A IMPORTÂNCIA DA SEGURANÇA EM BANCO DE DADOS: GARANTINDO A PROTEÇÃO DE INFORMAÇÕES SENSÍVEIS

THE IMPORTANCE OF DATABASE SECURITY: GUARANTEING THE PROTECTION OF SENSITIVE INFORMATION

Emily Bezerra Domingues
Fatec Araraquara – Prof. José Arana Varela
emily.domingues@fatec.sp.gov.br

Gustavo Henrique Augustini
Fatec Araraquara – Prof. José Arana Varela
gustavo.augustini01@fatec.sp.gov.br

Wdson de Oliveira
Fatec Araraquara – Prof. José Arana Varela
wdson.oliveira01@fatec.sp.gov.br

Resumo

Este artigo tem como objetivo destacar a importância da segurança em bancos de dados e a necessidade de medidas proativas para proteger informações sensíveis em um contexto de crescente dependência tecnológica. A abordagem metodológica adotada foi uma revisão de literatura, com a análise de fontes como o Google Acadêmico. O estudo revela que, com o aumento das ameaças cibernéticas, os bancos de dados são alvos frequentes de ataques que podem resultar em vazamento de informações, perdas financeiras e danos à reputação das organizações. Entre as medidas de segurança destacadas estão o controle de acesso, a autenticação de usuários, backups regulares e a atualização constante dos sistemas. As conclusões indicam que, para garantir a proteção das informações sensíveis, é fundamental a implementação de políticas de segurança da informação, treinamento contínuo e conformidade com as leis de proteção de dados.

Palavras-chave: Segurança. Banco de dados. Ataques cibernéticos.

Abstract

This article aims to highlight the importance of database security and the need for proactive measures to protect sensitive information in a context of growing technological dependence. The methodological approach adopted was a literature review, analyzing sources such as Google Scholar. The study reveals that, with the increase in cyber threats, databases are frequent targets of attacks that can result in data breaches, financial losses, and reputational damage to organizations. Among the highlighted security measures are access control, user authentication, regular backups, and continuous system updates. The conclusions indicate that, to ensure the

protection of sensitive information, it is essential to implement information security policies, provide ongoing training, and ensure compliance with data protection laws.

***Keywords**: Security. Database. Cyberattacks.*

1. Introdução

Na última década, os progressos tecnológicos têm transformado de forma significativa o modo como produzimos, organizamos e disponibilizamos informações. A capacidade de comunicação está em constante aumento, assim como a interação entre sistemas, o desenvolvimento de redes convergentes e o surgimento de redes móveis, proporcionando uma comunicação contínua e acessível de diferentes locais, o que permite várias formas de acesso às informações.

Incialmente, esses ambientes foram concebidos para fins de pesquisa, com o objetivo de possibilitar várias opções de conectividade para as partes envolvidas, e, por isso, a segurança não era uma preocupação primordial na sua concepção original. No entanto, dada a demanda comercial em crescimento e a utilização estratégica dessas comunicações, a segurança da informação (SI) tornou-se uma prioridade para as empresas que precisam garantir a segurança de suas informações, como o lançamento de um novo produto no mercado ou o número do cartão de crédito de seus clientes (SANTOS, SILVA, 2021).

A segurança da informação é uma área essencial para qualquer tipo de organização, e uma das principais preocupações está relacionada à proteção de dados sensíveis armazenados em bancos de dados. Com o crescente número de ataques cibernéticos e o aumento da exposição de informações valiosas, é fundamental adotar medidas proativas para garantir a integridade, confidencialidade e disponibilidade desses dados (CUNHA, 2018).

Com o avanço da tecnologia e a maior dependência de sistemas informatizados, a segurança da informação se tornou um desafio cada vez maior. Os bancos de dados são alvos constantes de ataques cibernéticos, que podem resultar em danos significativos às organizações, como o vazamento de informações estratégicas, perda de dados e prejuízos financeiros.

Diante disso, este artigo tem como objetivo geral abordar a importância da segurança em banco de dados e a necessidade de medidas proativas para proteger informações sensíveis.

O foco principal será ataques, ferramentas e meios para garantir a proteção de dados. Como objetivos específicos, inicialmente buscou-se investigar os diversos tipos de ataques cibernéticos direcionados a bancos de dados; em um segundo momento apresentar as principais ferramentas de segurança de banco de dados e analisar as medidas de prevenção mais eficientes para garantir um ambiente seguro; e por fim buscou-se discutir a importância da implementação de políticas de segurança da informação.

2. Referencial Teórico

Este capítulo apresenta os principais conceitos, teorias e boas práticas que fundamentam o tema deste estudo, oferecendo uma base teórica sólida para a análise das práticas de segurança em bancos de dados e a proteção de informações sensíveis.

2.1. Segurança da informação

No mundo globalizado, onde a troca de informações é rápida e constante, é essencial que as organizações protejam seu conhecimento. O sucesso de um negócio pode depender diretamente do cuidado com informações confiáveis e da prevenção de roubo ou fraude. Consequências graves como perda de mercado, clientes e financeira podem ser evitadas com a proteção adequada das informações, da infraestrutura de rede e do capital intelectual.

O conhecimento é o principal ativo de uma organização e garantir sua proteção significa assegurar o próprio sucesso do negócio. Portanto, a segurança da informação torna-se fundamental nos processos de negócio das organizações (CARVALHO, 2009).

