UNIVERSIDADE DE BRASÍLIA

Faculdade do Gama

Sistemas de Banco de Dados 2

Trabalho Final (TF)

Problemas de Segurança e Invasões em Bancos de Dados

Yuri Alves Bacarias - 180078640

Brasília, DF

2023

1. Definição da Tecnologia Pesquisada

Com o avanço da tecnologia digital durante o último século, houve um impacto direto no seu uso pela sociedade. Como resultado, ocorreu uma explosão na quantidade de dados coletados e armazenados em bancos de dados. Isso está presente no dia a dia de qualquer indivíduo, desde o nascimento até a morte, com seus registros guardados nos sistemas governamentais e até cadastramento em redes sociais.

Com todos esses dados sensíveis sendo armazenados, a preocupação com a segurança dos bancos de dados se torna uma prioridade indispensável. É essencial garantir que não ocorram falhas ou ataques que possam comprometer a integridade dos dados e evitar que os usuários sejam prejudicados com o compartilhamento ou uso inadequado de suas informações.

Para manter a segurança de um banco de dados, podemos utilizar os três fundamentos da segurança da informação, mais conhecidos pela sigla CID, que são citados em vários livros e por diferentes autores, como Ramez Elmasri em seu livro "Sistemas de Banco de Dados" e Michael E. Whitman em "Principles of Information Security". Esses autores abordam a importância dos princípios de confidencialidade, integridade e disponibilidade para garantir a proteção de um banco de dados.

O conceito de dispobilidade se resume a garantir que as informações e os recursos estejam disponíveis para aqueles que deles necessitam de forma a garantir justamente o nome do conceito. É essencial para garantir que os usuários possam utilizar os dados e recursos do sistema.

Sobre integridade, refere-se à garantia de manter os dados precisos, completos e consistentes ao longo do tempo. Esse conceito baseia-se em assegurar que modificações não autorizadas não passem pelo sistema, incluindo modificações acidentais, de forma que não comprometam a confiabilidade do banco de dados, isso pode ser alcançado por mecanismos de controle, como por exemplo restrições de acesso ou validação de dados. Já a confidencialidade refere-se à segurança da informação, de forma a garantir que os dados sejam acessíveis apenas para pessoas autorizadas, com o objetivo de manter a

privacidade e o sigilo dos dados.

O tema sobre segurança de dados está num tópico tão importante para os dias atuais que foram promovidas alterações na legislação brasileira com a inclusão da lei Nº 13.709, DE 14 DE AGOSTO DE 2018, mais conhecida como LGPD (Lei Geral de Proteção de Dados) que veio estabelecendo regras e princípios para garantir a privacidade e a proteção dos titulares de dados. Essa diretriz foi inspirada em regulamento já existente como o GDPR (Regulamento Geral de Proteção de Dados) presente na União Europeia vigente desde 2018. Esses regulamentos nos apresentam regras para o uso, coleta e armazenamento dos dados pessoais, alem de obrigar empresas a adotar medidas de segurança adequadas.

2. Objetivo(s) principal(is) da Tecnologia Pesquisada

Para compreender a segurança de dados, é necessário entender os principais desafios que ela enfrenta. Neste trabalho, o objetivo é citar alguns dos ataques mais comuns realizados nos sistemas, especialmente contra bancos de dados. Ataques como DDoS e ataques de força bruta serão o foco do trabalho com o a explicação do ataque além de formas utilizadas para combatê-las, além das vantagens e desvantagens que o sistema enfrenta. Também serão apresentados exemplos interessantes de ataques a empresas e instituições.

2.1 Principais desafios da segurança de um banco de dados

2.1.1 Ataque DoS

Um dos ataques mais comuns realizados por pessoas mal-intencionadas é o DDoS (Distributed Denial of Service), que em português significa "Negação Distribuída de Serviço". Para entendê-lo como um todo, é necessário compreender primeiro a forma mais simples desse ataque, conhecido como DoS (Denial of Service) ou "Negação de Serviço". O ataque de negação de serviço

visa impedir que os usuários acessem aplicativos de banco de dados ou de redes.

O ataque comumente funciona sobrecarregando o servidor, o que leva à exaustão dos recursos necessários para manter o sistema em funcionamento, como memória e CPU. Isso pode ocorrer devido ao envio excessivo de consultas ou requisições ao sistema, para as quais o sistema não foi adequadamente preparado. Como resultado, o servidor pode ficar lento, deixar de responder e, em alguns casos, até mesmo parar completamente de funcionar.

