1.Segurança *mobile* e wireless

Se você está instalando uma nova rede sem fio ou solucionando problemas em uma rede sem fio existente, pode ser útil realizar uma pesquisa de local. Isso permite entender melhor o desempenho da sua rede sem fio e também pode fornecer informações sobre como outras redes próximas podem estar afetando seu sinal.

Um dos primeiros passos em uma pesquisa de local é obter uma compreensão detalhada dos pontos de acesso que já estão instalados. Esses pontos de acesso podem fazer parte da sua rede ou podem ser pontos de acesso localizados em uma área geográfica próxima. Se houver pontos de acesso fora do seu controle, será necessário configurar sua rede para trabalhar em torno das frequências já em uso.

A pesquisa de local fornecerá detalhes sobre o espectro de frequência atual e ajudará a identificar quais canais podem ser os melhores para sua rede sem fio. Como a tecnologia está sempre mudando, pode ser uma boa ideia realizar essa pesquisa periodicamente para identificar novos pontos de acesso que possam exigir ajustes na sua rede.

Uma boa forma de visualizar a sua rede sem fio é por meio de um **mapa de calor**. Esse mapa mostra a intensidade do sinal em diferentes áreas, com cores como vermelho e amarelo indicando sinal forte, enquanto cores mais escuras ou azuladas indicam áreas com sinal mais fraco. Muitas vezes, é difícil prever como os sinais sem fio funcionarão em um determinado ambiente de trabalho, e esses mapas de calor permitem uma visão detalhada do alcance do sinal em cada cômodo ou área.

Também é possível usar ferramentas de pesquisa sem fio para coletar mais informações sobre as redes próximas. Essas ferramentas fornecem um resumo de todos os pontos de acesso ou SSIDs disponíveis na área, exibindo dados como **BSSID**, informações do canal, bandas de frequência em uso e outros detalhes. Essas informações ajudam a determinar quais pontos de acesso têm a melhor cobertura para sua área e como os sinais podem variar conforme você se move.

Além disso, essas ferramentas podem ser úteis para identificar **interferências** na rede. Se você está tentando diagnosticar problemas de conectividade, os dados coletados podem indicar quais áreas apresentam falhas e se há outros dispositivos causando interferência.

Os sistemas operacionais modernos já incluem algumas ferramentas integradas para análise de redes sem fio. Algumas dessas ferramentas são utilitários separados, enquanto outras fazem parte da interface de conexão Wi-Fi. Além disso, existem ferramentas de terceiros que podem ser baixadas para uma análise mais avançada. Um exemplo é o **NetSpot**, que pode ser instalado para fornecer uma lista detalhada de todas as redes sem fio próximas, incluindo métricas importantes para ajudar a entender quais pontos de acesso estão mais próximos e quais estão mais distantes.

Se houver suspeita de que outros dispositivos estão usando as mesmas frequências que seus pontos de acesso, pode ser interessante investir em um **analisador de espectro**. Esse equipamento identifica todos os sinais presentes em uma determinada frequência, sejam eles originados de um ponto de acesso ou de qualquer outro dispositivo.

Muitas empresas gerenciam seus dispositivos móveis por meio de um **Mobile Device Manager (MDM)**. Esse tipo de sistema é especialmente útil para administrar dispositivos pertencentes à empresa, mas também pode ser usado para gerenciar dispositivos pessoais dos funcionários, em uma política conhecida como **BYOD (Bring Your Own Device)**.

O MDM permite que os administradores configurem políticas de segurança e garantam que certos aplicativos essenciais estejam instalados nos dispositivos. Ele também pode impor restrições a algumas funcionalidades, como desativar a câmera enquanto o usuário estiver no escritório e reativá-la quando ele sair do local. Além disso, pode criar um ambiente separado dentro do dispositivo, isolando os dados pessoais dos dados da empresa para maior segurança.

