

Universidade Estadual de Maringá  
Centro de Tecnologia - Departamento de Informática  
Especialização em Desenvolvimento de Sistemas para *Web*

## **Segurança em Comércio Eletrônico**

**Rafael Alves Florindo**

Professor Mestre Ayslan Trevizan Possebom  
**Orientador**

Maringá, 2008

Universidade Estadual de Maringá  
Centro de Tecnologia - Departamento de Informática  
Especialização em Desenvolvimento de Sistemas para *Web*

**Rafael Alves Florindo**

## **Segurança em comércio eletrônico**

Trabalho submetido à Universidade Estadual de Maringá como requisito para a obtenção do Título de Especialista de Desenvolvimento de Sistemas para Web, sob orientação do professor Ms. Ayslan Trevizan Possebom.

Universidade Estadual de Maringá  
Centro de Tecnologia - Departamento de Informática  
Especialização em Desenvolvimento de Sistemas para *Web*

**Rafael Alves Florindo**

## **Segurança em comércio eletrônico**

---

Prof<sup>o</sup>. Ms. Ayslan Trevizan Possebom (orientador)

---

Prof<sup>o</sup>. Ms. Flávio Luiz Schiavoni

---

Prof<sup>o</sup>. Ms. Flávio Rogério Uber

## DEDICATÓRIA

Dedico esta monografia àqueles que de forma simples e honesta contribuíram para sua realização. Em especial à minha família que sempre me incentivou a buscar novos conhecimentos.

## AGRADECIMENTOS

Em primeiro lugar a Deus, pela certeza de que sempre esteve ao meu lado dando-me força e coragem para superar todos os obstáculos do caminho.

A minha esposa e meu filho que souberam compreender a minha ausência nos momentos em que me dedicava a esta tarefa, e por acreditar no meu conhecimento como forma de crescimento pessoal.

Ao Ms. Ayslan Trevizan Possebom, orientador, que me acolheu e me conduziu ao longo desta jornada.

## RESUMO

Esta monografia busca envolver as principais questões relacionadas ao comércio eletrônico. Constituído de pesquisa da literatura mundial e de relatórios técnicos, o trabalho analisa assuntos que atualmente mais influenciam no comércio eletrônico, com ênfase em segurança nas transações comerciais e as formas de pagamentos, relacionando as questões de segurança na rede mundial.

Do estudo, pode-se afirmar que os problemas hoje enfrentados pela rede mundial, em especial pelo comércio eletrônico - invasão de dados e comunicações, desconfiança nos meios de pagamentos digitais devido o aumento do uso pela rede - as informações passaram a ter um maior valor. Hoje em dia, não apenas as aplicações bancárias e de comércio eletrônico são as responsáveis pela necessidade de novas tecnologias de segurança na troca de informações, mas toda e qualquer aplicação que necessite de o mínimo sigilo pode contar com diversos recursos da computação atual. Por isso, o comércio eletrônico é o meio empregado pelas empresas para chegar até o consumidor que demanda maior rapidez, eficiência e segurança com menor consumo de tempo para realizar as transações comerciais através de computadores, permitindo uma distribuição de informações muito interativa e dinâmica entre o mercado e os consumidores.

**Palavras-Chave:** *comércio eletrônico, segurança, pagamentos, transações bancárias*

## ABSTRACT

This monograph investigates how to get the main questions related to the electronic commerce (e-commerce). Built on research from world literature and technical report, the work studies subjects that are most affected in e-commerce nowadays, with emphasis in commercial transactions security, bank and way of payment, reporting the security questions with e-commerce in the World Wide Web.

From this study, we can show that the problems faced in the World Wide Web nowadays, in special by e-commerce - invasion in data and communication, mistrust in ways of payment, due to the increase in use, the information go through best worth. Nowadays, not only the bank transactions and e-commerce are the responsible for the new technologies necessity for secure exchange information, but also all application that need minimum sigil can count on with various resources from present computing. Therefore, e-commerce is the mean used by business to get to the consumer that claim for more speed, efficiency and security with less time waste to accomplish their commercial transactions through the computers, allowing the distribution of information very interactive and dynamic among the commerce and the consumers.

**Key-Works:** business electronic, *reliability, fees, trading banker*

## LISTA DE FIGURAS

Figura 1: Faturamento anual do comércio eletrônico ( <i>e-commerce</i> ).....	19
Figura 2: Pagamento Virtual do tipo Cybercash .....	28
Figura 3: Esquema de Níveis da SSL .....	45
Figura 4: Total de incidentes reportados ao Cert.br por ano .....	49
Figura 5: Incidentes reportados ao Cert.br (Tipos de ataques acumulado) .....	51
Figura 6: Incidente reportado ao Cert.br (Top de 10 países com origem de ataques).....	52
Figura 7: Incidentes reportados ao Cert.br (Totais mensais).....	53
Figura 8: Incidentes reportados ao Cert.br (Por dia da semana) .....	54
Figura 9: Incidentes reportados ao Cert.br (Tipos de ataques).....	55
Figura 10: Incidentes reportados ao Cert.br ( <i>Scans</i> reportados por porta).....	56

## LISTA DE QUADROS

Quadro 1: Países com os maiores números de internautas em 2007 .....	16
Quadro 2: Quantidade de pessoas conectadas a Internet no Brasil .....	18
Quadro 3: Evolução de Vendas do comércio eletrônico no Natal.....	19
Quadro 4: Produtos mais vendidos no comércio eletrônico .....	20
Quadro 5: Totais Mensais e Trimestrais Classificados por Tipo de Ataque. ....	50

## LISTA DE ABREVIATURAS, SIGLAS E SÍMBOLOS

ARPA - *Advanced Research Projects Agency* (Agência para projetos de pesquisa avançada)

B2B - *Business to business* (negócio a negócio)

B2C - *Business to consumer* (negócio a consumidor)

DOC - Documento de ordem de crédito eletrônica

E-cash - Dinheiro eletrônico

E-check - Cheque eletrônico

FEBRABAN - Federação Brasileira de Bancos

HTTP: - *Hypertext Transfer Protocol* (Protocolo de Transferência de Hipertexto)

IBGE - Instituto Brasileiro de Geografia e Estatística

IDC - *International Data Corporation*

SET - *Secure Eletronic Tranfer* (Transferência Eletrônica Segura)

SI - Sistemas de Informação

SSL - *Secure Socket Layer*

TCP - *Transmission Control Protocol* (Protocolo de Controle de Transmissão/IP ou Protocolo da Internet)

TI - Tecnologia da Informação

WWW - *World Wide Web*

## SUMÁRIO

<b>1</b>	<b>CONSIDERAÇÕES INICIAIS.....</b>	<b>5</b>
1.1	Introdução.....	5
1.2	Definição do problema .....	6
1.3	Motivação .....	7
1.4	Importância do tema .....	8
1.5	Limitações da pesquisa .....	9
<b>2</b>	<b>METODOLOGIA E DESENVOLVIMENTO DA PESQUISA .....</b>	<b>10</b>
<b>3</b>	<b>INTERNET E COMÉRCIO ELETRÔNICO .....</b>	<b>11</b>
3.1	Comércio tradicional e comércio eletrônico.....	14
3.1.1	E-business .....	22
3.1.2	B2C.....	22
3.1.3	B2A.....	23
3.1.4	B2B.....	23
3.1.5	C2C.....	24
<b>4</b>	<b>FORMAS DE PAGAMENTOS VIRTUAIS.....</b>	<b>25</b>
4.1	Cartões de crédito .....	26
4.2	E-cash .....	27
4.3	Cybercash .....	27
4.4	Netcheque .....	29
4.5	Netcash .....	29
4.6	Débito on-line .....	29
<b>5</b>	<b>QUESTÕES DE SEGURANÇA .....</b>	<b>32</b>
5.1	Política de segurança .....	35
5.2	Motivos de implicações das inseguranças .....	35
5.3	Mecanismos de segurança .....	36
5.3.1	Firewalls .....	37
5.3.2	IDS.....	38
5.3.3	Criptografia.....	39
5.3.4	Protocolos (regras) de autenticação .....	41
5.3.5	Certificados digitais .....	41
5.3.6	Autoridade Certificadora .....	42
5.3.7	Assinaturas digitais .....	43
5.3.8	Selos digitais.....	44
5.3.9	Cookies .....	44
5.3.10	SSL.....	45
5.3.11	SET .....	46
5.3.12	HTTPS .....	47
5.4	Fraudes em Comércio Eletrônico .....	48
5.4.1	Engenharia Social .....	56
5.4.2	Cavalos de Tróia .....	59
5.4.3	Backdoors .....	60
5.4.4	Vírus .....	61
5.4.5	DDoS .....	61
5.4.6	SPAMS .....	63
5.4.7	Worms.....	64
	<b>CONCLUSÃO.....</b>	<b>66</b>
	<b>REFERÊNCIAS BIBLIOGRÁFICAS .....</b>	<b>68</b>

# **1 CONSIDERAÇÕES INICIAIS**

## **1.1 Introdução**

O Comércio Eletrônico é o meio empregado para realizar as transações comerciais através de computadores, numa infra-estrutura aberta de fácil acesso e baixo custo, podendo ocorrer com transações entre empresa-empresa, empresa-consumidor ou intraorganizacional, tanto em caráter nacional quanto mundial. Para que tudo isso se efetive, se vale a considerar os aspectos de segurança que tem passado por inúmeras mudanças nos últimos anos, as quais têm sido consideradas diretamente relacionadas com as tecnologias de informação e comunicação para interligar suas várias áreas, fornecedores e clientes durante as transações.

No atual estágio de desenvolvimento da Internet, a tecnologia permite uma distribuição de informações muito mais interativa e dinâmica do que há alguns anos. Permitindo um processamento muito grande de transações para atender a uma demanda de clientes de forma rápida, segura e, muitas vezes, personalizada, sendo aplicado em todos os setores.

Foi com o surgimento do ambiente digital - conjunto de características gerais de um computador, sistema operacional, ou programa, configuração, que proporciona um local de encontro entre a rede mundial de telecomunicação “Internet” com o homem - que passou a permitir, de fato, a realização de negócios entre clientes e empresas utilizando as tecnologias disponíveis. Desta forma, surgiu o que conhecemos por “Comércio Eletrônico”.

Com a pesquisa, pretendemos apresentar soluções relacionadas aos problemas de segurança nas transações que envolvem o comércio eletrônico, com a finalidade de oferecer aos usuários informações da segurança de uma loja física numa loja virtual, aumentando a credibilidade da empresa fornecedora frente ao cliente.

## **OBJETIVO GERAL**

Este trabalho tem como objetivo identificar os principais aspectos relacionados ao comércio eletrônico por meio da Internet, com ênfase em segurança das transações comerciais e os meios existentes de pagamentos.

## **OBJETIVOS ESPECÍFICOS**

Identificar os principais problemas de segurança na rede mundial em relação ao comércio eletrônico e comparar os principais mecanismos de segurança da Internet, incluindo métodos de autenticação e identificação de usuários.

Descrever os principais meios de pagamentos utilizados no ambiente digital.

### **1.2 Definição do problema**

De acordo com Silva (2000), “os principais problemas de segurança na rede mundial são aqueles relacionados às seguintes condições: privacidade, autenticação, autorização, recusa e integridade”.

- **Privacidade** - consiste em manter as informações inacessíveis a usuários não autorizados. Normalmente, quando se pensa em segurança na Internet, o primeiro raciocínio que vem à mente é o conceito de privacidade. Atualmente, as maiores empresas virtuais procuram criar e divulgar amplamente suas políticas de privacidade, cujo objetivo é garantir que dados pessoais dos internautas não sejam utilizados sem o seu consentimento.
- **Autenticação** - Autenticação de usuários é importante e necessário quando temos uma área restrita em nosso site ou aplicação onde somente pessoas cadastradas e autorizadas possuem acesso as informações e dados confidenciais. Tradicionalmente, os sistemas validam um usuário através de sua senha, que fica armazenada em arquivo ou tabela de banco de dados.
- **Autorização** - É o processo de permitir ou negar acesso ao usuário um ou mais recursos existentes numa rede. Nos sistemas de segurança, a autenticação é distinta de

autorização, que é o processo de atribuir a indivíduos o tipo de acesso a um sistema baseado na sua identidade. A maioria dos sistemas de segurança é baseada em duas etapas. A primeira é a autenticação, que assegura que o usuário é quem afirma ser. A segunda etapa é a autorização, que concede a um usuário acesso a recursos de uma rede com base na sua identidade.

- **Não-repudição** - Serve para provar (por meio de assinaturas digitais) que, por exemplo: um consumidor pediu a um fornecedor, certa quantidade de produtos a um determinado preço unitário. Mesmo que, mais tarde o consumidor afirme, no ato da entrega, ter encomendado menos produtos do que a quantidade solicitada, ou se cada produto tinha um preço inferior ao fornecido, o fornecedor utiliza dessa prova para que o consumidor não recuse a encomenda. Convém referir que pedidos falsos, enviados por alguém com intenções maliciosas, são ignorados, uma vez que é preciso a autenticação. As assinaturas digitais são um componente importante na maioria dos mecanismos de autenticação. Consiste em códigos digitais que podem ser enviados juntamente com uma mensagem eletrônica que identifica de uma forma única o usuário que enviou essa mesma mensagem. As assinaturas digitais devem ser encriptadas de forma que ninguém consiga falsificá-las.
- **Integridade** – Sempre que se quer que uma mensagem não seja alterada. Refere-se, portanto à integridade da informação que pode ser comprometida acidentalmente (erros humanos quando os dados são inseridos, erros de transmissão entre um computador e outro, vírus, bugs, etc.). Contudo, no comércio eletrônico, as situações a serem evitadas são aquelas em que pessoas mal intencionadas comprometam deliberadamente a integridade das mensagens, por benefício próprio, para lesar alguém, ou simplesmente para se promoverem.

### 1.3 Motivação

A segurança eletrônica, durante muito tempo, foi deixada para um segundo plano. Apenas aquelas pessoas e/ou empresas que, por um motivo técnico, perderam arquivos e até mesmo banco de dados inteiros, significando dias e meses de trabalho perdidos, começaram a dar a importância devida à segurança. Hoje, com o advento da Internet e a invasão de "piratas virtuais" - o assunto tornou-se prioridade para todas as pessoas e, principalmente, para as

empresas, em especial àquelas envolvidas no universo do comércio eletrônico. Segundo FREITAS (2007), “A segurança na informática pode ser dividida em cinco áreas:”.

- Segurança de computadores, periféricos e equipamentos;
- Segurança dos softwares;
- Segurança da rede interna de computadores;
- Segurança da Internet;
- Segurança do Comércio Eletrônico.

Para cada área de segurança existem técnicas, procedimentos e softwares de segurança que atuam de modo específico, protegendo os equipamentos e as informações contidas em banco de dados, ou as que estão em "trânsito".

A Internet segundo Bueno (2005).

“A Internet não é mais o parque de diversão de pessoas vistas como estranhos; hoje em dia todo mundo está ligado à “rede”. Assim, cada vez mais a Internet permite que as empresas *on-line* tenham acesso a uma ampla faixa de segmentos demográficos. É importante ressaltar que o comércio eletrônico não se limita a compras pela Internet e a transações da cadeia de suprimento entre grandes parceiros comerciais. Uma vez que Comércio Eletrônico significa fazer negócios eletronicamente, em todos os aspectos, desde o pedido, as vendas e o controle de estoque e até mesmo o suporte pós venda. A aplicação dessa tecnologia eletrônica na organização necessita de suporte através de um banco de dados e de equipamentos sofisticados para atender à busca de dados”.

#### **1.4 Importância do tema**

O surgimento de novas tecnologias sempre representou, em toda história da humanidade, um desafio à organização e à evolução das sociedades.

Atualmente, a utilização e o desenvolvimento de novas tecnologias estão presentes em quase todas as relações sociais, vez que desde a mais trivial atividade de um indivíduo, como a consulta a um saldo bancário, provavelmente estão sendo acompanhadas ou realizadas por meio de sistemas informatizados. A expansão e a popularização do uso de

computadores observadas na última década são, sem dúvida, um dos mais evidentes sinais da influência da tecnologia em nossa vida cotidiana.

### **1.5 Limitações da pesquisa**

A monografia envolvente o comércio eletrônico, abrangendo os temas, de segurança de redes de computadores e pagamentos eletrônicos. Não será descrito neste trabalho a legislação que envolve o Comércio Eletrônico.

## 2 METODOLOGIA E DESENVOLVIMENTO DA PESQUISA

O conteúdo da monografia foi organizado sob a seguinte forma:

- O capítulo 3 apresenta uma visão geral da Internet, como um mercado aberto aos internautas. São comparadas as características dos tipos de comércios da Internet com aquelas da mídia tradicional, enfatizando o caráter interativo das comunicações promovidas pela rede mundial. Enumeram-se as principais ferramentas de marketing existentes na Internet e descrevem-se suas vantagens e desvantagens.
- O capítulo 4 relata as formas de pagamento do comércio eletrônico – dinheiro virtual. São descritos e comparados os principais sistemas de transações eletrônicas atualmente existentes, como resposta do mercado à necessidade de se efetuar pagamentos seguros numa rede de computadores: cartão de crédito, *ecash*, *cybercash*, *netcheque*, dentre outros.
- O capítulo 5 trata sobre segurança e pagamento no comércio eletrônico. São analisadas razões da insegurança. Enumeram-se e se analisam os principais problemas de segurança na rede mundial. São descritos e comparados os principais mecanismos de proteção hoje existentes, tais como: *Firewall*, criptografia, protocolos de autenticação e selos digitais. Também são analisados os Certificados e as Assinaturas Digitais, os quais possibilitam a fé pública dos documentos eletrônicos e a atribuição de responsabilidades, respectivamente.
- E por fim, o capítulo de Conclusão final, junta em um enfeixe as considerações finais.