A segurança da informação é um assunto de extrema importância tanto para organizações empresariais quanto não empresariais, devido ao fato de que nos últimos tempos muitas empresas tiveram seus dados roubados por *hackers*, que aproveitaram essas falhas para cometer crimes virtuais. De acordo com Cunha (2018), para garantir que os dados sejam armazenados de forma segura e possam ser recuperados adequadamente apenas por pessoas autorizadas, é necessário ter uma estrutura adequada.

Os especialistas em segurança da informação estão sendo mais valorizados pelas empresas devido às grandes perdas de dados que ocorreram recentemente. Com isso, esses profissionais devem estar atentos aos três pilares fundamentais da tecnologia da informação: Essas medidas são baseadas em três princípios fundamentais: confidencialidade, integridade e disponibilidade. Devendo então manter as informações confidenciais, garantir sua integridade e assegurar sua disponibilidade, a fim de prevenir e combater invasões não autorizadas de forma eficaz (CUNHA, 2018).

Cunha (2018) enfatiza que a segurança da informação de maneira geral, refere-se à implementação de medidas para proteger a informação contra ameaças, minimizar riscos e maximizar o retorno dos investimentos. A confidencialidade envolve garantir que a informação só possa ser acessada por pessoas autorizadas. Qualquer acesso não autorizado é considerado quebra de confidencialidade.

A integridade garante que a informação armazenada ou transmitida esteja correta e precisa. A perda da integridade ocorre quando a informação é indevidamente alterada ou sua conformidade não pode ser garantida. A disponibilidade garante que a informação esteja acessível quando necessário. Isso inclui o funcionamento adequado da rede e do sistema, permitindo o acesso à informação.

Soares, Soares, Alves, (2021) enfatizam que a informação é um recurso crucial para uma organização e desempenha um papel fundamental nos negócios. Por isso, é essencial garantir a sua proteção adequada. À medida que os ambientes de trabalho se tornam cada vez mais interconectados, a informação está sujeita a uma ampla gama de ameaças.

Nesse contexto, implementar uma política de segurança da informação é fundamental para todas as organizações, o que pode ser feito através do uso de regulamentações normativas, padronizando os processos internos e fornecendo treinamento sobre proteção de informações. Isso reduzirá os gastos relacionados a incidentes e perdas de dados (SOARES, SOARES, ALVES, 2021).

2.2. A importância da segurança em banco de dados

Os bancos de dados têm a função de armazenar uma variedade de informações, desde dados simples de conta de e-mail até informações importantes da Receita Federal, números de cartões de crédito e senhas, entre outros. Dado o valor dessas informações, é crucial que elas sejam protegidas adequadamente. Diante desse cenário, a segurança dos bancos de dados está se tornando cada vez mais prioritária devido ao surgimento de novas formas de roubo de informações, como o *ransomware*.

Esse tipo de malware criptografa os dados armazenados em um dispositivo, tornando-os inacessíveis, e exige um pagamento de resgate para restabelecer o acesso ao usuário. Com o aparecimento dessas ameaças, a área de segurança deve crescer e se tornar ainda mais essencial nos bancos de dados das empresas (CAMPOS, 2018).

Em muitas empresas nos últimos anos, os bancos de dados são o local onde a maioria das informações confidenciais são armazenadas. Por essa razão, de acordo com Gaidargi, (2021) proteger esses bancos de dados contra invasões é uma responsabilidade crucial para administradores de banco de dados, programadores e equipes de DevOps (é uma cultura que promove a colaboração entre todas as funções envolvidas no desenvolvimento e na manutenção do software) desenvolvimento de software (Dev) e as operações de TI (Ops)) que dependem deles. Porém, essa tarefa não é simples.

Apesar dos criadores nos fornecerem ferramentas e implementarem medidas de segurança, além de documentá-las, é compreensível que ocorram dezenas de erros, omissões e até mesmo enganos simples, o que torna o desafio de manter a segurança do banco de dados uma tarefa constante e ininterrupta (GAIDARGI, 2021)

Soares, Soares, Alves, (2021) explicam que a segurança em banco de dados é de extrema importância para garantir a proteção dos ativos da empresa. A proteção dos ativos da empresa envolve a prevenção de atividades maliciosas, como o roubo, a modificação ou a exclusão de dados. Uma falha na segurança do banco de dados pode resultar em danos significativos para a empresa, como perda de dados, violação de privacidade, perda de clientes, danos à reputação e até mesmo ações legais.

Os dados armazenados em um banco de dados podem ser considerados um dos ativos mais valiosos de uma organização, contendo informações sensíveis e estratégicas. Além disso,

a segurança em banco de dados também é fundamental para garantir a disponibilidade dos dados. Uma interrupção do serviço de banco de dados devido a ataques ou falhas de segurança pode impactar negativamente a operação da empresa, causando prejuízos financeiros e atrasos em processos importantes (SOARES, SOARES, ALVES, 2021).

Outro aspecto importante da segurança em banco de dados é a conformidade com regulamentações e leis relacionadas à proteção de dados, onde empresas precisam adotar medidas de segurança adequadas para garantir o cumprimento dessas regulamentações e evitar multas e punições legais.

Existem diversas leis, regulamentações e normas que devem ser seguidas para garantir a privacidade dos dados, como o Regulamento Geral sobre a Proteção de Dados (GDPR) na União Europeia e a Lei Geral de Proteção de Dados (LGPD) no Brasil, onde o descumprimento dessas leis pode resultar em multas e penalidades significativas.