O ataque ao sistema do banco de dados se tornou um alvo, como citado por Adrian Lane, analista/CTO da Securosis LLC. Ele menciona que em alguns casos, os ataques funcionam consumindo uma grande quantidade de recursos do sistema. Por exemplo, executando uma operação de "search" em milhares de sessões diferentes simultaneamente ou carregando um carrinho de compras online com milhares de itens e atualizando-o constantemente. Essas formas de ataque exploram vulnerabilidades do banco de dados do sistema, resultando em travamentos e colapsos.

Essa forma de ataque ficou tão evidente que em 2013 o "Postgres" um dos maiores sistemas gerenciadores de bancos de dados, abriu uma issue para tratar de um *exploit* no seu sistema onde um ataque DoS no banco estava resultando no banco de dados travando e se recusando a reiniciar. Esse exploit foi tratado pelo sistema nos patchs seguintes.

2.1.2 Ataque DDoS

Depois de entender o DoS, agora é possível compreender como funciona um ataque de negação de serviço distribuído (DDoS). Esse tipo de ataque ocorre de forma extremamente similar ao DoS, com algumas peculiaridades adicionais. Resumidamente, o DDoS é um ataque de negação de serviço distribuído, onde um hacker invade vários computadores para serem os "computadores mestres". Esses computadores invadidos atuam como orquestradores do ataque, controlando outras máquinas conhecidas como "zumbis". Dessa forma, o ataque DoS é realizado de forma ampliada e simultânea, o que pode afetar sistemas

grandes, mesmo aqueles que estão preparados para enfrentar inúmeros ataques.

Esses ataques se tornaram tão comum que foram criadas empresas especializadas em combater esses ataques, pois um ataque de negação de serviço realizado em empresas gigantes do mercado gera prejuízo de milhares de dólares.

A forma de mitigação pode ser a mesma utilizada para previnir um ataque DDoS onde se usarmos um

As formas de mitigar esses ataques de acordo com a empresa “cloudflare” especialista em serviços de segurança são

- Rate limiting (limitação de taxa) onde o sistema só funcionara com limites de requests vindo do sistema.
- Web Application Firewall (WAF) é um sistema que atua como uma camada intermediária entre a internet e o servidor de aplicativos, filtrando os pedidos (requests) com base em um conjunto de regras pré-definidas.

2.1.3 Ataque de força Bruta

O ataque de força bruta é um método de invasão que se baseia em tentativa e erro, sendo um dos métodos mais antigos utilizados pela humanidade. De acordo com um artigo produzido pela empresa CloudFlare, esse tipo de ataque envolve o uso de scripts ou bots que tentam "adivinhar" senhas, chaves de API e logins de SSH, testando todas as combinações possíveis de caracteres até encontrar a combinação correta.

Podemos usar um exemplo tangível da vida real para ilustrar esse tipo de ataque: é como se um ladrão tentasse abrir um cofre experimentando todas as combinações possíveis.

Os pontos positivos do ataque de força bruta são que ele é relativamente simples e, se não houver estratégias efetivas de prevenção em vigor, ele pode ter sucesso se tempo suficiente for disponibilizado.

No entanto, como em tudo na vida, existem também desvantagens. Os aspectos negativos do ataque de força bruta estão relacionados à sua lentidão. Devido ao número de combinações possíveis, o ataque pode ser extremamente demorado, especialmente quando se trata de senhas com muitos caracteres. À

medida que o número de caracteres aumenta, o tempo necessário para realizar o ataque aumenta de forma exponencial.

Se considerarmos os dados fornecidos pela CloudFlare, se um sistema puder processar 15 milhões de combinações de caracteres por segundo, uma senha de 5 caracteres pode ser quebrada em 1 segundo. No entanto, se aumentarmos o número de caracteres para 9, o tempo necessário aumentará para cerca de 4 dias. Se aumentarmos ainda mais, como para 13 caracteres, levaria aproximadamente 359 mil anos para quebrar a senha.

Para proteger o sistema pode-se utilizar de metodos parecidos com os de prevenção a um DDoS onde se utiliza de um Rate Limiting que faz com que após certas quantidades de tentativas o IP de acesso seja bloqueado.

3. Vantagem da tecnologia pesquisada

Os dados de um sistema são extremamente valiosos e considerados o "ouro líquido" que mantém qualquer organização funcionando. O setor de segurança de dados exige um investimento significativo, pois proteger esses dados é fundamental para manter a credibilidade de qualquer empresa.

Além de ser uma questão de credibilidade, a proteção de dados se tornou uma obrigação legal em muitos países. Evitar ataques cibernéticos e garantir a segurança dos dados é uma responsabilidade das empresas, pois a ocorrência de falhas de segurança pode levar a ações legais.

