SUZILEIDE RODRIGUES DE MELO

FERRAMENTAS DE SEGURANÇA: CRIMES OCORRIDOS NA REDE

Trabalho de conclusão de curso apresentado ao Curso de Ciência da Computação.

UNIVERSIDADE PRESIDENTE ANTÔNIO CARLOS

Orientador: Prof. José da Silva Filho

Co-orientadora: Profa. Débora Maria Gomes Messias Amaral.

BARBACENA
2004

SUZILEIDE RODRIGUES DE MELO

FERRAMENTAS DE SEGURANÇA: CRIMES OCORRIDOS NA REDE

Este trabalho de conclusão de curso foi julgado adequado à obtenção do grau de Licenciado em Ciência da Computação e aprovado em sua forma final pelo Curso de Ciência da Computação da Universidade Presidente Antônio Carlos.

Barbacena – MG, 16 de junho de 2004.

_____

Prof. José da Silva Filho- Orientador do Trabalho

_____

Prof. Débora Maria Gomes Messias Amaral - Membro da Banca Examinadora

_____

Prof. Gustavo Campos Menezes - Membro da Banca Examinadora

AGRADECIMENTOS

Agradeço primeiramente a Deus. A minha mãe por me apoiar nas decisões. Ao meu pai pelo esforço para eu poder estudar. Aos meus irmãos pelo incentivo. À minha filha, alma gêmea da minha alma, flor de luz da minha vida. Eu agradeço por existir. Agradeço ao orientador Silva Filho, professora Débora e a todos os professores que contribuíram para aumentar o meu conhecimento.

RESUMO

Este trabalho visa apresentar os principais crimes que envolvem segurança na grande rede. Mostra quem são as pessoas que cometem tais crimes, bem como os diferentes tipos de *hackers*. Também envolve um assunto muito discutido atualmente, que são os projetos de lei, que tratam da forma de punir os criminosos digitais. Depois serão apresentadas formas simples de se evitar alguns crimes e os prejuízos causados por invasões.

Finalmente como ponto central do tema apresentado, serão mostradas as principais ferramentas de proteção para maior segurança.

Palavras-chave: crimes, *hackers*, projeto de lei, ferramentas de segurança.

SUMÁRIO

FIGURAS

1 INTRODUÇÃO

O fenômeno da Internet no mundo moderno, tem se apresentado como uma ferramenta de grande importância em todos os segmentos da sociedade, pois uma das suas características fundamentais, reside na elevada gama de benefícios oferecidos às pessoas, dentre eles a celeridade na comunicação, bastando apenas que um computador esteja efetivamente conectado a um provedor de acesso, para que o internauta, possa atravessar as fronteiras entre as diferentes nações, com um simples comando, mergulhando definitivamente no *world wide web* .

Dentre as inúmeras vantagens inseridas no contexto da grande rede, evidentemente o lastro reside na quantidade de subsídios existentes e, nas possibilidades de acesso, que via de regra, constituem um verdadeiro paraíso de informações .

O que vale dizer, a elevada gama de conteúdos destinados a formação e composição das *homepages* e dos *websites* , que na essência, são decorrentes de muito trabalho e dedicação de seus autores e/ou idealizadores, constituem riquezas imensuráveis neste universo, que em tese, na maioria das ocasiões se encontram disponíveis livremente para os navegadores da *Internet*.

A Internet nada mais é que uma forma moderna de comunicação entre as pessoas, cuja construção estrutural reside única e exclusivamente, na universalidade de conteúdos, que em linhas gerais demandam mecanismos tecnológicos de segurança.

1.1 CONSIDERAÇÕES INICIAIS

A cada minuto, milhões de computadores interligam-se por meio de diversas ligações, fazendo circular bilhões e bilhões de informações que se traduzem em movimentação financeira, intercâmbio cultural e inter-relacionamento pessoal entre pessoas e instituições de todas as partes e das mais variadas culturas. Segundo Damásio (2001, p.99) esta progressiva dependência do computador, obviamente, está trazendo em seu rol uma série de reflexos no mundo jurídico, na medida em que vão surgindo questões ainda carentes de regulamentação. Com efeito, é sumamente impossível dissociar tal aproximação, considerando-se até mesmo a característica das terminologias específicas de que se utilizam os usuários do computador, cujo jargão envolve freqüentemente procedimentos e tecnologias de ponta, essenciais para o pleno equacionamento de diversas questões a serem disciplinadas ou regulamentadas. A velocidade com que a tecnologia tem avançado e se popularizado tem sido bem maior que a legislação preventiva, o que é preocupante.

Ora, como definir o que seja o "crime digital", ou o crime "via Internet" ? Que espécie de infração ocorre quando o uso pacífico do computador é desvirtuado, causar dano a outras pessoas físicas ou jurídicas, seja pela apropriação de dados remotos ou por sua utilização para obter vantagens? E como podemos evitar que estes tipos de crimes cheguem até nós? É o que veremos nos próximos capítulos.

1.2 OBJETIVO ESPECÍFICO

O objetivo deste trabalho é conscientizar os usuários participantes de computadores sobre os perigos a que estão expostos se não adotarem procedimentos de segurança .Neste trabalho encontram-se as principais ferramentas para evitar alguns ataques.

Primeiramente, será abordado sobre os principais tipos de *hackers*. Depois serão especificado os tipos de crimes, seguido da proposta de lei encaminhada no congresso que está em anexo 1. Em seguida, mostra algumas medidas simples que podem ser tomadas de forma a evitar alguns ataques no uso do computador.

Finalmente, serão tratados as principais ferramentas de segurança.

2 EXEMPLO PRÁTICO QUE ENVOLVE CRIME DIGITAL

Um dos casos de sabotagem de computadores, ocorridos no Pará, Maranhão, Piauí e em Goiás foi taxada como uma das mais ativas de *hackers* do mundo.

Segundo estatísticas (Mesquita, 2003), na revista INFO, o Comitê Gestor da Internet no Brasil, mostrou que no ano de 2003, as fraudes cresceram 275% em relação a 2002, com 273 casos registrados até setembro.

A Polícia Federal, através da operação "Cavalo de Tróia", prendeu 21 acusados de desviar R$ 30 milhões no ano passado pela Internet. Em um único dia uma empresa foi flagrada em cerca de R$350.000.

Os golpistas praticavam a ação criminosa mediante o envio de mensagens, aparentemente inofensivas e hilárias ,informando sobre como ganhar um beijo de um artista famoso(a), para os correios eletrônicos de clientes de instituições bancárias, as quais, ao serem abertas pelos destinatários propiciavam a imediata instalação dos programas fraudadores nos computadores dos usuários.

O objetivo era capturar informações pessoais e sigilosas, remetendo-as, em seguida, aos integrantes da quadrilha. De posse dessas informações, os fraudadores conseguiam transferir dinheiro dos clientes dos bancos para contas de "laranjas", que as emprestavam para a efetivação do ciclo fraudulento.

Essa operação de prisão foi a primeira vitória, mas vai ser muito mal vista lá fora, principalmente por causa da impunidade, já que não existem leis específicas para tratar de crimes virtuais.

O total de ataques, considerando-se outros tipos de operações de *hackers*, soma uma média de 4,8 mil casos mensais. Metade das ocorrências registradas são *worms*, os chamados códigos maliciosos que têm a capacidade de interferir no sistema, e 46%, scams, uma espécie de rastreamento das fragilidades do sistema. Ambas estratégias seriam ferramentas para a aplicação de fraudes, resultando em 43 golpes mensais no país. Uma das mais comuns é a clonagem de páginas de bancos, induzindo o usuário a digitar seus dados no site errado.

O mais grave, é que os números de ocorrências representam uma mínima parte do problema. A maior parte das instituições bancárias sequer registra ocorrência, pois não tem interesse em expor fragilidades, pois isso afeta a confiabilidade da instituição.

2.1 OS CRIMINOSOS DIGITAIS

Geralmente os criminosos são oportunistas, e os delitos praticados por agentes que, na maioria das vezes, têm a sua ocupação profissional afeta a área de informática.

O perfil do criminoso, baseado em pesquisa empírica (Spyman, 2002, pag.7), indica jovens, inteligentes, educados, com idade entre 16 e 32 anos, do sexo masculino, magros, caucasianos, audaciosos e aventureiros, com inteligência bem acima da média e movidos pelo desafio da superação do conhecimento, além do sentimento de anonimato, que bloqueia seus parâmetros de entendimento para avaliar sua conduta como ilegal, sempre alegando ignorância do crime e, simplesmente, "uma brincadeira".

Preferem ficção científica, música, xadrez, jogos de guerra e não gostam de esportes, sendo que suas condutas geralmente passam por três estágios: o desafio, o dinheiro extra, e, por fim, os altos gastos e o comércio ilegal.

2.2 O MUNDO *HACKER*

Durante a década de 70, segundo (Duarte, 2003) os *hackers* se ocuparam do desenvolvimento de compiladores (ferramentas que transformam os códigos de um programa, em linguagem de máquina, que será entendida pelos computadores), *debugs* (ferramentas que depuram os erros de um programa, tornando mais fácil a um programador achar os erros que ele cometeu ao escrever o código) e programas para a recém- criada área de informática. Nessa época também nasceu o movimento ideológico e ético "hacker". Computadores eram peças intangíveis para a maioria das pessoas, por isto o movimento ficou restrito a poucos estudantes sonhadores.

