Aula 3

Sistema Gerenciador de Banco de Dados

Prof. Leonel da Rocha

1

Conversa Inicial

2

Monitoramento de SGBD

- **Nessa aula veremos como monitorar o desempenho de um SGBD e suas atividades, isso é importante para garantirmos um acesso eficaz ao servidor e seus dados**
- **Em seguida, vamos ver como é preciso cuidar dos dados armazenados e garantir a confidencialidade e saber como podemos garantir sua proteção de ameaças externas**

3

- **Outro ponto importante é a gestão de segurança dos dados, implementada através de chaves, certificados e criptografia**
- **Vamos estudar a importância e a necessidade de disponibilizar os dados e garantir a sua integridade**

4

- **Para finalizar essa terceira aula, trataremos do assunto de auditoria, onde veremos procedimentos para entender se tudo está em conformidade com as regras estabelecidas em nosso sistema de gerenciador de banco de dados e os dados armazenados e controlados por ele**

5

Análise de Desempenho e Atividades

6

- O uso de SGBD cresce junto com o volume de dados
- A partir desse panorama, aumentam as dificuldades de gerenciamento e de desempenho dos SGBD
- Configuração, tanto de segurança quanto de desempenho, com seus valores padrões
- Diversos parâmetros devem ser configurados e modificados

7

Otimização de desempenho

- Manter a versão do SGBD atualizada
- Verificar periodicamente se o banco de dados não contém tabelas e dados órfãos
- Revisões de limpeza, dados antigos: expurgo

8

Confidencialidade e Ameaças

9

- A confidencialidade de um dado tem a ver com a privacidade dos usuários que acessam e se cadastram em um banco de dados
- É um conceito que se relaciona às ações tomadas para garantir que informações confidenciais não sejam disponibilizadas ou caiam em mão erradas

10

- Para que a confidencialidade funcione, medidas preventivas devem ser implementadas, como permitir o acesso dessas informações somente para usuários autorizados e com senhas fortes
- Essa restrição de acesso pode ser definida por níveis de atividade e status do usuário

11

- Os dados podem ser categorizados como forma de aumentar a segurança e a confidencialidade
- Levar em consideração critérios específicos, como potencial de impacto nas operações da organização caso eles vazem

12

- **Para garantir a confidencialidade dos dados é possível implantar sistemas de criptografia, autenticação de dois fatores e verificação biométrica na infraestrutura de gerenciamento dos dados**

13

- **É importante lembrar que informações confidenciais não são apenas as da organização, mas de funcionários, clientes, fornecedores e outros que estejam sobre sua responsabilidade como administrador de um banco de dados**

14

- **Agora vamos ver o que é uma ameaça e exemplos de como ela se transforma em um ataque bem-sucedido**
- **Uma ameaça em segurança da informação pode ser definida como uma ação capaz de causar danos aos dados, comprometendo sua autenticidade, confidencialidade, integridade e disponibilidade** (ACID)

15

- **A seguir podemos verificar alguns exemplos de ameaça em segurança da informação e alguns fatores que podem ser tomados para evitá-las**
  - **Falhas humanas**
  - **Malware: é um software malicioso**
  - **Ransomware: tipo de ataque em que usuários sequestram dados corporativos, liberando-os após pagamento de resgate**
  - **Spyware: espiona computadores para coletar informações de relevância**

16

- **Existem alguns tipos de ameaça em segurança da informação, vamos ver a seguir**
  - **Ataques direcionados**
    - **São coletadas informações específicas sobre uma organização com técnicas de engenharia social para executar um ciberataque**

17

- **Ataques persistentes avançados**
  - **Ameaça com foco na espionagem**
- **Ataque DDoS**
  - **São enviadas múltiplas solicitações para o sistema invadido para sobrecarregá-lo e tornando-o indisponível**

18

Gestão de Segurança, Certificados e Criptografia

19

Gestão de segurança

- A segurança do banco de dados herda as mesmas dificuldades que a segurança da informação enfrenta, que é garantir a integridade, a disponibilidade e a confidencialidade
- Um SGBD deve fornecer mecanismos que auxiliem nesta tarefa

20

Objetivos de segurança de um BD

- A integridade de um BD é o requisito de que a informação seja protegida contra modificações não autorizadas
- A disponibilidade do BD é a sua capacidade de tornar disponível os objetos a um usuário que tenha direito legítimo
- A confidencialidade do BD é a proteção dos dados contra a exposição não autorizada

