Principais Riscos nas Redes

Independente do tipo de tecnologia usada, um equipamento conectado à rede, seja um computador, dispositivo móvel, modem ou roteador, pode ser invadido ou infectado por meio:

- De falhas de configuração.
- Da ação de códigos maliciosos.
- Da exploração de vulnerabilidades.
- De ataques de força bruta, pelo uso de senhas fracas, senhas padrão e senhas de conhecimento dos atacantes.

Após invadido ou infectado ele pode, de acordo com suas características:

- Ser usado em atividades maliciosas, como esconder a real identidade do atacante, participar de botnets e propagar códigos maliciosos.
- Estar sujeito a ameaças, como furto de dados e uso indevido de recursos.

Um atacante pode, por exemplo:

- Disponibilizar uma rede insegura ou fingir ser uma rede conhecida, induzir os dispositivos a se conectar a ela e, então, capturar dados (ataques de personificação).
- Invadir um equipamento de rede, alterar as configurações e direcionar as conexões para sites fraudulentos.
- Interceptar o tráfego e coletar dados que estejam sendo transmitidos sem o uso de criptografia (sniffing).
- Fazer varreduras na rede (scan), a fim de descobrir outros computadores e, então, tentar executar ações maliciosas, como ganhar acesso e explorar vulnerabilidades.
- Usar a rede para enviar grande volume de dados para um computador, até torná-lo inoperante ou incapaz de se comunicar (DoS).

Cuidados a Serem Tomados com os Equipamentos de Rede

Proteja seus equipamentos de rede.

Atualize o firmware:

- Seja cuidadoso ao fazer a atualização.
- Verifique no site do fabricante os detalhes do procedimento.
- Se necessário, peça ajuda a alguém mais experiente.

Altere a senha de administração:

- Use senhas bem elaboradas, com grande quantidade de caracteres e que não contenham dados pessoais, palavras conhecidas e sequências de teclado.
- Lembre-se de guardar tanto a senha nova como a original.
- Restaure a senha original somente quando necessário.

Proteja seus computadores e dispositivos móveis:

- Mantenha-os atualizados, com as versões mais recentes e com todas as atualizações aplicadas.
- Utilize e mantenha atualizados mecanismos de segurança como antivírus e firewall pessoal.
- Desative a função de compartilhamento de recursos, somente a ative quando necessário e usando senhas bem elaboradas.
- Ative as interfaces Wi-Fi e Bluetooth somente quando for usá-las e desabilite-as após o uso.

Proteja seus dados:

- Faça backups regularmente.
- Use aplicações e protocolos que ofereçam criptografia, como HTTPS para conexões web, PGP para o envio de e-mails e SSH para conexões remotas ou VPNs.

Configurando o Acesso de Internet da Sua Casa

O acesso residencial costuma ser realizado via roteadores ou modems de banda larga que podem prover também a funcionalidade de rede sem fio.

Acessíveis remotamente via senha de administração, que pode ser usada:

- Por você.
- Pelo provedor de serviços de internet.
- Por um atacante.

Infelizmente muitos destes equipamentos são instalados com senhas fracas, padrão ou de conhecimento dos atacantes e por isso precisam ser alteradas.

Siga os cuidados gerais para proteger seus equipamentos de rede, lembrando-se de:

- Atualizar o firmware.
- Alterar a senha de administração.

Desabilite:

- O gerenciamento do equipamento via internet (WAN). Funções de administração só estarão disponíveis via rede local.
- A funcionalidade de rede sem fio caso não for usá-la. Caso deseje usá-la siga as dicas de como montar uma rede Wi-Fi doméstica.

Desligue o equipamento de rede quando não estiver usando.

Configurando uma Rede Wi-Fi Doméstica

A conexão Wi-Fi em uma residência ou escritório pode ser feita via:

- Equipamentos específicos.
- Como uma funcionalidade do roteador banda larga.

Em ambos os casos é necessário que alguns cuidados mínimos de segurança sejam tomados.

Siga as recomendações gerais para proteger seus equipamentos de rede, lembrando-se de:

- Atualizar o firmware.
- Atualizar a senha de administração.
- Altere a senha de autenticação de usuários.
- Configure o modo WPA2 de criptografia (evite usar WPA e WEP).
- Altere o nome da rede (SSID), e evite usar dados pessoais ou nomes associados ao fabricante/modelo, pois essas informações podem ser associadas a possíveis vulnerabilidades existentes.

Desabilite:

- Difusão (broadcast) do SSID, evitando que o nome da rede seja anunciado para outros dispositivos, dificultando o acesso por quem não sabe a identificação.
- WPS (Wi-Fi Protected Setup), para evitar acessos indevidos.
- Gerenciamento remoto (via rede sem fio), funções de administração só estarão disponíveis por quem tiver acesso físico ao equipamento.

Cuidados ao se Conectar a Redes Wi-Fi

Não permita que seus dispositivos conectem-se automaticamente:

- A redes públicas.
- A redes que você já tenha visitado (um atacante pode configurar uma rede com o mesmo nome de uma rede já utilizada por você, sem saber você estará acessando essa rede falsa).

Lembre-se de apagar as redes que você visitou, isso ajuda a preservar a sua privacidade.

Algumas redes públicas, como as encontradas em aeroportos, hotéis e conferências, redirecionam a navegação no primeiro acesso para um site de autenticação, essa autenticação serve apenas para restringir os usuários e não garante que as informações trafegadas serão criptografadas.

Procure usar redes que ofereçam criptografia WPA2, evite usar WEP e WPA.

Certifique-se de usar conexão segura (alguns indícios apresentados pelo navegador web são):

- O endereço começa com https://
- O desenho de um “cadeado fechado” é mostrado na barra de endereço, ao clicar sobre ele são exibidos detalhes sobre a conexão e certificado digital em uso.
- Um recorte colorido (branco ou azul) com o nome de domínio do site é mostrado ao lado da barra de endereço. Ao passar o mouse ou clicar sobre o recorte são exibidos detalhes sobre a conexão e certificado digital em uso.
- A barra de endereço e/ou recorte são apresentados em verde e no recorte é colocado o nome da instituição dona do site.

Cuidados ao Usar Redes Móveis

Mantenha seus equipamentos seguros.

Um dispositivo infectado conectado via rede móvel pode ser usado para:

- Desferir ataques.
- Enviar as informações coletadas.
- Se propagar para outros dispositivos.

Caso use um modem 3G/4G:

- Siga as recomendações de como configurar a internet em sua casa.

Sobre o Bluetooth:

- Mantenha as interfaces inativas e somente as habilite quando for usar.
- Configure as interfaces para que a visibilidade seja “Oculto” ou “Invisível”.
- Altere o nome padrão do dispositivo (evite usar na composição do novo nome dados que identifiquem o proprietário ou características técnicas do dispositivo).
- Altere a senha (PIN) padrão do dispositivo.
- Evite realizar o pareamento em locais públicos, reduzindo as chances de ser rastreado ou interceptado por um atacante.
- Fique atento ao receber mensagens em seu dispositivo solicitando autorização ou PIN (não responda à solicitação se não tiver certeza que está se comunicando com o dispositivo correto).
- No caso de perda ou furto de um dispositivo Bluetooth, remova de seus outros equipamentos todas as relações de confiança já estabelecidas com este dispositivo.