SEGURANÇA NA INTERNET

Técnicas e métodos para se obter uma rede segura

Zenaide Aparecida Rios

Uberlândia, Dezembro/2000.

SEGURANÇA NA INTERNET

Técnicas e métodos para se obter uma rede segura

Zenaide Aparecida Rios

Monografia apresentada ao Curso de Ciência da Computação do Centro Universitário do Triângulo - Unit, como requisito básico à obtenção do grau de Bacharel em Ciência da Computação, sob a orientação do Prof. Clayder Cristiam Coêlho.

Uberlândia, Dezembro/2000

SEGURANÇA NA INTERNET

Técnicas e métodos para se obter uma rede segura

Zenaide Aparecida Rios

Monografia apresentada ao Curso de Ciência da Computação do Centro Universitário do Triângulo - Unit, como requisito básico à obtenção do grau de Bacharel em Ciência da Computação.

Clayder Cristiam Coêlho, Msc.	Marcos F. Resende , Msc.
(Orientador)	(Coordenador de Curso)
Alex Dias , Msc.	Eliane Teresa Borela, Msc.
(Avaliador)	(Avaliador)

Uberlândia, Dezembro/2000.

Agradeço a toda a minha família, em especial aos meus pais que me deram a oportunidade de fazer esse curso, ao meu noivo Wanderley que sempre me apoiou nos momentos difíceis.

RESUMO

A Internet é uma das maiores invenções do século XX; ela trouxe novas oportunidades e, hoje é essencial no dia a dia de cada uma das pessoas que a utilizam. Trouxe comodidade e agilidade na troca de informações entre as diversas civilizações, aproxima pessoas, mesmo estando em diferentes extremos do mundo. Entretanto, apesar de todas as vantagens que a Internet trouxe para o ser humano, um problema que vem assolando o seu desenvolvimento é a falta de segurança, que passou a ser mais observada e mais exigida nos últimos anos com o aumento de transações comerciais, na Internet. O objetivo dessa monografia é apresentar o perfil que a Internet está assumindo, os serviços que ela pode oferecer, os riscos que os usuários enfrentam e, principalmente, os mecanismos de segurança existentes para evitar os transtornos causados por pessoas mal intencionadas.

SUMÁRIO

1. INTRODUÇÃO

Hoje, a globalização é uma realidade; onde é exigido de cada um de nós, quer seja indivíduo ou empresa, competitividade, dinamismo, rapidez e domínio da informação, o que torna qualquer ação ou negócio um sucesso, independente da finalidade a que se é destinada.

Às portas do novo milênio, estamos sendo testemunhas e, ao mesmo tempo, participantes de um dos maiores fenômenos de expansão tecnológica que é a INTERNET: a rede das redes que interliga computadores em todo o mundo, com acesso rápido a informações e a comodidade de negociar via on-line, influenciando diretamente no comportamento e hábitos do usuário.

A Internet quebrou as últimas barreiras ou restrições das diversidades culturais que ainda resistiam à globalização, trazendo à tona um mercado consumidor de produtos, lazer, tecnologias e informações cada vez mais trocadas via computador.

Com o aumento do uso da Internet no dia a dia, surge também o problema da fragilidade da segurança que, muitas das vezes, é violada por intrusos de qualquer parte do mundo, tornando o uso de mecanismos de segurança cada vez mais essenciais para empresas e, até mesmo, para usuários comuns.

Hoje, o saber é armazenado na Internet. As novas tecnologias de informação tocam para frente a expansão das redes e modificam profundamente a economia e a sociedade. Informação mais comunicação é igual a conhecimento, que na sociedade é futuro; é a "www" (World Wide Web).

Através da Internet tornou-se possível acessar bancos, fazer movimentação financeira e transações econômicas quer seja de vendas ou compras, sem o inconveniente de perda de tempo na mobilidade para tal.

Com toda essa transmissão de conhecimento on-line, revela-se a fragilidade a que todos somos submetidos: a privacidade é ameaçada por pessoas mal intencionadas, que a cada dia usam técnicas novas e mais sofisticadas para driblar a segurança na rede e causar prejuízos irreparáveis, tornando evidente a necessidade de se desenvolver técnicas de proteção mais seguras e sem falhas, para que haja maior controle desses acessos indevidos.

No capítulo 1, há uma pequena introdução sobre a Internet. Em seguida, no capítulo 2, há uma breve discussão sobre a história da Internet, como ela surgiu, quais os serviços oferecidos por ela e como ela se encontra no Brasil e no mundo.

No capítulo 3, faz-se uma descrição dos tipos de acessos indevidos a que a rede está sujeita, como são feitos e por quem são executados.

O capítulo 4 refere-se aos mecanismos de segurança que podem ser usados para garantir a integridade e a confiabilidade da rede, para empresas e usuários domésticos.

O capítulo 5 faz um estudo de casos ocorridos sobre ataques de hackers, seguido de uma conclusão.

2- HISTÓRICO DA INTERNET

Neste capítulo será apresentado um breve histórico da Internet, o perfil e também dados atuais sobre o seu uso, além da abordagem sobre o seu surgimento, atuação e tendências.

2.1- Definição

Uma rede de computadores pode ser definida como a interligação física e lógica entre dois ou mais computadores, onde a interligação física se estabelece entre interfaces de comunicação conhecidas como placas de rede ou placas de modulação-demodulação, também chamados de "modems". A interligação lógica é feita pelos softwares de comunicação e envolve um conjunto de protocolos, especialmente desenvolvidos para este fim.

INTERNET é definida como diversas redes de computadores conectadas umas às outras. É considerada uma rede de redes, formada por redes universitárias, comerciais, militares e científicas conectando computadores do mundo inteiro.**[4]**

A Internet é uma única rede que engloba milhares de outras redes menores, por isso é conhecida como a "rede das redes", e tem um domínio mundial. É o conjunto de todos os computadores do mundo interligados. Dela fazem parte: governo, empresas, universidades, escolas, e principalmente, computadores pessoais. A Internet também é constituída por computadores chamados de servidores, onde são armazenadas as informações, e por vários outros equipamentos e linhas telefônicas que servem para interligar os computadores e rotear as informações.

A comunicação oferecida pela Internet a seus usuários é de baixo custo e de rápido acesso a infinitos tipos de informações; ela é o ponto que une todo o mundo, independente da distância e da língua falada no país.

Os sites da Web são uma maneira fácil e rápida de disponibilizar informações sobre diversos assuntos, projetos e empresas; suas possibilidades são quase que infinitas, contudo podemos encontrar informações completamente sem importância, desnecessárias e outras extremamente importantes.

2.2- História da Internet

A Internet surgiu durante a Guerra Fria, onde existia uma corrida tecnológica entre as grandes potências.

Os EUA foram os precursores dessa técnica, que criou em 1969 a ARPANET- *Advanced Reserch Projects Agency* (Agência de projetos e Pesquisas Avançadas) controlada pelo departamento de defesa do país, cujo acesso só era permitido a pesquisadores, cientistas e engenheiros.

Em 1980, a rede ARPANET foi dividida em dois seguimentos: a ARPANET e a MILNET. A MILNET concentrou-se nas operações militares; tinha a função de desenvolver uma tecnologia que garantisse a comunicação no caso de surgir uma guerra, eles precisavam transmitir dados à distância e manter esses dados a salvo, no caso de uma das bases serem destruídas. A ARPANET, que posteriormente foi substituída por DARPANET- *Defense Advanced Research Projects Agency Internet*, passou futuramente a ser chamada só de Internet.

As redes de computadores surgiram numa época em que a relação entre o usuário e o computador não era tão atrativa como hoje; suas interfaces eram à base cartões perfurados com códigos binários, sendo responsáveis pela relação homem e máquina. Contudo, essa rede hoje agrega aproximadamente 380 milhões de pessoas e vem crescendo a cada mês, pelo custo que pode ser de uma ligação telefônica local.

Atualmente, as empresas mundiais fizeram modificações no seu modelo tradicional de empresa para um modelo mais atualizado ao mundo da informática, adequando-se melhor à realidade da Internet, e garantindo sua sobrevivência e competitividade no mercado. A forma antiga de se fazer negócios vem, cada vez mais, sendo substituída pelos negócios eletrônicos.

2.3- Internet no Brasil

A Internet é um dos grandes fenômenos atualmente no Brasil e no mundo, revolucionando as telecomunicações e influenciando na maneira de viver e de pensar das pessoas. Hoje é possível, a partir de um computador pessoal, visitar e conhecer virtualmente lugares e pessoas em todas as partes do mundo, visitar museus, por exemplo, e adquirir um número maior de informações para o dia a dia. O mais importante é que, para tudo isso, só é preciso estar conectado à grande rede através de um computador e uma linha telefônica.

Desde 1989, as Universidades brasileiras estão ligadas à rede de computadores mundiais, os quais

tinham ligação com a Bitnet, uma rede semelhante à Internet cujos serviços se restringiam a correio eletrônico e transferência de arquivos.

Em 1995, o Ministério das Comunicações e o Ministério da Ciência e Tecnologia resolveram lançar uma rede integrada entre as instituições acadêmicas e comerciais, que deu origem a vários fornecedores de acesso e serviços privados no Brasil.

O crescimento da Internet no Brasil está sendo bem satisfatório, pois a infra-estrutura brasileira em telecomunicações tem melhorado muito atualmente; o acesso à Internet está ficando mais barato, rápido e acessível à grande maioria da população, uma vez que o uso do computador está se tornando cada vez mais comum entre as pessoas.

2.4- Internet no mundo

O número estimado de usuários da Internet em todo o mundo até o fim desse ano é estimado em 374,9 milhões. **[9]**

A Internet vai continuar crescendo e no final conquistará a maioria da população mundial. Hoje, já existem quase 140 milhões de usuários da Internet nos Estados Unidos e no Canadá e 84 milhões na Europa.

Segundo a pesquisa da Angus Reid Group e Columbus Group, 70% dos adultos canadenses acessam a Internet e, até o ano passado, esse número chegava aos 55%. A expectativa é de que, em breve, esse número ultrapasse os 80%. **[11]**

A figura 1 apresenta um quadro demonstrativo de como e quanto a Internet vem se desenvolvendo no mundo.

Ranking	País	Número de Internautas até o fim de 2000 (em milhões)	%
1	EUA	135,7	36,2
2	Japão	26,9	7,18
3	Alemanha	19,1	5,18
4	Reino Unido	17,9	4,77
5	China	15,8	4,20

6	Canadá	15,2	4,05
7	Coréia do sul	14,6	3,95
8	Itália	11,6	3,06
9	Brasil	10,6	2,84
10	França	9	2,39
11	Austrália	8,1	2,16
12	Rússia	6,6	1,77
13	Taiwan	6,5	1,73
14	Holanda	5,4	1,45
15	Espanha	5,2	1,39
TOTAL MUNDIAL 374,9 Milhões			

Figura 1 – Estimativa de usuários da Internet **[9]**

De acordo com o Estudo da Between and MT&T, o número de italianos conectados à rede vem crescendo muito. O número de internautas italianos de setembro do ano passado até agora aumentou 36%, atingindo 11,6 milhões de usuários conectados à rede Web. Segundo a pesquisa, existe uma grande probabilidade desse número dobrar no próximo ano, pois 15,8 milhões de italianos pretendem se conectar à rede nos próximos doze meses**. [12]**

Em Cuba, de acordo com o governo, existe um computador para cada cem habitantes e cerca de quarenta mil pessoas estão acessando a rede, e se levássemos em conta os estudantes e turistas da ilha, esse número chegaria a 60 mil internautas. Cuba possui quatro provedores de acesso à Internet, mas o serviço continua caro e limitado. Os usuários que desejam navegar na Web têm que provar que estão engajados em alguma pesquisa ou que pertencem a notórias instituições. Mesmo com esses obstáculos, o Governo pretende iniciar um programa que vai prover acesso à rede a 150 clubes de jovens e mais de duas mil agências de correio. **[13]**

De acordo com o Centro de Informação da Internet da China, apenas nos primeiros seis meses deste ano, quase nove milhões de chineses se conectaram a Web; eles já são 16,9 milhões de internautas.

