ESCOLA ESTADUAL DE EDUCAÇÃO PROFISSIONAL DEPUTADO ROBERTO MESQUITA

MÁRCIO GABRIEL SANTOS SILVA

SEGURANÇA DA INFORMAÇÃO:

"CRIPTOGRAFIA NA PROTEÇÃO DE DADOS SENSÍVEIS: ANÁLISE COMPARATIVA DE MÉTODOS DE CRIPTOGRAFIA EM AMBIENTES CORPORATIVOS"

18/09/2024

GENERAL SAMPAIO – CE

A criptografia é uma ferramenta essencial para a proteção de dados sensíveis em ambientes corporativos. Existem diversos métodos de criptografia, cada um com suas próprias vantagens e desvantagens. Vamos explorar alguns dos principais métodos e suas aplicações:

1. Criptografia Simétrica

Descrição: Utiliza a mesma chave para criptografar e descriptografar os dados.

Vantagens: Rápida e eficiente para grandes volumes de dados.

Desvantagens: A segurança depende da proteção da chave; se a chave for comprometida, os dados também estarão.

2. Criptografia Assimétrica

Descrição: Utiliza um par de chaves (pública e privada). A chave pública criptografa os dados, enquanto a chave privada os descriptografa.

Vantagens: Maior segurança, pois a chave privada não é compartilhada.

Desvantagens: Mais lenta e complexa em comparação com a criptografia simétrica.

3. Criptografia de Ponta a Ponta

Descrição: Garante que apenas as partes envolvidas na comunicação possam acessar os dados.

Vantagens: Alta segurança, ideal para comunicações sensíveis.

Desvantagens: Pode ser complexa de implementar em sistemas legados.

4. Criptografia Homomórfica

Descrição: Permite realizar cálculos em dados criptografados sem precisar descriptografá-los.

Vantagens: Mantém a privacidade dos dados durante o processamento.

Desvantagens: Ainda em desenvolvimento e pode ser computacionalmente intensiva.

5. Criptografia de Dados em Repouso e em Trânsito

Dados em Repouso: Protege dados armazenados em discos rígidos, bancos de dados, etc.

Dados em Trânsito: Protege dados que estão sendo transferidos pela rede.

Vantagens: Protege dados em diferentes estados, garantindo segurança abrangente.

Desvantagens: Requer a implementação de diferentes estratégias e ferramentas para cada estado.

Melhores Práticas para Implementação

Gerenciamento de Chaves: Utilize soluções robustas para o gerenciamento de chaves criptográficas.

Atualizações Regulares: Mantenha os algoritmos e sistemas de criptografia atualizados.

Treinamento de Funcionários: Garanta que todos os funcionários estejam cientes das melhores práticas de segurança.

AES (Advanced Encryption Standard)

Como funciona: Um algoritmo de criptografia simétrica amplamente utilizado.

Vantagens: Alta segurança e eficiência.

Desvantagens: Requer gerenciamento seguro das chaves

RSA (Rivest-Shamir-Adleman)

Como funciona: Um algoritmo de criptografia assimétrica.

Vantagens: Alta segurança para troca de chaves e autenticação.

Desvantagens: Mais lento que os algoritmos simétricos

Fontes de Pesquisa:

https://conceito.de/criptografia

https://fintech.com.br/blog/tecnologia/metodos-avancados-de-criptografia-para-protecao-digital/

https://bravotecnologia.com.br/criptografia-de-dados/