21

Certificados

- O certificado digital é a identidade eletrônica de uma pessoa física ou jurídica
- Funciona como uma carteira de identidade virtual, permitindo assinar documentos à distância com o mesmo valor jurídico da assinatura manual no papel
- Sem necessidade de reconhecimento de firma em cartório

22

- O certificado digital comprova a identidade de uma pessoa e é praticamente inviolável, sendo aceita legalmente
- O sistema utiliza um par de chaves criptografadas que não se repete

23

Chaves de um certificado digital

- Chave privada
  - Criptografa os dados que atestam a identidade sobre a pessoa, tanto para acesso a um sistema, quanto para assinatura de um documento eletrônico

24

- Chave pública
  - É compartilhada com quem precisa decodificar a criptografia que atesta a identidade de uma pessoa
  - A chave pública só serve para decodificar o que foi criptografado por uma chave privada

25

Criptografia

- Criptografia é o estudo dos princípios e técnicas pelas quais a informação pode ser transformada de sua forma original para uma forma ilegível
- Dessa maneira ela poderá ser lida apenas por seu destinatário legítimo, tornando a mensagem difícil de ser lida por alguém que não seja autorizado

26

- Podemos citar quatro objetivos principais da criptografia
  - Confidencialidade da mensagem
    - Só o destinatário autorizado deve extrair o conteúdo da mensagem da sua forma cifrada
  - Integridade da mensagem
    - O destinatário deve ser capaz de determinar se a mensagem foi ou não alterada no momento da transmissão

27

- Autenticação do remetente
  - O destinatário deve identificar o remetente e verificar que foi ele quem enviou a mensagem
- Não repúdio ou irretratabilidade do emissor
  - Não deverá ser possível ao emissor negar a autoria da mensagem enviada

28

Disponibilidade e Integridade dos Dados

29

Disponibilidade dos dados

- Disponibilidade de dados é a garantia de que os dados estarão disponíveis para usuários e sistemas no momento em que eles precisarem
- A disponibilidade de dados é usada, entre outras coisas, para criar contratos de nível de serviço (SLA) que definem e garantem a prestação do serviço

30

- A disponibilidade de dados exige a implementação de serviços, regras e procedimentos que garantam que os dados estejam disponíveis em operações normais e em recuperação de desastres
- A disponibilidade da informação é um dos requisitos de compliance, que é o ato de estar em conformidade com determinadas leis, normas e regras

31

Integridade dos dados

- Quando todas as informações da empresa estão registradas em um banco de dados e são alteradas ou excluídas, impactos podem ocorrer
- É para evitar a ocorrência de problemas que a integridade de dados é tratada como assunto primordial dentro da segurança da informação

32

- A integridade dos dados é referente à confiabilidade e consistência das informações ao longo do seu ciclo de vida
- Tem por objetivo preservar o dado para que nada seja comprometido ou perdido

33

- A integridade dos dados, devido a sua importância, é o foco principal de várias soluções de segurança
- Diversas ferramentas de proteção são implementadas para que o conteúdo armazenado seja preservado ao máximo

34

Auditoria

35

- Os bancos de dados são essenciais para que as organizações mantenham seus dados seguros
- Contudo, para garantir a qualidade do seu funcionamento é preciso contar com uma auditoria em banco de dados

36

- É através da auditoria em um banco de dados que é possível à organização detectar e prevenir eventuais meios de invasão e garantir a segurança dos seus processos e dados
- E ainda atestar sua conformidade com as leis

37

- A auditoria em banco de dados é um componente de conformidade dentro de uma organização
- Diz respeito à análise e entendimento das atividades de um banco de dados

38

- O objetivo de uma auditoria é verificar se as atividades auditadas estão em conformidade com as diretrizes preestabelecidas pela política da empresa ou por uma legislação específica
- E se a implementação dessas atividades foi realizada de maneira adequada para cumprir com seus objetivos

39

- A auditoria em base de dados é responsável por definir tabelas para armazenar logs com informações referentes à utilização das bases de dados
- Essa informações devem conter
  - Data e hora de acesso
  - Equipamento utilizado
  - Comandos feitos no banco
  - Usuário que fez o acesso

40

- A auditoria da segurança de dados procura auxiliar a empresa na identificação de uma possível violação dos dados antes que um incidente maior de segurança possa acontecer

41