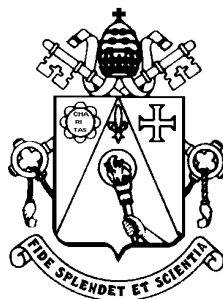


Segurança da Informação

Perigos do Mundo Virtual¹



Pontifícia Universidade Católica de Campinas
Faculdade de Análise de Sistemas

Guilherme Cestarolli Seleguim²

Resumo

Você precisa ter consciência de que seu computador é uma porta aberta para o mundo, com a agravante de não se poder ver quem o está olhando. Quem compartilha um universo tão diversificado, deveria, independentemente de qualquer coisa, prevenir-se contra surpresas desagradáveis.

Palavras-chave

Segurança da Informação; Internet; Hackers; Crackers; Trojans; Rede de Computadores;

Security of Information–Dangers in the Virtual World

Summary

You need to know that your computer is an open door to the world, the problem is that you can't see who is watching you. When you are sharing a universe that is so diversified, you should, be independent of anything, protect yourself against disagreeable surprises.

Keywords

Security of Information; Internet; Hackers; Crackers; Trojans; Computer Networks;

¹ Trabalho desenvolvido na Faculdade de Análise de Sistemas da PUC-Campinas

² Aluno da Faculdade de Análise de Sistemas da PUC-Campinas

1. Introdução

No final da década de 60, surgia a Internet. Inicialmente ela foi criada e desenvolvida para ser utilizada pelo exército americano, a fim de não centralizar todas as informações registradas em computadores em um único local do país. Desta forma, ficaria muito vulnerável quanto à destruição dos servidores por forças militares inimigas. Como solução, resolveram distribuir os dados em vários servidores distribuídos por todo o território nacional, todos interligados compartilhando as informações.

Para a comunicação entre os servidores, foram criados protocolos, dentre os quais está o protocolo IP³, que hoje em dia é o principal protocolo usado na Internet. O protocolo IP foi criado somente para a transmissão de informações entre os servidores do exército, então não se preocuparam com a segurança contra a captação de informações entre os servidores.

Com o crescimento e a popularização da Internet, englobando não só computadores militares americanos, mas muitos outros pelo mundo, com transmissão de vários tipos de informações, e acessados por vários perfis de pessoas, surge a necessidade de assegurar que as informações trafegadas na rede estarão seguras.

Transações bancárias e *e-commerce* (comércio via Internet) necessitam de muita segurança, pois trafegam informações dos usuários de suma importância e sigilo, tais como números de cartão de crédito e senhas. Estas informações devem ser protegidas tanto para a transmissão quanto no armazenamento e acesso posterior. Informações corporativas e documentos confidenciais também devem ser protegidos[BREDARIOL, 2001].

Muitas empresas e usuários domésticos não se preocupam tanto com a segurança de seus sistemas, podendo levar à perda de dados, indisponibilização de um serviço, indisponibilização de um sistema, entre outras possibilidades mais graves.

A maioria dos ataques são feitos à distância, geralmente por *Hackers*⁴ e *Crackers*⁵ que se utilizam da Internet para conseguirem acesso às máquinas internas das empresas, mas um ponto muito importante é a segurança física dos computadores e da própria rede corporativa.

3 IP: Internet Protocol. Endereço de computador em uma rede, utilizado para a comunicação entre computadores na rede. Exemplo de endereço IP: 200.231.13.13.

4 Hacker: Tem conhecimentos reais de programação e de sistemas operacionais, principalmente o Linux e o Unix, que são os mais usados em servidores da Internet. Conhece quase todas as falhas de segurança dos sistemas e está sempre em busca de outras. Desenvolve suas próprias técnicas e programas de invasão[M@RCIO, 2000].

5 Cracker: É o “Hacker do Mal”, que invade sistemas, rouba dados e arquivos, números de cartão de crédito, faz espionagem industrial e quase sempre provoca algum tipo de destruição, principalmente de dados. É confundido pela imprensa que lhe atribui erroneamente o nome de Hacker[M@RCIO, 2000].

2. Importância do Tema

Atualmente o investimento em segurança das informações não é mais uma opção e sim uma exigência da coletividade pois o vazamento de dados críticos pode causar prejuízos de grande quantidade para toda a sociedade.

Até pouco tempo atrás o investimento em segurança das informações era uma opção da empresa, pois não havia nenhuma exigência legal. Passado algum tempo, o investimento passou a ser necessário pois proporcionava maior confiança dos consumidores nas empresas e agregava valor aos produtos. Hoje, o investimento no setor de segurança das informações passou a ser uma exigência legal porque a própria lei, em diversos diplomas, passou a exigir a conservação de arquivos em formato digital. Como por exemplo:

O art. 11 da Lei nº 8.218, de 29 de agosto de 1991 determina que as pessoas jurídicas que possuem patrimônio líquido superior a Cr\$ 250.000.000,00 e utilizam sistema de processamento eletrônico de dados para registrar negócios e atividades econômicas, escriturar livros ou elaborar documentos de natureza contábil ou fiscal ficarão obrigados à manter, em meio magnético ou assemelhado, à disposição do Departamento da Receita Federal, os respectivos arquivos e sistemas durante o prazo de cinco anos. A inobservância poderá acarretar multa de meio por cento do valor da receita bruta da pessoa jurídica no período ou multa de cinco por cento sobre o valor da operação correspondente, aos que omitirem ou prestarem incorretamente as informações solicitadas.

