Redes de Computadores

Joseffe Barroso de Oliveira

AULA

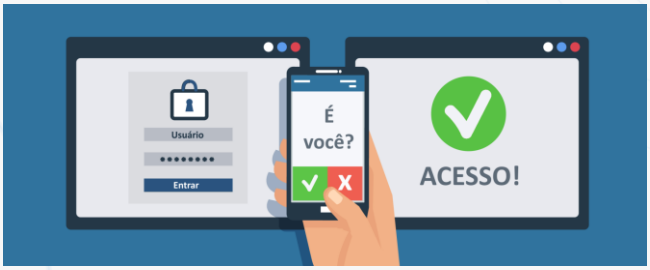
Conceitos básicos de segurança de redes - Parte 02

Introdução

Segurança de rede é qualquer atividade projetada para proteger o acesso, o uso e a integridade da rede corporativa e dos dados. A segurança da rede combina várias camadas de defesa na borda e na rede. Cada camada de segurança de rede implementa políticas e controles. Usuários autorizados obtêm acesso a recursos de rede, mas agentes mal-intencionados são impedidos de realizar explorações e ameaças.

Tipos de autenticação

- Algo que você conhece: Uma sequência de caracteres, números ou uma combinação daqueles que estão armazenados em seu cérebro. Hoje eles devem ser armazenados em um gerenciador de senhas.
- Algo que você tem: Um dispositivo ou software em um dispositivo que você precisa para autenticar. Isso inclui dispositivos como um token RSA ou o autenticador do Google em um smartphone.
- Algo que você é: Um aspecto de sua pessoa. Isso é biométrico, fisiológico, como uma impressão digital, ou comportamental, como uma impressão vocal.



Criptografia

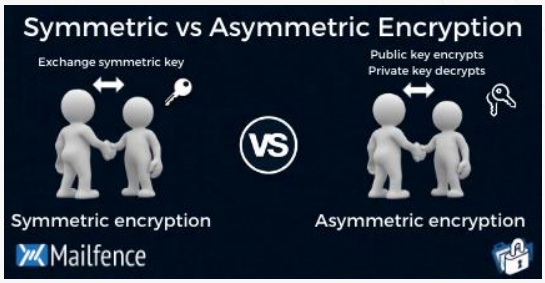
A criptografia é essencial para manter os dados confidenciais e as comunicações longe de olhares indiscretos. A criptografia protege arquivos no disco rígido do seu computador, uma sessão bancária, dados armazenados na nuvem, e-mails confidenciais e uma longa lista de outras aplicações. A criptografia também fornece verificação da integridade dos dados e autenticação da fonte dos dados.

A criptografia se divide em dois tipos básicos de criptografia: **simétrica** e **assimétrica.**

Criptografia

- A criptografia simétrica tem **uma única chave que criptografa e descriptografa**. Como resultado, ela deve ser compartilhada com outra pessoa para completar a comunicação criptografada. Os algoritmos comuns incluem o Advanced Encryption Standard (AES), Blowfish, Triple-DES (Data Encryption Standard), e muitos mais.

- A criptografia assimétrica tem **duas chaves distintas, uma pública e outra privada**, que funcionam como um conjunto correspondente. O conjunto de chaves pertence a um usuário ou um serviço: por exemplo, um servidor web Uma chave é para criptografia e a outra é para descriptografia.



O que levar em consideração para segurança da informação das empresas

- Elabore uma Política de Segurança da Informação (PSI)
- Implemente as tecnologias necessárias
- Proteja suas redes de Wi-Fi
- Faça backups
- Armazene seus documentos na nuvem

O que levar em consideração para segurança da informação das empresas

- Firme um contrato de confidencialidade
- Gerencie os riscos
- Treine sua equipe
- Tenha um plano de contingência