2.5- Serviços oferecidos pela Internet

Hoje, através da Internet, pode-se resolver quase tudo sem sair de casa, porque ela oferece inúmeras opções para isso. Um exemplo prático é o serviço bancário que, há um tempo atrás, gastaria

horas dentro de um banco com filas enormes. Atualmente, pode ser resolvida on-line e é oferecido por quase todos os bancos. O cliente tem a comodidade de fazer transações como transferências, investimentos, pagamentos de contas no aconchego de seu lar ou até mesmo no seu trabalho e, para garantir a segurança de dados, é usada a criptografia.

Existem vários tipos de serviço oferecidos pela Internet, seria quase que impossível citar todos, por isso serão enumerados os mais comuns e utilizados.

- **www (World Wide Web)**

A www nasceu em 1991 no Laboratório CERN na Suíça pelo seu criador Tim Bernes-lee, que a concedeu unicamente como uma linguagem que serviria para interligar computadores do laboratório a outras instituições de pesquisas e exibir documentos científicos de forma simples e fácil acesso.

A www (W3 ou simplesmente Web) também é conhecida como a teia mundial de informações. É nela que circulam as informações de multimídia como som, imagem e vídeo. É a área da Internet que contém documentos em formato de hipermídia, que é uma combinação de hipertexto com multimídia. Os documentos hipermídia da www são chamados de páginas de Web e podem conter textos, arquivos de vídeo, imagens e arquivos de áudio e também ligações com outros documentos na rede. A característica mais marcante da Internet é a multimídia.

A Web vista como um todo é um sistema distribuído que armazena informações em vários computadores, onde o documento tem muitos vínculos, o que torna a Web mais interessante, acessível e intuitiva.

O usuário, após conectar a Internet, navega na www através do software Browser, onde tem-se destacado o Netscape Navigator e o Microsoft Internet Explorer, os líderes de mercado com uma disputa acirrada entre si.

Cada Home-page tem um endereço próprio que não pode ser igual a outro, conhecido como URL (Uniform Resource Locator). A URL consiste em: nome, diretório, máquina onde está armazenado e o protocolo pela qual deve ser transmitido.

A www tem um forte impacto também dentro das empresas, através do serviço de Web interna, a Intranet, que pode ser definida como uma maneira de conduzir o funcionamento interno de uma empresa.

- **E-mail (Correio Eletrônico)**

Serviço para troca de mensagens entre usuários, é a forma mais popular de comunicação na Internet. Não é necessário

que o destinatário esteja conectado à rede no momento que a mensagem chegar. Um aviso indicando quantas mensagens novas existem será apresentado na tela, assim que o usuário conectar-se ao sistema. Podemos enviar várias cópias de uma mesma mensagem para várias pessoas e também guardar as mensagens enviadas.

É o serviço mais utilizado na Internet, onde os usuários trocam mensagens entre si, e para isso é necessário a utilização de softwares específicos. Atualmente, no mercado, encontra-se vários desses softwares, com destaque para o Eudora, para o Outlook Express que é distribuído com o Microsoft Internet Explorer ou o Netscape Messenger, distribuído com o pacote Netscape Navigator .

O endereço eletrônico de e-mail é formado por um apelido do usuário, seguido de @ (arroba) e do nome do domínio e do provedor de acesso, como por exemplo **wawa@bol.com.br.**

Apesar da comodidade e da facilidade de comunicação entre pessoas em várias partes do mundo, oferecidas pelo e-mail, a sua maior desvantagem é um certo desconforto gerado por mensagens indesejadas do tipo mala direta, chamadas de "spams", que aparecem nas caixas de e-mail, com mensagens indiscretas, ofensivas, terminando por congestionar à rede e os servidores.

- **Chat**

"Chat" é um termo americano que quer dizer bate-papo. É um serviço simultâneo de conversa entre diversas pessoas, que trocam mensagens, em tempo real, através do teclado de seu computador. São lugares onde se pode fazer novos amigos, ou até mesmo viver uma grande história de amor, como pode ser visto em algumas reportagens.

O *Chat* na Internet ficou famoso através dos servidores de IRC (Internet Relay Chat), onde são criadas as várias salas ou canais para abrigar os usuários.

O IRC é um sistema de conversa por computador em que várias pessoas podem participar, ao mesmo tempo, em canais dedicados a assuntos específicos.

- **Comércio Eletrônico**

Comércio Eletrônico significa comercializar eletronicamente; envolve todas as formas de transações entre indivíduos e organizações, baseadas no processamento e transmissão eletrônica de dados. Essas transações, nas quais as partes envolvidas se comunicam e interagem eletronicamente, integram a cadeia de valores das organizações além das fronteiras usuais.

Comércio Eletrônico tem várias definições que giram sempre em torno das idéias de transações de negócios por meio eletrônico. Abaixo, tem-se algumas delas: **[7]**

“Fazer negócio eletronicamente.”. (Information Society Project Office)

“E-Comm abrange um amplo espectro de atividades econômicas, da comercialização de bens e serviços aos contratos e pagamentos por eles.”. (Datapro)

“Todas as formas de transações comerciais envolvendo indivíduos e organizações que são baseadas no processamento e transmissão eletrônica de dados.”. (OECD, ICCP)

“Transação onde as partes envolvidas se comunicam e interagem fronteiras usuais.”. (G. Merdian)

O comércio Eletrônico é um investimento que não tem retorno imediato; é necessário um investimento e esperar um tempo para colher os frutos desejados. O marketing e a divulgação da corporação não possuem um custo alto; a Website de uma empresa atinge o usuário diretamente com qualidade melhor ou igual aos outros meios de comunicação. É o canal mais moderno e simples de vendas, não envolve pesados recursos de investimentos ou de pessoal e pode ser acessado com rapidez, simplesmente usando a Internet.

A base do crescimento do Comércio Eletrônico é a mudança de hábitos dos empresários e consumidores com a popularização da Internet. O consumidor tem acesso a uma base de dados reais, com recursos de multimídia, com imagens que despertam a atração e a motivação do cliente em adquirir um determinado produto com rapidez e mais comodidade, pois não precisará sair de sua casa.

Uma grande atração da rede para os fabricantes é a possibilidade de comercializar produtos mundialmente. A facilidade de acesso ao consumidor poderia fazer com que a distribuição direta se transformasse em regra, deixando de ser uma exceção.

Um outro aspecto que chama a atenção é relativo aos impactos na maneira pela qual as empresas se comunicam com os seus clientes. Deverá haver um redirecionamento na maneira de se relacionar com o mercado. A propaganda, a pesquisa de mercado e o marketing em geral deveriam mudar sua forma de atuação, saindo da veiculação de massa para a veiculação dirigida.

Vantagens do comércio eletrônico sobre o comércio tradicional

- O cliente tem mais opções de escolha e customização.
- Diminui o tempo e o custo de busca e escolha, tanto para o cliente, como para os fornecedores.
- Melhora a eficiência em atender o cliente, incluindo a entrega por demanda.
- Diminui os altos custos envolvidos em transporte, armazenamento e distribuição.
- Facilita a produção e o pagamento.

- Expansão de mercados locais e regionais para nacionais e internacionais, com níveis mínimos de capital.

Como atrair o cliente on-line

Para atrair os clientes, observam-se as técnicas que todos os sites da rede usam. Algumas regras que podem ajudar a conquistar os clientes:

- Manter o site sempre atualizado.
- O site tem que ser simples, fácil de operar e, principalmente, passar para o cliente profissionalismo, segurança e confiança.
- O site deve tornar fácil o acesso aos produtos específicos, usando um botão de procura em toda página, assim os cliente podem achar rapidamente o que procuram.
- Construir páginas que carreguem rapidamente.
- Manter os preços on-line iguais ou abaixo dos disponíveis em outros sites.
- Procurar vender produtos que as pessoas querem comprar on-line.
- Mostrar ao cliente que as transações são seguras.

Os vendedores e analistas dizem que transações no comércio eletrônico são mais seguras que nas compras com cartão de crédito no mundo real. As fraudes de cartão de crédito são realizadas no varejo por vendedores que manipulam os números do cartão de crédito. Os sistemas de comércio eletrônico removem essa tentação, codificando os números nos servidores de uma companhia O problema é que os clientes não acreditam nessa tese.

O *E-commerce* traz, além da comodidade e rapidez nas compras, algumas outras vantagens tanto para o consumidor como para a companhia: o custo para a busca de informações cai, sem contar que o *E-Commerce* é global. Os preços caem, porque vai haver uma competição no mercado e o consumidor terá novas oportunidades de negócios. Com todas essas e outras vantagens ainda não se sabe se o ato de comercializar na Internet é seguro.

A questão da segurança no comércio eletrônico é muito discutida. É seguro fornecer o número do cartão de crédito pela Internet? Essa é a pergunta mais freqüente que um usuário se faz quando resolve fazer compras on-line. Pode ser perigoso, mas não se pode esquecer que a insegurança não está relacionada somente ao ato de comercializar eletronicamente e, sim, a qualquer lugar no dia a dia de cada pessoa. Quando se faz compras em uma loja, jantar em um restaurante ou mesmo o simples fato de ir a um posto de gasolina abastecer o carro, se está sujeito a fraudes, pois o cartão de crédito é entregue a pessoas desconhecidas e não se sabe o que eles estão fazendo com o cartão. O mesmo acontece quando compra-se alguma coisa pelo telefone, quando se enviam cartões-resposta comercial pelo correio ou utilizam-se os serviços on-line de um banco. Isso não será tão perigoso quanto fazer compra pela Internet?

O mundo está cheio de pessoas mal intencionadas por isso todo cuidado é pouco, lembre-se sempre de que a decisão e a responsabilidade de quando, como e onde usar o seu cartão é sua. Quando for usar o seu cartão seja por telefone, Internet ou no seu cotidiano, existem cuidados que devem ser sempre obedecidos. É sempre bom verificar se a empresa com quem se está negociando é idônea, confiável; cuidados com sites que oferecem fotos eróticas (eles são os campeões em picaretagem). Escolha sempre fornecedores de boa reputação e de confiança, que você poderá assim, estar evitando muitos

problemas.

Para garantir a segurança no Comércio Eletrônico são usados sistemas criptográficos, que nem sempre são perfeitos, como se pode ver em noticiários o caso de várias mensagens que foram decifradas. No caso dos navegadores, o limite para exportação está fixado em 40 bits, o que não se considera completamente seguro para aplicações de internet-banking, por exemplo. A segurança das chaves aumenta geometricamente com o número de bits. Por isso, uma chave de 64 bits é milhões de vezes mais segura que a de 40 bits. **[7]**

O comércio eletrônico para os consumidores está em fase de amadurecimento. Muitos clientes ainda não se sentem seguros para realizar uma compra on-line, apesar de existirem mecanismos para garantir essa segurança.