As empresas que trabalham com venda ao consumidor final também estão obrigadas a aumentar seus investimentos em segurança da informação pois segundo o Código de Defesa do Consumidor (Lei nº 8.078/90) art. 39, inciso VIII, é vedado ao fornecedor de produtos ou serviços colocar no mercado de consumo qualquer produto ou serviço em desacordo com as normas expedidas pelos órgãos oficiais competentes ou, se normas específicas não existirem, pela Associação Brasileira de Normas Técnicas (ABNT).

Pela própria inteligência dos artigos supramencionados vê-se que o investimento em segurança das informações é uma obrigação e todos aqueles que não se atêm a esta situação poderão amargar grandes prejuízos[GOMES, 2002].

3. Como a Segurança é Burlada

3.1 Técnica de invasão

Invasão é a entrada em um site, servidor, computador ou serviço por alguém não autorizado. Mas antes da invasão propriamente dita, o invasor poderá fazer um teste de invasão, que é uma tentativa de invasão em partes, onde o objetivo é avaliar a segurança de uma rede e identificar seus pontos vulneráveis.

Mas não existe invasão sem um invasor, que pode ser conhecido, na maioria das vezes, como *Hacker* ou *Cracker*. Ambos usam seus conhecimentos para se dedicarem a testar os limites de um sistema, ou para estudo e busca de conhecimento ou por curiosidade, ou para encontrar formas de quebrar sua segurança ou ainda, por simples prazer.

Mas também pode ser por mérito, para promoção pessoal, pois suas descobertas e ataques são divulgados na mídia e eles se tornam conhecidos no seu universo, a diferença é que o *Cracker* utiliza as suas descobertas para prejudicar financeiramente alguém, em benefício próprio, ou seja, são os que utilizam seus conhecimentos para o mau.

Existem muitas ferramentas para facilitar uma invasão e a cada dia aparecem novidades a respeito. Abaixo serão descritas algumas das mais conhecidas.

3.1.1 Spoofing

Nesta técnica, o invasor convence alguém de que ele é algo ou alguém que não é, sem ter permissão para isso, conseguindo autenticação para acessar o que não deveria ter acesso, falsificando seu endereço de origem. É uma técnica de ataque contra a autenticidade, onde um usuário externo se faz passar por um usuário ou computador interno.

3.1.2 Sniffers

É um programa de computador que monitora passivamente o tráfego de rede, ele pode ser utilizado legitimamente, pelo administrador do sistema para verificar problemas de rede ou pode ser usado ilegalmente por um intruso, para roubar nomes de usuários e senhas. Este tipo de programa explora o fato dos pacotes das aplicações TCP/IP não serem criptografados.

Entretanto, para utilizar o sniffer, é necessário que ele esteja instalado em um ponto da rede, onde passe tráfego de pacotes de interesse para o invasor ou administrador.

3.1.3 Ataque do tipo DoS - Denial of Service

É um ataque de recusa de serviço, estes ataques são capazes de tirar um site do ar, indisponibilizando seus serviços. É baseado na sobrecarga da capacidade ou em uma falha não prevista.

Um dos motivos para existirem esse tipo de falha nos sistemas é um erro básico de programadores, na hora de testar um sistema, muitas vezes, eles não testam o que acontece se um sistema for forçado a dar erro, se receber muitos pacotes em pouco tempo ou se receber pacotes com erro, normalmente é testado o que o sistema deveria fazer e alguns erros básicos. O invasor parte deste princípio e fica fazendo diversos tipos de testes de falhas, até acontecer um erro e o sistema parar.

Este tipo de ataque não causa perda ou roubo de informações, mas é um ataque preocupante, pois os serviços do sistema atacado ficarão indisponíveis por um tempo indeterminado, dependendo da equipe existente na empresa para disponibilizá-lo novamente e dependendo do negócio da empresa, este tempo de indisponibilidade pode trazer muitos prejuízos.

De acordo com um estudo da Universidade da Califórnia, *Crackers* tentam realizar em torno de 4 mil ataques do tipo DoS por semana. Os alvos mais comuns são grandes empresas.

3.1.4 Ataque do tipo DDoS – Distributed Denial of Service

São ataques semelhantes ao DoS, tendo como origem diversos e até milhares de pontos disparando ataques DoS para um ou mais sites determinados. Para isto, o invasor coloca agentes para dispararem o ataque em uma ou mais vítimas. As vítimas são máquinas escolhidas pelo invasor por possuírem alguma vulnerabilidade. Estes agentes, ao serem executados, se transformam em um ataque DoS de grande escala. Uma ferramenta criada recentemente, de nome *DDoS Attack*, desenvolvida pelo programador brasileiro que se intitula OceanSurfer⁶, é capaz de causar negação de serviços em computadores na Internet através de uma inundação de conexões em determinada porta.

