com sucesso, mas todos os *logins* falhos ou bem sucedidos.

Ela é uma ferramenta importantíssima para o DBA, mas seu uso sem um planejamento adequado pode gerar *overhead*. Além dos sistemas de segurança relacionados anteriormente, não será de boa prática se o sistema operacional e o *hardware* não estiverem em locais seguros. Serão exemplificados alguns tópicos que precisam ser considerados fora do banco de dados como os problemas, conforme os estudos de Elmasri (2007):

1. Segurança do Sistema Operacional - Todo Sistema Operacional (SO) não é 100% seguro,é de boa praxe que o usuário ou responsável em questão faça regularmente diretrizes de atualizações para correções de *bugs* ou entradas no sistema por pessoa sem autorização.

2. Backups - A empresa deve limitar o uso de fitas, disco ou CD/DVD-ROM a um número limitado de pessoas, mesmo que um Sistema Operacional esteja seguro com senhas criptografadas, serão inúteis caso a cópia de *backups* seja extraviada para *hackers* ou usuários não autorizados.

3.Verificações de segurança em segundo plano - Levantar uma triagem dos funcionários que lidam com dados confidenciais sejam eles DBAS, Auditores ou Administradores do Sistema Operacional.

4. Educação sobre Segurança - Certificar que todos os usuários saibam de suas responsabilidades e deveres em relação às regras da Empresa, um usuário educado resistirá às tentativas externas por busca de informações internas da empresa.

5. Acesso Controlado ao Hardware - Todo *Hardware* que o BD esteja hospedado sua localização em meio seguro de preferência com acesso restrito a usuário com senhas e códigos seguros.

Duas outras formas de aumentar o nível de segurança seriam a Criptografia das senhas e as visões. Criptografia (Do Grego kryptós, "escondido", e gráphein, "escrita") é o estudo dos princípios e técnicas pelas quais a informação pode ser transformada da sua forma original para outra ilegível, de forma que possa ser conhecida apenas por seu destinatário (detentor da "chave secreta"), 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.

As visões são tabelas virtuais que o DBA pode criar com a finalidade de aumentar a segurança nas tabelas e simplificar o uso no sistema. As visões delimitam que usuários sem autorização possam conhecer dados de umas tabelas que não tenham a necessidade de conhecer, seu uso é bastante eficiente porque cede apenas informações necessárias ao usuário.

TÉCNICAS DE ATAQUE AO BANCO DE DADOS

"Um ataque corresponde a um comprometimento em nível de sistema de segurança através de um ato inteligente ou deliberado, afetando serviços e violando política de um sistema" (SHIREY, 1995). Uma técnica de ataque que está sendo muito usada para obter informações sigilosas é o SQL *Injection* que é uma manipulação de uma instrução SQL através das variáveis que compõem os parâmetros recebidos por um script, tal como PHP, ASP, entre outros. Segundo PHP Group,

> Injeção direta de comandos SQL é uma técnica onde um atacante cria ou altera comandos SQL existentes para expor dados escondidos, ou sobrescrever dados valiosos, ou ainda executar comandos de sistema perigosos no servidor. Isso é possível se a aplicação pegar a entrada do usuário e combinar com parâmetros estáticos para montar uma consulta SQL. (PHP GROUP, 1995, online)

Este tipo de ataque consiste em passar parâmetros com valores maiores via barra de navegação do navegador, inserindo instruções não esperadas pelo banco de dados. Geralmente o atacante utiliza essas ferramentas para roubar dados ou danificar a base de dados que está no servidor.

Um exemplo que podemos citar que saiu no site www.g1.com.br é de um *hacker* de 28 anos, Albert Gonzalez, que alegou ser um dos líderes de uma máfia de hackers que extorquiu mais de 130 milhões de pessoas, se fazendo passar pelas mesmas, por técnica "ataque de injeção SQL", que seu usuário em questão usurpar informações que não são de sua autorização para extraviar, manipular informações sobre cartões de crédito e de débito.

A seguir serão citadas algumas técnicas de ataque:

A) *E-mail* falso.

É um ataque em que o usuário recebe uma solicitação de complemento de informações para uma empresa, grupos ou amigos. O usuário em questão envia todas as informações que lhe foram solicitadas, essas informações são direcionadas para um email que não é do destinatário original.

