Comitê Gestor da Internet no Brasil

Cartilha de Segurança para Internet

Versão 3.1
2006

Cartilha de Segurança para Internet

Versão 3.1
2006

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

Comitê Gestor da Internet no Brasil
São Paulo

Cartilha de Segurança para Internet, versão 3.1 / CERT.br – São Paulo: Comitê Gestor da Internet no Brasil, 2006.

ISBN: 978-85-60062-06-5
ISBN: 85-60062-06-8

Textos e Revisão: Equipe do CERT.br
Jornalista Responsável: Mariana Balboni, MTB 28.997

Comitê Gestor da Internet no Brasil
http://www.cgi.br/
Tel: +55 11 5509-3511
Fax: +55 11 5509-3512

Prefácio

A Cartilha de Segurança para Internet é um documento com recomendações e dicas sobre como o usuário de Internet deve se comportar para aumentar a sua segurança e se proteger de possíveis ameaças.

Produzido pelo Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil – CERT.br, com o apoio do Comitê Gestor da Internet no Brasil – CGI.br, o documento apresenta o significado de diversos termos e conceitos utilizados na Internet e fornece uma série de procedimentos que visam melhorar a segurança de um computador.

Nós esperamos que esta Cartilha possa auxiliá-lo não só a compreender as ameaças do ambiente Internet, mas também a manter seu sistema mais seguro. Gostaríamos ainda de lembrar que é muito importante ficar sempre atento ao usar a Internet, pois somente aliando medidas técnicas a boas práticas é possível atingir um nível de segurança que permita o pleno uso da Internet.

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

Equipe do CERT.br
Outubro de 2006

Estrutura da Cartilha

Este documento conta com oito partes, que dividem o conteúdo em diferentes áreas relacionadas com a segurança da Internet, além de um glossário, um *checklist* e uma compilação de dicas rápidas.

Parte I: Conceitos de Segurança
Apresenta conceitos gerais de segurança de computadores, importantes para o entendimento das partes subseqüentes.

Parte II: Riscos Envolvidos no Uso da Internet e Métodos de Prevenção
Aborda diversos riscos envolvidos no uso da Internet e métodos de prevenção, como programas que possibilitam aumentar a segurança de um computador e medidas preventivas no dia-a-dia do uso da Internet.

Parte III: Privacidade
Discute questões relacionadas à privacidade do usuário ao utilizar a Internet e aos cuidados que ele deve ter com seus dados pessoais.

Parte IV: Fraudes na Internet
São abordadas questões relacionadas a fraudes na Internet e medidas preventivas que devem ser adotadas no acesso a *sites* de comércio eletrônico ou *Internet Banking*.

Parte V: Redes de Banda Larga e Redes Sem Fio (*Wireless*)
É dedicada aos usuários de conexões banda larga e de redes sem fio, sendo discutidas as implicações de segurança e métodos de prevenção peculiares a estes ambientes.

Parte VI: *Spam*
São discutidos os problemas acarretados pelo *spam*, principalmente aqueles que possam ter implicações de segurança, e métodos de prevenção.

Parte VII: Incidentes de Segurança e Uso Abusivo da Rede
Trata dos conceitos relacionados a incidentes de segurança, técnicas de detecção e recomendações sobre como proceder para notificar ataques recebidos via Internet.

Parte VIII: Códigos Maliciosos (*Malware*)
Agrupa informações detalhadas sobre os tipos mais comuns de códigos maliciosos que podem infectar os computadores dos usuários, dando ênfase no tipo de ameaça que cada código oferece e quais são as medidas de prevenção específicas para cada caso.

Glossário
Apresenta definições de diversos termos usados na Cartilha.

Checklist
Consiste em um resumo das boas práticas discutidas ao longo da Cartilha e que devem ser adotadas pelos usuários para se previnirem das ameaças discutidas. Pode ser usado como um guia rápido para conferir se as boas práticas estão sendo seguidas.

Dicas
Compilação de dicas básicas de segurança, que reúnem formas de prevenção contra os problemas mais freqüentes enfrentados pelos usuários de Internet.

Outros Formatos

A Cartilha de Segurança para Internet é um documento público e gratuito, disponível no *site* http://cartilha.cert.br/, em diversos formatos:

- arquivo PDF deste livro;
- arquivos PDF de cada uma das partes, do glossário e do *checklist*;
- dois *folders* de dicas:
  - em frente e verso (dobrável);
  - em tamanho A4;
- versão em HTML de todo o conteúdo.

Licença de Uso da Cartilha

Histórico da Cartilha

No início de 2000, um grupo de estudos que, entre outros, envolveu a Abranet e o CERT.br (que à época chamava-se NBSO – NIC BR Security Office), identificou a necessidade de um guia com informações sobre segurança que pudesse ser usado como referência pelos diversos setores usuários de Internet. Como conseqüência, a pedido do Comitê Gestor da Internet no Brasil e sob supervisão do CERT.br, em julho do mesmo ano foi lançada a Cartilha de Segurança para Internet Versão 1.0.

Em 2003 foi verificada a necessidade de uma revisão geral do documento, que não só incluísse novos tópicos, mas que também facilitasse sua leitura e a localização de assuntos específicos. Neste processo de revisão a Cartilha foi completamente reescrita, dando origem à versão 2.0. Esta versão, a primeira totalmente sob responsabilidade do CERT.br, consolidou o formato e a base de conteúdo que até hoje compõem o documento, trazendo a divisão em partes, o *checklist* e o glossário. Também nesta versão foram introduzidas as seções relativas a fraudes na Internet, banda larga, redes sem fio, *spam* e incidentes de segurança.

Na versão 3.0, de 2005, a Cartilha continuou com sua estrutura, mas, devido à evolução da tecnologia, novos assuntos foram incluídos. Foi criada uma parte específica sobre códigos maliciosos, expandida a parte sobre segurança de redes sem fio e incluídos tópicos específicos sobre segurança em dispositivos móveis, como telefones celulares e computadores de mão. Esta versão também foi a primeira a disponibilizar um folheto com as dicas básicas para proteção contra as ameaças mais comuns.

A versão 3.1 não introduziu partes novas, mas incorporou diversas sugestões de melhoria recebidas, corrigiu alguns erros de digitação e atendeu a um pedido de muitos leitores: lançá-la em formato de livro, para facilitar a leitura e a impressão do conteúdo completo.

Agradecimentos

Agradecemos a todos leitores da Cartilha, que têm contribuído para a elaboração deste documento, enviando comentários, críticas, sugestões ou revisões.

Agradecemos especialmente a Nelson Murilo pela contribuição na Parte V, em particular redes sem fio; a Luiz E. R. Cordeiro pelo texto da primeira versão; a Marcelo H. P. C. Chaves pela produção da Versão 2.0, que deu origem ao documento atual, e por ser o principal mantenedor da Cartilha; e a Rafael Rodrigues Obelheiro por ter sido nosso revisor externo e por ter contribuído com diversas idéias para tópicos a serem abordados no documento.

Sumário

Lista de Figuras

Parte I: Conceitos de Segurança

Esta parte da Cartilha apresenta conceitos de segurança de computadores, onde são abordados temas relacionados às senhas, engenharia social, *malware*, vulnerabilidade, ataques de negação de serviço, criptografia e certificados digitais. Os conceitos aqui apresentados são importantes para o entendimento de partes subseqüentes desta Cartilha.

1.1 Segurança de Computadores

Um computador (ou sistema computacional) é dito seguro se este atende a três requisitos básicos relacionados aos recursos que o compõem: confidencialidade, integridade e disponibilidade.

A confidencialidade diz que a informação só está disponível para aqueles devidamente autorizados; a integridade diz que a informação não é destruída ou corrompida e o sistema tem um desempenho correto, e a disponibilidade diz que os serviços/recursos do sistema estão disponíveis sempre que forem necessários.

Alguns exemplos de violações a cada um desses requisitos são:

Confidencialidade: alguém obtém acesso não autorizado ao seu computador e lê todas as informações contidas na sua declaração de Imposto de Renda;

Integridade: alguém obtém acesso não autorizado ao seu computador e altera informações da sua declaração de Imposto de Renda, momentos antes de você enviá-la à Receita Federal;

Disponibilidade: o seu provedor sofre uma grande sobrecarga de dados ou um ataque de negação de serviço e por este motivo você fica impossibilitado de enviar sua declaração de Imposto de Renda à Receita Federal.

1.1.1 Por que devo me preocupar com a segurança do meu computador?

Computadores domésticos são utilizados para realizar inúmeras tarefas, tais como: transações financeiras, sejam elas bancárias ou mesmo compra de produtos e serviços; comunicação, por exemplo, através de *e-mails*; armazenamento de dados, sejam eles pessoais ou comerciais, etc.

É importante que você se preocupe com a segurança de seu computador, pois você, provavelmente, não gostaria que:

- suas senhas e números de cartões de crédito fossem furtados e utilizados por terceiros;

- sua conta de acesso a Internet fosse utilizada por alguém não autorizado;
- seus dados pessoais, ou até mesmo comerciais, fossem alterados, destruídos ou visualizados por terceiros;
- seu computador deixasse de funcionar, por ter sido comprometido e arquivos essenciais do sistema terem sido apagados, etc.

1.1.2 Por que alguém iria querer invadir meu computador?

A resposta para esta pergunta não é simples. Os motivos pelos quais alguém tentaria invadir seu computador são inúmeros. Alguns destes motivos podem ser:

- utilizar seu computador em alguma atividade ilícita, para esconder a real identidade e localização do invasor;
- utilizar seu computador para lançar ataques contra outros computadores;
- utilizar seu disco rígido como repositório de dados;
- destruir informações (vandalismo);
- disseminar mensagens alarmantes e falsas;
- ler e enviar *e-mails* em seu nome;
- propagar vírus de computador;
- furtar números de cartões de crédito e senhas bancárias;
- furtar a senha da conta de seu provedor, para acessar a Internet se fazendo passar por você;
- furtar dados do seu computador, como por exemplo, informações do seu Imposto de Renda.

1.2 Senhas

Uma senha (*password*) na Internet, ou em qualquer sistema computacional, serve para autenticar o usuário, ou seja, é utilizada no processo de verificação da identidade do usuário, assegurando que este é realmente quem diz ser.

Se uma outra pessoa tem acesso a sua senha, ela poderá utilizá-la para se passar por você na Internet. Alguns dos motivos pelos quais uma pessoa poderia utilizar sua senha são:

- ler e enviar *e-mails* em seu nome;
- obter informações sensíveis dos dados armazenados em seu computador, tais como números de cartões de crédito;
- esconder sua real identidade e então desferir ataques contra computadores de terceiros.

Portanto, a senha merece consideração especial, afinal ela é de sua inteira responsabilidade.

1.2.1 O que não se deve usar na elaboração de uma senha?

Nomes, sobrenomes, números de documentos, placas de carros, números de telefones e datas[1] deverão estar **fora** de sua lista de senhas. Esses dados podem ser facilmente obtidos e uma pessoa mal intencionada, possivelmente, utilizaria este tipo de informação para tentar se autenticar como você.

Existem várias regras de criação de senhas, sendo que uma regra muito importante é **jamais** utilizar palavras que façam parte de dicionários. Existem *softwares* que tentam descobrir senhas combinando e testando palavras em diversos idiomas e geralmente possuem listas de palavras (dicionários) e listas de nomes (nomes próprios, músicas, filmes, etc.).

1.2.2 O que é uma boa senha?

Uma boa senha deve ter pelo menos oito caracteres[2] (letras, números e símbolos), deve ser simples de digitar e, o mais importante, deve ser fácil de lembrar.

Normalmente os sistemas diferenciam letras maiúsculas das minúsculas, o que já ajuda na composição da senha. Por exemplo, "`pAraleLepiPedo`" e "`paRalElePipEdo`" são senhas diferentes. Entretanto, são senhas fáceis de descobrir utilizando *softwares* para quebra de senhas, pois não possuem números e símbolos, além de conter muitas repetições de letras.

1.2.3 Como elaborar uma boa senha?

Quanto mais "bagunçada" for a senha melhor, pois mais difícil será descobrí-la[3]. Assim, tente misturar letras maiúsculas, minúsculas, números e sinais de pontuação. Uma regra realmente prática e que gera boas senhas difíceis de serem descobertas é utilizar uma frase qualquer e pegar a primeira, segunda ou a última letra de cada palavra.

Por exemplo, usando a frase "batatinha quando nasce se esparrama pelo chão" podemos gerar a senha "`!BqnsepC`" (o sinal de exclamação foi colocado no início para acrescentar um símbolo à senha). Senhas geradas desta maneira são fáceis de lembrar e são normalmente difíceis de serem descobertas.

Mas lembre-se: a senha "`!BqnsepC`" deixou de ser uma boa senha, pois faz parte desta Cartilha.

Vale ressaltar que se você tiver dificuldades para memorizar uma senha forte, é preferível anotá-la e guardá-la em local seguro, do que optar pelo uso de senhas fracas.

1.2.4 Quantas senhas diferentes devo usar?

Procure identificar o número de locais onde você necessita utilizar uma senha. Este número deve ser equivalente a quantidade de senhas **distintas** a serem mantidas por você. Utilizar senhas

[1] Qualquer data que possa estar relacionada com você, como por exemplo a data de seu aniversário ou de familiares.

[2] Existem serviços que permitem utilizar senhas maiores do que oito caracteres. Quanto maior for a senha, mais difícil será descobrí-la, portanto procure utilizar a senha de maior tamanho possível.

[3] Observe que a senha "`1qaz2wsx`" parece ser suficientemente "bagunçada", mas não é considerada uma boa senha, pois está associada à proximidade entre esses caracteres no teclado.

diferentes, uma para cada local, é extremamente importante, pois pode atenuar os prejuízos causados, caso alguém descubra uma de suas senhas.

Para ressaltar a importância do uso de senhas diferentes, imagine que você é responsável por realizar movimentações financeiras em um conjunto de contas bancárias e todas estas contas possuem a mesma senha. Então, procure responder as seguintes perguntas:

- Quais seriam as conseqüências se alguém descobrisse esta senha?
- E se fossem usadas senhas diferentes para cada conta, caso alguém descobrisse uma das senhas, um possível prejuízo teria a mesma proporção?

1.2.5 Com que freqüência devo mudar minhas senhas?

Você deve trocar suas senhas regularmente, procurando evitar períodos muito longos. Uma sugestão é que você realize tais trocas a cada dois ou três meses.

Procure identificar se os serviços que você utiliza e que necessitam de senha, quer seja o acesso ao seu provedor, *e-mail*, conta bancária, ou outro, disponibilizam funcionalidades para alterar senhas e use regularmente tais funcionalidades.

Caso você não possa escolher sua senha na hora em que contratar o serviço, procure trocá-la com a maior urgência possível. Procure utilizar serviços em que você possa escolher a sua senha.

Lembre-se que trocas regulares são muito importantes para assegurar a confidencialidade de suas senhas.

1.2.6 Quais os cuidados especiais que devo ter com as senhas?

De nada adianta elaborar uma senha bastante segura e difícil de ser descoberta, se ao usar a senha alguém puder vê-la. Existem várias maneiras de alguém poder descobrir a sua senha. Dentre elas, alguém poderia:

- observar o processo de digitação da sua senha;
- utilizar algum método de persuasão, para tentar convencê-lo a entregar sua senha (vide seção 1.4.1);
- capturar sua senha enquanto ela trafega pela rede.

Em relação a este último caso, existem técnicas que permitem observar dados, à medida que estes trafegam entre redes. É possível que alguém extraia informações sensíveis desses dados, como por exemplo senhas, caso não estejam criptografados (vide seção 1.8).

Portanto, alguns dos principais cuidados que você deve ter com suas senhas são:

- certifique-se de não estar sendo observado ao digitar a sua senha;
- não forneça sua senha para qualquer pessoa, em hipótese alguma;

- não utilize computadores de terceiros (por exemplo, em *LAN houses*, *cybercafes*, *stands* de eventos, etc) em operações que necessitem utilizar suas senhas;
- certifique-se que seu provedor disponibiliza serviços criptografados, principalmente para aqueles que envolvam o fornecimento de uma senha.

1.2.7 Que cuidados devo ter com o usuário e senha de *Administrator* (ou *root*) em um computador?

O usuário *Administrator* (ou *root*) é de extrema importância, pois detém todos os privilégios em um computador. Ele deve ser usado em situações onde um usuário normal não tenha privilégios para realizar uma operação, como por exemplo, em determinadas tarefas administrativas, de manutenção ou na instalação e configuração de determinados tipos de *software*.

Sabe-se que, por uma questão de comodidade e principalmente no ambiente doméstico, muitas pessoas utilizam o usuário *Administrator* (ou *root*) para realizar todo e qualquer tipo de atividade. Ele é usado para se conectar à Internet, navegar utilizando o *browser*, ler *e-mails*, redigir documentos, etc.

Este é um procedimento que deve ser **sempre evitado**, pois você, como usuário *Administrator* (ou *root*), poderia acidentalmente apagar arquivos essenciais para o funcionamento do sistema operacional ou de algum *software* instalado em seu computador. Ou ainda, poderia instalar inadvertidamente um *software* malicioso que, como usuário *Administrator* (ou *root*), teria todos os privilégios que necessitasse, podendo fazer qualquer coisa.

Portanto, alguns dos principais cuidados que você deve ter são:

- elaborar uma boa senha para o usuário *Administrator* (ou *root*), como discutido na seção 1.2.3, e seguir os procedimentos descritos na seção 1.2.6;
- utilizar o usuário *Administrator* (ou *root*) somente quando for estritamente necessário;
- criar tantos usuários com privilégios normais, quantas forem as pessoas que utilizam seu computador, para substituir assim o usuário *Administrator* (ou *root*) em tarefas rotineiras, como leitura de *e-mails*, navegação na Internet, produção de documentos, etc.

1.3 *Cookies*

Cookies são pequenas informações que os *sites* visitados por você podem armazenar em seu *browser*. Estes são utilizados pelos *sites* de diversas formas, tais como:

- guardar a sua identificação e senha quando você vai de uma página para outra;
- manter listas de compras ou listas de produtos preferidos em *sites* de comércio eletrônico;
- personalizar *sites* pessoais ou de notícias, quando você escolhe o que quer que seja mostrado nas páginas;

- manter a lista das páginas vistas em um *site*, para estatística ou para retirar as páginas que você não tem interesse dos *links*.

A Parte III: Privacidade apresenta alguns problemas relacionados aos *cookies*, bem como algumas sugestões para que se tenha maior controle sobre eles.

1.4 Engenharia Social

O termo é utilizado para descrever um método de ataque, onde alguém faz uso da persuasão, muitas vezes abusando da ingenuidade ou confiança do usuário, para obter informações que podem ser utilizadas para ter acesso não autorizado a computadores ou informações.

1.4.1 Que exemplos podem ser citados sobre este método de ataque?

Os dois primeiros exemplos apresentam casos onde foram utilizadas mensagens de *e-mail*. O último exemplo apresenta um ataque realizado por telefone.

Exemplo 1: você recebe uma mensagem *e-mail*, onde o remetente é o gerente ou alguém em nome do departamento de suporte do seu banco. Na mensagem ele diz que o serviço de *Internet Banking* está apresentando algum problema e que tal problema pode ser corrigido se você executar o aplicativo que está anexado à mensagem. A execução deste aplicativo apresenta uma tela análoga àquela que você utiliza para ter acesso a conta bancária, aguardando que você digite sua senha. Na verdade, este aplicativo está preparado para furtar sua senha de acesso a conta bancária e enviá-la para o atacante.

Exemplo 2: você recebe uma mensagem de *e-mail*, dizendo que seu computador está infectado por um vírus. A mensagem sugere que você instale uma ferramenta disponível em um *site* da Internet, para eliminar o vírus de seu computador. A real função desta ferramenta não é eliminar um vírus, mas sim permitir que alguém tenha acesso ao seu computador e a todos os dados nele armazenados.

Exemplo 3: algum desconhecido liga para a sua casa e diz ser do suporte técnico do seu provedor. Nesta ligação ele diz que sua conexão com a Internet está apresentando algum problema e, então, pede sua senha para corrigí-lo. Caso você entregue sua senha, este suposto técnico poderá realizar uma infinidade de atividades maliciosas, utilizando a sua conta de acesso a Internet e, portanto, relacionando tais atividades ao seu nome.

Estes casos mostram ataques típicos de engenharia social, pois os discursos apresentados nos exemplos procuram **induzir** o usuário a realizar alguma tarefa e o **sucesso** do ataque depende única e exclusivamente da **decisão** do usuário em fornecer informações sensíveis ou executar programas.

A Parte IV: Fraudes na Internet apresenta algumas formas de se prevenir deste tipo de ataque.

1.5 Vulnerabilidade

Vulnerabilidade é definida como uma falha no projeto, implementação ou configuração de um *software* ou sistema operacional que, quando explorada por um atacante, resulta na violação da segurança de um computador.

Existem casos onde um *software* ou sistema operacional instalado em um computador pode conter uma vulnerabilidade que permite sua exploração remota, ou seja, através da rede. Portanto, um atacante conectado à Internet, ao explorar tal vulnerabilidade, pode obter acesso não autorizado ao computador vulnerável.

A Parte II: Riscos Envolvidos no Uso da Internet e Métodos de Prevenção apresenta algumas formas de identificação de vulnerabilidades, bem como maneiras de prevenção e correção.

1.6 Códigos Maliciosos (*Malware*)

Código malicioso ou *Malware* (***Mal****icious Soft****ware***) é um termo genérico que abrange todos os tipos de programa especificamente desenvolvidos para executar ações maliciosas em um computador. Na literatura de segurança o termo *malware* também é conhecido por "*software* malicioso".

Alguns exemplos de *malware* são:

- vírus;
- *worms* e *bots*;
- *backdoors*;
- cavalos de tróia;
- *keyloggers* e outros programas *spyware*;
- *rootkits*.

A Parte VIII: Códigos Maliciosos (*Malware*) apresenta descrições detalhadas e formas de identificação e prevenção para os diversos tipos de código malicioso.

1.7 Negação de Serviço (*Denial of Service*)

Nos ataques de negação de serviço (DoS – *Denial of Service*) o atacante utiliza **um** computador para tirar de operação um serviço ou computador conectado à Internet.

Exemplos deste tipo de ataque são:

- gerar uma grande sobrecarga no processamento de dados de um computador, de modo que o usuário não consiga utilizá-lo;

- gerar um grande tráfego de dados para uma rede, ocupando toda a banda disponível, de modo que qualquer computador desta rede fique indisponível;
- tirar serviços importantes de um provedor do ar, impossibilitando o acesso dos usuários a suas caixas de correio no servidor de *e-mail* ou ao servidor *Web*.

1.7.1 O que é DDoS?

DDoS (*Distributed Denial of Service*) constitui um ataque de negação de serviço distribuído, ou seja, **um conjunto** de computadores é utilizado para tirar de operação um ou mais serviços ou computadores conectados à Internet.

Normalmente estes ataques procuram ocupar toda a banda disponível para o acesso a um computador ou rede, causando grande lentidão ou até mesmo indisponibilizando qualquer comunicação com este computador ou rede.

1.7.2 Se uma rede ou computador sofrer um DoS, isto significa que houve uma invasão?

Não. O objetivo de tais ataques é indisponibilizar o uso de um ou mais computadores, e não invadí-los. É importante notar que, principalmente em casos de DDoS, computadores comprometidos podem ser utilizados para desferir os ataques de negação de serviço.

Um exemplo deste tipo de ataque ocorreu no início de 2000, onde computadores de várias partes do mundo foram utilizados para indisponibilizar o acesso aos *sites* de algumas empresas de comércio eletrônico. Estas empresas não tiveram seus computadores comprometidos, mas sim ficaram impossibilitadas de vender seus produtos durante um longo período.

