Cartilha de Segurança para Internet

Checklist

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

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

Cartilha de Segurança para Internet

Checklist

Este *checklist* resume as principais recomendações contidas na Cartilha de Segurança para Internet. A numeração adotada neste *checklist* não possui relação com a adotada nas outras partes da Cartilha.

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

1 Prevenção Contra Riscos e Códigos Maliciosos (*Malware*)

1.1 Contas e senhas

- ❒ elaborar sempre uma senha que contenha pelo menos oito caracteres, compostos de letras, números e símbolos;
- ❒ jamais utilizar como senha seu nome, sobrenomes, números de documentos, placas de carros, números de telefones, datas que possam ser relacionadas com você ou palavras que façam parte de dicionários;
- ❒ utilizar uma senha diferente para cada serviço;
- ❒ alterar a senha com freqüência;
- ❒ criar tantos usuários com privilégios normais, quantas forem as pessoas que utilizam seu computador;
- ❒ utilizar o usuário *Administrator* (ou *root*) somente quando for estritamente necessário.

1.2 Vírus

- ❒ instalar e manter atualizado um bom programa antivírus;
- ❒ atualizar as assinaturas do antivírus, de preferência diariamente;
- ❒ configurar o antivírus para verificar os arquivos obtidos pela Internet, discos rígidos (HDs), flexíveis (disquetes) e unidades removíveis, como CDs, DVDs e *pen drives*;
- ❒ desabilitar no seu programa leitor de *e-mails* a auto-execução de arquivos anexados às mensagens;
- ❒ não executar ou abrir arquivos recebidos por *e-mail* ou por outras fontes, mesmo que venham de pessoas conhecidas. Caso seja necessário abrir o arquivo, certifique-se que ele foi verificado pelo programa antivírus;
- ❒ utilizar na elaboração de documentos formatos menos suscetíveis à propagação de vírus, tais como RTF, PDF ou *PostScript*;
- ❒ não utilizar, no caso de arquivos comprimidos, o formato executável. Utilize o próprio formato compactado, como por exemplo Zip ou Gzip.

1.3 *Worms*, *bots* e *botnets*

- ❒ seguir todas as recomendações para prevenção contra vírus;
- ❒ manter o sistema operacional e demais *softwares* sempre atualizados;
- ❒ aplicar todas as correções de segurança (*patches*) disponibilizadas pelos fabricantes, para corrigir eventuais vulnerabilidades existentes nos *softwares* utilizados;

- ❒ instalar um *firewall* pessoal, que em alguns casos pode evitar que uma vulnerabilidade existente seja explorada ou que um *worm* ou *bot* se propague.

1.4 Cavalos de tróia, *backdoors*, *keyloggers* e *spywares*

- ❒ seguir todas as recomendações para prevenção contra vírus, *worms* e *bots*;
- ❒ instalar um *firewall* pessoal, que em alguns casos pode evitar o acesso a um *backdoor* já instalado em seu computador, bloquear o recebimento de um cavalo de tróia, etc;
- ❒ utilizar pelo menos uma ferramenta anti-*spyware* e mantê-la sempre atualizada.

2 Cuidados no Uso da Internet

2.1 Programas Leitores de *E-mails*

- ❒ manter seu programa leitor de *e-mails* sempre atualizado;
- ❒ não clicar em *links* no conteúdo do *e-mail*. Se você realmente quiser acessar a página do *link*, digite o endereço diretamente no seu *browser*;
- ❒ desligar as opções que permitem abrir ou executar automaticamente arquivos ou programas anexados às mensagens;
- ❒ não abrir arquivos ou executar programas anexados aos *e-mails*, sem antes verificá-los com um antivírus;
- ❒ desconfiar sempre dos arquivos anexados à mensagem, mesmo que tenham sido enviados por pessoas ou instituições conhecidas. O endereço do remetente pode ter sido forjado e o arquivo anexo pode ser, por exemplo, um vírus ou um cavalo de tróia;
- ❒ fazer o *download* de programas diretamente do *site* do fabricante;
- ❒ evitar utilizar o seu programa leitor de *e-mails* como um *browser*, desligando as opções de execução de *JavaScript* e *Java* e o modo de visualização de *e-mails* no formato HTML.