A Lei 13.709/2018, amplamente conhecida como Lei Geral de Proteção de Dados do Brasil, tem por objetivo regularizar e estabelecer diretrizes para a coleta e o tratamento de dados. Essa lei é a mais recente no país e é de extrema importância para proteger a privacidade dos indivíduos e definir como as informações pessoais devem ser utilizadas (CARTOLARI, SILVA, 2019).

Portanto, investir em segurança em banco de dados e garantir a conformidade legal é fundamental para proteger a reputação da empresa, evitar prejuízos financeiros e cumprir com as obrigações legais. Isso envolve o uso de técnicas de criptografia, autenticação de usuários, controle de acesso, monitoramento de atividades suspeitas, backups regulares e atualizações de segurança. Além disso, é importante realizar auditorias internas e externas para garantir a conformidade com as leis e regulamentos aplicáveis (CARTOLARI, SILVA, 2019).

Outro ponto que merece destaque na visão de Cunha (2018) consiste no fato que a segurança em bancos de dados é fundamental para garantir a confiança dos clientes. Os dados armazenados em um banco de dados muitas vezes incluem informações sensíveis e confidenciais dos clientes, como detalhes de pagamento, informações pessoais e registros médicos. Se esses dados forem comprometidos devido a uma falha na segurança, os clientes podem perder a confiança na organização e buscar serviços em outro lugar.

Além disso, a segurança em bancos de dados é vital para prevenir violações de dados. Os *hackers* estão constantemente procurando maneiras de acessar sistemas de banco de dados para roubar informações valiosas. Uma violação de dados pode resultar em perdas financeiras significativas para uma organização, bem como danos à reputação. Investir em medidas de segurança robustas, como criptografia de dados e autenticação de usuário, é essencial para evitar esses tipos de violações (SOARES, SOARES, ALVES, 2021).

Basílio, Oliveira, (2022) enfatizam que a resiliência contra ameaças emergentes também é uma grande preocupação na segurança de bancos de dados. As ameaças cibernéticas estão continuamente evoluindo, e os hackers estão sempre descobrindo novas maneiras e métodos de contornar as medidas de segurança existentes. Portanto, segundo os autores, é crucial que as organizações estejam constantemente atualizando seus sistemas de segurança e adotando medidas proativas para se proteger contra as ameaças emergentes.

2.3. Principais ameaças e ataques cibernéticos

Segundo explica Stallings (2015) ameaça é uma possibilidade de violação da segurança que surge quando há uma circunstância, capacidade, ação ou evento que poderia comprometer a segurança e causar danos. Em outras palavras, uma ameaça implica um potencial perigo de explorar uma vulnerabilidade existente.

Por sua vez, um ataque é uma ação realizada com inteligência e intenção de violar a segurança de um sistema. Isso significa que é um ato deliberado, especialmente no sentido de empregar métodos ou técnicas para contornar os serviços de segurança e violar a política de segurança de um sistema (STALLINGS, 2015). Essa diferenciação se faz necessária, visto que, tanto ameaças, quanto ataques requerem uma abordagem específica na prevenção e na proteção dos sistemas e dados.

Quando se trata de garantir a segurança das informações, é essencial ter conhecimento sobre os principais tipos de ataques cibernéticos e saber como se proteger. Isso se deve ao fato de que essas ameaças podem representar um risco tanto para a empresa interna quanto externamente.

Indivíduos ou grupos com intenções criminosas, políticas ou pessoais realizam ataques

cibernéticos com o propósito de prejudicar ou obter informações sigilosas. Esses ataques têm como objetivo danificar ou obter controle/acesso a documentos e sistemas essenciais em redes de computadores pessoais ou empresariais (DIAS, FARINA, FLORIAN, 2024).

A utilização dos SGBD (sistema de gerenciamento de banco de dados, ou *database* em inglês) tem aumentado exponencialmente desde o seu surgimento, trazendo benefícios como agilidade, organização e economia de recursos no armazenamento de informações. No entanto, esse crescimento também resultou no surgimento de novas vulnerabilidades e falhas de segurança.

Ainda de acordo com Basílio, Oliveira (2022) é observado uma série de padrões frequentes de *ciberataques* voltados para bancos de dados, que se aproveitam de diferentes vulnerabilidades, como falhas operacionais, erros de código, falta de proteção, falhas cometidas por indivíduos, falta de conformidade, entre outros. Esses ataques podem ser resumidos na Tabela 1.

Tabela 1 - Principais ataques cibernéticos

Principais Ataques	Descrição
Phishing	São comunicações fraudulentas disfarçadas para que pareçam verídicas. O objetivo é obter informações confidenciais ou pessoais ou instalação de um malware ou software duvidoso.
Engenharia social	Consiste em uma técnica empregada por criminosos virtuais para induzir usuários desavisados a enviar dados confidenciais, infectar seus computadores com malware ou abrir links para sites infectados.
Privilégios excessivos	O que se define quando usuários, integradores ou aplicativos recebem usuários do banco de dados com privilégios adicionais as suas funções.
Exposição de Mídia	Ocorre a partir do mal armazenamento de mídias de backup, ou controle de acesso à mídia física do servidor, ou ausência de proteção para bancos alocados em nuvem podem ser caracterizados como a exposição de mídia.
Ausência de atualizações	Falhas e vulnerabilidades são descobertas de forma recorrente, o banco de dados e demais softwares devem também ser atualizados a fim de corrigi-las.
Malware	Termo usado para descrever software maliciosos. Os malwares são divididos em *Vírus, Trojan, Spyware, Worms, Ransoware, Adwaree Botnets*.