Do ponto de vista da segurança, o **MDM** possibilita a implementação de medidas como bloqueios de tela automáticos e a exigência de senhas ou PINs para desbloqueio. Essas políticas ajudam a reduzir o risco de acesso não autorizado aos dispositivos da empresa.

A política **BYOD** permite que funcionários utilizem seus próprios dispositivos para fins profissionais. No entanto, esses dispositivos precisam atender aos requisitos da empresa para que possam ser gerenciados pelo **MDM**. Se o dispositivo for relativamente moderno, é possível gerenciá-lo facilmente dentro do ambiente corporativo, garantindo que as informações pessoais e empresariais permaneçam protegidas.

Outro aspecto importante do gerenciamento de dispositivos móveis é definir políticas para quando um funcionário troca de telefone. Muitas pessoas vendem ou trocam seus dispositivos antigos ao adquirir um novo, por isso é essencial garantir que todos os dados empresariais sejam completamente apagados antes que o dispositivo seja descartado.

Nem todas as empresas adotam a política **BYOD**. Algumas preferem fornecer dispositivos próprios aos funcionários, seguindo o modelo **COPE (Corporate Owned, Personally Enabled)**. Nesse caso, a empresa compra os dispositivos e os distribui aos funcionários, que podem usá-los tanto para fins profissionais quanto pessoais. Essa abordagem é semelhante ao fornecimento de computadores corporativos, onde a empresa possui e gerencia os dispositivos.

Mesmo com dispositivos corporativos, a empresa pode implementar **segmentação de dados**, garantindo que os dados corporativos fiquem separados dos dados pessoais. Isso permite que o administrador remova apenas os dados empresariais sem afetar as informações pessoais armazenadas no aparelho. Algumas empresas também permitem que os funcionários escolham entre diferentes modelos de dispositivos corporativos, uma abordagem chamada **CYOD (Choose Your Own Device)**.

Os dispositivos móveis apresentam desafios significativos de segurança. Como podem ser transportados para qualquer lugar do mundo, eles podem ser mais vulneráveis a **rastreamento de localização**, **interceptação de tráfego de dados** e outras ameaças. Além disso, contêm uma grande quantidade de informações sensíveis e podem ser facilmente escondidos.

As redes celulares modernas, como **4G e 5G**, operam em áreas geográficas chamadas **células**, daí o nome "telefone celular". Como não temos controle total sobre os dados transmitidos por esses dispositivos, devemos nos preocupar com **monitoramento de tráfego** e **rastreadores de localização**. Para garantir a segurança, é essencial manter os dispositivos sempre atualizados e protegidos contra ameaças.

As redes Wi-Fi também apresentam riscos semelhantes. Como permitem o acesso total à internet, devemos garantir que todos os dados transmitidos por essas redes sejam criptografados. Nem sempre as redes públicas, como as de cafeterias e hotéis, possuem essa proteção, por isso o uso de uma **VPN** ou outra tecnologia de criptografia é altamente recomendado.

Os invasores também podem estar fisicamente próximos de uma rede Wi-Fi, permitindo que monitorem o tráfego de dados enviado e recebido. Além disso, podem utilizar ataques **Man-in-the-Middle** (ou **on-path attacks**), interceptando as comunicações entre dois dispositivos. Outro risco é o ataque de **negação de serviço (DoS)**, no qual um invasor pode gerar interferências para desativar uma rede sem fio.

O Bluetooth, que opera em frequências sem fio de curto alcance, também pode representar uma ameaça de segurança. Ele é frequentemente usado para conectar dispositivos como fones de ouvido, smartwatches e outros acessórios sem fio. No entanto, se não for configurado corretamente, um invasor pode explorar vulnerabilidades para acessar dados armazenados no dispositivo.

Para evitar ataques via Bluetooth, é importante realizar um **processo de pareamento seguro** sempre que um novo dispositivo for conectado. Além disso, nunca devemos permitir conexões automáticas a dispositivos desconhecidos, pois isso pode comprometer a segurança das informações.