Os princípios básicos da segurança são a confiabilidade, integridade e disponibilidade de informações, reduzindo riscos com vazamentos, fraudes, erros, uso indevido, sabotagens, roubo de informações e maior controle sobre os recursos da informática.

- **FTP**

O FTP (File Transfer Protocol) significa Protocolo de Transferência de Arquivos. É a maneira usada para transferir um arquivo independente, seja ele um texto, uma foto, uma home page ou um programa de um computador distante para o seu micro ou vice-versa. A FTP só permite a transferência de arquivos completos.

O FTP é feito através de programas específicos, cujo funcionamento é muito parecido. Você se conecta à Internet e inicia o seu software de FTP como faria com o seu navegador, informa o nome do servidor ao qual deseja se conectar, entra nos diretórios de seu interesse, seleciona o arquivo desejado e o transfere para o seu computador.

O servidor de FTP permite a qualquer usuário enviar ou receber arquivos em diretórios especialmente disponibilizados para esse fim. Para operar uma transferência de arquivos entre um servidor e um computador local, basta conectar o seu computador local à rede Internet, e após esta conexão ter sido efetivada o usuário deve ativar no seu computador local um software ***FTP client***. Num servidor FTP, os diretórios disponibilizados para usuários anônimos são separados de outros diretórios, de modo a evitar que usuários anônimos tenham acesso, ou venham a causar danos a outros diretórios, que são normalmente utilizados por ***usuários registrados.*** **[8]**

- **Listas de discussão**

Serviço que permite o intercâmbio de mensagens entre diversos usuários. Funciona como se fosse uma extensão do correio eletrônico. Utilizados para a comunicação de um grupo de pessoas com interesses comuns em um determinado assunto. Qualquer usuário da Internet pode se cadastrar nestas listas e enviar mensagens para as mesmas, permitindo aos internautas realizarem negócios, trocar conhecimentos e informações.

- **Gopher**

É uma ferramenta baseada em menus que possibilita ao usuário buscar e recuperar informações distribuídas por diversos computadores da rede. Através do Gopher, o usuário tem acesso tanto a informações armazenadas localmente, como àquelas armazenadas em qualquer outro computador da rede que aceite esse serviço.

Para usar esse serviço é necessário instalar um programa cliente Gopher no seu computador, ou ter acesso via Internet a "mainframe", onde isso tenha sido feito.

- **IRC**

O IRC (Internet Relay Chat) é um tipo de bate-papo semelhante às salas de Chat, porém utilizando um programa cliente próprio. Um servidor IRC possibilita a hospedagem e gerenciamento de mensagens emitidas em tempo real pelos seus participantes.

2.6- Acesso à Internet

O acesso à Internet é simples, basta para isso se ter uma linha telefônica comum para pessoas fisicas ou uma linha privativa, no caso de grandes empresas e um computador.

A comunicação com todos os outros computadores que estejam na rede é feita através dos provedores de acesso. Tais provedores (ou ISPs-Internet Service Provide), podem ser organizações governamentais ou não-governamentais, comerciais e até educacionais, cuja função é fornecer o acesso à rede, cuja função é fornecer acesso a rede.

Quando um usuário acessa um computador na França, Japão ou em qualquer outro país, ele não paga nenhum adicional por isso: o acesso à Internet permite o direito de transferência de dados disponíveis na rede, independente da distância de onde venham os dados, lembrando que, ao acessar à Internet por um provedor, você terá acesso a todos os outros provedores e a todas as redes da Internet.

O custo da Internet varia de acordo com a conexão. Conexões através de uma linha telefônica comum, chamadas de conexões discadas, são mais baratas e são mais usadas para usuários domésticos e pequenas empresas; já as grandes empresas que necessitam de maior velocidade e têm um volume maior de informações para receber e enviar, usam as conexões dedicadas que são mais caras, porém mais rápidas e permanentes , sendo mais adequadas na transmissão de dados.

O acesso discado é o tipo de acesso dos usuários comuns. Para utilizá-lo, é necessário um computador, uma linha telefônica e um "modem". O usuário utiliza o computador para fazer a ligação até o fornecedor de acesso. Ao ser recebido pelo computador do fornecedor de acesso, deve fornecer seu nome de usuário e senha para poder entrar no sistema.

O acesso dedicado é uma forma de acesso à Internet, no qual o computador fica conectado permanentemente com a

rede. Normalmente, o acesso dedicado é utilizado por empresas que vendem acesso a serviços aos usuários finais. Empresas de grande porte também estão conectando suas redes internas de forma dedicada à Internet. Todos os servidores encontrados na rede, como Web sites e servidores de FTP, mantêm uma ligação permanente para que os usuários possam acessá-los a qualquer momento. Nesse tipo de ligação, o computador recebe um único endereço pela qual pode ser localizado.

2.7- Uma nova tendência

Uma nova tendência da Internet no Brasil é a chegada da tecnologia WAP- Wireless Aplication Protocol (Protocolo de Aplicações sem fio) aos telefones móveis, onde as pessoas não vão consultar enciclopédia, é claro, mas receberão informações e serviços rápidos. Porém, é importante salientar que a Internet com PCs ainda é o melhor meio de troca e interação de informações.

No Brasil, isso já está se tornando realidade, pois, já faz parte dos projetos imediatos de praticamente todos os bancos brasileiros. A primeira aproximação entre comunicação móvel e Internet aconteceu por meio do serviço de mensagens curtas via celular, o SMS, onde as pessoas passaram a ler recados, notícias e extratos bancários no visor do seu aparelho celular.

Segundo o presidente da Ericssom no Brasil, Gerde Weise, "A Internet sem fio vai mudar para melhor o trabalho e a vida das pessoas.". **[3]**

Na Europa, o serviço é muito popular e chega a 2 milhões de mensagens por mês. **[3]**

O WAP permitirá o acesso à Internet que, normalmente, é feito por um portal da Web. Ela é uma especificação global, isto é, um conjunto de tecnologias que permitem aos donos de aparelhos sem fio, incluindo celulares, PDAs, rádios, pagers, acessar e interagir com serviços e informações da Internet. Essa idéia começa a ser desenvolvida em conjunto, pela Phone.com, Ericsson e a Nokia .

Segundo o Forrester Institute, por volta de 2004, um terço de todos os usuários de celulares da Europa, mais de 219 milhões de pessoas, estará usando seus telefones para acessar serviços na Internet. **[3]**

No Brasil, estima-se que os terminais WAP devam chegar a 1,5 milhão até o fim desse ano. **[3]**

2.8- Conclusão

Com a velocidade em que a Internet está chegando às empresas e, sobretudo aos lares dos consumidores, não existe momento melhor que esse para sua empresa fazer parte desta revolução do mercado brasileiro e mundial.

Apesar de todos os pontos positivos que a Internet traz para os usuários, infelizmente a segurança é um ponto a ser considerado com grande atenção. No capítulo 3, será apresentado um panorama geral sobre a falta de segurança na rede, quais são e quem pratica esses ataques.

3- INSEGURANÇA NA REDE

Um dos principais problemas da Internet é a vulnerabilidade a que a rede está exposta. Nesse capítulo, será apresentado uma espécie de guia que conterá alguns dos riscos a que se está sujeito, formas de identificá-los, principais formas de invasões e incidentes provocados por tais riscos.

3.1- Panorama de acessos indevidos

A informática vem se desenvolvendo muito a cada dia; por isso, é um dos assuntos mais discutidos no momento. Atualmente, ter computador em casa ou no trabalho é algo muito comum em todo o mundo, pois ele está se tornando cada vez mais indispensável no dia a dia das pessoas.

Os problemas relativos à segurança de informações existem desde o momento em que alguém possui determinada informação e deseja protegê-la. Essas informações se tornaram mais vulneráveis com a implantação, expansão e inter-conexão de redes de computadores.

A Internet é capaz de interligar computadores de todas as partes do mundo, portanto a segurança é uma das suas maiores preocupações, porque as pessoas que a utilizam desejam manter suas informações em sigilo. Ela se preocupa em garantir que pessoas mal-intencionadas leiam ou modifiquem mensagens enviadas a outros destinatários, evitar a tentativa de acesso a serviços remotos os quais elas não estão autorizadas a usar, fazer a distinção entre uma mensagem verdadeira e um trote e, principalmente, com a segurança nas negociações pela Internet, já que lida com dados pessoais de clientes.

As redes de computadores são usadas diariamente por empresas e até mesmo no uso doméstico, em nossas residências, onde se pode trocar informações com grande facilidade e rapidez.

Apesar da comodidade que a Internet oferece, se está sujeito a ataques de pessoas com a intenção

de prejudicar, de vírus que podem trazer danos irreparáveis, por isso alguns cuidados devem ser priorizados.

Durante as primeiras décadas de sua existência, as redes de computadores foram principalmente usadas por pesquisadores universitários, para enviar mensagens de correio eletrônico, e por funcionários de empresas, para compartilhar impressoras. Sob essas condições, a segurança nunca precisou de maiores cuidados. Mas atualmente, como milhões de cidadãos comuns estão usando as redes para executar operações bancárias, para fazer compras e arquivar suas devoluções de impostos, a segurança das redes está despontando como um problema potencial.

A maior parte dos problemas de segurança são intencionalmente causados por pessoas que tentam obter algum benefício ou prejudicar alguém. De todas essas pessoas, as que mais merecem destaque são os *hackers*.

A hierarquia do mundo "underground" é muito simples: se a pessoa tem o conhecimento aprofundado em qualquer assunto, ela pode ser considerada um *hacker*; caso contrário, se a pessoa não tem nenhuma novidade em nenhum campo da computação ou correlatos, apenas utiliza o conhecimento dos *hackers* para fazer suas investidas, ela é considerada inferior, pouco ou nada interessante, e é sumariamente ignorada.

Dentro do fechado e pequeno grupo dos verdadeiros gênios de computadores, podem-se distinguir três subgrupos principais:

Hacker

Hacker é aquela pessoa que possui uma grande facilidade de análise, assimilação, compreensão e capacidades surpreendentes de conseguir fazer, literalmente, o que quiser com um computador. Ele tem um conhecimento profundo de sistemas operacionais e sabe perfeitamente que nenhum sistema é completamente livre de falhas, conhece tais falhas e está sempre a procura de outras usando sempre técnicas sofisticadas e variadas.

Os verdadeiros *hackers* desenvolvem os seus próprios programas e, para isso, são os maiores estudiosos dos principais softwares utilizados na Internet, conhecem os sistemas operacionais do meio, alteram seus códigos, criando seus próprios utilitários. Nunca estão satisfeitos e continuam estudando cada vez mais as fontes de outros bons programas. As maiores virtudes dos *hackers* são a força de vontade e a dedicação aos estudos.

Cracker

Crackers possuem tanto conhecimento quanto os *hackers*, mas com a diferença de utilizar para o mal; para eles não basta entrar no sistema, quebrar senhas e descobrir falhas eles precisam deixar um aviso de que conseguiram burlar o sistema e, para provar que estiveram ali, geralmente deixam recados malcriados, algumas vezes destruindo partes do sistema ou aniquilando tudo que encontram pela frente. São atribuídos aos *crackers* programas que retiram travas em softwares, que alteram suas características, adicionando ou modificando opções, muitas vezes relacionadas com a pirataria. Para o *craker*, as palavras de ordem são "roubar e destruir".