Outro ponto que deve ser discutido neste trabalho é também a existência de uma organização social no meio *hacker*. Originalmente, o *hacker* interage com os demais dentro de uma estrutura anarquista, sem liderança forte ou padrão rígido a seguir. Geralmente, associam-se em pequenos grupos, que trocam informações entre si, mas que agem isolados. Dentro deste grupo menor, há um líder, mas como organizador apenas, senão violaria as premissas de descentralização e antiautoritarismo.

A finalidade é sempre desbravar novos horizontes, mesmo que o objetivo principal seja a infiltração de novos valores para a sociedade *hacker*, a contra-cultura.

A contra-cultura cerca a cultura vigente através de uma rede especial de comunicação (hoje a internet), rituais, práticas comportamentais peculiares, formas de expressão e representação.

Bem, esta cultura que se formou durante os anos 60 e 70, teve o começo de seu auge na década de 80. Bem, na década de oitenta o PC, foi criado. A criação do PC se deu principalmente pela chegada do circuito. Dois dos *hackers* que tornaram isto possível foram Clive Sinclair e Steve Wozniac (um dos fundadores da Apple). Com isto o privilégio de universitárias e grandes empresas foi levado finalmente ao grande público.

Com isto a proliferação da informática pelo mundo se tornou extremamente crescente e assim, o número de pessoas que dominavam o computador também. Então, *hackers*

começaram a surgir de todos os cantos do mundo, já que o computador se tornava mais acessível a uma parcela muito maior de pessoas.

A década de 90 chegou, e com ela a popularização da informática, principalmente após o advento da internet, que trouxe muita coisa de nova para o mundo.

Esta grande rede de computadores foi que trouxe, a esta década uma mudança de paradigmas dos mais diversos tipos, e uma análise mais geral do conceito internet deve ser feita com mais profundidade.

Quem são os *hackers*? De acordo com documentos especializados nos mesmos, e em *newsgroups* especializados no assunto, nota-se que o *hacker* se caracteriza principalmente pela inquietação intelectual, e pelo desejo incansável de solucionar problemas. A genialidade destes informatas é o que assusta a sociedade. Com computadores nas mãos eles podem causar desde panes em sistemas, até entender profundamente o sistema e todo o funcionamento de algo em sua empresa.

Esta característica, é inerente ao termo "hacker" desde o seu início. A palavra "hacker" surgiu nos anos 50, no MIT (Massachussets Institute of Tecnology). O termo deriva da palavra *hack*, que era empregada para definir as atividades de alta tecnologia com os quais se ocupavam os estudantes do Comitê de Sinal e Poder. Ou seja, a palavra designava os criadores do que temos hoje em termos de tecnologia. Na computação, existem diversos tipos de *hackers.*

A seguir são apresentados os seguintes tipos de invasores:

Carders - Segundo Spyman, *carders* são aqueles que fazem compras com cartão de crédito alheio, ou seja, os *carders* tem uma grande facilidade para fazer compras na internet. "Podem, desde gerar o número aleatoriamente com programas específicos, ou então, roubar imensos bancos de dados de lojas virtuais e usá-los em seu prazer próprio”.

Hackers - “os *hackers* invadem em benefício próprio. Eles pegam tudo e não destroem nada. Portanto diferem dos *crackers*" (Spyman , 2002).

Furmankiewic e Figueiredo, fala que um *hacker* é uma pessoa intensamente interessada nos aspectos mais misteriosos e recônditos de qualquer sistema operacional de computador. Os *hackers* são mais freqüentemente programadores. Como tal, os *hackers* têm conhecimento avançado de sistemas operacionais e linguagens de programação. "Talvez eles descubram brechas dentro de sistemas e as razões para tais brechas". Os *hackers* constantemente buscam mais conhecimento, compartilham livremente o que eles descobriram, e nunca, jamais corrompem dados intencionalmente.

Crackers : Para (Furmankiewic e Figueiredo, 2001) um *cracker* é alguém que domina ou de outro modo viola a integridade de um sistema de máquinas remotas com intenção maliciosa. Tenho ganho acesso não-autorizado, os *crackers* destroem dados vitais, negam serviço a usuários legítimos ou causam problemas para seus alvos. Os *crackers* podem ser facilmente identificados porque suas ações são maliciosas.

> Os crackers são como os hackers, mas gostam de ver a destruição; Eles invadem e destoem só para ver o caos. São os ladrões da internet. Eles roubam dinheiro, roubam informações . Eles apagam todo o sistema deixando sempre sua marca registrada.(Spyman, 2002).

Phreackers : Conforme (Spyman, 2002,p.15) os *preackers* são os piratas da telefonia, eles fazem de tudo o que é relativo aos telefones convencionais ou celulares. São poucos, pois, é necessário um alto conhecimento tanto de computação quanto de telefonia.

Lammers : Segundo (Spyman, 2002, p.17) são aqueles *hackers* que estão adentrando na filosofia e normalmente não conhecem muito sobre o que estão fazendo. Utiliza-se de ferramentas pré-fabricadas, ou seja, não implementam (fabricam), suas próprias soluções para problemas seus e por exemplo, de invasão de algum sistema.

Dando continuidade, após falar dos criminosos, veremos no próximo capítulo alguns tipos de crimes que ocorrem na rede.

3 TIPOS DE CRIMES NA REDE

Existem vários tipos de crimes pela Internet, que exploram falhas de software, hardware e que burlam esquemas de segurança com falhas. Os mais comuns são:

a)Cavalo de Tróia;

b) Vírus e Worms;

c) Abuso quanto aos cartões de crédito;

d)Spoof;

e)Sniffer;

f)Engenharia Social;

a) O que é um Cavalo de Tróia?

Segundo (Caruso & Steffen, 1999, p.130) os Cavalos de Tróia apresentam mais dificuldades em definição do que a princípio possa aparecer. Enquanto vírus são definidos

principalmente por sua capacidade de replicar, os cavalos de tróia são definidos principalmente por seu *payload (*carga, dano causado) ou, para utilizar um termo menos emotivo, sua função. A replicação é um valor absoluto. Ou um programa replica, ou não o faz. O dano e a intenção entretanto, não são absolutos, pelo menos em termos de função de programa. O primeiro indício para sua natureza reside na história antiga e na mitologia clássica.

> Um programa de cavalo de tróia pode ser um programa que faz algo útil ou algo meramente interessante. Ele sempre faz algo inesperado, como roubar senhas ou copiar arquivos sem seu conhecimento. (autor anônimo, 2001).

Que nível de risco os cavalos de tróia apresentam?

Os cavalos de tróia podem representar um nível de risco moderado a sério, principalmente porque:

No livro Segurança Máxima (autor anônimo, 2001) diz que novos cavalos de tróia são difíceis de ser dectados utilizando deteccção heurística. Não há nenhum teste absoluto para o código determinar se é (ou não é) um cavalo de Tróia porque a intenção do autor as expectativas do usuário não geralmente suscetíveis a uma análise automatizada.

Na maioria dos casos, os cavalos de Tróia estão localizados em binários, que permanecem amplamente na forma não - legível para os seres humanos. Entretanto, o fato de o código ser amplamente estático torna os cavalo de Tróia pelo menos tão suscetíveis à detecçãode “algo conhecido” quanto os vírus. Em outras palavras, quando um programa malicioso conhecido é identificado, ele pode ser detectado por software atualizado com uma string de pesquisa apropriada. Os cavalos de Tróia se espalham pela ação de serem copiados por um invasor ou uma vítima socialmente motivada a executar os desejos do invasor, não por autocópia. Assim, normalmente não é factível o invasor utilizar técnicas como polimorfismo para reduzir a chance de detecção.

Contudo, os cavalos de Tróia não-detectados podem conduzir ao comprometimento total do sistema .Um cavalo de Tróia pode ficar num lugar durante semanas ou até meses antes de ser descoberto. Nesse tempo, um *cracker* com nível técnico pode alterar o sistema

inteiro para servir às suas necessidades. Mesmo quando um cavalo de Tróia é descoberto, muitas brechas ocultas podem ser deixadas para trás quando ele for removido.

b) Vírus e *Worms*

O que é um *worm* de computador ?

A replicação também é a característica de definição de um *worm* e algumas autoridades (incluindo Fred Cohen, o "pai" da virologia de computador) consideram os *worm* como um subconjunto dos vírus. Entretanto, os *worm* apresentam problemas particulares de definição. Uma definição viável distingue entre *worm* e vírus em termos de anexo. Enquanto um vírus em algum sentido se "anexa" a um programa legítimo, um *worm* copia a si próprio através de redes e/ ou sistemas sem anexação. Pode ser dito que um *worm* infecta o ambiente (um sistema operacional ou sistema de correio, por exemplo), em vez de objetos específicos infectáveis, como arquivos.

Alguns observadores utilizaram o termo *worm* para se referirem ao *malware (*MALcious *softWARE)* auto- replicante que se espalha através de redes. Isso não chega realmente a ser uma distinção significativa porque muitos vírus podem viajar entre máquinas em uma rede local, por exemplo , sem estar "cientes" de que um volume-alvo não está na mesma máquina. Isso não quer dizer que naturalmente , os vírus nunca sejam "cientes" da rede.

Os vírus de computador talvez sejam as ameaças de segurança mais bem conhecidas. Todos os vírus acarretam necessariamente um certo grau de dano, mas seu impacto, com algumas exceções muito importantes, é principalmente social.