### 3 INTERNET E COMÉRCIO ELETRÔNICO

Segundo Silva (2000), a Internet nasceu em 1969, desenvolvida pela empresa ARPA (*Advanced Research and Projects Agency*) sob o nome de ARPANET, tendo como seu principal objetivo interligar as bases militares e os centros de pesquisas (universidades) do governo americano. A ARPANET além de fazer esta conexão também fornecia alguns serviços tais como: correio eletrônico, transferência de arquivos e compartilhamento de impressoras. Primeiramente ela foi projetada para uso restrito de usuários do governo americano. Com o passar do tempo, os sites foram aumentando e a necessidade de velocidade aumentava, foi quando surgiu o protocolo de comunicação TCP/IP (*Transfer Control Protocol/Internet Protocol*), usado até os dias de hoje.

A Internet possibilitou a participação das empresas numa economia global, na qual, é possível explorar um vasto mercado e dispor de oferta personalizada para cada cliente instantaneamente. A Internet passará a ser um ambiente de elevada segurança e grande comodidade para fazer compras.

Segundo o mesmo autor, torna-se fundamental para o sucesso destas organizações o uso adequado das ferramentas disponíveis na rede mundial, algumas das quais mostradas a seguir: WWW (*dados gráficos em multimídia: textos+imagens+som+vídeo=Hipermissão*), Transferência de Arquivos (*FTP*), Correio Eletrônico (*E-mail*), Terminal Remoto (*Telnet*).

- WWW (*World Wide Web*): denominada de Teia de Alcance Mundial. Foi desenvolvido no laboratório de Pesquisas Nucleares de Genebra (*CERN*) a partir de 1989, sendo um serviço de procura por hipermissão. Ao contrário do Gopher que cria a imagem de uma árvore de navegação. A Web cria a imagem de uma teia que interliga documentos através da Internet. O mecanismo de navegação é o hipertexto, onde as informações dos caminhos de navegação estão embutidas nos documentos e não nos títulos deles, como no Gopher. Graças a Web, podemos desfrutar de uma tecnologia multimídia de ponta, onde os sons e animações proporcionam à Internet a receita ideal para uma navegação mais prazerosa.

Os recursos de multimídia são obtidos através de documentos HTML (*Hipertext Markup Language*), traduzido como: Linguagem de Marcação de Hipertexto. É uma linguagem que é interpretada pelo navegador. Ela não mantém estruturas de decisão, iteração

e subprogramas que são características de linguagens de programação. Os documentos HTML permitem comunicação usando gráficos, texto, links e e-mail. Os recursos da WWW estão sempre em desenvolvimento para efetuar as transações seguras que possibilitam a realização de Comércio Eletrônico de forma econômica. Esta tecnologia usa o conceito de encriptação de informações confidenciais, tais como senhas, pedidos, códigos de cartões de crédito e outras formas de dados que se queira ter segurança ou privacidade.

- **FTP (*File Transfer Protocol*):** É uma ferramenta que permite fazer transferência de arquivos entre computadores através da Internet. Basicamente os programas que implementam o FTP fazem transferência de arquivos entre seu computador local e outro remoto chamado de Upload. Por outro lado a transferência dos dados do computador remoto para o computador local é denominada Download. O FTP é um dos recursos mais importantes disponível na Internet, e também responsável por um grande volume de tráfego de dados.

Não tão efetivo como o World Wide Web, FTP constitui-se num método de baixo custo para a obtenção de informações por parte dos usuários. Seu maior problema é a falta de interatividade, o que não impede que as empresas criem diretórios com informações acessíveis por FTP.

- **Correio Eletrônico (*E-mail*):** Uma das ferramentas de comunicação mais práticas e eficientes da Internet é o E-mail. Diariamente, milhões de pessoas enviam mensagens umas às outras, de pessoas para computadores e vice-versa usando um endereço eletrônico como referência para localização do destinatário da mensagem. O e-mail é uma maneira excelente para se trocar informações sobre negócios, uma vez que é rápido, barato e confiável. É especialmente útil se você tiver que repartir o trabalho entre vários escritórios, localizados em diferentes países.

Também se pode fazer a distribuição da mesma mensagem para uma lista de endereços, ou seja, uma lista de discussão (*mailing list*). Embora a maioria das mensagens trocadas via rede seja constituída por informação puramente textual, o correio eletrônico permite também a transmissão de outros tipos de informação, tais como sons e imagens, desde que devidamente codificadas.

- **Telnet:** Com este serviço é possível conectar um determinado servidor por meio de login e senha, possibilitando desta maneira, um acesso a serviços da Internet não

disponibilizados. Permite acesso remoto à qualquer máquina que esteja rodando o módulo servidor (assim como no SSH) mas é mais inseguro, pois os dados não são criptografados. Manter o servidor Telnet ativo representa um grande risco numa máquina conectada à Internet, pois qualquer um que descubra uma das senhas de usuário, ou pior, a senha de root, terá acesso à sua máquina. E com o Telnet isso é muito fácil, pois bastaria snifar a sua conexão e pegar sua senha quando usasse o serviço. O comando existe tanto no Linux, quanto no Windows (no prompt do MS-DOS). Via Telnet você tem acesso via terminal como se estivesse sentado na frente da máquina, pode até mesmo abrir aplicativos de modo texto, além de poder usar todos os comandos. Naturalmente, o que você poderá fazer estará limitado à conta de usuário que utilizar. Por questões de segurança você não poderá logar-se como root, embora nada impeça que você use um login de usuário para ter acesso ao sistema e depois use o comando "su" para virar root.

- SSH: é um pacote de programas cujo objetivo é aumentar a segurança de um sistema de redes. Ele, basicamente fornece um substituto mais seguro para os programas "remotos" - rsh, rlogin, rcp. Além de ser uma boa alternativa para o telnet. O problema de segurança que este pacote tenta solucionar é o da escuta de rede para obter informações sigilosas. Os comandos remotos e o telnet usam transferência direta de dados sem codificação. Isto permite que redes abertas a "escutas" tenham informações críticas vazadas. Uma "escuta" é facilmente instalada numa rede ethernet na qual não é possível controlar o acesso de máquinas ou usuários suspeitos. Sendo assim o SSH é uma espécie de versão evoluída do Telnet, que também permite executar arquivos remotamente, mas com várias vantagens, a sigla vem de Secure Shell. Assim como no Telnet, uma máquina com o serviço habilitado pode ser acessada via linha de comando por usuários que tenham o login e senha de uma das contas do sistema. O SSH permite ter acesso completo ao sistema via terminal, seja via rede ou via Internet, limitado aos privilégios do login usado.

### 3.1 Comércio tradicional e comércio eletrônico

Tradicionalmente quando se fala em compra ou venda de mercadorias, logo se pensa em um estabelecimento físico aonde se pode escolher um produto, ter a oportunidade de ser atendido e ainda a de escolher por quem será atendido. Ainda, poderá tirar dúvidas sobre o produto a qualquer momento. Tendo a mercadoria em mãos, poderá pechinchar o preço, conseguir descontos em pagamentos à vista ou um parcelamento que o satisfaça. Na maioria das vezes poderá até levar o produto, dependendo da disponibilidade de entrega da loja.

O comércio veio se atualizando com a introdução de máquinas em seus estabelecimentos e a venda de mercadorias pode ser feita on-line. Porém agora os clientes estão sentados em suas poltronas em frente a um monitor, no qual é o seu único elo com a mercadoria, ou seja, não sentirá a satisfação de ter pelo menos tocado a amostra do produto no qual esta comprando, não poderá mais ter preferência no atendimento, não tem atendimento exclusivo, e nem poderá mais pechinchar preço com a empresa, mas sim com as empresas do comércio, suas formas de pagamentos estão pré-estabelecidos, com pagamentos em cartão ou em outra forma de pagamento. Todas as mercadorias compradas passam por um processo e entrega que depende de localidade e de empresa entregadora.

Segundo Albertin (2000), desde a pré-história o ser humano sempre faz inovações para melhorar ou criar novas formas de comercializar bens. De lá para cá a tecnologia foi se adequando a realidade com o surgimento da Internet, resultando-se na abertura das portas dos comércios físicos para o mundo em operações de compra expondo a mercadoria ao comprador, estabelecendo um método de pagamento e entregar a mercadoria depois do negócio fechado.

O objetivo maior do Comércio Eletrônico é, e sempre foi o de expandir mundialmente as fronteiras comerciais, tendo em vista a facilidade de comunicações entre os compradores e vendedores, ou seja, qualquer negócio, qualquer produto quando colocado na rede torna-se acessível para o planeta todo.

Partindo deste princípio, produtores de sistemas de bancos de dados colocam no mercado ferramentas ou soluções completas para criar sites voltados ao comércio eletrônico. Tendo em vista que comércio eletrônico é o mesmo de um comércio físico, pois possui compra e venda de bens ou serviços, mas este por sua vez é realizado através de redes de

computadores, como a Internet, onde sua transação é realizada eletronicamente, e não pessoalmente. No comércio físico têm-se clientes, no comércio eletrônico abrange navegantes, que procuram de forma mais cômoda o melhor preço a hora que desejar.

De acordo com as estatísticas de julho a agosto de 2006 obtidos pelo órgão de estatística TIC DOMICÍLIOS (2007) a porcentagem e proporção de indivíduos que já compraram produtos e serviços pela Internet possuem um índice de 14% que já acessaram de qualquer lugar (lan house, cyber café, etc.) e 85,5% desses nunca acessaram a Internet, 0,45% não souberam responder.

A relação de indivíduos que compraram produtos e serviços pela Internet há pelo menos 3 meses é de 6,12%, já nos 12 meses foram de 11,32%, enquanto que há mais de 12 meses foram de 2,67%. Todavia 85,5% nunca compraram nada pela Internet.

As categorias de produtos e serviços adquiridos são:

- Comida/produtos alimentícios 1,45%,
- Produtos para a casa / eletrodomésticos 13,32%,
- Filmes e música 20,78%;
- Livros, revistas, ou jornais 30%,
- Roupas, calçados, materiais esportivos e acessórios 13,04%,
- Software 4,60%,
- Jogos de computador ou videogame 4,79%,
- Computadores e equipamentos de informática 19,32%,
- Equipamentos eletrônicos (ex. câmeras) 23,57%,
- Viagens (reservas de avião, hotel, etc.) 3,59%,
- Ingresso para eventos 4,12%,
- Serviços financeiros, seguros 0.64%,

- Material para educação à distância 6,55%,
- Loterias e apostas 0,34% e
- Outros 13,82%.

Agora com uma base de 396 entrevistados 9,17 % apresentaram problemas ao adquirir produtos e serviços pela Internet, 90,53 % não apresentaram problemas, considerando uma projeção populacional: 5,8 milhões de pessoas.

Em outro estudo com 3.012 entrevistados que usaram a Internet, não realizaram compras pela rede, com uma projeção populacional de 43,8 milhões de pessoas:

- 43,45% não tiveram necessidade ou interesse em comprar pela Internet;
- 39,19% preferem comprar pessoalmente por gostas de ver o produto;
- 19,87% têm preocupação em relação à segurança;
- 16,71 % não confiam no produto em que irão receber;
- 25,71 % não opinaram.

Em uma amostra com 3.502 entrevistados aonde 3,69% usaram a Internet divulgando ou vendendo algum bem ou serviços pela Internet e 96,15% que não, 0,15% não responderam.

De acordo com o órgão de pesquisas E-commerce.org (2007) mesmo os Estados Unidos com uma população 209 milhões de pessoas sendo menor do que a da China com 1.306 milhões de pessoas, possui um maior número de usuário internautas chegando a 299 milhões de pessoas contra 123 milhões da China. O Brasil vem em décimo lugar com apenas 30 milhões de pessoas conectadas a Internet, onde sua população é de 188 milhões de pessoas.

**Quadro 1: Países com os maiores números de internautas em 2007**

	<b>País</b>	<b>Usuários da Internet (milhões)</b>	<b>População (milhões)</b>	<b>Adoção da Internet</b>	<b>Fonte</b>
<b>1</b>	Estados Unidos	209	299	70 %	Nielsen//NR

<b>2</b>	China	123	1.306	9 %	CNNIC
<b>3</b>	Japão	86	128	67 %	eTForecasts
<b>4</b>	Alemanha	51	83	61 %	C.I.Almanac
<b>5</b>	Índia	40	1.112	4 %	C.I.Almanac
<b>6</b>	United Kingdom	38	60	63 %	ITU
<b>7</b>	Koreia do Sul	34	51	67 %	eTForecast
<b>8</b>	Itália	31	59	52 %	ITU
<b>9</b>	França	30	61	48 %	Nielsen//NR
<b>10</b>	Brasil	30	188	16 %	eTForecasts
TOP 20 Países		836	4.064	19.9 %	IWS
Total de Usuários do mundo		1,076	6,499	15.7 %	IWS

Fonte: <http://www.e-commerce.org.br>

No Brasil, segundo pesquisa do órgão e-commerce.org, o número de internautas teve um aumento de julho de 1997 a dezembro de 2006, passando de 1,15 milhões de usuários, 07% da população nacional, informado pelo IBGE, para 30,01 milhões de pessoas, correspondendo cerca de 16% da população brasileira, um aumento muito expressivo.

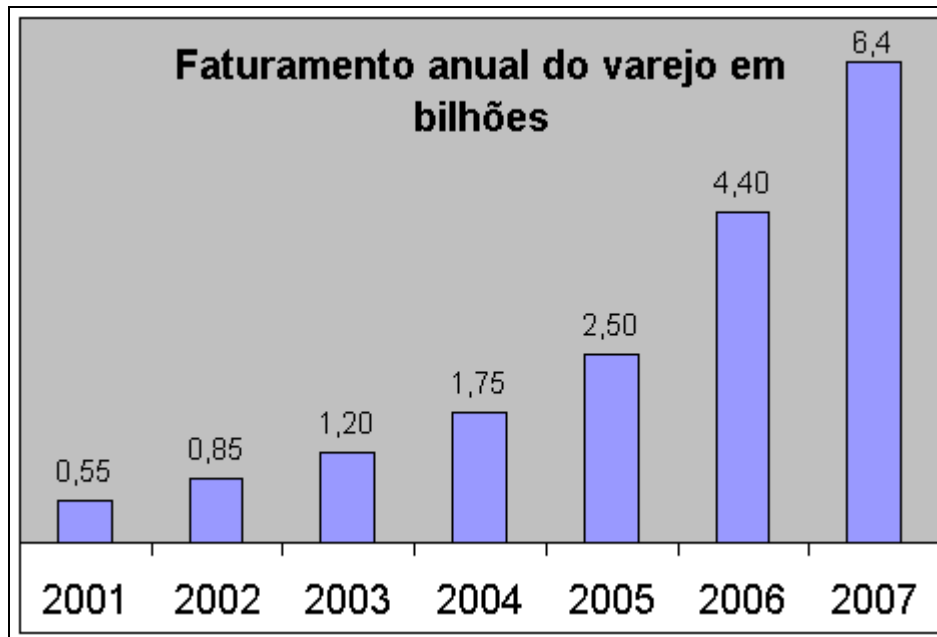
**Quadro 2: Quantidade de pessoas conectadas a Internet no Brasil**

<b>Data da Pesquisa</b>	<b>População total IBGE</b>	<b>Internautas (milhões)</b>	<b>% da População Brasileira</b>	<b>Nº de Meses (base=jan/96)</b>	<b>Crescimento Acumulado (base=jul/97)</b>	<b>Fontes de pesquisa Internautas</b>
<b>2006 /dez</b>	188,6	30,01	16%	106	2.508%	Internet WorldStats
<b>2005 /jan</b>	185,6	25,90	13,9%	106	2.152%	Internet WorldStats
<b>2004 /jan</b>	178,4	20,05	11,5%	95	1.686%	Nielsen NetRatings
<b>2003 /jan</b>	176,0	14,32	8,1%	83	1.143%	Nielsen NetRatings
<b>2002/ago</b>	175,0	13,98	7,9%	78	1.115%	Nielsen NetRatings
<b>2001/set</b>	172,3	12,04	7,0%	67	947%	Nielsen NetRatings
<b>2000/nov</b>	169,7	9,84	5,8%	59	756%	Nielsen NetRatings
<b>1999/dez</b>	166,4	6,79	7,1%	48	490%	Computer Ind. Almanac
<b>1998/dez</b>	163,2	2,35	1,4%	36	104%	IDC
<b>1997/dez</b>	160,1	1,30	0,8%	24	13%	Brazilian ISC
<b>1997/jul</b>	160,1	1,15	0,7%	18	-	Brazilian ISC

Fonte: <http://www.e-commerce.org.br/STATS.htm>

Para Turban (2000), comércio eletrônico é a entrega de informações, produtos/serviços ou pagamentos através de linhas telefônicas, redes de computadores ou outros meios eletrônicos.

O comércio eletrônico brasileiro se infiltrou por completo na cadeia de suprimento e matérias primas a itens domésticos como: livros, cds, aparelhos eletrônicos e leilões. As grandes empresas do comércio eletrônico tendem a reinventarem suas cadeias de suprimento para suprirem os requisitos dos consumidores. Ambos os comércios - entre empresas (B2B) e entre fornecedor e cliente (B2C) denominados e-business – estão experimentando considerável mudança na Internet, possuindo um no ano de 2007 um faturamento de R\$ 6,4 Bilhões de reais no varejo on-line, uma diferença 55% se comparada com o ano de 2001 onde era de R\$ 0,55 bilhões de reais, não considerando as vendas de automóveis, passagens aéreas e leilões on-line.