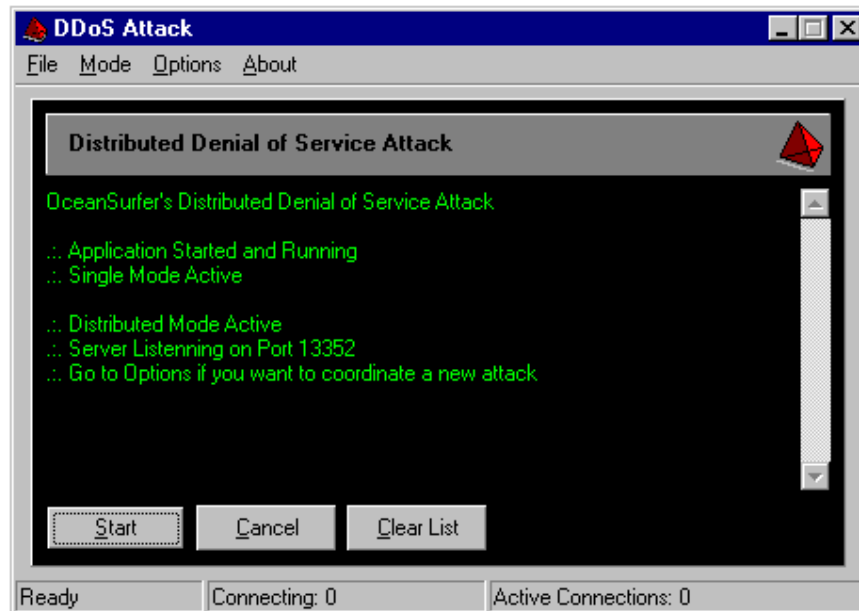


Fig. 1 – *DDoS Attack* de OceanSurfer

3.1.4.1 Funcionamento Técnico do DDoS Attack

O software foi escrito em Delphi 5 com o intuito de ajudar administradores de redes a sanarem possíveis falhas em configurações de softwares na rede que se utilizam de *sockets* para funcionarem, especificamente softwares servidores de serviços. À seguir seguem informações técnicas sobre o programa.

3.1.4.1.1 Portas

Portas identificam serviços que rodam em servidores. Um servidor pode conter vários serviços instalados, ou seja, o mesmo computador pode ser um servidor de correio eletrônico, servidor de FTP (*File Transfer Protocol* ou Protocolo de Transferência de Arquivos) e servidor Web (páginas na Internet);

O servidor é identificado por um endereço IP, mas os serviços também precisam

6 OceanSurfer: Pode ser encontrado em: oceansurfer@newocean.cjb.net e pelo UIN:69340992 no programa ICQ.

ser identificados individualmente. Para cada serviço, então, é associada uma **porta** que é um número de identificação entre 0 e 65535. Existem programas chamados de *scanners* que podem verificar quais portas estão abertas em um computador remoto como por exemplo o *scanner* construído também por OceanSurfer.

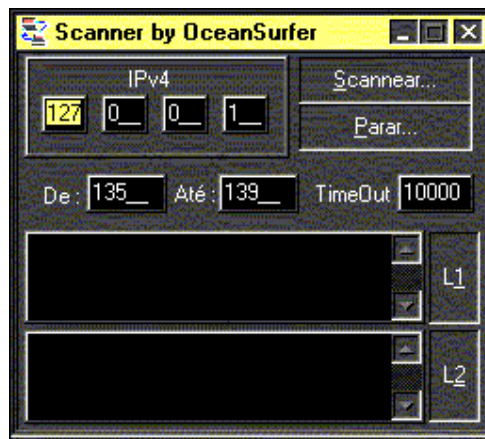


Fig. 2 – Scanner de portas de OceanSurfer

3.1.4.1.2 Os Sockets

Um *socket*, por definição, é um canal de comunicação entre computadores em uma rede e identifica uma conexão entre eles, normalmente entre um cliente e um servidor. Através dos *sockets* os computadores podem trocar informações através de uma rede. Para identificar uma conexão entre dois computadores, um *socket* deve ser definido, por meio das seguintes informações:

- Endereço IP do servidor;
- Porta onde se encontra o serviço solicitado;
- Endereço IP do cliente;
- Porta através da qual o cliente solicita o serviço.

Um bom exemplo de um estabelecimento de uma conexão entre computadores através de *socket* seria o acesso à uma página da Internet. Um servidor Web tem a porta 80 como porta padrão de comunicação entre os clientes. Quando digitamos um endereço de um site no Internet Explorer do Windows, automaticamente esse endereço é convertido em seu respectivo endereço IP. Se estamos numa rede, nosso micro tem um único endereço IP. E finalmente, junto deste processo, uma porta em seu computador é disponibilizada dinamicamente, sendo um número maior que 1024, para esta conexão.

Então, temos todas as informações necessárias para estabelecer a conexão, tendo assim um *socket*. O cliente, no caso de uma conexão à uma página da Internet, é quem a solicita através de um *browser* (Internet Explorer, por exemplo), e o servidor é quem disponibiliza a página para ser acessada.

Como visto, o servidor Web trabalha na porta 80, enquanto que outros serviços têm também suas respectivas portas padrão, como o FTP que trabalha na porta 21, o Telnet que trabalha na porta 23, o SMTP que trabalha na porta 25 e o POP3 que trabalha na porta 110.

3.1.4.1.3 A ação do programa

Para o programa funcionar, é necessário saber qual a porta que se quer testar e qual o IP do computador alvo na rede. É solicitado a quantidade de tentativas de conexões simultâneas que se deseja fazer para a determinada porta. Basta então clicar no botão *Start* e é iniciado o ataque e se o software que estiver trabalhando na porta determinada for mal construído, com certeza será derrubado e parará de operar, indisponibilizando aquele serviço.