1.8 Criptografia

Criptografia é a ciência e arte de escrever mensagens em forma cifrada ou em código. É parte de um campo de estudos que trata das comunicações secretas, usadas, dentre outras finalidades, para:

- autenticar a identidade de usuários;
- autenticar e proteger o sigilo de comunicações pessoais e de transações comerciais e bancárias;
- proteger a integridade de transferências eletrônicas de fundos.

Uma mensagem codificada por um método de criptografia deve ser **privada**, ou seja, somente aquele que enviou e aquele que recebeu devem ter acesso ao conteúdo da mensagem. Além disso, uma mensagem deve poder ser **assinada**, ou seja, a pessoa que a recebeu deve poder verificar se o remetente é mesmo a pessoa que diz ser e ter a capacidade de identificar se uma mensagem pode ter sido modificada.

Os métodos de criptografia atuais são seguros e eficientes e baseiam-se no uso de uma ou mais **chaves**. A chave é uma seqüência de caracteres, que pode conter letras, dígitos e símbolos (como uma senha), e que é convertida em um número, utilizado pelos métodos de criptografia para codificar e decodificar mensagens.

Atualmente, os métodos criptográficos podem ser subdivididos em duas grandes categorias, de acordo com o tipo de chave utilizada: a criptografia de chave única (vide seção 1.8.1) e a criptografia de chave pública e privada (vide seção 1.8.2).

1.8.1 O que é criptografia de chave única?

A criptografia de chave única utiliza a mesma chave tanto para codificar quanto para decodificar mensagens. Apesar deste método ser bastante eficiente em relação ao tempo de processamento, ou seja, o tempo gasto para codificar e decodificar mensagens, tem como principal desvantagem a necessidade de utilização de um meio seguro para que a chave possa ser compartilhada entre pessoas ou entidades que desejem trocar informações criptografadas.

Exemplos de utilização deste método de criptografia e sugestões para o tamanho mínimo da chave única podem ser vistos nas seções 1.8.4 e 1.8.5, respectivamente.

1.8.2 O que é criptografia de chaves pública e privada?

A criptografia de chaves pública e privada utiliza duas chaves distintas, uma para codificar e outra para decodificar mensagens. Neste método cada pessoa ou entidade mantém duas chaves: uma pública, que pode ser divulgada livremente, e outra privada, que deve ser mantida em segredo pelo seu dono. As mensagens codificadas com a chave pública só podem ser decodificadas com a chave privada correspondente.

Seja o exemplo, onde José e Maria querem se comunicar de maneira sigilosa. Então, eles terão que realizar os seguintes procedimentos:

1. José codifica uma mensagem utilizando a chave pública de Maria, que está disponível para o uso de qualquer pessoa;
2. Depois de criptografada, José envia a mensagem para Maria, através da Internet;
3. Maria recebe e decodifica a mensagem, utilizando sua chave privada, que é apenas de seu conhecimento;
4. Se Maria quiser responder a mensagem, deverá realizar o mesmo procedimento, mas utilizando a chave pública de José.

Apesar deste método ter o desempenho bem inferior em relação ao tempo de processamento, quando comparado ao método de criptografia de chave única (seção 1.8.1), apresenta como principal vantagem a livre distribuição de chaves públicas, não necessitando de um meio seguro para que chaves sejam combinadas antecipadamente. Além disso, pode ser utilizado na geração de assinaturas digitais, como mostra a seção 1.8.3.

Exemplos de utilização deste método de criptografia e sugestões para o tamanho mínimo das chaves pública e privada podem ser vistos nas seções 1.8.4 e 1.8.5, respectivamente.

1.8.3 O que é assinatura digital?

A assinatura digital consiste na criação de um código, através da utilização de uma chave privada, de modo que a pessoa ou entidade que receber uma mensagem contendo este código possa verificar se o remetente é mesmo quem diz ser e identificar qualquer mensagem que possa ter sido modificada.

Desta forma, é utilizado o método de criptografia de chaves pública e privada, mas em um processo inverso ao apresentado no exemplo da seção 1.8.2.

Se José quiser enviar uma mensagem assinada para Maria, ele codificará a mensagem com sua chave privada. Neste processo será gerada uma assinatura digital, que será adicionada à mensagem enviada para Maria. Ao receber a mensagem, Maria utilizará a chave pública de José para decodificar a mensagem. Neste processo será gerada uma segunda assinatura digital, que será comparada à primeira. Se as assinaturas forem idênticas, Maria terá certeza que o remetente da mensagem foi o José e que a mensagem não foi modificada.

É importante ressaltar que a segurança do método baseia-se no fato de que a chave privada é conhecida apenas pelo seu dono. Também é importante ressaltar que o fato de assinar uma mensagem não significa gerar uma mensagem sigilosa. Para o exemplo anterior, se José quisesse assinar a mensagem e ter certeza de que apenas Maria teria acesso a seu conteúdo, seria preciso codificá-la com a chave pública de Maria, depois de assiná-la.

1.8.4 Que exemplos podem ser citados sobre o uso de criptografia de chave única e de chaves pública e privada?

Exemplos que combinam a utilização dos métodos de criptografia de chave única e de chaves pública e privada são as conexões seguras, estabelecidas entre o *browser* de um usuário e um *site*, em transações comerciais ou bancárias via *Web*.

Estas conexões seguras via *Web* utilizam o método de criptografia de chave única, implementado pelo protocolo SSL (*Secure Socket Layer*). O *browser* do usuário precisa informar ao *site* qual será a chave única utilizada na conexão segura, antes de iniciar a transmissão de dados sigilosos.

Para isto, o *browser* obtém a chave pública do certificado[4] da instituição que mantém o *site*. Então, ele utiliza esta chave pública para codificar e enviar uma mensagem para o *site*, contendo a chave única a ser utilizada na conexão segura. O *site* utiliza sua chave privada para decodificar a mensagem e identificar a chave única que será utilizada.

A partir deste ponto, o *browser* do usuário e o *site* podem transmitir informações, de forma sigilosa e segura, através da utilização do método de criptografia de chave única. A chave única pode ser trocada em intervalos de tempo determinados, através da repetição dos procedimentos descritos anteriormente, aumentando assim o nível de segurança de todo o processo.

1.8.5 Que tamanho de chave deve ser utilizado?

Os métodos de criptografia atualmente utilizados, e que apresentam bons níveis de segurança, são publicamente conhecidos e são seguros pela robustez de seus algoritmos e pelo tamanho das chaves que utilizam.

[4] Certificados são discutidos na seção 1.9 e na Parte IV: Fraudes na Internet.

Para que um atacante descubra uma chave ele precisa utilizar algum método de força bruta, ou seja, testar combinações de chaves até que a correta seja descoberta. Portanto, quanto maior for a chave, maior será o número de combinações a testar, inviabilizando assim a descoberta de uma chave em tempo hábil. Além disso, chaves podem ser trocadas regularmente, tornando os métodos de criptografia ainda mais seguros.

Atualmente, para se obter um bom nível de segurança na utilização do método de criptografia de chave única, é aconselhável utilizar chaves de no mínimo 128 bits. E para o método de criptografia de chaves pública e privada é aconselhável utilizar chaves de 2048 bits, sendo o mínimo aceitável de 1024 bits. Dependendo dos fins para os quais os métodos criptográficos serão utilizados, deve-se considerar a utilização de chaves maiores: 256 ou 512 bits para chave única e 4096 ou 8192 bits para chaves pública e privada.

1.9 Certificado Digital

O certificado digital é um arquivo eletrônico que contém dados de uma pessoa ou instituição, utilizados para comprovar sua identidade. Este arquivo pode estar armazenado em um computador ou em outra mídia, como um *token* ou *smart card*.

Exemplos semelhantes a um certificado digital são o CNPJ, RG, CPF e carteira de habilitação de uma pessoa. Cada um deles contém um conjunto de informações que identificam a instituição ou pessoa e a autoridade (para estes exemplos, órgãos públicos) que garante sua validade.

Algumas das principais informações encontradas em um certificado digital são:

- dados que identificam o dono (nome, número de identificação, estado, etc);
- nome da Autoridade Certificadora (AC) que emitiu o certificado (vide seção 1.9.1);
- o número de série e o período de validade do certificado;
- a assinatura digital da AC.

O objetivo da assinatura digital no certificado é indicar que uma outra entidade (a Autoridade Certificadora) garante a veracidade das informações nele contidas.

1.9.1 O que é Autoridade Certificadora (AC)?

Autoridade Certificadora (AC) é a entidade responsável por emitir certificados digitais. Estes certificados podem ser emitidos para diversos tipos de entidades, tais como: pessoa, computador, departamento de uma instituição, instituição, etc.

Os certificados digitais possuem uma forma de assinatura eletrônica da AC que o emitiu. Graças à sua idoneidade, a AC é normalmente reconhecida por todos como confiável, fazendo o papel de "Cartório Eletrônico".

1.9.2 Que exemplos podem ser citados sobre o uso de certificados?

Alguns exemplos típicos do uso de certificados digitais são:

- quando você acessa um *site* com conexão segura, como por exemplo o acesso a sua conta bancária pela Internet (vide Parte IV: Fraudes na Internet), é possível checar se o *site* apresentado é realmente da instituição que diz ser, através da verificação de seu certificado digital;
- quando você consulta seu banco pela Internet, este tem que se assegurar de sua identidade antes de fornecer informações sobre a conta;
- quando você envia um *e-mail* importante, seu aplicativo de *e-mail* pode utilizar seu certificado para assinar "digitalmente" a mensagem, de modo a assegurar ao destinatário que o *e-mail* é seu e que não foi adulterado entre o envio e o recebimento.

A Parte IV: Fraudes na Internet apresenta algumas medidas de segurança relacionadas ao uso de certificados digitais.

Parte II: Riscos Envolvidos no Uso da Internet e Métodos de Prevenção

Esta parte da Cartilha aborda diversos riscos envolvidos no uso da Internet e seus métodos de prevenção. São discutidos os programas que possibilitam aumentar a segurança de um computador, como antivírus e *firewalls*, e apresentados riscos e medidas preventivas no uso de programas leitores de *e-mails*, *browsers*, programas de troca de mensagens, de distribuição de arquivos e recursos de compartilhamento de arquivos. Também é discutida a importância da realização de cópias de segurança.

2.1 Programas Leitores de *E-mails*

2.1.1 Quais são os riscos associados ao uso de um programa leitor de *e-mails*?

Grande parte dos problemas de segurança envolvendo *e-mails* estão relacionados aos conteúdos das mensagens, que normalmente abusam das técnicas de engenharia social (vide Parte I: Conceitos de Segurança e Parte IV: Fraudes na Internet) ou de características de determinados programas leitores de *e-mails*, que permitem abrir arquivos ou executar programas anexados às mensagens automaticamente.

2.1.2 É possível configurar um programa leitor de *e-mails* de forma mais segura?

Sim. Algumas dicas de configuração para melhorar a segurança do seu programa leitor de *e-mails* são:

1. desligar as opções que permitem abrir ou executar automaticamente arquivos ou programas anexados às mensagens;
2. desligar as opções de execução de *JavaScript* e de programas *Java* (vide seção 2.2.2);
3. desligar, se possível, o modo de visualização de *e-mails* no formato HTML (mais detalhes na Parte IV: Fraudes na Internet e Parte VI: *Spam*).

Estas configurações podem evitar que o seu programa leitor de *e-mails* propague automaticamente vírus e cavalos de tróia, entre outros. Existem programas leitores de *e-mails* que não implementam tais funções e, portanto, não possuem estas opções.

É importante ressaltar que se o usuário seguir as recomendações dos itens 1 e 2, mas ainda assim abrir os arquivos ou executar manualmente os programas que vêm anexados aos *e-mails*, poderá ter algum problema que resulte na violação da segurança do seu computador.

2.1.3 Que medidas preventivas devo adotar no uso dos programas leitores de *e-mails*?

Algumas medidas preventivas que minimizam os problemas trazidos com os *e-mails* são:

- manter sempre a versão mais atualizada do seu programa leitor de *e-mails*;
- não clicar em *links* que, por ventura, possam aparecer no conteúdo do *e-mail*. Se você realmente quiser acessar a página do *link*, digite o endereço diretamente no seu *browser*, seguindo as orientações da seção 2.2.7;
- evitar 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[1] 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 o modo de visualização de *e-mails* no formato HTML.

Atualmente, usuários da Internet têm sido bombardeados com *e-mails* indesejáveis e, principalmente, com mensagens fraudulentas cuja finalidade é a obtenção de vantagens financeiras. Alguns exemplos são:

- mensagens oferecendo grandes quantias em dinheiro, mediante uma transferência eletrônica de fundos;
- mensagens com ofertas de produtos com preços muito abaixo dos preços praticados pelo mercado;
- mensagens que procuram induzir o usuário a acessar uma determinada página na Internet ou a instalar um programa, abrir um álbum de fotos, ver cartões virtuais, etc, mas cujo verdadeiro intuito é fazer com que o usuário forneça dados pessoais e sensíveis, como contas bancárias, senhas e números de cartões de crédito.

Mais detalhes sobre estes tipos de *e-mail*, bem como formas de prevenção, podem ser vistos na Parte IV: Fraudes na Internet.

[1] Existem vírus e outros tipos de *software* malicioso que utilizam o *e-mail* como meio para sua propagação e quase sempre forjam o endereço do remetente.

2.2 *Browsers*

2.2.1 Quais são os riscos associados ao uso de um *browser*?

Existem diversos riscos envolvidos na utilização de um *browser*. Dentre eles, podem-se citar:

- execução de *JavaScript* ou de programas *Java* hostis;
- execução de programas ou controles *ActiveX* hostis;
- obtenção e execução de programas hostis em *sites* não confiáveis ou falsos;
- acesso a *sites* falsos, se fazendo passar por instituições bancárias ou de comércio eletrônico;
- realização de transações comerciais ou bancárias via *Web*, sem qualquer mecanismo de segurança.

Nos dois primeiros casos o *browser* executa os programas automaticamente, ou seja, sem a interferência do usuário.

2.2.2 Quais são os riscos associados à execução de *JavaScripts* e de programas *Java*?

Normalmente os *browsers* contêm módulos específicos para processar programas *Java*. Apesar destes módulos fornecerem mecanismos de segurança, podem conter falhas de implementação e, neste caso, permitir que um programa *Java* hostil cause alguma violação de segurança em um computador.

JavaScripts, entre outros *scripts Web* disponíveis, são muito utilizados atualmente para incorporar maior funcionalidade e melhorar a aparência de páginas *Web*. Apesar de nem sempre apresentarem riscos, vêm sendo utilizados por atacantes para causar violações de segurança em computadores. Um tipo de ataque envolvendo *JavaScript* consiste em redirecionar usuários de um *site* legítimo para um *site* falso, para que o usuário instale programas maliciosos ou forneça informações pessoais.

2.2.3 Quais são os riscos associados à execução de programas *ActiveX*?

Antes de receber um programa *ActiveX*, o seu *browser* verifica sua procedência através de um esquema de certificados digitais (vide Parte I: Conceitos de Segurança e Parte IV: Fraudes na Internet). Se você optar por aceitar o certificado, o programa é executado em seu computador.

Ao serem executados, os programas *ActiveX* podem fazer de tudo, desde enviar um arquivo qualquer pela Internet, até instalar programas (que podem ter fins maliciosos) em seu computador.

2.2.4 Quais são os riscos associados ao uso de *cookies*?

Muitos *sites* utilizam *cookies* para obter informações, como por exemplo, as preferências de um usuário. Estas informações, muitas vezes, são compartilhadas entre diversas entidades na Internet e podem afetar a privacidade do usuário.

Maiores detalhes sobre os riscos envolvidos no uso de *cookies*, bem como formas de se ter maior controle sobre eles, podem ser vistos na Parte III: Privacidade.

2.2.5 Quais são os riscos associados às *pop-up windows*?

Pop-up windows são janelas que aparecem automaticamente e sem permissão, sobrepondo a janela do *browser*, após o usuário acessar um *site*. Este recurso tem sido amplamente utilizado para apresentar mensagens com propaganda para usuários da Internet e, por este motivo, tem sido também classificado como *pop-up spam*.

Em muitos casos, as mensagens contidas nas *pop-up windows* apresentam *links*, que podem redirecionar o usuário para uma página fraudulenta ou induzí-lo a instalar algum *software* malicioso para, por exemplo, furtar senhas bancárias ou números de cartões de crédito. Exemplos do uso malicioso de *pop-up windows* podem ser vistos na Parte IV: Fraudes na Internet.

2.2.6 Quais são os cuidados necessários para realizar transações via *Web*?

Normalmente as transações, sejam comerciais ou bancárias, envolvem informações sensíveis, como senhas ou números de cartões de crédito.

Portanto, é muito importante que você, ao realizar transações via *Web*, certifique-se da procedência dos *sites* e se estes *sites* são realmente das instituições que dizem ser. Também é fundamental que eles forneçam mecanismos de segurança para evitar que alguém conectado à Internet possa obter informações sensíveis de suas transações, no momento em que estiverem sendo realizadas.

Maiores detalhes sobre estes cuidados, bem como formas de prevenção na realização de transações via *Web* podem ser vistos na Parte IV: Fraudes na Internet.

2.2.7 Que medidas preventivas devo adotar no uso de *browsers*?

Algumas medidas preventivas para o uso de *browsers* são:

- manter o seu *browser* sempre atualizado;
- desativar a execução de programas *Java* na configuração de seu *browser*[2]. Se for absolutamente necessário o *Java* estar ativado para que as páginas de um *site* possam ser vistas, basta ativá-lo antes de entrar no *site* e, então, desativá-lo ao sair;
- desativar a execução de *JavaScripts* antes de entrar em uma página desconhecida e, então, ativá-la ao sair. Caso você opte por desativar a execução de *JavaScripts* na configuração de seu *browser*, é provável que muitas páginas *Web* não possam ser visualizadas;
- permitir que programas *ActiveX* sejam executados em seu computador **apenas** quando vierem de *sites* conhecidos e confiáveis;

[2] Os programas *Java* não são utilizados na maioria das páginas *Web* e, quando utilizados, a desativação de sua execução não costuma comprometer a visualização da página.

- manter maior controle sobre o uso de *cookies*, caso você queira ter maior privacidade ao navegar na Internet (vide Parte III: Privacidade);
- 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* (vide Parte IV: Fraudes na Internet);
- 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*. Assim, você pode evitar ser redirecionado para uma página fraudulenta ou ser induzido a instalar algum *software* malicioso, que tem como objetivo furtar seus dados pessoais (incluindo senhas e números de cartões de crédito).

2.2.8 Que características devo considerar na escolha de um *browser*?

Existem características muito importantes que você deve considerar no momento de escolher um *browser*. Algumas destas características são:

- histórico de vulnerabilidades associadas ao *browser* e o tempo decorrido entre a descoberta da vulnerabilidade e o lançamento da correção;
- **não** instalação/execução automática de programas;
- facilidade para identificar se o *site* usa conexão segura e para visualizar dados do certificado digital;
- disponibilidade de mecanismos para desabilitar a execução de programas *Java*, *JavaScript*, *ActiveX*, entre outros;
- disponibilidade de mecanismos que permitam bloquear (incluindo bloqueio seletivo) *cookies* e *pop-up windows*.

2.3 Antivírus

Os antivírus são programas que procuram detectar e, então, anular ou remover os vírus de computador. Atualmente, novas funcionalidades têm sido adicionadas aos programas antivírus, de modo que alguns procuram detectar e remover cavalos de tróia e outros tipos de código malicioso[3], barrar programas hostis e verificar *e-mails*.

[3] A definição de código malicioso (*malware*) pode ser encontrada na Parte I: Conceitos de Segurança.

2.3.1 Que funcionalidades um bom antivírus deve possuir?

Um bom antivírus deve:

- identificar e eliminar a maior quantidade possível de vírus e outros tipos de *malware*;
- analisar os arquivos que estão sendo obtidos pela Internet;
- verificar continuamente os discos rígidos (HDs), flexíveis (disquetes) e unidades removíveis, como CDs, DVDs e *pen drives*, de forma transparente ao usuário;
- procurar vírus, cavalos de tróia e outros tipos de *malware* em arquivos anexados aos *e-mails*;
- criar, sempre que possível, uma mídia de verificação (disquete ou CD de *boot*) que possa ser utilizado caso um vírus desative o antivírus que está instalado no computador;
- atualizar as assinaturas de vírus e *malwares* conhecidos, pela rede, de preferência diariamente.

Alguns antivírus, além das funcionalidades acima, permitem verificar *e-mails* enviados, podendo detectar e barrar a propagação por *e-mail* de vírus, *worms*, e outros tipos de *malware*.

2.3.2 Como faço bom uso do meu antivírus?

As dicas para o bom uso do antivírus são simples:

- mantenha o antivírus e suas assinaturas sempre atualizados;
- configure-o para verificar automaticamente arquivos anexados aos *e-mails* e arquivos obtidos pela Internet;
- configure-o para verificar automaticamente mídias removíveis (CDs, DVDs, *pen drives*, disquetes, discos para Zip, etc);
- configure-o para verificar todo e qualquer formato de arquivo (qualquer tipo de extensão de arquivo);
- se for possível, crie o disquete de verificação e utilize-o esporadicamente, ou quando seu computador estiver apresentando um comportamento anormal (mais lento, gravando ou lendo o disco rígido fora de hora, etc);

Algumas versões de antivírus são gratuitas para uso pessoal e podem ser obtidas pela Internet. Mas antes de obter um antivírus pela Internet, verifique sua procedência e certifique-se que o fabricante é confiável.

2.3.3 O que um antivírus não pode fazer?

Um antivírus não é capaz de impedir que um atacante tente explorar alguma vulnerabilidade (vide seção 2.5) existente em um computador. Também não é capaz de evitar o acesso não autorizado a um *backdoor*[4] instalado em um computador.

Existem também outros mecanismos de defesa, conhecidos como *firewalls*, que podem prevenir contra tais ameaças (vide seção 2.4);

2.4 *Firewalls*

Os *firewalls* são dispositivos constituídos pela combinação de *software* e *hardware*, utilizados para dividir e controlar o acesso entre redes de computadores.

Um tipo específico é o ***firewall* pessoal**, que é um *software* ou programa utilizado para proteger **um** computador contra acessos não autorizados vindos da Internet.

2.4.1 Como o *firewall* pessoal funciona?

Se alguém ou algum programa suspeito tentar se conectar ao seu computador, um *firewall* bem configurado entra em ação para bloquear tentativas de invasão, podendo barrar também o acesso a *backdoors*, mesmo se já estiverem instalados em seu computador.

Alguns programas de *firewall* permitem analisar continuamente o conteúdo das conexões, filtrando vírus de *e-mail*, cavalos de tróia e outros tipos de *malware*, antes mesmo que os antivírus entrem em ação.

Também existem pacotes de *firewall* que funcionam em conjunto com os antivírus, provendo um maior nível de segurança para os computadores onde são utilizados.

2.4.2 Por que devo instalar um *firewall* pessoal em meu computador?

É comum observar relatos de usuários que acreditam ter computadores seguros por utilizarem apenas programas antivírus. O fato é que a segurança de um computador não pode basear-se apenas em **um** mecanismo de defesa.

Um antivírus não é capaz de impedir o acesso a um *backdoor* instalado em um computador. Já um *firewall* bem configurado pode bloquear o acesso a ele.

Além disso, um *firewall* poderá bloquear as tentativas de invasão ao seu computador e possibilitar a identificação das origens destas tentativas.

Alguns fabricantes de *firewalls* oferecem versões gratuitas de seus produtos para uso pessoal. Mas antes de obter um *firewall*, verifique sua procedência e certifique-se que o fabricante é confiável.

[4] Detalhes sobre *backdoors* podem ser vistos na Parte VIII: Códigos Maliciosos (*Malware*).

2.4.3 Como posso saber se estão tentando invadir meu computador?

Normalmente os *firewalls* criam arquivos em seu computador, denominados arquivos de registro de eventos (*logs*). Nestes arquivos são armazenadas as tentativas de acesso não autorizado ao seu computador, para serviços que podem ou não estar habilitados.