Cada vírus causa uma negação(normalmente limitada) de serviço porque todos roubam espaço em disco, memória e/ou ciclos de *clock* (tempo de processador). Alguns causam danos não intencionais (acidentais) em alguns sistemas. Outros causam dano intencional aos arquivos e sistemas de arquivos e alguns podem tornar hardware efetivamente

inutilizável invalidando o *firmware* (o CIH por exemplo). Entretanto, alguns dos vírus mais bem - sucedidos (em termos de sobrevivência) alcançam longevidade por força do fato de que eles não fazem nada além de replicar e, portanto não são notáveis. Entretanto, alguns vírus causam dano sério aos dados pela lenta e insidiosa corrupção e outros continuam a sobreviver apesar de seu alto perfil de dano.

Tipos de Vírus de Computador

Conforme autor anônimo do livro Segurança Máxima, traduzido em (Edson Furmankiewic e Sandra Figueiredo, 2001, p. 67) os tipos de vírus existentes são:

1 - Vírus de Arquivos

Esse tipo de vírus agrega-se a arquivos executáveis (normalmente extensão COM e EXE), embora possam também infectar arquivos que sejam requisitados para a execução de algum programa, como os arquivos de extensão SYS, DLL, PRG, OVL, BIN, DRV (esta última é a extensão dos arquivos que controlam o funcionamento do mouse, do CD-ROM, da impressora, do scanner ...).

Arquivo de extensão SCR, que é a extensão dos *screen saver* (protetores de tela), também podem ser infectado, pois estes arquivos são, na verdade, executáveis comuns, salvos com outra extensão. Isto é feito para que o Windows possa reconhecer automaticamente esse tipo de arquivo.

Neste tipo de virose, programas limpos normalmente se infectam quando são executados com o vírus na memória em um computador corrompido.

Os vírus de arquivos dividem-se em duas classes, os de Ação Direta e os Residentes.

2 - Vírus de Ação Direta

Essa classe de vírus seleciona um ou mais programas para infectar cada vez que o programa que o contém é executado. Ou seja, toda vez que o arquivo infectado for executado, novos programas são contaminados, mesmo não sendo usados.

Como isto acontece?

Uma vez contaminado um arquivo, o programa (vírus) faz uma procura no winchester por arquivos executáveis. Cada arquivo encontrado é colocado em uma lista, após, na nova execução do arquivo contaminado, o vírus seleciona aleatoriamente um ou mais arquivos, e esses também serão contaminados.

3 - Vírus Residentes

Essa classe esconde-se em algum lugar na memória na primeira vez que um programa infectado é executado. Da memória do computador, passa a infectar os demais programas que forem executados, ampliando progressivamente as frentes de contaminação.

Um vírus também pode ser ativado a partir de eventos ou condições pré-determinadas pelo criador, como data (como o Sexta-feira 13, por exemplo), número de vezes que um programa é rodado, um comando específico, etc.

4 - Vírus de Sistema ou Vírus de Boot

Infectam códigos executáveis localizados nas áreas de sistema do disco. Todo drive físico, seja disco rígido, disquete ou cd-rom, contém um setor de boot. Esse setor de boot contém informações relacionadas à formatação do disco, dos diretórios e dos arquivos armazenados nele.

Além disso pode conter um pequeno programa chamado de programa de boot (responsável pela inicialização do sistema), que executa a "carga" dos arquivos do sistema operacional (o DOS, por exemplo). Contudo, como todos os discos possuem área de boot, o vírus pode esconder-se em qualquer disco ou disquete, mesmo que ele não seja de inicialização ou de sistema (de boot).

Um comportamento comum entre os vírus de boot que empregam técnicas mais avançadas invisibilidade é exibir os arquivos de boot originais sempre que for feita uma solicitação de leitura do sector 1 da *track* 0. Enquanto o vírus estiver residente na memória, ele redireciona todas as solicitações de leitura desse setor para o local onde o conteúdo original está armazenado. Essa técnica engana as versões mais antigas de alguns antivírus.

Alguns vírus, ainda mais avançados, chegam a marcar o setor onde os arquivos de boot originais foram colocados, como sendo um setor ilegível, para que os usuários não possam descobrir o setor de boot em um lugar considerado incomum.

5 - Vírus Múltiplos

São aqueles que visam tanto os arquivos de programas comuns como os setores de Boot do DOS e / ou MBR., ou seja, correspondem a combinação dos dois tipos descritos acima. Tais vírus são relativamente raros, mas o número de casos aumenta constantemente. Esse tipo de vírus é extremamente poderoso, pois pode agir tanto no setor de boot infectando arquivos assim que eles forem usados, como pode agir como um vírus de ação direta, infectando arquivos sem que eles sejam executados.

6 - Vírus de Macro

É a categoria de vírus mais recente, ocorreu pela primeira vez em 1995, quando aconteceu o ataque do vírus CONCEPT, que se esconde em macros do processador de textos MicroSoft WORD.

Esse tipo de vírus se dissemina e age de forma diferente das citadas acima, sua disseminação foi rápida especialmente em função da popularidade do editor de textos Word (embora também encontramos o vírus na planilha eletrônica Excel, da própria MicroSoft).

Eles contaminam planilhas e documentos (extensões XLS e DOC). São feitos com a própria linguagem de programação do Word. Entretanto a tendência é de que eles sejam cada vez mais eficazes, devido ao fato da possibilidade do uso da linguagem Visual Basic, da própria Microsoft, para programar macros do Word.

O vírus macro é adquirido quando se abre um arquivo contaminado. Ele se autocopia para o modelo global do aplicativo, e, a partir daí, se propaga para todos os documentos que forem abertos. Outra capacidade inédita deste tipo de vírus é a sua disseminação multiplataforma, infectando mais de um tipo de sistema (Windows e Mac, por exemplo).

7 - Vírus Stealth ou Furtivo

Por volta de 1990 surgiu o primeiro vírus furtivo. Esse tipo de vírus utiliza técnicas de dissimulação para que sua presença não seja detectada nem pelos antivírus nem pelos usuários. Por exemplo se o vírus detectar a presença de um antivírus na memória, ele não ficará na atividade. Interferirá em comandos como Dir e o Chkdsk do DOS, apresentando os tamanhos originais dos arquivos infectados, fazendo com que tudo pareça normal. Também efetuam a desinfecção de arquivos no momento em que eles forem executados, caso haja um antivírus em ação; com esta atitude não haverá detecção e conseqüente alarme.

8 - Vírus Encripitados

Um dos mais recentes vírus. Os encripitados são vírus que, por estarem codificados dificultam a ação de qualquer antivírus. Felizmente, esses arquivos não são fáceis de criar e nem muito populares.

9 - Vírus mutantes ou polimórficos

Têm a capacidade de gerar réplicas de si mesmo utilizando-se de chaves de encripitação diversas, fazendo que as cópias finais possuam formas diferentes. A polimorfia visa dificultar a detecção de utilitários antivírus, já que as cópias não podem ser detectadas a partir de uma única referência do vírus. Tal referência normalmente é um pedaço do código virótico, que no caso dos vírus polimórficos varia de cópia para cópia.

Vejam alguns exemplos de janelas geradas por vírus

Figura 1- Esta é uma janela com vírus.
Fonte: http://www.avertlabs.com/public/datafiles/valerts/vinfo/melissa.asp, 2004.

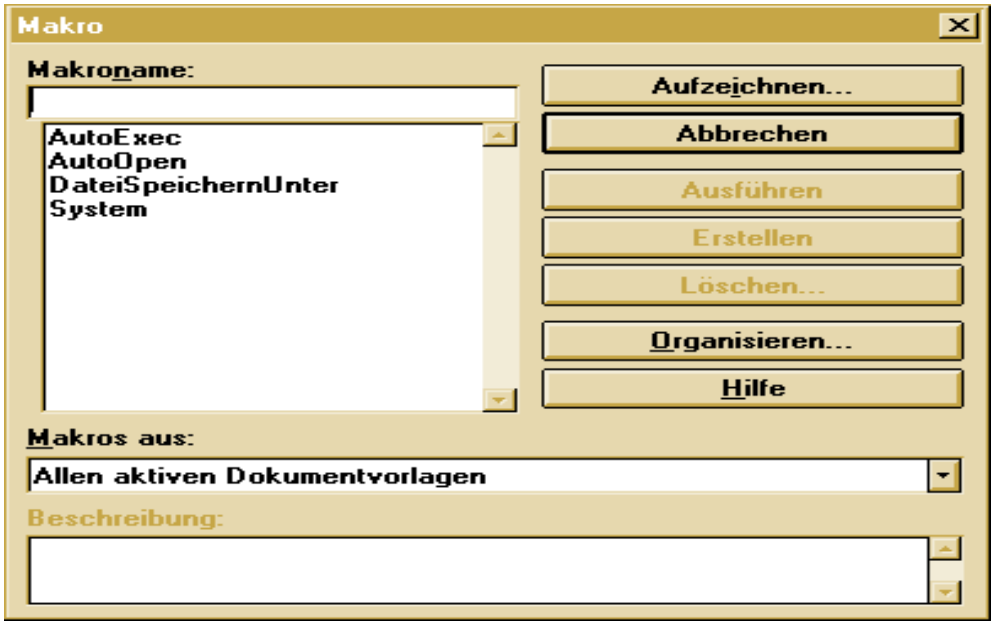

Figura 2- Esta é outra janela infectada por vírus.
Fonte: http://www.nai.com.br/about/news/melissa.htm, 2004.

c) abuso quanto aos cartões de crédito:

Atualmente estão sendo desenvolvidos muitos mecanismos visando a constituição e consolidação do " dinheiro eletrônico ", tais como, o *e-cash* e os bancos via Internet *Internet banking*, ampliando a capacidade de utilização de moeda pelos caminhos da grande rede.

