NORMAS MEDIDAS DE SEGURANÇA DE REDE

As normas de segurança de rede são focadas em proteger as redes de computadores contra ameaças externas e internas. Elas incluem recomendações sobre a configuração de firewalls, a implementação de sistemas de detecção de intrusões e a adoção de políticas de acesso restrito.

- **Firewall**

  O firewall é uma barreira de segurança que monitora e controla o tráfego de rede com base em um conjunto de regras pré-definidas. Ele ajuda a proteger a rede bloqueando acessos não autorizados e filtrando pacotes de dados maliciosos.

- **Criptografia**

  A criptografia envolve a codificação das informações para que somente as partes autorizadas possam acessá-las. Ela é usada para proteger a confidencialidade dos dados durante a transmissão pela rede, garantindo que apenas os destinatários corretos possam decifrá-los.

- **Virtual Private Network (VPN)**

  Uma VPN estabelece uma conexão segura e criptografada entre dispositivos remotos e a rede corporativa. Ela é amplamente utilizada para proteger a comunicação em redes públicas, permitindo que os usuários acessem recursos internos com segurança.

- **Sistemas de detecção e prevenção de intrusões (IDS/IPS)**

  Esses sistemas monitoram o tráfego de rede em busca de atividades suspeitas ou maliciosas. O IDS identifica possíveis ameaças, enquanto o IPS atua para bloquear ou responder a essas ameaças em tempo real.

- **Autenticação e controle de acesso**

  Esses recursos garantem que apenas usuários autorizados tenham acesso aos recursos de rede. Eles incluem senhas, autenticação de dois fatores, certificados digitais e políticas de acesso baseadas em funções.

- **Antivírus e anti malware**

Softwares de antivírus e anti malware são usados para detectar, bloquear e remover ameaças como vírus, worms, trojans e spyware, protegendo a rede contra programas maliciosos.

Como melhorar a segurança da Organização

I. Avaliação de riscos: Realize uma avaliação abrangente dos riscos de segurança de rede da organização. Identifique os ativos críticos, as vulnerabilidades existentes e as possíveis ameaças.

II. Políticas de segurança: Estabeleça políticas de segurança claras e documentadas. Isso inclui políticas de senhas fortes, acesso privilegiado, uso adequado da rede, atualização de software e política de uso aceitável. Eduque os funcionários sobre essas políticas e a importância de segui-las.

III. Monitoramento e registro de atividades: Defina um sistema de monitoramento de ambiente contínuo para detectar atividades suspeitas. Registre e analise logs de eventos para identificar possíveis incidentes de segurança e responder a eles de forma adequada.

IV. Atualizações e patches: Mantenha todos os sistemas e softwares atualizados com as últimas correções de segurança. Isso inclui sistemas operacionais, aplicativos, firewalls e antivírus. Aplique regularmente os patches de segurança para corrigir vulnerabilidades conhecidas.

V. Conscientização e treinamento: Realize treinamentos regulares de conscientização em segurança para todos os funcionários. Eduque-os sobre as ameaças de segurança, como phishing e engenharia social, e incentive boas práticas, como evitar clicar em links suspeitos ou compartilhar informações confidenciais.

VI. Backup de dados: é uma das principais medidas de segurança administrativa, pois ele permite recuperar os dados em caso de perda, roubo ou corrupção.

VII. Atualização dos sistemas: é uma estratégia de segurança lógica que corrige as falhas e as vulnerabilidades que podem ser exploradas pelos hackers.

VIII. Garantir que os usuários autorizados tenham acesso seguro aos recursos de redep