A Parte VII: Incidentes de Segurança e Uso Abusivo da Rede apresenta um guia para que você não só identifique tais tentativas, mas também reporte-as para os responsáveis pela rede ou computador de onde a tentativa de invasão se originou.

2.5 Vulnerabilidades

2.5.1 Como posso saber se os *softwares* instalados em meu computador possuem alguma vulnerabilidade?

Existem *sites* na Internet que mantêm listas atualizadas de vulnerabilidades em *softwares* e sistemas operacionais. Alguns destes *sites* são `http://www.cert.org/`, `http://cve.mitre.org/` e `http://www.us-cert.gov/cas/alerts/`.

Além disso, fabricantes também costumam manter páginas na Internet com considerações a respeito de possíveis vulnerabilidades em seus *softwares*.

Portanto, a idéia é estar sempre atento aos *sites* especializados em acompanhar vulnerabilidades, aos *sites* dos fabricantes, às revistas especializadas e aos cadernos de informática dos jornais, para verificar a existência de vulnerabilidades no sistema operacional e nos *softwares* instalados em seu computador.

2.5.2 Como posso corrigir as vulnerabilidades dos *softwares* em meu computador?

A melhor forma de evitar que o sistema operacional e os *softwares* instalados em um computador possuam vulnerabilidades é mantê-los **sempre atualizados**.

Entretanto, fabricantes em muitos casos não disponibilizam novas versões de seus *softwares* quando é descoberta alguma vulnerabilidade, mas sim correções específicas (*patches*). Estes *patches*, em alguns casos também chamados de *hot fixes* ou *service packs*, têm por finalidade corrigir os problemas de segurança referentes às vulnerabilidades descobertas.

Portanto, é **extremamente importante** que você, além de manter o sistema operacional e os *softwares* sempre atualizados, instale os *patches* sempre que forem disponibilizados.

2.6 Programas de Troca de Mensagens

2.6.1 Quais são os riscos associados ao uso de salas de bate-papo e de programas como o ICQ ou IRC?

Os maiores riscos associados ao uso destes programas estão no conteúdo dos próprios diálogos. Alguém pode utilizar técnicas de engenharia social (vide Parte I: Conceitos de Segurança e Parte IV: Fraudes na Internet) para obter informações (muitas vezes sensíveis) dos usuários destes programas.

Você pode ser persuadido a fornecer em uma conversa "amigável" seu *e-mail*, telefone, endereço, senhas (como a de acesso ao seu provedor), número do seu cartão de crédito, etc. As conseqüências podem ser desde o recebimento de mensagens com conteúdo falso/alarmante ou mensagens não solicitadas contendo propagandas, até a utilização da conta no seu provedor para realizar atividades ilícitas ou a utilização de seu número de cartão de crédito para fazer compras em seu nome (vide Parte IV: Fraudes na Internet).

Além disso, estes programas podem fornecer o seu endereço na Internet (endereço IP[5]). Um atacante pode usar esta informação para, por exemplo, tentar explorar uma possível vulnerabilidade em seu computador.

2.6.2 Existem problemas de segurança específicos nos programas de troca instantânea de mensagens?

Programas, tais como o ICQ, AOL Instant Messenger, Yahoo! Messenger e MSN Messenger, por se comunicarem constantemente com um servidor (senão não teriam como saber quem está no ar), ficam mais expostos e sujeitos a ataques, caso possuam alguma vulnerabilidade.

2.6.3 Que medidas preventivas devo adotar no uso de programas de troca de mensagens?

Algumas medidas preventivas para o uso de programas de troca de mensagens são:

- manter seu programa de troca de mensagens sempre atualizado, para evitar que possua alguma vulnerabilidade (vide seção 2.5);
- 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 através do programa de troca de mensagens, 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.

[5] O significado de endereço IP pode ser encontrado no Apêndice A: Glossário.

2.7 Programas de Distribuição de Arquivos

2.7.1 Quais são os riscos associados ao uso de programas de distribuição de arquivos?

Existem diversos riscos envolvidos na utilização de programas de distribuição de arquivos, tais como o Kazaa, Morpheus, Edonkey, Gnutella e BitTorrent. Dentre estes riscos, podem-se citar:

Acesso não autorizado: o programa de distribuição de arquivos pode permitir o acesso não autorizado ao seu computador, caso esteja mal configurado ou possua alguma vulnerabilidade;

***Softwares* ou arquivos maliciosos:** os *softwares* ou arquivos distribuídos podem ter finalidades maliciosas. Podem, por exemplo, conter vírus, ser um *bot* ou cavalo de tróia, ou instalar *backdoors* em um computador;

Violação de direitos autorais (*Copyright*): a distribuição não autorizada de arquivos de música, filmes, textos ou programas protegidos pela lei de direitos autorais constitui a violação desta lei.

2.7.2 Que medidas preventivas devo adotar no uso de programas de distribuição de arquivos?

Algumas medidas preventivas para o uso de programas de distribuição de arquivos são:

- 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.

2.8 Compartilhamento de Recursos do Windows

2.8.1 Quais são os riscos associados ao uso do compartilhamento de recursos?

Um recurso compartilhado aparece no Explorer do Windows como uma "mãozinha" segurando a parte de baixo do ícone (pasta, impressora ou disco), como mostra a figura 2.1.

Figura 2.1: Exemplos de ícones para recursos compartilhados.

Alguns dos riscos envolvidos na utilização de recursos compartilhados por terceiros são:

- abrir arquivos ou executar programas que contenham vírus;
- executar programas que sejam cavalos de tróia ou outros tipos de *malware*.

Já alguns dos riscos envolvidos em compartilhar recursos do seu computador são:

- permitir o acesso não autorizado a recursos ou informações sensíveis;
- permitir que um atacante possa utilizar tais recursos, sem quaisquer restrições, para fins maliciosos. Isto pode ocorrer se não forem definidas senhas para os compartilhamentos.

2.8.2 Que medidas preventivas devo adotar no uso do compartilhamento de recursos?

Algumas medidas preventivas para o uso do compartilhamento de recursos do Windows são:

- 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 ou cavalos de tróia, entre outros tipos de *malware*;
- estabelecer senhas para os compartilhamentos, caso seja estritamente necessário compartilhar recursos do seu computador. Procure elaborar senhas fáceis de lembrar e difíceis de serem descobertas (vide Parte I: Conceitos de Segurança).

É importante ressaltar que você deve sempre utilizar senhas para os recursos que deseje compartilhar, principalmente os que estão habilitados para leitura e escrita. E, quando possível, não compartilhe recursos ou não deixe-os compartilhados por muito tempo.

2.9 Realização de Cópias de Segurança (*Backups*)

2.9.1 Qual é a importância de fazer cópias de segurança?

Cópias de segurança dos dados armazenados em um computador são importantes, não só para se recuperar de eventuais falhas, mas também das conseqüências de uma possível infecção por vírus, ou de uma invasão.

2.9.2 Quais são as formas de realizar cópias de segurança?

Cópias de segurança podem ser simples como o armazenamento de arquivos em CDs ou DVDs, ou mais complexas como o espelhamento de um disco rígido inteiro em um outro disco de um computador.

Atualmente, uma unidade gravadora de CDs/DVDs e um *software* que possibilite copiar dados para um CD/DVD são suficientes para que a maior parte dos usuários de computadores realizem suas cópias de segurança.

Também existem equipamentos e *softwares* mais sofisticados e específicos que, dentre outras atividades, automatizam todo o processo de realização de cópias de segurança, praticamente sem intervenção do usuário. A utilização de tais equipamentos e *softwares* envolve custos mais elevados e depende de necessidades particulares de cada usuário.

2.9.3 Com que freqüência devo fazer cópias de segurança?

A freqüência com que é realizada uma cópia de segurança e a quantidade de dados armazenados neste processo depende da periodicidade com que o usuário cria ou modifica arquivos. Cada usuário deve criar sua própria política para a realização de cópias de segurança.

2.9.4 Que cuidados devo ter com as cópias de segurança?

Os cuidados com cópias de segurança dependem das necessidades do usuário. O usuário deve procurar responder algumas perguntas antes de adotar um ou mais cuidados com suas cópias de segurança:

- Que informações realmente importantes precisam estar armazenadas em minhas cópias de segurança?
- Quais seriam as conseqüências/prejuízos, caso minhas cópias de segurança fossem destruídas ou danificadas?
- O que aconteceria se minhas cópias de segurança fossem furtadas?

Baseado nas respostas para as perguntas anteriores, um usuário deve atribuir maior ou menor importância a cada um dos cuidados discutidos abaixo.

Escolha dos dados. Cópias de segurança devem conter apenas arquivos confiáveis do usuário, ou seja, que não contenham vírus e nem sejam algum outro tipo de *malware*. Arquivos do sistema operacional e que façam parte da instalação dos *softwares* de um computador não devem fazer parte das cópias de segurança. Eles podem ter sido modificados ou substituídos por versões maliciosas, que quando restauradas podem trazer uma série de problemas de segurança para um computador. O sistema operacional e os *softwares* de um computador podem ser reinstalados de mídias confiáveis, fornecidas por fabricantes confiáveis.

Mídia utilizada. A escolha da mídia para a realização da cópia de segurança é extremamente importante e depende da importância e da vida útil que a cópia deve ter. A utilização de alguns disquetes para armazenar um pequeno volume de dados que estão sendo modificados constantemente é perfeitamente viável. Mas um grande volume de dados, de maior importância, que deve perdurar por longos períodos, deve ser armazenado em mídias mais confiáveis, como por exemplo os CDs ou DVDs.

Local de armazenamento. Cópias de segurança devem ser guardadas em um local condicionado (longe de muito frio ou muito calor) e restrito, de modo que apenas pessoas autorizadas tenham acesso a este local (segurança física).

Cópia em outro local. Cópias de segurança podem ser guardadas em locais diferentes. Um exemplo seria manter uma cópia em casa e outra no escritório. Também existem empresas especializadas em manter áreas de armazenamento com cópias de segurança de seus clientes. Nestes casos é muito importante considerar a segurança física de suas cópias, como discutido no item anterior.

Criptografia dos dados. Os dados armazenados em uma cópia de segurança podem conter informações sigilosas. Neste caso, os dados que contenham informações sigilosas devem ser armazenados em algum formato criptografado.

2.9.5 Que cuidados devo ter ao enviar um computador para a manutenção?

É muito importante fazer cópias de segurança dos dados de um computador antes que ele apresente algum problema e seja necessário enviá-lo para manutenção ou assistência técnica.

Em muitos casos, o computador pode apresentar algum problema que impossibilite a realização de uma cópia de segurança dos dados antes de enviá-lo para a manutenção. Portanto, é muito importante que o usuário tenha disponível cópias de segurança recentes de seus dados. Não se pode descartar a possibilidade de, ao receber seu computador, ter a infeliz surpresa que todos os seus dados foram apagados durante o processo de manutenção.

Tenha sempre em mente que procurar uma assistência técnica de confiança é fundamental, principalmente se existirem dados sensíveis armazenados em seu computador, como declaração de Imposto de Renda, documentos e outras informações sigilosas, certificados digitais, entre outros.

Parte III: Privacidade

Esta parte da Cartilha discute questões relacionadas à privacidade do usuário ao utilizar a Internet. São abordados temas relacionados à privacidade dos *e-mails*, à privacidade no acesso e disponibilização de páginas *Web*, bem como alguns cuidados que o usuário deve ter com seus dados pessoais e ao armazenar dados em um disco rígido.

3.1 Privacidade dos *E-mails*

O serviço de *e-mails* foi projetado para ter como uma de suas principais características a simplicidade. O problema deste serviço é que foi comparado com o correio convencional, dando a falsa idéia de que os *e-mails* são cartas fechadas. Mas eles são, na verdade, como cartões postais, cujo conteúdo pode ser lido por quem tiver acesso a eles.

3.1.1 É possível alguém ler *e-mails* de outro usuário?

As mensagens que chegam à caixa postal do usuário ficam normalmente armazenadas em um arquivo no servidor de *e-mails* do provedor, até o usuário se conectar na Internet e obter os *e-mails* através do seu programa leitor de *e-mails*.

Portanto, enquanto os *e-mails* estiverem no servidor, poderão ser lidos por pessoas que tenham acesso a este servidor[1]. E enquanto estiverem em trânsito, existe a possibilidade de serem lidos por alguma pessoa conectada à Internet.

3.1.2 Como é possível assegurar a privacidade dos *e-mails*?

Se a informação que se deseja enviar por *e-mail* for confidencial, a solução é utilizar programas que permitam criptografar o *e-mail* através de chaves (senhas ou frases), de modo que ele possa ser lido apenas por quem possuir a chave certa para decodificar a mensagem. Maiores informações sobre criptografia podem ser encontradas na Parte I: Conceitos de Segurança.

Alguns *softwares* de criptografia podem estar embutidos nos programas leitores de *e-mails*, outros podem ser adquiridos separadamente e integrados aos programas leitores de *e-mails*.

Devem ser usados, preferencialmente, programas de criptografia que trabalhem com pares de chaves, como o GnuPG, que pode ser obtido no site `http://www.gnupg.org/`.

[1] Normalmente existe um consenso ético entre administradores de redes e provedores de nunca lerem a caixa postal de um usuário sem o seu consentimento.

Estes programas, apesar de serem muito utilizados na criptografia de mensagens de *e-mail*, também podem ser utilizados na criptografia de qualquer tipo de informação, como por exemplo, um arquivo sigiloso a ser armazenado em uma cópia de segurança (vide Parte II: Riscos Envolvidos no Uso da Internet e Métodos de Prevenção).

3.1.3 A utilização de programas de criptografia é suficiente para assegurar a privacidade dos *e-mails*?

Os programas de criptografia são utilizados, dentre outras finalidades, para decodificar mensagens criptografadas, recebidas por um usuário, no momento em que este desejar lê-las.

Ao utilizar um programa de criptografia para decodificar uma mensagem, é possível que o programa leitor de *e-mails* permita salvar a mensagem no formato decodificado, ou seja, em texto claro. No caso da utilização de programas leitores de *e-mails* com esta característica, a privacidade do conteúdo da mensagem é garantida durante a transmissão da mensagem, mas não necessariamente no seu armazenamento.

Portanto, é extremamente importante o usuário estar atento para este fato, e também certificar-se sobre o modo como suas mensagens estão sendo armazenadas. Como uma mensagem pode ser decodificada sempre que o usuário desejar lê-la, é aconselhável que ela seja armazenada de forma criptografada e não em texto claro.

3.2 Privacidade no Acesso e Disponibilização de Páginas *Web*

Existem cuidados que devem ser tomados por um usuário ao acessar ou disponibilizar páginas na Internet. Muitas vezes o usuário pode expor informações pessoais e permitir que seu *browser* receba ou envie dados sobre suas preferências e sobre o seu computador. Isto pode afetar a privacidade de um usuário, a segurança de seu computador e até mesmo sua própria segurança.

3.2.1 Que cuidados devo ter ao acessar páginas *Web* e ao receber *cookies*?

Cookies são muito utilizados para rastrear e manter as preferências de um usuário ao navegar pela Internet. Estas preferências podem ser compartilhadas entre diversos *sites* na Internet, afetando assim a privacidade de um usuário. Não é incomum acessar pela primeira vez um *site* de música, por exemplo, e observar que todas as ofertas de CDs para o seu gênero musical preferido já estão disponíveis, sem que você tenha feito qualquer tipo de escolha.

Além disso, ao acessar uma página na Internet, o seu *browser* disponibiliza uma série de informações, de modo que os *cookies* podem ser utilizados para manter referências contendo informações de seu computador, como o *hardware*, o sistema operacional, *softwares* instalados e, em alguns casos, até o seu endereço de *e-mail*.

Estas informações podem ser utilizadas por alguém mal intencionado, por exemplo, para tentar explorar uma possível vulnerabilidade em seu computador, como visto na Parte I: Conceitos de Segurança e Parte II: Riscos Envolvidos no Uso da Internet e Métodos de Prevenção.

Portanto, é aconselhável que você desabilite o recebimento de *cookies*, exceto para *sites* confiáveis, onde sejam realmente necessários.

As versões recentes dos *browsers* normalmente permitem que o usuário desabilite o recebimento, confirme se quer ou não receber e até mesmo visualize o conteúdo dos *cookies*.

Também existem *softwares* que permitem controlar o recebimento e envio de informações entre um *browser* e os *sites* visitados. Dentre outras funções, estes podem permitir que *cookies* sejam recebidos apenas de *sites* específicos[2].

Uma outra forma de manter sua privacidade ao acessar páginas na Internet é utilizar *sites* que permitem que você fique anônimo. Estes são conhecidos como *anonymizers*[3] e intermediam o envio e recebimento de informações entre o seu *browser* e o *site* que se deseja visitar. Desta forma, o seu *browser* não receberá *cookies* e as informações por ele fornecidas não serão repassadas para o *site* visitado.

Neste caso, é importante ressaltar que você deve certificar-se que o *anonymizer* é confiável. Além disso, você não deve utilizar este serviço para realizar transações via *Web*.

3.2.2 Que cuidados devo ter ao disponibilizar uma página na Internet, como por exemplo um *blog*?

Um usuário, ao disponibilizar uma página na Internet, precisa ter alguns cuidados, visando proteger os dados contidos em sua página.

Um tipo específico de página *Web* que vem sendo muito utilizado por usuários de Internet é o *blog*. Este serviço é usado para manter um registro freqüente de informações, e tem como principal vantagem permitir que o usuário publique seu conteúdo sem necessitar de conhecimento técnico sobre a construção de páginas na Internet.

Apesar de terem diversas finalidades, os *blogs* têm sido muito utilizados como diários pessoais. Em seu *blog*, um usuário poderia disponibilizar informações, tais como:

- seus dados pessoais (*e-mail*, telefone, endereço, etc);
- informações sobre seus familiares e amigos (como árvores genealógicas, datas de aniversário, telefones, etc);
- dados sobre o seu computador (dizendo, por exemplo, "...comprei um computador da marca X e instalei o sistema operacional Y...");
- dados sobre os *softwares* que utiliza (dizendo, por exemplo, "...instalei o programa Z, que acabei de obter do *site* W...");
- 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);

É extremamente importante estar atento e avaliar com cuidado que informações serão disponibilizadas em uma página *Web*. Estas informações podem não só ser utilizadas por alguém mal-intencionado, por exemplo, em um ataque de engenharia social (vide Parte I: Conceitos de Segurança), mas também para atentar contra a segurança de um computador, ou até mesmo contra a segurança física do próprio usuário.

[2] Um exemplo deste tipo de *software* pode ser encontrado em http://internet.junkbuster.com/.

[3] Exemplos desse tipo de *site* podem ser encontrados em http://anonymouse.org/ (serviço gratuito) e http://www.anonymizer.com/ (serviço pago).

3.3 Cuidados com seus Dados Pessoais

Procure não fornecer seus dados pessoais (como nome, *e-mail*, endereço e números de documentos) para terceiros. Também **nunca** forneça 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*.

Estas informações geralmente são armazenadas em servidores das instituições que mantêm os *sites*. Com isso, corre-se o risco destas informações serem repassadas sem sua autorização para outras instituições ou de um atacante comprometer este servidor e obter acesso a todas as informações.

Fique atento aos ataques de engenharia social, vistos na Parte I: Conceitos de Segurança. Ao ter acesso a seus dados pessoais, um atacante poderia, por exemplo, utilizar seu *e-mail* em alguma lista de distribuição de *spams* (vide Parte VI: *Spam*) ou se fazer passar por você na Internet (através do uso de uma de suas senhas).

3.3.1 Que cuidados devo ter em *sites* de redes de relacionamentos, como por exemplo o orkut?

Os *sites* de redes de relacionamentos, como o orkut, tiveram uma ampla aceitação e inserção de usuários da Internet, por proporcionarem o encontro de pessoas (amigos) e permitirem a criação e participação em comunidades com interesses em comum.

Um *site* de redes de relacionamento normalmente permite que o usuário cadastre informações pessoais (como nome, endereços residencial e comercial, telefones, endereços de *e-mail*, data de nascimento, etc), além de outros dados que irão compor o seu perfil. Se o usuário não limitar o acesso aos seus dados para apenas aqueles de interesse, todas as suas informações poderão ser visualizadas por qualquer um que utilize este *site*. Além disso, é recomendável que o usuário evite fornecer muita informação a seu respeito, pois nenhum *site* está isento do risco de ser invadido e de ter suas informações furtadas por um invasor.

A participação de um usuário em determinados tipos de comunidades também pode fornecer muita informação para terceiros. Por exemplo, a comunidade de donos de um determinado veículo, ou dos freqüentadores do estabelecimento X, pode dizer qual é a classe social de um usuário, que locais ele gosta de freqüentar, etc.

Desta forma, é extremamente importante estar atento e avaliar com cuidado que informações você disponibilizará nos *sites* de redes de relacionamentos, principalmente aquelas que poderão ser vistas por todos, e em que comunidades você participará. Estas informações podem não só ser utilizadas por alguém mal-intencionado, por exemplo, em um ataque de engenharia social (vide Parte I: Conceitos de Segurança), mas também para atentar contra a segurança física do próprio usuário.

3.4 Cuidados com os Dados Armazenados em um Disco Rígido

É importante ter certos cuidados no armazenamento de dados em um computador. Caso você mantenha informações sensíveis ou pessoais que você não deseja que sejam vistas por terceiros (como números de cartões de crédito, declaração de Imposto de Renda, senhas, etc), estas devem ser armazenadas em algum formato criptografado.

Estes cuidados são extremamente importantes no caso de *notebooks*, pois são mais visados e, portanto, mais suscetíveis a roubos, furtos, etc.

Caso as informações não estejam criptografadas, se você necessitar levar o computador a alguma assistência técnica, por exemplo, seus dados poderão ser lidos ou copiados por uma pessoa não autorizada.

Para criptografar estes dados, como visto na seção 3.1.2, existem programas que, além de serem utilizados para a criptografia de *e-mails*, também podem ser utilizados para criptografar arquivos.

Um exemplo seria utilizar um programa que implemente criptografia de chaves pública e privada[4], como o GnuPG. O arquivo sensível seria criptografado com a sua chave pública e, então, decodificado com a sua chave privada, sempre que fosse necessário.

É importante ressaltar que a segurança deste método de criptografia depende do sigilo da chave privada. A idéia, então, é manter a chave privada em um CD ou outra mídia (como *pen drive*, disco rígido removível ou externo) e que este não acompanhe o computador, caso seja necessário enviá-lo, por exemplo, para a assistência técnica.

Também deve-se ter um cuidado especial ao trocar ou vender um computador. Apenas apagar ou formatar um disco rígido não é suficiente para evitar que informações antes armazenadas possam ser recuperadas. Portanto, é importante **sobrescrever** todos os dados do disco rígido (vide seção 3.4.1).

3.4.1 Como posso sobrescrever todos os dados de um disco rígido?

Para assegurar que informações não possam ser recuperadas de um disco rígido é preciso sobrescrevê-las com outras informações. Um exemplo seria gravar o caracter 0 (zero), ou algum caracter escolhido aleatoriamente, em todos os espaços de armazenamento do disco.

É importante ressaltar que é preciso repetir algumas vezes a operação de sobrescrever os dados de um disco rígido, para minimizar a chance de recuperação de informações anteriormente armazenadas.

Existem *softwares* gratuitos e comerciais que permitem sobrescrever dados de um disco rígido e que podem ser executados em diversos sistemas operacionais, como o Windows (95/98, 2000, XP, etc), Unix (Linux, FreeBSD, etc), Mac OS, entre outros.

3.5 Cuidados com Telefones Celulares, PDAs e Outros Aparelhos com *Bluetooth*

Telefones celulares deixaram de ser meramente aparelhos utilizados para fazer ligações telefônicas e passaram a incorporar diversas funcionalidades, tais como: calendário, despertador, agenda telefônica e de compromissos, câmera fotográfica, envio e recebimento de texto e imagens, etc.

