



Cartilha de Segurança para Internet

Parte V: Redes de Banda Larga e Redes Sem Fio (*Wireless*)

Versão 3.0
Setembro de 2005
<http://cartilha.cert.br/>

cgi.br

CERT.br – Centro de Estudos, Resposta e Tratamento
de Incidentes de Segurança no Brasil

Cartilha de Segurança para Internet

Parte V: Redes de Banda Larga e Redes Sem Fio (*Wireless*)

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

Sumário

1	Serviços de Banda Larga	3
1.1	Por que um atacante teria maior interesse por um computador com banda larga e quais são os riscos associados?	3
1.2	O que fazer para proteger um computador conectado por banda larga?	3
1.3	O que fazer para proteger uma rede conectada por banda larga?	4
2	Redes Sem Fio (<i>Wireless</i>)	5
2.1	Quais são os riscos do uso de redes sem fio?	5
2.2	Que cuidados devo ter com um cliente de uma rede sem fio?	5
2.3	Que cuidados devo ter ao montar uma rede sem fio doméstica?	6
	Como Obter este Documento	8
	Nota de Copyright e Distribuição	8
	Agradecimentos	8

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, normalmente sem limite de uso ou custos adicionais.

1.1 Por que um atacante teria maior interesse por um computador com banda larga e quais são os riscos associados?

Geralmente um computador conectado através de banda larga possui boa velocidade de conexão, muda o endereço IP¹ com pouca frequência e fica por longos períodos ligado à Internet, mas não possui os mesmos mecanismos de segurança que servidores. Isto os torna alvos mais fáceis para os atacantes.

Por estas características, estes computadores podem ser usados pelos atacantes 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: Conceitos de Segurança](#);
- usar a máquina comprometida como ponto de partida para atacar outras redes, dificultando o rastreamento da real origem do ataque;
- furtar informações, tais como números de cartões de crédito, senhas, etc;
- 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.

Vale ressaltar que todas essas atividades podem ser realizadas de maneira automatizada, caso o computador seja infectado por um *bot*. Maiores detalhes sobre *bots* podem ser encontrados na parte [VIII: Códigos Maliciosos \(Malware\)](#).

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

Os usuários de serviços de banda larga devem tomar os seguintes cuidados com o seu computador:

¹O conceito de endereço IP pode ser encontrado no [Glossário](#).

- 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: Incidentes de Segurança e Uso Abusivo da Rede](#);
- instalar e manter atualizado um bom programa antivírus;
- atualizar as assinaturas do antivírus diariamente;
- manter os seus *softwares* (sistema operacional, programas que utiliza, etc) sempre atualizados e com as últimas correções de segurança aplicadas (*patches*);
- desligar o compartilhamento de disco, impressora, etc;
- mudar a senha padrão do seu equipamento de banda larga² (*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: Conceitos de Segurança](#).

A parte [II: Riscos Envolvidos no Uso da Internet e Métodos de Prevenção](#) mostra maiores detalhes sobre os cuidados citados acima.

1.3 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 a Internet. Nesses casos, alguns cuidados importantes, além dos citados anteriormente, são:

- instalar um *firewall* separando a rede interna da Internet;
- 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: 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](#).

²Verifique no contrato se é permitida a alteração da configuração do equipamento. Caso seja permitida, guarde a senha original e lembre de restaurá-la sempre que for necessário, como por exemplo em caso de manutenção do equipamento.

2 Redes Sem Fio (*Wireless*)

As redes sem fio (*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 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 sem fio?

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 equipamento³ poderá interceptar os dados transmitidos por um cliente da rede sem fio (como *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.

2.2 Que cuidados devo ter com um cliente de uma rede sem fio?

Vários cuidados devem ser observados quando se pretende conectar à uma rede sem fio como cliente, 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:
 - instalar um *firewall* pessoal;
 - instalar e manter atualizado um bom programa antivírus;
 - atualizar as assinaturas do antivírus diariamente;

³Um PDA ou *notebook* com uma placa de rede sem fio.

- 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;
 - sempre que possível usar WEP (*Wired Equivalent Privacy*), 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;
 - verificar com seu provedor de rede sem fio sobre a possibilidade de usar WPA (*Wi-Fi Protected Access*) em substituição ao WEP, uma vez que este padrão pode aumentar significativamente a segurança da rede. Esta tecnologia inclui duas melhorias em relação ao protocolo WEP que envolvem melhor criptografia para transmissão de dados e autenticação de usuário. Mesmo que seu equipamento seja mais antigo, é possível que exista uma atualização para permitir o uso de WPA;
 - 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;
 - evitar o acesso a serviços que não utilizem conexão segura, ao usar uma rede sem fio em local público. Por exemplo, se for necessário ler *e-mails* ou acessar a Intranet da sua empresa, dê preferência a serviços que usem criptografia;
 - habilitar a rede sem fio 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 sem fio através de comandos ou botões específicos. No caso de *notebooks* com cartões 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 sem fio doméstica?

Pela conveniência e facilidade de configuração das redes sem fio, muitas pessoas têm 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 podem ser obtidas na parte [I: Conceitos de Segurança](#);
 - alterar o SSID (*Server Set ID*);

- desabilitar o *broadcast* de SSID;
- permitir que um computador se conecte ao AP para alterar as configurações apenas através da rede cabeada, se esta opção estiver disponível. Desta maneira um possível atacante externo (via rede sem fio) não poderá acessar o AP diretamente para promover mudanças na configuração. Verifique a documentação do seu AP sobre como efetuar estas mudanças, caso estejam disponíveis;
- verificar se seus equipamentos já suportam WPA (*Wi-Fi Protected Access*) e utilizá-lo sempre que possível. Esta tecnologia é mais recente e inclui melhorias em relação ao protocolo WEP para prover uma segurança adicional contra acesso e escuta de tráfego não autorizada. Lembre-se que atualizações para WPA estão disponíveis para a maior parte dos equipamentos mais antigos;
- caso o WPA não esteja disponível, 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;
- se for utilizar WEP, trocar as chaves que acompanham a configuração padrão do equipamento. Procure usar o maior tamanho de chave possível (128 bits);
- desligar seu AP quando não estiver usando sua rede.

Existem configurações de segurança mais avançadas para redes sem fio, que requerem conhecimentos de administração de redes. Estes conhecimentos não são abordados neste documento.

Como Obter este Documento

Este documento pode ser obtido em <http://cartilha.cert.br/>. 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@cert.br.

Nota de *Copyright* e Distribuição

Este documento é Copyright © 2000–2005 CERT.br. Ele pode ser livremente copiado desde que sejam respeitadas as seguintes condições:

1. É permitido fazer e distribuir cópias inalteradas deste documento, completo ou em partes, contanto que esta nota de *copyright* e distribuição seja mantida em todas as cópias, e que a distribuição não tenha fins comerciais.
2. Se este documento for distribuído apenas em partes, instruções de como obtê-lo por completo devem ser incluídas.
3. É vedada a distribuição de versões modificadas deste documento, bem como a comercialização de cópias, sem a permissão expressa do CERT.br.

Embora todos os cuidados tenham sido tomados na preparação deste documento, o CERT.br não garante a correção absoluta das informações nele contidas, nem se responsabiliza por eventuais consequências que possam advir do seu uso.

Agradecimentos

O CERT.br agradece a todos que contribuíram para a elaboração deste documento, enviando comentários, críticas, sugestões ou revisões.

Agradece, especialmente, ao Nelson Murilo pelas sugestões e revisão desta parte da Cartilha.