SQL *Injection*	É uma técnica para que sejam injetadas consultas ou comandos maliciosos no banco de dados disfarçados como uma variável, adquirida através de campos editáveis de texto.
Ransomware	Ocorre quando uma pessoa acessa um site sem segurança ou abre anexos de e-mails não confiáveis, resultando em um programa malicioso que toma conta do computador e exige um resgate para a devolução da máquina ou informações.
Cavalo de Troia	Consiste em um tipo de ataque inspirado na história da Guerra de Troia, em que os criminosos enviam mensagens enganosas oferecendo brindes ou presentes, mas que contêm um malware oculto. Isso resulta em perda de arquivos e acesso não autorizado a informações confidenciais.
Ataques de força bruta	São táticas usadas para invadir sistemas através de tentativas repetitivas de descobrir nomes de usuário e senhas
Spoofingo	Se configura em um ataque em que a identidade de uma pessoa ou empresa é falsificada, geralmente através de invasões no sistema operacional.
Cryptojacking	É uma ameaça direcionada a empresas que utilizam moedas digitais, em que os invasores tentam acessar as criptomoedas armazenadas

Fonte: Os autores (2024)

Carvalho (2009) enfatiza que, devido à variedade dos sistemas, ao aumento do número de usuários e de aplicativos, e ao consequente aumento das ameaças, a importância da Segurança da Informação tem se tornado cada vez mais significativa nas organizações. Todavia, acrescenta o autor que é necessário entender certos aspectos para realizar uma avaliação precisa dos possíveis riscos ou ameaças aos quais a empresa pode estar sujeita.

No geral, os ataques cibernéticos são ações empreendidas por criminosos virtuais na tentativa de obter acesso a um objeto virtual ou causar a sua indisponibilidade ao seu proprietário (BASILIO, OLIVEIRA, 2022).

2.4. Estudos de caso de ataques a bancos de dados

Ataques de injeção SQL são uma séria ameaça à segurança da informação, podendo afetar a confidencialidade, integridade e disponibilidade dos dados. Nesse contexto a pesquisa

de Pereira, Pelli, Pereira, (2024) buscou realizar um estudo de caso, aplicando de forma ética, técnicas de ataque de injeção SQL em sistemas web. Os autores analisaram o caso OWASP (é uma comunidade aberta dedicada a possibilitar que as organizações projetem, desenvolvam, adquiram, operem e mantenham software para aplicações seguras que possam ser confiáveis.). Em 2023, a OWASP identificou vulnerabilidades relacionadas a esse tipo de ataque em 94% das aplicações analisadas, totalizando 274 mil ocorrências.

Foram utilizados dois sistemas, incluindo um proveniente da cidade de Diamantina, além do site http://testphp.vulnweb.com, para testar formas de detecção e prevenção para esse tipo de ataque. A ferramenta SQLmap foi utilizada para automatizar a detecção e exploração das vulnerabilidades.

Os resultados mostraram que essas técnicas de ataque permitem que um invasor manipule, exclua, extraia ou duplique dados dos servidores do banco de dados em sistemas que não possuem medidas de segurança adequadas. Segundo Pereira, Pelli, Pereira, (2024), para prevenir ataques de injeção SQL, é essencial implementar a validação dos dados do usuário, configurar permissões apropriadas e evitar a exposição de mensagens de erro detalhadas aos usuários.

Em conclusão, o estudo demonstrou que os ataques de injeção SQL representam uma ameaça significativa à segurança das aplicações web, comprometendo a privacidade e integridade dos dados.

Outro ataque que chama atenção consiste no caso da Sony PlayStation Network (2011): O PlayStation Network, serviço online da Sony para jogos de console, foi vítima de um ataque que comprometeu as informações pessoais de cerca de 77 milhões de usuários. Os dados roubados incluíam nomes, endereços, senhas e até mesmo informações de cartões de crédito.

A Sony divulgou que mais de 77 milhões de usuários do PlayStation Network tiveram suas informações pessoais acessadas por um hacker. A empresa não descartou o roubo de dados de cartão de crédito e pediu aos usuários que verifiquem suas contas. Dados como nome, endereço, e-mail, data de nascimento, histórico de compras, endereço de cobrança e senhas foram acessados.

A invasão ocorreu entre 17 e 19 de abril de 2011 e a Sony contratou uma empresa de

segurança para investigar o caso. A empresa recomendou que os usuários trocassem logins e senhas quando o serviço fosse restabelecido. O impacto dessa invasão se mostrou desastroso para a imagem da empresa.

Após analisar os casos anteriormente, a questão que fica é: Como se prevenir de ataques cibernéticos?

Existem diversas táticas para evitar ataques cibernéticos, tais como implementar medidas de segurança da informação, adquirir um firewall confiável, utilizar uma rede privada virtual (VPN), capacitar a equipe para reconhecer ameaças, evitar conectividade com dispositivos desconhecidos e utilizar a computação em nuvem para garantir uma cópia segura dos dados. Essas medidas são cruciais para manter a empresa em posição competitiva no mercado (STEFANINIGROUP, 2021)

Segundo Silva, Alves Júnior, Santana, (2022) a segurança do banco de dados é fundamental para proteger os dados corporativos e evitar ataques cibernéticos. Métodos como o uso de SGBDs, controle de acesso, certificados digitais e criptografia ajudam a mitigar possíveis ataques. Os mecanismos de segurança discricionários e obrigatórios são utilizados para conceder permissões aos usuários e reforçar a segurança com base na classificação dos dados e usuários.

