Redes de Computadores

Joseffe Barroso de Oliveira

AULA

Conceitos básicos de segurança de redes - Parte 01

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.

Firewall

Firewalls colocam uma barreira entre a rede interna confiável e as redes externas não confiáveis, como a Internet. Eles usam um conjunto de regras definidas para permitir ou bloquear o tráfego. Um firewall pode ser um hardware, software ou ambos.

Segurança de e-mails

Os gateways de e-mail são os principais vetores de ameaça de uma violação de segurança. Os invasores usam informações pessoais e táticas de engenharia social para criar campanhas de phishing sofisticadas, com o objetivo de enganar destinatários e enviá-los para sites de malware. Um aplicativo de segurança de e-mail bloqueia a entrada de ataques e controla mensagens de saída para impedir a perda de dados confidenciais.

Software antivírus e antimalware

"Malware", abreviação de "malicious software" (software mal-intencionado), inclui vírus, worms, Trojans, ransomware e spyware. Às vezes, o malware infecta uma rede, mas permanece inativo por dias ou até semanas. Os melhores programas antimalware não apenas analisam o malware na entrada, mas também sempre rastreiam os arquivos posteriormente para encontrar anomalias, remover malware e corrigir danos.

Segmentação de rede

A segmentação definida por software coloca o tráfego de rede em diferentes classificações e facilita a aplicação de políticas de segurança . De preferência, as classificações são baseadas na identidade do endpoint, não em meros endereços IP. Você pode atribuir direitos de acesso com base na função, local e muito mais, para que o nível certo de acesso seja concedido às pessoas certas, e os dispositivos suspeitos sejam contidos e corrigidos.

Controle de acesso

Nem todo usuário deve ter acesso à rede. Para impedir possíveis invasores, você precisa reconhecer cada usuário e cada dispositivo. Em seguida, você pode aplicar as políticas de segurança. Você pode bloquear dispositivos de endpoint não compatíveis ou conceder a eles apenas acesso limitado. Esse processo é um controle de acesso à rede (NAC).

Segurança de aplicações

Qualquer software usado para administrar os negócios precisa ser protegido, independentemente de sua equipe de TI criar ou comprar de terceiros. Infelizmente, qualquer aplicação pode conter falhas ou vulnerabilidades que os invasores usam para se infiltrar na rede. A segurança da aplicação abrange o hardware, software e processos que você usa para corrigir essas falhas.

Análise de comportamento

Para detectar um comportamento anormal da rede, você deve saber como é o comportamento normal. As ferramentas de análise comportamental distinguem automaticamente as atividades que se desviam da norma. A equipe de segurança pode identificar melhor os indicadores de comprometimento que apresentam um possível problema e remediar rapidamente as ameaças.

Prevenção contra perda de dados

As empresas devem garantir que a equipe não envie informações confidenciais para fora da rede. As tecnologias de prevenção contra perda de dados, ou DLP, podem impedir as pessoas de enviar, encaminhar ou, até mesmo, imprimir informações importantes de modo não seguro.

Segurança web

Uma solução de segurança da Web controlará o uso da Web da equipe, bloqueará ameaças baseadas na Web e negará acesso a sites mal-intencionados. Ela protegerá o gateway da Web no local ou na nuvem. "Segurança da Web" também se refere às etapas que você executa para proteger o próprio site.

VPN

A VPN é a sigla para Virtual Private Network, e **se trata de uma conexão entre computadores feita de forma privada**. Normalmente, é utilizada para oferecer maior privacidade e segurança de rede nas trocas de dados no dia a dia.

A VPN é bastante utilizada, por exemplo, para:

- Bloquear a navegação;
- Impedir o compartilhamento de dados internos da empresa em redes públicas;
- Realizar uma conexão criptografada;
- Esse tipo de conexão de computador é fundamental para quem deseja evitar que informações privadas possam ser obtidas por meio de cibercriminosos;