Cada vez que uma empresa sofre um ataque, além do prejuízo à sua reputação, também há um impacto econômico significativo.

Para mitigar muitos ataques, é frequentemente benéfico fazer alterações no banco de dados, como mencionado por Martins, Fábio em "Segurança em Banco de Dados: Conceito e Aplicações". Uma dessas alterações envolve a implementação de mecanismos de acesso obrigatórios para estabelecer diferentes níveis de acesso, com base na classificação dos dados e dos usuários, seguindo o conceito de papéis e as políticas de segurança da empresa. Esses mecanismos auxiliam na criação de uma política de controle de acesso, garantindo que a maioria dos usuários do sistema não precise ter acesso a todos

os dados do banco de dados para realizar suas tarefas de trabalho.

4. Desvantagem da tecnologia pesquisada

Uma das desvantagens de ter um nível de segurança mais alto é que o sistema pode ser prejudicado em termos de tempo de resposta em comparação a um sistema menos protegido. Isso ocorre porque um sistema protegido geralmente possui camadas adicionais de autenticação, criptografia, troca de chaves e outros mecanismos de segurança que podem adicionar complexidade e exigir mais recursos computacionais.

Consequentemente, o uso de recursos computacionais adicionais para fortalecer a segurança implica em maiores investimentos e custos operacionais. No entanto, é um investimento essencial, considerando o cenário atual de ameaças cibernéticas. Um levantamento realizado pela empresa Fortinet em 2022 revelou que foram registrados mais de 100 bilhões de ataques isso só no brasil.

5. Exemplos de uso em empresas

5.1 Maior Ataque DDoS da historia

A empresa Google sofreu um dos maiores ataques DDoS da história, com uma taxa de 2,54 terabits por segundo de pacotes sendo enviados aos servidores da Google. Esse número é extremamente elevado, mas a equipe da Google conseguiu trabalhar para mitigar qualquer impacto negativo no sistema. Graças às medidas de segurança implementadas, como o Cloud Armor Adaptive Protection, foi possível identificar e bloquear o tráfego malicioso.

5.2 Ataque ao GitHub

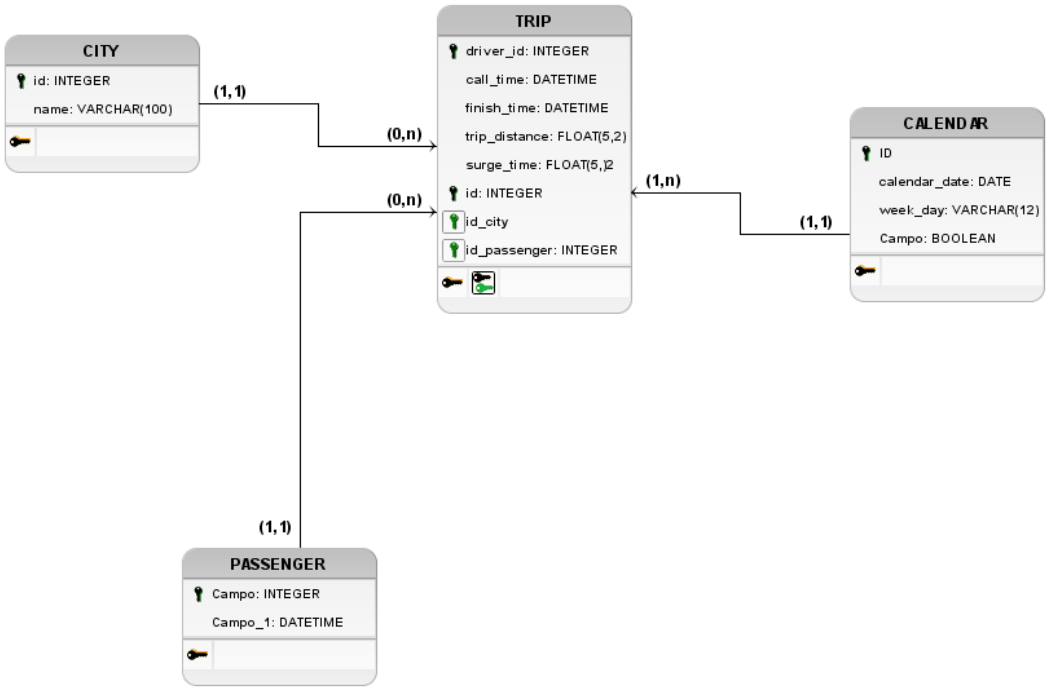
O ataque ao GitHub foi um dos maiores já registrados, no qual uma taxa

de ataque de 1,3 terabits por segundo foi direcionada aos servidores do GitHub. Devido à implementação de um serviço de proteção de dados, o GitHub foi alertado automaticamente cerca de 10 minutos após o início do ataque. A equipe conseguiu responder rapidamente e mitigar o ataque, que durou aproximadamente 20 minutos.