(Scambray, 2002, p. 70), diz em seu livro que é importante frisar que, pelo fato de os cartões oferecerem uma significativa proteção para seus usuários, fazem com que sua popularidade seja bem maior do que a dos outros mecanismos. Outro fator seria a facilidade de funcionamento. Ocorre que, justamente devido à simplicidade do mecanismo de utilização, os cartões de crédito são suscetíveis de um grande número de abusos e fraudes.

Uma vez preenchida a autorização de débito pela rede, o titular do cartão não tem nenhum meio de determinar com quem está fazendo negócio. A partir daí começam os abusos. O interessante é que a fraude não se limita ao comerciante. Pelo fato de que a Internet, até o presente momento, não é muito segura, as transmissões podem ser interceptadas, e os dados do cartão de crédito, conseqüentemente, também. Toda página carregada ou transmitida fica armazenada temporariamente dentro do sistema, e, a partir daí, o provedor tem acesso a todo o conteúdo.

Pelo fato de não existir regulamentação específica, em termos, desses serviços no Brasil, a não ser vários projetos de lei, é de se afirmar em última análise, que qualquer pessoa responsável por um provedor de acesso tem condições de utilizar tais informações para fins ilícitos.

Também é correto afirmar que tanto os provedores que transmitem quanto os que recebem informações têm acesso aos dados de cartão de crédito e podem utilizá-los ilegalmente. Porém, os provedores não são os únicos capazes de interceptar tais informações, sendo que, qualquer pessoa que tenha as ferramentas e o conhecimento necessário para tanto, pode fazê-lo.

As empresas de cartão de crédito, devido à fragilidade dos mecanismos de segurança na Internet, vêm aconselhando, em alguns casos, seus clientes a não fornecerem seus dados de cartão de crédito por meio da rede. Para evitar tais problemas, têm investido no

desenvolvimento de programas que implementem a segurança, como a tecnologia da criptografia ou o mecanismo SET (*secure electronic transaction*) que funciona como uma máscara para os dados enviados pela Internet. A segurança dessas transações, além de ser de fundamental importância para o crescimento do comércio eletrônico, poderá tornar as transações na grande rede muito mais seguras.

d) *Spoof*

Um assunto muito pouco explorado segundo (Spyman, 2002, p.89), atualmente é o *Spoof*. Esta é uma técnica que consiste em assumir a identidade de um outro computador numa rede, visando estabelecer o controle de uma máquina que confie no DNS/IP de outra máquina.

Tornando possível estabelecer conexão sem utilização de senha.

Segundo (Scambray, 2002, p. 82), o *Spoof* é uma técnica de ataque extremamente complexa que consiste numa, diríamos falsidade ideológica", de DNS/IP.

É mais ou menos assim: o Servidor1 tem um acesso confiável no Servidor2, isto é, nenhuma senha é necessária para os dois se falarem (isso nos serviços rexec, rlogin, rsh).

Acho que fica mais fácil com esse esquema:

Acesso confiável

Servidor1----------Servidor2

Figura 3 – Conexão de dois servidores.
Fonte: Segurança Máxima, 2001, p.256.

Portanto, o *cracker* irá dizer ao Servidor2 que o seu DNS/IP é o Servidor1, tornando, assim, possível a conexão.

O ataque por *Spoof* é um ataque ao qual estão sujeitos todos os SO (Sistemas Operacionais). Os únicos SO que podem ser atacados são aqueles que rodam uma versão completa do TCP/IP, isto é, que possuem todos os serviços funcionando (não todos, mas aqueles que rodam um pacote TCP/IP completo).

e) *Sniffers*

De acordo com o livro Segurança Máxima (autor anônimo, 2001), cujo autor anônimo, os ataques de *sniffers* são comuns, particularmente na Internet. Um sniffer bem colocado pode capturar não só algumas, mas milhares de senhas.

Os *sniffers* representam um alto nível de risco porque:

- podem capturar nomes de conta e senhas.
- Podem capturar informações confidenciais de proprietário.
- Podem ser utilizados para abrir brechas na segurança de redes vizinhas ou ganhar acessos de alto nível.

Os *sniffers* capturam todos os pacotes na rede, mas na prática, um invasor tem de ser altamente seletivo. Um ataque de *sniffers* não é tão fácil quanto parece, segundo George Kurtz. Ele requer algum conhecimento de rede. Simplesmente configurar um *sniffer* e deixá-lo trabalhando levará a problemas porque mesmo uma rede de cinco estações transmite milhares de pacotes por hora. Dentro de um breve tempo, o arquivo de saída de um *sniffer* pode facilmente encher uma unidade de disco rígido (se capturar todos os pacotes).

Um *sniffer* pode ser encontrado em quase todo lugar. Há alguns pontos estratégicos que um cracker talvez prefira. Um desses pontos está em qualquer lugar adjacente a uma máquina ou rede que recebe muitas senhas. Alguns sistemas operacionais agora empregam criptografia no nível de pacote e, portanto, mesmo se um ataque de *sniffer* conseguir obter dados valiosos, esses dados estão criptografados.

f) Engenharia Social

Engenharia social é o termo utilizado para a obtenção de informações importantes de uma empresa, através de seus usuários e colaboradores.

Segundo (Figueiredo, 2003), essas informações podem ser obtidas pela ingenuidade ou confiança. Os ataques desta natureza podem ser realizados através de telefonemas, envio de mensagens por correio eletrônico, salas de bate-papo e pasmem, até mesmo pessoalmente.

Já foram identificados conforme Freyre (2002) casos em que alguém, se passando por um funcionário do suporte técnico de um provedor de acesso Internet, telefonou para um usuário informando que a conexão estava com algum tipo de problema e que para consertar necessitava da sua senha. O usuário, na sua ingenuidade, fornece a senha e depois vai ver no extrato mensal do provedor que utilizou muito mais recursos do que realmente o tinha feito. Outra técnica muito utilizada na Internet são os sites anônimos que prometem horas grátis de acesso, bastando você fornecer a eles seu nome de usuário e senha. Na verdade, trata-se de um ataque de engenharia social, e eles utilizarão estas informações para conseguir horas extras sim, mas para eles.

Com o crescente avanço da tecnologia, as empresas estão dedicando uma boa parte do tempo para resolver os problemas técnicos de segurança. São investidos muitos recursos para garantir a segurança de servidores e aplicações, e devido a esta consciência que hoje está bem evoluída, as técnicas de ataques têm se aprimorado. Tentar invadir um site ou uma empresa torna-se um desafio ainda maior, e nesta situação, a engenharia social vem tendo destaque e passa a ser a nova moda.

3.1 Os crimes digitais na legislação atual

A consolidação da Internet como meio de comunicação, trabalho, lazer, negócios aponta para uma inovação tecnológica sem volta. Nasce também com ela, uma sociedade virtual que não se conforma com as normas do mundo físico. Essa mesma sociedade não se conforma com os limites jurisdicionais dos Estados, ou seja, legislações locais que não se mostram suficientes para a resolução do problema dos crimes de informática. O direito positivo é posto em xeque, e princípios brasileiros de aplicação de leis como o da territorialidade são questionados nessa nova ordem mundial emergente. Não resolvem o problema, mas com certeza amenizam as perdas e danos, as legislações de crime de informática, ainda que ineficazes a todos os Estados do mundo.

No Brasil encontra-se em tramitação no Congresso Nacional o projeto de lei nº 84/ 1999 que trata da tipificação dos crimes digitais (conforme anexo1).Neste projeto encontram-

se elencados os seguintes crimes: acesso indevido ou, não autorizado, alteração de senha ou meio e acesso a programa de computador ou dados, obtenção, manutenção ou fornecimento indevido, ou não autorizado, de dado ou instrução de computador, dano a dado ou programa de computador, violação de segredo armazenado em computador, meio magnético, de natureza magnética, óptica ou similar.

A Internet necessita da elaboração de normas específicas em virtude de sua natureza global, função que está sendo assumida, não unicamente, mas em grande parte pelo Direito da Informática. Os juristas e representantes dos Estados de todo o mundo devem se reunir para discutir tal questão, que é da maior importância contemporaneamente, estabelecendo normas globais e comum a todos os povos. Ao fazer isso, deve-se ainda ter o seguinte cuidado de não transformar a Internet em um mundo virtual privado, com uma bandeira e uma nacionalidade, pois como observado, a maior característica da rede mundial de computadores é o livre acesso e a não vinculação com qualquer entidade ou Estado, não possuindo dono a rede.

Enquanto a grande integração mundial de juristas e autoridade acerca do tema não se concretiza em leis e normas de eficácia global, não é concebível que os usuários da Internet fiquem vulneráveis a delitos praticados por *hackers* ou criminosos do mundo real, que usam o computador como arma de crime. Para a prevenção contra qualquer tipo de crime de informática, a informação apresenta-se como pressuposto para tal.

A apuração de responsabilidades nos crimes de Internet é tarefa primordialmente das autoridades e polícias judiciárias, que para isso devem equipar e preparar setores e pessoal especializados na investigação e apuração dessa modalidade criminosa tão peculiar. Conhecimento, capacitação e a formação de expertos são estratégias vitais para a formação de uma unidade capaz de rastrear, identificar e imputar a responsabilidade ao agente do crime.

Paralelamente a Internet cresce também uma modalidade de crimes que ainda são recentes e desconhecidos em muitos casos, razão pela qual faz com que a impunidade ainda seja, hoje, a regra para o autor da prática delituosa. Acreditamos, ainda, que com a experiência e maturidade no desenvolvimento de novas idéias e sistemas preventivos de crimes de informática, maior se tornará a segurança na rede. Porém, como radiar maior dessa

segurança, a cooperação e trabalho em conjunto de juristas de todo o mundo com especialistas na Informática será essencial para o alcance desse objetivo.