Além disso, a concessão cuidadosa de privilégios administrativos aos usuários do banco de dados é importante para evitar violações de dados, sendo necessário escolher um bom banco de dados, como o PostgreSQL, que oferece segurança e estabilidade. Ainda para os supramencionados autores, as formas como os comandos SQL são utilizadas também deve ser cuidadosa para evitar ataques de injeção de SQL. A segurança do banco de dados é essencial para a sobrevivência e competitividade das empresas no mercado.

O estudo de Basilio, Oliveira (2022) teve por objetivo descobrir e apresentar recursos que visam proteger bancos de dados, com foco principal na prevenção de ataques de SQL *Injection*. Esses recursos incluem medidas como autenticação e autorização baseadas em credenciais e níveis de acesso diferenciados, criptografia de dados, configuração de consultas com parâmetros, uso de consultas pré-armazenadas, backups e armazenamento seguro, entre outros.

Para os autores, essas são as cinco ferramentas, conforme apresentada na Tabela 2, para segurança do banco de dados:

1) Credenciais e Níveis Diferentes de Acesso: o uso de diferentes níveis de controles de acesso, como permissões e negação de privilégios, permite que cada usuário tenha acesso apenas ao necessário.

2) Criptografia de Dados: a criptografia protege as informações por meio do uso de códigos, garantindo que apenas pessoas autorizadas possam ler e processar os dados.

3) Stored Procedure: é um conjunto de instruções em T-SQL que fica armazenado no banco de dados de forma pré-compilada, permitindo reutilização e economia de recursos.

4) Backup: consiste em fazer uma cópia do banco de dados em um momento específico, como medida de segurança em caso de problemas.

5) Ocultação de Mensagens de Erros: garantir que as mensagens de erro sejam genéricas e não forneçam informações sensíveis que possam ser exploradas por invasores.

Tabela 2 - Principais ferramentas contra ataques

Credenciais e Níveis Diferentes de Acesso	O uso de diferentes níveis de controles de acesso, como permissões e negação de privilégios, permite que cada usuário tenha acesso apenas ao necessário.
Criptografia de Dados	A criptografia protege as informações por meio do uso de códigos, garantindo que apenas pessoas autorizadas possam ler e processar os dados.
Stored Procedure	É um conjunto de instruções em T-SQL que fica armazenado no banco de dados de forma pré-compilada, permitindo reutilização e economia de recursos.
Backup	Consiste em fazer uma cópia do banco de dados em um momento específico, como medida de segurança em caso de problemas.
Ocultação de Mensagens de Erros	Garantir que as mensagens de erro sejam genéricas e não forneçam informações sensíveis que possam ser exploradas por invasores.

Fonte: Os autores (2024)

Além dessas ferramentas, Basílio, Oliveira (2022) destacam outras práticas importantes, são as atualizações de sistemas para corrigir falhas, validação de entradas de formulários para evitar injeções de SQL, registro de transações em logs de banco de dados, auditoria para verificar conformidade e testes de vulnerabilidade e monitoramento do banco de dados e ambientes.

A pesquisa de Marques e Cruz (2021) buscou esclarecer questões pertinentes à segurança em banco de dados, procurando entender a relevância da segurança em banco de dados para uma empresa, bem como, esclarecer de que forma é possível garantir a confidencialidade, integridade e disponibilidade da informação de acordo com a política de segurança.

Para os supramencionados autores, a importância da segurança em banco de dados consiste em apresentar medidas de prevenção a informações e com o crescente avanços tecnológicos tem se notado grande melhoras no gerenciamento de segurança da informação, isso porque as informações são a maior riqueza das empresas e pessoas, e mantê-las de forma correta e segura é primordial.

Os acontecimentos de invasões estão sujeitos a serem realizados a qualquer momento, empresas e pessoas precisam estar sempre atentos a esses tipos de ataques e diante disso, a importância da segurança em banco de dados está para auxiliar e também direcionar de forma correta a como estar protegido.

Manter a segurança não é um trabalho fácil de ser feito, pois requer conhecimentos, altos investimentos, e dedicação e no referido estudo foi possível identificar que utilizando os métodos corretamente, mantendo os dispositivos sempre atualizados, procurar através de equipes qualificadas garantir os principais conceitos de integridade das informações, disponibilidade e a confidencialidade é possível obter resultados satisfatórios e prevenir das despesas com a percas de informações.

Ainda quanto à importância da segurança em banco de dados e da necessidade de medidas proativas para proteger informações sensíveis, Cabral e Caprino (2015) entendem que a segurança da informação busca primordialmente a gestão de risco, que pode ser definido de diversas maneiras em diferentes disciplinas, mas, de forma geral, como a probabilidade e

potencial magnitude de perda futura.

Nesse sentido, os autores defendem que o primeiro passo para uma gestão adequada de riscos é identificá-los. Em seguida, é necessário analisá-los e definir qual ação adotar, sendo que as sugestões incluem:

a) mitigar o risco, o que envolve tomar precauções para reduzi-lo, geralmente diminuindo vulnerabilidades, e requer um monitoramento frequente para acompanhar as probabilidades de causar danos à organização;

b) aceitar o risco, quando este não representa uma ameaça direta ou é aceitável para a organização, o que leva a empresa a prosseguir sem adotar nenhuma medida em relação ao risco;

c) transferir o risco, que consiste em terceirizar alguns riscos, independentemente de sua magnitude, sendo uma opção a contratação de seguros, por exemplo.