A tecnologia *bluetooth*[5] tem sido introduzida em diversos tipos de telefones celulares para permitir a transmissão de dados entre eles (por exemplo, contatos da agenda telefônica, agenda de compromissos, texto, imagens, etc), bem como conectar um telefone a outros tipos de dispositivo (por exemplo,

[4] Detalhes sobre criptografia de chaves pública e privada estão disponíveis na Parte I: Conceitos de Segurança.
[5] A definição deste termo pode ser encontrada no Apêndice A: Glossário.

fones de ouvido, sistema viva-voz de automóveis, etc). Outros exemplos de aparelhos que podem fornecer esta tecnologia são PDAs e *notebooks*.

O fato é que a inclusão da tecnologia *bluetooth* em aparelhos como telefones celulares e PDAs, entre outros, trouxe alguns riscos que podem afetar a privacidade de seus usuários.

3.5.1 Que riscos estão associados ao uso de aparelhos com *bluetooth*?

Muitas vezes, um aparelho que fornece a tecnologia *bluetooth* vem configurado de fábrica, ou é posteriormente configurado, de modo que qualquer outro aparelho possa se conectar a ele, indiscriminadamente. Esta configuração normalmente permite que dados sejam obtidos do aparelho sem qualquer tipo de controle.

O problema não reside no fato do aparelho disponibilizar a tecnologia, mas sim na má configuração das opções de *bluetooth*, que podem permitir que terceiros obtenham diversas informações de um aparelho. Estas informações podem incluir: agenda telefônica, agenda de compromissos, arquivos, imagens, entre outras.

Pode-se citar como exemplos os casos de algumas celebridades que tiveram todos os contatos telefônicos armazenados em seus aparelhos furtados e disponibilizados na Internet.

3.5.2 Que cuidados devo ter para evitar a exposição de informações de um aparelho com *bluetooth*?

É preciso tomar alguns cuidados para evitar a exposição de informações de um aparelho que fornece a tecnologia *bluetooth*. Alguns dos principais cuidados são:

- mantenha o *bluetooth* do seu aparelho desabilitado e somente habilite-o quando for necessário. Caso isto não seja possível, consulte o manual do seu aparelho e configure-o para que não seja identificado (ou "descoberto") por outros aparelhos (em muitos aparelhos esta opção aparece como "Oculto" ou "Invisível");
- fique atento às notícias, principalmente àquelas sobre segurança, veiculadas no *site* do fabricante do seu aparelho;
- aplique 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, restaure as opções de fábrica (em muitos aparelhos esta opção aparece como "Restaurar Configuração de Fábrica" ou "Restaurar Configuração Original") e configure-o como no primeiro item, antes de inserir quaisquer dados.

Parte IV: Fraudes na Internet

Esta parte da cartilha aborda questões relacionadas a fraudes na Internet. São apresentadas algumas maneiras de prevenção contra ataques de engenharia social, situações envolvendo fraudes comerciais e bancárias via Internet, bem como medidas preventivas que um usuário deve adotar ao acessar *sites* de comércio eletrônico ou *Internet Banking*. Também é apresentado o conceito de boato (*hoax*) e são discutidas algumas implicações de segurança e formas para se evitar sua distribuição.

4.1 Engenharia Social

Nos ataques de engenharia social, normalmente, o atacante se faz passar por outra pessoa e utiliza meios, como uma ligação telefônica ou *e-mail*, para persuadir o usuário a fornecer informações ou realizar determinadas ações. Exemplos destas ações são: executar um programa, acessar uma página falsa de comércio eletrônico ou *Internet Banking* através de um *link* em um *e-mail* ou em uma página, etc.

O conceito de engenharia social, bem como alguns exemplos deste tipo de ataque, podem ser encontrados na Parte I: Conceitos de Segurança. Exemplos específicos destes ataques, envolvendo diversos tipos de fraude, são abordados nas seções 4.2.1 e 4.2.2.

4.1.1 Como me protejo deste tipo de abordagem?

Em casos de engenharia social o bom senso é essencial. Fique atento para qualquer abordagem, seja via telefone, seja através de um *e-mail*, onde uma pessoa (em muitos casos falando em nome de uma instituição) solicita informações (principalmente confidenciais) a seu respeito.

Procure não fornecer muita informação e **não** forneça, sob hipótese alguma, informações sensíveis, como senhas ou números de cartões de crédito.

Nestes casos e nos casos em que receber mensagens, procurando lhe induzir a executar programas ou clicar em um *link* contido em um *e-mail* ou página *Web*, é extremamente importante que você, **antes de realizar qualquer ação**, procure identificar e entrar em contato com a instituição envolvida, para certificar-se sobre o caso.

4.2 Fraudes via Internet

Normalmente, não é uma tarefa simples atacar e fraudar dados em um servidor de uma instituição bancária ou comercial. Então, atacantes têm concentrado seus esforços na exploração de fragilidades dos usuários, para realizar fraudes comerciais e bancárias através da Internet.

Para obter vantagens, os fraudadores têm utilizado amplamente *e-mails* com discursos que, na maioria dos casos, envolvem engenharia social e que tentam persuadir o usuário a fornecer seus dados pessoais e financeiros. Em muitos casos, o usuário é induzido a instalar algum código malicioso ou acessar uma página fraudulenta, para que dados pessoais e sensíveis, como senhas bancárias e números de cartões de crédito, possam ser furtados. Desta forma, é muito importante que usuários de Internet tenham certos cuidados com os *e-mails* que recebem e ao utilizarem serviços de comércio eletrônico ou *Internet Banking*.

A seções 4.2.1 e 4.2.2 ilustram algumas situações envolvendo estes tipos de fraudes. A seção 4.2.3 descreve alguns cuidados a serem tomados pelos usuários de Internet, ao acessarem *sites* de comércio eletrônico ou *Internet Banking*. As seções 4.2.4, 4.2.5 e 4.2.6 apresentam alguns procedimentos para verificar a legitimidade de um *site*. E a seção 4.2.7 recomenda o que o usuário deve fazer se perceber que seus dados financeiros podem estar sendo usados por terceiros.

4.2.1 O que é *scam* e que situações podem ser citadas sobre este tipo de fraude?

O *scam* (ou "golpe") é qualquer esquema ou ação enganosa e/ou fraudulenta que, normalmente, tem como finalidade obter vantagens financeiras.

As subseções 4.2.1.1 e 4.2.1.2 apresentam duas situações envolvendo este tipo de fraude, sendo que a primeira situação se dá através de páginas disponibilizadas na Internet e a segunda através do recebimento de *e-mails*. Observe que existem variantes para as situações apresentadas e outros tipos de *scam*. Além disso, novas formas de *scam* podem surgir, portanto é muito importante que você se mantenha informado sobre os tipos de *scam* que vêm sendo utilizados pelos fraudadores, através dos veículos de comunicação, como jornais, revistas e *sites* especializados.

4.2.1.1 *Sites* de leilões e de produtos com preços "muito atrativos"

Você acessa um *site* de leilão ou de venda de produtos, onde os produtos ofertados têm preços muito abaixo dos praticados pelo mercado.

Risco: ao efetivar uma compra, na melhor das hipóteses, você receberá um produto que não condiz com o que realmente foi solicitado. Na maioria dos casos, você não receberá nenhum produto, perderá o dinheiro e poderá ter seus dados pessoais e financeiros furtados, caso a transação tenha envolvido, por exemplo, o número do seu cartão de crédito.

Como identificar: faça uma pesquisa de mercado sobre preço do produto desejado e compare com os preços oferecidos. Então, você deve se perguntar por que estão oferecendo um produto com preço tão abaixo do praticado pelo mercado.

É importante ressaltar que existem muitos *sites* confiáveis de leilões e de vendas de produtos, mas nesta situação a intenção é ilustrar casos de *sites* especificamente projetados para realizar atividades ilícitas.

4.2.1.2 O golpe da Nigéria (*Nigerian 4-1-9 Scam*)

Você recebe um *e-mail* em nome de uma instituição governamental da Nigéria (por exemplo, o Banco Central), onde é solicitado que você atue como intermediário em uma transferência internacional de fundos. O valor mencionado na mensagem normalmente corresponde a dezenas ou centenas de milhões de dólares.

Como recompensa, você terá direito de ficar com uma porcentagem (que é normalmente alta) do valor mencionado na mensagem. Para completar a transação é solicitado que você pague antecipadamente uma quantia, normalmente bem elevada, para arcar com taxas de transferência de fundos, custos com advogados, entre outros.

Este tipo de golpe também é conhecido como *Advance Fee Fraud*, ou "a fraude de antecipação de pagamentos", e já foram registrados casos originados ou que mencionavam a África do Sul, Angola, Etiópia, Libéria, Marrocos, Serra Leoa, Tanzânia, Zaire, Zimbábue, Holanda, Iugoslávia, Austrália, Japão, Malásia e Taiwan, entre outros.

No nome dado a este tipo de fraude, *Nigerian 4-1-9 Scam*, o número "419" refere-se à seção do código penal da Nigéria que é violada por este golpe. É equivalente ao artigo 171 do código penal brasileiro, ou seja, **estelionato**.

Risco: ao responder a este tipo de mensagem e efetivar o pagamento antecipado, você não só perderá o dinheiro investido, mas também nunca verá os milhares ou milhões de dólares prometidos como recompensa.

Como identificar: normalmente, estas mensagens apresentam quantias astronômicas e abusam da utilização de palavras capitalizadas (todas as letras maiúsculas) para chamar a atenção do usuário. Palavras como "URGENT" (urgente) e "CONFIDENTIAL" (confidencial) também são comumente usadas no assunto da mensagem para chamar a atenção do usuário.

Você deve se perguntar por que foi escolhido para receber estes "milhares ou milhões" de dólares, entre os inúmeros usuários que utilizam a Internet.

4.2.2 O que é *phishing* e que situações podem ser citadas sobre este tipo de fraude?

Phishing, também conhecido como *phishing scam* ou *phishing/scam*, foi um termo originalmente criado para descrever o tipo de fraude que se dá através do envio de mensagem não solicitada, que se passa por comunicação de uma instituição conhecida, como um banco, empresa ou *site* popular, e que procura induzir o acesso a páginas fraudulentas (falsificadas), projetadas para furtar dados pessoais e financeiros de usuários.

A palavra *phishing* (de "*fishing*") vem de uma analogia criada pelos fraudadores, onde "iscas" (*e-mails*) são usadas para "pescar" senhas e dados financeiros de usuários da Internet.

Atualmente, este termo vêm sendo utilizado também para se referir aos seguintes casos:

- mensagem que procura induzir o usuário à instalação de códigos maliciosos, projetados para furtar dados pessoais e financeiros;
- mensagem que, no próprio conteúdo, apresenta formulários para o preenchimento e envio de dados pessoais e financeiros de usuários.

A subseções a seguir apresentam cinco situações envolvendo *phishing*, que vêm sendo utilizadas por fraudadores na Internet. Observe que existem variantes para as situações apresentadas. Além disso, novas formas de *phishing* podem surgir, portanto é muito importante que você se mantenha informado sobre os tipos de *phishing* que vêm sendo utilizados pelos fraudadores, através dos veículos de comunicação, como jornais, revistas e *sites* especializados.

Também é muito importante que você, ao identificar um caso de fraude via Internet, notifique a instituição envolvida, para que ela possa tomar as providências cabíveis[1].

4.2.2.1 Mensagens que contêm *links* para programas maliciosos

Você recebe uma mensagem por *e-mail* ou via serviço de troca instantânea de mensagens, onde o texto procura atrair sua atenção, seja por curiosidade, por caridade, pela possibilidade de obter alguma vantagem (normalmente financeira), entre outras. O texto da mensagem também pode indicar que a não execução dos procedimentos descritos acarretarão conseqüências mais sérias, como, por exemplo, a inclusão do seu nome no SPC/SERASA, o cancelamento de um cadastro, da sua conta bancária ou do seu cartão de crédito, etc. A mensagem, então, procura induzí-lo a clicar em um *link*, para baixar e abrir/executar um arquivo.

Alguns exemplos de temas e respectivas descrições dos textos encontrados em mensagens deste tipo são apresentados na tabela 4.1.

Tabela 4.1: Exemplos de temas de mensagens de *phishing*.

Tema	Texto da mensagem
Cartões virtuais	UOL, *Voxcards*, Humor Tadela, O Carteiro, *Emotioncard*, Criança Esperança, AACD/Teleton.
SERASA e SPC	débitos, restrições ou pendências financeiras.
Serviços de governo eletrônico	CPF/CNPJ pendente ou cancelado, Imposto de Renda (nova versão ou correção para o programa de declaração, consulta da restituição, dados incorretos ou incompletos na declaração), eleições (título eleitoral cancelado, simulação da urna eletrônica).
Álbuns de fotos	pessoa supostamente conhecida, celebridades, relacionado a algum fato noticiado (em jornais, revistas, televisão), traição, nudez ou pornografia, serviço de acompanhantes.
Serviço de telefonia	pendências de débito, aviso de bloqueio de serviços, detalhamento de fatura, créditos gratuitos para o celular.
Antivírus	a melhor opção do mercado, nova versão, atualização de vacinas, novas funcionalidades, eliminação de vírus do seu computador.
Notícias/boatos	fatos amplamente noticiados (ataques terroristas, *tsunami*, terremotos, etc), boatos envolvendo pessoas conhecidas (morte, acidentes ou outras situações chocantes).
Reality shows	BigBrother, Casa dos Artistas, etc – fotos ou vídeos envolvendo cenas de nudez ou eróticas, discadores.

continua na próxima página

[1] Veja detalhes sobre como realizar a notificação na Parte VII: Incidentes de Segurança e Uso Abusivo da Rede.

Tabela 4.1: Continuação.

Tema	Texto da mensagem
Programas ou arquivos diversos	novas versões de *softwares*, correções para o sistema operacional Windows, músicas, vídeos, jogos, acesso gratuito a canais de TV a cabo no computador, cadastro ou atualização de currículos, recorra das multas de trânsito.
Pedidos	orçamento, cotação de preços, lista de produtos.
Discadores	para conexão Internet gratuita, para acessar imagens ou vídeos restritos.
Sites de comércio eletrônico	atualização de cadastro, devolução de produtos, cobrança de débitos, confirmação de compra.
Convites	convites para participação em *sites* de relacionamento (como o orkut) e outros serviços gratuitos.
Dinheiro fácil	descubra como ganhar dinheiro na Internet.
Promoções	diversos.
Prêmios	loterias, instituições financeiras.
Propaganda	produtos, cursos, treinamentos, concursos.
FEBRABAN	cartilha de segurança, avisos de fraude.
IBGE	censo.

Cabe ressaltar que a lista de temas na tabela 4.1 não é exaustiva, nem tampouco se aplica a todos os casos. Existem outros temas e novos temas podem surgir.

Risco: ao clicar no *link*, será apresentada uma janela, solicitando que você salve o arquivo. Depois de salvo, se você abrí-lo ou executá-lo, será instalado um programa malicioso (*malware*) em seu computador, por exemplo, um cavalo de tróia ou outro tipo de *spyware*, projetado para furtar seus dados pessoais e financeiros, como senhas bancárias ou números de cartões de crédito[2]. Caso o seu programa leitor de *e-mails* esteja configurado para exibir mensagens em HTML, a janela solicitando que você salve o arquivo poderá aparecer automaticamente, sem que você clique no *link*.

Ainda existe a possibilidade do arquivo/programa malicioso ser baixado e executado no computador automaticamente, ou seja, sem a sua intervenção, caso seu programa leitor de *e-mails* possua vulnerabilidades.

Esse tipo de programa malicioso pode utilizar diversas formas para furtar dados de um usuário, dentre elas: capturar teclas digitadas no teclado; capturar a posição do cursor e a tela ou regiões da tela, no momento em que o *mouse* é clicado; sobrepor a janela do *browser* do usuário com uma janela falsa, onde os dados serão inseridos; ou espionar o teclado do usuário através da *Webcam* (caso o usuário a possua e ela esteja apontada para o teclado). Mais detalhes sobre algumas destas técnicas podem ser vistos na seção de *keyloggers*, na Parte VIII: Códigos Maliciosos (*Malware*).

Depois de capturados, seus dados pessoais e financeiros serão enviados para os fraudadores. A partir daí, os fraudadores poderão realizar diversas operações, incluindo a venda dos seus dados para terceiros, ou utilização dos seus dados financeiros para efetuar pagamentos, transferir valores para outras contas, etc.

Como identificar: seguem algumas dicas para identificar este tipo de mensagem fraudulenta:

[2] O conceito de *malware* pode ser encontrado na Parte I: Conceitos de Segurança. Os conceitos de cavalo de tróia e *spyware* estão disponíveis na Parte VIII: Códigos Maliciosos (*Malware*).

- leia atentamente a mensagem. Normalmente, ela conterá diversos erros gramaticais e de ortografia;
- os fraudadores utilizam técnicas para ofuscar o real *link* para o arquivo malicioso, apresentando o que parece ser um *link* relacionado à instituição mencionada na mensagem. Ao passar o cursor do *mouse* sobre o *link*, será possível ver o real endereço do arquivo malicioso na barra de *status* do programa leitor de *e-mails*, ou *browser*, caso esteja atualizado e não possua vulnerabilidades. Normalmente, este *link* será diferente do apresentado na mensagem;
- qualquer extensão pode ser utilizada nos nomes dos arquivos maliciosos, mas fique particularmente atento aos arquivos com extensões ".exe", ".zip" e ".scr", pois estas são as mais utilizadas. Outras extensões freqüentemente utilizadas por fraudadores são ".com", ".rar" e ".dll";
- fique atento às mensagens que solicitam a instalação/execução de qualquer tipo de arquivo/programa;
- acesse a página da instituição que supostamente enviou a mensagem, seguindo os cuidados apresentados na seção 4.2.3, e procure por informações relacionadas com a mensagem que você recebeu. Em muitos casos, você vai observar que não é política da instituição enviar *e-mails* para usuários da Internet, de forma indiscriminada, principalmente contendo arquivos anexados.

Recomendações:

- no caso de mensagem recebida por *e-mail*, o remetente **nunca** deve ser utilizado como parâmetro para atestar a veracidade de uma mensagem, pois pode ser facilmente forjado pelos fraudadores;
- se você ainda tiver alguma dúvida e acreditar que a mensagem pode ser verdadeira, entre em contato com a instituição para certificar-se sobre o caso, antes de enviar qualquer dado, principalmente informações sensíveis, como senhas e números de cartões de crédito.

4.2.2.2 Páginas de comércio eletrônico ou *Internet Banking* falsificadas

Você recebe uma mensagem por *e-mail* ou via serviço de troca instantânea de mensagens, em nome de um *site* de comércio eletrônico ou de uma instituição financeira, por exemplo, um banco. Textos comuns neste tipo de mensagem envolvem o recadastramento ou confirmação dos dados do usuário, a participação em uma nova promoção, etc. A mensagem, então, tenta persuadí-lo a clicar em um *link* contido no texto, em uma imagem, ou em uma página de terceiros.

Risco: o *link* pode direcioná-lo para uma página *Web* falsificada, semelhante ao *site* que você realmente deseja acessar. Nesta página serão solicitados dados pessoais e financeiros, como o número, data de expiração e código de segurança do seu cartão de crédito, ou os números da sua agência e conta bancária, senha do cartão do banco e senha de acesso ao *Internet Banking*.

Ao preencher os campos disponíveis na página falsificada e clicar no botão de confirmação (em muitos casos o botão apresentará o texto "Confirm", "OK", "Submit", etc), os dados serão enviados para os fraudadores.

A partir daí, os fraudadores poderão realizar diversas operações, incluindo a venda dos seus dados para terceiros, ou utilização dos seus dados financeiros para efetuar pagamentos, transferir valores para outras contas, etc.

Como identificar: seguem algumas dicas para identificar este tipo de mensagem fraudulenta:

- os fraudadores utilizam técnicas para ofuscar o real *link* para a página falsificada, apresentando o que parece ser um *link* relacionado à instituição mencionada na mensagem. Ao passar o cursor do *mouse* sobre o *link*, será possível ver o real endereço da página falsificada na barra de *status* do programa leitor de *e-mails*, ou *browser*, caso esteja atualizado e não possua vulnerabilidades. Normalmente, este *link* será diferente do apresentado na mensagem;
- acesse a página da instituição que supostamente enviou a mensagem, seguindo os cuidados apresentados na seção 4.2.3, e procure por informações relacionadas com a mensagem que você recebeu;
- *sites* de comércio eletrônico ou *Internet Banking* confiáveis **sempre** utilizam conexões seguras (vide seção 4.2.4) quando dados pessoais e financeiros de usuários são solicitados. Caso a página não utilize conexão segura, desconfie imediatamente. Caso a página falsificada utilize conexão segura, um novo certificado (que não corresponde ao *site* verdadeiro) será apresentado e, possivelmente, o endereço mostrado no *browser* será diferente do endereço correspondente ao *site* verdadeiro.

Recomendações:

- no caso de mensagem recebida por *e-mail*, o remetente **nunca** deve ser utilizado como parâmetro para atestar a veracidade de uma mensagem, pois pode ser facilmente forjado pelos fraudadores;
- se você ainda tiver alguma dúvida e acreditar que a mensagem pode ser verdadeira, entre em contato com a instituição para certificar-se sobre o caso, antes de enviar qualquer dado, principalmente informações sensíveis, como senhas e números de cartões de crédito.

4.2.2.3 *E-mails* contendo formulários para o fornecimento de informações sensíveis

Você recebe um *e-mail* em nome de um *site* de comércio eletrônico ou de uma instituição bancária. O conteúdo da mensagem envolve o recadastramento ou confirmação de seus dados, a participação em uma nova promoção, etc.

A mensagem apresenta um formulário, com campos para a digitação de informações envolvendo dados pessoais e financeiros, como o número, data de expiração e código de segurança do seu cartão de crédito, ou os números da sua agência e conta bancária, senha do cartão do banco e senha de acesso ao *Internet Banking*. A mensagem, então, solicita que você preencha o formulário e apresenta um botão para confirmar o envio das informações preenchidas.

Risco: ao preencher os dados e confirmar o envio, suas informações pessoais e financeiras serão transmitidas para fraudadores, que, a partir daí, poderão realizar diversas operações, incluindo a venda dos seus dados para terceiros, ou utilização dos seus dados financeiros para efetuar pagamentos, transferir valores para outras contas, etc.

Como identificar: o serviço de *e-mail* convencional não fornece qualquer mecanismo de criptografia, ou seja, as informações, ao serem submetidas, trafegarão em claro pela Internet. Qualquer instituição confiável **não** utilizaria este meio para o envio de informações pessoais e sensíveis de seus usuários.

4.2.2.4 Comprometimento do serviço de resolução de nomes

Ao tentar acessar um *site* de comércio eletrônico ou *Internet Banking*, mesmo digitando o endereço diretamente no seu *browser*, você é redirecionado para uma página falsificada, semelhante ao *site* verdadeiro.

Duas possíveis causas para este caso de *phishing* são:

- o atacante comprometeu o servidor de nomes do seu provedor (DNS), de modo que todos os acessos a determinados *sites* passaram a ser redirecionados para páginas falsificadas;
- o atacante o induziu a instalar um *malware*, por exemplo, através de uma mensagem recebida por *e-mail* (como mostrado na seção 4.2.2.1), e este *malware* foi especificamente projetado para alterar o comportamento do serviço de resolução de nomes do seu computador, redirecionando os acessos a determinados *sites* para páginas falsificadas.

Apesar de não ter uma definição consolidada na data de publicação desta Cartilha, os veículos de comunicação têm utilizado o termo ***pharming*** para se referir a casos específicos de *phishing*, que envolvem algum tipo de redireção da vítima para *sites* fraudulentos, através de alterações nos serviços de resolução de nomes.