4 OS PREJUÍZOS

Encontrados em (Rezende, 2003) diz que a Informática é o centro da empresa. Qualquer pequeno problema no(s) servidor(es) corporativo(s) ou em algum servidor departamental pode paralisar vários ou mesmo todos os departamentos da empresa. Quanto maior o grau de integração dos sistemas, quanto maior o volume e a complexidade dos negócios, maior será a dependência em relação à Informática.

Quando ocorre algum problema que provoque uma paralisação, os prejuízos menos importantes são percebidos imediatamente. Outros, normalmente os maiores, somente serão percebidos posteriormente, e será muito difícil, ou mesmo impossível, repará-los.

Problemas de segurança com graus de severidade insignificante e pequeno somente causam prejuízos imediatos, tais como:

- Paralisação das atividades normais da empresa;
- Danos materiais, variáveis conforme o problema ocorrido;

- Sobrecarga na estrutura da empresa, que deve mobilizar os seus recursos, normalmente exíguo, para a tentativa de recuperação dos problemas decorrentes do erro;

- Atritos internos em função da responsabilização pelo erro;

Normalmente problemas com grau de severidade médio causam poucos prejuízos a médios e longos prazos, que são:

- Desvio nos objetivos da empresa;
- Perda de mercado;
- Perda de imagem ;
- Perda de credibilidade;
- Desânimo e perda de funcionários
- Atritos internos extremamente sérios e atritos externos em função da responsabilização pelo erro

Problemas com grau de severidade grande e catastrófico certamente causam os mesmos prejuízos já citados, a médio e longo prazo, podendo causar o encerramento das atividades da empresa e pendências com a Justiça para seus diretores e funcionários.

4.1 MEDIDAS SIMPLES PARA EVITAR SURPRESAS DESAGRADÁVEIS

Algumas medidas para evitar alguns transtornos, conforme (Duarte, 2003):

Só entre em páginas de instituições financeiras digitando o nome do site. O acesso por meio de links não é recomendado porque pode conduzir o usuário a páginas clonadas de bancos, que "roubam" dados pessoais, como números de conta e cartão de crédito. Ao efetuar transações bancárias via Internet, observe atentamente o site. Páginas falsas tendem a apresentar pequenas variações no nome da página, como www.nomedobanco2003.com.br, em

vez de www.nomedobanco.com.br.

Clique duas vezes sobre o cadeado que aparece no canto direito inferior da tela para conferir se o certificado da página está atualizado. Deve aparecer uma janela contendo o número do registro e a sua validade.

Bancos não costumam enviar e-mails. Em caso de suspeita, ligue para o banco para confirmar se a tal promoção ou pedido de senha adicional são verdadeiros.

Suspeite de e-mails que dão ordens a ser seguidas e oferecem vantagens incomuns. Tenha cautela especial com pedido de cadastros.

Passe sempre um antivírus antes de abrir um anexo. Nem sempre uma terminação ".doc" corresponde a um arquivo de texto. Pode ser um disfarce.

A tentativa de golpes deve aumentar no fim do ano, pelo maior volume de propagandas e cartões virtuais circulando na Internet. Fique atento ao abrir um cartão, já que é preciso clicar em um link para fazê-lo. Se, ao fazer isso, perceber um arquivo com extensão ".exe" se instalando em sua máquina, interrompa a operação.

Mantenha programas em versões atualizadas e passe o antivírus semanalmente no computador. No windows, há uma janela de atualização do sistema no menu iniciar (atualizar versão). O procedimento demora cerca de cinco minutos.

Antes de usar o cartão na Internet, preste atenção se digitou o nome do site corretamente. Às vezes surgem clones de páginas de bancos ou lojas com nomes parecidos (por exemplo, sem o ".br" do final dos endereços brasileiros). A intenção dessas empresas é capturar a senha bancária dos distraídos.

Ao comprar, prefira páginas de empresas que tenham telefone para contato e endereço conhecido. Se desconfiar, ligue antes para ver se elas existem. Ou consulte o órgão de defesa do consumidor de seu Estado.

Ao acessar a página que pede o número de seu cartão, verifique se surge na moldura de seu navegador o desenho de um cadeado (no caso do Internet Explorer) ou de uma chave (no

Netscape). Esses ícones significam que você está num site seguro, com linguagem criptografada (em código).

Para se certificar, clique no ícone do cadeado ou da chave. Deve aparecer o nome da loja, da empresa responsável pela tecnologia de segurança do site e outras informações técnicas.

Alguns sites costumam guardar o número de seu cartão num banco de dados para evitar que você tenha de digitá-lo novamente numa próxima compra. Na ocasião dessa nova transação eles perguntam algo do tipo: "Confirme se o número do cartão para débito é...". Nesse caso, certifique-se de que o site só mostra os últimos algarismos, e não todos, o que facilita a ação de *hackers* e invasores.

Uma medida básica de segurança que envolve *Spoof* e que resolve cerca de 85% dos casos segundo (Spyman, 2002, p. 104), é a não utilização de serviços que usam autenticação por IP. Os outros 15% podem ser prevenidos pela monitoração da sua rede utilizando programas especiais como TCP *Wrappers* (foi lançado pela empresa de auditoria de redes de Módulo).

Para minimizar o problema de engenharia social, pode seguir os procedimentos conforme (Freyre, 2002):

- Estabeleça uma política de controle de acesso físico na empresa;
- Classifique as informações de sua empresa, onde cada colaborador saiba o que pode ser divulgado e o que não pode;
- Desconfie das ofertas mirabolantes que circulam pela Internet;
- Ao receber um telefonema de uma pessoa estranha, que conhece todos os seus dados e lhe transmite confiança, retenha desta pessoa o máximo de informações possíveis.

5 AMEAÇAS E ATAQUES

Algumas das principais ameaças segundo Lima (2002), as redes de computadores são:

- Destruição de informação ou de outros recursos.

- Modificação ou deturpação da informação.

- Roubo, remoção ou perda da informação ou de outros recursos.

- Revelação de informações.

- Interrupção de Serviços.

As ameaças podem ser acidentais, ou intencionais, podendo ser ambas ativas ou passivas.

Ameaças acidentais são as que não estão associadas à intenção premeditada.

Exemplo:

- Descuidos operacionais;

- *Bugs* de Software e Hardware;

- Ameaças intencionais são as que estão associadas à intenção premeditada;

Exemplos:

Observação de dados com ferramentas simples de monitoramento da redes.

Alteração de dados, baseados no conhecimento do sistema.

Ameaças Passivas são as que, quando realizadas não resultam em qualquer modificação nas informações contidas em um sistema.

Ameaças Ativas envolvem alterações de informações contidas no sistema, ou modificações em seu estado ou operação.

Os principais ataques que podem ocorrer em um ambiente de processamento e comunicação de dados são os seguintes:

Personificação: uma entidade faz-se passar por outra. Uma entidade que possui poucos privilégios pode fingir ser outra, para obter privilégios.

Replay: Uma mensagem, ou parte dela, é interceptada, e posteriormente transmitida para produzir um efeito não autorizado.

Modificação: O conteúdo de uma mensagem é alterado implicando em efeitos não autorizados sem que o sistema consiga identificar a alteração.

Exemplo: Alteração da mensagem "Aumentar o salário do José para R$300,00" para "Aumentar o salário do José para R$3000,00"

Recusa ou Impedimento de Serviço: ocorre quando uma entidade não executa sua função apropriadamente ou atua de forma a impedir que outras entidades executem suas funções.

Exemplo: Geração de mensagens com o intuito de atrapalhar o funcionamento de algoritmos de roteamento.

Ataques Internos: Ocorrem quando usuário legítimos comportam-se de modo não autorizado ou não esperado.

Armadilhas (*Trapdoor*): ocorre quando uma entidade do sistema é alterada para produzir efeitos não autorizados em resposta a um comando (emitido pela entidade que está atacando o sistema) ou a um evento, ou seqüência de eventos, premeditado.

Exemplo: A modificação do processo de autenticação de usuários para dispensar a senha, em resposta a uma combinação de teclas específicas.

6 FERRAMENTAS PARA SEGURANÇA

Esta parte da monografia apresenta conceitos de segurança de computadores, onde são abordados temas relacionados às senhas, certificados digitais, antivirus, *firewall*, criptografia.

Todas as grandes empresas (e as pequenas também) devem tomar todas as medidas possíveis no sentido de proteger os sistemas de suas redes de computadores.

Isto porque, como foi visto, os ataques de *hackers* tendem a se multiplicar.

6.1.1 FIREWALL

Segundo (Furmankiewic e Figueiredo, 2001, p.78) em redes de computadores, *firewall* são barreiras interpostas entre a rede privada e a rede externa com a finalidade de evitar intrusos (ataques); ou seja, são mecanismos (dispositivos) de segurança que protegem os recursos de hardware e software da empresa dos perigos (ameaças) aos quais o sistema está

exposto. Estes mecanismos de segurança são baseados em hardware e software e seguem a política de segurança estabelecida pela empresa.

