Publicação cert.br

Cartilha de Segurança para Internet

Fascículo Redes

https://cartilha.cert.br/

nic.br

cgi.br

Equipamentos de rede também precisam de cuidados de segurança

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 nele existentes
- ✓ de ataques de força bruta, pelo uso de senhas fracas, padrão e/ou de conhecimento dos atacantes

Após invadido ou infectado ele pode, de acordo com suas características, ser usado em atividades maliciosas, como propagação de códigos maliciosos, e 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 conectarem a ela e, então, capturar dados
- ✓ 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 gerais
a serem tomados

- ✓ **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
  - utilize sempre aplicações e protocolos que ofereçam criptografia, como o HTTPS para conexões Web, o PGP para o envio de *e-mails*, o SSH para conexões remotas ou ainda VPNs

Configurando o acesso Internet da sua casa

O acesso residencial costuma ser feito por meio de roteadores ou *modems* de banda larga que podem prover também a funcionalidade de rede sem fio. Esses equipamentos possuem senha de administração que pode ser usada para acesso remoto, tanto por você como pelo provedor de serviços Internet. 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 principalmente de atualizar o *firmware* e de alterar a senha de administração**

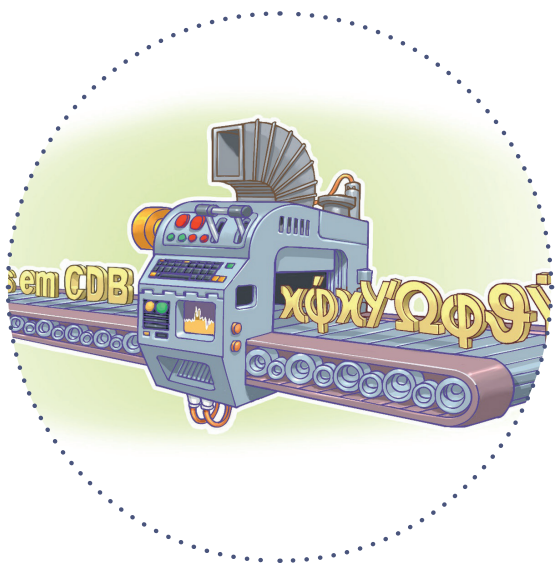
- ✓ **desabilite:**
  - o gerenciamento do equipamento de rede via Internet (WAN), assim as funções de administração só estarão disponíveis via rede local
  - a funcionalidade de rede sem fio caso não for usá-la. Caso deseje usá-la siga as dicas de como montar uma rede Wi-Fi doméstica

- ✓ **desligue o equipamento de rede quando não estiver utilizando**

Configurando uma rede Wi-Fi doméstica

A conexão Wi-Fi em uma residência ou escritório pode ser feita via equipamentos específicos ou 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* e de alterar a senha de administração**
- ✓ **altere também a senha de autenticação de usuários**
- ✓ **configure o modo WPA2 de criptografia. Evite usar WPA e WEP**
- ✓ **altere o nome da rede (SSID - *Server Set IDentifier*)**
  - evite usar dados pessoais ou nomes associados ao fabricante/modelo, pois essas informações podem ser associadas a possíveis vulnerabilidades existentes
- ✓ **"esconda" a sua rede**
  - desabilite a difusão (*broadcast*) do SSID, evitando que o nome da rede seja anunciado para outros dispositivos, dificultando o acesso por quem não sabe a identificação
- ✓ **desabilite:**
  - o WPS (*Wi-Fi Protected Setup*) para evitar acessos indevidos
  - o gerenciamento remoto (via rede sem fio), assim as 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 já utilizada por você e, sem saber, você estará acessando essa rede falsa)

- ✓ lembre-se de apagar as redes que você visitou, pois 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

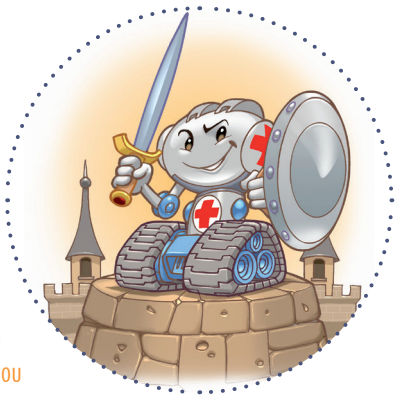
- ✓ certifique-se de usar conexão segura e observe se os dados do certificado digital correspondem ao da instituição a que pertence a página que você está acessando
  - detalhes sobre como fazer isso estão disponíveis nos fascículos *Internet Banking* e Comércio Eletrônico (https://cartilha.cert.br/fasciculos/)

Cuidados ao usar redes móveis (3G/4G)

Ao usar redes móveis é importante estar atento à segurança dos seus equipamentos. Um dispositivo infectado conectado via rede móvel pode ser usado para desferir ataques, enviar as informações coletadas e se propagar para outros dispositivos.

- ✓ caso você use um *modem* 3G/4G siga as recomendações de como configurar a Internet em sua casa

Cuidados ao usar conexões *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 e seja cuidadoso ao elaborar a nova
- ✓ 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

Consulte a **Cartilha de Segurança** para a Internet para mais detalhes sobre os cuidados a serem tomados ao utilizar redes:

https://cartilha.cert.br/redes

INTERNET SEGURA.BR

Precisa conversar sobre o uso seguro da Internet com **crianças e adolescentes**? O **Portal Internet Segura** apresenta uma série de iniciativas e de recomendações sobre esse assunto, confira!

http://internetsegura.br/

cert.br

Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

O CERT.br é o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Desde 1997, o grupo é responsável por tratar incidentes de segurança envolvendo redes conectadas à Internet no Brasil. O Centro também desenvolve atividades de análise de tendências, treinamento e conscientização, com o objetivo de aumentar os níveis de segurança e de capacidade de tratamento de incidentes no Brasil. Mais informações em https://www.cert.br/.

nic.br

Núcleo de Informação e Coordenação do Ponto BR

O Núcleo de Informação e Coordenação do Ponto BR - NIC.br (http://www.nic.br/) é uma entidade civil, sem fins lucrativos, que implementa as decisões e projetos do Comitê Gestor da Internet no Brasil. São atividades permanentes do NIC.br coordenar o registro de nomes de domínio - Registro.br (http://www.registro.br/), estudar e tratar incidentes de segurança no Brasil - CERT.br (https://www.cert.br/), estudar e pesquisar tecnologias de redes e operações - CEPTRO.br (http://www.ceptro.br/), produzir indicadores sobre as tecnologias da informação e da comunicação - CETIC.br (http://www.cetic.br/) e abrigar o escritório do W3C no Brasil (http://www.w3c.br/).

cgi.br

Comitê Gestor da Internet no Brasil

O Comitê Gestor da Internet no Brasil coordena e integra todas as iniciativas de serviços Internet no país, promovendo a qualidade técnica, a inovação e a disseminação dos serviços ofertados. Com base nos princípios de multilateralidade, transparência e democracia, o CGI.br representa um modelo de governança multissetorial da Internet com efetiva participação de todos os setores da sociedade nas suas decisões. Uma de suas formulações são os 10 Princípios para a Governança e Uso da Internet (http://www.cgi.br/principios). Mais informações em http://www.cgi.br/.

março / 2017