Diante desse cenário segundo Cunha (2018) a segurança em banco de dados é extremamente importante devido ao armazenamento das informações de uma empresa e requer cuidados especiais. Diante disso, é necessário adotar uma lista rigorosa de métodos e práticas para garantir a integridade das informações. Nesse contexto, é importante lembrar que o conceito de segurança em banco de dados é padrão, embora as estruturas dos sistemas de gerenciamento de banco de dados possam variar.

Sendo assim, a segurança da informação deve considerar os pilares da confidencialidade, integridade e disponibilidade. A vulnerabilidade de uma estrutura de banco de dados pode ser examinada por meio de auditorias, que identificam possíveis brechas e propõem medidas para manter as informações segura (CUNHA, 2018).

De acordo com Borchert, (2019) para garantir a proteção das informações é importante implementar políticas de controle de acesso, que determinem quem pode acessar e modificar os dados armazenados no banco de dados. Além disso, é fundamental adotar medidas de segurança física, como proteção contra incêndio e cópias de segurança, para prevenir a perda de dados.

Outra medida essencial segundo o autor é a criptografia dos dados, que garante que apenas pessoas autorizadas possam visualizá-los, sendo também importante realizar auditorias

e monitoramentos regulares do banco de dados, a fim de identificar possíveis ataques e vulnerabilidades.

Ainda para garantir a segurança das informações armazenadas em um banco de dados, Borchert, (2019) acrescenta que é necessário implementar medidas como monitoramento e detecção de ataques, criptografia de dados, backup e recuperação de dados, e atualizações e patches de segurança. Essas medidas são essenciais para proteger as informações valiosas e sensíveis de uma empresa ou de seus clientes, minimizando o risco de divulgação não autorizada, perda de dados e danos à reputação da empresa

Por fim, destaca o autor ser fundamental educar e conscientizar os funcionários sobre a importância da segurança da informação e a importância de seguir as diretrizes e políticas estabelecidas pela empresa. Essas medidas em conjunto garantem a proteção efetiva das informações e a segurança do banco de dados e entende que a segurança não deve ser vista apenas como um mecanismo de proteção, mas como um elemento que permite a execução dos negócios da empresa.

Por ser um ativo valioso, a informação está sujeita a ameaças e precisa ser protegida. O autor ainda sugere a realização de pesquisas futuras em bancos de dados de código aberto para entender como a comunidade lida com a segurança da informação. Isso é especialmente importante para organizações que não possuem licenças de bancos de dados e funcionários especializados nessa área (BORCHERT, 2019).

3. Metodologia

No que diz respeito à abordagem de pesquisa, ela é definida basicamente como pesquisa qualitativa. Este ensaio considera o estudo exploratório e explicativo que visa criar maior familiaridade com o problema para torná-lo mais explícito.

Foram selecionados trabalhos por meio de pesquisa bibliográfica, com o corte temporal a partir de estudos em artigos científicos e teses desenvolvidas de 2009 a 2024 publicados nas bases biblioteca digital de teses e dissertações (BDTD), Capes Scielo. Todavia, houve a necessidade de ampliação do corte temporal, face a necessidade de inclusão de alguns autores, que se fazem pertinentes ao estudo ora proposto. As obras pesquisadas foram nos idiomas,

inglês, português e espanhol.

Os textos foram examinados com rigor, considerando critérios como a coerência teórica, a solidez da fundamentação metodológica em relação aos objetivos do estudo.

4. Resultados e Discussões

Através da análise dos dados coletados e dos estudos de caso apresentados, foi possível observar que os ataques de SQL *injection* e os vazamentos de dados continuam sendo as ameaças mais comuns contra bancos de dados. A exploração de falhas de segurança em sistemas de autenticação e a falta de criptografia adequada foram identificadas como as principais vulnerabilidades (Pereira, Pelli, Pereira, 2024).

Os resultados encontrados no presente estudo corroboram com os estudos de Pereira, Pelli, Pereira, (2024) que apontam o SQL *injection* como a técnica mais explorada por atacantes. Os estudos levantados para a pesquisa em questão levantaram artigos feitos por autores diferentes, revelando que bancos de dados mal configurados, especialmente aqueles que não utilizam validação de entrada adequada, apresentaram maior vulnerabilidade e probabilidade de ataques.

Embora o estudo tenha revelado as vulnerabilidades críticas em bancos de dados relacionais, uma limitação importante é a falta de análise de bancos de dados NoSQL, que estão ganhando popularidade em muitas organizações. Futuros estudos poderiam expandir a análise para incluir diferentes tipos de banco de dados e comparar a eficácia das técnicas de segurança em cada contexto.

Em resumo, a pesquisa confirma que a segurança em bancos de dados é um desafio contínuo e exige a implementação de múltiplas camadas de proteção. Organizações devem priorizar o uso de criptografia, controle de acesso robusto e a validação de entradas para mitigar os riscos de ataques. As vulnerabilidades em bancos de dados não são apenas uma preocupação técnica, mas têm sérias implicações para a privacidade dos dados e para a confiança dos clientes.

5. Considerações Finais

A segurança em banco de dados é de extrema importância para proteger as informações sensíveis de uma organização. O aumento dos ataques cibernéticos e a exposição cada vez maior

de dados valiosos tornam essas medidas de segurança proativas essenciais. Os bancos de dados são alvos constantes de invasões, podendo resultar em danos significativos para as empresas, como o vazamento de informações estratégicas, perda de dados e prejuízos financeiros.