B) Orkut

O Orkut é uma rede de relacionamento que tem a finalidade de criar comunidades, enviar *scraps*(recados) em seus contatos. Seus usuários recebem um *email* ao qual lhe são solicitados que no período de 72 horas eles devem executar um programa para que suas contas continuem funcionando.

Esse programa não é reconhecido pela maioria dos antivírus e faz o *download* de um outro t*rojan*, que abre uma porta para *hackers*. O objetivo é roubar informações do usuário. Além disso, o vírus faz com que janelas Pop-Up abram automaticamente, com anúncios de *sites* eróticos.

Assim como *Orkut*, atualmente, outras redes sociais também fazem parte desse cenário de ataques como *Facebook, Instagram, Twitter* e outras redes de relacionamento como o Tinder.

ATAQUES POR PROGRAMAS MALICIOSOS

São programas maliciosos com a intenção de roubar informações,sem que o usuário se de conta que seus dados estão sendo copiados , esses ataques podem ser por : vírus , trojans ou *worms*. A seguir serão citados alguns programas maliciosos:

A) Páginas clone.

É uma página criada com a finalidade de enganar o usuário ao qual este deveria completar informações sigilosas ao mesmo e são direcionadas para o criminoso

B) **Link Spoofing**
É um ataque em o usuário receber um email que de uma fonte ao qual ele ostenta fidelidade, mas na verdade pertence a um endereço de terceiros com a intenção de roubar informações.

Segundo o site do professor Dailson Fernandes, diversas técnicas são utilizadas por *hackers* para obter, extrair e manipular informações sem a definida autorização de seus proprietários como *scanning* de memória (DLL *Injection*), cujo foi mencionada anteriormente na página 6 deste mesmo artigo.

Existem também as técnicas usadas por um programa para acessar a memória ocupada por outro programa, podendo assim ler dados sensíveis como a senha informada pelo usuário e chaves criptográficas.

Outra técnica muito usada é o *sniffing*. Ela permite capturar as informações de uma determinada máquina ou o tráfego de uma rede sem autorização para coletar dados, senhas, nomes e comportamento dos usuários. Os programas geralmente capturam tudo que passa e depois utilizam filtros para que possa facilitar a vida do "*sniffador*".

Existem *sniffers* específicos de protocolos como o *im sniffer* que captura apenas as conversas via MSN Messenger em uma rede. Segundo o professor Dailson Fernandes existem outras técnicas de ataque como:

A)Scamming: É uma Técnica que engana o usuário o qual recebe um email falso de um banco pedindo informações como senha e número de conta do proprietário, é uma técnica que se apropria da falta de informações do usuário, já que informações de senha e número de conta são informações sigilosas que a maioria dos bancos tratam apenas com a presença da mesma pessoa .

B) Teclado virtual: Como forma de segurança muitos bancos utilizam o teclado clonado que é um *software* que simula um teclado virtual possibilitando maior segurança ao usuário, o falsário em questão simula um teclado virtual falso que lhe passa informações confidenciais do usuário.

C) Keyloggers: É um software que copia informações como senha , *logins* dos usuários e transfere para pessoas que não são autorizadas a ter o acesso a essas informações.

D) Clonagem de URLs(Páginas da Web): É uma forma de clonagem de endereços na internet "URLs" geralmente são clonadas de páginas de bancos com um nome semelhante ao original, com a intenção de enganar o usuário .

Um exemplo é o da página do banco Itaú, www.itau.com.br , que com o uso da clonagem aparece de diferentes formas como : www.itau.com.br, www.itaul.com.br, www.itauu.com.br, www.itaubanko.com.br ou www.iitauu.com.br.

Segundo o especialista em análise de risco Denny, algumas dicas podem reduzir os riscos relacionados a ameaças digitais como:

A)Restringir todo conteúdo da empresa , de modo que o conteúdo que não posso ser verificado

seja bloqueado inicialmente;
B) Software de segurança como antivírus e firewalls devem estar atualizados regularmente.
C)Verificações de seguranças sobre *links* e mensagens que receber por email.
D) Atualizar-se sobre boletins de segurança e acompanhar as notícias relacionadas à segurança da informação.