Risco: ao preencher os campos disponíveis na página falsificada e confirmar o envio dos dados, suas informações pessoais e financeiras serão transmitidas para fraudadores, que, a partir daí, poderão realizar diversas operações, incluindo a venda dos seus dados para terceiros, ou utilização dos seus dados financeiros para efetuar pagamentos, transferir valores para outras contas, etc.

Como identificar: neste caso, onde fraudadores alteram o comportamento do serviço de resolução de nomes, para redirecionar acessos para páginas falsificadas, não são válidas dicas como digitar o endereço diretamente no seu *browser*, ou observar o endereço apresentado na barra de *status* do *browser*.

Deste modo, a melhor forma de identificar este tipo de fraude é estar atento para o fato de que *sites* de comércio eletrônico ou *Internet Banking* confiáveis **sempre** utilizam conexões seguras quando dados pessoais e financeiros de usuários são solicitados. Caso a página não utilize conexão segura, desconfie imediatamente. Caso a página falsificada utilize conexão segura, um novo certificado, que não corresponde ao *site* verdadeiro, será apresentado (mais detalhes sobre verificação de certificados na seção 4.2.6).

Recomendação: se você ainda tiver alguma dúvida e acreditar que a página pode ser verdadeira, mesmo não utilizando conexão segura, ou apresentando um certificado não compatível, entre em contato com a instituição para certificar-se sobre o caso, antes de enviar qualquer dado, principalmente informações sensíveis, como senhas e números de cartões de crédito.

4.2.2.5 Utilização de computadores de terceiros

Você utiliza um computador de terceiros, por exemplo, em uma *LAN house*, *cybercafe* ou *stand* de um evento, para acessar um *site* de comércio eletrônico ou *Internet Banking*.

Risco: como estes computadores são utilizados por muitas pessoas, você pode ter todas as suas ações monitoradas (incluindo a digitação de senhas ou número de cartões de crédito), através de programas especificamente projetados para este fim (como visto na seção 4.2.2.1) e que podem ter sido instalados previamente.

Recomendação: não utilize computadores de terceiros em operações que necessitem de seus dados pessoais e financeiros, incluindo qualquer uma de suas senhas.

4.2.3 Quais são os cuidados que devo ter ao acessar *sites* de comércio eletrônico ou *Internet Banking*?

Existem diversos cuidados que um usuário deve ter ao acessar *sites* de comércio eletrônico ou *Internet Banking*. Dentre eles, podem-se citar:

- 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 (vide seção 4.2.4);
- 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 (vide seção 4.2.6);
- estar atento e prevenir-se dos ataques de engenharia social (como visto na seção 4.1.1);
- 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*.

Além dos cuidados apresentados anteriormente é muito importante que você tenha alguns cuidados adicionais, tais como:

- manter o seu *browser* sempre atualizado e com todas as correções (*patches*) aplicadas;
- alterar a configuração do seu *browser* para restringir a execução de *JavaScript* e de programas *Java* ou *ActiveX*, exceto para casos específicos;
- configurar seu *browser* para bloquear *pop-up windows* e permití-las apenas para *sites* conhecidos e confiáveis, onde forem realmente necessárias;
- configurar seu programa leitor de *e-mails* para não abrir arquivos ou executar programas automaticamente;
- não executar programas obtidos pela Internet, ou recebidos por *e-mail*.

Com estes cuidados adicionais você pode evitar que seu *browser* contenha alguma vulnerabilidade, e que programas maliciosos (como os cavalos de tróia e outros tipos de *malware*) sejam instalados em seu computador para, dentre outras finalidades, furtar dados sensíveis e fraudar seus acessos a *sites* de comércio eletrônico ou *Internet Banking*. Maiores detalhes sobre estes cuidados podem ser obtidos na Parte II: Riscos Envolvidos no Uso da Internet e Métodos de Prevenção e Parte VIII: Códigos Maliciosos (*Malware*).

4.2.4 Como verificar se a conexão é segura (criptografada)?

Existem pelo menos dois itens que podem ser visualizados na janela do seu *browser*, e que significam que as informações transmitidas entre o *browser* e o *site* visitado estão sendo criptografadas.

O primeiro pode ser visualizado no local onde o endereço do *site* é digitado. O endereço deve começar com `https://` (diferente do `http://` nas conexões normais), onde o **s** antes do sinal de dois-pontos indica que o endereço em questão é de um *site* com conexão segura e, portanto, os dados serão criptografados antes de serem enviados. A figura 4.1 apresenta o primeiro item, indicando uma conexão segura, observado nos *browsers Firefox* e *Internet Explorer*, respectivamente.

Alguns *browsers* podem incluir outros sinais na barra de digitação do endereço do *site*, que indicam que a conexão é segura. No *Firefox*, por exemplo, o local onde o endereço do *site* é digitado muda de cor, ficando amarelo, e apresenta um cadeado fechado do lado direito.

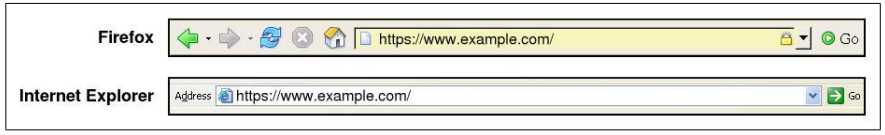

Figura 4.1: **https** - identificando site com conexão segura.

O segundo item a ser visualizado corresponde a algum desenho ou sinal, indicando que a conexão é segura. Normalmente, o desenho mais adotado nos *browsers* recentes é de um "**cadeado fechado**", apresentado na barra de *status*, na parte inferior da janela do *browser* (se o cadeado estiver aberto, a conexão não é segura).

A figura 4.2 apresenta desenhos dos cadeados fechados, indicando conexões seguras, observados nas barras de *status* nos *browsers Firefox* e *Internet Explorer*, respectivamente.

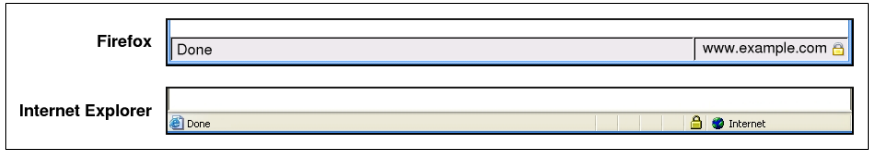

Figura 4.2: **Cadeado** – identificando site com conexão segura.

Ao clicar sobre o cadeado, será exibida uma tela que permite verificar as informações referentes ao certificado emitido para a instituição que mantém o *site* (veja seção 4.2.6), bem como informações sobre o tamanho da chave utilizada para criptografar os dados.

É muito importante que você verifique se a chave utilizada para criptografar as informações a serem transmitidas entre seu *browser* e o *site* é de no mínimo 128 bits. Chaves menores podem

comprometer a segurança dos dados a serem transmitidos. Maiores detalhes sobre criptografia e tamanho de chaves podem ser obtidos na Parte I: Conceitos de Segurança.

Outro fator muito importante é que a verificação das informações do certificado deve ser feita clicando única e exclusivamente no cadeado exibido na barra *status* do *browser*. Atacantes podem tentar forjar certificados, incluindo o desenho de um cadeado fechado no conteúdo da página. A figura 4.3 ilustra esta situação no *browser Firefox*.

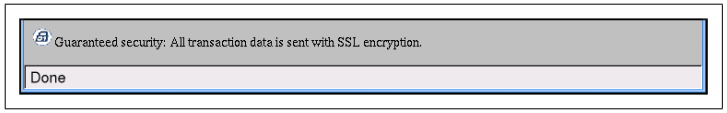

Figura 4.3: Cadeado forjado.

Compare as barras de *status* do *browser Firefox* nas figuras 4.2 e 4.3. Observe que na figura 4.3 **não** é apresentado um cadeado fechado dentro da barra de *status*, indicando que a conexão **não** é segura.

4.2.5 Como posso saber se o *site* que estou acessando não foi falsificado?

Existem alguns cuidados que um usuário deve ter para certificar-se que um *site* não foi falsificado.

O primeiro cuidado é checar se o endereço digitado permanece inalterado no momento em que o conteúdo do *site* é apresentado no *browser* do usuário. Existem algumas situações, como visto na seção 4.2.2, onde o acesso a um *site* pode ser redirecionado para uma página falsificada, mas normalmente nestes casos o endereço apresentado pelo *browser* é diferente daquele que o usuário quer realmente acessar.

E um outro cuidado muito importante é verificar as informações contidas no certificado emitido para a instituição que mantém o *site*. Estas informações podem dizer se o certificado é ou não legítimo e, conseqüentemente, se o *site* é ou não falsificado (vide seção 4.2.6).

4.2.6 Como posso saber se o certificado emitido para o *site* é legítimo?

É extremamente importante que o usuário verifique algumas informações contidas no certificado. Um exemplo de um certificado, emitido para um *site* de uma instituição é mostrado abaixo.

```
This Certificate belongs to:   This Certificate was issued by:
 www.example.org                www.examplesign.com/CPS Incorp.by Ref.
 Terms of use at                LIABILITY LTD.(c)97 ExampleSign
 www.examplesign.com/dir (c)00  ExampleSign International Server CA -
 UF Tecno                       Class 3
 Example Associados, Inc.       ExampleSign, Inc.
 Cidade, Estado, BR

Serial Number:
  70:DE:ED:0A:05:20:9C:3D:A0:A2:51:AA:CA:81:95:1A
This Certificate is valid from Sat Aug 20, 2005 to Sun
Aug 20, 2006
Certificate Fingerprint:
  92:48:09:A1:70:7A:AF:E1:30:55:EC:15:A3:0C:09:F0
```

O usuário deve, então, verificar se o certificado foi emitido para o *site* da instituição que ele deseja acessar. As seguintes informações devem ser checadas:

- o endereço do *site*;
- o nome da instituição (dona do certificado);
- o prazo de validade do certificado.

Ao entrar pela primeira vez em um *site* que usa conexão segura, seu *browser* apresentará uma janela pedindo para confirmar o recebimento de um novo certificado. Então, verifique se os dados do certificado correspondem à instituição que você realmente deseja acessar e se seu *browser* reconheceu a Autoridade Certificadora que emitiu o certificado[3].

Se ao entrar em um *site* com conexão segura, que você utilize com freqüência, seu *browser* apresentar uma janela pedindo para confirmar o recebimento de um novo certificado, fique atento. Uma situação possível seria que a validade do certificado do *site* tenha vencido, ou o certificado tenha sido revogado por outros motivos, e um novo certificado foi emitido para o *site*. Mas isto também pode significar que você está recebendo um certificado ilegítimo e, portanto, estará acessando um *site* falsificado.

Uma dica para reconhecer esta situação é que as informações contidas no certificado normalmente não corresponderão às da instituição que você realmente deseja acessar. Além disso, seu *browser* possivelmente informará que a Autoridade Certificadora que emitiu o certificado para o *site* não pôde ser reconhecida.

De qualquer modo, caso você receba um novo certificado ao acessar um *site* e tenha alguma dúvida ou desconfiança, não envie qualquer informação para o *site* antes de entrar em contato com a instituição que o mantém, para esclarecer o ocorrido.

4.2.7 O que devo fazer se perceber que meus dados financeiros estão sendo usados por terceiros?

Caso você acredite que terceiros possam estar usando suas informações pessoais e financeiras, como o número do seu cartão de crédito ou seus dados bancários (senha de acesso ao *Internet Banking* e senha do cartão de banco), entre em contato com a instituição envolvida (por exemplo, seu banco ou operadora do seu cartão de crédito), informe-os sobre o caso e siga as orientações que serão passadas por eles.

Monitore regularmente suas movimentações financeiras, por exemplo, através de extratos bancários e/ou de cartões de crédito, e procure por débitos, transferências ou cobranças inesperadas.

É recomendado que você procure uma delegacia de polícia, para registrar um boletim de ocorrência, caso tenha sido vítima de uma fraude via Internet.

[3] Os conceitos de Autoridade Certificadora e certificados digitais, bem como as principais informações encontradas em um certificado podem ser encontradas na Parte I: Conceitos de Segurança.

4.3 Boatos

Boatos (*hoaxes*) são *e-mails* que possuem conteúdos alarmantes ou falsos e que, geralmente, têm como remetente ou apontam como autora da mensagem alguma instituição, empresa importante ou órgão governamental. Através de uma leitura minuciosa deste tipo de *e-mail*, normalmente, é possível identificar em seu conteúdo mensagens absurdas e muitas vezes sem sentido.

Dentre os diversos boatos típicos, que chegam às caixas postais de usuários conectados à Internet, podem-se citar as correntes, pirâmides, mensagens sobre pessoas que estão prestes a morrer de câncer, entre outras.

Histórias deste tipo são criadas não só para espalhar desinformação pela Internet, mas também para outros fins maliciosos.

4.3.1 Quais são os problemas de segurança relacionados aos boatos?

Normalmente, o objetivo do criador de um boato é verificar o quanto ele se propaga pela Internet e por quanto tempo permanece se propagando. De modo geral, os boatos não são responsáveis por grandes problemas de segurança, a não ser ocupar espaço nas caixa de *e-mails* de usuários.

Mas podem existir casos com conseqüências mais sérias como, por exemplo, um boato que procura induzir usuários de Internet a fornecer informações importantes (como números de documentos, de contas-corrente em banco ou de cartões de crédito), ou um boato que indica uma série de ações a serem realizadas pelos usuários e que, se forem realmente efetivadas, podem resultar em danos mais sérios (como instruções para apagar um arquivo que supostamente contém um vírus, mas que na verdade é parte importante do sistema operacional instalado no computador).

Além disso, *e-mails* de boatos podem conter vírus, cavalos de tróia ou outros tipos de *malware* anexados. Maiores detalhes podem ser encontrados na Parte VIII: Códigos Maliciosos (*Malware*).

É importante ressaltar que um boato também pode comprometer a credibilidade e a reputação tanto da pessoa ou entidade referenciada como suposta criadora do boato, quanto daqueles que o repassam.

4.3.2 Como evitar a distribuição dos boatos?

Normalmente, os boatos se propagam pela boa vontade e solidariedade de quem os recebe. Isto ocorre, muitas vezes, porque aqueles que o recebem:

- confiam no remetente da mensagem;
- não verificam a procedência da mensagem;
- não checam a veracidade do conteúdo da mensagem.

Para que você possa evitar a distribuição de boatos é muito importante checar a procedência dos *e-mails*, e mesmo que tenham como remetente alguém conhecido, é preciso certificar-se que a mensagem não é um boato (veja seção 4.3.3).

É importante ressaltar que você **nunca** deve repassar este tipo de mensagem, pois estará endossando ou concordando com o seu conteúdo.

4.3.3 Como posso saber se um *e-mail* é um boato?

Um boato normalmente apresenta pelo menos uma das características listadas abaixo. Observe que estas características devem ser usadas apenas como guia. Nem todo boato apresenta uma destas características e mensagens legítimas podem apresentar algumas delas.

Muitas vezes, um boato:

- sugere conseqüências trágicas se uma determinada tarefa não for realizada;
- promete ganhos financeiros ou prêmios mediante a realização de alguma ação;
- fornece instruções ou arquivos anexados para, supostamente, proteger seu computador de um vírus não detectado por programas antivírus;
- afirma não ser um boato;
- apresenta diversos erros gramaticais e de ortografia;
- apresenta uma mensagem contraditória;
- contém algum texto enfatizando que você deve repassar a mensagem para o maior número de pessoas possível;
- já foi repassado diversas vezes (no corpo da mensagem normalmente é possível observar cabeçalhos de *e-mails* repassados por outras pessoas).

Existem *sites* especializados na Internet onde podem ser encontradas listas contendo os boatos que estão circulando e seus respectivos conteúdos.

Alguns destes *sites* são:

- *Hoaxbusters* – http://hoaxbusters.ciac.org/
- QuatroCantos – http://www.quatrocantos.com/LENDAS/ (em português)
- *Urban Legends and Folklore* – http://urbanlegends.about.com/
- *Urban Legends Reference Pages* – http://www.snopes.com/
- *TruthOrFiction.com* – http://www.truthorfiction.com/
- *Symantec Security Response Hoaxes* – http://www.symantec.com/avcenter/hoax.html
- *McAfee Security Virus Hoaxes* – http://vil.mcafee.com/hoax.asp

Além disso, os cadernos de informática dos jornais de grande circulação, normalmente, trazem matérias ou avisos sobre os boatos mais recentes.

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.

5.1 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.

5.1.1 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 IP[1] com pouca freqüência 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 rastreio da real origem do ataque;

[1] O conceito de endereço IP pode ser encontrado no Apêndice A: Glossário.

- 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*).

5.1.2 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:

- 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 larga[2] (*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.

5.1.3 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:

[2] Verifique 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.

- 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 5.2.3.

5.2 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.

5.2.1 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 equipamento[3] 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.

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

5.2.2 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;
  - 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.

5.2.3 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.

Parte VI: *Spam*

Esta parte da Cartilha aborda o conceito de *spam* e os problemas que ele pode acarretar para usuários, provedores e empresas. Também são citadas técnicas de filtragem que podem ser utilizadas por usuários para tentar bloquear o recebimento de *spams*.

6.1 *Spam*

Spam é o termo usado para se referir aos *e-mails* não solicitados, que geralmente são enviados para um grande número de pessoas. Quando o conteúdo é exclusivamente comercial, este tipo de mensagem também é referenciada como UCE (do inglês *Unsolicited Commercial E-mail*).

6.1.1 Quais são os problemas que o *spam* pode causar para um usuário da Internet?

Os usuários do serviço de correio eletrônico podem ser afetados de diversas formas. Alguns exemplos são:

Não recebimento de *e-mails*. Boa parte dos provedores de Internet limita o tamanho da caixa postal do usuário no seu servidor. Caso o número de *spams* recebidos seja muito grande o usuário corre o risco de ter sua caixa postal lotada com mensagens não solicitadas. Se isto ocorrer, o usuário não conseguirá mais receber *e-mails* e, até que possa liberar espaço em sua caixa postal, todas as mensagens recebidas serão devolvidas ao remetente. O usuário também pode deixar de receber *e-mails* em casos onde estejam sendo utilizadas regras anti-*spam* ineficientes, por exemplo, classificando como *spam* mensagens legítimas.

Gasto desnecessário de tempo. Para cada *spam* recebido, o usuário necessita gastar um determinado tempo para ler, identificar o *e-mail* como *spam* e removê-lo da caixa postal.

Aumento de custos. Independentemente do tipo de acesso a Internet utilizado, quem paga a conta pelo envio do *spam* é quem o recebe. Por exemplo, para um usuário que utiliza acesso discado a Internet, cada *spam* representa alguns segundos a mais de ligação que ele estará pagando.

Perda de produtividade. Para quem utiliza o *e-mail* como uma ferramenta de trabalho, o recebimento de *spams* aumenta o tempo dedicado à tarefa de leitura de *e-mails*, além de existir a chance de mensagens importantes não serem lidas, serem lidas com atraso ou apagadas por engano.

Conteúdo impróprio ou ofensivo. Como a maior parte dos *spams* são enviados para conjuntos aleatórios de endereços de *e-mail*, é bem provável que o usuário receba mensagens com conteúdo que julgue impróprio ou ofensivo.

Prejuízos financeiros causados por fraude. O *spam* tem sido amplamente utilizado como veículo para disseminar esquemas fraudulentos, que tentam induzir o usuário a acessar páginas clonadas de instituições financeiras ou a instalar programas maliciosos projetados para furtar dados pessoais e financeiros. Este tipo de *spam* é conhecido como *phishing/scam* (maiores detalhes na Parte IV: Fraudes na Internet). O usuário pode sofrer grandes prejuízos financeiros, caso forneça as informações ou execute as instruções solicitadas neste tipo de mensagem fraudulenta.

6.1.2 Quais são os problemas que o *spam* pode causar para os provedores de acesso, *backbones* e empresas?

Para as empresas e provedores os problemas são inúmeros e, muitas vezes, o custo adicional causado pelo *spam* é transferido para a conta a ser paga pelos usuários.

Alguns dos problemas sentidos pelos provedores e empresas são:

Impacto na banda. Para as empresas e provedores o volume de tráfego gerado por causa de *spams* os obriga a aumentar a capacidade de seus *links* de conexão com a Internet. Como o custo dos *links* é alto, isto diminui os lucros do provedor e muitas vezes pode refletir no aumento dos custos para o usuário.

Má utilização dos servidores. Os servidores de *e-mail* dedicam boa parte do seu tempo de processamento para tratar das mensagens não solicitadas. Além disso, o espaço em disco ocupado por mensagens não solicitadas enviadas para um grande número de usuários é considerável.

Inclusão em listas de bloqueio. O provedor que tenha usuários envolvidos em casos de *spam* pode ter sua rede incluída em listas de bloqueio. Esta inclusão pode prejudicar o recebimento de *e-mails* por parte de seus usuários e ocasionar a perda de clientes.

Investimento em pessoal e equipamentos. Para lidar com todos os problemas gerados pelo *spam*, os provedores necessitam contratar mais técnicos especializados, comprar equipamentos e acrescentar sistemas de filtragem de *spam*. Como conseqüência os custos do provedor aumentam.

6.1.3 Como os *spammers* conseguem endereços de *e-mail*?

Os *spammers* utilizam diversas formas para obter endereços de *e-mail*, desde a compra de bancos de dados com *e-mails* variados, até a produção de suas próprias listas de *e-mails* obtidos via programas maliciosos, *harvesting* e ataques de dicionário.

A obtenção através de programas maliciosos é possível devido à grande ligação entre os *spammers* e aqueles que desenvolvem estes programas. Um programa malicioso, muitas vezes, é projetado também para varrer o computador onde foi instalado em busca de endereços de *e-mail*, por exemplo, na lista de endereços (*address book*) do usuário. Os endereços de *e-mail* coletados são, então, repassados para os *spammers*.

Já o *harvesting* é uma técnica utilizada por *spammers* que consiste em varrer páginas *Web*, arquivos de listas de discussão, entre outros, em busca de endereços de *e-mail*.

Muitas vezes, os endereços de *e-mail* aparecem de forma ofuscada. Exemplos são as páginas *Web* ou listas de discussão que apresentam os endereços de *e-mail* com o "`@`" substituído por "`(at)`" e os pontos substituídos pela palavra "`dot`". Vale lembrar, entretanto, que os programas que implementam as técnicas de *harvesting* utilizadas pelos *spammers* podem prever estas substituições.

Nos ataques de dicionário, por sua vez, o *spammer* forma endereços de *e-mail* a partir de listas de nomes de pessoas, de palavras presentes em dicionários e/ou da combinação de caracteres alfanuméricos.

6.1.4 Como os *spammers* confirmam que um endereço de *e-mail* existe?

Os *spammers* utilizam vários artifícios para confirmar a existência de endereços de *e-mail*. Um destes artifícios consiste em enviar mensagens para os endereços formados em ataques de dicionários e, com base nas respostas enviadas pelo servidores de *e-mail* que receberam as mensagens, identificar quais endereços são válidos e quais não são.

Outro artifício largamente utilizado é a inclusão no *spam* de um suposto mecanismo para a remoção da lista de *e-mails*, que pode ser um *link* ou endereço de *e-mail*. Ao receberem uma solicitação de remoção, os *spammers* confirmam que o endereço de *e-mail* é válido e realmente alguém o utiliza.

Uma outra forma para verificar endereços é o *Web bug*. *Web bug* é uma imagem, normalmente muito pequena e invisível, que faz parte de uma página *Web* ou de uma mensagem de *e-mail*, e que é projetada para monitorar quem está acessando esta página *Web* ou mensagem de *e-mail*.

Quando o *Web bug* é visualizado, diversas informações são armazenadas no servidor onde está hospedado, tais como: o endereço IP do computador que o acessou, a URL completa da imagem que corresponde ao *Web bug*, o horário em que foi visualizado, etc.