**Figura 1: Faturamento anual do comércio eletrônico (e-commerce)**

Fonte: <http://www.e-commerce.org.br>

A cada ano o varejo tem aumentado sua renda, como pode se ver no quadro abaixo, onde no natal de 2003 o faturamento foi de 204 milhões e já no ano de 2005 teve um acréscimo de mais de 60% chegando a 458 milhões de reais.

**Quadro 3: Evolução de Vendas do comércio eletrônico no Natal**

Data da Pesquisa	FATURAMENTO (R\$ milhões)	Varição em relação ao mesmo período do ano anterior	Faturamento acumulado no ano (R\$ milhões)	Ticket Médio
<b>NATAL 2005 (15/11 a 23/12)</b>	458,0	61%	2.500,0	272,00
<b>NATAL 2004 (15/11 a 23/12)</b>	284,0	39%	1.750,0	320,00
<b>NATAL 2003 (15/11 a 23/12)</b>	204,0	55%	+1.180,0	315,00

Fonte: <http://www.e-commerce.org.br>

O mercado on-line brasileiro vem buscando cada ano atender melhor os internautas, com a inclusão de vários produtos, mas os produtos mais procurados pelos brasileiros são os CD's e DVD's, mesmo com a pirataria existente no país, os e-commercer faturam milhões com estes produtos.

**Quadro 4: Produtos mais vendidos no comércio eletrônico**

<b>Produto</b>	<b>2003</b>	<b>2004</b>	<b>2005</b>
CD's e DVD's	32%	26%	21%
Livros e Revistas	26%	24%	18%
Eletrônicos	-	-	9%
Saúde e Beleza	3,3%	7,2%	8%
Informática	4,7%	6,0%	7%
Outros	-	-	37%

Fonte: <http://www.e-commerce.org.br>

Entretanto todo comércio seja ele físico ou virtual sofre suas conseqüência de crescimento, seja ela na falta de suporte financeiro, ou mesmo na segurança de seus produtos ou dados. O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil CERT. Br (2007), um dos serviços coordenados pelo Núcleo de Informação e Coordenação do Ponto br (NIC.br), divulga estatísticas de incidentes envolvendo redes brasileiras, referentes ao segundo trimestre de 2007. Estatísticas estas mensuradas com base nos dados relatados espontaneamente por administradores de rede e usuários.

De acordo com as notificações recebidas de abril a junho de 2007, o número total de incidentes foi de 38.513 milhões, o que representa queda de 31% em relação ao primeiro trimestre de 2007 e baixa de 22% em relação ao mesmo período de 2006. A principal razão dessa diminuição foi à redução no número de notificações de incidentes relacionados à Worms neste mesmo período.

O número de notificações relacionadas a fraudes aumentou 46% em relação ao primeiro trimestre de 2007 e 3% se comparado ao mesmo período de 2006. "Esse crescimento se deve ao aumento nas notificações de fraudes relacionadas a casos de quebra de direitos autorais referentes à distribuição de material pirata por meio de redes P2P". Já as varreduras diminuíram 17% em relação ao primeiro trimestre de 2007 e aumentaram 8% em relação ao mesmo período de 2006, nota-se a continuidade da procura por serviços que possam sofrer ataques de força bruta, como SSH, FTP e TELNET. Também tem sido grande a procura por serviços que possam ser explorados para envio de spam, como proxies SOCKS e SMTP.

De acordo com o mesmo núcleo agora relacionado ao terceiro trimestre de 2007, o número total de notificações de incidentes recebidas de julho a setembro deste ano foi de 34.201, o que representa queda de 11% em relação ao segundo trimestre de 2007 e diminuição de 43%, se comparado ao mesmo período do ano passado. O principal motivo da redução foi

à diminuição no número de notificações de incidentes relacionados à Worms e varreduras neste período.

Em relação ao segundo trimestre de 2007, as notificações de Worms diminuíram 18% e 40%, respectivamente. O comparativo com 2006 mostra que os registros de Worms foram 61% menores e as de varreduras, 40%. A grande quantidade de ocorrências, aliada ao tempo cada vez menor que os administradores de redes têm para notificar esses incidentes ao CERT.br, são os responsáveis para que os números deste trimestre sejam inferiores aos demais.

Ainda de acordo com as estatísticas do CERT.br, o número de notificações relacionadas a fraudes foi 21% maior em relação ao segundo trimestre de 2007 e teve aumento de 30% se comparado ao mesmo período de 2006. Essa alteração se deve ao contínuo aumento nas notificações de fraudes relacionadas a casos de quebra de direitos autorais referentes à distribuição deste tipo de material por meio de redes P2P.

Foi constatado o crescimento no número de varreduras pela porta 5168/TCP, que podem estar relacionadas a vulnerabilidades descobertas no software antivírus Trend Micro ServerProtect. Com relação aos outros tipos mais comuns, nota-se a procura por serviços que possam sofrer ataques de força bruta como SSH (22/TCP), FTP (21/TCP) e TELNET (23/TCP).

Segundo a autora Bueno (2005), define o comércio eletrônico como sendo caracterizado pelo uso de meios eletrônicos para a condução de transações comerciais entre empresas, governo e consumidores. Sendo considerado como um mecanismo de realização de negócios por meio do uso de tecnologias de informação. Esta nova ferramenta virtual possibilita o surgimento de novos processos de comercialização e novos meios de comunicação.

### 3.1.1 E-business

Segundo Turban (2000) e-business, refere-se a uma definição mais ampla, não apenas a compra e venda, mas serviços ao consumidor e colaboração com parceiros de negócios e condução de transações eletrônicas dentro da organização.

De acordo Albertin (2000), o e-business é subdividido a partir da natureza de suas transações nos seguintes tipos:

- B2B (*business to Business*);
- B2C (*business to Consumer*)
- C2C (*Consumer to Consumer*)
- B2A (*business-To-administration*)

### 3.1.2 B2C

B2C (*business-to-consumer, também chamada de business-to-customer*) (B2C), refere-se à venda de produtos feita na Internet diretamente da empresa para o consumidor. Este tipo de transação é formado por consumidores que adquirem bens ou serviços para uso próprio. Similar a loja física, a loja virtual busca o melhoramento do atendimento via web, na forma de facilidade e comodidade para o consumidor. Também demonstra uma empresa moderna e apta a oferecer um produto ou serviço de qualidade.

Ainda segundo o mesmo autor este segmento caracteriza-se pelo estabelecimento de relações comerciais eletrônicas entre as empresas e os consumidores finais. Este tipo de comércio desenvolve-se de forma acentuada devido ao advento da web, existindo já várias lojas e centros comerciais virtuais na Internet a comercializar todo o tipo de bens de consumo.

### 3.1.3 B2A

De acordo com Albertin (2000) este tipo de transação on-line ainda se encontra numa fase inicial de desenvolvimento. Este e-commerce designado como B2A (*business-To-administration*) é realizada entre as empresas privadas e com empresas da Administração Pública. Este segmento engloba uma grande quantidade e diversidade de serviços, designadas as áreas fiscais, da segurança social, do emprego, etc.

### 3.1.4 B2B

Segundo Albertin (2000), as transações realizadas no comércio eletrônico entre empresas através da Internet recebem o nome de B2B (*Business-to-Business*).

São exemplos de transações eletrônicas realizadas entre empresas:

- As empresas compram ou vendem os produtos uma das outras empresas regularmente, utilizando a Internet.
- Realizam licitações para escolha de fornecedores de suprimentos ou participa como concorrente à fornecedora de suprimentos.
- Realizam também leilões para compra de matéria-prima, nas condições solicitadas, com o menor preço; ou participa do leilão como concorrente a fornecedora dos produtos.
- Pequenas e médias empresas compradoras, mediadas por um terceiro, fazem compra conjunta, em maior escala, de matéria-prima, obtendo, uma redução do custo unitário do produto.

A utilização de meios eletrônicos, como a Internet, nas transações comerciais com outras empresas é uma tendência, uma vez que quase todas as empresas utilizam esse novo canal para realizar suas transações. Benefícios tangíveis, como a redução de custos na realização de pedidos e no preço de matéria-prima, a maior agilidade nos procedimentos de escolha de fornecedores ou compradores, o maior controle dos processos de licitações, entre outros benefícios, tornam a Internet uma tendência para realizar suas transações.

Segundo a autora Bueno (2006), para obter um B2B eficaz, não bastam Website bem elaborado, sendo também necessário o uso de outras ferramentas do E-Business para que as estratégias de relacionamento com clientes, políticas eficazes de cadeia de suprimento e elementos de automatização de processos dentro da cadeia de comercialização sejam estratégias efetivadas com sucesso.

O mercado B2B vem crescendo de forma mais consistente e representa a maior parte dos negócios efetuados por esse novo meio de comunicação. Os benefícios trazidos pelas transações B2B pela Internet não são novidade, bem como a possibilidade de troca rápida de informações, a automação de gestão da cadeia de suprimentos, a possibilidade de otimização e a redução de estoque.

### **3.1.5 C2C**

De acordo com Albertin (2000), conhecida pelo mundo da Internet como C2C (*Consumer to Consumer*), é uma transação comercial on-line realizada entre pessoas. No início a predominação era a transação entre empresas B2B. A partir do momento em que as pessoas físicas ganharam confiança na Internet, começaram a fazer transações comerciais com as empresas e também diretamente com outras pessoas, do mesmo modo que as vendas de porta em porta, ou seja, venda física, como as promovidas por Avon, Natura e outras. Na Internet, a grande líder do mercado C2C é a empresa Mercado Livre.

Estes negócios são realizados por meio de uma plataforma eletrônica na Internet e intermediados por uma empresa que oferece a infra-estrutura tecnológica e administrativa. Tanto o comprador quanto o vendedor devem estar cadastrados no sistema e podem ser avaliados por todos os membros da comunidade de negócios pela quantidade de transações que já realizaram e pelas notas que receberam em cada transação, numa espécie de ranking dos bons negociadores.

Outro mecanismo que oferece mais segurança aos usuários é o chamado “mercado pago”, um sistema com o qual o Mercado Livre recebe o pagamento do comprador e o transfere ao vendedor, após a entrega normal da mercadoria.

#### 4 FORMAS DE PAGAMENTOS VIRTUAIS

Segundo Silva (2000) e Albertin (2000) com o rápido avanço da tecnologia para web, as lojas virtuais têm ficado cada vez mais relativas à loja física, além disso, estão surgindo diversos tipos de pagamento, ou seja, várias formas de pagamento (moeda) virtual para intermediar as transações nas lojas virtuais.

Segundo TIC DOMICÍLIOS (2007), uma base de 396 entrevistados, a porcentagem e proporção das formas de pagamento para as compras na Internet tendem a um índice para:

- Uso de cartão de crédito de 49,47%,;
- Boleto bancário de 39,06%;
- Pagamento na entrega de 5,41%;
- Débito on-line/transferência eletrônica é de 7,21%;
- Outras formas de pagamento de 4,87%;
- 1,45% não souberam responder.

Albertin (1999), afirma que as transações financeiras por meio eletrônico somente obterão sucesso se ocorrerem de maneira simples, segura, barata e universalmente aceita. A chave será encontrar uns poucos mecanismos, largamente aceitos, que possam ser utilizados pela maioria dos participantes.

De acordo com Silva (2000), possuímos diversas formas de pagamento virtuais sendo algumas delas: Cartões de crédito, Ecash, Cybercash, Netcheque, NetCash, Chekfree, Débito on-line, etc.

#### 4.1 Cartões de crédito

De acordo Silva (2000) o cartão de crédito (*e-cred*) foi primeira forma de pagamento que surgiu via web. Este sistema é muito difundido nas lojas físicas, pois em qualquer parte do mundo desde que qualquer pessoa possua um cartão de crédito e que este seja aceito pelo comerciante, e via consulta, é realizado seu pagamento. Com o aperfeiçoamento do uso dos cartões de créditos, logo ele foi incorporado nas lojas virtuais como uma forma de pagamento das compras realizadas nos e-commerce.

Para o uso dos cartões de créditos o consumidor acessa a página do comerciante, verifica e escolhe os produtos e propõe o pagamento por cartão de crédito ao comerciante. Este acessa o seu banco e pede autorização do crédito pelo número de cartão do consumidor e respectiva quantia. O banco conclui a autorização e informa o comerciante para concluir a venda, este informando em seguida ao consumidor que a transação foi completada. Depois o comerciante acessa o seu banco e pede o pagamento de uma série de vendas feitas por cartão de crédito. O banco acessa a entidade emissora do cartão e obtém desta o respectivo valor, a entidade emissora do cartão atualiza a conta do consumidor.

Este método apresenta uma grande vantagem para o comerciante, que é a imediata verificação da legalidade do cartão. Neste sistema, o pagamento pode ser realizado quase instantaneamente sem necessidade de o comerciante esperar um tempo significativo para que o banco proceda aos pagamentos, o que acontece em regra com o comércio tradicional com cartões de crédito.

Para que não haja perdas de informações relacionadas com os cartões de crédito. O sistema deve garantir a não repudição e a geração de documentos que possam resolver possíveis controvérsias. Os recibos são gerados eletronicamente, e como tal, as demandas deverão ser resolvidas baseando-se em documentação digital disponível.

## 4.2 E-cash

Segundo Albertin (2000) o *E-cash* é uma das formas de pagamento eletrônico em grande expansão sendo um novo conceito nos sistemas de pagamento *on-line*, porque combina conveniência computadorizada com a segurança e a privacidade considerada como uma das mais avançadas tecnologias. Na prática esta é uma forma de proceder ao pagamento de baixo valor, reduzindo os custos de taxas burocráticas, existente no cartão de crédito.

A moeda virtual *E-cash* são parecidas com a moeda real, como as notas têm valor em si mesmo, o *E-cash* também tem o seu valor predeterminado, devendo por isso também ser portadores de um certificado de valor, e cuja transferência para outra pessoa deve ser fácil e rápida, sem grandes necessidades de correções, ou de verificação de autenticidade.

O *E-cash* é fornecido por um banco emissor aos usuários em troca de dinheiro real, por meio de uma transação com cartão de crédito ou caixa automático, enviando dinheiro a um banco, de forma criptografada, contendo uma lista de números de 64 bits (de difícil reprodução). Cada número corresponde a um valor especificado em dinheiro, que é registrado pelo banco emitente através de uma mensagem de correio eletrônico informando a quantia equivalente em dinheiro e satisfaz o alto grau de segurança dos bancos exigido nos ambientes de rede eletrônica, exclusivamente através das inovações obtidas na criptografia por chave-pública. Depois de gasto o *E-cash*, o fornecedor da mercadoria troca o *E-cash* por dinheiro real.

## 4.3 Cybercash

Segundo Silva (2000), a forma de pagamento utilizando a moeda virtual Cybercash, oferece uma moeda eletrônica, que estará vinculado a uma conta bancária, ou a um cartão de crédito. Para que o dinheiro entre no Cybercash, é necessário que faça um depósito via conta bancária ou cartão de crédito. Este recurso só existe em sites apropriados na Internet.

Todo o sistema possui dois pares de chaves pública-privada. A transação pode ser descrita em sete etapas:

- O cliente dá uma ordem de compra ao vendedor, e recebe a fatura;

- O cliente usa a cartão de CyberCash, o qual gera um pagamento codificado que é enviado ao vendedor;
- O vendedor decodifica a ordem de pagamento e envia-a para o servidor de CyberCash;
- Servidor de CyberCash recebe a mensagem da Internet, usa ferramentas dedicadas para decodifica-la e a envia para o banco do vendedor;
- O banco do vendedor envia então a transação ao banco do cliente que emite uma aprovação ou negação para o banco do vendedor;
- Este código é enviado ao servidor de CyberCash;
- Servidor CyberCash emite então um código de aprovação ou de negação ao vendedor.
- As etapas 1, 2, 3 e 7 ocorrem na Internet e envolvem uma combinação de chave pública codificada e chave simétrica. As etapas 4 e 6 ocorrem sobre linhas dedicadas. A etapa 5 ocorre nas redes dedicadas dos bancos.

Modelo simplificado de uma transação com a Cybercash.