Firewall é um sistema ou um grupo de sistemas que garante uma política de controle de acesso entre duas redes (normalmente a Internet e uma rede local). Em princípio *firewalls* podem ser vistos como um par de mecanismos: um que existe para bloquear o tráfego e outro que existe para permitir o tráfego. Alguns *firewalls* dão maior ênfase ao bloqueio de tráfego, enquanto outros enfatizam a permissão do tráfego, o importante é configurar o *firewall* de acordo com a política de segurança da organização que o utiliza, estabelecendo o tipo de acesso que deve ser permitido ou negado

O conceito de *firewall* está ligado às paredes interna*s* de uma construção que impedem que o fogo se propague de uma sala para outra da construção mas em termos práticos está mais para antigos castelos medievais. Fundamentalmente, uma *firewall* tem três objetivos principais:

- Restringir o acesso de pessoas a ambientes controlados.
- Impedir que eventuais atacantes cheguem muito perto das defesas internas.
- Impedir que as pessoas passem por um ponto controlado sem que tenham autorização para tanto.

Normalmente uma *firewall* é instalada no ponto de interligação de uma rede interna com a Internet. Todo o tráfego, nos dois sentidos, tem de passar por esse ponto e, dessa forma, atender aos requisitos da política de segurança da instalação. Uma "firewall" funciona como separador de ambientes e, ao mesmo tempo, como controlador de acesso e analisador de tráfego.

Para (Caruso & Steffen, 2002, p. 172) uma *firewall* é composta por diversos dispositivos, variando em função de cada ambiente , e implica uma complexidade razoável, o que pode significar um profisional de alto salário. Além do custo, uma *firewall* tem outras desvantagens; entretanto, ainda é o meio mais efetivo de proteger uma instalação.

Abaixo na figura 4 explica o funcionamento de um *firewall* em um laboratório de pesquisa.

Figura 4- Proteção de acesso com *firewall.*
Fonte: livro segurança em informática e de informação, p.77.

Firewalls são classificados em três categorias principais : filtros de pacotes, gateways de aplicação e gateways de circuitos.

Os filtros de pacotes utilizam endereços IP de origem e de destino, e portas UDP e TCP para tomar decisões de controle de acesso. O administrador elabora uma lista de máquinas e serviços que estão autorizados a transmitir datagramas nos possíveis sentidos de transmissão (entrado ou saindo da rede interna), que é então usada para filtrar os datagramas IP que tentam atravessar o *firewall*. Um exemplo de política de filtragem de pacotes seria permitir o tráfego de datagramas carregando mensagens de SMTP e DNS nas duas direções, tráfego Telnet só para pacotes saindo da rede interna e impedir todos os outros tipos de tráfego.

A filtragem de pacotes é vulnerável a adulteração de endereços IP e não fornece uma granularidade muito fina de controle de acesso, já que o acesso é controlado com base nas máquinas de origem e de destino dos datagramas.

Na segunda categoria de *firewalls*, um gateway de circuitos atua como intermediário de conexões TCP, funcionando como um TCP modificado. Para transmitir dados, o usuário origem conecta-se a uma porta TCP no gateway, que por sua vez, conecta-se ao usuário destino usando outra conexão TCP. Para que seja estabelecido um circuito o usuário de origem deve fazer uma solicitação para o gateway no *firewall*, passando como parâmetros a máquina e o serviço de destino. O gateway então estabelece ou não o circuito, note que um mecanismo de autenticação pode ser implementado neste protocolo.

Firewalls onde os gateways atuam em nível de aplicação utilizam implementações especiais das aplicações desenvolvidas especificamente para funcionar de forma segura. Devido a grande flexibilidade desta abordagem ela é a que pode fornecer maior grau de proteção. Por exemplo, um gateway FTP pode ser programado para restringir as operações de transferência a arquivos fisicamente localizados em um único host de acesso externo (bastion host). Além disso, a aplicação FTP pode ser modificada para limitar a transferência de arquivos da rede interna para a externa, dificultando ataques internos.

O que um *firewall* pode e o que não pode fazer

Algumas tarefas cabíveis a um *firewall*:

Um *firewall* é um checkpoint; ou seja, ele é um foco para as decisões referentes à segurança, é o ponto de conexão com o mundo externo, tudo o que chega à rede interna passa pelo *firewall;*

Um *firewall* pode aplicar a política de segurança;

Um *firewall* pode logar eficientemente as atividades na Internet;

Um *firewall* limita a exposição da empresa ao mundo externo.

Algumas tarefas que um *firewall* não pode realizar:

Um *firewal* não pode proteger a empresa contra usuários internos mal intencionados: se o inimigo mora dentro da própria casa, certamente não será esta uma morada segura;

Um *firewall* não pode proteger a empresa de conexões que não passam por ele: "do que adianta colocar uma porta da frente em aço maciço e uma dúzia de fechaduras se alguém deixou a porta da cozinha aberta?";

Um *firewall* não pode proteger contra ameaças completamente novas: "qual será o próximo furo a ser descoberto?";

Um *firewall* não pode proteger contra vírus.

***Firewall* é indispensável em redes ligadas à Internet (Caruso & Steffen, 2002, p. 174)**

Até meados da década de 90, a instalação de um *firewall* era vendida como a forma de resolver todos os problemas de segurança, e os vendedores faziam os potenciais clientes imaginarem que a simples existência de um equipamento separando sua rede local da Internet tornaria o ambiente seguro. Ainda é muito comum em serviços para identificar a origem e o grau de comprometimento de uma invasão, algum funcionário dizer que não sabe como o ataque pode acontecer, já que “nós temos um *firewall*. Por outro lado tenho clientes em cujas instalações nunca existiu tal equipamento, as redes funcionam sem grandes restrições de uso, todos os servidores são atualizados quanto a problemas de segurança e a rede é monitorada em tempo integral, e nesse ambiente não foi (ainda) reportado qualquer ataque bem-sucedido, apesar das tentativas diárias. É importante perceber que cada rede tem suas características próprias, um perfil técnico particular e necessidades distintas de qualquer outro ambiente de rede. Com isso em mente nota-se claramente que a existência de um "firewall" não é fundamental e muito menos garantia de segurança para determinado ambiente.

É certo que, nos locais onde a presença de um *firewall* for uma necessidade, a única forma de ele colaborar na segurança é quando corretamente configurado, ter suas regras revistas regularmente e estar constantemente atualizado.

***Firewall* é para Internet, não faz sentido em redes locais (Caruso & Steffen, 2002, p. 179)**

Cada ambiente de rede tem suas próprias características, é muito arriscado generalizar que componentes devem ou não existir, principalmente em se tratando de mecanismos de proteção. Algumas redes de grandes proporções não utilizam *firewall* algum, outras utilizam vários, algumas redes locais têm particularidades que fazem por exigir a existência de alguma forma de controle de tráfego, e nesses casos esse componente pode ser de fundamental importância sob o aspecto de segurança, mesmo que não existam conexões com a Internet.

6.1.2 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 você fornece sua senha para uma outra pessoa, esta 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.

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

O seu sobrenome, números de documentos, placas de carros, números de telefones e datas deverão estar fora de sua lista de senhas. Esses dados são muito fáceis de se obter e qualquer pessoa tentaria utilizar 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.).

O que é uma boa senha para (Edson Furmankiewic e Sandra Figueiredo, 2001, p.56)?

Uma boa senha deve ter pelo menos oito caracteres (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 e contém muitas repetições de letras.

Como elaborar uma boa senha?

Quanto mais "bagunçada" for a senha melhor, pois mais difícil será descobri-la. 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.

Quantas senhas diferentes devem usar?

Procure identificar o número de locais onde vocês necessita utilizar uma senha. Este número deve ser equivalente a quantidade de senhas distintas a serem mantidas por você. Utilizar senhas 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 elas fossem diferentes, uma para cada conta, caso alguém descobrisse uma das senhas, um possível prejuízo teria a mesma proporção?

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.

Trocas regulares são muito importantes para assegurar a integridade de suas senhas.

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 ;

- capturar sua senha enquanto ela trafega pela rede.

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;

6.1.3 CRIPTOGRAFIA

Muitas empresas têm estado preocupadas com a transmissão de dados sensíveis através das redes. Empresas de seguro, bancos, instituições financeiras, governo, entre outras, transmitem informações vitais de suas atividades pelas redes, informações essas que podem se tornar alvo de defraudadores.

A criptografia, ainda que uma prática antiga, ganhou força nestes últimos tempos devido à quantidade avassaladora de informações trafegadas de modo econômico pela Internet.

Para (Steve Burnett & Stephen Paine, 2002) criptografia é a tecnologia que tenta manter em segredo mensagens em trânsito. Para criptografar qualquer mensagem são necessários dois componentes: a chave e o algoritmo. A chave é uma seqüência de caracteres, usada como elemento matemático para a transformação de uma mensagem comum em mensagem cifrada. A mensagem cifrada contém seqüências de caracteres ininteligíveis e que só são decifradas se quem as decifra conhece a chave. O algoritmo são funções matemáticas usadas para transformar a chave e a mensagem original em mensagem cifrada e vice-versa.

Existe um método para obter uma transmissão de dados realmente segura, onde apenas o receptor da mensagem poderá lê-la, e ainda terá como saber se o transmissor é realmente quem diz ser e se a mensagem foi alterada no caminho. Este método chama-se criptografia ou

encriptação de dados. O programa de criptografia mais famoso segundo Steve Burnett & Stephen Paine é o PGP (Pretty Good Privacy - Ótima Privacidade). É também um dos programas mais polêmicos da Internet. O seu autor, Phil Zimmermann, sofreu uma série de investigações por parte do FBI e teve de recorrer a grupos de apoio que se formaram na Internet para conseguir pagar seus advogados. O uso do programa chegou a ser proibido durante dois anos nos EUA, por infringir a patente do algoritmo RSA. Hoje, porém, o PGP é totalmente legal e não há nenhuma restrição ao seu uso.

