
CYBER
ACADEMY
FEBRABAN

MÓDULO 6

Segurança de Redes e Comunicações

A importância da Segurança de Redes

As redes são o tecido que conecta todos os dispositivos e sistemas em sua organização. A segurança de redes é fundamental para garantir que apenas as pessoas autorizadas tenham acesso aos recursos disponíveis.

Firewall

Firewalls são barreiras de segurança que controlam o tráfego de rede. Eles podem bloquear o acesso não autorizado e impedir a propagação de malware por exemplo. Configurar firewalls é um passo fundamental na segurança de redes.

Criptografia

A criptografia é o processo de embaralhar dados de modo que só possam ser lidos por pessoas autorizadas com a chave correta. Isso é essencial para proteger informações confidenciais durante a transmissão pela rede.

VPNs – Redes Privadas Virtuais

As VPNs permitem que os dados sejam transmitidos com segurança através de redes públicas, como a internet. Elas criptografam a comunicação, tornando-a privada e segura.

Ataques de Rede Comuns

Vários tipos de ataques de rede podem ameaçar a segurança cibernética. Isso inclui ataques de negação de serviço (DoS) que sobrecarregam redes e ataques de intermediários (Man-in-the-middle) que interceptam comunicações.

Autenticação e Controle de Acesso

Tem como objetivo, garantir que apenas pessoas autorizadas tenham acesso a sistemas e redes. Isso envolve a implementação de autenticação forte, como senhas complexas e autenticação de dois fatores.

Monitoramento de Rede
Monitorar a rede é uma parte essencial da segurança. Isso permite identificar atividades suspeitas e responder a ameaças em tempo real.

Políticas de Segurança de Redes
Desenvolver políticas de segurança de redes claras e aplicá-las de forma consistente em toda a organização é vital para manter a segurança.

Treinamento de Conscientização de Segurança
Treinar os colaboradores acerca das práticas de segurança de redes é uma linha de defesa importante. As ameaças podem muitas vezes ser evitadas com um bom programa de conscientização junto aos colaboradores e fornecedores de sua empresa.

Segurança em Dispositivos e Endpoint

Significado e Princípios Básicos
Dispositivos e endpoint são terminais de rede, como computadores, smartphones, tablets e servidores. Eles são os pontos de entrada e saída para informações e são frequentemente alvos de ataques cibernéticos.

Ativos Digitais em Dispositivos
Dispositivos contêm informações valiosas, como documentos, e-mails, senhas e outros dados. A proteção desses ativos é essencial para a segurança cibernética geral.

Segurança em Sistemas Operacionais
Manter sistemas operacionais atualizados com as últimas correções de segurança é fundamental para evitar vulnerabilidades que podem ser exploradas por invasores.

Proteção contra Malware
A instalação de software antivírus e antimalware ajuda a prevenir e detectar ameaças, como vírus, cavalos de Troia e Ransomware.

Políticas de Senhas Fortes
Exigir senhas fortes e a troca regular delas aumenta a segurança dos dispositivos e sistemas.

Atualizações de Software e Patching
Manter todos os softwares e aplicativos atualizados com patches de segurança é uma medida crítica para evitar exploração de vulnerabilidades.

Controle de Acesso e Privilégios
Restringir o acesso a sistemas e dados apenas a funcionários autorizados e atribuir privilégios com base nas funções ajuda a evitar acessos não autorizados.

Segurança Física de Dispositivos
Proteger fisicamente dispositivos é importante para evitar o roubo ou acesso não autorizado.

Monitoramento e Detecção de Ameaças
A implementação de ferramentas de monitoramento e detecção ajuda a identificar atividades suspeitas em dispositivos e endpoint.

Referências Bibliográficas:

Capeletti, Lucas. Fundamentos de Gestão de Acesso e Identidade (IAM) (Portuguese Edition).
Lisboa Melo, Jefferson; Vieira de Oliveira, Alexandre; Mauser, Daniel. Do Iniciante ao Profissional em Segurança Cibernética. SF Editorial e AcademiaTI.
Fernandes, Victor. Inteligência Artificial para Leigos (Portuguese Edition).
Wendt, Emerson; Jorge, Higor Vinicius Nogueira. Crimes Cibernéticos 3a edição: Ameaças e procedimentos de investigação (Portuguese Edition). BRASPORT.
Baars, Hans; Hintzbergen, Kees; Hintzbergen, Jule; Smulders, André. Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002 (Portuguese Edition). BRASPORT.
R., Raphael. Segurança Cibernética: Protegendo Infraestruturas e Dados (Portuguese Edition).

CYBER
ACADEMY

FEBRABAN