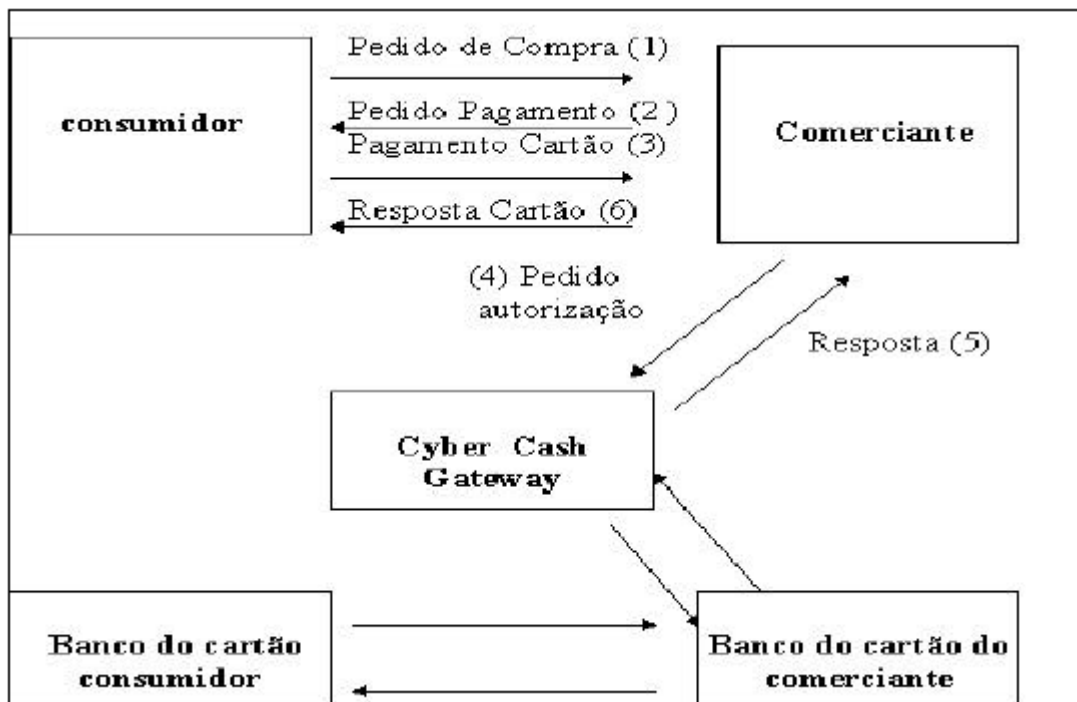


Figura 2: Pagamento Virtual do tipo Cybercash

Fonte: Silva (2000), página 98

#### 4.4 Netcheque

Segundo Abdala (2004) e Albertin (2000), “O NetCheque é uma forma de pagamento eletrônico que pode ser utilizado da mesma forma que os cheques tradicionais.” Porém os cheques eletrônicos utilizam os meios eletrônicos para assinar, endossar e autenticar o pagador, ou seja, confirmar a validade do Netcheque banco pagador e a conta do banco. Os cheques eletrônicos contêm o nome do pagador; a identificação da instituição financeira; o número da conta bancária; o valor do cheque; e o nome de quem vai recebê-lo.

O autor ainda cita que esta transação pode ser definida como:

“Os NetCheques são, então, e-mails assinados pelo pagador, autorizados através da sua assinatura eletrônica (código criptográfico) e enviados para o receptor. Este processo é protegido pelo sistema de criptografia. A assinatura do usuário cria o cheque, enquanto o endosso da pessoa a quem se paga o transforma numa ordem para o computador do banco. O mecanismo pode funcionar mesmo se o consumidor não tiver saldo, pois o banco pode emprestar o dinheiro. O mecanismo de crédito é equivalente ao do cartão de crédito.”

#### 4.5 Netcash

Silva (2000) definiu que esta moeda de pagamento virtual pode ser descrita da seguinte forma:

“A NetCash é uma moeda digital que funciona do seguinte modo: atribui um número de série a cada moeda, que é gravado durante a emissão. Quando a moeda é apresentada no servidor, este vai verificar se ela existe na lista de moedas emitidas. Se existir, é uma moeda válida e pode ser utilizada. Entretanto, se o número de série da moeda não estiver atualizado na lista, significa que a moeda foi gasta e suprimida da lista ou que nunca esteve na lista. Em qualquer dos casos, a moeda é inválida.”

#### 4.6 Débito on-line

Este foi criado com o intuito de atender com maior mobilidade, conforto e segurança as transações bancárias. A opção de fazer o pagamento através do débito on-line é válida somente para os clientes associados a alguma agência bancária tais como: Sicoob, Banco do Brasil e outros; e que possuam uma senha de acesso ao Internet Banking de

8 dígitos específica para a Internet ("senha de auto-atendimento"), diferente da senha de 6 dígitos que é utilizado com o cartão de crédito, por motivos de segurança. Senha esta que é ativado, automaticamente, em sua tela por um teclado virtual que é utilizado somente pelo mouse por meio de cliques no número/letra desejada. A utilização do teclado evita que pessoas maliciosas por meio de técnicas, obtenham as suas informações confidenciais. A transação é realizada diretamente pelo site da agência bancaria na Internet, em ambiente seguro. O débito on-line é válido apenas para conta corrente. Conta-poupança geralmente é aceita para esta opção. Após a realização do pagamento, o banco pode levar o prazo de até 2 (dois) dias úteis para informar que o pagamento foi realizado. Somente após essa confirmação é que entra em vigor seu prazo de entrega, que geralmente as empresas de comércio eletrônico colocam em sua política de privacidade sobre a entrega do produto comprado. Esta opção disponibiliza apenas pagamentos à vista.

Esta forma de pagamento também é muito utilizada para efetuar pagamentos de títulos. Normalmente os bancos colocam um horário máximo de pagamento, ou seja, quando for efetuado um pagamento depois daquela hora determinada pelo banco, o pagamento só será efetivado no dia seguinte mediante ao saldo existente na conta, caso o saldo seja insuficiente o pagamento é cancelado.

Também podem realizar transações de consulta, como: saldo, extrato, lançamentos futuros, histórico de operações, carteira de cobrança, extrato de investimento, tarifas, indicadores econômicos. Você pode realizar transações de pagamentos de ficha de compensação e contas de consumo, cancelar um agendamento, emitir recibos de pagamentos já efetuados e efetuar transferências tipo TED, entre contas e DOC.

As agências bancárias possuem modernos recursos disponíveis no mercado para que suas transações pela Internet sejam feitas com a máxima segurança possível, evitando que sejam interceptadas por outras pessoas ou equipamentos. Os dados de sua conta corrente e senhas trafegam pela Internet de forma embaralhada, codificadas (Criptografadas) com chave de 128 bits. Isso garante a troca segura das informações. Além disso, a imagem do cadeado de segurança fechado ou de uma chave no seu navegador indica a segurança das informações transmitidas.

Segundo FEBRABAN (2007), Federação Brasileira dos Bancos, as transações bancárias efetuadas por meio dos sites de Internet banking cresceram 50% entre 2003 de 2004

respondendo a 13% do total das movimentações das agências bancárias. Tendo uma grande adesão de correntistas à Internet devido à melhora na segurança dos sites e na oferta e facilidade de serviços oferecidos. Segundo o mesmo os bancos investiram na segurança física de seus pontos de atendimento um investimento R\$ 6 bilhões em 2006.

As operações bancárias feitas no Brasil via Internet chegaram a 6 bilhões em 2005. O número ultrapassa as transações feitas em caixas comuns de banco. Os caixas comuns registram 4 bilhões de operações no mesmo período. Em 2000, 8 milhões de pessoas acessavam a Internet banking. Hoje, são mais de 26 milhões de usuários utilizam Internet banking.

## 5 QUESTÕES DE SEGURANÇA

A Internet tem se transformado em uma ponte de ligação entre o comércio eletrônico e os internautas, para as transferências de dados ou transações bancárias, as quais trouxeram novas oportunidades de negócios para todos os tipos de usuários. Com o rápido crescimento, a preocupação em como conduzir negócios on-line resultou em que a segurança é fator fundamental para o sucesso dos negócios na Internet, devido aos ataques de criminosos *on-line*.

De acordo com TIC DOMICÍLIOS (2007), em uma base de 2924 entrevistados:

- 44,56 % não tiveram problemas de segurança usando a Internet;
- 2,34 % apresentaram problema com ataques, resultando em acesso não autorizado ou perda de informação;
- 7,89 % sofreram ataques de vírus, resultando em danos no software ou hardware (conjunto de peças físicas que compõe um computador);
- 1,85 % tiveram abuso de informação pessoal enviada pela Internet;
- 0,60 % sofreram fraudes bancárias ou algum outro tipo de problema com o banco;
- 0,26% tiveram fraudes com cartão de crédito;
- 1,14 % tiveram outros problemas de seguranças;
- 29,95% não responderam.

Alguns usuários tomaram medidas de segurança com relação com seu computador, tendo:

- 70,24 % que usam antivírus;
- 14,25 % usaram firewall pessoal;
- 13,93 % usaram software de anti-spyware;
- 16,40 % não tomaram nenhuma medida de segurança;

- 10,87 % não responderam.

Segundo Thomson (2003) e Gonçalves (et al, 1999), o primeiro passo para se falar de segurança é identificar quais os principais tipos de ameaças que podem existir a essa segurança, que podem ser: Acesso não autorizado (*unauthorized access*), Alteração de dados (*data alteration*), exposição de dados confidenciais, monitorização (*Monitoring*), negação de serviço (*Service Denial*), perda ou destruição de dados, repúdio (*Repudiation*), spoofing e vulnerabilidade ou erros no software.

- Acesso não autorizado (*unauthorized access*) - consiste em acessar ilegalmente ou abusar de um sistema de informática para capturar dados de transações comerciais ou não.
- Alteração de dados (*data alteration*) - altera os conteúdos de uma transação durante uma transmissão, tais como “usernames”, números de cartões de crédito, quantias envolvidas, etc., para a aquisição de dados confidenciais.
- Exposição de dados confidenciais - Qualquer dado, independente que seja do lado do usuário ou do sistema, quando cai na rede, esta vulnerável a ataques. Quando os dados caem na rede, se tornam acessíveis a qualquer tipo de usuário, e até que possa chegar à outra ponta, passa por diversos pontos, dividindo seus dados em pacotes, isso não assegura que todos os pacotes passaram pelos mesmos computadores, essa divisão de dados em pacote é clássico do protocolo TCP/IP (*Transfer Control Protocol / Internet Protocol*).

Contorna-se isso reduzindo as informações necessárias no servidor web, restringindo o público alvo, os meios de acesso a essas informações, utilizando algum critério de segurança como a autenticação e SSL (*Secure Sockets Layer*). Os *Sites Web* devem ser atualizados constantemente, devido às atualizações de software por parte da hospedagem para manter a integridade dos dados do usuário.

De acordo com Thomson (2003), “O servidor Web é inerentemente uma máquina publicamente acessível e só deve conter informações que precisam ser fornecidas ao público ou que foram recentemente coletados do público.”.

- Monitorização (*Monitoring*) - baseia-se em espiar informações confidenciais que são trocadas durante uma transação.
- Negação de serviço (*service denial*) - consiste na negação de acesso ao serviço, ou até ao encerramento do mesmo.
- Perda ou destruição de dados - Independente do dado a ser guardado no servidor Web, este deve ser constantemente feito um backup (copia de todos os arquivos selecionados, aonde podem ser gravadas em diversas mídias tais como: próprio HD, CD, DVD, Fita, etc), pois nenhum dado estará totalmente seguro, fisicamente. O hardware de hoje esta cada vez mais veloz. As qualidades de discos rígidos estão melhorando, os administradores estão buscando um desempenho maior. Mas mesmo assim deve ser realizada uma copia fiel do sistema em questão, em várias mídias e guarda-las em locais seguros e diferentes. Certificando-se também de que este backup funcionará, quando for necessária fazer uma recuperação dos dados, devida a alguma falha qualquer, seja de software, hardware ou ataque.
- Repudiação (*repudiation*) - ocorre quando uma das partes envolvidas na transação nega que a mesma aconteceu ou foi autorizada.
- Spoofing - consiste num site falso passando por servidor de modo a acessar ilicitamente dados de potenciais clientes ou simplesmente tentando sabotar o serviço prestado pelo servidor.
- Vulnerabilidade ou erros no software - Um dos maiores problemas de segurança em qualquer software é em geral na sua construção. Estes problemas são causados por más especificações no projeto, a falta de atenção na estruturação, alterações no projeto, profissionais envolvidos, custo reduzido, e o curto prazo para entrega. Desta forma os erros de construção podem conter brechas de segurança, chamada de vulnerabilidade. A vulnerabilidade é definida como uma falha no projeto ou na implementação de um software ou sistema operacional, que quando explorada resulta na violação da segurança de um computador. Existem casos onde um software ou sistema operacional instalado em um computador pode conter uma vulnerabilidade que permite sua exploração remota, ou seja, através da rede. Muitas das vezes os softwares não são testados como deveriam, sendo assim a fase de teste quase sempre fica a cargo do cliente.

## 5.1 Política de segurança

A política de segurança é o ato de atribuir direito e responsabilidades aos usuários de uma empresa e com as informações neles armazenados. Ela também define as atribuições de cada um em relação à segurança dos recursos com os quais trabalham, devendo prever o que pode ou não ser feito na rede da empresa e o que será considerado inaceitável.

A política de segurança da informação é o conjunto de diretrizes, normas e procedimentos que devem ser seguidos que tem por objetivo de dar a noção e orientar os funcionários, clientes, parceiros e fornecedores para o uso seguro do ambiente informatizado, com informações sobre como gerenciar, distribuir e proteger seus principais ativos.

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

## 5.2 Motivos de implicações das inseguranças

No momento a Internet proporciona ao usuário um acesso fácil e rápido às informações uma vez que ao andar pelas ruas de uma cidade, encontram-se vários comércios que oferecem serviço de disponibilidade de navegação pela Internet (lanHouse, cybercafe, etc.). De olho nessas facilidades os donos de comércios de lojas físicas estão se juntando a esta rede com os seus sistemas voltados para o comércio virtual (*e-commerce*), para tanto as empresas sentem a necessidade de restringir o acesso de usuário malicioso, que tentam de toda forma conseguir algum benefício, ou lesar alguém roubando números de cartão de crédito, entre outras. Dados estes confidencias que por sua vez são protegidos por via barreiras físicas: firewalls, IDS, SSL, entre outros mecanismos.

Em conseqüência ao rápido crescimento da Web, as empresas sentem a necessidade de expandir, caso contrário podem retardar o seu crescimento. Muitas vezes consumidores desconfiados, preferem fazer compras na própria loja física ao invés de fazer sua compra on-line, por causa da insegurança que algumas empresas transmitem.

Quando pensamos em segurança, do lado do *Site Web* deve se levar em conta à importância dos dados a serem protegidos de qualquer praga virtual. Isso não quer dizer que

se deve para qualquer site construir a maior barreira de segurança, pois se leva em consideração o custo benefício. Do lado do internauta não tem como prever o nível de segurança nele empregado, pois na rede temos diversos tipos de usuário, sendo assim uma brecha para a invasão.

### 5.3 Mecanismos de segurança

Sabemos que no mundo real não existem sistemas totalmente seguros e o mundo virtual segue a mesma natureza. Por maior que seja a proteção adotada pelos administradores de rede, estaremos sempre sujeitos as invasões, roubos e ataques.

Segundo Silva (2000),

“Atualmente já nos utilizamos da Internet para realizar diversos serviços corriqueiros, como compras, serviços bancários, investimentos, além de negócios ou troca de informações confidenciais via e-mail. Grandes partes dos problemas ocorrem por puro desconhecimento dos procedimentos básicos de segurança por parte dos usuários. Como mecanismos de segurança no comércio eletrônico podem ser citados os seguintes”.

- Barreiras físicas (firewall)
- IDS (*Intrusion Detect System*)
- Criptografia
- Protocolos (regras) de autenticação
- Certificados digitais
- Assinaturas digitais
- Selos digitais
- SSL

### 5.3.1 Firewalls

Segundo Albertin (2000) e Silva (2000) foi desenvolvido com o intuito de impedir o acesso não autorizado às redes de comunicações utilizadas por empresas. O Firewall é um mecanismo de segurança resistente a invasões, composto por um único sistema, ou por um conjunto de componentes básicos que o constituem. O Firewall pode em sua arquitetura trabalhar em conjunto com softwares de antivírus, para que ambos façam a filtragem de dados da rede, centralizando assim o controle de todo o tráfego que passa pela rede, tendo como finalidade proteger as redes das outras possibilitando ainda um nível maior de segurança.

O Firewall deve estar sempre presente entre redes públicas e privadas ou entre duas ou mais redes privadas. Esse controle é chamado de política de segurança durante a sua implementação, que bloqueia ou permite a passagem dos dados entre as redes.

De acordo com Silva (2000), “O uso de Firewall limita o acesso, e como tal, certas operações como publicidade e compra/venda de produtos poderão não ser feitas ou então serem minimizadas”.

Este mecanismo gerencia os acessos entre duas redes diferentes, evitando que a rede protegida fique facilmente vulnerável e exposta a ataques externos, centralizando e controlando todo o tráfego de entrada e saída, ele pode bloquear a entrada ou saída de qualquer serviço que fuja da sua política de segurança, evitando assim que a segurança se torne vulnerável.

Sua forma de implantação é local, ou seja, dentro da própria rede, onde a segurança é monitorada de forma mais eficaz, no caso de alguma intercorrência quanto a sua política de segurança os procedimentos de defesa necessários tais como: disparo de alarmes, registro de ocorrências, contra-ataque, bloqueio à passagem de todo o tráfego, etc.

Para que um Firewall seja eficaz, é necessário que todo o tráfego da rede atenda sua política de segurança que por sua vez deve ser bem estruturada, ou seja, bem configurada, pois assim não será capaz de proteger uma rede dos ataques que não passam por ele.

Como qualquer outro software ou hardware, o Firewall, possui limitações tais como: uma vez sofra uma infiltração de qualquer usuário ou código malicioso de nada irá adiantar mais a sua política de segurança.

A sensibilidade do Firewall sofre muitas alterações, pois a cada instante surgem novos tipos de ataques, entre outros, fazendo-se necessário uso de outros serviços de segurança auxiliar IDS, para que sua política de segurança não seja quebrada.

O alto custo envolvido na implementação e na manutenção e as regras de segurança embutidas por ele limitam acesso a operações comerciais para compra e venda de produtos, resultando numa minimização de transações comerciais.