Por exemplo, um *spammer* poderia utilizar *Web bugs* para a validação de endereços de *e-mail* da seguinte forma:

- criando a imagem do *Web bug* com o nome do endereço de *e-mail* que quer validar;
  Exemplo: `fulano.png`
- hospedando o *Web bug* em um servidor onde tenha acesso a informações que serão geradas quando o *Web bug* for visualizado;
- criando uma mensagem de *e-mail* no formato HTML, que tenha em seu conteúdo a URL completa da imagem correspondente ao *Web bug*;
  Exemplo: `http://www.dominio-do-spammer.example.org/fulano.png`
- enviando a mensagem criada para o endereço de *e-mail* a ser validado.
  Exemplo: `fulano@dominio-do-fulano.example.org`

Quando o usuário "fulano" abre a mensagem enviada pelo *spammer* em seu programa leitor de *e-mails*, o *Web bug* é acessado e o *spammer* tem a confirmação de que o endereço de *e-mail* do "fulano" é válido.

Para impedir que este artifício tenha sucesso e evitar que um endereço de *e-mail* seja validado por um *spammer*, é possível desabilitar no programa leitor de *e-mails* o modo de visualização no formato HTML.

6.1.5 Como fazer para filtrar os *e-mails* de modo a barrar o recebimento de *spams*?

Existem basicamente dois tipos de *software* que podem ser utilizados para barrar *spams*: aqueles que são colocados nos servidores, e que filtram os *e-mails* antes que cheguem até o usuário, e aqueles que são instalados nos computadores dos usuários, que filtram os *e-mails* com base em regras individuais de cada usuário.

Podem ser encontradas referências para diversas ferramentas de filtragem de *e-mails* nas páginas abaixo:

- *Spam e-mail blocking and filtering* – http://spam.abuse.net/userhelp/#filter
- *Anti Spam Yellow Pages* – http://www.antispamyellowpages.com/

Também é interessante consultar seu provedor de acesso, ou o administrador de sua rede, para verificar se existe algum recurso anti-*spam* disponível e como utilizá-lo.

6.1.6 Para quem devo reclamar quando receber um *spam*?

Deve-se reclamar de *spams* para os responsáveis pela rede de onde partiu a mensagem. Se esta rede possuir uma política de uso aceitável, a pessoa que enviou o *spam* pode receber as penalidades que nela estão previstas.

Muitas vezes, porém, é difícil conhecer a real origem do *spam*. Os *spammers* costumam enviar suas mensagens através de máquinas mal configuradas, que permitem que terceiros as utilizem para enviar os *e-mails*. Se isto ocorrer, a reclamação para a rede de origem do *spam* servirá para alertar os seus responsáveis dos problemas com suas máquinas.

Além de enviar a reclamação para os responsáveis pela rede de onde saiu a mensagem, procure manter o *e-mail* mail-abuse@cert.br na cópia de reclamações de *spam*. Deste modo, o CERT.br pode manter dados estatísticos sobre a incidência e origem de *spams* no Brasil e, também, identificar máquinas mal configuradas que estejam sendo abusadas por *spammers*.

Vale comentar que recomenda-se não responder a um *spam* ou enviar uma mensagem solicitando a remoção da lista de *e-mails*. Geralmente, este é um dos métodos que os *spammers* utilizam para confirmar que um endereço de *e-mail* é válido e realmente alguém o utiliza.

Informações sobre como encontrar os responsáveis por uma rede são apresentadas na Parte VII: Incidentes de Segurança e Uso Abusivo da Rede.

6.1.7 Que informações devo incluir numa reclamação de *spam*?

Para que os responsáveis por uma rede possam identificar a origem de um *spam* é necessário que seja enviada a mensagem recebida acompanhada do seu **cabeçalho completo** (*header*).

É no cabeçalho de uma mensagem que estão as informações sobre o endereço IP de origem da mensagem, por quais servidores de *e-mail* a mensagem passou, entre outras.

Informações sobre como obter os cabeçalhos de mensagens podem ser encontradas em http://www.antispam.org.br/header.html.

Informações sobre como entender os diversos campos normalmente encontrados nos cabeçalhos de *e-mails* estão disponíveis nas páginas abaixo (em inglês):

- *Reading Email Headers* – http://www.stopspam.org/email/headers.html
- *Tracking Spam* – http://www.claws-and-paws.com/spam-l/tracking.html

6.1.8 O que devo fazer ao identificar em um *spam* um caso de *phishing/scam*?

Ao identificar um *spam* como sendo um caso de *phishing/scam*, você deve enviar uma reclamação para os responsáveis pela rede de onde partiu a mensagem e para os responsáveis pelo *site* onde o esquema fraudulento está sendo hospedado[1]. A reclamação deve conter não só o cabeçalho (como visto na seção 6.1.7), mas também o **conteúdo completo** da mensagem recebida.

Dicas sobre como obter o conteúdo completo de mensagens em diversos programas leitores de *e-mails* estão disponíveis em http://www.spamcop.net/fom-serve/cache/19.html (em inglês).

Além de enviar a reclamação para os responsáveis pela rede de onde saiu a mensagem e pelo *site* onde o esquema fraudulento está sendo hospedado, procure manter o *e-mail* cert@cert.br na cópia da reclamação. Deste modo, o CERT.br pode manter dados estatísticos sobre a incidência e origem de fraudes no Brasil e, também, repassar a reclamação para os contatos dos responsáveis que, por ventura, não tenham sido identificados.

É muito importante incluir o conteúdo completo da mensagem na reclamação, pois só assim será possível identificar o *site* utilizado para hospedar o esquema fraudulento, que pode ser uma página clonada de uma instituição financeira, um arquivo malicioso para furtar dados pessoais e financeiros de usuários, entre outros.

Mais detalhes sobre *phishing/scam* e outros tipos de fraude via Internet podem ser encontrados na Parte IV: Fraudes na Internet.

6.1.9 Onde posso encontrar outras informações sobre *spam*?

Diversas informações podem ser encontradas no *site* http://www.antispam.br/, mantido pelo Comitê Gestor da Internet no Brasil (CGI.br), e que constitui uma fonte de referência sobre o *spam*. Este *site* tem o compromisso de informar o usuário e o administrador de redes sobre o *spam*, suas implicações e formas de proteção e combate.

[1] Informações sobre como obter contatos dos responsáveis de uma rede estão na Parte VII: Incidentes de Segurança e Uso Abusivo da Rede.

Parte VII: Incidentes de Segurança e Uso Abusivo da Rede

Esta parte da Cartilha aborda tópicos relativos a incidentes de segurança e uso abusivo da rede. São discutidos os conceitos de política de segurança, política de uso aceitável, registros de eventos e sistemas de detecção de intrusão. Também são discutidos os procedimentos relativos ao processo de identificação e notificação de incidentes de segurança.

7.1 Incidentes de Segurança e Abusos

7.1.1 O que é incidente de segurança?

Um incidente de segurança pode ser definido como qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de computação ou de redes de computadores.

São exemplos de incidentes de segurança:

- tentativas de ganhar acesso não autorizado a sistemas ou dados;
- ataques de negação de serviço;
- uso ou acesso não autorizado a um sistema;
- modificações em um sistema, sem o conhecimento, instruções ou consentimento prévio do dono do sistema;
- desrespeito à política de segurança ou à política de uso aceitável de uma empresa ou provedor de acesso.

7.1.2 O que é política de segurança?

A política de segurança atribui direitos e responsabilidades às pessoas que lidam com os recursos computacionais de uma instituição e com as informações neles armazenados. Ela também define as atribuições de cada um em relação à segurança dos recursos com os quais trabalham.

Uma política de segurança também deve prever o que pode ser feito na rede da instituição e o que será considerado inaceitável. Tudo o que descumprir a política de segurança pode ser considerado um incidente de segurança.

Na política de segurança também são definidas as penalidades às quais estão sujeitos aqueles que não cumprirem a política.

7.1.3 O que é política de uso aceitável (AUP)?

A política de uso aceitável (AUP, de *Acceptable Use Policy*) é um documento que define como os recursos computacionais de uma organização podem ser utilizados. Também é ela quem define os direitos e responsabilidades dos usuários.

Os provedores de acesso a Internet normalmente deixam suas políticas de uso aceitável disponíveis em suas páginas. Empresas costumam dar conhecimento da política de uso aceitável no momento da contratação ou quando o funcionário começa a utilizar os recursos computacionais da empresa.

7.1.4 O que pode ser considerado uso abusivo da rede?

Não há uma definição exata do que possa ser considerado um uso abusivo da rede.

Internamente às empresas e instituições, situações que caracterizam o uso abusivo da rede estão definidas na política de uso aceitável. Na Internet como um todo, os comportamentos listados abaixo são geralmente considerados como uso abusivo:

- envio de *spam* (mais informações na Parte VI: *Spam*);
- envio de correntes da felicidade e de correntes para ganhar dinheiro rápido (mais informações na Parte IV: Fraudes na Internet);
- envio de *e-mails* de *phishing/scam* (mais informações na Parte IV: Fraudes na Internet);
- cópia e distribuição não autorizada de material protegido por direitos autorais;
- utilização da Internet para fazer difamação, calúnia e ameaças;
- ataques a outros computadores;
- comprometimento de computadores ou redes.

7.2 Registros de Eventos (*logs*)

7.2.1 O que são *logs*?

Os *logs* são registros de atividades gerados por programas de computador. No caso de *logs* relativos a incidentes de segurança, eles normalmente são gerados por *firewalls*[1] ou por sistemas de detecção de intrusão.

[1] Maiores detalhes na seção *Firewalls* da Parte II: Riscos Envolvidos no Uso da Internet e Métodos de Prevenção.

7.2.2 O que é um sistema de detecção de intrusão (IDS)?

Um sistema de detecção de intrusão (IDS – *Intrusion Detection System*) é um programa, ou um conjunto de programas, cuja função é detectar atividades maliciosas ou anômalas.

IDSs podem ser instalados de modo a monitorar as atividades relativas a um computador ou a uma rede.

7.2.3 Que tipo de atividade pode ocasionar a geração de um *log*?

Os *firewalls*, dependendo de como foram configurados, podem gerar *logs* quando alguém tenta acessar um computador e este acesso é barrado pelo *firewall*. Sempre que um *firewall* gera um *log* informando que um determinado acesso foi barrado, isto pode ser considerado uma tentativa de invasão, mas também pode ser um falso positivo (vide seção 7.2.4).

Já os sistemas de detecção de intrusão podem gerar *logs* tanto para casos de tentativa de invasão, quanto para casos em que um ataque teve sucesso. Apenas uma análise detalhada pode dizer se uma atividade detectada por um IDS foi um ataque com sucesso. Assim como os *firewalls*, os sistemas de detecção de intrusão também podem gerar falsos positivos.

7.2.4 O que é um falso positivo?

O termo "falso positivo" é utilizado para designar uma situação em que um *firewall* ou IDS aponta uma atividade como sendo um ataque, quando na verdade esta atividade não é um ataque.

Um exemplo clássico de falso positivo ocorre no caso de usuários que costumam se conectar em servidores de IRC e que possuem um *firewall* pessoal. Atualmente boa parte dos servidores de IRC possui uma política de uso que define que um usuário, para se conectar em determinados servidores, não deve possuir em sua máquina pessoal nenhum *software* que atue como *proxy*[2]. Para verificar se um usuário tem algum *software* deste tipo, ao receberem uma solicitação de conexão por parte de um cliente, os servidores enviam para a máquina do cliente algumas conexões que checam pela existência destes programas. Se o usuário possuir um *firewall* é quase certo que estas conexões serão apontadas como um ataque.

Outro caso comum de falso positivo ocorre quando o *firewall* não está devidamente configurado e indica como ataques respostas a solicitações feitas pelo próprio usuário.

7.2.5 Que tipo de informação está presente em um *log*?

Os *logs* relativos a ataques recebidos pela rede, em geral, possuem as seguintes informações:

- Data e horário em que ocorreu uma determinada atividade;
- Endereço IP[3] de origem da atividade;

[2] A definição de *proxy* pode ser encontrada no Apêndice A: Glossário.
[3] A definição de endereço IP pode ser encontrada no Apêndice A: Glossário.

- Portas envolvidas;

Dependendo do grau de refinamento da ferramenta que gerou o *log* ele também pode conter informações como:

- O *time zone*[4] do horário do *log*;
- Protocolo utilizado (TCP, UDP, ICMP, etc).
- Os dados completos que foram enviados para o computador ou rede.

7.3 Notificações de Incidentes e Abusos

7.3.1 Por que devo notificar incidentes?

Quando um ataque é lançado contra uma máquina ele normalmente tem uma destas duas origens:

- um programa malicioso que está fazendo um ataque de modo automático, como por exemplo um *bot* ou um *worm*[5];
- uma pessoa que pode estar ou não utilizando ferramentas que automatizam ataques.

Quando o ataque parte de uma máquina que foi vítima de um *bot* ou *worm*, reportar este incidente para os responsáveis pela máquina que originou o ataque vai ajudá-los a identificar o problema e resolvê-lo.

Se este não for o caso, a pessoa que atacou o seu computador pode ter violado a política de uso aceitável da rede que utiliza ou, pior ainda, pode ter invadido uma máquina e a utilizado para atacar outros computadores. Neste caso, avisar os responsáveis pela máquina de onde partiu o ataque pode alertá-los para o mau comportamento de um usuário ou para uma invasão que ainda não havia sido detectada.

7.3.2 Para quem devo notificar os incidentes?

Os incidentes ocorridos devem ser notificados para os responsáveis pela máquina que originou a atividade e também para os grupos de resposta a incidentes e abusos das redes envolvidas. De modo geral a lista de pessoas/entidades a serem notificadas inclui:

- os responsáveis pela rede que originou o incidente, incluindo o grupo de segurança e abusos, se existir um para aquela rede;
- o grupo de segurança e abusos da rede em que você está conectado (seja um provedor, empresa, universidade ou outro tipo de instituição);

Mantenha o CERT.br (cert@cert.br) na cópia da mensagem, caso algum dos *sites* envolvidos seja brasileiro.

[4] Fuso horário. Mais informações em http://www.cert.br/docs/faq1.html.
[5] Mais detalhes sobre *bot* e *worm* estão na Parte VIII: Códigos Maliciosos (*Malware*).

7.3.3 Por que devo manter o CERT.br na cópia das notificações?

O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br[6]), mantido pelo Comitê Gestor da Internet no Brasil (CGI.br), é responsável pelo tratamento de incidentes de segurança em computadores envolvendo redes conectadas à Internet no Brasil.

Dentre as atribuições do CERT.br estão:

- ser um ponto central para notificações de incidentes de segurança no Brasil, de modo a prover a coordenação e o apoio no processo de resposta a incidentes, colocando as partes envolvidas em contato quando necessário;
- manter estatísticas sobre os incidentes a ele reportados[7];
- desenvolver documentação[8] de apoio para usuários e administradores de redes Internet.

Manter o CERT.br nas cópias das notificações de incidentes de segurança é importante para permitir que:

- as estatísticas geradas reflitam os incidentes ocorridos na Internet brasileira;
- o CERT.br escreva documentos direcionados para as necessidades dos usuários da Internet no Brasil;
- o CERT.br possa correlacionar dados relativos a vários incidentes, identificar ataques coordenados, novos tipos de ataques, etc.

7.3.4 Como encontro os responsáveis pela máquina de onde partiu um ataque?

Na Internet são mantidas diversas bases de dados com as informações a respeito dos responsáveis por cada bloco de números IP[9] existente. Estas bases de dados estão nos chamados "Servidores de *Whois*".

O servidor de *Whois* para os IPs alocados ao Brasil pode ser consultado em http://registro.br/. Para os demais países e continentes existem diversos outros servidores. O *site* http://www.geektools.com/whois.php aceita consultas referentes a qualquer número IP e redireciona estas consultas para os servidores de *Whois* apropriados.

Os passos para encontrar os dados dos responsáveis incluem:

- Acessar o *site* http://registro.br/ e fazer uma pesquisa pelo número IP ou pelo nome de domínio da máquina de onde partiu a atividade;
- Se o IP da máquina estiver alocado para o Brasil, os dados dos responsáveis serão exibidos;

[6] Anteriormente denominado NBSO – NIC BR *Security Office*.
[7] http://www.cert.br/stats/
[8] http://www.cert.br/docs/
[9] O conceito de número IP pode ser encontrado no Apêndice A: Glossário.

- Se aparecer a mensagem: "`Não alocado para o Brasil`", significa que o IP está alocado para algum outro país. Uma consulta no *site* `http://www.geektools.com/whois.php` pode retornar os *e-mails* dos responsáveis.

Vale lembrar que os *e-mails* que são encontrados a partir destas consultas não são necessariamente os *e-mails* da pessoa que praticou o ataque. Estes *e-mails* são dos responsáveis pela rede onde a máquina está conectada, ou seja, podem ser os administradores da rede, sócios da empresa, ou qualquer outra pessoa que foi designada para cuidar da conexão da instituição com a Internet.

7.3.5 Que informações devo incluir em uma notificação de incidente?

Para que os responsáveis pela rede de onde partiu o incidente possam identificar a origem da atividade é necessário que a notificação contenha dados que permitam esta identificação.

São dados essenciais a serem incluídos em uma notificação:

- *logs* completos;
- data, horário e *time zone* (fuso horário) dos *logs* ou da ocorrência da atividade sendo notificada;
- dados completos do incidente ou qualquer outra informação que tenha sido utilizada para identificar a atividade.

7.3.6 Como devo proceder para notificar casos de *phishing/scam*?

Um caso de *phishing/scam* deve ser tratado de forma diferente de outros tipos de incidente, pois não necessariamente haverá *logs* gerados por um *firewall* ou IDS, por exemplo.

O *phishing/scam* é uma mensagem de *e-mail* que procura induzir o usuário a fornecer dados pessoais e financeiros. Desta forma, uma notificação de incidente deste tipo deve conter o cabeçalho e conteúdo completos da mensagem recebida pelo usuário.

A notificação deve ser enviada para os responsáveis pelas redes envolvidas, mantendo o CERT.br (`cert@cert.br`) na cópia da mensagem de notificação. As informações de contato dos responsáveis pelas redes envolvidas, ou seja, do servidor de onde partiu o *e-mail* e do *site* que está hospedando o esquema fraudulento, devem ser obtidas no cabeçalho e conteúdo da mensagem de *phishing/scam*.

Mais detalhes sobre *phishing/scam* podem ser obtidos na Parte IV: Fraudes na Internet. Informações sobre como obter cabeçalhos e conteúdos completos de mensagens de *e-mail* podem ser encontradas na Parte VI: *Spam*.

7.3.7 Onde posso encontrar outras informações a respeito de notificações de incidentes?

O CERT.br mantém uma FAQ (*Frequently Asked Questions*) com respostas para as dúvidas mais comuns relativas ao processo de notificação de incidentes. A FAQ pode ser encontrada em: `http://www.cert.br/docs/faq1.html`.

Parte VIII: Códigos Maliciosos (*Malware*)

Esta parte da Cartilha aborda os conceitos e métodos de prevenção para diversos códigos maliciosos (*malwares*), que são programas especificamente desenvolvidos para executar ações danosas em um computador. Dentre eles serão discutidos vírus, cavalos de tróia, *spywares*, *backdoors*, *keyloggers*, *worms*, *bots* e *rootkits*.

8.1 Vírus

Vírus é um programa ou parte de um programa de computador, normalmente malicioso, que se propaga infectando, isto é, inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos de um computador. O vírus **depende** da execução do programa ou arquivo hospedeiro para que possa se tornar ativo e dar continuidade ao processo de infecção.

Nesta seção, entende-se por computador qualquer dispositivo computacional passível de infecção por vírus. Computadores domésticos, *notebooks*, telefones celulares e PDAs são exemplos de dispositivos computacionais passíveis de infecção.

8.1.1 Como um vírus pode afetar um computador?

Normalmente o vírus tem controle total sobre o computador, podendo fazer de tudo, desde mostrar uma mensagem de "feliz aniversário", até alterar ou destruir programas e arquivos do disco.

8.1.2 Como o computador é infectado por um vírus?

Para que um computador seja infectado por um vírus, é preciso que um programa previamente infectado seja executado. Isto pode ocorrer de diversas maneiras, tais como:

- abrir arquivos anexados aos *e-mails*;
- abrir arquivos do Word, Excel, etc;
- abrir arquivos armazenados em outros computadores, através do compartilhamento de recursos;
- instalar programas de procedência duvidosa ou desconhecida, obtidos pela Internet, de disquetes, *pen drives*, CDs, DVDs, etc;
- ter alguma mídia removível (infectada) conectada ou inserida no computador, quando ele é ligado.

Novas formas de infecção por vírus podem surgir. Portanto, é importante manter-se informado através de jornais, revistas e dos *sites* dos fabricantes de antivírus.

8.1.3 Um computador pode ser infectado por um vírus sem que se perceba?

Sim. Existem vírus que procuram permanecer ocultos, infectando arquivos do disco e executando uma série de atividades sem o conhecimento do usuário. Ainda existem outros tipos que permanecem inativos durante certos períodos, entrando em atividade em datas específicas.

8.1.4 O que é um vírus propagado por *e-mail*?

Um vírus propagado por *e-mail* (*e-mail borne virus*) normalmente é recebido como um arquivo anexado à uma mensagem de correio eletrônico. O conteúdo dessa mensagem procura induzir o usuário a clicar sobre o arquivo anexado, fazendo com que o vírus seja executado. Quando este tipo de vírus entra em ação, ele infecta arquivos e programas e envia cópias de si mesmo para os contatos encontrados nas listas de endereços de *e-mail* armazenadas no computador do usuário.

É importante ressaltar que este tipo específico de vírus não é capaz de se propagar automaticamente. O usuário precisa executar o arquivo anexado que contém o vírus, ou o programa leitor de *e-mails* precisa estar configurado para auto-executar arquivos anexados.

8.1.5 O que é um vírus de macro?

Uma macro é um conjunto de comandos que são armazenados em alguns aplicativos e utilizados para automatizar algumas tarefas repetitivas. Um exemplo seria, em um editor de textos, definir uma macro que contenha a seqüência de passos necessários para imprimir um documento com a orientação de retrato e utilizando a escala de cores em tons de cinza.

Um vírus de macro é escrito de forma a explorar esta facilidade de automatização e é parte de um arquivo que normalmente é manipulado por algum aplicativo que utiliza macros. Para que o vírus possa ser executado, o arquivo que o contém precisa ser aberto e, a partir daí, o vírus pode executar uma série de comandos automaticamente e infectar outros arquivos no computador.

Existem alguns aplicativos que possuem arquivos base (modelos) que são abertos sempre que o aplicativo é executado. Caso este arquivo base seja infectado pelo vírus de macro, toda vez que o aplicativo for executado, o vírus também será.

Arquivos nos formatos gerados por programas da Microsoft, como o Word, Excel, Powerpoint e Access, são os mais suscetíveis a este tipo de vírus. Arquivos nos formatos RTF, PDF e *PostScript* são menos suscetíveis, mas isso não significa que não possam conter vírus.

8.1.6 Como posso saber se um computador está infectado?

A melhor maneira de descobrir se um computador está infectado é através dos programas antivírus[1].

É importante ressaltar que o antivírus e suas assinaturas devem estar **sempre atualizados**, caso contrário poderá **não** detectar os vírus mais recentes.

8.1.7 Existe alguma maneira de proteger um computador de vírus?

Sim. Algumas das medidas de prevenção contra a infecção por vírus são:

- instalar e manter atualizados um bom programa antivírus e suas assinaturas;
- 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;
- procurar utilizar na elaboração de documentos formatos menos suscetíveis à propagação de vírus, tais como RTF, PDF ou *PostScript*;
- procurar não utilizar, no caso de arquivos comprimidos, o formato executável. Utilize o próprio formato compactado, como por exemplo Zip ou Gzip.