Phreaker

O *phreaker* é especializado em telefonia. Faz parte de suas atividades a obtenção de ligações gratuitas, tanto para ligações locais como interurbanos e ligações internacionais, instalação de escutas, reprogramação de centrais telefônicas, facilitando o ataque a sistemas a partir de acesso no exterior, tornando-se invisíveis ao rastreamento e colocando a responsabilidade em terceiros. O conhecimento de um *phreaker* é essencial para se buscar informações que seriam muito úteis em mãos de pessoas mal intencionadas, além de permitir que um possível ataque a um sistema tenha como ponto de partida, provedores de acesso em outros países. Sua técnicas permitem ficar invisível diante de um provável rastreamento e ainda conseguir forjar o culpado da ligação fraudulenta, fazendo com que outra pessoa seja penalizada.

Devido ao grande número de pessoas que se dizem *hackers*, pode-se encontrar outras definições além das já citadas, onde se enquadram os pretendentes a *hackers*. Alguns desses termos são:

Lamers

Lamer é aquela pessoa que quer aprender a ser *hacker*, pergunta a todo mundo o que fazer para se tornar um. Os *hackers*, como qualquer outra categoria, não gostam disso, e passam a insultá-los chamando o de *Lamer*, que significa "novato".

Wannabe

Wannabe é aquele principiante que já aprendeu a usar os programas prontos dos verdadeiros *hackers* e acha que é o bom e pode entrar nos computadores da Nasa, por exemplo.

Arackers

Os *Arackers* são os piores; conhecidos como "hackers de araque" são a maioria no submundo cibernético. Fingem ser os mais ousados e espertos usuários de computadores, planejam ataques, fazem reuniões durante as madrugadas, contam casos fantasiosos. Resumindo: pensam que sabem tudo e no final acabam acessando revistas pornográficas, ou simplesmente, jogando no computador.

A grande maioria dos *hackers* são jovens e fazem muitas proezas durante essa fase; e quando ficam adultos, normalmente trabalham na área de segurança de computadores, deixando de invadir sistemas e causar danos.

3.2- Invasões

Quase todos já ouviram falar, conheceram ou até mesmo presenciaram os danos provocados por invasões no micro através da Internet.

A pergunta mais comum, quando se pensa em segurança na Internet, é o que o invasor pode fazer? Os danos que uma pessoa pode provocar quando tem acesso aos dados de seu computador são vários: vão desde o mais simples, que é observar os diretórios de seu HD, o que invade a sua privacidade, até os danos materiais. Se ele estiver com a intenção de prejudicar, pode alterar senhas, apagar programas, desligar o Windows ou até mesmo formatar o seu HD. Tem acesso para fazer tudo que você pode fazer no seu micro, causando grandes transtornos, podendo perder arquivos importantes. Contudo, coisas piores podem acontecer, como ter a senha do seu provedor de acesso roubada e ele acessar no seu lugar, dando-lhe um prejuízo financeiro sem você saber, a não ser quando chegar a conta milionária de seu provedor de acesso. Até mesmo para quem usa o Home banking, e tem seus dados da conta descobertos, por uma pessoa que nem conhece, que nunca viu, dando um prejuízo muito maior ao usuário, que só perceberá quando for muito tarde.

Os ataques aos sites vêm crescendo e se aprimorando cada vez mais com novas tecnologias usadas para quebrar sistemas. Com o aumento das redes locais e com a grande rede Internet estão ficando mais fáceis as invasões.

No passado, as ameaças à segurança dos micros eram associadas a problemas mecânicos e ambientais, como danos físicos, roubos, ataques dentro da própria empresa e desastres naturais, o que era mais fácil de controlar. Hoje, existem inúmeras tecnologias que podem ser usadas, *hackers* que têm como objetivo burlar a segurança na Web, explorando a vulnerabilidade do sistema usando softwares, vírus, *worms* e "*Cavalo de Tróia*". As ameaças mudaram e tornaram-se mais difíceis de serem descobertas e controladas.

3.3- Tipo de Invasões

Os ataques que serão descritos abaixo têm um ponto em comum que é a vulnerabilidade ou implementações errôneas do protocolo TCP/IP ou a vulnerabilidade na sua própria especificação.

Estas são algumas das técnicas de invasão muito usadas por invasores de sistemas.

- **WinNuke (Nukes)**

São programas criados por *hackers* que finalizam prematuramente com uma conexão TCP, através do envio de pacotes ICMP (Internet Control Message Protocol) com mensagens de erro. Esses programas têm a propriedade de terminar com a conexão, fazendo com que o cliente ou o servidor sejam enganados por uma mensagem de erro que normalmente indicaria um problema de conexão entre os dois. O resultado desse ataque para a vítima é a desconexão do seu servidor, geralmente sem efeitos mais drásticos.

O *Nuke* tem sido a atividade mais popular em escolas. É um tipo de ataque voltado para computadores que rodam Windows e o seu principal efeito é o congelamento da máquina que precisa ser reiniciada.

Esse ataque é muito simples de ser realizado, tem sido implementado com uma linha de código na linguagem Perl. Normalmente esse ataque é direcionado contra a porta 139 (Serviço Netbios Session) do computador.

Considera-se fácil proteger os computadores desse tipo de ataque. A Microsoft desenvolveu patches que, quando instalados, protegem os micros do ataque Nuke, evitando transtornos maiores.

- **Varreduras de portas**

Para acelerar a transmissão de dados que entram nas redes provenientes de vários computadores, são agrupados em pacotes. O *hacker* cria programas para farejar esses pacotes.

O atacante usa o empacotamento de mensagens para ter acesso às informações desejadas. Ele envia pacotes para todas as portas de uma máquina, para descobrir quais são os serviços oferecidos por ela. As informações, assim que são encontradas, são enviadas pelo programa para o computador do *hacker* , que vai utilizar métodos para decodificá-las, pois estão criptografadas.

- **Syn Flooding**

Syn Flooding é um dos ataques da família Ddos (Denial-of-Service) que visam paralisar o funcionamento de um serviço específico ou de uma máquina. O ataque consiste em sobrecarregar um servidor com uma quantidade excessiva de solicitações de serviço.

O ataque é realizado enviando uma stream de pacotes para o computador que deseja invadir, requisitando uma conexão. Cada vez que esse computador receber essa mensagem, ele vai armazenando em uma fila especial com tamanho definido, sem que seja efetivada nenhuma conexão. Quando muitas dessas requisições são recebidas pelo computador alvo, ele não consegue mais alocar esses recursos para o tráfego da rede, pois a fila já está cheia. Então, esse pacote é descartado. Esse processo dura alguns segundos; se demorar a confirmação, o servidor remove a conexão da lista de conexão; mas se o atacante continuar enviando os pacotes continuamente, eles continuarão inutilizados, o que pode fazer com que a máquina pare.

- **Ping Bomb**

Ping significa Packet Internet Groper. O uso mal intencionado desse programa, a partir de uma conexão rápida com a rede, faz com que a vítima caia num espaço de tempo, entre a digitação de uma mensagem e a recepção dela pelo destinatário. Isso, provavelmente, o levará a uma desconexão por *Ping Timeout*, devido à quantidade de pacotes recebidos superando a sua capacidade de responder.

- **Smurf**

Smurf é um tipo de ataque de negação de serviço, e é considerado um ataque muito perigoso. O ataque *Smurf* não tem a intenção de parar um computador, mas sim uma rede inteira. Ele é realizado enviando contínuas *stream* de pacotes ICMP modificados para a rede alvo. Os pacotes são modificados de maneira que o endereço da máquina que envia os dados é idêntico ao endereço alvo, e são enviados para os endereços broadcast, ou seja, são enviados para todos os computadores de uma rede. Os computadores dessa rede irão responder enviando uma mensagem para o computador que eles assumem ter enviado a mensagem e não para o *hacker*, inundando-o pelo *Ping* que é uma verificação se um servidor da Internet está disponível. Se o atacante tiver uma conexão rápida, a quantidade de dados gerada pode parar a rede atacada, até que o atacante deixe de enviar os pacotes ou o tráfego seja bloqueado. Esse tipo de ataque tem sido usado para vários provedores de acesso à Internet e todos os seus usuários.

- **IP Spoofing**

É a técnica de se fazer passar por outro computador da rede para conseguir acesso a um sistema. Usando essa técnica, o invasor pode assumir a identidade de qualquer máquina na Internet. Para atingir a sua meta, o invasor usa um programa que altera o cabeçalho dos pacotes IP de modo que pareçam estar vindo de outra máquina.

- **Sniffing**

***Sniffer* é um programa ou dispositivo que analisa o tráfego na rede. Ele é útil para o gerenciamento de redes, mas nas mãos dos *hackers* se torna uma arma, pois permite a eles roubar senhas e outras informações sigilosas. Funcionam como "farejadores" de redes, com o objetivo de coletar *usernames* e *passwords* do sistema, trazendo comprometimento á rede e aos usuários.**

- **Phreaking**

O *Phreaking* consiste no uso indevido de linhas telefônicas fixas ou celulares. Antigamente, os *Phreakers* empregavam gravadores de fita e outros dispositivos para produzir sinais de controle e enganar o sistema de telefonia. Hoje, as empresas telefônicas se desenvolveram e reforçaram a sua segurança e usam tecnologia sofisticadas para impedir esses ataques, tornando mais complexo e difícil esse tipo de ataque.

- **Scanners de Portas**

É usada para os invasores descobrirem todos os serviços TCP que estão rodando em uma rede, mesmo que ela esteja sendo protegida por filtros de pacotes.

Os Scanners são programas que buscam portas TCP abertas por onde pode ser feita uma invasão. Para que não seja percebida pela vítima, os scanners testam as portas de um computador durante muitos dias, com um intervalo de tempo e em diferentes horários.

- **Mail Bomb**

Atinge principalmente os usuários que se utilizam de provedores de acesso. O *Mail Bomb* consiste em uma técnica de inundar a caixa postal do usuário com mensagens eletrônicas. São enviadas através de programas apropriados que geralmente usam script, para gerar um número maior de mensagens até que ultrapassem o limite da caixa postal para receber mensagens.

Quando ocorre uma sobrecarga de mensagens na caixa postal do cliente, os provedores passam a rejeitar a entrada de novas mensagens para o usuário. Às vezes, mensagens importantes para a empresa deixam de chegar, provocando transtornos e prejuízos.

- **Quebra-cabeça**

Um jeito simples de desvendar senhas é a velha tentativa de erro. Os invasores criam programas capazes de montar combinações de letras e números, para acessar os seus alvos. Esses programas funcionam bem para senhas de até seis caracteres; um número acima disso já fica mais complexo.

Esse processo é longo e demorado e as tentativas devem ser feitas em períodos curtos, se possível com intervalos de dias para evitar que sejam descobertos. O Brasil é um país onde esse processo é muito difundido, porque as senhas geralmente são simples e fáceis de quebrar.

- **Cavalo de Tróia**

O *Cavalo de Tróia* ou “Trojan Horse”, como é conhecido, é um tipo de programa que é infiltrado em computadores com o objetivo principal de fazer com que alguém entre em seu sistema sem ser percebido. “Um verdadeiro presente de grego!”.

O *Cavalo de Tróia* não é considerado um tipo de vírus, apesar de ter algumas semelhanças. Ele não é infiltrado no computador com o objetivo de destruir arquivos e programas e, sim, descobrir senhas. O *Cavalo de Tróia* não possui a capacidade de se auto-reproduzir como os vírus, ele precisa ser executado para se instalar.

Quando se recebe uma mensagem de amigos como joguinhos, programinhas simples ou qualquer tipo de arquivos por email ou disquete e instala no seu computador, você pode estar instalando um cavalo de Tróia embutido neles sem saber. Por isso, muito cuidado, não é porque recebeu de uma pessoa de confiança que não vai estar infectado!