O teste pode ser feito de um atacante só, ou também em modo distribuído, com quantos atacantes quiserem. O interessante é que mesmo sem estar em modo distribuído, foi constatada falha em diversos programas, inclusive em *Firewalls*, que travavam, comprometendo em muito a segurança das redes.

3.1.5 Quebra de Senhas

Para acessar algo é necessário uma senha de acesso, muitos invasores tentam quebrar estas senhas através de técnicas de quebras de senhas, como tentar as senhas padrões de sistemas ou as senhas simples como nomes pessoais, nome da empresa, datas, entre outros. Mas para facilitar a descoberta da senha, existem diversos programas, como dicionários de senhas e programas que tentam todas as combinações possíveis de caracteres para descobrir a senha.

3.1.6 Vírus

O vírus de computador é outro exemplo de programa de computador, utilizado maliciosamente ou não, que se reproduz embutindo-se em outros programas. Quando estes programas são executados, o vírus é ativado e pode se espalhar ainda mais, geralmente danificando sistemas e arquivos do computador onde ele se encontra. Um exemplo deste tipo de programa é o *Worm*, criado por Robert Morris[**SETTE, 2001**].

Os vírus não surgem do nada, ou seja, seu computador não tem a capacidade de criar um vírus, quem cria os vírus são programadores de computador mal intencionados. Os vírus se ocultam em arquivos executáveis, ou seja, com extensão .EXE ou .COM, e de bibliotecas compartilhadas, de extensão .DLL.

Quanto a arquivos de dados, você pode abrí-los sem medo! Assim, pode rodar tranquilamente seus arquivos de som (.WAV, .MID, .MP3), imagem (.BMP, .PCX, .GIF, .JPG), vídeo (.AVI, .MOV) e os de texto que não contenham macros (.TXT, .WRI, .DOC), mas Kerñell⁷, um especialista em sistemas Linux, afirma que esses arquivos não são totalmente seguros e que as falhas podem ser exploradas.

Para que o vírus faça alguma coisa, não basta você tê-lo em seu computador.

7 Kerñell: Certificado como Engenheiro Linux e Desenvolvedor de Sistemas Linux, pode ser encontrado em: kernel_hacked@ig.com.br e pelo UIN:117168826 no programa ICQ.

Para que ele seja ativado, passando a infectar o micro, é preciso executar o programa que o contém. E isto você só faz se quiser, mesmo que não seja de propósito. Ou seja, o vírus só é ativado se você der a ordem para que o programa seja aberto, por ignorar o que ele traz de mal pra você. Se eles não forem “abertos”, “executados”, o vírus simplesmente fica alojado inativo, aguardando ser executado para infectar o computador.

Após infectar o computador, eles passam a atacar outros arquivos. Se um destes arquivos infectados for transferido para outro computador, este também vai passar a ter um vírus alojado, esperando o momento para infectá-lo, ou seja, quando for também executado. Daí o nome de vírus, devido à sua capacidade de auto-replicação, parecida com a de um ser vivo.

Por que os vírus são escritos ? Esta pergunta foi feita na convenção de Hackers e fabricantes de vírus na Argentina. As respostas seguem abaixo:

- *Beacause it's fun;*
- Para estudar as possibilidades relativas ao estudo de vida artificial (de acordo com a frase de Stephen Hawkind: “Os vírus de computador são as primeiras formas de vida feitas pelo homem”). Esta proposta é seguida por vários cientistas.
- Para descobrir se são capazes de fazer isso, tentando seus conhecimentos de computação, ou para mostrarem aos colegas que são capazes de fazer;
- Para conseguir fama;
- Fins militares. Falou-se sobre isso na Guerra do Golfo, mas os vírus para uso militar são uma possibilidade.

3.1.7 Trojans

A denominação “Cavalo de Tróia” (Trojan Horse) foi atribuída aos programas que permitem a invasão de um computador alheio com espantosa facilidade. Nesse caso, o termo é análogo ao famoso artefato militar fabricado pelos gregos espartanos. Um “amigo” virtual presenteia o outro com um “presente de grego”, que seria um aplicativo qualquer. Quando o leigo o executa, o programa atua de forma diferente do que era esperado.

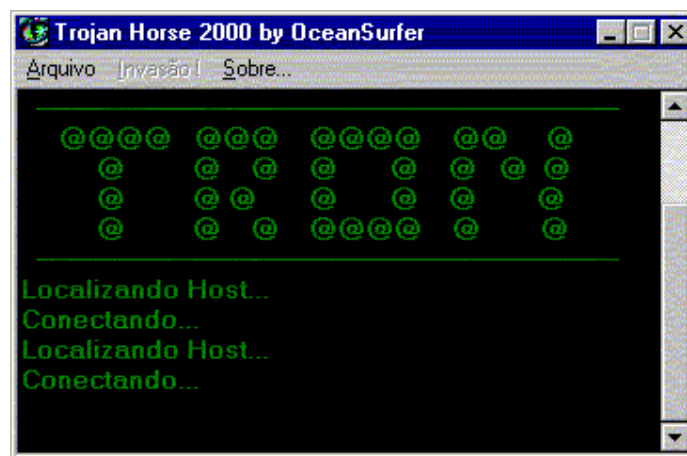


Fig. 3 – Trojan Horse (parte cliente) de OceanSurfer

Ao contrário do que é erroneamente informado na mídia, que classifica o Cavalo de Tróia como um vírus, ele não se reproduz e não tem nenhuma comparação com vírus

de computador, sendo que seu objetivo é totalmente diverso. Deve-se levar em consideração, também, que a maioria dos antivírus fazem a sua detecção e os classificam como tal. A expressão “Trojan” deve ser usada, exclusivamente, como definição para programas que capturam dados sem o conhecimento do usuário.