### 5.3.2 IDS

As ferramentas para segurança de computadores e redes são necessárias para proporcionar transações seguras. Geralmente, as empresas concentram suas defesas em ferramentas preventivas como firewalls, antivírus, mas acabam ignorando as ferramentas de detecção de intrusão IDS (*Intrusion Detection System*), que é um composto de hardware e software que trabalham em parceria para vigiar e descrever todos e quaisquer eventos imprevistos ou anormais que relata a existência de um ataque seja quando ele ainda irá acontecer, ou está acontecendo no momento ou ainda que já aconteceu.

Podemos descrever um ataque seja ele forte ou fraco, como uma invasão por meio de hacker, ou códigos maliciosos a sua política de segurança. Caracteriza-se como um ataque bem sucedido a conclusão de uma invasão ou até mesmo a negação de serviço que infiltrou sua segurança interna.

O IDS monitora a segurança da sua rede interna, varrendo todo tráfego que por ele passar. Focaliza também os ataques corriqueiros mais freqüentes utilizados, juntamente fica de prontidão para novos tipos de ataques, fornecendo assim uma varredura sempre atualizada, que pode limitar os ataques perdidos, ou não identificados, baseados principalmente no nível de ameaça a sua política de segurança e freqüência de utilização.

Para que o IDS funcione corretamente, é necessário que um administrador de rede bem treinado e capacitado para faz a manutenção do sistema de segurança, atualizando o sistema constantemente com as novas definições de ataques que são fornecidos e identificados por instituições de segurança ou fornecedor do IDS.

Um dos principais benefícios do IDS é monitoração de negação de serviço, pois possui um conjunto de assinaturas que é fornecida pelo fornecedor, provendo assim uma usabilidade do recurso. O seu monitoramento não afetará o desempenho da sua rede.

A implementação do IDS para redes, é composto de sensores que são colocados nos segmentos da rede que se deseja monitorar. Pode também instalar o IDS na máquina, que usará o sistema de log do seu sistema operacional para dizer exatamente o que o atacante fez. Mais usado em sistemas de tráfego crítico, apresentando um menor risco a sua segurança.

Possui também um verificador de integridade de arquivos baseado em máquina.

O IDS instalado em redes, monitora apenas o segmento da rede aonde foi instalado. Sendo assim inadequado para tratar de ataques mais complexos e ele também não consegue monitorar tráfego em sessões encriptadas. Já o IDS instalado na máquina irá monitorar apenas aquela máquina local, sendo assim um recurso mais caro, ainda ele requer mais desempenho de máquina para que funcione corretamente.

### **5.3.3 Criptografia**

Criptografia é o ato de codificar dados em informações aparentemente sem sentido, ou seja, as mensagens e dados são convertidos em um formato ilegível para que pessoas não consigam ter acesso às informações confidenciais. Apenas quem possuir o algoritmo de decodificação, poderá fazer a conversão para um formato legível. Segundo Silva (2000), “Contudo, as técnicas modernas de encriptação são virtualmente “inquebráveis”.

A criptografia também faz parte de um campo de estudos que trata das comunicações secretas, usadas, dentre outras finalidades, para: autenticar a identidade de usuários; autenticar e proteger o sigilo de comunicações pessoais e de transações comerciais e bancárias; proteger a integridade de transferências eletrônicas de fundos.

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

Os métodos de criptografia atuais são seguros e eficientes e baseiam-se no uso de uma ou mais chaves. Uma chave é uma seqüência de caracteres, que pode conter letras, dígitos e símbolos (como uma senha), e que é convertida em um número, utilizada pelos métodos de criptografia para codificar e decodificar mensagens. Atualmente, os métodos de criptografias são divididos em: a criptografia de chave única e a criptografia de chave pública e privada.

De acordo com Silva (2000) a criptografia de chave única ou privada utiliza a mesma chave tanto para codificá-la quanto para decodificar mensagens. Apesar de este método ser bastante eficiente em relação ao tempo de processamento, ou seja, o tempo gasto para codificar e decodificar mensagens tem como principal desvantagem à necessidade de utilização de um meio seguro para que a chave possa ser compartilhada entre pessoas ou entidades que desejem trocar informações criptografadas.

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

Seja o exemplo abaixo, onde pessoa 1 e pessoa 2 querem se comunicar de maneira sigilosa. Então, eles terão que realizar os seguintes procedimentos:

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

Apesar de este método ter o desempenho bem inferior em relação ao tempo de processamento, quando comparada ao método de criptografia de chave única ou privada,

apresenta como principal vantagem a livre distribuição de chaves públicas, não necessitando de um meio seguro para que chaves sejam combinadas antecipadamente. Além disso, pode ser utilizado na geração de assinaturas digitais.

#### **5.3.4 Protocolos (regras) de autenticação**

Os Protocolos de autenticação são conjuntos de regras estabelecidos em sua configuração, que têm como objetivo principal a realização de trocas seguras de dados entre as redes. Sendo assim, são capazes de ignorar, e também de tomar medidas de segurança, em relação a qualquer identidade falsa, que tentar entrar na rede. De acordo com Silva (2000), “Os três mais utilizados ou pelo menos mais conhecidos são: o SSL, o HTTPS, SET.”.

#### **5.3.5 Certificados digitais**

Como a Internet é amplamente utilizada para o processamento de dados, troca de informação e documentos entre cidadãos, governo e empresas, veio a tornar-se um meio de comunicação alternativo para a disponibilização de diversos serviços, com uma maior agilidade, facilidade de acesso e redução de custos. Mas para que estas transações eletrônicas não se tornem uma dor de cabeça necessitam de mecanismos de segurança capazes de garantir autenticidade, confidencialidade e integridade das informações eletrônicas. A certificação digital é a tecnologia que provê estes mecanismos. Sendo um arquivo eletrônico que contém dados de uma pessoa ou instituição, que são utilizados para comprovar sua identidade, como semelhante o RG, CPF, etc. São encontradas em certificados digitais algumas informações tais com:

- Dados que identificam o dono (nome, número de identificação, estado, etc);
- Nome da Autoridade Certificadora (AC) que emitiu o certificado;
- O número de série do certificado;
- O período de validade do certificado;
- A assinatura digital da AC.

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

O certificado digital contém a chave pública do usuário e os dados necessários para informar sua identidade. Permite ser usado em aplicações do tipo de comércio eletrônico, transferência eletrônica, etc. O certificado pode ser distribuído na Internet. Com isso, uma pessoa ou instituição que queira comprovar a assinatura digital de um documento pode obter o certificado digital a ela correspondente.

De acordo com Silva (2000),

“O Certificado Digital é emitido e assinado por uma Autoridade Certificadora Digital (*Certificate Authority*), que emite o Certificado utilizando as mais avançadas técnicas de criptografia disponíveis e de padrões internacionais (norma ISO X.509 para Certificados Digitais)”.

Vimos rotineiramente o uso dos certificados digitais nas conexões seguras com sistemas na Internet, uma delas é o seu acesso à sua conta bancária pela Internet, é possível checar se o site apresentado é realmente da instituição que diz ser, através da verificação de seu certificado digital; este tem que se assegurar de sua identidade antes de fornecer informações sobre a conta; ou através de e-mail, seu aplicativo de e-mail pode utilizar seu certificado para assinar "digitalmente" a mensagem, de modo a assegurar ao destinatário que o e-mail é seu e que não foi adulterado entre o envio e o recebimento.

### **5.3.6 Autoridade Certificadora**

Autoridade Certificadora (AC) é a entidade responsável por emitir certificados digitais, ou seja, uma espécie de cartório virtual. Estes certificados podem ser emitidos para diversos tipos de entidades, tais como: pessoa, computador, departamento de uma instituição, instituição, etc. Os certificados digitais possuem uma forma de assinatura eletrônica da (AC) que o emitiu. Graças à sua idoneidade, a (AC) é normalmente reconhecida por todos como confiável, fazendo o papel de "Cartório Eletrônico".

A (AC) realiza a emissão dos certificados seguros SSL, elas também são responsáveis por validar a identidade de um Website. O que mais se aproxima de uma

entidade normatizadora das autoridades certificadoras é o "Webtrust Compliancy Program" administrado pela AICPA/CICA. A maioria das CA's obedece aos critérios da Webtrust.

A utilização de chaves de encriptação assimétricas, uma pública e outra privada, implicam a existência de uma autoridade de certificação, no qual é garantida a identidade entre a chave pública e o titular a que ela pertence, se procede à identificação deste último e se atesta a validade da referida chave.

Um exemplo de Autoridade Certificadora é a entidade ICP-Brasil que regula um conjunto de entidades governamentais ou de iniciativa privada que serão responsáveis por assegurar que aquele par de chaves: privada e pública; pertence ao usuário.

Hoje em dia um dos grandes problemas que acontece na escolha de um certificado é o reconhecimento embutido nos navegadores e a marca do emissor do certificado.

O reconhecimento pelos navegadores da web é importante, porque existem sistemas operacionais tais como: Windows, Linux, Macintosh; e em cada um destes sistemas operacionais, existe mais de uma opção de navegador. O fato de utilizar um certificado que não tem o reconhecimento pela maioria dos navegadores, poderá fazer com que o internauta deixe de realizar negócios eletrônicos com a sua empresa pelo fato de ocorrer problemas de compatibilidade ou ainda pedindo a instalação de "plug-ins" por parte de usuário, o que certamente cria um efeito contrário ao desejado.

### **5.3.7 Assinaturas digitais**

A segurança, é a maior preocupação de todos aqueles que negociam pelos meios eletrônicos. A confiabilidade do documento digital está ligada à sua originalidade e à certeza de que ele não foi alterado pelos caminhos que percorreram até chegar ao seu destinatário.

De acordo com Silva (2000),

“Tal como as assinaturas escritas, o propósito de uma assinatura digital é garantir que um indivíduo que envie uma mensagem e realmente seja quem afirma ser. Resume-se a um código que pode ser enviado juntamente com uma mensagem que identifica de forma única o emissor da mensagem.”

### **5.3.8 Selos digitais**

Segundo o ICPBrasil (2007). O sistema de assinatura digital e registro de documentos eletrônicos (selos digitais ou e-Selo) garantem a integridade, a autoria e a validade jurídica de conteúdos eletrônicos através do uso de assinaturas digitais confiáveis. Com o selo um sistema baseado via web, pode incluir suporte a certificados digitais e carimbos de tempo, viabilizaria a utilização da assinatura digital de conteúdos eletrônicos em empresas comerciais. Possui ferramentas necessárias para permitir o armazenamento e o controle de fluxo porque ficam armazenados em bancos de dados criptografados, podendo ser acessados somente pelas partes contratadas ou previamente autorizadas pelo criador do documento, garantindo assim a privacidade das informações, prevenindo e detectando alterações ou manipulações conteúdos eletrônicos, qualquer pessoa pode verificar a autenticidade de um documento ou arquivo eletrônico.

Serve para gerar rubricas que associam data e hora a um documento digital. Utilizado na prova da existência de certo documento eletrônico em determinada data. Esta rubrica pode ser aplicada em vários casos como, por exemplo: e-mails, formulários web, contratos, imagens, notificações, procurações, relatórios, resultados de exames, prontuários médicos, entre outras; viabilizando assim a eliminação do uso do papel e a diminuição dos custos de emissão, armazenamento e descarte destes documentos.

### **5.3.9 Cookies**

Segundo Thomson (2003), os cookies são pequenas informações que os sites visitados por você podem armazenar em seu computador, ou seja, um cookie é uma informação (uma seqüência de caracteres) que os sites enviam aos navegadores e mantidos na memória, para que nas visitas posteriores o navegador reenvie os dados para o servidor dono do cookie. Ao encerrar a sua sessão com seu browser, todos os cookies que ainda não expiraram são gravados em um arquivo.

Sendo um recurso muito utilizado no comércio eletrônico, ele pode guardar informações do tipo: sua identificação como usuário e senha, preferências de layout; manter

listas de compras ou listas de produtos preferidos em sites de comércio eletrônico; personalizar sites pessoais ou de notícias, manter a lista das páginas visitadas em um site.

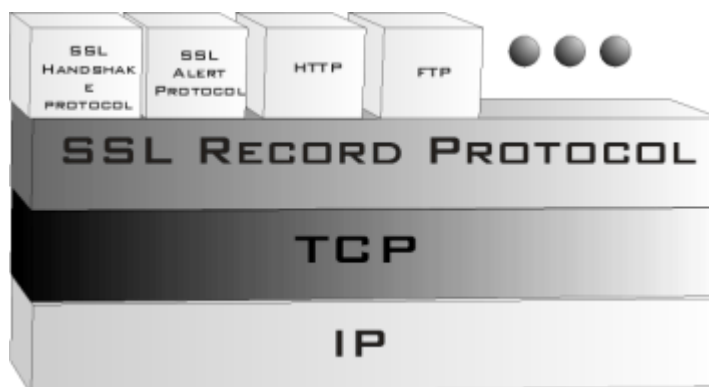
Estas preferências podem ser compartilhadas entre diversos sites na Internet, afetando assim a privacidade de um usuário.

### 5.3.10 SSL

Segundo o autor Krishnamurthy (2001) o SSL (*Secure Sockets Layer*) foi introduzido em 1994 pela Netscape e é a base padrão do TLS (Transporte Layer Security). O SSL é um protocolo entre as camadas de transporte e aplicação sendo comumente utilizada para codificar os dados trafegados entre o computador do usuário e o um Website de forma mais segura. Este protocolo previne que os dados trafegados possam ser capturados, ou mesmo alterados entre o navegador do usuário e o site visitado através de um processo de criptografia de dados, garantindo desta forma que as informações sigilosas fiquem intactas como os dados de cartão de crédito.

De acordo com site RNP (2008)

“A SSL é um conjunto de três protocolos situados, dois deles, a nível de aplicação e, o terceiro, entre o protocolo de aplicação e o TCP, como esquematizado na figura abaixo. Seu objetivo é prover um canal seguro, isto é, com privacidade, com garantia opcional de autenticidade dos pares e garantia de integridade da mensagem.”



Fonte: <http://www.rnp.br/newsgen/9803/https.html>

**Figura 3: Esquema de Níveis da SSL**

Segundo o autor Barros (2005), quando um visitante se conecta a um servidor que está utilizando o protocolo SSL, nota-se que o protocolo passa a ser https:// (no lugar do http:// padrão). Aliado a isto, a maioria dos browsers (como o Internet Explorer, por exemplo) mostram um cadeado. Quando este cadeado está sendo mostrado, o usuário sabe que as informações fornecidas por aquele Website não poderão ser interceptadas no seu trajeto, tornando assim segura a transação.

De acordo com Barros (2000) ainda pode-se obter um certificado digital SSL e para isso é necessário fornecer informações sobre o detentor do Website, tais como endereço, documentação e pessoa de contato. Com estes dados, é gerado um par de chaves de criptografia, que irão garantir o processo de codificação dos dados. Estas chaves são duas: Uma chave privada, que fica no servidor e uma chave pública que é utilizada, para gerar um CSR (Certificate Signing Request) que é submetido a uma autoridade certificadora (CA) que para validação dos dados cadastrais, através da comprovação da autenticidade dos documentos e da propriedade do Website, garantindo a validade do certificado. Ficando a cargo de a autoridade certificadora gerar o certificado definitivo, que deverá ser instalado pelo seu provedor responsável pela hospedagem de seu Website. Em geral, os browsers têm internamente gravados de fábrica uma lista de CA válidas fixa, e alguns browsers permitem que o usuário acrescente novas certificadoras a esta lista.

De acordo do com autor Kurose (2003), a SSL é muito simples e precoce, sendo muito implementada em browsers, servidores e produtos para comércio pela Internet fornecendo assim plataforma popular para transações com cartões de pagamento. No entanto, a SSL não foi produzida especificamente para com cartões de pagamento, mas sim para comunicações genéricas seguras entre um cliente e um servidor.

### **5.3.11 SET**

Segundo Abdala (2004) o protocolo SET (*Secure Eletronic Transactions*) foi desenvolvido visando atender o rápido crescimento no setor do comércio eletrônico junto com a exigência dos consumidores ao efetuar com segurança suas transações comerciais visando a atual forma de pagamento das operadoras de cartão de crédito. Ele não e por si só um sistema de pagamento, mas um conjunto de protocolos de segurança que habilita os usuários a

aplicarem a infra-estrutura existente de pagamento com cartão de crédito em uma rede aberta, como a Internet, de maneira segura.

A segurança do pagamento é obtida autenticando donos de cartão de crédito, comerciantes e bancos, garantindo a integridade e confiabilidade dos dados de pagamento e definindo os algoritmos e protocolos necessários para isso.

SET assegura o dono de cartão que as informações de seu pagamento são mantidas seguras e que só podem ser acessadas pelo destinatário desejado. SET cifra as mensagens para garantir confiabilidade das informações. A especificação precisa garantir que o conteúdo das mensagens não é alterado durante as transmissões entre emissor e receptor. SET provê assinaturas digitais, que garantem a integridade da informação de pagamento.

De acordo do com autor Kurose (2003), o protocolo SET requer os três participantes tenham certificados. Os certificados dos clientes e dos comerciantes são emitidos por seus bancos, assegurando, dessa maneira, que esses participantes tenham permissão para fazer compras e receber por vendas realizadas com cartões de pagamento. Comerciantes precisam verificar que o portador de um cartão é um usuário legítimo de um cartão de crédito, para resolver isto o SET usa assinaturas digitais e certificados do clientes para garantir a autenticação do portador de cartão de crédito. Ele é uma representação eletrônica do cartão de pagamento do cliente e contém informações sobre sua conta, a instituição financeira que o emitiu e outras informações criptografadas. O certificado do comerciante assegura ao consumidor que aquele comerciante está autorizado a aceitar compras feitas por cartões de crédito contendo informações do banco do comerciante da instituição financeira que emitiu o certificado de validade.