Resumindo, o *Cavalo de Tróia* é um arquivo executável com aparência inocente e interessante que pode trazer outro aplicativo destrutivo escondido dentro dele, o qual é ativado quando o usuário executa o arquivo. Cada vez que é executado, o *Cavalo de Tróia* grava os dados e envia para o criador .

- **Engenharia social**

Consiste na ação de observar os usuários de computadores no seu ambiente de trabalho, observa quando o usuário digita a sua senha, investiga dados pessoais como data de nascimento, nome da esposa, filhos, namorado, número de telefone. Essas são as primeiras tentativas que o *hacker* faz para alcançar seus objetivos, pois é muito comum usar senhas que nos lembram algo da vida particular.

Alguns *hackers*, para conseguir descobrir algo que possa ser usado como meio de quebrar senhas, arrumam empregos temporários nas empresas.

3.4- Vírus

Vírus são programas como outros quaisquer, com a diferença que foram escritos com um único objetivo, o de atormentar a vida do usuário. Eles são pequenos programas que se autocopiam e alojam-se em outros programas ou arquivos, fazendo alterações, sem o seu conhecimento e muitas vezes podem destruir arquivos do sistema, causando danos, às vezes, irreparáveis. São acionados pelos mais diversos eventos como por uma data, algum comando, execução do programa ou arquivo hospedeiro, ou até mesmo pela inicialização do computador.

As manifestações dos vírus podem ser as mais diversas como mostrar mensagens, alterar determinados tipos de arquivos, diminuir a performance do sistema, deletar arquivos, erros na execução de um programa, danificação de drives, alocação desnecessária da memória do computador ou até mesmo a formatação indesejada do HD.

O vírus são formados por instruções com dois objetivos. O primeiro é de atracar um arquivo para, mais tarde, poder disseminar de um arquivo para outro, sem a permissão ou comando do usuário.

Normalmente, os vírus são criados por pessoas com uma grande capacidade inventiva e muito inteligentes, que poderiam estar usando esses conhecimentos de forma mais sensata, como trabalhando em empresas de informática.

Os vírus são escritos por alguém e colocados em circulação até atingirem o seu computador através de um programa ou disquete contaminado. Quando você roda um arquivo contaminado, ou inicializa um computador com um disco infectado, o vírus alcança a memória dele. Após esse processo, ele passa a infectar outros arquivos, normalmente os executáveis com extensão .COM e .EXE, podendo infectar também outros arquivos que sejam requisitados para a execução de algum programa, como os arquivos de extensão .SYS, .OVL, .OVY, .PRG, .BIN, .MNU, .DRV. Também existem os vírus que atacam arquivos não executáveis, arquivos de dados, como os arquivos .DOC do Word e os .XLS do Excel.

Ciclo de vida de um vírus

Os vírus desconhecidos passam por 6 fases que são:

- *Criação* é quando o autor decide que tipo de ação maliciosa ele quer desenvolver.
- *Desenvolvimento* é a fase em que o autor escolhe a linguagem de programação e escreve as linhas de código do programa.
- *Teste* é a fase em que ele espalha o vírus para algumas pessoas de seu ciclo para ver se ele funciona como o esperado.
- *Propagação* é a fase em que ele fará tudo que é possível para espalhar o vírus com rapidez e, assim, conquistar território.
- *Incubação* é o período em que o vírus já foi bem disseminado, mas ainda não causou os prejuízos.
- *Condições bombas*: O vírus dispara sua programação maliciosa quando as condições pré-programadas são acionadas. Essa condições podem ser uma data, um horário, um comando, entre outras.

Os vírus já conhecidos passam por somente 4 fases. São elas:

- *Identificação do novo vírus* é a fase em que o laboratório isola o código malicioso e conhece a fundo seu funcionamento.
- *Identificação da assinatura* identifica um conjunto de informações que acusam a presença do vírus e incorpora essas informações à lista de vírus.
- *Vacina*: Identifica-se como excluir o vírus sem prejudicar o arquivo infectado e incorpora a vacina à lista de vírus.
- *Distribuição da nova lista*: Os usuários podem utilizar seus antivírus com a nova lista que identificará, limpará e eliminará o novo vírus.

O não-uso de um bom programa antivírus pode causar grandes transtornos para a empresa ou usuário doméstico, que terá seu tempo desperdiçado com a paralisação de seus computadores infectados, custo com técnico especialista em informática no suporte para resolver o problema, perda de tempo na reconstrução dos arquivos infectados e na atualização de versões do produto e listas de vírus, multiplicação do prejuízo quando se trata de ambiente corporativo e a perda de informações armazenadas em arquivos infectados, que podem gerar um não aproveitamento das oportunidades de negócios.

A empresa contaminada tem uma grande chance de transmitir vírus, uma vez que se comunica com outras empresas, fornecedores e clientes através da rede, o que a deixaria com uma imagem corrompida no mercado, surgindo uma falta de confiança no sistema de segurança de informação dessa empresa.

3.5- Tipos de Vírus

O crescimento da Internet contribuiu muito para a disseminação dos vírus, pois facilitou a troca de arquivos entre computadores, que antes eram feitas basicamente através de disquetes. Os vírus se propagam através de arquivos transmitidos via Internet, da mesma forma que por meio de arquivos contaminados em disquetes.

3.5.1- Vírus de Arquivo

Esses tipos de vírus se agregam em arquivos executáveis (normalmente com extensão .COM e .EXE) , embora infectem arquivos que são necessários para a execução de algum programa, como os arquivos de extensão .SYS, .DLL, .PRG, .BIN, .DRV, .OVL.

Nesse 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: Vírus de Ação Direta e Vírus Residentes.

Vírus de Ação Direta

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

Isto acontece porque uma vez contaminado um arquivo, o vírus (programa) procura no Winchester por arquivos executáveis. Cada arquivo por ele encontrado é colocado em uma lista, que na nova execução do arquivo contaminado, o vírus seleciona aleatoriamente um ou mais arquivos que serão contaminados.

Vírus Residentes

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

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

3.5.2 Vírus de Sistema ou Vírus de Boot

O vírus de Boot é o tipo mais comum entre todos os tipos de vírus existentes no mundo. Para se infectar, é necessário somente esquecer um disco contaminado no drive A:\, e que não precisa ser do tipo que dá boot.

Eles infectam códigos executáveis localizados nas áreas de sistema de 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, como por exemplo: o DOS. Contudo, todos os discos possuem uma 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 vírus de boot que empregam técnicas mais avançadas em invisibilidade é exibir os arquivos de boot originais sempre que for feita uma solicitação de leitura do sector 1 e 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 lugar considerado incomum.

Track ou trilha: Uma série de anéis concêntricos finos em um disco magnético, que a cabeça de leitura / gravação acessa e, ao longo da qual os dados são armazenados em setores separados.

Sector ou setor: Menor área em um disco magnético que pode ser endereçada por um computador. Um disco é dividido em trilhas que, por sua vez são divididas em setores que podem armazenar um certo número de bits.

3.5.3- Vírus Múltiplos

São aqueles que visam tanto os arquivos de programas comuns como os de setores de Boot do DOS e / ou MBR, ou seja, correspondem à 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.

3.5.4- 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 anteriormente. Sua disseminação foi rápida, especialmente em função da popularidade do editor de textos Word, embora possam ser encontrados na planilha eletrônica do Excel. Eles contaminam planilhas e documentos de extensões .XLS e .DOC e são feitas com a própria linguagem de programação do Word. A tendência é de que eles sejam cada vez mais eficazes, devido à possibilidade do uso da linguagem Visual Basic, da própria Microsoft,

para programar macros do Word.

O vírus de 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 desse tipo de vírus é a sua disseminação multiplataforma, infectando mais de um tipo de sistema como por exemplo Windows e Mac.

3.5.5- Vírus Stealth ou furtivo

Por volta de 1990, surgiu o primeiro vírus *stealth* (furtivo). Esse tipo de vírus é inspirado no caça *Stealth,* invisível a radares. Ele utiliza técnicas de dissimulação para que sua presença não seja detectada nem pelos antivírus e 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 desinfeção de arquivo no momento em que eles forem executados, caso haja um antivírus em ação. Com esta atitude, não haverá detecção e conseqüente alarme.

3.5.6- 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.

3.5.7 Vírus Mutantes ou polimórficos

Têm a capacidade de gerar réplicas de si mesmos utilizando-se de chaves de encripitação diversas, fazendo com 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.

3.6- Ficha técnica de vírus [2]

- **Navidad**

O vírus *Navidad* é um verme que apareceu no início de novembro de 2000. Atacou mais de 100 empresas, muitas na América do Sul. Ele traz uma mensagem de Natal em espanhol e se espalha automaticamente,

respondendo a qualquer e-mail mandado a um computador infectado.

O vírus envia uma cópia de si mesmo em forma de resposta à mensagem original, que contém um arquivo anexo chamado “Navidade.exe”. Se o usuário abrir o arquivo anexado, o programa é executado e aparece uma série de mensagens de erro em espanhol na tela do computador. A primeira mensagem diz, “Não clique nesse botão.”. Se o usuário desobedecer, aparece outra caixa de mensagem dizendo “Feliz Navidade!”(Feliz Natal! em espanhol). A nova praga virtual cria e carrega os arquivos “winsvrc.exe”e “winsvrc.vxd” no sistema, exibe uma mensagem: “Lamentablemente cayo en la tentation y perdio su computadora.”, depois associa-se aos arquivos executáveis do usuário e se auto envia por e-mail para listas e grupos de usuários, um pequeno ícone no formato de um olho aparece no canto direito inferior da tela.

- **VBS/Love Letter**

Esse vírus foi criado por um estudante nas Filipinas, e também é conhecido como *LoveBug* e *I Love You*. Ele vem atingindo computadores do mundo inteiro, causando sérios estragos e multiplicando-se de uma forma antes nunca vista. Ele vem atachado a uma mensagem de correio eletrônico na forma de arquivo VBS (Visual Basic Script), com o nome de “love-letter-for-you.txt.vbs” e se auto transmite via e-mail, assim que aberto o arquivo. As primeiras ocorrências foram na Ásia, e logo depois surgiram casos na Europa e nos Estados Unidos.

O VBS/love letter é um vírus de *Worm* que se espalha por canais mIRC e por e-mail, através do Ms Outlook. Ele tem amplo poder de disseminação, e contamina as máquinas isoladas e em rede local. Destrói vários tipos de arquivos, e seu poder de disseminação é ampliado através de variantes que alteram o assunto dos e-mails que ele auto-envia através do livro de endereços do Ms Outlook. Os e-mails que ele envia são facilmente identificados porque, além de um arquivo com extensão VBS em anexo, os e-mails têm subjects (assunto) conhecidos, como: I LOVE YOU.

- **Chernobyl(W95.CHI)**

Ativação: 26 de abril e algumas versões no dia 26 de junho ou 26 de qualquer mês.

É um vírus perigoso, altamente destrutivo que aproveita os espaços livres no disco para se instalar. Atacou e destruiu informações em vários computadores no ano de 1999. Infecta arquivos de 32 bits do Windows 95, 98 e NT, com extensão .EXE. Ele ataca a Bios do sistema que é responsável pela inicialização do computador e grava o seu código sobre a Flash Bios do Chip. Com isso, ela não pode ser inicializada. Ele é pouco percebido porque não aumenta o tamanho dos arquivos infectados, podendo permanecer na máquina por muito tempo sem ser notado.