Pensando na segurança do banco de dados, Ramakrishnan e Gehrke (2008), defendem que a criptografia de dados é uma das melhores soluções para transferir ou armazenar dados com segurança. Os autores explicam que quando os dados estão criptografados, em caso de acesso não autorizado ou invasão, haverá grandes dificuldades para decifrar as informações, porque a criptografia permite a compreensão somente por pessoas que são previamente autorizadas.

Esses usuários autorizados recebem previamente chaves (algoritmos) de codificação ou decodificação para decifrar os dados. Ramakrishnan e Gehrke (2008,p.590) explicam que "sem a chave de descriptografia correta, o algoritmo de descriptografia produz lixo".

As organizações precisam tomar medidas necessárias para garantir a manutenção da segurança de seu banco de dados visando evitar danos às empresas que podem ser irreparáveis. O DBA precisa ter muita cautela no momento de conceder acessos e liberação aos usuários evitando privilégios desnecessários e atuando de forma preventiva contra diversos tipos de ataques.

REDES SOCIAIS E APLICATIVOS DE MENSAGENS

Moraes (2011, p. 138) diz que "as redes sociais podem ser definidas como comunidades virtuais que possibilitam diversos meios de comunicação e interação com outros usuários". Atualmente as redes sociais adquiriram diversas finalidades, tanto com uso residencial quanto comercial. O uso das redes assim como os aplicativos de mensagens faz parte da rotina da humanidade.

E por ter um fluxo grande de contas e acessos, o número de golpes aumenta cada vez mais , visto que os golpistas utilizam da fragilidade dos sistemas, da inocência e da desatenção das empresas e pessoas e da falta de preparo e de informação por parte dos usuários ao fazer o uso das tecnologias.

POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO

Abordando a temática de ataques e de banco de dados, se faz necessário pontuar as políticas de segurança da informação. De acordo com Campos (2006) essa política é precisa nas organizações para indicar como as coisas precisam acontecer quando se refere à segurança da informação. Esse tipo de pesquisa apresenta papel de prevenção e se torna fundamental e indispensável em qualquer empresa, abrangendo toda estrutura empresarial e não somente a

área da TI.

Fontes (2012, p.72) explica que “uma segurança da informação efetiva exige o desenvolvimento dos executivos da organização para participar da avaliação das novas ameaças e da definição de prioridades”. Essa ação de maneira conjunta oferece para as empresas uma visão mais ampla dos possíveis riscos e soluções visando o desenvolvimento das organizações.

A política de Segurança da Informação apresenta como funções “atender à legislação, atender à exigência do mercado e dos próprios clientes, se adequar às melhores práticas, acompanhar o avanço tecnológico e atender às necessidades do próprio negócio".

Geus e Nakamura (2007) explica que é preciso fazer umas considerações importantes para as organizações sobre as políticas de Segurança de Informação,

> a) Conheça seus possíveis inimigos: identifique possíveis ações e perigos antes que aconteçam; b) Contabilize os valores: uma política de SI eficaz pode requerer a contratação de novos profissionais ou a compra de novos equipamentos. Todos estes valores devem ser levantados antecipadamente para evitar alterações no plano; c) Identifique, examine e justifique suas hipóteses: qualquer aspecto que não for previamente identificado pode ocasionar uma grande mudança no escopo do plano, atrasando os trabalhos e gerando desconforto; d) Controle os seus segredos: estabeleça quais são as informações totalmente secretas; e) Avalie os serviços estritamente necessários para o andamento dos negócios na organização: este fator é válido para evitar conflitos com os usuários; f) Considere os fatores humanos: muitas das falhas nos procedimentos de segurança são causados pelas pessoas. É preciso convencer os usuários de sua responsabilidade em todos os processos; g) Conheça seus pontos fracos: seja crítico e reconheça suas fraquezas; h) Limite a abrangência do acesso: crie barreiras como uma zona desmilitarizada, equilibrando a força entre toda a rede; i) Entenda o ambiente: é preciso conhecer o funcionamento regular da rede para identificar de maneira rápida quando algo está fora do normal (GEUS E NAKAMURA, 2007, p.194).

Sendo assim, percebe-se que o mundo da segurança apresenta uma constante e contínua evolução, visto que as técnicas de ataque também se atualizam, e agir de maneira preventiva permite que as organizações possam se antecipar aos riscos. E assim criar algumas estratégias de segurança, como a política de senhas, por exemplo, que consiste em fortalecer as senhas.