### **5.3.12 HTTPS**

De acordo com Albertin (2000) o protocolo HTTPS (HyperText Transfer Protocol Secure), é uma implementação do protocolo HTTP sobre uma camada SSL essa camada adicional permite que os dados sejam transmitidos através de uma conexão criptografada com autenticação do servidor e do cliente, através de certificados digitais. Com o SSL estabelece

que qualquer serviço será realizado com segurança ativada na Internet ou em sua intranet privada.

No uso de HTTPS, os certificados digitais são criptografados para garantir a sessão. HTTP sobre SSL é seguro e protegido de intrusões externas partido. Basicamente, qualquer outro site pode utilizar o protocolo HTTPS. Quase todos os tipos de browsers poderiam facilmente e facilmente conectar-se à Internet usando http ou https protocolos.

SSL utiliza um protocolo de reconhecimento de segurança para iniciar uma conexão segura entre o cliente e o servidor. Durante o protocolo de reconhecimento, o cliente e o servidor concordam sobre as chaves de segurança a serem utilizadas para a sessão e os algoritmos que a serem utilizados para criptografia. O cliente autentica o servidor; opcionalmente, o servidor pode solicitar o certificado do cliente. Depois do protocolo de reconhecimento, o SSL criptografa e decriptografa todas as informações no pedido HTTPS e na resposta do servidor.

O HTTPS representa um protocolo exclusivo que combina SSL e HTTP. Especifique https:// como uma âncora em documentos HTML que fazem link a documentos protegidos por SSL. Um usuário cliente também pode abrir uma URL especificando o https:// para solicitar um documento protegido por SSL.

Esta função permite que uma empresa revendedora na Internet possa permitir que usuários consultem as mercadorias sem segurança, mas preencham formulários de pedidos e enviem seus números de cartão de crédito utilizando segurança. Na maioria dos navegadores é exibido um ícone na forma de cadeado indicando que o site esta seguro.

#### **5.4 Fraudes em Comércio Eletrônico**

Os invasores vêm concentrando seus esforços na exploração de fragilidades dos usuários, para realizar fraudes comerciais e bancarias através da Internet, pois fraudar dados de servidores tanto comerciais ou de instituições financeiras atualmente não é fácil.

Segundo o órgão CERT.BR (2007) (*Centro de estudos resposta e tratamento de incidentes de segurança no Brasil*) o número de incidentes detectados na Internet tem

crescido muito rapidamente com um curto período de tempo. Normalmente estes ataques são relacionados com: Worm, D-Dos, Invasão, Ataques a servidores de Web e Fraudes.

De acordo com a pesquisa do mesmo órgão:

- Em 1999 foram detectados 3.107 casos;
- Em 2000 foram registrados 5.997 casos;
- Em 2001 foram detectados 12.301 casos;
- Em 2002 foram detectados 25.092 casos;
- Em 2003 foram reportados 54.607 casos;
- Em 2004 foram detectados 75.722 casos;
- Em 2005 foram detectados 68.000 casos;
- Em 2006 foram detectados 197.892 casos;
- Em 2007 foram relacionados 94.809 casos.

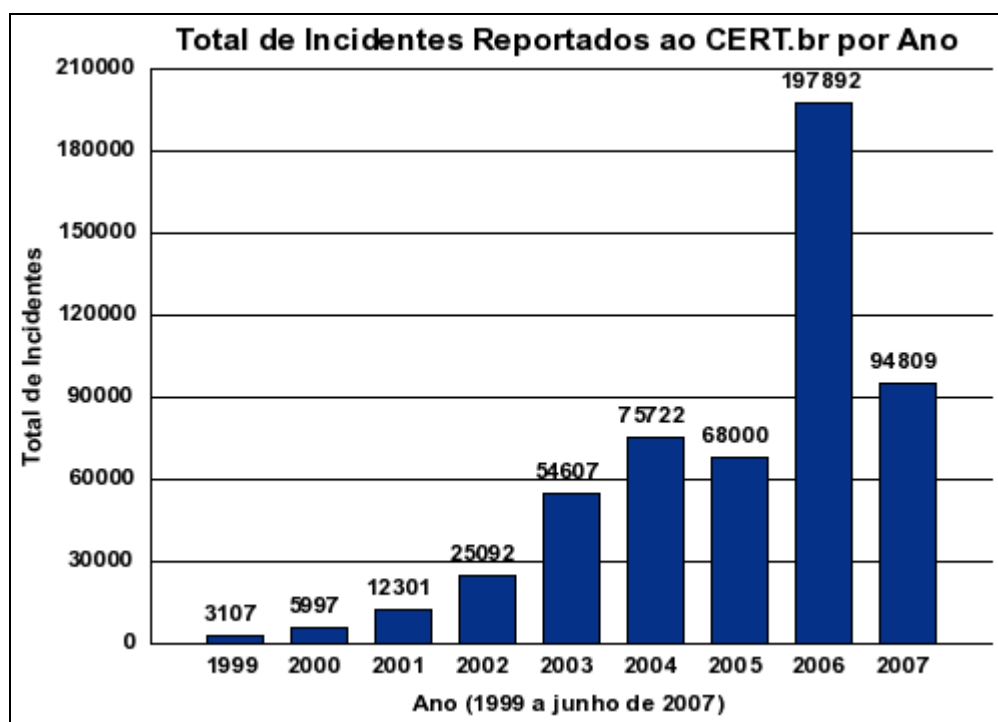


Figura 4: Total de incidentes reportados ao Cert.br por ano

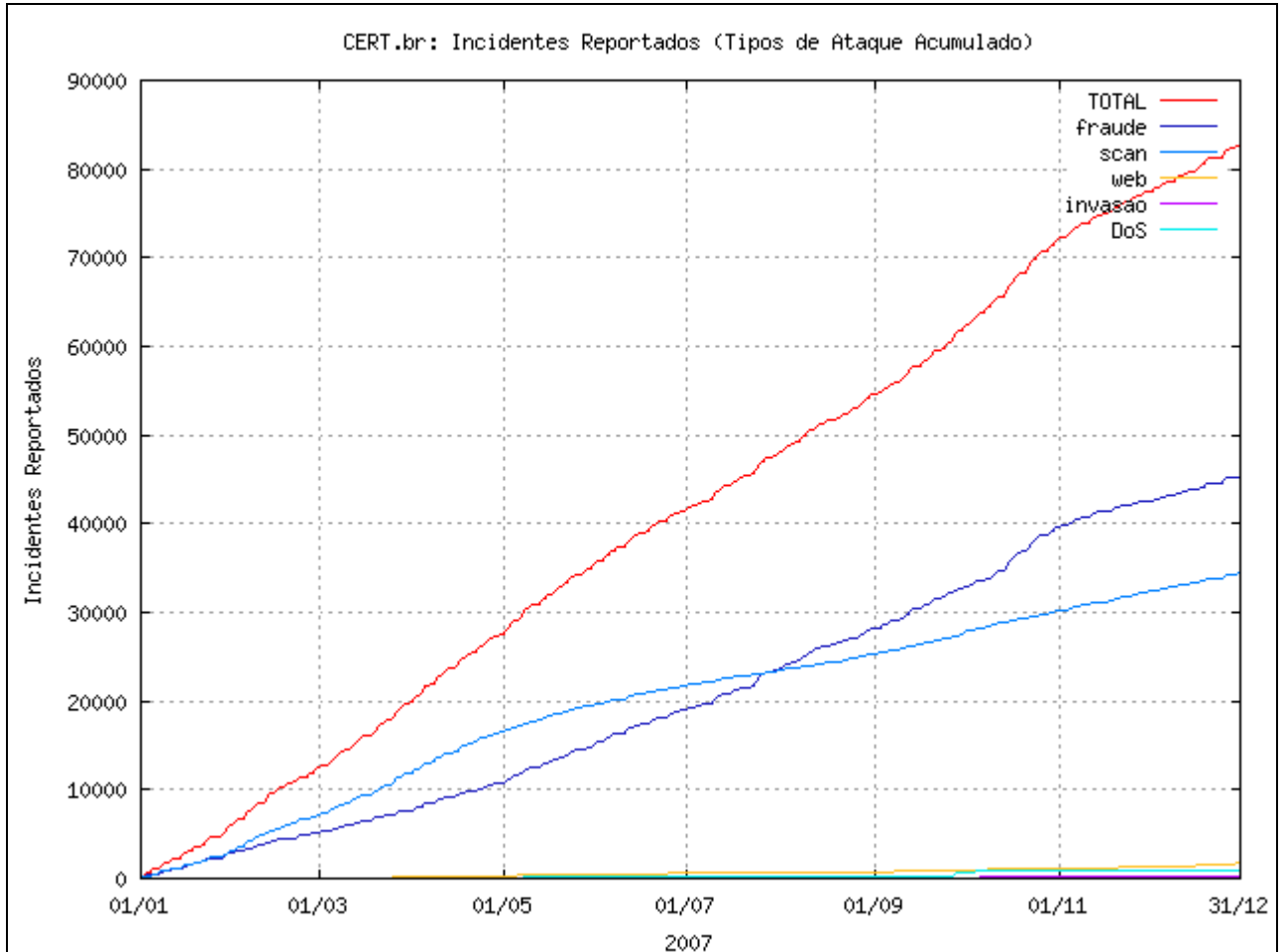
Fonte: <http://www.cert.br/stats/incidentes/>

Ainda segundo o mesmo órgão, agora no período dos meses de abril a junho de 2007, seguindo os tipos de ataques: Worm, Dos, Invasão AW (*Ataques a servidores Web*), Scan e Fraudes; vejamos abaixo:

**Quadro 5: Totais Mensais e Trimestrais Classificados por Tipo de Ataque.**

Mês	Total	worm (%)	dos (%)	invasão (%)	aw (%)	scan (%)	fraude (%)						
Jan	<b>24181</b>	18109	74	0	0	8	0	21	0	3132	12	2911	12
Fev	<b>15482</b>	9302	60	0	0	4	0	19	0	3907	25	2250	14
Mar	<b>16633</b>	9124	54	1	0	3	0	125	0	4850	29	2530	15
Abr	<b>14152</b>	6416	45	11	0	6	0	147	1	4584	32	2988	21
Mai	<b>13623</b>	5776	42	179	1	5	0	139	1	3107	22	4417	32
Jun	<b>10738</b>	4621	43	8	0	15	0	121	1	2092	19	3881	36
Jul	<b>10858</b>	4349	40	2	0	18	0	88	0	1779	16	4622	42
Ago	<b>11437</b>	4831	42	0	0	2	0	114	1	1831	16	4659	40
Set	<b>11906</b>	4620	38	480	4	33	0	152	1	2227	18	4394	36
Out	<b>13644</b>	3535	25	260	1	110	0	192	1	2648	19	6899	50
Nov	<b>9152</b>	3674	40	0	0	43	0	200	2	2188	23	3047	33
Dez	<b>8274</b>	3116	37	13	0	11	0	371	4	2063	24	2700	32
Total	<b>160080</b>	77473	48	954	0	258	0	1689	1	34408	21	45298	28

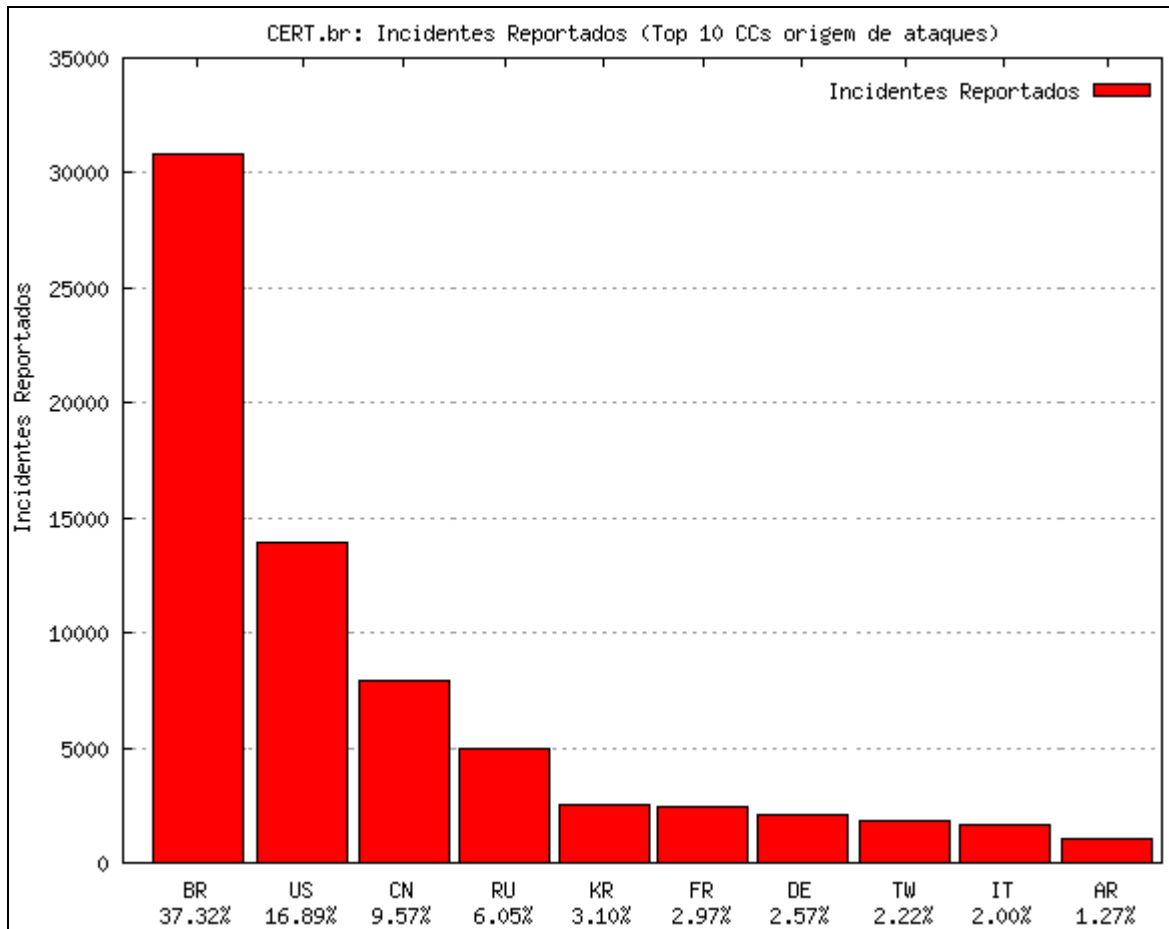
Fonte: <http://www.cert.br/stats/incidentes/2007-jan-dec/total.html>



**Figura 5: Incidentes reportados ao Cert.br (Tipos de ataques acumulado)**

Fonte: <http://www.cert.br/stats/incidentes/2007-jan-dec/tipos-ataque-acumulado.html>

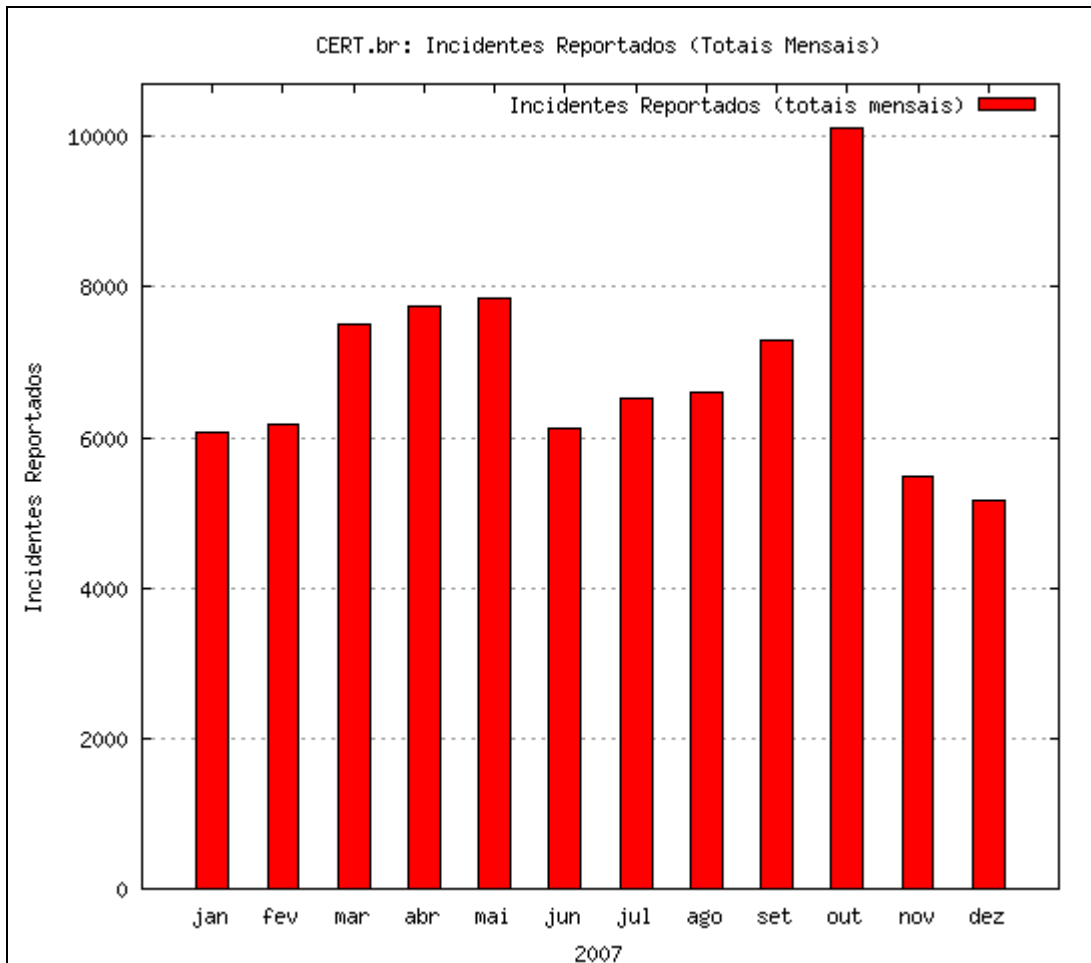
Nota-se que nesta figura acima a linha que representa as varreduras e as fraudes aumentam gradativamente não sofrendo quedas durante ano de 2007, já os ataques via Web, Ddos e Invasão não obtiveram muito sucesso neste ano, devido ao avanço das tecnologias de segurança. Ainda neste mesmo período e mesmo órgão, vejamos os incidentes reportados com ênfase nos países aonde o numero de transações eletrônicas é grande, como podemos ver abaixo o Brasil é o campeão em ataques com 34,75%.