O Cavalo de Tróia é um programa que se aloca como um arquivo no computador da vítima. Ele tem o intuito de roubar informações como passwords, logins e quaisquer dados, sigilosos ou não, mantidos no micro da vítima. Quando a máquina contaminada por um Trojan conectar-se à Internet, poderá ter todas as informações contidas no HD visualizadas e capturadas por um intruso qualquer. Estas visitas são feitas imperceptivelmente. Só quem já esteve dentro de um computador alheio sabe as possibilidades oferecidas[M@RCIO, 2000].

4. Acontecimentos

4.1 Kevin Mitnick

Periodicamente, muitas histórias sobre *Hackers* e *Crackers* são contadas através dos veículos de comunicação. A mais popularizada no mundo foi a de dois personagens feríssimas. Eles se chamam Kevin Mitnick e Tsutomu Shimomura (o farejador). Kevin era um garotão californiano, autoconfiante, que roubou, nada mais, nada menos, que cerca de 20.000 números de cartões de crédito dos associados da rede Netcom, que também é uma provedora de acesso à Internet. Não satisfeito com sua façanha e tendo conhecimento da existência de Shimomura como o principal especialista em segurança de redes de computadores ligado ao FBI, Mitnick desconfiou que estaria sendo perseguido por ele. Então invadiu o computador desse gênio nipo-americano e, por várias vezes, deixou mensagens de desafio e afronta – do tipo “sou o melhor” – para chamar-lhe mais ainda a atenção.



Com o sangue frio que caracteriza sua ascendência, Shimomura começou um processo de investigação digno de cinema e ficou sabendo que os dados que haviam sido tirados de seu computador por Kevin estavam armazenados na Netcom. O segurança cibernético não titubeou e rumou para San Jose, na Califórnia, onde está localizada a empresa.

Um dos erros de Kevin Mitnick foi subestimar a capacidade de Shimomura e pensar que jamais poderia ser rastreado pelo agente americano, o que resultou numa tremenda caçada por parte desse que é considerado o maior farejador cibernético da atualidade. Ao chegar à cidade, Shimomura descobriu que as ligações de Mitnick eram provenientes de um telefone celular da Carolina do Norte. Com toda colaboração da companhia telefônica e após muitas peregrinações, ele conseguiu um carro munido de aparelhos sofisticados, capazes de captar a frequência de telefones celulares. De posse destes recursos, ficou fácil a captura de Mitnick.

4.2 John Draper

Pelas informações obtidas até hoje, este foi o primeiro *Hacker* a receber a conotação de *Phreaker* (especialista em sistemas de telefonia no *underground*). Ele desenvolveu uma técnica simples e ao mesmo tempo inteligente para fazer ligações interurbanas gratuitamente, usando um apito de brinquedo que era dado à quem comprasse uma determinada marca de cereal, muito consumido nos Estados Unidos. Também foi preso e sua pena não foi divulgada.



4.3 Phiber Optik

Discípulo de John Draper, este foi e continua sendo o fera entre os especialistas em *Phreak*. Na época, Optik (Mark Abene) fazia parte do grupo nova-iorquino “Mestres da Fraude” e deu início à toda uma nova geração de *Hackers*, interessados nos meandros dos sistemas de telefonia no país do Tio Sam. Optik também cumpriu parte da pena que lhe foi atribuída e foi solto em liberdade condicional. Recentemente, ministrou várias palestras em alguns estados brasileiros, acompanhado de mais dois ex-*Hackers*, cobrando somas consideráveis por cada palestra. Hoje é especialista em montar sistemas de segurança para grandes empresas.



4.4 Vladimir Levin

Proveniente da Rússia, onde atualmente se concentram um grande número de piratas cibernéticos, Levin passou a fazer parte da lista de *Hackers* famosos quando penetrou no sistema de segurança dos computadores do Citibank e desviou alguns milhões de dólares das contas de clientes deste conceituado banco. Quando estava quase embarcando de volta ao seu país, foi preso pela Interpol no aeroporto de Londres. Em seu processo, Vladimir recusava todos os advogados públicos que eram oferecidos para defendê-lo, afirmando sempre que os mesmos eram, na verdade, agentes secretos prontos para espioná-lo. Sua pena também não foi divulgada pela mídia.



4.5 Robert Morris

Na condição de filho do principal encarregado do *National Computer Security Center*, rapaz inteligente e com futuro promissor, Robert ficou conhecido nos meios jornalísticos por contaminar a Internet, propositalmente, com um vírus de nome “*Worm*” (minhoca). Em pouco tempo, inúmeros computadores foram infectados e entraram em pane. Em seu julgamento, Robert afirmou que a contaminação não tinha sido intencional, mas pagou seu erro com uma pena



relativamente rigorosa, sendo condenado a cinco anos de prisão com direito a liberdade condicional. Hoje, as Worms voltaram à moda e são largamente disseminadas através da Internet, propagando-se e contaminando computadores em massa, principalmente via e-mail.