2.2 *Browsers*

- ❒ manter o seu *browser* sempre atualizado;
- ❒ desativar a execução de programas *Java* na configuração de seu *browser*, a menos que seja estritamente necessário;
- ❒ desativar a execução de *JavaScripts* antes de entrar em uma página desconhecida e, então, ativá-la ao sair;

- ❒ permitir que programas *ActiveX* sejam executados em seu computador **apenas** quando vierem de *sites* conhecidos e confiáveis;
- ❒ manter maior controle sobre o uso de *cookies*, caso você queira ter maior privacidade ao navegar na Internet;
- ❒ bloquear *pop-up windows* e permití-las apenas para *sites* conhecidos e confiáveis, onde forem realmente necessárias;
- ❒ certificar-se da procedência do *site* e da utilização de conexões seguras ao realizar transações via *Web*;
- ❒ somente acessar *sites* de instituições financeiras e de comércio eletrônico digitando o endereço diretamente no seu *browser*, nunca clicando em um *link* existente em uma página ou em um *e-mail*.

2.3 Programas de troca de mensagens

- ❒ manter seu programa de troca de mensagens sempre atualizado;
- ❒ não aceitar arquivos de pessoas desconhecidas, principalmente programas de computadores;
- ❒ utilizar um bom antivírus, sempre atualizado, para verificar todo e qualquer arquivo ou *software* obtido, mesmo que venha de pessoas conhecidas;
- ❒ evitar fornecer muita informação, principalmente a pessoas que você acabou de conhecer;
- ❒ não fornecer, em hipótese alguma, informações sensíveis, tais como senhas ou números de cartões de crédito;
- ❒ configurar o programa para ocultar o seu endereço IP.

2.4 Programas de distribuição de arquivos

- ❒ manter seu programa de distribuição de arquivos sempre atualizado e bem configurado;
- ❒ ter um bom antivírus instalado em seu computador, mantê-lo atualizado e utilizá-lo para verificar qualquer arquivo obtido, pois eles podem conter vírus, cavalos de tróia, entre outros tipos de *malware*;
- ❒ certificar-se que os arquivos obtidos ou distribuídos são **livres**, ou seja, não violam as leis de direitos autorais.

2.5 Compartilhamento de recursos

- ❒ ter um bom antivírus instalado em seu computador, mantê-lo atualizado e utilizá-lo para verificar qualquer arquivo ou programa compartilhado, pois eles podem conter vírus, cavalos de tróia, entre outros tipos de *malware*;
- ❒ estabelecer senhas para os compartilhamentos, caso seja estritamente necessário compartilhar recursos do seu computador.

2.6 Cópias de segurança

- ❒ fazer cópias dos dados do computador regularmente;
- ❒ criptografar dados sensíveis;
- ❒ armazenar as cópias em local acondicionado, de acesso restrito e com segurança física;
- ❒ considerar a necessidade de armazenar as cópias em um local diferente daquele onde está o computador.

3 Fraude

3.1 Engenharia social

- ❒ não fornecer dados pessoais, números de cartões e senhas através de contato telefônico;
- ❒ ficar atento a *e-mails* ou telefonemas solicitando informações pessoais;
- ❒ não acessar *sites* ou seguir *links* recebidos por *e-mail* ou presentes em páginas sobre as quais não se saiba a procedência;
- ❒ sempre que houver dúvida sobre a real identidade do autor de uma mensagem ou ligação telefônica, entrar em contato com a instituição, provedor ou empresa para verificar a veracidade dos fatos.

3.2 Cuidados ao realizar transações bancárias ou comerciais

- ❒ seguir todas as recomendações sobre utilização do programa leitor de *e-mails* e do *browser* de maneira segura;
- ❒ estar atento e prevenir-se dos ataques de engenharia social;
- ❒ realizar transações somente em *sites* de instituições que você considere confiáveis;
- ❒ procurar sempre digitar em seu *browser* o endereço desejado. Não utilize *links* em páginas de terceiros ou recebidos por *e-mail*;
- ❒ certificar-se de que o endereço apresentado em seu *browser* corresponde ao *site* que você realmente quer acessar, antes de realizar qualquer ação;
- ❒ certificar-se que o *site* faz uso de conexão segura (ou seja, que os dados transmitidos entre seu *browser* e o *site* serão criptografados) e utiliza um tamanho de chave considerado seguro;
- ❒ antes de aceitar um novo certificado, verificar junto à instituição que mantém o *site* sobre sua emissão e quais são os dados nele contidos. Então, verificar o certificado do *site* antes de iniciar qualquer transação, para assegurar-se que ele foi emitido para a instituição que se deseja acessar e está dentro do prazo de validade;

- ❒ não acessar *sites* de comércio eletrônico ou *Internet Banking* através de computadores de terceiros;
- ❒ desligar sua *Webcam* (caso você possua alguma), ao acessar um *site* de comércio eletrônico ou *Internet banking*.

3.3 Boatos

- ❒ verificar sempre a procedência da mensagem e se o fato sendo descrito é verídico;
- ❒ verificar em *sites* especializados e em publicações da área se o *e-mail* recebido já não está catalogado como um boato.