- **Sonic Youth**

Na verdade, ele é um *Cavalo de Tróia*, que chega aos usuários como uma mensagem inofensiva e, usa a lista de contatos do Outlook para fazer seus ataques. No campo assunto, vem a frase "I'm your poison."(Eu sou seu veneno.) e, traz como anexo um arquivo que pode ter os nomes girls.exe ou lovers.exe.

Se o usuário clicar, o arquivo anexo irá disparar a instalação do vírus. Depois disso, ele entrará em ação toda vez que o micro for ligado e, quando uma conexão à Internet for estabelecida, alguns arquivos complementares do vírus serão copiados para o computador.

O *Sonic Youth* cria um *Backdoor* (porta dos fundos), que permite a seu criador invadir os micros infectados, daí a classificação como um *Cavalo de Tróia*.

- **QAZ**

É um *Cavalo de Tróia*, que apesar de não ter o mesmo poder de propagação do *Sonic Youth*, ele é extremamente destrutivo. O seu truque é criar um *Backdoor* por meio da substituição do aplicativo bloco de notas, do Windows, por um clone infectado. A partir daí, o criador do vírus pode tomar o controle do Pc remoto.

- **MTX**

O vírus MTX é de origem alemã e está trazendo muita dor de cabeça para os internautas brasileiros, ele chega anexado aos e-mails com os nomes de Tiazinha.jpg, Metallica_song.mp3, New_Playboy_screen_saver.scr e Jimi_Hendrix.mp3, entre outros bem sugestivos.

Depois de instalado, ele começa a se propagar anexado às mensagens enviadas pelo usuário, trocando de nome todos os dias. Além de chegar com uma extensão de arquivo executável (exe), ele também utiliza pif e src. Ele tenta ocultar a extensão verdadeira e deixar uma falsa. Também instala o arquivo MTX.EXE e executa-o, trata-se de um programa de download que baixa plug-ins para vírus, transformando-os em uma espécie de *Cavalo de Tróia* e permitindo que os dados da máquina sejam acessados por *hackers*.

- **Pretty Park**

O PrettyPark.exe é um *Worm*. Seu objetivo não é provocar danos ao disco rígido ou aos softwares instalados, mas abrir uma porta para que internautas mal-intencionados possam roubar informações do micro.

O vírus instala um arquivo que faz o programa de e-mail enviar para todos os integrantes da lista de contatos do usuário uma mensagem com seu arquivo de instalação atachado. Assim, garante sua disseminação em escala mundial. O PrettyPark e seus semelhantes afetam somente aqueles que desconhecem a sua finalidade, já que infecta o micro apenas quando é executado pelo usuário executa o arquivo.

- **Wscript/KaK.B**

É uma variante do vírus KaK.A, que foi amplamente disseminado. O KaK.B atinge o Microsoft Outlook e o Outlook Express, mas requer um ambiente muito especifico para atacar e se propagar.

Esse vírus é disparado de modo simples, através da leitura da mensagem do e-mail e, irá se auto-anexar como assinatura dos e-mails que estão na caixa de saída.

Ele explora um conhecido furo de segurança no Internet Explorer 5. Uma vez que o usuário recebe o e-mail HTML infectado, o código de script, que está escondido, é auto-executável e irá atuar sem que o usuário perceba.

É ativado no dia 11 de cada mês, às 17 horas ou depois, e apresentará a seguinte mensagem: “Days it was a day to be a days!”. Depois disso, o vírus acionará a função Desligar (shutdown) do sistema e irá interromper o uso da máquina infectada até o dia seguinte. Toda mensagem que for enviada terá embutido no HTML do e-mail o KAK.HTML, propagando o *Worm* para outros usuários.

- **Win32/Melting**

Ele tem potencial para derrubar plataformas Windows e fazer com que o sistema operacional fique indisponível. Apesar disso, ele apresenta um risco moderado.

A contaminação é feita pelo MS Outlook dos Windows 95, 98, 2000 ou NT. Uma vez propagada, o worm põe uma cópia dele no diretório do Windows denominada “MeltingScree.exe” e a mantém em memória. Os demais arquivos com extensão “.exe” instalados no diretório Windows são renomeados com a terminação “.bin”. Essas mudanças podem impedir a execução de tarefas básicas do sistema operacional. Ele também tem o poder de acionar o envio de mensagens para os nomes cadastrados no Outlook e executar randomicamente outros arquivos com extensão “.exe”.

3.7- Conclusão

Pode-se perceber através desse capítulo as várias formas de invasões que se está sujeito, mas não se pode esquecer que existem mecanismos para impedir que esses ataques sejam bem sucedidos, e no caso de já ter ocorrido o pior, tentar e diminuir os prejuízos.

No próximo capítulo será demonstrados os mecanismo de segurança que existem para proteger os usuários e empresas de ataques de vírus ou de pessoas não autorizadas.

4- PROPOSTAS DE SEGURANÇA

Com o crescimento do uso das redes de computadores e do número de usuários que estão usando a Internet para fazer negócios, a questão da segurança que já era importante passou a ser imprescindível, pois durante as transações, informações confidenciais podem ser violadas por pessoas mal intencionadas, intrusos da Internet. A cada dia surgem novos métodos cada vez mais sofisticados para violar a privacidade e a segurança das comunicações.

A segurança de dados é um dos maiores problemas e mais difíceis de resolver, pois envolve as instalações físicas, procedimentos operacionais, características do hardware do computador e convenções do software e da programação.

Embora o desenvolvimento e o uso de equipamentos criptográficos para a transmissão sigilosa de dados constitua uma preocupação há várias décadas em alguns países, no Brasil, por diversos fatores, essa utilização historicamente tem sido lenta e o desenvolvimento inibido. Os fatores que contribuem para isso é a falta de conhecimentos a nível nacional, sobre a crescente importância da proteção de dados; ausência de empresas nacionais que tenham efetivamente ocupado o mercado; ausência de uma política de segurança de comunicações; falta de incentivo a empresas nacionais, mesmo na época em que as importações estavam restritas. Com o objetivo de proteger a indústria nacional, a indústria criptográfica não obteve êxito, pela falta de cultura específica ou talvez porque os órgãos governamentais continuaram a importar segurança, o que não deve acontecer pois é melhor ser desenvolvida.

Como hoje a base da nossa sociedade é a informação, com uma crescente facilidade para coletar e armazenar dados, daí a necessidade de se ter mecanismos de segurança realmente eficientes. O computador tem demonstrado, nos últimos anos sua incrível capacidade de melhorar o rendimento das atividades humanas e a sua qualidade de vida.

O crescimento das redes de comunicação tornou possível a integração de um grande número de sistemas computacionais, que passaram a compartilhar aplicativos e bancos de dados. Apesar de grandes benefícios, surgiram também algumas dificuldades referentes ao sigilo de dados, tanto aqueles armazenados internamente numa máquina quanto aqueles que trafegam pelas redes, aumentando assim a

necessidade de implementar medidas de segurança físicas e lógicas.

O principal objetivo da segurança em informática é a preservação do patrimônio da empresa (dados e as informações) que deve ser protegido contra as revelações acidentais, erros operacionais e infiltrações.

As infiltrações podem ser de dois tipos: a infiltração deliberada que tem como objetivos principais o acesso às informações dos arquivos, descobrir os interesses das informações dos usuários, alterar ou destruir arquivos e obter livre uso dos recursos do sistema, e a Infiltração ativa consiste no exame periódico dos conteúdos das cestas de lixo da área do computador até a gravação clandestina de dados armazenados. Inclui também o acesso legítimo ao sistema para obtenção de informação não-autorizada ao infiltrar-se através de canais ativos de comunicações, tendo acesso a profissionais que ocupam cargos importantes e deliberam informações a terceiros, entre outros.

A segurança absoluta não existe, ninguém está imune a ataques de *hackers*, por isso deve ser criado um plano de segurança com o objetivo de evitar os problemas. Esse plano consiste em descobrir os pontos vulneráveis, avaliar os riscos e tomar as providências adequadas para que os prejuízos não sejam maiores recomenda-se, ainda, criar um plano de contingência para no caso do problema acontecer, a empresa já estar apta a resolvê-lo.

4.1- Segurança

A segurança de dados em computação se divide em segurança lógica e segurança física tanto para computadores ligados em redes (Internet ou Rede interna) ou PCs individuais (Standalones).

A segurança de dados abrange desde uma fechadura na porta da sala de um computador até o uso de técnicas criptográficas sofisticadas e códigos de autorização

A segurança física consiste em proteger os dados contra o acesso de pessoas não autorizadas e os riscos naturais ou intencionais; para isso, devemos atentar para problemas que nem sempre são lembrados como incêndios, desabamentos, relâmpagos, problemas de rede elétrica, acesso de pessoas indevidas ao CPD, treinamento inadequado de funcionários, entre vários outros. As medidas de proteção físicas começam com o planejamento de todas as etapas, desde a escolha da localização do CPD até a instalação dos equipamentos, computadores e periféricos.

A segurança lógica já é mais complicada; exige um estudo maior, pois envolve investimentos em softwares de segurança ou a elaboração dos mesmos. Deve-se ter uma atenção especial aos problemas causados por vírus e invasores de redes, backups desatualizados e distribuição de senhas de acesso .

Os princípios básicos da segurança em sistemas são:

Confidencialidade, que é a proteção da informação compartilhada contra o acesso de pessoas não autorizadas. Essa confidencialidade pode ser obtida através do controle de acesso, como as senhas, e também do controle das operações individuais de cada usuário.

Autenticidade, que é a garantia da identidade do usuário. Verificar o transmissor de cada mensagem e tornar possível aos usuários documentos eletronicamente assinados.

Disponibilidade, que é a prevenção de interrupções na operação de todo o sistema, onde uma quebra de sistema não pode impedir o acesso aos dados.

Integridade, que é a garantia da veracidade da informação, evitando que pessoas não autorizadas realizem alterações em mensagens.

A seguir, serão expostas algumas propostas de segurança importantes para manter a segurança na rede.

4.1.1- Firewall

Firewall significa "parede de fogo", feita para impedir a entrada ou a saída de informações, baseadas em uma lista de restrições e permissões, devidamente configurada para suprir necessidades básicas de comunicação da rede interna com a Internet e vice-versa.

Firewalls são mecanismos muito usados para aumentar a segurança de redes ligadas à Internet, espécies de barreira de proteção, constituídas de um conjunto de hardware e software. É um sistema ou um grupo de sistemas que garantem 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 a ser permitido ou negado.

É importante lembrar que ele deve estar presente em todas as conexões da rede interna com a Internet , pois não adianta nada colocar um *firewall* super sofisticado na ligação do backbone se, dentro da rede interna, existir um micro com o modem conectado a outra rede.

Um *firewall* é tanto um dispositivo de hardware (como um roteador) como um pacote de software rodando em um computador especialmente configurado que fica entre uma rede segura (sua rede interna) e uma rede insegura (a Internet). Realiza várias tarefas importantes, como evitar o acesso não autorizado de pessoas à rede, limitar o tráfego de entrada e saída, autenticar os usuários, registrar as informações sobre tráfego e produzir relatórios.

O papel fundamental de um *firewall* é monitorar todo o tráfego que flui entre duas redes e bloquear certos tipos de tráfegos completamente; se o *firewall* fizer direito o seu trabalho, um intruso nunca vai poder chegar a sua rede interna, que ficará assim protegida.