4.6 Kevin Poulsen

Em 1990 a Rádio KIIS-FM, de Los Angeles, Califórnia, EUA, estava oferecendo um Porsche para o autor da centésima segunda chamada telefônica do dia. Kevin assumiu o controle de todas as ligações feitas e colocou sua ligação como se fosse a centésima segunda e levou o ambicioso prêmio. Mais tarde, foi preso por invadir computadores operados por agentes do FBI. A vida de Poulsen inspirou o jornalista Jon Littman a escrever o livro *"The Watching"*.



4.7 Tsutomu Shimomura

Tsutomu Shimomura trabalha no *San Diego Super Computer Center* nas áreas de Física Computacional e Segurança da Informação. Em 1995 ele ajudou muitas companhias ligadas à Internet à capturar Kevin Mitnick, que tinha roubado software e e-mails dos computadores de Shimomura. Autor do livro *Takedown: The Pursuit and Capture of America's Most Wanted Computer Outlaw -- By The Man Who Did It, with John Markoff* (Hyperion, January 1996).



5. Países

5.1 Brasil

Os modernos conhecimentos, nutridos com maciças doses de reportagens diárias por parte da mídia, e o crescimento cada vez maior dos milhões de fanáticos pelo “ciberespaço”, são as substâncias que dão poder e refúgio ao *underground Hacker* da grande rede, principalmente porque, ao que parece, o Brasil despertou definitivamente para esta nova era tecnológica.

Esta influência transformada em poder é muito grande. Basta ler jornais e revistas, assistir à televisão e ouvir rádio, para se ter conhecimento das notícias constantes sobre a invasão de *Hackers* e *Crackers* aos sistemas de segurança mais bem

montados que existem, como é o caso quase que diário da CIA, Pentágono, bancos e grandes empresas. Tudo isso é feito através da Internet.

A todo momento, dinheiro é desviado de contas bancárias. Informações valiosas, como pesquisas científicas, projetos bélicos, desenhos industriais e navais, documentos de repartições públicas, são roubados. Não há nenhum exagero nestas afirmações. Também aqui, em nosso país, existem milhares de casos de invasões, mas somente agora há divulgação por parte da mídia[M@RCIO, 2000].

5.2 Estados Unidos

Há algum tempo, o assunto era polêmico. Na época, o termo *Hacker* se encontrava associado à piratas digitais, invasores de sistemas e criminosos. Isso, graças ao maior país do mundo, que, ao invés de aproveitar os seus talentos, colocava crianças inteligentíssimas atrás das grades, somente por terem feito algum tipo de incursão, mesmo sem causarem nenhum prejuízo material ou econômico. Atualmente alguns países desenvolvidos aproveitam os conhecimentos de *Hackers* com intenções diversas e, às vezes, até óbvias.

5.3 Israel

Por acaso você já parou para fazer uma análise sobre os motivos em que os israelenses têm para contratar os grandes *Hackers* do mundo ? Esses *Hackers* já cumpriram pena ou sofreram algum tipo de discriminação em países como Estados Unidos e França mas são recebidos de braços abertos ou até mesmo como gênios em Israel, que oferece ótimos salários e condições tecnológicas de última geração, com todo o apoio necessário.

6. Segurança

6.1 Segurança Física

Devemos atentar para ameaças sempre presentes, mas nem sempre lembradas: incêndios, desabamentos, relâmpagos, alagamentos, problemas na rede elétrica, acesso indevido de pessoas no CPD, treinamento inadequado de funcionários e etc...

Medidas de proteção física, tais como serviço de guarda, uso de *no-breaks*, alarmes e fechaduras, circuito interno de televisão e sistemas de escuta são realmente uma parte da segurança de dados. As medidas de proteção física são frequentemente citadas como “segurança computacional”, visto que têm um importante papel na prevenção dos problemas citados no parágrafo anterior.

O ponto-chave é que as técnicas de proteção de dados, por mais sofisticadas que sejam, não têm serventia nenhuma se a segurança física não for garantida.

Por mais seguro que seu ambiente seja, ele não estará cem por cento seguro se a pessoa que deseja invadir seu sistema tiver acesso físico ao mesmo.

6.2 Segurança Lógica

Esta requer um estudo maior, pois envolve investimento em softwares de segurança ou elaboração dos mesmos.

Um recurso muito utilizado para se proteger dos “bisbilhoteiros” da Internet é a utilização de um programa de criptografia que embaralha o conteúdo da mensagem de modo que ela se torna incompreensível para aqueles que não sejam o receptor ou emissor da mesma.

6.2.1 Senhas

Uma senha fácil de se deduzir é a causa mais comum dos problemas de segurança. Se você não souber como trocar sua senha, coloque essa tarefa como item número um da sua lista de coisas a aprender. Você nunca deve criar senhas tomando por base o seu próprio nome, mesmo que seja o seu nome de trás para frente. A senha também não pode ser fácil de adivinhar, como o nome do marido ou da mulher, do namorado ou namorada, do seu cão, a placa do carro, a rua onde mora, a data do nascimento ou outra informação conhecida. Os *Hackers* costumam usar os programas e dicionários online para adivinhar expressões como, por exemplo, “dedicação”.