CONSIDERAÇÕES FINAIS

Por base dos estudos de segurança de banco de dados, podemos ter certeza que não existe um banco de dados 100% seguro. Algumas técnicas podem minimizar que o BD fique exposto a acessos não autorizados externamente e internamente.

Em nível externo medidas como restrição de conteúdo da empresa preservando dados que não devem ser extraviados , vistos ou manipulados por terceiros sem autorização da mesma, o uso de antivírus com atualizações constantes , a educação aos funcionários para que modifiquem suas senhas constantemente para evitar ataques por terceiros tanto em nível externo

ou interno.

A nível interno medidas como atualizações de antivírus e firewall ajudam a prevenir ataques externos e restrições a informações por setores da empresa também é uma boa prática para dificultar o acesso a setores externos e internos da empresa.

Após esse estudo, sugere-se que as empresas conheçam a sua real necessidade mediante a segurança da informação, principalmente no conhecimento que o profissional responsável por essa área possui. Quanto mais prática e certificações esse profissional adquirir,ele vai estar mais apto e habilitado para garantir a segurança e informações das empresas.

REFERÊNCIAS BIBLIOGRÁFICAS

BRYLA BOB, LONEY ,KEVIN, Manual do DBA. Porto Alegre: Bookman, 2009

CAMPOS, André L. N. Sistema de Segurança da Informação: Controlando os Riscos. Florianópolis: Visual Books, 2006.

CASTANO, S. *Database Security Reading*. Addison-Wesley, 1994.

Criptografia.Origem :Wikipédia,a enciclopédia livre.Disponível em:<http://pt.wikipedia.org/wiki/Criptografia>Acesso em :16 Novembro de 2023.

DATE, Christopher J. Introdução a sistemas de banco de dados. 8. ed. Rio de Janeiro: Elsevier,2003.

ELMASRI, Ramez; NAVATHE, Shamkant B. Sistemas de Banco de dados. 4ª ed. São Paulo: Pearson Addison Wesley, 2005.

FONTES, Edison. Políticas e Normas para a Segurança da Informação. Rio de Janeiro: Brasport, 2012.

GEUS, Paulo Lício de; NAKAMURA, Emilio Tissato. Segurança de Redes em ambientes corporativos. São Paulo: Novatec, 2007.

MINAYO, M. C. S. (Org.). Pesquisa social: teoria, método e criatividade. Petrópolis: Vozes, 2001.

MORAES, Paulo. Mente Anti-hacker - Proteja-se! Rio de Janeiro: Brasport, 2011.

OLSON, I. and A., M. D.Computer access control policy choices. Computers and Security.*1990*

PHP, Group. Manual do PHP: Injeção de SQL. Disponível em: <http://php.net/manual/pt_BR/security.database.sql-injection.php>. Acesso em: 28 nov. 2023

RAMAKRISHNAN, RAGHU; GEHRKE, Johannes. Sistemas de gerenciamento de banco de dados. 3.ed. São Paulo: McGraw-Hill, 2008.

SEVERINO, A. J. A formação profissional do educador: pressupostos filosóficos e implicações curriculares. ANDE, Ano 10, n° 17, 1991.

SHIRLEY, Robert W. Security requirements for network management data.2008

SILVA, Thaynara; ROSA, Paulo Roberto. Segurança em banco de dados. Colloquium Exactarum, vol. 9, n. Especial, Jul–Dez, 2017

SQL Injection.Origem:Microsoft. Disponível em:< http://msdn.microsoft.com/en-us/library/ms161953.aspx> Acesso em :16 Novembro de 2023.

VERGARA, S. C. Métodos de pesquisa em administração. São Paulo: Atlas, 2005.

INTERNATIONAL INTEGRALIZE SCIENTIFIC

Publicação Mensal da INTEGRALIZE

Aceitam-se permutas com outros periódicos.

Para obter exemplares da Revista impressa, entre em contato com a Editora Integralize pelo (48) 99175-3510

INTERNATIONAL INTEGRALIZE SCIENTIFIC
Florianópolis-SC
Rodovia SC 401, Bairro Saco Grande,
CEP 88032-005.
Telefone: (48) 99175-3510
https://www.integralize.onlin

INTERNATIONAL INTEGRALIZE SCIENTIFIC **ISSN/2675-520**