Diante disso, é fundamental adotar medidas proativas e eficientes para proteger o banco de dados, como o uso de tecnologias de criptografia, controle de acesso, autenticação de usuários, backups regulares e atualizações de segurança. Além disso, é importante implementar políticas de segurança da informação, treinar e conscientizar os funcionários sobre a importância da proteção de dados e garantir a conformidade com as leis e regulamentos aplicáveis.

A falta de segurança em banco de dados pode trazer consequências graves para uma organização, como perda de reputação, confiança dos clientes e ações legais. Por outro lado, investir em medidas eficazes de segurança da informação pode trazer benefícios, como proteção de dados sensíveis, conformidade com normas regulatórias e vantagem competitiva no mercado.

No entanto, é importante lembrar que a segurança em banco de dados não é um processo único, mas sim um esforço contínuo e sistemático que requer atualizações constantes e a adoção de medidas de proteção adequadas. É necessário monitorar e avaliar regularmente o sistema de segurança, identificar possíveis ameaças e vulnerabilidades e implementar as ações corretivas necessárias.

Em resumo, a segurança em banco de dados é essencial para garantir a proteção das informações valiosas de uma organização, minimizando riscos, prevenindo ataques cibernéticos e garantindo a confidencialidade, integridade e disponibilidade dos dados. Investir em medidas de segurança eficazes e adotar uma abordagem proativa é fundamental para proteger a reputação da empresa, evitar prejuízos financeiros e cumprir com as obrigações legais.

As futuras pesquisas devem se concentrar no aprimoramento de algoritmos de criptografia, particularmente em relação ao impacto no desempenho e à escalabilidade de sistemas de grande volume de dados. Além disso, a inteligência artificial e o aprendizado de máquinas para detectar intrusões e responder a incidentes é uma área promissora que pode aumentar significativamente a capacidade de resposta a ataques cibernéticos em tempo real.

Referências

ALCARAZ, Paulo Cesar Fernandez. Desenvolvimento de uma política de segurança para uma empresa real. 2018. 41 p. Monografia de Especialização em Configuração e Gerenciamento de Servidores e Equipamentos de Redes, Departamento Acadêmico de Eletrônica, Universidade Tecnológica Federal do Paraná. Curitiba, 2018

BASILIO, Guilherme Manfrim DE OLIVEIRA, Wdson de . Ferramentas de segurança para banco de dados: focando em SQL Injection. Revista Brasileira em Tecnologia da Informação, [S. l.], v. 4, n. 2, p. 10 - 19, 2022. Disponível em: https://www.fateccampinas.com.br/rbti/index.php/fatec/article/view/76. Acesso em: 5 set. 2024

BORCHERT, Antonio Marcos. Banco de dados: Vulnerabilidade na Segurança. 2019. 27 páginas. Ciência da Computação – UNIDERP, Campo Grande, 2019 .Disponível em: https://repositorio.pgsscogna.com.br/bitstream/123456789/30213/1/ANTONIO_MARCOS_BORCHERT_VERS%C3%83O_FINAL.pdf. Acesso em: 7 set. 2024.

CABRAL, Carlos. O que o vazamento do Marriott nos ensina sobre ataques persistentes. Por Carlos Cabral. 2018. Disponível em: https://cryptoid.com.br/ciberseguranca-seguranca-da-informacao/o-que-o-vazamento-do-marriott-nos-ensina-sobre-ataques-persistentes-por-carlos-cabral-da-tempest/. Acesso em: 7 set.2024.

CARTOLARI, Lucas Rabello. SILVA, Danilo Pierote. A lei geral de proteção de dados como ferramenta de proteção dos direitos fundamentais. Fundação de Ensino Eurípides Soares da Rocha, Marília, São Paulo;

CARVALHO, Rodrigo de Oliveira. Segurança da informação nas organizações / Rodrigo de Oliveira Carvalho. - - Brasília: UniCEUB, 2009. 39 f. : il. ; 29,7 cm. Orientadora: MSc Mariângela Abrão TCC (graduação) – Centro Universitário de Brasília, FATECS, Administração, 2009.

CABRAL, Carlos; CAPRINO, William. **Trilhas em Segurança da Informação:** Caminhos e ideias para a proteção de dados. Rio de Janeiro: Brasport, 2015.

CAMPOS, Fábio da Silva Viana. **Uma abordagem a segurança em banco de dados**

/ Fábio da Sil- va Viana Campos. – Assis, 2018. 88p. Trabalho de conclusão do curso (Análise e Desenvolvimento de Sistemas). – Fundação Educacional do Município de Assis-FEMA. Disponível em: https://cepein.femanet.com.br/BDigital/arqTccs/1611320139.pdf. Acesso em 15 ago. 2024.

CUNHA, Welliton Sousa Da. **Segurança em banco de dados:** métodos de prevenção contra possíveis falhas e ataques. IMPERATRIZ – MA 2018. Trabalho de Conclusão de Curso – Artigo Cientifico. Disponível em: https://www.academia.edu/37713600/SEGURAN%C3%87A_EM_BANCO_DE_DADOS_M%C3%89TODOS_DE_PREVEN%C3%87%C3%83O_CONTRA_POSS%C3%8DVEIS_FALHAS_E_ATAQUES. Acesso em 14 ago. 2024.

