Administrador de Banco de Dados (extra Abril) - Turma 2024A

5.18 Princípios de segurança de banco de dados

Os bancos de dados são uma parte fundamental de muitas organizações e armazenam informações críticas e confidenciais. Por essa razão, é crucial garantir que esses dados sejam protegidos por meio de práticas adequadas de segurança de banco de dados. Aqui estão alguns princípios importantes de segurança de banco de dados que devem ser seguidos:

1. Autenticação e autorização: A autenticação refere-se à verificação da identidade de um usuário que está acessando o banco de dados, enquanto a autorização se refere à concessão de permissões para acessar recursos específicos no banco de dados. A autenticação e a autorização adequadas ajudam a garantir que apenas usuários autorizados possam acessar e manipular dados.
2. Criptografia: A criptografia é uma técnica usada para proteger dados em trânsito ou em repouso, tornando-os ilegíveis para qualquer pessoa que não possua a chave para decifrar os dados. A criptografia é importante para proteger os dados de acesso não autorizado.
3. Monitoramento e auditoria: O monitoramento e a auditoria do banco de dados são importantes para identificar atividades suspeitas, como tentativas de acesso não autorizado ou alterações indevidas nos dados. As práticas de monitoramento e auditoria ajudam a garantir a integridade dos dados e a detectar ameaças de segurança.
4. Controle de acesso: O controle de acesso refere-se à gestão de permissões de usuários para acessar e manipular dados. O controle de acesso adequado ajuda a garantir que apenas usuários autorizados possam acessar os dados e que as informações sejam protegidas contra acesso não autorizado.
5. Gerenciamento de vulnerabilidades: O gerenciamento de vulnerabilidades é o processo de identificação, avaliação e mitigação de vulnerabilidades em um sistema. O gerenciamento de vulnerabilidades ajuda a garantir que as vulnerabilidades sejam identificadas e corrigidas antes que sejam exploradas por ameaças de segurança.
6. Backup e recuperação de desastres: O backup e a recuperação de desastres são essenciais para garantir que os dados sejam protegidos contra a perda em caso de falhas do sistema ou desastres naturais. O backup regular dos dados ajuda a garantir que as informações estejam disponíveis em caso de perda de dados.

A implementação adequada desses princípios de segurança de banco de dados pode ajudar a proteger os dados contra ameaças de segurança e garantir a integridade dos dados. É importante que as organizações implementem práticas de segurança adequadas e monitorem regularmente seus sistemas para identificar possíveis ameaças à segurança. A segurança de banco de dados é um processo contínuo e deve ser avaliado e aprimorado regularmente para garantir a proteção dos dados contra ameaças de segurança em constante evolução.

Um hacker tentou invadir o banco de dados de uma empresa de serviços financeiros. Ele usou uma técnica de ataque conhecida como SQL injection, que permite ao invasor inserir comandos maliciosos em um formulário da web, explorando vulnerabilidades no software. O hacker conseguiu acessar o banco de dados da empresa, mas foi impedido de prosseguir graças aos princípios de segurança de banco de dados que foram implementados.

Primeiro, a empresa implementou a autenticação e a autorização adequadas para garantir que apenas usuários autorizados pudessem acessar o banco de dados. Isso impediu que o hacker se movimentasse livremente pelos dados da empresa.

Em segundo lugar, a empresa havia criptografado os dados armazenados no banco de dados. Como resultado, o hacker não conseguiu entender as informações que havia roubado do banco de dados.

Terceiro, a empresa havia implementado um sistema de monitoramento e auditoria do banco de dados. Quando o hacker tentou acessar informações confidenciais, o sistema detectou a atividade suspeita e enviou um alerta para a equipe de segurança da empresa.

Em seguida, a equipe de segurança agiu rapidamente e implementou um controle de acesso mais rígido para impedir o acesso não autorizado ao banco de dados. A equipe também iniciou uma investigação completa para identificar a origem do ataque e implementar medidas de segurança adicionais.

Por fim, a empresa havia implementado um backup e um plano de recuperação de desastres. Isso permitiu à empresa restaurar os dados perdidos durante o ataque e continuar suas operações sem interrupção.

Graças aos princípios de segurança de banco de dados que foram implementados, a empresa conseguiu impedir o hacker de causar danos significativos e proteger seus dados confidenciais.

Última atualização: terça, 21 mar 2023, 13:44

◄ 5.17 Soluções de alta disponibilidade e recuperação de desastres

Seguir para...

5.19 Auditoria e monitoramento de segurança ►