Cartilha de Segurança para Internet
Parte V: Redes de Banda Larga e Redes Sem Fio (*Wireless*)

NIC BR Security Office
nbso@nic.br

Versão 2.0
11 de março de 2003

Resumo

Esta parte da Cartilha discute implicações de segurança peculiares aos serviços de banda larga e *wireless*. Também apresenta algumas recomendações para que usuários destes serviços possam utilizá-los de forma mais segura.

Como Obter este Documento

Este documento pode ser obtido em http://www.nbso.nic.br/docs/cartilha/. Como ele é periodicamente atualizado, certifique-se de ter sempre a versão mais recente.

Caso você tenha alguma sugestão para este documento ou encontre algum erro, entre em contato através do endereço doc@nic.br.

Nota de *Copyright* e Distribuição

Sumário

1 Serviços de Banda Larga

Serviços de banda larga são aqueles que permitem ao usuário conectar seus computadores à Internet com velocidades maiores do que as normalmente usadas em linhas discadas. Exemplos desse tipo de serviço são ADSL, *cable modem* e acesso via satélite.

Além da maior velocidade, outra característica desse tipo de serviço é a possibilidade do usuário deixar seu computador conectado à Internet por longos períodos de tempo, sem limite de uso ou custos adicionais.

1.1 Quais são os riscos do uso de banda larga?

O uso dos serviços de banda larga torna um computador, ou rede, mais exposto a ataques. Alguns dos motivos são:

- os longos períodos que o computador fica ligado à Internet;
- a pouca freqüência com que o endereço IP[1] do computador muda ou, em alguns casos, o fato deste endereço nunca mudar;
- a maior velocidade de conexão, que pode facilitar alguns tipos de ataque.

1.2 Por que um atacante teria maior interesse por um computador com banda larga?

Geralmente um computador conectado através de banda larga possui boa velocidade de conexão e fica por longos períodos ligados à Internet, mas não possui os mesmos mecanismos de segurança que servidores. Isto os torna alvos mais fáceis para os atacantes.

Além disso, estes computadores podem ser usados para diversos propósitos, como por exemplo:

- realizar ataques de negação de serviço, aproveitando-se da maior velocidade disponível. Diversas máquinas comprometidas podem também ser combinadas de modo a criar um ataque de negação de serviço distribuído. Maiores informações sobre ataque de negação de serviço podem ser encontradas na parte I dessa cartilha (Conceitos de Segurança);
- usar a máquina comprometida como ponto de partida para atacar outras redes, dificultando o rastreio da real origem do ataque. Mais detalhes sobre abusos e incidentes de segurança podem ser encontrados na parte VII dessa cartilha (Incidentes de Segurança e Uso Abusivo da Rede);
- furtar informações tais como números de cartão de crédito, senhas, etc;

[1] O conceito de endereço IP pode ser encontrado no Glossário desta Cartilha.

- usar recursos do computador. Por exemplo, o invasor pode usar o espaço disponível em seu disco rígido para armazenar programas copiados ilegalmente, música, imagens, etc. O invasor também pode usar a CPU disponível, para por exemplo, quebrar senhas de sistemas comprometidos;

- enviar SPAM ou navegar na Internet de maneira anônima, a partir de certos programas que podem estar instalados no seu computador, tais como AnalogX e WinGate, e que podem estar mal configurados.

1.3 O que fazer para proteger um computador conectado por banda larga?

É recomendável que o usuário de serviços de banda larga tome os seguintes cuidados com o seu computador:

- instalar um *firewall* pessoal e ficar atento aos registros de eventos (*logs*) gerados por este programa. Maiores detalhes sobre registros de eventos podem ser encontrados na parte VII da Cartilha (Incidentes de Segurança e Uso Abusivo da Rede);

- instalar um bom antivírus e atualizá-lo freqüentemente;

- manter o seu *software* (sistema operacional, programas que utiliza, etc) sempre atualizado e com as últimas correções aplicadas (*patches*);

- desligar o compartilhamento de disco, impressora, etc;

- mudar a senha padrão[2] do seu equipamento de banda larga (modem ADSL, por exemplo) pois as senhas destes equipamentos podem ser facilmente encontradas na Internet com uma simples busca. Esse fato é de conhecimento dos atacantes e bastante abusado. A escolha de uma boa senha é discutida na parte I desta cartilha (Conceitos de Segurança).

A parte II desta cartilha (Riscos Envolvidos no Uso da Internet e Métodos de Prevenção) mostra maiores detalhes sobre os itens acima, bem como cuidados que também podem ser seguidos no tratamento de arquivos anexados, etc.

1.4 O que fazer para proteger uma rede conectada por banda larga?

Muitos usuários de banda larga optam por montar uma pequena rede (doméstica ou mesmo em pequenas empresas), com vários computadores usando o mesmo acesso à Internet. Nesses casos, alguns cuidados importantes, além dos citados anteriormente, são:

- instalar um *firewall* separando a rede interna da Internet;

[2] É importante que você guarde a senha original e lembre de restaurá-la sempre que for necessário, como por exemplo em caso de manutenção do equipamento.

- caso seja instalado algum tipo de *proxy* (como AnalogX, WinGate, WinProxy, etc) configurá-lo para que apenas aceite requisições partindo da rede interna;
- caso seja necessário compartilhar recursos como disco ou impressora entre máquinas da rede interna, devem-se tomar os devidos cuidados para que o *firewall* não permita que este compartilhamento seja visível pela Internet.