Como podem ser as senhas então ? Não há pistas, certo ? Pois bem, seja criativo. Pegue a sua frase preferida, como “Até que a morte nos separe, querida” e utiliza a primeira letra de cada palavra: **aqamnsq**. Dessa forma, a senha não é propriamente uma palavra, mas é fácil de lembrar e difícil de adivinhar. Você pode também combinar palavras com números, o que é bem aconselhável. Mas nunca crie uma senha somente com números pois é muito fácil adivinhar.

6.2.2 Regras

Usuários

- Não usar a conta do superusuário ou administrador para outros setores / funcionários;
- Criar grupos por setores / áreas afins;
- Criar contas dos usuários de acordo com seus nomes, dentro dos grupos.

Senhas – Nunca Utilizar

- Mesmo nome de usuário, nome de login;
- Senha em branco;
- Palavras óbvias, tais como: “senha”, “pass” ou “password”;
- A mesma senha para diversos usuários;
- Primeiro e último nome do usuário;
- Nome da esposa / marido, pais ou filhos;
- Informação sobre si mesmo, tais como: placa do carro, data de nascimento, telefone, CPF, etc;
- Palavra com menos de seis caracteres.

Senhas – Sempre Usar

- Letras maiúsculas e minúsculas;
- Palavras com caracteres não alfabéticos como números ou sinais;
- Fácil de lembrar para não ter que escrever;
- Fácil de digitar, sem ter que olhar o teclado [OLIVEIRA, 2000].

7. Ferramentas de Segurança

7.1 Firewalls

Quando o assunto é segurança, uma das primeiras ferramentas mencionadas é o Firewall, no sentido amplo, ele nega o acesso de usuários não autorizados a um determinado *host* ou arquivo, em sentido restrito, ele examina cada pacote e determina a origem, se está em uma lista aprovada ele permite o acesso, senão, não permite o acesso. Já numa definição mais usual ele é uma barreira de proteção entre duas redes, geralmente, ele fica entre uma rede local e a Internet.

Firewall é o equipamento que garante o controle da conexão entre duas ou mais redes, ou seja, é um equipamento que roda uma aplicação específica de controle de acesso e que é responsável por interligar, de forma segura, duas ou mais redes, garantindo o controle, a verificação e o log (auditoria) dos pacotes que passam entre elas. Seu nome foi originado das paredes corta-fogo, existentes para impedir a passagem do fogo em prédios.

Firewall filtra os acessos feitos da empresa para a Internet, e da Internet para a empresa. Apesar de ser uma ferramenta de extrema importância para a proteção da empresa de acessos indevidos externos, a utilização dele isoladamente não garante segurança. A solução seria implementar duas medidas de segurança, Política e Controle. A empresa deve ter uma Política de Segurança que descreve o papel dos recursos de Tecnologia da Informação dentro da empresa, e elaborar mecanismos para controlar estas políticas.

Isto mostra que o Firewall protege a rede interna de ataques externos, mas não de ataques internos. Além disso, o Firewall quando instalado corretamente é uma barreira contra ataques, mas caso o invasor consiga quebrar a segurança do Firewall ou este estiver mal configurado, o invasor terá acesso ao sistema.

7.2 Sistemas de Detecção de Intrusos

São sistemas inteligentes, capazes de detectar tentativas de invasão em tempo real. Estes sistemas podem apenas alertar sobre a invasão, como, também, aplicar ações necessárias contra o ataque. Eles podem ser sistemas baseados em regras ou adaptáveis, no primeiro as regras de tipos de invasões e a ação a ser tomada são previamente cadastradas. O problema é que a cada dia surgem novos tipos de ataques e estas regras precisam estar sempre atualizadas para o sistema ser realmente eficaz. No segundo tipo, são empregadas técnicas mais avançadas, inclusive de inteligência artificial, para detectarem novos ataques, sempre que surgirem.

7.3 Logs

Logs são registros gerados pelos sistemas ou aplicações, sobre informações de eventos ocorridos. É considerado uma medida básica de segurança, mas muitas vezes não é utilizado pelos administradores, ou porque está desativado, pois dependendo do sistema e do hardware, a geração do Log pode se tornar lenta, ou porque esquecem ou não querem analisá-lo, já que os logs geralmente são relatórios enormes. Mas é uma ferramenta útil para auditorias de acesso, verificação do que está sendo utilizado, possível falha nos sistemas, entre outros.

7.4 Antivírus

Software que verifica a existência de vírus em uma máquina, pasta, arquivo e ao encontrá-lo, executa a limpeza. A maneira como ele fará isso pode ser totalmente configurada pelo usuário. O padrão é o antivírus analisar e quando encontrar algum vírus, tentar eliminar apenas o vírus, caso não consiga, se o usuário autorizar, ele removerá o arquivo também. Uma vez instalado o antivírus em um micro, ele pode ser configurado, dependendo da sua característica, para ficar ativo e analisar tudo o que for aberto no micro, caso apareça algum vírus, ele avisa imediatamente. Mas como diariamente surgem novos tipos de vírus, é importante o usuário ficar atento e atualizar o seu antivírus sempre que possível.