4 Privacidade

4.1 *E-mails*

- ❒ utilizar criptografia sempre que precisar enviar um *e-mail* com informações sensíveis;
- ❒ certificar-se que seu programa leitor de *e-mails* grava as mensagens criptografadas, para garantir a segurança das mensagens armazenadas no disco.

4.2 *Cookies*

- ❒ desabilitar *cookies*, exceto para *sites* confiáveis e onde sejam realmente necessários;
- ❒ considerar o uso de *softwares* que permitem controlar o envio e recebimento de informações entre o *browser* e o *site* visitado.

4.3 Cuidados com dados pessoais em páginas *Web*, *blogs* e *sites* de redes de relacionamentos

- ❒ evitar disponibilizar seus dados pessoais ou de familiares e amigos (*e-mail*, telefone, endereço, data de aniversário, etc);
- ❒ evitar disponibilizar dados sobre o seu computador ou sobre os *softwares* que utiliza;
- ❒ evitar fornecer informações sobre o seu cotidiano (como, por exemplo, hora que saiu e voltou para casa, data de uma viagem programada, horário que foi ao caixa eletrônico, etc).
- ❒ **nunca** fornecer informações sensíveis (como senhas e números de cartão de crédito), a menos que esteja sendo realizada uma transação (comercial ou financeira) e se tenha certeza da idoneidade da instituição que mantém o *site*.

4.4 Cuidados com os dados armazenados em um disco rígido

- ❒ criptografar todos os dados sensíveis, principalmente se for um *notebook*;
- ❒ sobrescrever os dados do disco rígido antes de vender ou se desfazer do seu computador usado.

4.5 Cuidados com telefones celulares, PDAs e outros aparelhos com *bluetooth*

- ❒ manter o *bluetooth* do seu aparelho desabilitado e somente habilite-o quando for necessário;
- ❒ ficar atento às notícias, principalmente àquelas sobre segurança, veiculadas no *site* do fabricante do seu aparelho;
- ❒ aplicar todas as correções de segurança (*patches*) que forem disponibilizadas pelo fabricante do seu aparelho, para evitar que possua vulnerabilidades;
- ❒ caso você tenha comprado uma aparelho usado, restaurar as opções de fábrica e configurá-lo como no primeiro item, antes de inserir quaisquer dados.

5 Banda Larga e Redes Sem Fio (*Wireless*)

5.1 Proteção de um computador utilizando banda larga

- ❒ instalar um *firewall* pessoal e ficar atento aos registros de eventos (*logs*) gerados por este programa;
- ❒ 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 aplicadas;
- ❒ desligar o compartilhamento de disco, impressora, etc;
- ❒ mudar, se possível, a senha padrão do seu equipamento de banda larga (modem ADSL, por exemplo).

5.2 Proteção de uma rede utilizando banda larga

- ❒ 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.

5.3 Cuidados com um cliente de rede sem fio

- ❒ instalar um *firewall* pessoal;
- ❒ instalar e manter atualizado um bom programa antivírus;
- ❒ atualizar as assinaturas do antivírus diariamente;
- ❒ 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;
- ❒ verificar 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;
- ❒ 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;
- ❒ habilitar a rede *wireless* somente quando for usá-la e desabilitá-la após o uso.

5.4 Cuidados com uma rede sem fio doméstica

- ❒ mudar configurações padrão que acompanham o seu AP;
- ❒ verificar se seus equipamentos já suportam WPA (Wi-Fi *Protected Access*) e utilizá-lo sempre que possível;
- ❒ caso o WPA não esteja disponível, usar sempre que possível WEP (*Wired Equivalent Privacy*);
- ❒ 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.

6 *Spam*

- ❒ seguir todas as recomendações sobre utilização do programa leitor de *e-mails*;
- ❒ considerar a utilização de um *software* de filtragem de *e-mails*;
- ❒ verificar com seu provedor ou com o administrador da rede se é utilizado algum *software* de filtragem no servidor de *e-mails*;
- ❒ evitar responder a um *spam* ou enviar um *e-mail* solicitando a remoção da lista.

7 Incidentes de Segurança e Uso Abusivo da Rede

7.1 Registros de eventos (*logs*)

- ❒ verificar sempre os *logs* do *firewall* pessoal e de IDSs que estejam instalados no computador;
- ❒ verificar se não é um falso positivo, antes de notificar um incidente.

7.2 Notificações de incidentes

- ❒ incluir *logs* completos, com data, horário, *time zone* (fuso horário), endereço IP de origem, portas envolvidas, protocolo utilizado e qualquer outra informação que tenha feito parte da identificação do incidente;
- ❒ enviar a notificação para os contatos da rede e para os grupos de segurança das redes envolvidas;
- ❒ manter cert@cert.br na cópia das mensagens.