DIAS, Jhonatan Rodrigues Guzella. FARINA, Renata Mirella .FLORIAN, Fabiana. **Segurança cibernética** - estudo das técnicas de ataques cibernéticos (phishing, ransmware, ddos) de engenharia social e medidas de prevenção. FORTALEZA-CE. EDIÇÃO 248. V.12. ANO 2024. Revista Científica Semana. Fortaleza-CE. EDIÇÃO 248. V.12. ANO 2024. Disponível em: https://semanaacademica.org.br/system/files/artigos/seguranca_cibernetica_-_estudo_das_tecnicas_de_ataques_ciberneticos_phishing_ransmware_ddos_de_engenharia_social_e_medidas_de_prevencao_0.pdf. Acesso em 30 ago. 2024.

FERREIRA, Fernando Nicolau Freitas; ARAUJO, Márcio Tadeu de. **Política de segurança da informação**: Guia prático para elaboração e implementação. 2 ed. Rio de Janeiro: Ciência Moderna, 2008.

GAIDARGI. Juliana. **Erros que comprometem a segurança do seu banco de dados**, INFONOVA, 2021. Disponível em: (https://www.infonova.com.br/seguranca/errosseguranca-banco-dados/). Acesso em: 2 set. 2024.

LGPD & PRIVACY, **Marriott sofre segunda violação, expondo dados de 5,2 milhões de hóspedes**.2020. Disponível em: https://minutodaseguranca.blog.br/marriott-sofre-segunda-violacao-expoe-dados-de-52-milhoes-de-hospedes/. Acesso em 23 ago. 2024

MATIOLI, D. C. **Importância da segurança em banco de dados.** 2010. 55f. Trabalho de Conclusão de Curso -Fundação Educacional do Município de Assis, Assis, 2010.

MARQUES, Gleice Ferreira. CRUZ, Rafael Cardoso Costa. **Importância da**

Segurança em Banco de Dados. Revista De Tecnologia Invest. Volume 5, número 1, dezembro de 2021. Disponível em: http://revista.institutoinvest.edu.br/index.php/revistainvest/article/view/43/37. Acesso em: 12 set. 2024.

NUNES, Bianca Pivetta. MARQUES, Mariana da Rocha. **"Ciberataque" enquanto uma análise da proteção de dados pessoais na internet**: estudo de caso sobre o ataque cibernético no hospital de câncer de Barretos (SP). Anais do 5º Congresso Internacional de Direito e Contemporaneidade: mídias e direitos da sociedade em rede (2019) https://www.ufsm.br/cursos/pos-graduacao/santa-maria/ppgd/congresso-direito-anais. Disponível em: https://www.ufsm.br/app/uploads/sites/563/2019/09/5.22.pdf. Acesso em 12 set. 2024

PEREIRA, Eva Francisca; PELLI, Eduardo; PEREIRA, Eva Francisca. **Estudo De Caso:** Aplicação E Avaliação De Técnicas De Detecção E Prevenção De Ataques De Injeção SQL... In: . Disponível em: https//www.even3.com.br/anais/sintegra/746353-estudo-de-caso--aplicacao-e-avaliacao-de-tecnicas-de-deteccao-e-prevencao-de-ataques-de-injecao-sql. Acesso em: 5 set. 2024.

ROTHKE, Ben. **Nove lições de segurança aprendidas com a violação de dados da Equifax**. Senior Security Consultant, Nettitude. 2019. Disponível em: https://www.beyondtrust.com/pt/blog/entry/9-infosec-lessons-from-the-equifax-data-breach. Acesso em: 30 ago. 2024

SANTOS, Rogério Batista dos. SILVA, Tiago Barros Pontes e. **Gestão da segurança da informação e comunicações análise ergonômica para avaliação de comportamentos inseguros**. RDBCI: Rev. Dig. Bibliotec e Ci. Info. / RDBCI: Dig. J. of Lib. and Info. Sci.| Campinas, SP | v.19| e021024 | 2021

SÊMOLA, M. **Você já fez uma análise de riscos de verdade?** Rio de Janeiro, n. 41, jun. 2002. Disponível em: http://www.semola.com.br/disco/Coluna_IDGNow_41.pdf . Acesso em: 7 set. 2024.

SILVA, Chryslayny Thays Dos Santos. ALVES JÚNIOR, Cleyton Fausto. SANTANA, Marcos Alexandre Melo Alves. **Segurança de redes nos bancos de dados**. Recife: O autor,

2022. 34 p. Trabalho de conclusão de curso (graduação) - Centro Universitário Brasileiro – UNIBRA. Tecnólogo em Redes de Computadores, 2022. Disponível em: https://www.grupounibra.com/repositorio/REDES/2022/seguranca-de-redes-nos-bancos-de-dados13.pdf. Acesso em 14 ago. 2024

SOARES, Sória Pereira Lima. SOARES, Augusto Cezar da Silva . ALVES, Aldo Agustinho. **A importância da implementação de uma política de segurança da informação**. Brazilian Journal of Development, Curitiba, v.7, n.4, p. 37162-37171 apr 2021. Disponível em: https://ojs.brazilianjournals.com.br/ojs/index.php/BRJD/article/download/28009/22181/71917 . Acesso em: 15 ago. 2024.

STEFANINI, GROUP. **Tudo sobre segurança da Informação**! Confira nosso guia completo do assunto. Stefanini. 2021. Disponível em: https://stefanini.com/pt- 34 br/trends/artigos/guia-sobre-seguranca-da-informacao. Acesso em: 2 set. 2024.

STALLINGS, William. **Criptografia e segurança de redes**: Princípios e práticas. 6. ed. São Paulo: Pearson, 2015.