Alguns firewalls permitem que somente certos tipos de tráfegos de rede passem por eles; outros firewalls são menos restritivos e bloqueiam somente os serviços da rede que, reconhecidamente, são causa de problemas, como o FTP. Os firewalls baseados em roteadores, em vez de em sistemas de computadores completos, tendem a ter menos funções de relatórios disponíveis.

Benefícios de usar um Firewall

A seguir algumas vantagens ao acrescentar um *firewall* ao seu arsenal de ferramentas de segurança:

- Acesso controlado a sistemas confidenciais e importantes.
- Proteção dos serviços Internet vulneráveis.
- Administração centralizada da segurança.
- Utilização dos registros e das informações estatísticas na rede.
- Esquemas de filtragem de pacotes mais sofisticados.
- Configuração de sistemas de hardware independentes, que não dependem de outros sistemas de hardware e software.

Um *firewall* pode funcionar como um mecanismo muito eficiente de amortecimento, fornecendo um controle acentuado no ponto onde a rede conecta-se com a Internet. Você pode usá-lo como o centro das metodologias de segurança.

Razões para não usar um Firewall

Apresentadas as vantagens, seguem-se as desvantagens de se usar um *firewall*:

- Acesso desejado a certos serviços será mais limitado do que você gostaria ou pode se tornar mais complicado do que o normal.
- O potencial de acessos pela porta dos fundos aumenta se algo não for feito para evitar isso.
- É necessário mais treinamento e a administração é mais difícil.
- O custo pode se tornar proibitivo.
- A configuração pode ser tão complicada que se torna difícil implementá-la corretamente.

Além disso, por mais capaz e eficiente que seja, há ameaças de que nenhum *firewall* pode evitar, como os vírus, equipes mal intencionadas com acesso à parte mais segura de rede e novos perigos vindos de fora do sistema.

4.1.2- Senhas

A senha é uma chave pessoal para um sistema de computador que tem como função garantir que apenas os indivíduos autorizados acessem determinados serviços.

Hoje, se está sujeito a fraudes com os cartões de crédito, nos caixas eletrônicos, roubos de linhas celulares e com a Internet não poderia ser diferente.

Alguns cuidados na hora de escolher a sua senha

- Não escolher senhas fáceis como seu nome ou sobrenome, sua data de nascimento, número de telefone, nome de esposa, filhos ou qualquer nome que esteja relacionado diretamente com a sua vida pessoal. Escolha senhas complexas, difíceis de serem quebradas (as senhas de oito dígitos, que intercalam números e letras). Pode-se intercalar também letras maiúsculas com minúsculas, tornando-as mais difíceis de serem quebradas, porém, mais seguras.
- Nunca revele sua senha a ninguém, nem a seu melhor amigo. Sempre que for digitar a sua senha,

peça a outra pessoa para virar o rosto; você poderá estar evitando muitos problemas posteriormente. Não esquecer de mudar a sua senha pelo menos a cada 3 meses.

- Troque a senha logo no início de sua assinatura e, principalmente, não deixe gravada no seu computador.

- Acompanhe sempre o seu extrato de acesso, que está disponível a qualquer momento na tela de seu computador. Com esse hábito você poderá evitar transtornos e prejuízos maiores. Caso ocorra algum problema como, por exemplo, um acesso que você não fez, procure imediatamente o seu provedor.

4.1.3- Criptografia

A palavra criptografia é de origem grega (Kriptos = escondido, oculto e grafos = grafia), e é definida como a arte ou ciência de escrever em cifras ou códigos, usando um conjunto de técnicas que torna uma mensagem incompreensível, chamada de texto cifrado. Através de um processo chamado de cifragem, permite-se que somente a pessoa destinatária consiga decodificar e ler a mensagem com clareza, usando o processo inverso, a decifragem. **[5]**

A criptografia surgiu da necessidade de se enviar informações sensíveis através de meios de comunicação não confiáveis, ou seja, em meios onde não é possível garantir que um intruso não irá interceptar o fluxo de dados para leitura (intruso passivo) ou para modificá-lo (intruso ativo). **[14]**

A criptografia tem a função de garantir o sigilo e a integridade da mensagem, ou seja, que somente o usuário destinatário tenha acesso à informação e que ela chegue original, sem sofrer modificações, seja ela intencional ou acidental.

Historicamente, foram os militares, os diplomatas e as pessoas que gostam de guardar memórias que utilizaram e contribuíram para a arte da criptografia. Porém, os militares tiveram o papel mais importante e foram eles que definiram as bases para essa tecnologia. Na batalha, o número de mensagens era muito grande, era difícil alternar os métodos criptográficos rapidamente, porque havia poucos equipamentos e o local não era o mais adequado. Eles deveriam estar sempre preparados para alterar esses métodos instantaneamente, pois, caso acontecesse do auxiliar de criptografia ser capturado pelos inimigos, seria uma catástrofe.

Há duas maneiras básicas de se criptografar uma mensagem: a primeira, através de cifras e a outra, através de códigos. A criptografia através de códigos esconde o conteúdo da mensagem através de códigos predefinidos entre as partes envolvidas na troca de mensagens, enquanto na criptografia através de cifras o conteúdo da mensagem é cifrado através da mistura ou substituição de letras da mensagem original.

Os sistemas criptográficos podem ser assimétricos ou simétricos.

- **Sistemas criptográficos simétricos**

Os sistemas criptográficos simétricos são aqueles que se caracterizam pela utilização de chaves idênticas para cifrar e decifrar mensagens, ou seja, tanto o remetente como o destinatário usam a mesma chave para encriptação e decriptação.

A desvantagem desse sistema é que ele necessita de um canal seguro para transmissão das chaves, que devem permitir o acesso e o conhecimento apenas dos participantes.

- **Sistemas criptográficos assimétricos**

Sistemas criptográficos Assimétricos se caracterizam pela utilização de duas chaves distintas, uma para a encripitação e outra para decriptação, ou seja, o remetente tem uma chave e o destinatário tem outra.

4.1.4- Assinatura Digital

O mecanismo de assinatura digital envolve dois procedimentos:

1. Que o receptor possa verificar a identidade declarada pelo transmissor (assinatura).

2. Que o transmissor não possa mais tarde negar a autoria da mensagem (verificação).

O procedimento de assinatura envolve a codificação da unidade de dados completa ou a codificação de uma parte. O procedimento de verificação envolve a utilização de um método e uma chave pública para determinar se a assinatura foi produzida com a informação privada do signatário.

A característica essencial do mecanismo de assinatura digital é que ele deve garantir que uma mensagem assinada só pode ter sido gerada com informações privadas do signatário. Portanto, uma vez verificada a assinatura com a chave pública, é possível posteriormente provar para um terceiro, que só o proprietário da chave primária poderia ter gerado a mensagem.

4.1.5- Autenticação

A escolha do mecanismo de autenticação apropriado depende do ambiente onde se dará a autenticação. Em uma primeira situação, os parceiros e os meios de comunicação são todos de confiança, nesse caso, a identificação pode ser confirmada por uma senha. Na segunda situação, cada entidade confia em seu parceiro, porém não confia no meio de comunicação. Assim, a proteção contra ataques pode ser fornecida com o emprego de métodos de criptografia e, na terceira situação, as entidades não confiam nos seus parceiros nem no meio de comunicação. Deverão, portanto, ser usadas técnicas que impeçam que uma entidade negue que enviou ou recebeu uma unidade de dados. Ou seja, devem ser empregados mecanismos de assinatura digital, ou mecanismos que envolvam o compromisso de um terceiro confiável.

4.1.6- Programas Antivírus

A melhor forma de proteger seu computador contra vírus é possuir um bom software antivírus, que deve ser instalado e atualizado freqüentemente, pois a cada dia surgem novos e perigosos vírus. Ele deve ser o mais recente possível, para que detecte os vírus mais novos.

Os programas antivírus são programas utilizados para detectar vírus num computador ou disquete. A maioria usa métodos simples de procura por uma seqüência de bytes que constituem o programa vírus. Desde que alguém tenha detectado e analisado a seqüência de bytes de um vírus, é possível escrever um programa que procura por esta 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 em busca de sinal de invasores.

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 recursos especiais, como a Tecnologia *Push* e o *ScreenScan*.

A 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 McAfee sem a necessidade do usuário fazer *downloads* manuais.

O *ScreenScan* varre o disco rígido enquanto o micro está ocioso. Funciona da seguinte maneira: Toda vez que o *ScreenSaver* é acionado, o VirusScan entra em ação. Alem de não atrapalhar a rotina do usuário, evita a queda de desempenho do PC.

Os melhores antivírus

Após o computador ser infectado por um vírus, a única solução é o uso dos programas antivírus, alguns dos quais conseguem reparar os arquivos contaminados, o que nem sempre é possível. No processo de descontaminação do computador, é importante checar todos os seus disquetes, mesmo aqueles com programas e drives originais a fim de evitar uma recontaminação.

Existem muitos programas antivírus que podem ser adquiridos no formato *Shareware* em sites de pesquisadores, empresas ou em BBS. As versões *shareware* são programas que normalmente não possuem todas as funções da versão comercial plena; eventualmente, tais versões têm um tempo limitado; a vantagem é que, geralmente, são gratuitas.

Não basta apenas instalar um bom antivírus no computador para estar livre dos invasores para sempre, pois a cada dia surgem uma média de 15 novos vírus. Então é preciso estar sempre muito bem atualizado. A maioria dos antivírus oferecem atualizações mensais ou bimestrais, que podem ser adquiridas gratuitamente por até um ano, por quem comprou o antivírus.

A seguir serão apresentados alguns dos mais conhecidos e usados antivírus; lembre-se de que é extremamente necessário ter pelo menos um deles em seu computador; porém o ideal é pelo menos dois.

VirusScan

O VirusScan é produzido pela McAfee; é o antivírus mais conhecido do mundo, e com ele é possível encontrar versões para vários sistemas operacionais desde o Ms-Dos até o Windows.

As novas versões desse programa possuem um sistema chamado de *Hunter* (Caçador), que possui uma execução de multiponto de 32 bits projetada para utilizar os avanços mais atuais em termos de memória e gerenciamento de hardware, conferindo ao software um alto nível de detecção de vírus e rápido rastreamento. Quando entra em ação, o sistema cruza informações sobre comportamentos virais para detectar invasores não catalogados. O *Hunter* é um sistema inteligente, que utiliza *webcasting* para atualizar registros via Internet.

O software possui um módulo chamado *ScreenScan* que lança automaticamente o programa de análise quando se ativa o protetor de tela, ou seja, enquanto sua máquina estiver ligada e você não estiver trabalhando o programa procura sozinho por vírus.

Além disso, devido ao aumento dos Applets Hostis, a McAfee está lançando uma nova versão do VirusScan. Trata-se do WebScanX, especializado em policiar o comportamento de aplicações Java,

activeX e programas que viajam de carona em mensagens de e-mail.

Norton antivírus- NAV

O Norton Antivírus, também conhecido como NAV, é produzido pela Sysmatec, que ganhou a confiança de seus usuários e passou a ser um dos mais usados atualmente.

O Norton Antivírus possui um sistema de procura, além dos vírus listados também por vírus desconhecidos. O que chama mais atenção na sua nova versão é um sistema desenvolvido especialmente para o Netscape Navigator, que monitora a presença de vírus durante a realização de download de arquivos na Internet. Se um vírus for encontrado, ele automaticamente trata de reparar o arquivo que está sendo baixado.