6. Base de dados

Para a base dedados foi utilizado uma Datasheet do kaggle sobre um mercado seus motoristas e seus passageiros. Esse datasheet se basea num teste realizado para a contratação de um funcionário trazendo caracteristicas de um uso real.

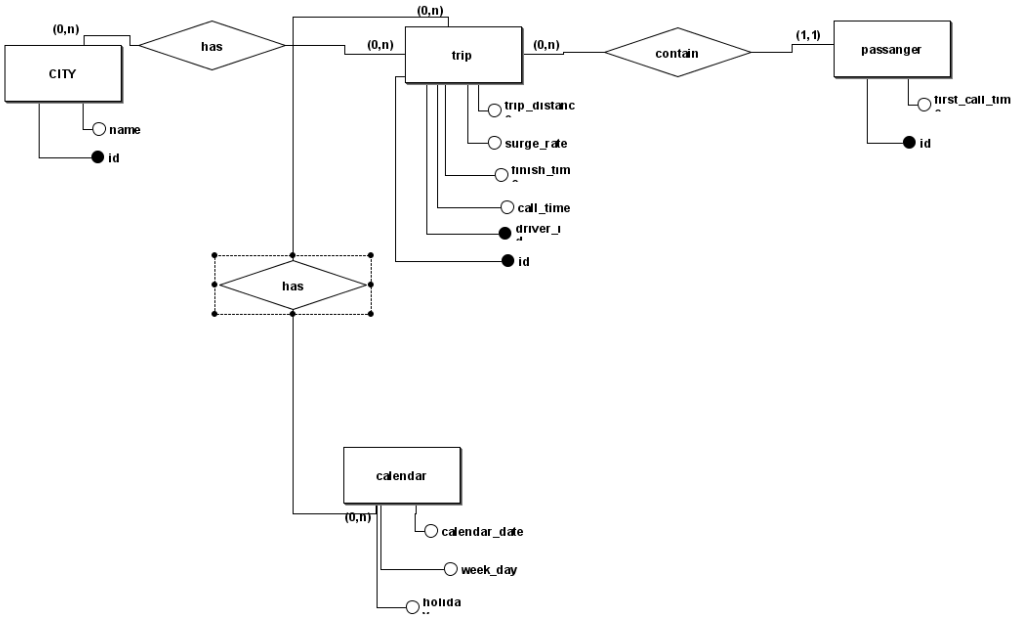
DLD



DE-R

Tuplas

- Trip : 2318357
- Calendar: 1096
- Passenger : 1235782



Datasheet disponivel

https://www.kaggle.com/datasets/ivanchvez/99littleorange

1. "Database Denial of Service: The Attacks" - Securosis. Disponível em: https://securosis.com/blog/database-denial-of-service-the-attacks.
2. "PostgreSQL Security FAQ" - PostgreSQL Global Development Group. Disponível em: https://www.postgresql.org/support/security/faq/2013-04-04/.
3. "Denial of Service (DoS)" - Cloudflare. Disponível em: https://www.cloudflare.com/learning/ddos/glossary/denial-of-service/.
4. "99littleorange" - Kaggle. Disponível em:

https://www.kaggle.com/datasets/ivanchvez/99littleorange.

5. "Lei nº 13.709/2018" - Planalto. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.
6. "Famous DDoS Attacks" - Cloudflare. Disponível em: https://www.cloudflare.com/pt-br/learning/ddos/famous-ddos-attacks/.
7. "Brasil é segundo país mais atingido por ciberataques na América Latina" - Febraban Tech. Disponível em: https://febrabantech.febraban.org.br/temas/seguranca/brasil-e-segundo-pais-mais-atingido-por-ciberataques-na-america-latina-diz-relatorio.
8. "Brute Force Attack" - Cloudflare. Disponível em: https://www.cloudflare.com/pt-br/learning/bots/brute-force-attack/.
9. Sistemas de Banco de Dados" - Ramez Elmasri and Shamkant B. Navathe - Editora: Pearson Brasil - Disponível em: https://www.amazon.com.br/Sistemas-Banco-Dados-Ramez-Elmasri/dp/8543025001.
10. "Principles of Information Security" - Michael E. Whitman and Herbert J. Mattord - Editora: Cengage Learning - Disponível em: https://www.amazon.com.br/Principles-Information-Security-Michael-Whitman/dp/1337102067.