Banco de Dados II
Aula 2

Prof: Uemerson Pinheiro Junior

Sobre a aula

- O que é a segurança de dados ?
- Tríade CID (CIA Triad)
- A importância da segurança dos dados
- Dados críticos que necessitam de proteção
- Os desafios da proteção dos dados
- Algumas formas de manter os dados seguros
- Exercícios

O que é a segurança de dados ?

- A segurança de dados envolve garantir a proteção de informações digitais contra acesso não autorizado, corrupção ou roubo durante todo o seu ciclo de vida.
- Abrange diversos aspectos da segurança da informação:
  - proteção física de equipamentos e dispositivos de armazenamento
  - medidas administrativas
  - controle de acesso
  - segurança lógica de aplicativos de software
  - procedimentos organizacionais

Tríade CID (CIA Triad)

Existem três aspectos chave da segurança da informação comumente referidos como CIA Triad, ou Tríade CID: **Confidencialidade, Integridade e Disponibilidade.**

Tríade CID: Confidencialidade

As empresas devem evitar que pessoas não autorizadas acessem informações confidenciais. Para garantir isso, elas implementam diversas medidas de segurança, como **controle de acesso, criptografia, políticas rigorosas de senha, autenticação em várias etapas, gestão de configurações e sistemas de monitoramento com alertas.**

Tríade CID: Integridade

É essencial garantir que os dados não sejam apagados ou alterados de forma inadequada. Para assegurar a autenticidade das informações e facilitar transações seguras, muitas empresas optam por empregar assinaturas digitais.

Tríade CID: Disponibilidade

É crucial que as informações estejam prontamente acessíveis quando requeridas. Por exemplo, é fundamental que o banco de dados financeiro esteja acessível para que os contadores possam realizar transações de pagamento. **Garantir a disponibilidade também implica em assegurar a resiliência dos dados**, isto é, a capacidade de recuperar rapidamente o conteúdo em situações como ciberataques, falhas de hardware ou outras circunstâncias adversas.

A importância da segurança dos dados

Quando executadas de forma eficaz, medidas sólidas de segurança de dados protegem os ativos de informação de uma empresa contra ações criminosas cibernéticas. **Também oferecem defesa contra ameaças internas e equívocos humanos, que persistem como fatores proeminentes nas violações de dados contemporâneas.**

A segurança de dados requer a implementação de tecnologias para rastrear e proteger informações cruciais. **É essencial aplicar criptografia, mascaramento e ocultação de dados, automatizando relatórios para simplificar auditorias e cumprir regulamentos.**

A importância da segurança dos dados

Assegurando a continuidade das operações: A implementação de medidas de segurança de dados auxilia na prevenção de interrupções nas atividades comerciais que podem surgir devido à perda de confidencialidade, integridade ou disponibilidade dos dados.

Minimizando o risco financeiro: Incidentes de violação de dados podem acarretar consequências econômicas significativas para além das perturbações operacionais, tais como despesas legais, penalidades por falta de conformidade e redução de receita a longo prazo devido à perda de confiança por parte dos clientes.

A importância da segurança dos dados

Atendendo aos requisitos legais e de conformidade: Falhar em seguir as normativas de proteção de dados, como o **LGPD, GDPR e o CCPA**, pode acarretar em pesadas penalidades financeiras e prejudicar a reputação da empresa por um longo período.

Protegendo a propriedade intelectual: A implementação de medidas sólidas de segurança de dados auxilia as empresas a preservarem seus planos financeiros, projetos, segredos comerciais e outras informações preciosas contra acessos não autorizados.

Dados críticos que necessitam de proteção

Os dados vitais para a empresa são os conjuntos de dados essenciais para a operação e sustentação do seu negócio. Exemplos disso são os planos financeiros, acordos com fornecedores, inventário e ativos intelectuais, como projetos e informações confidenciais.

Dados confidenciais compreendem informações pessoais e sensíveis, como registros de funcionários, detalhes de remuneração, perfis de clientes, informações médicas particulares e detalhes de cartões de crédito ou débito.

Os desafios da proteção dos dados

A transformação digital está mudando profundamente a maneira como as empresas operam e competem atualmente. **As empresas estão gerando, manipulando e armazenando uma quantidade cada vez maior de dados, o que aumenta a necessidade de governança desses dados.** Os ambientes de computação também estão se tornando mais complexos, abrangendo frequentemente a nuvem pública, os centros de dados corporativos e diversos dispositivos periféricos, como sensores de Internet das Coisas (IoT), robôs e servidores remotos. **Essa complexidade eleva o risco de ciberataques, dificultando a monitoração e a proteção desses sistemas.**

Algumas formas de manter os dados seguros

1. Criptografia
2. Excluir os dados
3. Mascaramento de dados
4. Resiliência de dados
5. Autenticação
6. Controle de acesso

Criptografia

Ao utilizar criptografia em dados sensíveis, asseguramos que, mesmo em caso de acesso não autorizado, essas informações se tornem indecifráveis. A aplicação de criptografia é eficaz tanto durante a transmissão quanto no armazenamento dos dados.

Excluir os dados

Quando os dados já não são mais úteis, é essencial eliminá-los de maneira que não seja possível recuperá-los. A exclusão completa dos dados é particularmente crucial ao retirar de uso ou reutilizar hardware.

Mascaramento de dados

O mascaramento de dados é uma técnica que oculta determinadas informações dentro de bancos de dados, permitindo que estes sejam utilizados para testes, análises ou outros propósitos, sem expor a privacidade dos dados.

Resiliência de dados

A capacidade de resiliência está relacionada à habilidade de uma organização em lidar ou se recuperar de qualquer tipo de falha, seja ela relacionada a problemas de hardware, falta de energia ou outros eventos que afetem a disponibilidade de dados. A rapidez na recuperação é fundamental para minimizar os impactos.

Autenticação

Autenticação é garantir que as pessoas que acessam informações sensíveis sejam de fato quem dizem ser.

Enquanto as senhas têm sido tradicionalmente usadas para autenticação, as organizações estão adotando a autenticação multifatorial (MFA) para dificultar que adversários com credenciais roubadas obtenham acesso, exigindo uma forma adicional de verificação de identidade, como biometria.

Controle de acesso

Usuários autenticados devem ter acesso apenas aos dados e outros recursos de TI necessários para realizar suas tarefas.

Listas de Controle de Acesso (LCA), Controle de Acesso Baseado em Função (CABF) e Gerenciamento de Acesso Privilegiado (GAP) são exemplos de controles de acesso.

Exercícios

1. Defina o que é a segurança de dados ?
2. Defina os três aspectos chave da segurança: Confidencialidade, Integridade e Disponibilidade.
3. Por que é importante manter os dados em segurança ?
4. Quais dados críticos que necessitam de proteção ?
5. Quais são os desafios da proteção dos dados ?
6. Explique cada uma das formas de manter os dados seguros: Criptografia, Excluir os dados, Mascaramento de dados, Resiliência de dados, Autenticação, Controle de acesso.

Referências

What is data security? Disponível em: <https://www.ibm.com/topics/data-security>

Data Security Explained: Challenges and Solutions. Disponível em: <https://blog.netwrix.com/data-security/>