De modo algum a criptografia é a única ferramenta necessária para assegurar a segurança dos dados, nem resolverá todos os problemas de segurança. É um instrumento entre vários outros. Além disso, a criptografia não é a prova de falhas. Toda criptografia pode ser quebrada e, sobretudo, se for implementada incorretamente, ela não agrega nenhuma segurança real.

A criptografia converte dados legíveis em algo sem sentido, com a capacidade de recuperar os dados originais a partir desses dados sem sentido.

Dois são os objetivos principais da criptografia:

- Provar a identidade do usuário (autenticação);

- Esconder o conteúdo de um feixe de dados (criptografia);

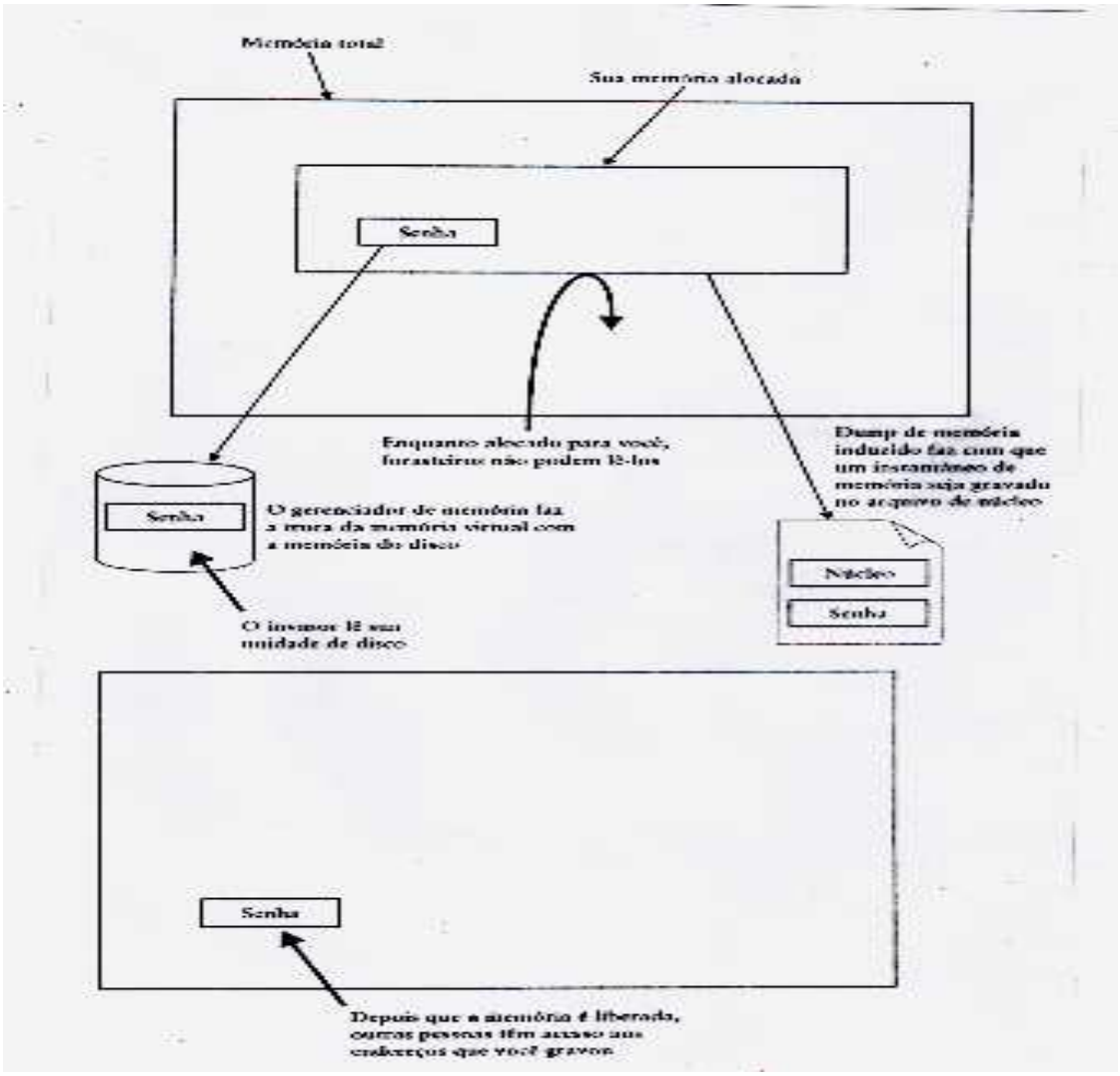

Figura 5- Proteção usando criptografia.
Fonte: livro Segurança em Informática e de Informações, 2001, p. 126.

6.1.4 ANTIVÍRUS

> São programas utilizados para detectar vírus num computador ou disquete. A maioria usa método simples de procura por uma sequência de bytes que constituem o programa vírus. (autor anônimo, 2002).

Desde que alguém tenha detectado e analisado a seqüência de bytes de um vírus, é possível escrever um programa que procura por essa seqüência. Se existe algo parecido, o programa antivírus anuncia que encontrou um vírus. O antivírus, por sua vez, funciona como uma vacina dotada de um banco de dados que cataloga milhares de vírus conhecidos. Quando

o computador é ligado ou quando o usuário deseja examinar algum programa suspeito, ele varre o disco rígido em busca de sinais de invasores.

> No meu modo de entender, um bom aplicativo antivírus é o que reconhece o maior número possível deles, pode ser atualizado fácilmente online (eu o faço semanalmente), varre arquivos compactados, monitora downloads, cria discos de sistema para emergências e detecta vírus de macro, trojans e applets hostis.(autor anônimo, 2002).

Quando um possível vírus é detectado, o antivírus parte para o extermínio. Alguns antivírus conseguem reparar os arquivos contaminados, entretanto nem sempre isso é possível. Muitas vezes a única saída é substituir o arquivo infectado pelo mesmo arquivo *clean* do software original, ou de outro computador com programas e sistema operacional idênticos ao infectado. Dependendo do vírus e das proporções dos danos ocasionados pela virose, apenas alguém que realmente compreenda do assunto poderá limpar o seu computador e, se possível, recuperar os arquivos afetados.

Alguns antivírus são dotados de alguns recursos especiais, são eles conforme a página de Ray Informática (José, 2003) cita:

1) Tecnologia Push : atualiza a lista de vírus. Ao conectar-se à INTERNET, o micro aciona o software Backweb, que busca automaticamente novas versões da lista de vírus no site da McAfee sem a necessidade do usuário fazer dowloads manuais;

2) ScreenScan: varre o disco rígido enquanto o micro está ocioso. Funciona da seguinte maneira: toda vez que o screen saver é acionado, o VirusScan entra em ação. Além de não atrapalhar a rotina do usuário, evita a queda de desempenho do PC.

Os programas antivirus, como os outros programas dividem-se em três principais categorias: Comerciais (Norton), Shareware (Scan) e Freeware(Inoculate).

Nota-se vantagens do Inoculate: - Freeware (você não precisa pagar nada por ele, baixa da internet e ele avisa para fazer as atualizações na data correta, mais ou menos um mês após e é feita automatizamente pela internet). Faz também que não precisemos estar pirateando programas (Norton) nem correndo o risco de ter um antivirus vencido em 30 dias (Scan) ;

- É eficiente, tem mostrado-se eficiente em todos os testes que efetuamos;
- Ao encontrar um virus ele remove e depois avisa que removeu (ideal para leigos);
- Vem com um utilitário de recuperação do HD;
- Funciona também em rede.
- É o menor dos três citados (menos de 3MB) e também o mais leve.

6.1.5 CERTIFICAÇÃO DIGITAL

Segundo (Furmankiewic e Figueiredo 2001, p.154) o certificado digital é um arquivo eletrônico que contém dados de uma pessoa ou instituição, utilizados para comprovar sua identidade. Exemplos semelhantes a um certificado são o RG, CPF e carteira de habilitação de uma pessoa. Cada um deles contém um conjunto de informações que identificam a pessoa e alguma autoridade (para estes exemplos, órgãos públicos) garantindo 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;
- o número de série do certificado;
- 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 nela contidas.

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".

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 à sua conta bancária pela 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 assegurar-se 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.

7 CONCLUSÃO

Sob o ponto de vista legal, os crimes digitais ainda estão em caminhamento, mas não atingiu ainda o esperado.

Neste trabalho, mostra as principais ferramentas de segurança e de acordo com meus estudos concluí que não existe a ferramenta mais eficaz. Tudo vai depender da necessidade que cada instituição vai ter.

Espero que tudo que escrevi aqui, não só auxilie outras pessoas a evitar certos constrangimentos (crimes), mas também que as ajude a julgar o melhor meio para se defender quando estiver usando o computador. Espero também que ajude alguns técnicos na área de informática a se concientizarem-se e unirem-se ao poder legislativo para achar o melhor meio de punição para tais crimes.

REFERÊNCIA BIBLIOGRÁFICA

Autor Anônimo, traduzido por Edson Furmankiewic e Sandra Figueiredo. **Segurança Máxima**. 3º edição.Rio de Janeiro, 2001

Burnett, Steve; Paine, Stephen. **Criptografia e segurança.** 2 ºedição, Rio de Janeiro: Campus,2002.

Caruso, Carlos A. A.; Steffen , Flávio Deny. **Segurança em Informática e de Informações.**

São Paulo, SP, 1999.

Scambray, Joel; Stuart, McClure; Kurtz, George. **Hackers Expostos.** 5º edição ampliada e atualizada. Rio de Janeiro, 2002.

Spyman. **Manual Completo do Hacker.** Rio de Janeiro, RJ, 2002.