8.1.8 O que é um vírus de telefone celular?

Um vírus de celular se propaga de telefone para telefone através da tecnologia *bluetooth*[2] ou da tecnologia MMS[3] (*Multimedia Message Service*). A infecção se dá da seguinte forma:

1. O usuário recebe uma mensagem que diz que seu telefone está prestes a receber um arquivo.
2. O usuário permite que o arquivo infectado seja recebido, instalado e executado em seu aparelho.
3. O vírus, então, continua o processo de propagação para outros telefones, através de uma das tecnologias mencionadas anteriormente.

Os vírus de celular diferem-se dos vírus tradicionais, pois normalmente não inserem cópias de si mesmos em outros arquivos armazenados no telefone celular, mas podem ser especificamente projetados para sobrescrever arquivos de aplicativos ou do sistema operacional instalado no aparelho.

Depois de infectar um telefone celular, o vírus pode realizar diversas atividades, tais como: destruir/sobrescrever arquivos, remover contatos da agenda, efetuar ligações telefônicas, drenar a carga da bateria, além de tentar se propagar para outros telefones.

[1] Maiores detalhes sobre antivírus podem ser encontrados na Parte II: Riscos Envolvidos no Uso da Internet e Métodos de Prevenção.
[2] Mais detalhes sobre a tecnologia *bluetooth* podem ser encontrados na Parte III: Privacidade.
[3] A definição deste termo pode ser encontrada no Apêndice A: Glossário.

8.1.9 Como posso proteger um telefone celular de vírus?

Algumas das medidas de prevenção contra a infecção por vírus em telefones celulares são:

- mantenha o *bluetooth* do seu aparelho desabilitado e somente habilite-o quando for necessário. Caso isto não seja possível, consulte o manual do seu aparelho e configure-o para que não seja identificado (ou "descoberto") por outros aparelhos (em muitos aparelhos esta opção aparece como "Oculto" ou "Invisível");
- não permita o recebimento de arquivos enviados por terceiros, mesmo que venham de pessoas conhecidas, salvo quando você estiver esperando o recebimento de um arquivo específico;
- fique atento às notícias veiculadas no *site* do fabricante do seu aparelho, principalmente àquelas sobre segurança;
- aplique 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, restaure as opções de fábrica (em muitos aparelhos esta opção aparece como "Restaurar Configuração de Fábrica" ou "Restaurar Configuração Original") e configure-o como descrito no primeiro item, antes de inserir quaisquer dados.

Os fabricantes de antivírus têm disponibilizado versões para diversos modelos de telefones celulares. Caso você opte por instalar um antivírus em seu telefone, consulte o fabricante e verifique a viabilidade e disponibilidade de instalação para o modelo do seu aparelho. Lembre-se de manter o antivírus sempre atualizado.

8.2 Cavalos de Tróia

Conta a mitologia grega que o "Cavalo de Tróia" foi uma grande estátua, utilizada como instrumento de guerra pelos gregos para obter acesso a cidade de Tróia. A estátua do cavalo foi recheada com soldados que, durante a noite, abriram os portões da cidade possibilitando a entrada dos gregos e a dominação de Tróia. Daí surgiram os termos "Presente de Grego" e "Cavalo de Tróia".

Na informática, um cavalo de tróia (*trojan horse*) é um programa, normalmente recebido como um "presente" (por exemplo, cartão virtual, álbum de fotos, protetor de tela, jogo, etc), que além de executar funções para as quais foi aparentemente projetado, também executa outras funções normalmente maliciosas e sem o conhecimento do usuário.

Algumas das funções maliciosas que podem ser executadas por um cavalo de tróia são:

- instalação de *keyloggers* ou *screenloggers* (vide seção 8.5);
- furto de senhas e outras informações sensíveis, como números de cartões de crédito;
- inclusão de *backdoors*, para permitir que um atacante tenha total controle sobre o computador;
- alteração ou destruição de arquivos.

8.2.1 Como um cavalo de tróia pode ser diferenciado de um vírus ou *worm*?

Por definição, o cavalo de tróia distingue-se de um vírus ou de um *worm* por não infectar outros arquivos, nem propagar cópias de si mesmo automaticamente.

Normalmente um cavalo de tróia consiste em um único arquivo que necessita ser explicitamente executado.

Podem existir casos onde um cavalo de tróia contenha um vírus ou *worm*. Mas mesmo nestes casos é possível distinguir as ações realizadas como conseqüência da execução do cavalo de tróia propriamente dito, daquelas relacionadas ao comportamento de um vírus ou *worm*.

8.2.2 Como um cavalo de tróia se instala em um computador?

É necessário que o cavalo de tróia seja executado para que ele se instale em um computador. Geralmente um cavalo de tróia vem anexado a um *e-mail* ou está disponível em algum *site* na Internet.

É importante ressaltar que existem programas leitores de *e-mails* que podem estar configurados para executar automaticamente arquivos anexados às mensagens. Neste caso, o simples fato de ler uma mensagem é suficiente para que um arquivo anexado seja executado.

8.2.3 Que exemplos podem ser citados sobre programas contendo cavalos de tróia?

Exemplos comuns de cavalos de tróia são programas que você recebe ou obtém de algum *site* e que **parecem ser** apenas cartões virtuais animados, álbuns de fotos de alguma celebridade, jogos, protetores de tela, entre outros.

Enquanto estão sendo executados, estes programas podem ao mesmo tempo enviar dados confidenciais para outro computador, instalar *backdoors*, alterar informações, apagar arquivos ou formatar o disco rígido.

Existem também cavalos de tróia, utilizados normalmente em esquemas fraudulentos, que, ao serem instalados com sucesso, apenas exibem uma mensagem de erro.

8.2.4 O que um cavalo de tróia pode fazer em um computador?

O cavalo de tróia, na maioria das vezes, instalará programas para possibilitar que um invasor tenha controle total sobre um computador. Estes programas podem permitir que o invasor:

- tenha acesso e copie todos os arquivos armazenados no computador;
- descubra todas as senhas digitadas pelo usuário;
- formate o disco rígido do computador, etc.

8.2.5 Um cavalo de tróia pode instalar programas sem o conhecimento do usuário?

Sim. Normalmente o cavalo de tróia procura instalar, sem que o usuário perceba, programas que realizam uma série de atividades maliciosas.

8.2.6 É possível saber se um cavalo de tróia instalou algo em um computador?

A utilização de um bom programa antivírus (desde que seja atualizado freqüentemente) normalmente possibilita a detecção de programas instalados pelos cavalos de tróia.

É importante lembrar que nem sempre o antivírus será capaz de detectar ou remover os programas deixados por um cavalo de tróia, principalmente se estes programas forem mais recentes que as assinaturas do seu antivírus.

8.2.7 Existe alguma maneira de proteger um computador dos cavalos de tróia?

Sim. As principais medidas preventivas contra a instalação de cavalos de tróia são semelhantes às medidas contra a infecção por vírus e estão listadas na seção 8.1.7.

Uma outra medida preventiva é utilizar um *firewall* pessoal. Alguns *firewalls* podem bloquear o recebimento de cavalos de tróia, como descrito na Parte II: Riscos Envolvidos no Uso da Internet e Métodos de Prevenção.

8.3 *Adware* e *Spyware*

Adware (*Advertising software*) é um tipo de *software* especificamente projetado para apresentar propagandas, seja através de um *browser*, seja através de algum outro programa instalado em um computador.

Em muitos casos, os *adwares* têm sido incorporados a *softwares* e serviços, constituindo uma forma legítima de patrocínio ou retorno financeiro para aqueles que desenvolvem *software* livre ou prestam serviços gratuitos. Um exemplo do uso legítimo de *adwares* pode ser observado no programa de troca instantânea de mensagens MSN Messenger.

Spyware, por sua vez, é o termo utilizado para se referir a uma grande categoria de *software* que tem o objetivo de monitorar atividades de um sistema e enviar as informações coletadas para terceiros.

Existem *adwares* que também são considerados um tipo de *spyware*, pois são projetados para monitorar os hábitos do usuário durante a navegação na Internet, direcionando as propagandas que serão apresentadas.

Os *spywares*, assim como os *adwares*, podem ser utilizados de forma legítima, mas, na maioria das vezes, são utilizados de forma dissimulada, não autorizada e maliciosa.

Seguem algumas funcionalidades implementadas em *spywares*, que podem ter relação com o uso legítimo ou malicioso:

- monitoramento de URLs acessadas enquanto o usuário navega na Internet;
- alteração da página inicial apresentada no *browser* do usuário;
- varredura dos arquivos armazenados no disco rígido do computador;
- monitoramento e captura de informações inseridas em outros programas, como IRC ou processadores de texto;
- instalação de outros programas *spyware*;
- monitoramento de teclas digitadas pelo usuário ou regiões da tela próximas ao clique do *mouse* (vide seção 8.5);
- captura de senhas bancárias e números de cartões de crédito;
- captura de outras senhas usadas em *sites* de comércio eletrônico.

É importante ter em mente que estes programas, na maioria das vezes, comprometem a privacidade do usuário e, pior, a segurança do computador do usuário, dependendo das ações realizadas pelo *spyware* no computador e de quais informações são monitoradas e enviadas para terceiros.

A seção 8.3.1 apresenta alguns exemplos de *spywares* usados de modo legítimo e de *spywares* maliciosos.

8.3.1 Que exemplos podem ser citados sobre programas *spyware*?

Alguns exemplos de utilização de programas *spyware* de modo legítimo são:

- uma empresa pode utilizar programas *spyware* para monitorar os hábitos de seus funcionários, desde que tal monitoramento esteja previsto em contrato ou nos termos de uso dos recursos computacionais da empresa;
- um usuário pode instalar um programa *spyware* para verificar se outras pessoas estão utilizando o seu computador de modo abusivo ou não autorizado.

Na maioria das vezes, programas *spyware* são utilizados de forma dissimulada e/ou maliciosa. Seguem alguns exemplos:

- existem programas cavalo de tróia que instalam um *spyware*, além de um *keylogger* ou *screenlogger*. O *spyware* instalado monitora todos os acessos a *sites* enquanto o usuário navega na Internet. Sempre que o usuário acessa determinados *sites* de bancos ou de comércio eletrônico, o *keylogger* ou *screenlogger* é ativado para a captura de senhas bancárias ou números de cartões de crédito;
- alguns *adwares* incluem componentes *spyware* para monitorar o acesso a páginas *Web* durante a navegação na Internet e, então, direcionar as propagandas que serão apresentadas para o usuário. Muitas vezes, a licença de instalação do *adware* não diz claramente ou omite que tal monitoramento será feito e quais informações serão enviadas para o autor do *adware*, caracterizando assim o uso dissimulado ou não autorizado de um componente *spyware*.

A seção 8.3.2 apresenta algumas formas de se prevenir a instalação de programas *spyware* em um computador.

8.3.2 É possível proteger um computador de programas *spyware*?

Existem ferramentas específicas, conhecidas como "anti-*spyware*", capazes de detectar e remover uma grande quantidade de programas *spyware*. Algumas destas ferramentas são gratuitas para uso pessoal e podem ser obtidas pela Internet (antes de obter um programa anti-*spyware* pela Internet, verifique sua procedência e certifique-se que o fabricante é confiável).

Além da utilização de uma ferramenta anti-*spyware*, as medidas preventivas contra a infecção por vírus (vide seção 8.1.7) são fortemente recomendadas.

Uma outra medida preventiva é utilizar um *firewall* pessoal[4], pois alguns *firewalls* podem bloquear o recebimento de programas *spyware*. Além disso, se bem configurado, o *firewall* pode bloquear o envio de informações coletadas por estes programas para terceiros, de forma a amenizar o impacto da possível instalação de um programa *spyware* em um computador.

8.4 *Backdoors*

Normalmente um atacante procura garantir uma forma de retornar a um computador comprometido, sem precisar recorrer aos métodos utilizados na realização da invasão. Na maioria dos casos, também é intenção do atacante poder retornar ao computador comprometido sem ser notado.

A esses programas que permitem o retorno de um invasor a um computador comprometido, utilizando serviços criados ou modificados para este fim, dá-se o nome de *backdoor*.

8.4.1 Como é feita a inclusão de um *backdoor* em um computador?

A forma usual de inclusão de um *backdoor* consiste na disponibilização de um novo serviço ou substituição de um determinado serviço por uma versão alterada, normalmente possuindo recursos que permitam acesso remoto (através da Internet). Pode ser incluído por um invasor ou através de um cavalo de tróia.

Uma outra forma é a instalação de pacotes de *software*, tais como o *BackOrifice* e *NetBus*, da plataforma Windows, utilizados para administração remota. Se mal configurados ou utilizados sem o consentimento do usuário, podem ser classificados como *backdoors*.

8.4.2 A existência de um *backdoor* depende necessariamente de uma invasão?

Não. Alguns dos casos onde a existência de um *backdoor* não está associada a uma invasão são:

- instalação através de um cavalo de tróia (vide seção 8.2).
- inclusão como conseqüência da instalação e má configuração de um programa de administração remota;

[4] Mais informações podem ser obtidas na Parte II: Riscos Envolvidos no Uso da Internet e Métodos de Prevenção.

Alguns fabricantes incluem/incluíam *backdoors* em seus produtos (*softwares*, sistemas operacionais), alegando necessidades administrativas. É importante ressaltar que estes casos constituem uma séria ameaça à segurança de um computador que contenha um destes produtos instalados, mesmo que *backdoors* sejam incluídos por fabricantes conhecidos.

8.4.3 *Backdoors* são restritos a um sistema operacional específico?

Não. *Backdoors* podem ser incluídos em computadores executando diversos sistemas operacionais, tais como Windows (por exemplo, 95/98, NT, 2000, XP), Unix (por exemplo, Linux, Solaris, FreeBSD, OpenBSD, AIX), Mac OS, entre outros.

8.4.4 Existe alguma maneira de proteger um computador de *backdoors*?

Embora os programas antivírus não sejam capazes de descobrir *backdoors* em um computador, as medidas preventivas contra a infecção por vírus (seção 8.1.7) são válidas para se evitar algumas formas de instalação de *backdoors*.

A idéia é que você **não** execute programas de procedência duvidosa ou desconhecida, sejam eles recebidos por *e-mail*, sejam obtidos na Internet. A execução de tais programas pode resultar na instalação de um *backdoor*.

Caso você utilize algum programa de administração remota, certifique-se de que ele esteja bem configurado, de modo a evitar que seja utilizado como um *backdoor*.

Uma outra medida preventiva consiste na utilização de um *firewall* pessoal[5]. Apesar de não eliminarem os *backdoors*, se bem configurados, podem ser úteis para amenizar o problema, pois podem barrar as conexões entre os invasores e os *backdoors* instalados em um computador.

Também é importante visitar constantemente os *sites* dos fabricantes de *softwares* e verificar a existência de novas versões ou *patches* para o sistema operacional ou *softwares* instalados em seu computador.

Existem casos onde a disponibilização de uma nova versão ou de um *patch* está associada à descoberta de uma vulnerabilidade em um *software*, que permite a um atacante ter acesso remoto a um computador, de maneira similar ao acesso aos *backdoors*.

8.5 *Keyloggers*

Keylogger é um programa capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado de um computador.

[5] Mais informações podem ser obtidas na Parte II: Riscos Envolvidos no Uso da Internet e Métodos de Prevenção.

8.5.1 Que informações um *keylogger* pode obter se for instalado em um computador?

Um *keylogger* pode capturar e armazenar as teclas digitadas pelo usuário. Dentre as informações capturadas podem estar o texto de um *e-mail*, dados digitados na declaração de Imposto de Renda e outras informações sensíveis, como senhas bancárias e números de cartões de crédito.

Em muitos casos, a ativação do *keylogger* é condicionada a uma ação prévia do usuário, como por exemplo, após o acesso a um *site* específico de comércio eletrônico ou *Internet Banking*. Normalmente, o *keylogger* contém mecanismos que permitem o envio automático das informações capturadas para terceiros (por exemplo, através de *e-mails*).

8.5.2 Diversos *sites* de instituições financeiras utilizam teclados virtuais. Neste caso eu estou protegido dos *keyloggers*?

As instituições financeiras desenvolveram os teclados virtuais para evitar que os *keyloggers* pudessem capturar informações sensíveis de usuários. Então, foram desenvolvidas formas mais avançadas de *keyloggers*, também conhecidas como *screenloggers*, capazes de:

- armazenar a posição do cursor e a tela apresentada no monitor, nos momentos em que o *mouse* é clicado, ou
- armazenar a região que circunda a posição onde o *mouse* é clicado.

De posse destas informações um atacante pode, por exemplo, descobrir a senha de acesso ao banco utilizada por um usuário.

8.5.3 Como é feita a inclusão de um *keylogger* em um computador?

Normalmente, o *keylogger* vem como parte de um programa *spyware* (veja a seção 8.3) ou cavalo de tróia (veja a seção 8.2). Desta forma, é necessário que este programa seja executado para que o *keylogger* se instale em um computador. Geralmente, tais programas vêm anexados a *e-mails* ou estão disponíveis em *sites* na Internet.

Lembre-se que existem programas leitores de *e-mails* que podem estar configurados para executar automaticamente arquivos anexados às mensagens. Neste caso, o simples fato de ler uma mensagem é suficiente para que qualquer arquivo anexado seja executado.

8.5.4 Como posso proteger um computador dos *keyloggers*?

Para se evitar a instalação de um *keylogger*, as medidas são similares àquelas discutidas nas seções de vírus (8.1.7), cavalo de tróia (8.2.7), *worm* (8.6.3), *bots* (8.7.5) e na Parte IV: Fraudes na Internet.

8.6 *Worms*

Worm é um programa capaz de se propagar automaticamente através de redes, enviando cópias de si mesmo de computador para computador.

Diferente do vírus, o *worm* **não** embute cópias de si mesmo em outros programas ou arquivos e **não** necessita ser explicitamente executado para se propagar. Sua propagação se dá através da exploração de vulnerabilidades existentes ou falhas na configuração de *softwares* instalados em computadores.

8.6.1 Como um *worm* pode afetar um computador?

Geralmente o *worm* não tem como conseqüência os mesmos danos gerados por um vírus, como por exemplo a infecção de programas e arquivos ou a destruição de informações. Isto não quer dizer que não represente uma ameaça à segurança de um computador, ou que não cause qualquer tipo de dano.

Worms são notadamente responsáveis por consumir muitos recursos. Degradam sensivelmente o desempenho de redes e podem lotar o disco rígido de computadores, devido à grande quantidade de cópias de si mesmo que costumam propagar. Além disso, podem gerar grandes transtornos para aqueles que estão recebendo tais cópias.

8.6.2 Como posso saber se meu computador está sendo utilizado para propagar um *worm*?

Detectar a presença de um *worm* em um computador não é uma tarefa fácil. Muitas vezes os *worms* realizam uma série de atividades, incluindo sua propagação, sem que o usuário tenha conhecimento.

Embora alguns programas antivírus permitam detectar a presença de *worms* e até mesmo evitar que eles se propaguem, isto nem sempre é possível.

Portanto, o melhor é evitar que seu computador seja utilizado para propagá-los (vide seção 8.6.3).

8.6.3 Como posso proteger um computador de *worms*?

Além de utilizar um bom antivírus, que permita detectar e até mesmo evitar a propagação de um *worm*, é importante que o sistema operacional e os *softwares* instalados em seu computador não possuam vulnerabilidades.

Normalmente um *worm* procura explorar alguma vulnerabilidade disponível em um computador, para que possa se propagar. Portanto, as medidas preventivas mais importantes são aquelas que procuram evitar a existência de vulnerabilidades, como discutido na Parte II: Riscos Envolvidos no Uso da Internet e Métodos de Prevenção.

Uma outra medida preventiva é ter instalado em seu computador um *firewall* pessoal[6]. Se bem

[6] Mais informações podem ser obtidas na Parte II: Riscos Envolvidos no Uso da Internet e Métodos de Prevenção.

configurado, o *firewall* pessoal pode evitar que um *worm* explore uma possível vulnerabilidade em algum serviço disponível em seu computador ou, em alguns casos, mesmo que o *worm* já esteja instalado em seu computador, pode evitar que explore vulnerabilidades em outros computadores.

8.7 *Bots e Botnets*

De modo similar ao *worm* (seção 8.6), o *bot* é um programa capaz se propagar automaticamente, explorando vulnerabilidades existentes ou falhas na configuração de *softwares* instalados em um computador. Adicionalmente ao *worm*, dispõe de mecanismos de comunicação com o invasor, permitindo que o *bot* seja controlado remotamente.

8.7.1 Como o invasor se comunica com o *bot*?

Normalmente, o *bot* se conecta a um servidor de IRC (*Internet Relay Chat*) e entra em um canal (sala) determinado. Então, ele aguarda por instruções do invasor, monitorando as mensagens que estão sendo enviadas para este canal. O invasor, ao se conectar ao mesmo servidor de IRC e entrar no mesmo canal, envia mensagens compostas por seqüências especiais de caracteres, que são interpretadas pelo *bot*. Estas seqüências de caracteres correspondem a instruções que devem ser executadas pelo *bot*.

8.7.2 O que o invasor pode fazer quando estiver no controle de um *bot*?

Um invasor, ao se comunicar com um *bot*, pode enviar instruções para que ele realize diversas atividades, tais como:

- desferir ataques na Internet;
- executar um ataque de negação de serviço (detalhes na Parte I: Conceitos de Segurança);
- furtar dados do computador onde está sendo executado, como por exemplo números de cartões de crédito;
- enviar *e-mails* de *phishing* (detalhes na Parte IV: Fraudes na Internet);
- enviar *spam*.

8.7.3 O que são *botnets*?

Botnets são redes formadas por computadores infectados com *bots*. Estas redes podem ser compostas por centenas ou milhares de computadores. Um invasor que tenha controle sobre uma *botnet* pode utilizá-la para aumentar a potência de seus ataques, por exemplo, para enviar centenas de milhares de *e-mails* de *phishing* ou *spam*, desferir ataques de negação de serviço, etc.

8.7.4 Como posso saber se um *bot* foi instalado em um computador?

Identificar a presença de um *bot* em um computador não é uma tarefa simples. Normalmente, o *bot* é projetado para realizar as instruções passadas pelo invasor sem que o usuário tenha conhecimento.

Embora alguns programas antivírus permitam detectar a presença de *bots*, isto nem sempre é possível. Portanto, o melhor é procurar evitar que um *bot* seja instalado em seu computador (vide seção 8.7.5).

8.7.5 Como posso proteger um computador dos *bots*?

Da mesma forma que o *worm*, o *bot* é capaz de se propagar automaticamente, através da exploração de vulnerabilidades existentes ou falhas na configuração de *softwares* instalados em um computador.

Portanto, a melhor forma de se proteger dos *bots* é manter o sistema operacional e os *softwares* instalados em seu computador sempre atualizados e com todas as correções de segurança (*patches*) disponíveis aplicadas, para evitar que possuam vulnerabilidades.

A utilização de um bom antivírus, mantendo-o sempre atualizado, também é importante, pois em muitos casos permite detectar e até mesmo evitar a propagação de um *bot*. Vale lembrar que o antivírus só será capaz de detectar *bots* conhecidos.

Outra medida preventiva consiste em utilizar um *firewall* pessoal[7]. Normalmente, os *firewalls* pessoais não eliminam os *bots*, mas, se bem configurados, podem ser úteis para amenizar o problema, pois podem barrar a comunicação entre o invasor e o *bot* instalado em um computador.

Podem existir outras formas de propagação e instalação de *bots* em um computador, como por exemplo, através da execução de arquivos anexados a *e-mails*. Portanto, as medidas apresentadas na Parte II: Riscos Envolvidos no Uso da Internet e Métodos de Prevenção também são fortemente recomendadas.

8.8 *Rootkits*

Um invasor, ao realizar uma invasão, pode utilizar mecanismos para esconder e assegurar a sua presença no computador comprometido. O conjunto de programas que fornece estes mecanismos é conhecido como *rootkit*.