Tem detecção polimórfica, que utiliza um compartimento de limpeza virtual, no qual os vírus mutantes são introduzidos antes que possam atuar sobre os arquivos no disco rígido. Além disso, também trabalha em segundo plano vigiando a entrada de invasores.

Dr. Solomons Tool Kit

Um dos destaques do kit é o modulo *MailGuard*, que foi desenvolvido para proteger o computador dos vírus que chegam da Internet ou correios eletrônicos. O sistema elimina automaticamente o vírus, caso seja encontrado. Possui também um módulo que trabalha em segundo plano, que fica constantemente procurando por vírus enquanto você trabalha.

Se você copia arquivos de programas pela Internet a partir de instalações FTP ou de outros computadores, ou usa disquetes para transferir dados de um computador para outro, é bem possível que seu computador seja contaminado com algum tipo de vírus.

Um arquivo de programa carregado da Internet, ou transferido de qualquer outro computador, pode estar infectado por um vírus; disquetes usados em outros computadores também são passíveis de estarem contaminados. Os vírus são específicos para as plataformas, porque os arquivos de programa que infectam são feitos para serem executados em um tipo de computador. Os computadores usando Ms-Dos parecem ter maiores riscos que outros tipos de computadores, provavelmente devido ao número maior de computadores Ms-Dos no mundo. Entretanto, outros tipos como os da linha Macintosh , sistema Unix, também correm risco.

4.2- Conclusão

Existem métodos capazes de garantir quase que totalmente a segurança de dados, seja ela durante uma transação financeira ou até mesmo durante a transmissão de um simples e-mail. Basta conhecê-los e aplicá-los. Os mecanismos de segurança a serem usados vai depender do grau de necessidade de sua empresa.

5- ESTUDO DE CASO

5.1- OS ZUMBIS QUE ATACAM NA WEB. [10]

Como agem os programas usados por hackers para tirar do ar grandes sites na Internet.

Enquanto os bugs e os vírus experimentaram um momento de calmaria em fevereiro de 2000, a temporada foi dominada pelos incidentes de segurança. Um "arrastão" promovido por foras-da-lei digitais forçou alguns dos maiores sites do mundo – Yahoo, Amazon, ZDNet, eBay, Buy.com e Trade – a sair do ar temporariamente. A proeza dos *crackers* caiu como uma bomba no noticiário não-especializado. O problema desse tipo de cobertura jornalística é que tende a sugerir que toda a Internet – e, na linha de frente, o comércio eletrônico – é tão frágil quanto um castelo de cartas. Pior ainda: faz-se confusão entre invasão de sites com roubo de dados e o bombardeio externo para retirar um site do ar.

Ambas as ações, é claro, são ilegais. Mas a semelhança acaba aí. Uma é coisa de ladrões e outra, de predadores digitais. Os servidores bombardeados foram vítimas de uma técnica conhecida como "denial of service"(DoS), ou recusa de serviço. O ataque provém de muitas máquinas que disparam, ao mesmo tempo, milhões de solicitações a um servidor, tornando o site cada vez mais lento. Para isso, os *hackers* coordenaram ataques executados com seus próprios computadores e também com outros micros de usuários inocentes. É o que os técnicos batizaram de DdoS, sigla de Distributed Denial of Service.

Um ataque desse tipo é planejado com antecedência. Para recrutar os micros “escravos”, os *hackers* usam programas que têm o apelido de “Smurfs”. O *DoS* já era conhecido. Os *Smurfs* é que são a novidade. Minúsculos, eles são como vírus e passam a residir em máquinas on-line com brechas de segurança. Em dado momento, eles recebem a ordem de atacar um alvo, e começa o bombardeio. O poder de fogo é multiplicado porque também são envolvidos computadores poderosos, como servidores de universidades. Devido a essa cadeia de máquinas escravizadas – os chamados zumbis -, torna-se difícil identificar as fontes primárias do ataque. É mais um desafio para as empresas que desenvolvem tecnologias de segurança on-line.

UOL também é atacado por hackers. [5]

O Universo Online também afirmou que foi vítima de ataques semelhantes aos realizados em fevereiro de 2000 a grandes portais como Yahoo!, ZDNet e CNN. Segundo o portal, as requisições maciças vieram da rede UUNet dos Estados Unidos pelo link da Embratel.

Caio Túlio Costa, diretor-geral do UOL, explica que a grande maioria dos assinantes não teve nenhuma dificuldade em navegar pelo UOL. "O problema foi navegar por outros sites pela rede Internet", diz.

Apesar da lentidão, a segurança do UOL não foi afetada. Mesmo assim, a empresa vai dar início às investigações para tentar identificar a origem dos ataques.

Ataques de hackers não expõem dados. [5]

Os ataques concentrados promovidos Em fevereiro de 2000 aos sites de empresas como Yahoo, eBay, Amazon, CNN e ZDNet espalharam o pânico na Internet e até provocaram uma queda nos negócios da Bolsa de Nova York. Embora a ação dos *hackers* seja altamente preocupante, essa reação do mercado se deve em parte ao desconhecimento do problema.

Conforme a Yahoo, o total de pedidos aos seus servidores atingiu o pico de 1 gigabit por segundo volume de informação que muitos Web sites não recebem durante um ano. Nesse caso, acredita-se que foram usados no mínimo 50 computadores. O lado preocupante da história é que não há um consenso entre os especialistas sobre as formas de impedir esse tipo de vandalismo. Também é óbvio que a desativação do site provoca enormes prejuízos.

No entanto, o mercado talvez esteja confundindo a capacidade de tirar um grande site do ar por sobrecarga de solicitações com a possibilidade de roubar informações desse site. Uma coisa nada tem a ver com a outra. A técnica do "denial of service" é totalmente externa, baseada na força bruta. Para invadir um site de e-commerce e driblar seus sistemas de segurança, é necessário empregar um nível de conhecimento técnico muito maior.

FBI sai à caça dos hackers.[5]

Vários portais da Internet, entre eles o Yahoo!, a CNN e a ZDNet.

Segundo o *New York Times*, os especialistas em segurança da computação acreditam que a natureza dos ataques deve dificultar a ação da polícia. Para eles, os hackers levaram semanas - ou até meses - planejando o ataque em massa.

O oficial do FBI Ron Dick chegou a dizer que as ferramentas usadas nos ataques são encontradas facilmente na Web, sugerindo que qualquer garoto de 15 anos poderia ser responsável pelos ataques.

De acordo as leis federais americanas, esses casos podem levar os réus primários a cinco anos de prisão, sem contar a indenização que os hackers teriam de pagar às empresas pelos danos causados

Ataque ao Yahoo causa falhas no webmail [5]

Depois do ataque de *hackers* que deixou seu site fora do ar por algumas horas no dia 07/02/2000, o Yahoo passou a apresentar problemas em seu webmail. Algumas mensagens recebidas pelo serviço não incluíam nem o assunto nem os nomes do destinatário e do remetente. Outras, simplesmente chegavam completamente vazias.

Segundo declarações da Yahoo, o bug no webmail decorreu da correria para recolocar o site no ar após o ataque. Mas a empresa garante que todas as mensagens poderão ser recuperadas.

O "apagamento" dos servidores do Yahoo foi causado por uma condição técnica conhecida como "denial of service" ou negação de serviço. Para produzir essa condição, um grupo de *hackers* reúne esforços para que suas máquinas (e, em certos casos, outras, sem a permissão dos donos) enviem ao servidor-alvo um verdadeiro bombardeio de requisições de serviço. Sufocado com o número crescente de solicitações, o servidor vai perdendo desempenho e afinal trava.

5.2- COMPLÔ PODE TER ATACADO CNN [1]

Por Renata Aquino (9 de fevereiro de 2000)

Após o ataque ao Yahoo!, a CNN e a Amazon são atacadas por *hackers* levantando suspeita de complô

O site da CNN foi tirado do ar no dia 08/02/2000 por causa de um ataque de *hackers*. O problema começou às 19h e o site voltou ao normal apenas às 20h45. A CNN diminuiu o conteúdo aos visitantes durante esse período, normalizando o serviço após o final do ataque.

Também no dia 09/02/2000, a Amazon foi atacada por volta das 17h. O serviço de comércio ficou indisponível do mesmo modo como no Yahoo e em outros sites atacados ontem, o e Bay e o Buy.com.

A Buy.com foi atacada ao mesmo tempo em que a companhia fazia sua oferta pública de ações, apesar disto, um porta-voz declarou não há provas que ligassem o movimento financeiro com o ataque. Antes do ataque, no entanto, o tráfego no site estava muito acima do normal.

6- CONCLUSÃO

A segurança é indispensável a uma rede, pois a cada dia aumenta a influência da Internet no panorama econômico brasileiro e mundial. Com o surgimento de novas tecnologias torna-se possível a realização de operações financeiras de diversas localizações do mundo em tempo real, como também a administração de uma empresa.

A cada dia surgem e são executados inúmeros tipos de ameaças, causando transtorno e prejuízos para as vítimas. Os invasores e os vírus são os principais ameaças a que a Internet está sujeita.

Para amenizar essa ameaças existem vários mecanismo de segurança que foram desenvolvidos para proteger os sistemas sigilosos de informações e dados, que muitas vezes ficam expostos durante determinadas transações on-line.

A Internet rompeu as últimas barreiras da globalização do mundo, socializando com isso o conhecimento. A rede das redes fascina cada vez mais o crescente número de internautas que a acessam com desejos de adquirir cada vez mais o saber.

7- REFERÊNCIAS BIBLIOGRÁFICAS

[1] Aquino, Renata; http://www.magnet.com.br/magnet/magnet/bits/internet/bits/ bits2000-02-09b_dtml; Complô pode ter atacado CNN; 23:45; Abril de 2000.

[2] Beceiro, Francisco Panizo; http://csvir.cjb.net; CSV; 00:25; Julho de 2000.

[3] Fortes, Débora; Revista Info Exame; Os sete pecados capitais do WAP; ed.174; setembro de 2000.

[4] http://www.crystalnet.com.br/inter2.html; A Internet; 1:30; Março de 2000.

[5]http://www.cybercities.com/h/homehelp/news_hacker_interhacker.html; 02:42; Março de 2000.

[6] http://www.di.ufbe.br/~flash/ais98/cripto/criptografia.html; 1:30; Julho de 2000.

[7] http://www.geocities.com/CollegePark/Hall/3521/Intodução.html; Definição de comércio eletrônico; 13:10; julho de 2000.

[8] http://netgas.com/cursos.html; 8:33; 28 de julho.

[9] IBOPE INTERACTIVE; http://www.ibope.com.br; 00:50; Abril de 2000.

[10] Machado, Carlos; Revista Info Exame; Os zumbis que atacam na Web; ed.168; Março de 2000; pg. 159.

[11] Mesquita, Renata http://www.uol.com.br/info/infonews/082000/04082000-1.shl; Info Exame- Plantão Info- Maioria de canadenses acessa a Internet; 00:15; Agosto de 2000.

[12] Mesquita, Renata; http://www.uol.com.br/info/infonews/082000/04082000-13.shl; Info Exame- Plantão Info- Itália tem mais de onze milhões de internauta; 00:30; Agosto de 2000.

[13] Mesquita, Renata; http://www.uol.com.br/info/infonews/082000/04082000-3.shl; Info Exame- Plantão Info- Em cuba, um a cada 100 habitantes tem computador; 00:50; Agosto de 2000.

[14] Soares, Luiz Fernando Gomes; Lemos, Guido; Colcher, Sérgio; Redes de Computadores; Editora Campus;