Gandelman, Henrique. De Gutenberg à Internet: **direitos autorais na era digital.** 4º edição ampliada e atualizada.Rio de Janeiro, 2003

Müler, Mary Stela; Cornelsen, Julce Mary**. Normas e padrões para teses, dissertações e monografias.** 5º edição. Londrina: Eduel,2003.

Damásio, Jesus. **Direito Penal**: Parte Geral e Especial.24º edição. São Paulo, Editora Saraiva, 2001.

Brancao, Figueiredo Ricardo. **Engenharia Social.** 3.ed. São Paulo, Editora Moderna, 2003.

Mello, Freyre Fernando. **Engenharia Social – Formas de Ataques.** .ed. São Paulo, Editora Moderna, 2001.

Mesquita, Renata. **Revista Info.** Acessado http://info.abril.com.br/aberto/infonews/112003/06112003-3.shl. Acesso em 11 junho. 2004.

Duarte**,**Hélio. **Site ubbi.** http://www.xrafaelx.ubbi.com.br. Acesso em 20 maio 2004.

Rezende, José. **Sucesu- ES.**
http://www.sucesues.org.br/eventos/ agenda_passada.asp?cod_evento=74. Acesso em 16 março 2004.

Duarte, Letícia.
http://www.rnp.br/noticias/imprensa/2003/not-imp-031109.html.Acesso em 02 de maio 2004.

Lima, Ronaldo. Segurança. Site da IBM.
http://www.br.ibm.com/businesscenter/solucoes_sec.shtml site da IBM .Acesso em 15 de maio 2004.

José, Paulo. Ray Informatica.
http://www.rayinformatica.com.br/virus.htm. Acesso em 15 de maio 2004.

8 ANEXO 1 - COMISSÃO DE CONSTITUIÇÃO E JUSTIÇA E DE REDAÇÃO PROJETO DE LEI Nº 84, DE 1999 (SUBSTITUTIVO)

Regula o uso de bancos de dados, a prestação de serviços por redes de computadores, dispõe sobre os crimes cometidos na área de informática, e dá outras providências.

O CONGRESSO NACIONAL decreta:

1. Art. 1º Esta Lei regula o uso de bancos de dados e a prestação de serviços por redes de computadores, dispõe sobre os crimes cometidos na área de informática, e dá outras providências.

CAPÍTULO I
DOS PRINCÍPIOS QUE REGULAM A PRESTAÇÃO DE SERVIÇO POR REDES DE COMPUTADORES

Art. 2º O acesso, o processamento e a disseminação de informações através das redes de computadores devem estar a serviço do cidadão e da sociedade, respeitados os critérios de garantia dos direitos individuais e coletivos e de privacidade e segurança de pessoas físicas e jurídicas e da garantia de acesso às informações disseminadas pelos serviços da rede.

Art. 3º É livre a estruturação e o funcionamento das redes de computadores e seus serviços, ressalvadas as disposições específicas reguladas em lei.

CAPÍTULO II
DO USO DE INFORMAÇÕES DISPONÍVEIS EM COMPUTADORES OU REDES DE COMPUTADORES

Art. 4° Para fins desta Lei, entendem-se por informações privadas aquelas relativas à pessoa física ou jurídica identificada ou identificável.
Parágrafo único. É identificável a pessoa cuja individuação não envolva custos ou prazos desproporcionados.
Art. 5° Ninguém será obrigado a fornecer informações sobre si ou sobre terceiros, salvo nos casos previstos em lei.
Art. 6° A coleta, o processamento e a distribuição, com finalidades comerciais, de informações privadas ficam sujeitas à prévia aquiescência da pessoa a que se referem, que poderá retirá-la a qualquer momento, ressalvando-se o pagamento de indenizações a terceiros, quando couberem.
§ 1° Salvo por disposição legal ou determinação judicial em contrário, nenhuma informação privada será mantida à revelia da pessoa a que se refere ou além do tempo previsto para a sua validade.
§ 2° A toda pessoa cadastrada dar-se-á conhecimento das informações privadas armazenadas a ela referentes, bem como das respectivas fontes, ficando-lhe assegurado o direito à retificação gratuita de qualquer informação privada incorreta.
§ 3° Qualquer pessoa, física ou jurídica, tem o direito de interpelar o proprietário de rede de computadores ou provedor de serviço para saber se mantém informações a seu respeito, e o respectivo teor.
Art. 7º As entidades que coletam, armazenam, processam, distribuem ou comercializam informações privadas, ou utilizam tais informações para fins comerciais ou para prestação de serviço de qualquer natureza, ficam obrigadas a explicitar, desde o início de tais atividades:
I - os fins para os quais se destinam tais informações; e
II os limites de suas responsabilidades no caso de fraude ou utilização imprópria das informações sob sua custódia, bem como as medidas adotadas para garantir a integridade dos dados armazenados e a segurança dos sistemas de informação.
Art. 8° As entidades mencionadas no artigo anterior não poderão divulgar ou tornar disponíveis, para finalidade distinta daquela que motivou a estruturação do banco de dados, informações privadas referentes, direta ou indiretamente, à origem racial, opinião política, filosófica ou religiosa, crenças, ideologias, saúde física ou mental, vida sexual, registros policiais, assuntos familiares ou profissionais, vida privada, honra e imagem das pessoas, informações nominais restritivas de crédito, oriundas de títulos ou documentos de dívida que não tenham sido regularmente protestados, bem como as relativas a ações, processos e feitos ajuizados, cujas decisões não tenham transitado em julgado e que a lei definir como sigilosas, salvo por ordem judicial ou com anuência expressa da pessoa a que se referem ou do seu representante legal.

CAPÍTULO III
DOS CRIMES DE INFORMÁTICA
Seção I
Acesso indevido ou, não autorizado

Art. 9° Acesso, indevido ou não autorizado, a dados ou informações armazenadas no computador ou em rede de computadores.
Pena – detenção, de um mês a um ano, e multa.
Parágrafo único. Na mesma pena incorre quem, sem autorização ou indevidamente, obtém, mantém ou fornece a terceiro meio de acesso a computador ou rede de computadores.

Seção II

Alteração de senha ou meio de acesso a programa de computador ou dados

Art. 10. Apagar, destruir, alterar, ou de qualquer forma inutilizar, senha ou qualquer outro meio de acesso a computador, programa de computador ou de dados, de forma indevida ou não autorizada.

Pena – detenção, de seis meses a dois anos, e multa.

Seção III

Obtenção, manutenção ou fornecimento indevido, ou não autorizado, de dado ou instrução de computador

Art. 11. Obter, manter ou fornecer, de forma indevida ou não autorizada, dado ou instrução de computador.

Pena – detenção, de um mês a um ano, e multa.

Seção IV

Dano a dado ou programa de computador

Art. 12. Apagar, destruir, modificar ou de qualquer forma inutilizar, total ou parcialmente, dado ou programa de computador, de forma indevida ou não autorizada.

Pena: detenção, de um a seis meses, e multa.

Seção V

Criação, desenvolvimento ou inserção em computador de dados ou programa de computador com fins nocivos

Art. 13. Criar, desenvolver, inserir ou fazer inserir, dado ou programa de computador, em computador ou rede de computadores, de forma indevida ou não autorizada, com a finalidade de apagar, destruir, inutilizar ou modificar dado ou programa de computador, ou de qualquer forma dificultar ou impossibilitar, total ou parcialmente, a utilização de computador ou rede de computadores, ou o acesso a estes.

Pena – detenção, de um ano a dois anos, e multa.

Seção VI

Violação de segredo armazenado em computador, meio magnético, de natureza magnética, óptica ou similar

Art. 14. Obter ou fornecer segredos, de indústria ou comércio, ou informações pessoais armazenadas em computador, rede de computadores, meio eletrônico de natureza magnética, óptica ou similar, de forma indevida ou não autorizada.

Pena: detenção, de seis meses a dois anos, e multa.

CAPÍTULO IV

DAS DISPOSIÇÕES FINAIS

Art. 15. Se qualquer dos crimes previstos nesta Lei é praticado no exercício de atividade profissional ou funcional, a pena é aumentada de um sexto até a metade.

Art. 16. Se qualquer dos crimes previstos nesta Lei, é cometido:

I – contra a União, Estado, Distrito Federal, Município, órgão ou entidade da administração direta ou indireta ou de empresa concessionária de serviços públicos;

II – com considerável prejuízo para a vitima;

III – com intuito de lucro ou vantagem de qualquer espécie, própria ou de terceiro;

IV – com abuso de confiança;

V – por motivo fútil;

VI – com o uso indevido de senha ou processo de identificação de terceiro; ou

VII – com a utilização de qualquer outro meio fraudulento.
Pena – reclusão, de dois a seis anos, e multa.
Art. 17. Nos crimes definidos nesta Lei, somente se procede mediante queixa ou representação do ofendido, salvo se cometidos contra o interesse da União, Estado, Distrito Federal, Município, órgão ou entidade da administração direta ou indireta, empresa concessionária de serviços públicos, fundações instituídas ou mantidas pelo poder público, serviços sociais autônomos, instituições financeiras ou empresas que explorem ramo de atividade controlada pelo poder público, casos em que a ação é pública incondicionada.
Art. 18. Esta Lei regula os crimes relativos à informática sem prejuízo das demais cominações legais.
Art. 19. Revogam-se os arts. da Lei nº 9.507, de 12 de novembro de1997.
Art. 20. Esta Lei entra em vigor no prazo de noventa dias decorridos de sua publicação.

Sala da Comissão, em de de 2000
Deputado LEO ALCÂNTARA
Relator