CENTRO UNIVERSITÁRIO FEI

JOÃO PEDRO ROSA CEZARINO - R.A: 22.120.021-5

HUGO LINHARES OLIVEIRA - R.A: 22.120.046-2

VITOR MARTINS OLIVEIRA - R.A: 22.120.067-8

THALES LACERDA OLIVEIRA - R.A: 22.120.056-1

SEGURANÇA EM BANCO DE DADOS: Workshop

São Bernardo do Campo

2022

SUMÁRIO

1	**INTRODUÇÃO**	3
2	**A SEGURANÇA DA INFORMAÇÃO**	3
3	**OS BANCOS DE DADOS**	4
4	**A HISTÓRA DA SEGURANÇA EM BANCOS DE DADOS**	5
5	**PRINCIPAIS VULNERABILIDADES E VETORES**	6
6	**ESTRATÉGIA DE APRESENTAÇÃO**	7
	REFERÊNCIAS	8

1 INTRODUÇÃO

O tema escolhido pelo grupo é “Segurança em Banco de Dados”. Tema este, que discorre acerca da segurança durante o uso, configuração e desenvolvimento dos mais diversos modelos de bancos de dados existentes atualmente. À medida que as grandes empresas aumentam sua confiança em sistemas distribuídos, elas, consequentemente, tornam-se cada vez mais vulneráveis à falhas de segurança, ainda que haja um aumento na produtividade e eficiência nas atividades do dia a dia.

2 A SEGURANÇA DA INFORMAÇÃO

Em primeiro plano, é importante definirmos o conceito de segurança no meio da Tecnologia da Informação. A segurança da informação é conhecida como a prática que protege computadores, servidores, dispositivos móveis, sistemas eletrônicos, softwares, redes e dados contra ataques maliciosos e acessos indesejados.

A Confidencialidade, Integridade e Disponibilidade(Tríade ‘CIA’) são os 3 pilares que dão suporte à segurança da informação. Ambos os pilares têm a importante função de assegurar a confiabilidade das informações que serão disponibilizadas. A confidencialidade garante a restrição do acesso à informação por usuários não previamente autorizados. A Integridade é responsável por garantir que a informação esteja completa e exata, sem modificações inesperadas. Por fim, a Disponibilidade fica responsável por garantir que a informação esteja acessível e utilizável sempre que necessário.

Os 3 pilares mencionados acima, aparecem praticamente em qualquer ambiente de software presente no cenário atual. Como exemplo, podemos considerar um sistema de reserva de uma companhia aérea: É imprescindível que as reservas dos consumidores sejam apenas acessíveis aos consumidores à que elas se referem, que a reserva de um consumidor não seja modificada sem prévio aviso e que as informações do voo e da reserva estejam sempre disponíveis ao consumidor.

Com a utilização de softwares e sistemas cada vez mais avançados e distribuídos, as falhas de segurança tem tornado-se cada vez mais recorrentes e corriqueiras. Uma falha de segurança é classificada como qualquer incidente que resulte em acesso não autorizado a dados, aplicativos, redes e dispositivos. Falhas como: erros durante a configuração do sistema, fracas políticas de segurança, má conscientização do usuário, desenvolvimento não seguro de software, controle de

acesso mal distribuído e etc, podem resultar em incidentes de segurança de escala inimaginável, podendo impactar o serviço disponibilizado, os clientes atendidos, o lucro da empresa e até, em certos casos, a vida de pessoas que utilizam o serviço afetado.

Embora o constante crescimento e sofisticação da Internet e dos sistemas distribuídos tenha trazido uma grande melhora na eficiência e no uso do tempo, a crescente dependência de mais e mais serviços à um banco de dados aumenta ainda mais os riscos aos quais estes Bancos de Dados estão sujeitos. Devido a isso, a segurança dos dados presente nestes bancos, tem tornado-se mais crucial do que jamais antes visto, tornando os BD's importantes ativos a serem protegidos.

3 OS BANCOS DE DADOS

"Um banco de dados é uma coleção de dados relacionados- (Elmasri e Navathe [3]). Com dados, queremos dizer fatos conhecidos que podem ser registrados e possuem significado implícito. Um Banco de Dados nada mais é do que uma coleção organizada de informações, que geralmente é armazenada de forma eletrônica. Com o advento dos mais diversos sistemas e um crescimento exponencial da quantidade de dados produzidos e trafegados, os bancos de dados tiveram sua importância destacada no cenário da tecnologia mundial.

Para melhor gerenciar um Banco de Dados, criaram-se os sistemas gerenciadores de banco de dados (SGBD — Sistema de Gerenciamento de Banco de Dados), que são uma coleção de programas que permitem aos usuários criar e manter um banco de dados - (Elmasri e Navathe [3]). O SGBD é um sistema de software de uso geral que facilita o processo de definição, construção, manipulação e compartilhamento entre diversos usuários e aplicações.

A correta organização dos dados e informações através do uso de um BD, ajudam não só a melhor experiência por parte do usuário, mas também asseguram diversos benefícios a maioria das organizações, como por exemplo: Potencial para garantir padrões, Tempo reduzido para desenvolvimento de aplicações, Flexibilidade, Escalabilidade, Disponibilidade de informações, Redundância(Backups) e até Reduções de Gastos.

Desta forma, fica evidente que, os Bancos de Dados possuem uma elevada relevância dentro da lista de ativos de uma organização, por serem parte integral da grande maioria dos sistemas e carregar em seu interior dados sensíveis à empresa. Por isso, proteger e garantir a segurança de uma base de dados é uma das principais tarefas em uma política de Segurança da Informação.

4 A HISTÓRA DA SEGURANÇA EM BANCOS DE DADOS

A importância da garantia da Segurança em Bancos de Dados têm tomado notável relevância, ano após ano, já que a maioria dos serviços prestados por empresas têm se digitalizado. Nos últimos trinta anos, a Tecnologia da Informação sofreu incontáveis avanços e os pesquisadores de segurança buscaram sempre ficar um passo à frente das ameaças que poderiam comprometer a segurança dos Bancos de Dados, já que, a medida que estes ficaram cada vez mais modulares e sofisticados, os atacantes foram apresentados à novos vetores para condução de um ataque.

Em torno de 1980, as organizações governamentais , como o Departamento de Defesa Americano(DOD), foram as primeiras a dar uma relevada importância à segurança em Bancos de Dados, já que, naquela época, seus databases continham dados cruciais como informações militares e dados censográficos. Em contrapartida, as organizações e a população em geral não tinham tanta preocupação com o tema, já que poucos tinham acesso a esta tecnologia e havia um número ínfimo de vulnerabilidades identificadas.

No período de 1981 – 1990, as aplicações comerciais utilizando sistemas de Bancos de Dados espalharam-se pelo mundo, devido aos benefícios oferecidos por este tipo de sistema. A atenção dos atacantes foi então despertada e ataques improvisados buscando a exploração de vulnerabilidades tornaram-se mais recorrentes. Foi também neste período que os Bancos de Dados começaram a ser armazenados em outros pontos da rede, seguindo a arquitetura Cliente-Servidor. O foco no controle de acessos e na criptografia eram importantes tópicos discutidos nestes anos.

De 1991 até 2000, o ambiente digital passou por uma transformação massiva devido à expansão dos comércios em geral. A criação do “Windows Browser” juntamente da percepção de que a então World Wide Web poderia ser usada para fins além do compartilhamento de informações trouxe um impacto tremendo na exposição dos dados e informações. Usuários comuns, sem conhecimento da tecnologia envolvida, passaram a ser os principais consumidores dos Bancos de Dados e a restrição dos acessos passou a ser mais rigorosa. Neste período, alguns mecanismos de defesa como os Firewalls surgiram, numa tentativa de prevenção de acessos indesejados aos databases.

Após o ano de 2001, as informações pessoais tornaram-se publicamente disponíveis com o advento das redes sociais e a disponibilização de diversos dados públicos. A criptografia tornou-se cada vez mais comum em todos os dados trafegados, até mesmo nos armazenados nos Bancos de Dados. A autenticação dos usuários foi melhorada gradativamente, devido à

exploração de aplicações Web que faziam um intermédio com as bases de dados. Este período foi marcado por uma expansão dos ataques a sistemas de TI, já que os atacantes agora possuíam ferramentas e conhecimentos profundos e refinados acerca dos sistemas até então desenvolvidos. A privacidade e proteção de dados começam a tornar-se um assunto importante no meio da tecnologia,

Atualmente, percebe-se que muitos dos problemas que concernem armazenamento de dados, são causados por falta de políticas de segurança durante a implementação e configuração das Bases de Dados. A descentralização do armazenamento e os imensos volumes de dados produzidos têm trazido grandes desafios aos especialistas, assim como emergido novas vulnerabilidades nunca antes imaginadas. Por outro lado, uma noção de segurança em conjunto tem se desenvolvido através de políticas de restrição de uso de dados, como a LGPD e a GDPR e a adoção dos conceitos de segurança desde as primeiras etapas do desenvolvimento de um software.

5 PRINCIPAIS VULNERABILIDADES E VETORES

É evidente que os dados são o ativo mais importante de uma empresa, assim como dito por Clive Humby: “Os dados são o novo petróleo”. Mundialmente, milhões de empresas geram dados a respeito de suas atividades e seus clientes e estes dados são armazenados em enormes Bancos de Dados, tornando-se suscetíveis a diversas formas de ataques, acessos indesejados e vazamentos.

A segurança dos Bancos de Dados deve começar na esfera física. Por isso, apenas funcionários expressamente permitidos devem poder ter acesso à infraestrutura do Banco de Dados, seja ela o próprio servidor ou Data Center. Porém, existem outros riscos internos e externos que podem comprometer a segurança de um Banco de dados, alguns estão mencionados abaixo:

a) Falta de Configuração do Banco de Dados;
b) Autenticação fraca;
c) Usuários com privilégios excessivos;
d) Vulnerabilidades no protocolo de comunicação;
e) Exposição de Backups;
f) Dados sensíveis não gerenciados;
g) SQL Injections;

h) Denial of service attacks;

i) Malwares.

Apesar de os Bancos de Dados estarem abertamente vulneráveis à uma lista de ataques e falhas, é possível reduzir as chances de um ataque e/ou vazamento de dados focando nos principais riscos listados acima.

6 ESTRATÉGIA DE APRESENTAÇÃO

Para demonstrar a importância da segurança nos Bancos de Dados atuais e explicar mais profundamente o tema à turma, o grupo optou por criar um conjunto de slides para guiar uma apresentação oral sobre o tema. Para a parte prática, as vulnerabilidades de SQL Injection e Denial of Service(DOS) serão demonstradas no dia à turma, em um ambiente controlado e apartado, criado especialmente para a demonstração. O banco de dados escolhido para a demonstração foi o MySQL.

Alguns tópicos importantes estão elencados abaixo e serão norteadores para a apresentação:

a) A história e importância dos Bancos de Dados;

b) A segurança da informação;

c) A segurança da informação aplicada aos Bancos de Dados;

d) 9 Vulnerabilidades conhecidas;

e) Possíveis correções para as vulnerabilidades elencadas.

Deste modo, a apresentação se conclui e demonstra todo o caminho percorrido desde a importância dos Bancos de Dados até a importância de se garantir a segurança nos Bancos de Dados atualmente, passando por uma demonstração de um ataque real e concluindo com possíveis correções para falhas de segurança observadas atualmente.

REFERÊNCIAS

[1] Shulman Amichai. “Top Ten Database Security Threats”. Em: *Imperva, Inc* (2006), pp. 1–14. Disp. em: https://schell.com/Top_Ten_Database_Threats.pdf.

[2] E. Bertino e R. Sandhu. “Database security - concepts, approaches, and challenges”. Em: *IEEE Transactions on Dependable and Secure Computing* 2.1 (2005), pp. 2–19. DOI: 10.1109/TDSC.2005.9.

[3] Ramez Elmasri e Shamkant B. Navathe. *Sistemas de banco de dados*. v. 6. Pearson Education do Brasil, 2011. ISBN: 9788543013817.

[4] Kaspersky. *Centro de Recursos Kaspersky*. Last accessed on 2022-09-21. Disp. em: https://www.kaspersky.com.br/resource-center.

[5] Paul Lesov. “Database Security: A Historical Perspective”. Em: (2010), pp. 1–19. DOI: 10.48550/ARXIV.1004.4022. Disp. em: https://arxiv.org/abs/1004.4022.

[6] Crepaldi Fábio Martins e Candido Eli Junior. “SEGURANÇA EM BANCO DE DADOS: CONCEITOS E APLICAÇÕES”. Em: (2014), pp. 1–13. Disp. em: http://intertemas.toledoprudente.edu.br/index.php/ETIC/article/view/4412/4172.

[7] Abdulazeez Mousa, Murat Karabatak e Twana Mustafa. “Database Security Threats and Challenges”. Em: *IEEE Transactions on Dependable and Secure Computing* (2020), pp. 1–5. DOI: 10.1109/ISDFS49300.2020.9116436.