**Figura 6: Incidente reportado ao Cert.br (Top de 10 países com origem de ataques)**

Fonte: <http://www.cert.br/stats/incidentes/2007-jan-dec/top-atacantescc.html>

O Brasil ocupa o primeiro lugar no ranking em ataques sofridos chegando a ter mais de 30.000 milhões de ataques reportados, como sendo de Womrs e ataques a servidores Web, analisado o gráfico da figura abaixo temos que os meses variavam nas épocas de datas comemorativas aonde o mês de outubro ocupa o primeiro lugar chegando a ter mais de 1.000 de incidentes seguido pelo mês de maio com aproximadamente 8 milhões de incidentes.

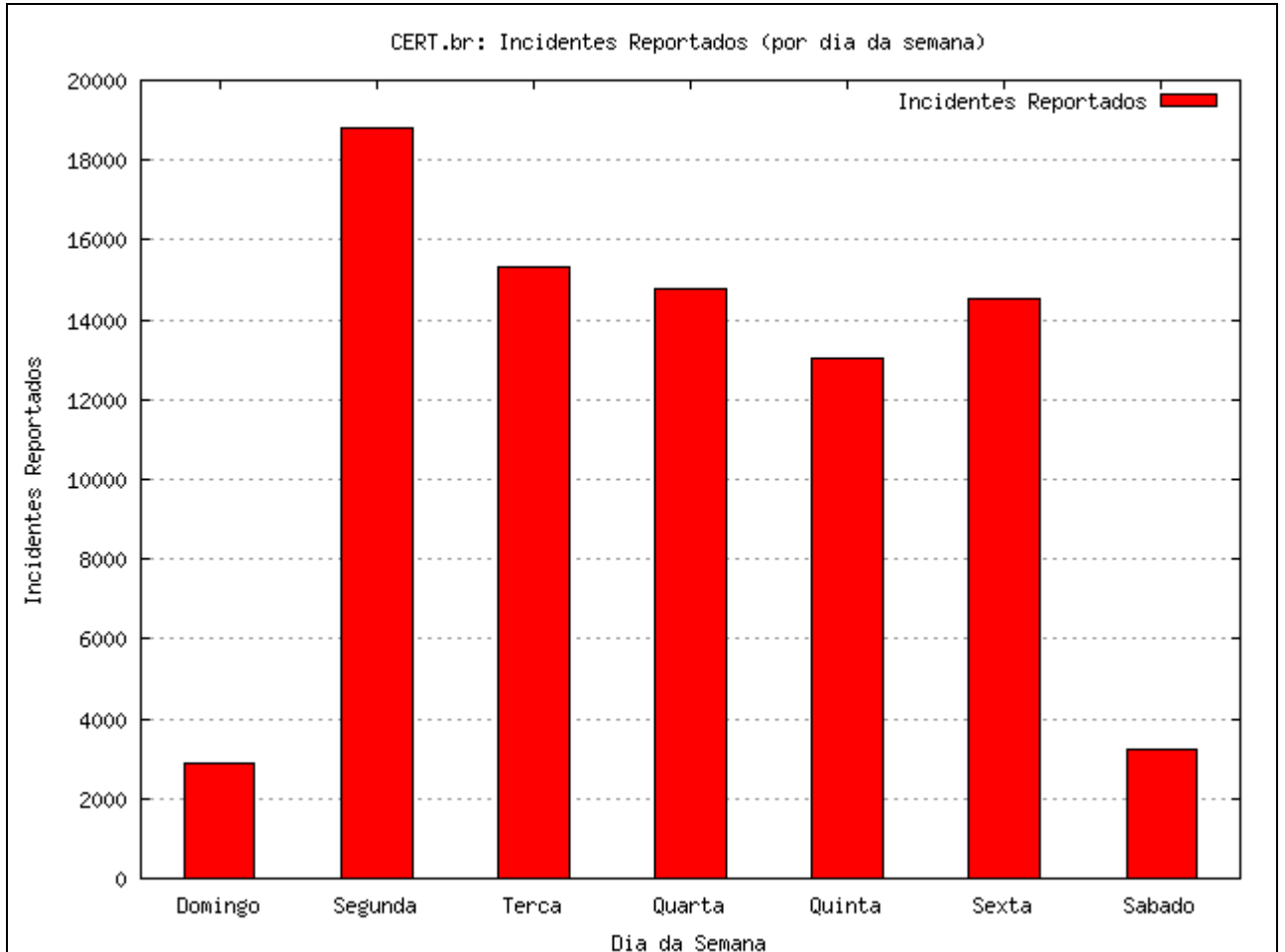


**Figura 7: Incidentes reportados ao Cert.br (Totais mensais)**

Fonte: <http://www.cert.br/stats/incidentes/2007-jan-dec/ataques-mensal.html>

De acordo com o mesmo autor o dia da semana, aonde é constatado que a sexta-feira é o dia mais favorável aos incidentes, com aproximadamente 4.000 incidentes.

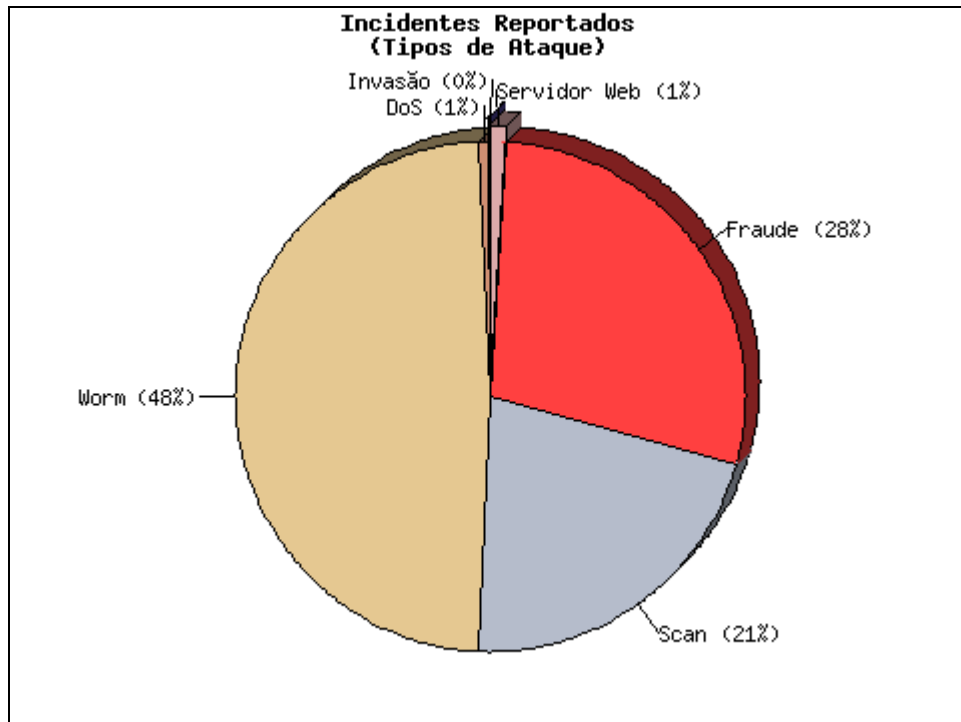
De acordo com o gráfico da figura abaixo, reporta que o dia mais favorável aos ataques é o da segunda-feira com aproximadamente 18 milhões de incidentes.



**Figura 8: Incidentes reportados ao Cert.br (Por dia da semana)**

Fonte: <http://www.cert.br/stats/incidentes/2007-jan-dec/weekdays-incidentes.html>

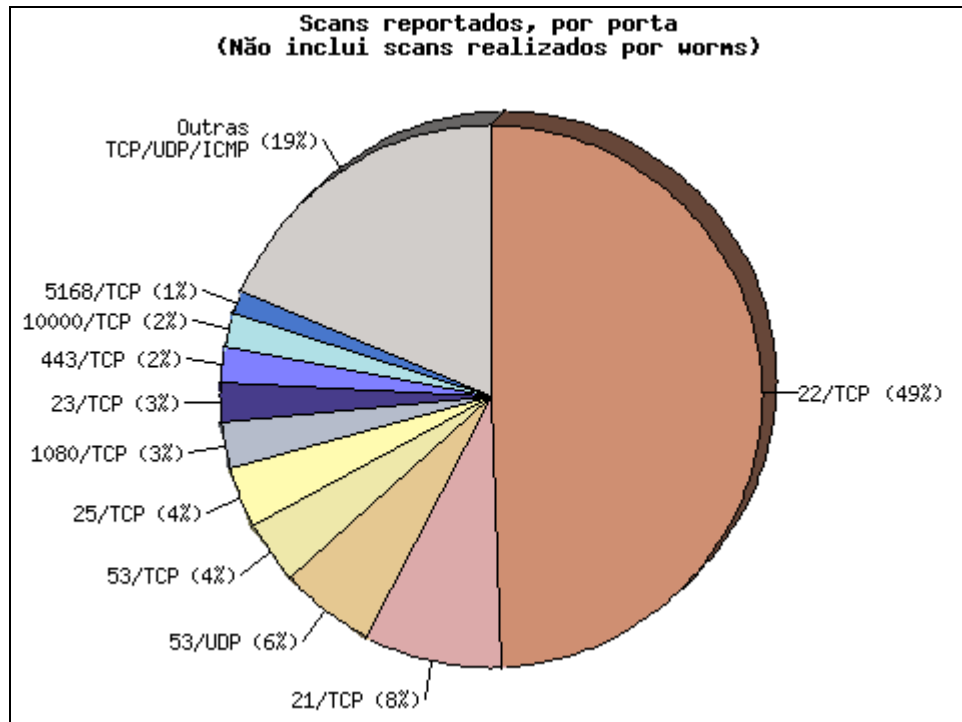
A maioria dos incidentes reportados no ano de 2007, foram de ataques de Worms com 48% aproveitando das brechas de segurança e se prolifera pela rede, seguido das fraudes bancárias com 28%. As empresas investem milhões em sistemas para burlar estes tipos de ataques, os usuários domésticos muitas das vezes não usam sequer um antivírus para se proteger do vírus de computador.



**Figura 9: Incidentes reportados ao Cert.br (Tipos de ataques)**

Fonte: <http://www.cert.br/stats/incidentes/2007-jan-dec/tipos-ataque.html>

Com a proliferação da Web no momento os canais de comunicação de dados em relação ao tráfego estão ficando cada vez mais no gargalo, umas das portas mais atacadas é a porta 80 aonde trafega o maior protocolo da rede no momento, o TCP/IP chegando a 63% de ataques por esta porta.



**Figura 10: Incidentes reportados ao Cert.br (Scans reportados por porta)**

Fonte: <http://www.cert.br/stats/incidentes/2007-jan-dec/scan-portas.html>

### 5.4.1 Engenharia Social

“Segundo o autor Mitnick (2006), o engenheiro social, ou atacante hábil que usa a arte de enganar como uma das armas de seu kit de ferramentas procura explorar as melhores qualidades da natureza humana: a tendência natural de ajudar, dar apoio, ser educado, participante de uma equipe e o desejo de realizar um trabalho.”

De acordo com o autor Santos (2004), a engenharia social se tornou um dos meios mais utilizados para obtenção de informações sigilosas e importantes pela Internet. As empresas têm investido muito dinheiro com novas tecnologias de segurança de informações para proteger fisicamente seus sistemas, mas na maioria não possui métodos que protegem seus funcionários das armadilhas de engenharia social, alvo principal do atacante “falha humana”. O ser humano é induzido a passar informações sobre ele ou da empresa para o atacante. O atacante fraudula a sua identidade, se fazendo passar por outra pessoa, e utilizam meios de comunicações como uma ligação telefônica ou e-mail, para convencer o usuário a fornecer informações ou realizar determinadas ações, como por exemplo, executar um programa, acessar uma página falsa de comércio eletrônico ou Internet Banking através de um

link em um e-mail ou em uma página, etc. Em casos de engenharia social o bom senso é essencial.

A engenharia social é utilizada para o levantamento de informações preliminares que possam tornar a tentativa de invasão mais eficiente, para isso o uso de técnicas esteja ele na forma eletrônica, em papel ou em outras formas. As técnicas mais usadas segundo o mesmo autor.

- *Vírus que se espalham por e-mail*: os criadores de vírus geralmente usam e-mail para o alastramento de seus vírus. Uma vez que o e-mail chegue ao destinatário, normalmente ele vem em forma de arquivo anexado, para tanto é preciso que o usuário execute o arquivo, possibilitando assim o infiltração do vírus no computador da vítima. Geralmente estes arquivos são acoplados em textos ou imagens que chamam a atenção da vítima, comumente estes se tratam de sexo, de amor, de notícias atuais, propagandas de comércio eletrônico, como por exemplo, jogos de cassino.
- *E-mails falsos (Scam)*: é o ataque de engenharia social mais comum usado principalmente para obter informações financeiras da pessoa, como número de conta corrente e senha para roubar o dinheiro presente em suas contas bancárias. Porém, os sistemas dos bancos são muito bem protegidos, dificultando assim a invasão, então o meio mais fácil é tentar enganar as pessoas. Para tanto o atacante adquire uma lista de e-mails usados para SPAM que contém milhões de endereços, depois vai a um site de um banco muito conhecido, copia o layout da página e o salva em um site provisório, que tem a url semelhante ao site do banco. Por exemplo, imagine que o nome do banco seja Banco do Brasil e o site seja [www.bancodobrasil.com.br](http://www.bancodobrasil.com.br). O criminoso cria um site semelhante: [www.bamcodobrasil.com.br](http://www.bamcodobrasil.com.br) ou [www.bancodobrazil.com.br](http://www.bancodobrazil.com.br). Primeiramente ele envia a todos os usuários da sua lista de spam, com o layout semelhante ao do site. Esse e-mail é acompanhado por um link que leva ao site falso. A fim de despertar a atenção do internauta para que ele clique no link, o texto da mensagem pode, por exemplo, sugerir uma atualização de seu cadastro. Como a instituição bancária escolhida geralmente é muito conhecida, as chances de que o internauta que recebeu o e-mail seja cliente do banco são grandes. Assim, ele pode pensar que de fato foi o banco que enviou aquela mensagem, afinal, o e-mail e o site do link tem o layout da instituição. No site clonado é tudo muito idêntico ao site original, então o usuário acessa a sua conta bancaria digitando os seus dados

cadastrais. Como consequência, dias depois percebe que todo o dinheiro da sua conta sumiu, ou seja, o atacante usou da confiabilidade da instituição financeira para poder enganar as pessoas.

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

- *Salas de bate-papo (chat)*: o grande alvo deste meio é as crianças e os adolescentes. Nas salas de bate-papo, os atacantes ganham a confiança durante as conversas. E aos poucos vão convencendo as pessoas a fornecerem os seus dados, como telefone, endereço residencial, endereço escolar, etc. Geralmente os criminosos, convencem as pessoas com conversas de relacionamento íntimo, as pessoas são iludidas e acabam cedendo espaço para estes criminosos.

Ainda temos as informações que acabam por sua vez sendo expostas de forma involuntária pelos administradores de redes e funcionários através do uso indevido da Internet, tais como: sala de bate-papo, MSN, chat, etc. o que motivaria também um contato posterior mais estruturado. O uso do telefônico público para dificultar a detecção e disfarce dos criminosos.

“De acordo com Mitnick (2006), O engenheiro social emprega as mesmas técnicas persuasivas que usamos no dia-a-dia. Assumimos papéis. Tentamos obter credibilidade. Cobramos obrigações recíprocas. Mas o engenheiro social aplica essas técnicas de uma maneira manipuladora, enganosa, altamente antética, frequentemente com efeito devastador.”

Os peritos garantem que à medida que nossa sociedade torna-se cada vez mais dependente da informação, a engenharia social tende a crescer e constituir-se numa das principais ameaças aos sistemas de segurança das grandes organizações.

De acordo com Mitnick (2006), “atenuar os ataques de engenharia social requer uma série de esforços coordenados, tais como:”

- Desenvolver protocolos claros e concisos que sejam cumpridos consistentemente em toda a organização.