7.5 Backup

Uma das ferramentas existentes para segurança dos dados são os softwares de *backup* e *restore*, que servem para fazer cópias de segurança das informações e de sistemas de uma empresa e recuperar as informações quando necessário. Todos os dados e sistemas de uma empresa devem possuir cópias de segurança íntegras, atuais e armazenadas em local seguro. Em geral, o backup é feito em fita, disquete ou outra mídia portátil que pode ser armazenado para futura utilização, como no caso de algum desastre ou perda de informações. As informações podem ser perdidas por causa de acidentes, desastres, ataques, erros de sistema ou hardware ou falha humana, entre outros motivos. Com as informações atualizadas copiadas através de backups para alguma mídia, quando houver uma perda de dados, basta restaurar estas informações.

8. Conclusão

De fato, Segurança da Informação é um assunto muito sério, e não pode ser deixado de lado. Deve ter um lugar de destaque, não apenas para as pessoas que trabalham diretamente na área de informática, como técnicos, analistas, programadores, como também para as pessoas que, de alguma forma, utilizam a informática como ferramenta para facilitar seus trabalhos, pois, a informação não tem preço. Nas palavras de Felipe Moniz⁸: “as empresas não têm discernimento entre boas e más soluções em segurança da informação”, que trazem assim graves problemas, como um HD danificado ou os perigos de um ataque.

8 Felipe Moniz: Fundador da N-Stalker Inc., empresa voltada para a Segurança da Informação. Exímio programador autodidata, construiu o software N-Stealth, considerado o melhor scanner de vulnerabilidades para servidores web da atualidade.

Referências

- [**ALEXANDRE BREDARIOL, 2001**] Bredariol, Alexandre. - "Aspectos de Segurança em Redes de Computadores: IP Security e Segurança em e-mail". Monografia – Universidade São Francisco-Itatiba, Novembro 2001, p.6.
- [**M@RCIO(VASCONCELLOS), 2001**] Vasconcellos, Márcio José Acciolo de. - "A Internet e os hackers: ataques e defesas". Chantal Editora, São Paulo, 2000, p.54-55, p.221, p.37-42.
- [**RICARDO REIS GOMES, 2001**] Gomes, Ricardo Reis. - "Crimes Puros de Informática". Monografia – Centro Universitário de Brasília, Brasília, 2001, p.10.
- [**ADRIANA APARECIDA SETTE, 2001**] Sette, Adriana Aparecida. - "Um Guia para Implementação de Segurança Básica em Sistemas". Monografia – Universidade Luterana do Brasil, Canoas, Novembro 2001, p.18-28.
- [**WILSON JOSÉ DE OLIVEIRA, 2001**] Oliveira, Wilson José de. - "Hacker – Invasão e Proteção". Bookstore Livraria Ltda., Florianópolis, Janeiro 2000, p.11-13.
- [**STEPHEN NORTHCUTT, 2000**] Northcutt, Stephen. - "Como detectar invasão em rede – um guia para analistas". Editora Ciência Moderna Ltda., Rio de Janeiro, 2000.
- [**LEANDRO CRISTOVÃO, 2000**] Cristovão, Leandro. - "Administração Remota em Delphi". Visual Books - Agosto 2000.
- [**LEANDRO CRISTOVÃO, 2000**] Cristovão, Leandro. – “Registry com Delphi – Aprenda Rápido”. Visual Books - Maio 2000.
- [**FABIO CAMARA E HUGO NOVAES, 2000**] Camara, Fabio –Novaes, Hugo. - "Delphi APIs e Sockets – A Caixa Preta das Tecnologias". Visual Books, Junho 2000.
- [**LUCIANA PALMA e RUBENS PRATES, 2000**] Palma, Luciana – Prates, Rubens. - "TCP/IP Guia de Consulta Rápida". Novatec Editora, 2000.
- [**ANDRÉ FERNANDES, 1999**] Fernandes, André. - "Delphi 5 Básico e Avançado". Editora Book Express Ltda., 1999.
- [**RODRIGO LOBO e CARLA LOBO, 2000**] Lobo, Rodrigo e Carla. - "Delphi 5 Dicas e Truques”. Editora Advanced Books, 2000.

ANEXO I

Sites Interessantes na Internet sobre Segurança da Informação

N-Stalker

<http://www.nstalker.com>

Takedown

<http://www.takedown.com>

Módulo Security

<http://www.modulo.com.br>

Info Guerra

<http://www.infoguerra.com.br>

Secure Net

<http://www.securenet.com.br>

Net Security

<http://www.net-security.org>

Buffer Overflow

<http://www.bufferoverflow.org>

InSecure Net

<http://www.insecurenet.com.br>

Security Focus

<http://www.securityfocus.com>

HideAway

<http://www.hideaway.net>

Packet Storm Security

<http://packetstormsecurity.org>

IIS FAQ

<http://www.iisfaq.com>

UNICAMP - Security

<http://www.security.unicamp.br>

ANEXO II

Filmes sobre Segurança da Informação

War Games, 1983 – Primeiro filme de redes de computadores, conta a história de um garoto que sem querer entrou no sistema de lançamento de mísseis nucleares do Governo Americano e quase causou um desastre nuclear.

Hackers – Piratas de Computador, 1995 – Grupo de *Hackers* adolescentes luta para desmascarar um vilão que iria lançar um suposto vírus na Internet.

Caçada Virtual, 2000 – Filme conta a história de Kevin Mitnick e Tsutomu Shimomura, desde o início até a prisão de Mitnick.

A Senha, 2001 – *Hacker* é contratado para colocar um vírus em um banco e roubar milhões de dólares.