É muito importante ficar claro que o nome *rootkit* **não** indica que as ferramentas que o compõem são usadas para obter acesso privilegiado (*root* ou *Administrator*) em um computador, mas sim para mantê-lo. Isto significa que o invasor, após instalar o *rootkit*, terá acesso privilegiado ao computador previamente comprometido, sem precisar recorrer novamente aos métodos utilizados na realização da invasão, e suas atividades serão escondidas do responsável e/ou dos usuários do computador.

[7] Mais informações podem ser obtidas na Parte II: Riscos Envolvidos no Uso da Internet e Métodos de Prevenção.

8.8.1 Que funcionalidades um *rootkit* pode conter?

Um *rootkit* pode fornecer programas com as mais diversas funcionalidades. Dentre eles, podem ser citados:

- programas para esconder atividades e informações deixadas pelo invasor (normalmente presentes em todos os *rootkits*), tais como arquivos, diretórios, processos, conexões de rede, etc;
- *backdoors* (vide seção 8.4), para assegurar o acesso futuro do invasor ao computador comprometido (presentes na maioria dos *rootkits*);
- programas para remoção de evidências em arquivos de *logs*;
- *sniffers*[8], para capturar informações na rede onde o computador está localizado, como por exemplo senhas que estejam trafegando em claro, ou seja, sem qualquer método de criptografia;
- *scanners*[9], para mapear potenciais vulnerabilidades em outros computadores;
- outros tipos de *malware*, como cavalos de tróia, *keyloggers*, ferramentas de ataque de negação de serviço, etc.

8.8.2 Como posso saber se um *rootkit* foi instalado em um computador?

Existem programas capazes de detectar a presença de um grande número de *rootkits*, mas isto não quer dizer que são capazes de detectar todos os disponíveis (principalmente os mais recentes). Alguns destes programas são gratuitos e podem ser obtidos pela Internet (antes de obter um programa para a detecção de *rootkits* pela Internet, verifique sua procedência e certifique-se que o fabricante é confiável).

Como os *rootkits* são projetados para ficarem ocultos, ou seja, não serem detectados pelo responsável ou pelos usuários de um computador, sua identificação é, na maioria das vezes, uma tarefa bem difícil. Deste modo, o melhor é procurar evitar que um *rootkit* seja instalado em seu computador (vide seção 8.8.3).

8.8.3 Como posso proteger um computador dos *rootkits*?

Apesar de existirem programas específicos para a detecção de *rootkits*, a melhor forma de se proteger é manter o sistema operacional e os *softwares* instalados em seu computador sempre atualizados e com todas as correções de segurança (*patches*) disponíveis aplicadas, para evitar que possuam vulnerabilidades.

Desta forma, você pode evitar que um atacante consiga invadir seu computador, através da exploração de alguma vulnerabilidade, e instalar um *rootkit* após o comprometimento.

[8] A definição de *sniffer* pode ser encontrada no Apêndice A: Glossário.
[9] A definição de *scanner* pode ser encontrada no Apêndice A: Glossário.

Apêndice A: Glossário

802.11 Refere-se a um conjunto de especificações desenvolvidas pelo IEEE para tecnologias de redes sem fio.

AC Veja Autoridade certificadora.

ADSL Do Inglês ***A**symmetric **D**igital **S**ubscriber **L**ine*. Sistema que permite a utilização das linhas telefônicas para transmissão de dados em velocidades maiores que as permitidas por um *modem* convencional.

Adware Do Inglês ***Ad**vertising Soft**ware***. *Software* especificamente projetado para apresentar propagandas. Constitui uma forma de retorno financeiro para aqueles que desenvolvem *software* livre ou prestam serviços gratuitos. Pode ser considerado um tipo de *spyware*, caso monitore os hábitos do usuário, por exemplo, durante a navegação na Internet para direcionar as propagandas que serão apresentadas.

Antivírus Programa ou *software* especificamente desenvolvido para detectar, anular e eliminar de um computador vírus e outros tipos de código malicioso.

AP Do Inglês ***A**ccess **P**oint*. Dispositivo que atua como ponte entre uma rede sem fio e uma rede tradicional.

Artefato De forma geral, artefato é qualquer informação deixada por um invasor em um sistema comprometido. Pode ser um programa ou *script* utilizado pelo invasor em atividades maliciosas, um conjunto de ferramentas usadas pelo invasor, *logs* ou arquivos deixados em um sistema comprometido, a saída gerada pelas ferramentas do invasor, etc.

Assinatura digital Código utilizado para verificar a integridade de um texto ou mensagem. Também pode ser utilizado para verificar se o remetente de uma mensagem é mesmo quem diz ser.

Atacante Pessoa responsável pela realização de um ataque. Veja também Ataque.

Ataque Tentativa, bem ou mal sucedida, de acesso ou uso não autorizado a um programa ou computador. Também são considerados ataques as tentativas de negação de serviço.

Autoridade certificadora Entidade responsável por emitir certificados digitais. Estes certificados podem ser emitidos para diversos tipos de entidades, tais como: pessoa, computador, departamento de uma instituição, instituição, etc.

Backdoor Programa que permite a um invasor retornar a um computador comprometido. Normalmente este programa é colocado de forma a não ser notado.

Banda Veja Largura de banda.

Bandwidth Veja Largura de banda.

Bluetooth Termo que se refere a uma tecnologia de rádio-freqüência (RF) de baixo alcance, utilizada para a transmissão de voz e dados.

Boato *E-mail* que possui conteúdo alarmante ou falso e que, geralmente, tem como remetente ou aponta como autora da mensagem alguma instituição, empresa importante ou órgão governamental. Através de uma leitura minuciosa deste tipo de *e-mail*, normalmente, é possível identificar em seu conteúdo mensagens absurdas e muitas vezes sem sentido.

Bot Programa que, além de incluir funcionalidades de *worms*, sendo capaz de se propagar automaticamente através da exploração de vulnerabilidades existentes ou falhas na configuração de *softwares* instalados em um computador, dispõe de mecanismos de comunicação com o invasor, permitindo que o programa seja controlado remotamente. O invasor, ao se comunicar com o *bot*, pode orientá-lo a desferir ataques contra outros computadores, furtar dados, enviar *spam*, etc.

Botnets Redes formadas por diversos computadores infectados com *bots*. Podem ser usadas em atividades de negação de serviço, esquemas de fraude, envio de *spam*, etc.

Cable modem *Modem* projetado para operar sobre linhas de TV a cabo.

Cavalo de tróia
Programa, normalmente recebido como um "presente" (por exemplo, cartão virtual, álbum de fotos, protetor de tela, jogo, etc), que além de executar funções para as quais foi aparentemente projetado, também executa outras funções normalmente maliciosas e sem o conhecimento do usuário.

Certificado digital
Arquivo eletrônico, assinado digitalmente, que contém dados de uma pessoa ou instituição, utilizados para comprovar sua identidade. Veja também Assinatura digital.

Código malicioso
Termo genérico que se refere a todos os tipos de programa que executam ações maliciosas em um computador. Exemplos de códigos maliciosos são os vírus, *worms*, *bots*, cavalos de tróia, *rootkits*, etc.

Comércio eletrônico
Também chamado de *e-commerce*, é qualquer forma de transação comercial onde as partes interagem eletronicamente. Conjunto de técnicas e tecnologias computacionais utilizadas para facilitar e executar transações comerciais de bens e serviços através da Internet.

Comprometimento
Veja Invasão.

Conexão segura
Conexão que utiliza um protocolo de criptografia para a transmissão de dados, como por exemplo, HTTPS ou SSH.

Correção de segurança
Correção especificamente desenvolvida para eliminar falhas de segurança em um *software* ou sistema operacional.

Criptografia Ciência e arte de escrever mensagens em forma cifrada ou em código. É parte de um campo de estudos que trata das comunicações secretas. É usada, dentre outras finalidades, para: autenticar a identidade de usuários; autenticar transações bancárias; proteger a integridade de transferências eletrônicas de fundos, e proteger o sigilo de comunicações pessoais e comerciais.

DDoS Do Inglês ***D**istributed **D**enial **o**f **S**ervice*. Ataque de negação de serviço distribuído, ou seja, **um conjunto** de computadores é utilizado para tirar de operação um ou mais serviços ou computadores conectados à Internet. Veja Negação de serviço.

DNS Do Inglês ***D**omain **N**ame **S**ystem*. Serviço que traduz nomes de domínios para endereços IP e vice-versa.

DoS Do Inglês ***D**enial **o**f **S**ervice*. Veja Negação de serviço.

E-commerce Veja Comércio eletrônico.

Endereço IP Este endereço é um número único para cada computador conectado à Internet, composto por uma seqüência de 4 números que variam de 0 até 255, separados por ".". Por exemplo: 192.168.34.25.

Engenharia social
Método de ataque onde uma pessoa faz uso da persuasão, muitas vezes abusando da ingenuidade ou confiança do usuário, para obter informações que podem ser utilizadas para ter acesso não autorizado a computadores ou informações.

Exploit Programa ou parte de um programa malicioso projetado para explorar uma vulnerabilidade existente em um *software* de computador.

Falsa identidade
Ato onde o falsificador atribui-se identidade ilegítima, podendo se fazer passar por outra pessoa, com objetivo de obter vantagens indevidas, como por exemplo, obter crédito, furtar dinheiro de contas bancárias das vítimas, utilizar cartões de crédito de terceiros, entre outras.

Firewall Dispositivo constituído pela combinação de *software* e *hardware*, utilizado para dividir e controlar o acesso entre redes de computadores.

***Firewall* pessoal**
Software ou programa utilizado para proteger **um** computador contra acessos não autorizados vindos da Internet. É um tipo específico de *firewall*.

GnuPG Conjunto de programas gratuito e de código aberto, que implementa criptografia de chave única, de chaves pública e privada e assinatura digital.

GPG Veja GnuPG.

Harvesting Técnica utilizada por *spammers*, que consiste em varrer páginas *Web*, arquivos de listas de discussão, entre outros, em busca de endereços de *e-mail*.

Hoax Veja Boato.

HTML Do Inglês ***H**yper**T**ext **M**arkup **L**anguage*. Linguagem universal utilizada na elaboração de páginas na Internet.

HTTP Do Inglês ***H**yper**T**ext **T**ransfer **P**rotocol*. Protocolo usado para transferir páginas *Web* entre um servidor e um cliente (por exemplo, o *browser*).

HTTPS Quando utilizado como parte de uma URL, especifica a utilização de HTTP com algum mecanismo de segurança, normalmente o SSL.

Identity theft Veja Falsa identidade.

IDS Do Inglês ***I**ntrusion **D**etection **S**ystem*. Programa, ou um conjunto de programas, cuja função é detectar atividades maliciosas ou anômalas.

IEEE Acrônimo para *Institute of Electrical and Electronics Engineers*, uma organização composta por engenheiros, cientistas e estudantes, que desenvolvem padrões para a indústria de computadores e eletro-eletrônicos.

Invasão Ataque bem sucedido que resulte no acesso, manipulação ou destruição de informações em um computador.

Invasor Pessoa responsável pela realização de uma invasão (comprometimento). Veja também Invasão.

IP Veja Endereço IP.

Keylogger Programa capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado de um computador. Normalmente, a ativação do *keylogger* é condicionada a uma ação prévia do usuário, como por exemplo, após o acesso a um *site* de comércio eletrônico ou *Internet Banking*, para a captura de senhas bancárias ou números de cartões de crédito.

Largura de banda Quantidade de dados que podem ser transmitidos em um canal de comunicação, em um determinado intervalo de tempo.

Log Registro de atividades gerado por programas de computador. No caso de *logs* relativos a incidentes de segurança, eles normalmente são gerados por *firewalls* ou por IDSs.

Malware Do Inglês ***Mal**icious soft**ware*** (*software* malicioso). Veja Código malicioso.

MMS Do Inglês ***M**ultimedia **M**essage **S**ervice*. Tecnologia amplamente utilizada em telefonia celular para a transmissão de dados, como texto, imagem, áudio e vídeo.

Modem Dispositivo que permite o envio e recebimento de dados utilizando as linhas telefônicas.

Negação de serviço Atividade maliciosa onde o atacante utiliza **um** computador para tirar de operação um serviço ou computador conectado à Internet.

Número IP Veja Endereço IP.

Opt-in Regra de envio de mensagens que define que é proibido mandar *e-mails* comerciais/*spam*, a menos que exista uma concordância prévia por parte do destinatário. Veja também *Soft opt-in*.

Opt-out Regra de envio de mensagens que define que é permitido mandar *e-mails* comerciais/*spam*, mas deve-se prover um mecanismo para que o destinatário possa parar de receber as mensagens.

P2P Acrônimo para *peer-to-peer*. Arquitetura de rede onde cada computador tem funcionalidades e responsabilidades equivalentes. Difere da arquitetura cliente/servidor, onde alguns dispositivos são dedicados a servir outros. Este tipo de rede é normalmente implementada via *softwares* P2P, que permitem conectar o computador de um usuário ao de outro para compartilhar ou transferir dados, como MP3, jogos, vídeos, imagens, etc.

Password Veja Senha.

Patch Veja Correção de segurança.

PGP Do Inglês ***P**retty **G**ood **P**rivacy*. Programa que implementa criptografia de chave única, de chaves pública e privada e assinatura digital. Possui versões comerciais e gratuitas. Veja também GnuPG.

Phishing Também conhecido como *phishing scam* ou *phishing/scam*. Mensagem não solicitada que se passa por comunicação de uma instituição conhecida, como um banco, empresa ou *site* popular, e que procura induzir usuários ao fornecimento de dados pessoais e financeiros. Inicialmente, este tipo de mensagem induzia o usuário ao acesso a páginas fraudulentas na Internet. Atualmente, o termo também se refere à mensagem que induz o usuário à instalação de códigos maliciosos, além da mensagem que, no próprio conteúdo, apresenta formulários para o preenchimento e envio de dados pessoais e financeiros.

Porta dos fundos Veja *Backdoor*.

Proxy Servidor que atua como intermediário entre um cliente e outro servidor. Normalmente é utilizado em empresas para aumentar a performance de acesso a determinados serviços ou permitir que mais de uma máquina se conecte à Internet. *Proxies* mal configurados podem ser abusados por atacantes e utilizados como uma forma de tornar anônimas algumas ações na Internet, como atacar outras redes ou enviar *spam*.

Rede sem fio Rede que permite a conexão entre computadores e outros dispositivos através da transmissão e recepção de sinais de rádio.

Rootkit Conjunto de programas que tem como finalidade esconder e assegurar a presença de um invasor em um computador comprometido. É importante ressaltar que o nome *rootkit* **não** indica que as ferramentas que o compõem são usadas para obter acesso privilegiado (*root* ou *Administrator*) em um computador, mas sim para manter o acesso privilegiado em um computador previamente comprometido.

Scam Esquemas ou ações enganosas e/ou fraudulentas. Normalmente, têm como finalidade obter vantagens financeiras.

Scan Técnica normalmente implementada por um tipo de programa, projetado para efetuar varreduras em redes de computadores. Veja *Scanner*.

Scanner Programa utilizado para efetuar varreduras em redes de computadores, com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles. Amplamente utilizado por atacantes para identificar potenciais alvos, pois permite associar possíveis vulnerabilidades aos serviços habilitados em um computador.

Screenlogger Forma avançada de *keylogger*, capaz de armazenar a posição do cursor e a tela apresentada no monitor, nos momentos em que o *mouse* é clicado, ou armazenar a região que circunda a posição onde o *mouse* é clicado. Veja também *Keylogger*.

Senha Conjunto de caracteres, de conhecimento único do usuário, utilizado no processo de verificação de sua identidade, assegurando que ele é realmente quem diz ser.

Site Local na Internet identificado por um nome de domínio, constituído por uma ou mais páginas de hipertexto, que podem conter textos, gráficos e informações multimídia.

SMS Do Inglês ***S**hort **M**essage **S**ervice*. Tecnologia amplamente utilizada em telefonia celular para a transmissão de mensagens de texto curtas. Diferente do MMS, permite apenas dados do tipo texto e cada mensagem é limitada em 160 caracteres alfanuméricos.

Sniffer Dispositivo ou programa de computador utilizado para capturar e armazenar dados trafegando em uma rede de computadores. Pode ser usado por um invasor para capturar informações sensíveis (como senhas de usuários), em casos onde estejam sendo utilizadas conexões inseguras, ou seja, sem criptografia.

Soft opt-in Regra semelhante ao *opt-in*, mas neste caso prevê uma exceção quando já existe uma relação comercial entre remetente e destinatário. Desta forma, não é necessária a permissão explícita por parte do destinatário para receber *e-mails* deste remetente. Veja *Opt-in*.

Spam Termo usado para se referir aos *e-mails* não solicitados, que geralmente são enviados para um grande número de pessoas. Quando o conteúdo é exclusivamente comercial, este tipo de mensagem também é referenciada como UCE (do Inglês *Unsolicited Commercial E-mail*).

Spammer Pessoa que envia *spam*.

Spyware Termo utilizado para se referir a uma grande categoria de *software* que tem o objetivo de monitorar atividades de um sistema e enviar as informações coletadas para terceiros. Podem ser utilizados de forma legítima, mas, na maioria das vezes, são utilizados de forma dissimulada, não autorizada e maliciosa.

SSH Do Inglês ***S**ecure **Sh**ell*. Protocolo que utiliza criptografia para acesso a um computador remoto, permitindo a execução de comandos, transferência de arquivos, entre outros.

SSID Do Inglês ***S**ervice **S**et **Id**entifier*. Conjunto único de caracteres que identifica uma rede sem fio. O SSID diferencia uma rede sem fio de outra e um cliente normalmente só pode conectar em uma rede sem fio se puder fornecer o SSID correto.

SSL Do Inglês ***S**ecure **S**ockets **L**ayer*. Protocolo que fornece confidencialidade e integridade na comunicação entre um cliente e um servidor, através do uso de criptografia. Veja também HTTPS.

Time zone Fuso horário.

Trojan horse Veja Cavalo de tróia.

UCE Do inglês ***U**nsolicited **C**ommercial **E**-mail*. Termo usado para se referir aos *e-mails* comerciais não solicitados.

URL Do Inglês **U**niversal **R**esource **L**ocator. Seqüência de caracteres que indica a localização de um recurso na Internet, como por exemplo, http://cartilha.cert.br/.

Vírus Programa ou parte de um programa de computador, normalmente malicioso, que se propaga infectando, isto é, inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos de um computador. O vírus **depende** da execução do programa ou arquivo hospedeiro para que possa se tornar ativo e dar continuidade ao processo de infecção.

VPN Do Inglês ***V**irtual **P**rivate **N**etwork*. Termo usado para se referir à construção de uma rede privada utilizando redes públicas (por exemplo, a Internet) como infra-estrutura. Estes sistemas utilizam criptografia e outros mecanismos de segurança para garantir que somente usuários autorizados possam ter acesso a rede privada e que nenhum dado será interceptado enquanto estiver passando pela rede pública.

Vulnerabilidade Falha no projeto, implementação ou configuração de um *software* ou sistema operacional que, quando explorada por um atacante, resulta na violação da segurança de um computador.

Web bug Imagem, normalmente muito pequena e invisível, que faz parte de uma página *Web* ou de uma mensagem de *e-mail*, e que é projetada para monitorar quem está acessando esta página *Web* ou mensagem de *e-mail*.

WEP Do Inglês ***W**ired **E**quivalent **P**rivacy*. Protocolo de segurança para redes sem fio que implementa criptografia para a transmissão dos dados. Este protocolo apresenta algumas falhas de segurança.

Wi-Fi Do Inglês ***Wi**reless **Fi**delity*. Termo usado para se referir genericamente a redes sem fio que utilizam qualquer um dos padrões 802.11.

Wireless Veja Rede sem fio.

WLAN Do Inglês ***W**ireless **L**ocal-**A**rea **N**etwork*. Refere-se a um tipo de rede que utiliza ondas de rádio de alta freqüência, ao invés de cabos, para a comunicação entre os computadores.

Worm Programa capaz de se propagar automaticamente através de redes, enviando cópias de si mesmo de computador para computador. Diferente do vírus, o *worm* não embute cópias de si mesmo em outros programas ou arquivos e não necessita ser explicitamente executado para se propagar. Sua propagação se dá através da exploração de vulnerabilidades existentes ou falhas na configuração de *softwares* instalados em computadores.

WPA Do Inglês **W**i-Fi ***P**rotected **A**ccess*. Protocolo de segurança para redes sem fio desenvolvido para substituir o protocolo WEP, devido a suas falhas de segurança. Esta tecnologia foi projetada para, através de atualizações de *software*, operar com produtos Wi-Fi que disponibilizavam apenas a tecnologia WEP. Inclui duas melhorias em relação ao protocolo WEP que envolvem melhor criptografia para transmissão de dados e autenticação de usuário.

Apêndice B: *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.

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

B.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.

B.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.

B.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.

B.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.

B.2 Cuidados no Uso da Internet

B.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.

B.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*.

B.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.

B.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.

B.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.

B.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.

B.3 Fraude

B.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.

B.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*.

B.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.

B.4 Privacidade

B.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.

B.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.

B.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*.

B.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.

B.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.

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

B.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).

B.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.

B.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.

B.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.

B.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.

B.7 Incidentes de Segurança e Uso Abusivo da Rede

B.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.

B.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.

Apêndice C: Dicas

Este Apêndice contém um folheto com dicas básicas de segurança, uma compilação feita com base no conteúdo da Cartilha.

Este folheto está disponível para impressão na página http://cartilha.cert.br/dicas/, onde também pode ser encontrado o mesmo conteúdo em formato de *folder* dobrável e em formato HTML.

Dicas de Segurança

Proteja-se de fraudes

- Atualize seu antivírus diariamente.
- Não clique em *links* recebidos por *e-mail*.
- Não execute arquivos recebidos por *e-mail* ou via serviços de mensagem instantânea.

Proteja-se de vírus, cavalos de tróia, *spywares*, *worms* e *bots*

- Mantenha todos os programas que você usa sempre atualizados.
- Instale todas as correções de segurança.
- Use antivírus, *firewall* pessoal e anti-*spyware*.

Mais detalhes em:
http://cartilha.cert.br/fraudes/
http://cartilha.cert.br/malware/

Navegue com segurança

- Mantenha seu navegador sempre atualizado.
- Desative *Java* e *ActiveX*. Use-os apenas se for estritamente necessário.
- Só habilite *JavaScript*, *cookies* e *pop-up windows* ao acessar *sites* confiáveis.

Cuide-se ao ler *e-mails*

- Mantenha o programa leitor de *e-mails* sempre atualizado.
- Desative a visualização de *e-mails* em HTML.
- Desative as opções de execução automática de arquivos anexados.
- Desative a execução de *JavaScript* e *Java*.

Mais detalhes em:
http://cartilha.cert.br/prevencao/

Proteja sua privacidade

- Use senhas com letras, números e símbolos.
- Nunca use como senha dados pessoais ou palavras de dicionários.
- Não coloque dados pessoais em páginas *Web*, *blogs* ou *sites* de redes de relacionamentos.

Use celulares e PDAs com segurança

- Habilite *bluetooth* só quando for utilizá-lo.
- Consulte o fabricante sobre atualizações para seu aparelho.
- Não aceite qualquer arquivo enviado para seu aparelho. Cheque a procedência.

Mais detalhes em:
http://cartilha.cert.br/privacidade/

Dicas para quem usa banda larga

- Use antivírus e *firewall* pessoal.
- Desligue o compartilhamento de recursos.
- Mantenha todos os programas que você usa sempre atualizados.
- Instale todas as correções de segurança.

Dicas para quem usa redes sem fio

- Use antivírus e *firewall* pessoal.
- Use WEP ou WPA sempre que possível.
- Use somente serviços com conexão segura.
- Implemente também as dicas para quem usa banda larga.

Mais detalhes em:
http://cartilha.cert.br/bandalarga/