- Estabeleça uma política de controle de acesso físico na empresa;
- Organizar um treinamento em consciência da segurança;
- Classifique as informações de sua empresa, onde cada colaborador saiba o que pode ser divulgado e o que não pode, ou seja, as regras de segurança;
- Desconfie das ofertas mirabolantes que circulam pela Internet;
- Treinar funcionários para resistir a ataques de engenharia social
- Ao receber um telefonema de uma pessoa estranha, que conhece todos os seus dados e lhe transmite confiança, retenha desta pessoa o máximo de informações possíveis. Não divulgue nada e peça o número de retorno dela para garantir que a ligação é procedente;
- Estabeleça uma política de segurança na sua empresa onde a informação, que é o seu principal patrimônio, receba o tratamento correto com relação à segurança;
- Evite compartilhar sua senha de acesso, pois ela pode ser divulgada sem que você tenha sido a vítima do ataque de engenharia social;
- Desconfie das mensagens de correio eletrônico onde você não conhece o remetente.

#### **5.4.2 Cavalos de Tróia**

Conforme Mitnick (2006). O cavalo de tróia são softwares criados geralmente em linguagem C e tem a finalidade de abrir uma porta para que hacker's e cracker's possam invadir os sistemas. Estes softwares podem ser criados com essa finalidade ou softwares comuns podem ter seu código adulterado por hacker's ou cracker's com a finalidade de enganar o usuário.

Utilizam as chaves do registro dos sistemas operacionais, para que os execute, na inicialização, com isso os cavalos de tróia sempre serão executados sem que o usuário perceba, mas também são utilizados para ataques a computadores domésticos que destroem ou modificam dados, no momento em que são ativados ou tentam descobrir ou roubar senhas,

números de cartão de crédito e outras informações confidenciais. Eles chegam disfarçados dentro de arquivos ou de programas considerados aparentemente inofensivos, como, por exemplo, em jogos, animações, protetores de telas, etc. também podem representar um problema maior de que outros tipos de vírus, pois são desenvolvidos para serem destrutivos.

Entretanto para que os invasores tenham acesso total ao seu computador, é desenvolvido o trojan do subtipo BackDoor (que abre uma PORTA DOS FUNDOS no micro contaminado, cujo objetivo é o de coletar todas as teclas pressionadas pelo usuário (através de um componente "key-logger", cujo objetivo é transmitir as senhas bancárias e de cartões de crédito digitadas pelo usuário ao navegar por sites de compras, ou em Net-banking. Outra forma de capturar é a posição do cursor e tela nos momentos em que o mouse foi clicado. Outra forma de capturar é a filmagem feita por câmeras digitais ou Webcam: que direciona para o teclado, capturando a filmagem de todas as teclas digitadas. Quando um atacante consegue se infiltrar em um servidor de nomes do provedor, ele redireciona todos os acessos a um site de comércio eletrônico ou Internet Banking para um Website falso, semelhante ao site verdadeiro. Neste caso, monitorar todas as ações do usuário, incluindo, por exemplo, a digitação de sua senha bancária ou do número de seu cartão de crédito.

### **5.4.3 Backdoors**

De acordo com Silva (2000) & Mitnick (2006), um Backdoor mais conhecido como "Porta dos fundos" é um trecho de código fonte mal-intencionado, produzido em qualquer linguagem de programação, comumente utiliza-se linguagem C que cria uma ou mais falhas de segurança para dar acesso ao sistema operacional para pessoas não autorizadas. Esta falha de segurança criada é idêntica a uma porta dos fundos por onde o intruso mal intencionado invade o sistema. Backdoors podem ser inseridos propositalmente pelos criadores do sistema ou podem ser obra de terceiros mal intencionados usando para isso o Cavalo de Tróia, como visto anteriormente. A melhor maneira de evitar os ataques ainda é trazer sistemas atualizados.

Os backdoors podem ser divididos em duas partes, um cliente e um servidor, o software servidor é passado para a vítima, enquanto que à parte cliente é utilizada pelo hacker para se comunicar com o servidor. Quando a parte servidora é executada o cavalo de tróia cria alguns arquivos necessários para a conexão com o cliente e para executar as funções enviadas

pelo mesmo, começando assim a comunicação estação-servidor, o hacker ou cracker tem acesso ao seu sistema.

Silva (2000) diz que, “Programas de Firewall pessoal, no entanto, podem ser úteis para amenizar (mas não eliminar) este tipo de problema.”

#### 5.4.4 Vírus

De acordo com Silva (2000), ao longo do avanço da informática foram criados vírus computacionais que nada mais é que um código fonte malicioso desenvolvido por programadores em linguagem de baixo nível, infectando o sistema operacional, fazendo cópias de si mesmo e se espalhando para outros computadores.

As contaminações geralmente ocorrem quando o usuário executa um anexo de e-mail. Outra forma de contaminação é por Sistema Operacional, ou software desatualizado, sem a aplicação de corretivos (*patches*) que tendem a aniquilar movimentações por portas do computador.

#### 5.4.5 DDoS

De acordo com Mitnick (2006), o DDoS (*Distributed Denial of Service*) constitui um ataque distribuído de negação de serviço. Este tipo de ataque é ampliado pela instalação de várias entidades autônomas remotas em diversos computadores localizadas em várias partes da Internet. O invasor consegue coordenar essas entidades em massa para amplificar o ataque, podendo utilizar milhares de computadores para atacar uma determinada máquina ou rede. Essa técnica é eficaz. Na maioria das vezes estes ataques podem ocupar toda a banda disponível para o acesso a um computador ou rede, causando grande lentidão até que fique indisponível qualquer tipo de comunicação com este computador ou rede, impedindo que usuários legítimos de utilizarem um determinado serviço de um computador comum ocorrer com servidores de hospedagem de sites comerciais.

Os ataques do tipo DoS mais comuns podem ser feitos devido a algumas características do protocolo TCP/IP (Transmission Control Protocol / Internet Protocol),

sendo possível ocorrer em qualquer computador que o utilize. Uma das formas de ataque mais conhecidas é a SYN Flooding, onde um computador tenta estabelecer uma conexão com um servidor através de um sinal do TCP conhecido por SYN (Synchronize). Se o servidor atender ao pedido de conexão, enviará ao computador solicitante um sinal chamado ACK (Acknowledgement). O problema é que em ataques desse tipo, o servidor não consegue responder a todas as solicitações e então passa a recusar novos pedidos.

Um exemplo das mais recentes tentativas de ataques Ddos era com a empresa Google. Sabemos que hoje é um dos canais de comunicação mais utilizado por bilhões de internautas o dia todo, o site oferece muitos serviços que vão desde busca aprimorada de informação, orkut, e-mail. Mas não esta fora da lista de sites a serem invadidos por invasores. Ele se tornou um dos portais de pesquisas de maior conteúdo, possui um mecanismo de detecção de informação mais atualizável. Existem ferramentas de busca muito boas na Internet, como o Altavista, o AlltheWeb, o Yahoo e o MSN. No entanto, nenhum desses sites consegue ter a amplitude do Google. Existem boas razões para isso.

Outra razão para o sucesso do Google é o sistema PageRank. Trata-se de um algoritmo desenvolvido pelos próprios fundadores do Google que atribui uma pontuação (um PageRank) a páginas web, de acordo com a quantidade e a qualidade das ligações (externos ou internos) que apontem para ela; o PageRank é um dos fatores de maior peso na definição do ordenamento das páginas apresentadas pela Google. Em outras palavras, quanto mais ligações existirem apontando para uma página, maior é seu grau de importância no Google. Como consequência, essa página tem maior probabilidade de obter um bom posicionamento nas buscas, pois o PageRank indica que a comunidade da Web (por meio de ligações) elegeu aquela página como de maior relevância o assunto pesquisado. Além disso, o Google analisa os assuntos mais pesquisados e verifica quais sites tratam aquele tema de maneira significativa. Para isso, ele checa a quantidade de vezes que o termo pesquisado aparece na página, por exemplo.

Mas atualmente quando isso começa a acontecer de muitas chamadas para o mesmo IP, vindo do site da Google, a equipe de tecnologia da Google detecta e impede a continuação de solicitação para aquele IP, ou seja, um número grande de pessoas pesquisa a mesma informação e todos clicam na mesma pagina de trazida. O Google automaticamente bloqueia essa pesquisa e verifica os IPs de onde vieram e colocam numa lista negra, por

alguns instantes, voltando a ser liberado depois. Isso visa reter os ataques Ddos aos seus servidores.

#### **5.4.6 SPAMS**

São mensagens de correio eletrônico utilizado para fins comerciais e maliciosos, tendo o envio dessas mensagens realizado em massa, devido a grandes números de endereços de e-mail contidos nas listas de malas diretas. O índice de crescimento do Spam foi crescendo de acordo com o avanço da Internet na vida dos internautas, que passaram a compartilhar com um dos principais problemas da comunicação eletrônica em geral: o envio em massa de mensagens não-solicitadas.

O envio dos Spams é feito via correio eletrônico, os Spammers que são os autores dos Spams usam programas especiais para obtenção de endereços eletrônicos, depois formam uma lista de e-mail e envia os Spams para esta lista. Os Spams chegam à lista de endereço dos internautas como sendo uma mensagem de alerta sobre algum fato da atualidade ou pessoal. Embora existam mensagens comerciais legítimas, enviadas por empresas licenciadas e conhecidas, nota-se que não é raro que o produto ou serviço oferecido pela mensagem tenha alguma característica ilegal e o Spammer e a empresa seja desconhecida ou completamente anônima.

Contudo ainda não existe uma legislação definitiva que regule a prática do Spam ou a caracterize como sendo crime. Apesar desta atual indefinição legal, diversas entidades governamentais, comerciais e independentes declaram que o Spam é caracterizado como um dos maiores problemas atuais da comunicação eletrônica.

No Brasil não é crime enviar Spam, mas esta prática acaba sendo auto regulamentada, pois o Spammer é mal visto, seu produto ou empresa é desacreditado, seu provedor, domínio ou IP pode ser incluído nas listas de bloqueio dos administradores de rede.

De acordo com o órgão CERT.br, (2007) o número de Spams diminuíram em relação que na pesquisa realizada me 2003 o índice de incidente de Spams eram de 4.072.334 casos, hoje a pesquisa constatou um número de 1.229.370 casos, aproximadamente 77% por

cento de redução de incidente devido aos programas anti-Spams, instalados nos computadores dos internautas, além dos provedores de e-mail, que já detectam os envios de e-mails em massas e denominam como Spam, bloqueando o envio de todos os Spams vindo daquela fonte, e as vezes da própria conscientização dos internautas em não abrir estes e-mails.

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

De acordo com o CGI.br (2007), as listas negras (blacklists) possuem endereços IP de máquinas que, segundo o critério do mantenedor da lista, estão envolvidos em envio de spam. Estas listas são implementadas através de zonas de DNS. Dado um endereço IP a ser bloqueado, na lista este IP será incluído com o nome de domínio. Se ao consultar uma lista negra pelo nome e for obtida uma resposta, significa que o IP faz parte da lista negra. A resposta obtida costuma indicar a razão pela qual o IP foi incluído na lista de bloqueio, e varia de lista para lista.

#### **5.4.7 Worms**

Um Worm, tal como um vírus, normalmente espalha-se sem interação por parte do utilizador aproveitando-se de brechas ou vulnerabilidades nos sistemas, para se instalarem e replicarem suas cópias completas (possivelmente modificadas) em grandes volumes de si próprias através de computadores conectados em rede local ou pela Internet, o e-mail se torna o principal canal de distribuição atualmente.

Ele toma o controle de funções do computador que permitem transportar informações. Uma vez infectado o Worm, movimenta-se sozinho, e consome memória, fazendo com que um computador possa a vir ficar bloqueado. Por exemplo, ele procura pela sua lista de endereços de e-mail e se reenvia a todos, e ao mesmo tempo quando sua lista recebe este arquivo, ele faz os mesmos procedimentos enviando para cada lista de endereços

eletrônicos encontrado, resultando em congestionamentos nas redes das empresas e em toda a Internet.

## CONCLUSÃO

O comércio eletrônico ainda é pequeno se comparado com o comércio físico. A Internet demonstrou ao longo dos anos ser um poderoso instrumento de venda e propaganda, facilitando a atuação das empresas na exploração do mercado. A Internet permitiu ao comércio tradicional: acessibilidade a sua clientela. A acessibilidade era dependente de localização, hoje depende cada vez mais do aumento da velocidade de comunicação para poder haver a troca de informação entre fornecedor e consumidor.

A Internet supre as deficiências da mídia tradicional, reduzindo tempo de venda e facilitando acesso a informações adicionais. Com o seu intermédio as vendas cresceram, disponibilizando de varias ferramentas já prontas para efetuar as vendas e as compras de mercadorias, sendo a mais utilizada a World Wide Web, ao permitir o tratamento de dados da rede mundial como hipertexto.

Sobre a segurança, têm surgido vários sistemas de pagamentos para utilização em transações eletrônicas e também, surgiram vários mecanismos de segurança. O uso de barreiras físicas e de criptografia na transmissão de dados via rede bloqueiam os acessos indevidos a informações confidenciais. Tecnologia de segurança criptográfica como o SSL (Secure Socket Layer), pode evitar que estranhos manipulem transações on-line; mas não conseguem resolver o problema da autenticação do usuário. A questão da segurança é uma das principais preocupações no desenvolvimento dos sistemas de pagamento virtual, que precisam assegurá-la sem comprometer a privacidade. O comércio eletrônico, crescente, exige outros meios de pagamentos dotados de qualidades como forma digital, aceitação e segurança, no momento, há muitas formas de pagamento digitais mas a mais utilizada é o cartão de crédito porque as pessoas sentem-se melhor ao comprar na Web utilizando os seus cartões de crédito, ambiente é mais seguro de os usar do que noutros locais, como em restaurantes e lojas, pois os mecanismos de segurança tais como: criptografia, assinatura e certificados digitais; garantem um nível de segurança aceitável para o uso da moeda virtual.

Ao efetuar uma compra ou transação bancária, certifique-se de que a empresa no qual onde esta comprando seja de confiança, como por exemplo [americanas.com.br](http://americanas.com.br), [pernambucanas.com.br](http://pernambucanas.com.br), <http://www.bancodobrasil.com.br>, entre outras, se a empresa oferece política de privacidade, se é garantido o prazo de entrega, troca de mercadoria, que na verdade é direito do consumidor. Normalmente, para se efetuar estes tipos de transações é necessária a

utilização de um cadastro. Neste cadastro, a empresa pode disponibilizar diversos tipos de serviço como, por exemplo, acompanhamento do pedido desde a compra até a entrega. Confira se o site possui protocolos de segurança tais como HTTPS. Para isso, basta verificar na barra de endereços se contem no início do endereço do site o protocolo HTTPS:// e também o cadeado que indica site seguro. Quando o usuário acessa este tipo de página, o navegador pode informar que o site é seguro, porém, normalmente, isto ocorre na parte final da compra quando estiver prestes a informar qualquer dado confidencial, tais como usuário, senha ou número do cartão de crédito.

Vale à pena ressaltar que devemos sempre verificar se o endereço eletrônico está digitado de forma correta, pois os invasores duplicam páginas fazendo páginas idênticas, mas quando informado os dados, estes são passados para outra fonte e não para o local correto, iniciando os roubos eletrônicos. Por exemplo, certifique-se de que acessou <http://www.pernambucanas.com.br> e não <http://www.pernanbucanas.com.br>, uma simples letra faz a diferença. O acesso a determinadas páginas deve ser feito de um lugar seguro, ou que pelo menos tenha certeza da natureza da máquina, evitando lanhouse, cybercafe, entre outros.

## REFERÊNCIAS BIBLIOGRÁFICAS

ABDALA, Ricardo Almeida, **Avaliação dos fatores que influenciam a decisão de utilização dos serviços bancários através de Internet na cidade de Belo Horizonte**. Florianópolis, 2004. 121f.. Dissertação (Mestrado em Engenharia da Produção. Área: Gestão de Negócios - Marketing) - Programa de Pós Graduação em Engenharia de Produção, Universidade Federal de Santa Catarina.

ALBERTIN, Alberto Luiz. **O comércio Eletrônico evolui consolida-se no mercado brasileiro**. RAE - Revista de Administração de Empresas. EAESP / FGV, São Paulo, Brasil, v. 40, n. 4, p.1-9, out./dez. 2000.

\_\_\_\_\_. **Comércio eletrônico: modelo, sua aplicação**. São Paulo: Atlas, 1999. 220 p.

\_\_\_\_\_. **Comércio Eletrônico: Aspectos e Benefícios**. São Paulo, Brasil: EAESP/FGV/NPP – Núcleo de pesquisas e publicações: Relatório de pesquisa nº. 23/1999. 43p.

ALLEMAND, Marcos; VIEIRA, Fernando José Travassos. **Comércio Eletrônico e Segurança na Intranet**. Disponível em: <<http://www.serpro.gov.br/publicacao/tematec/1997/ttec35>>. Acessado em: 19 de fevereiro de 2007.

ALVES, Maria Bernadete Martins; ARRUDA, Susana Margareth . **Como fazer referências bibliográficas**. Atualizada em setembro de 2003, conforme NBR 6023/2002. Universidade Federal de Santa Catarina - Biblioteca Universitária. Disponível em <<http://www.bu.ufsc.br>>. Acessado em: 10 de abril de 2007.

BARROS, Marco Antonio. **Uso de SSL em Sites**. Maringá, 2005. 31f. Monografia (Especialização Desenvolvimento de Sistemas para Web) – Pós Graduação, Universidade Estadual de Maringá

BAPTISTELLA, Márcia Maria Tereza & BARRELLA, Wagner Daumichen. **Comércio Eletrônico: Motivos para utilização e Tendências Futuras**. 2000. 8 F. UFSC - