UNIVERSIDADE DE BRASÍLIA

Faculdade do Gama

Sistemas de Banco de Dados 1

Trabalho Final (TF)

TEMA 1 - Energia

Artur Alves - 211043638
Bruno Ribeiro - 211039288
Bruno Kishibe - 200072854
Erick Santos - 18006067

Brasília, DF

2023

Existem falhas nos bancos de dados? Quais?

Os bancos de dados desempenham um papel crucial no armazenamento, gerenciamento e recuperação de dados em sistemas de informação modernos. No entanto, mesmo com toda a sua importância, eles não estão imunes a falhas. Devido à complexidade dos sistemas e à variedade de fatores envolvidos, diversas falhas podem ocorrer nos bancos de dados, afetando a disponibilidade, a integridade e a confiabilidade dos dados. Nesta apresentação, exploraremos algumas das falhas comuns que podem ocorrer nos bancos de dados.

1. Queda de Sistema

Uma das falhas mais evidentes nos bancos de dados é a queda do sistema, quando o servidor de banco de dados ou o sistema como um todo se torna inacessível. Essa falha pode ser causada por problemas de hardware, como falhas de disco, sobrecarga do servidor ou problemas de rede. Quando ocorre uma queda do sistema, os dados podem ficar temporariamente inacessíveis, resultando em interrupção de serviços, perda de produtividade e insatisfação dos usuários.

2. Erro durante a execução da transação

As transações são unidades lógicas de trabalho no banco de dados, compostas por várias operações. Erros durante a execução de transações podem levar a inconsistências nos dados. Por exemplo, uma transação de transferência de fundos entre contas bancárias pode falhar, deixando os fundos temporariamente indisponíveis para o cliente.

3. Falhas no disco, problemas físicos ou catástrofes

Problemas físicos, como falhas de disco ou danos ao hardware, podem causar a perda de dados ou levar o banco de dados a um estado inoperável. Além disso, catástrofes naturais, como incêndios, inundações ou terremotos, também podem causar danos físicos aos servidores de banco de dados, resultando em perda irreparável de informações.

4. Vulnerabilidades de segurança e ataques cibernéticos

Os bancos de dados podem estar sujeitos a vulnerabilidades de segurança que podem ser exploradas por invasores maliciosos. Ataques cibernéticos, como injeção de SQL, podem permitir que invasores acessem, alterem ou excluam dados sensíveis, causando graves prejuízos à empresa e aos seus clientes.

Conclusão

Embora os bancos de dados sejam projetados para serem robustos e confiáveis, as falhas são inevitáveis em ambientes complexos. É crucial que as organizações implementem práticas adequadas de gerenciamento de banco de dados, backups regulares, planos de recuperação de desastres e medidas de segurança para proteger os dados e mitigar os riscos de falhas. Além disso, o monitoramento contínuo do sistema e a resposta rápida a incidentes são essenciais para garantir a saúde e a integridade dos bancos de dados em ambientes modernos e conectados.

Exemplos reais de falhas em Bancos de Dados:

Exemplo 1

Um caso real que ilustra as possíveis falhas em bancos de dados ocorreu em Goiânia, onde um empresário dono de um restaurante recebeu um depósito de R$ 18 milhões por engano em sua conta bancária, devido a uma falha no sistema do banco entre os dias 26 e 27 de dezembro.

Ao perceber o valor inesperado, o empresário decidiu comprar um Porsche de luxo e também efetuou transferências para outras contas, desviando R$ 1,1 milhão. As investigações mostraram que ele também tentou um acordo com o banco para devolver o valor, mas devido a divergências, não foi possível alcançar um acordo.

Esse tipo de incidente realça a necessidade contínua de aprimorar as práticas de segurança cibernética e a implementação de medidas de controle para evitar situações semelhantes e garantir a confiabilidade e a proteção dos dados em sistemas de informação modernos.

Exemplo 2

Recentemente, o setor de informática do Sistema Único de Saúde (SUS), conhecido como DataSUS, foi alvo de um novo ataque cibernético, realizado por um invasor autointitulado "HACKER_SINCERO". O invasor já havia atacado o sistema anteriormente, e desta vez, foi ainda mais enfático em suas críticas à segurança do site do governo.

Em suas mensagens, "HACKER_SINCERO" alegou que o site do DataSUS continuava vulnerável e que poucas ações foram tomadas para corrigir as falhas após a invasão anterior. Além disso, ele divulgou imagens supostamente obtidas do sistema, contendo informações confidenciais de funcionários públicos do Ministério da Saúde.

As falhas de segurança apontadas pelo invasor incluem três vulnerabilidades distintas no sistema: execução remota de código (RCE), injeção de SQL (SQLi) e codificação dentre sites (XSS). Essas falhas permitem ao atacante programar remotamente dentro do servidor da vítima, manipular o banco de dados e injetar comandos para roubar dados dos usuários.

A invasão revelou que o sistema do DataSUS estava suscetível a ataques devido ao uso impróprio de aspas nos campos do formulário, o que permitiu ao invasor enviar comandos ao servidor. Essa má prática de programação contribuiu para a exploração das vulnerabilidades mencionadas pelo invasor.

Esse exemplo real destaca a importância crítica da segurança cibernética em sistemas de banco de dados, especialmente quando se tratam de dados confidenciais de saúde e informações pessoais. A proteção adequada contra ataques e o uso de boas práticas de programação são fundamentais para evitar violações de segurança e garantir a integridade dos dados em sistemas governamentais e de saúde. O caso do DataSUS serve como um lembrete de que as vulnerabilidades devem ser tratadas com seriedade e prontidão para proteger a confidencialidade e a privacidade dos cidadãos.