É muito importante notar que apenas instalar um *firewall* **não** é suficiente – todos os computadores da rede devem estar configurados de acordo com as medidas preventivas mencionadas na parte II desta Cartilha (Riscos Envolvidos no Uso da Internet e Métodos de Prevenção).

Muitos equipamentos de banda larga, como roteadores ADSL, estão incluindo outras funcionalidades, como por exemplo concentradores de acesso (*Access Points*) para redes *wireless*. Nesse caso, além de seguir as dicas dessa seção também pode ser interessante observar as dicas da seção 2.3.

2 Redes *Wireless*

As redes *wireless*, também conhecidas como IEEE 802.11, Wi-Fi ou WLANs, são redes que utilizam sinais de rádio para a sua comunicação.

Este tipo de rede define duas formas de comunicação:

modo infraestrutura: normalmente o mais encontrado, utiliza um concentrador de acesso (*Access Point* ou AP);

modo ponto a ponto (*ad-hoc*): permite que um pequeno grupo de máquinas se comunique diretamente, sem a necessidade de um AP.

Estas redes *wireless* ganharam grande popularidade pela mobilidade que provêem aos seus usuários e pela facilidade de instalação e uso em ambientes domésticos e empresariais, hotéis, conferências, aeroportos, etc.

2.1 Quais são os riscos do uso de redes *wireless*?

Embora esse tipo de rede seja muito conveniente, existem alguns problemas de segurança que devem ser levados em consideração pelos seus usuários:

- estas redes utilizam sinais de rádio para a comunicação e qualquer pessoa com um mínimo de equipamento[3] poderá interceptar os dados transmitidos por um cliente *wireless* (*notebooks*, PDAs, estações de trabalho, etc);
- por serem bastante simples de instalar, muitas pessoas estão utilizando redes desse tipo em casa, sem nenhum cuidado adicional, e até mesmo em empresas, sem o conhecimento dos administradores de rede.

[3] Um PDA ou *notebook* com uma placa de rede *wireless*.

2.2 Que cuidados devo ter com um cliente *wireless*?

Vários cuidados devem ser observados quando pretende-se conectar à uma rede *wireless* como cliente, quer seja com *notebooks*, PDAs, estações de trabalho, etc. Dentre eles, podem-se citar:

- considerar que, ao conectar a uma WLAN, você estará conectando-se a uma rede pública e, portanto, seu computador estará exposto a ameaças. É muito importante que você tome os seguintes cuidados com o seu computador:
  - possuir um *firewall* pessoal;
  - possuir um antivírus instalado e atualizado;
  - aplicar as últimas correções em seus *softwares* (sistema operacional, programas que utiliza, etc);
  - desligar compartilhamento de disco, impressora, etc.
- desabilitar o modo *ad-hoc*. Utilize esse modo apenas se for absolutamente necessário e desligue-o assim que não precisar mais;
- usar WEP (*Wired Equivalent Privacy*) sempre que possível, que permite criptografar o tráfego entre o cliente e o AP. Fale com o seu administrador de rede para verificar se o WEP está habilitado e se a chave é diferente daquelas que acompanham a configuração padrão do equipamento. O protocolo WEP possui diversas fragilidades e deve ser encarado como uma camada adicional para evitar a escuta não autorizada;
- considerar o uso de criptografia nas aplicações, como por exemplo o uso de PGP para o envio de *e-mails*, SSH para conexões remotas ou ainda o uso de VPNs;
- habilitar a rede *wireless* somente quando for usá-la e desabilitá-la após o uso. Algumas estações de trabalho e *notebooks* permitem habilitar e desabilitar o uso de redes *wireless* através de comandos ou botões específicos. No caso de *notebooks* com cartões *wireless* PCMCIA, insira o cartão apenas quando for usar a rede e retire-o ao terminar de usar.

2.3 Que cuidados devo ter ao montar uma rede *wireless* doméstica?

Pela conveniência e facilidade de configuração das redes *wireless*, muitas pessoas tem instalado estas redes em suas casas. Nestes casos, além das preocupações com os clientes da rede, também são necessários alguns cuidados na configuração do AP. Algumas recomendações são:

- ter em mente que, dependendo da potência da antena de seu AP, sua rede doméstica pode abranger uma área muito maior que apenas a da sua casa. Com isto sua rede pode ser utilizada sem o seu conhecimento ou ter seu tráfego capturado por vizinhos ou pessoas que estejam nas proximidades da sua casa.
- mudar configurações padrão que acompanham o seu AP. Alguns exemplos são:

  - alterar as senhas. Dicas para a escolha de uma boa senha pode ser obtidas na parte I desta Cartilha (Conceitos de Segurança);
  - alterar o SSID (*Server Set ID*);
  - desabilitar o *broadcast* de SSID;

- usar sempre que possível WEP (*Wired Equivalent Privacy*), para criptografar o tráfego entre os clientes e o AP. Vale lembrar que o protocolo WEP possui diversas fragilidades e deve ser encarado como uma camada adicional para evitar a escuta não autorizada;
- trocar as chaves WEP que acompanham a configuração padrão do equipamento. Procure usar o maior tamanho de chave possível (128 bits);
- desligue seu AP quando não estiver usando sua rede.

Existem configurações de segurança mais avançadas para redes *wireless*, que requerem conhecimentos de administração de redes. Estes conhecimentos não serão abordados neste documento.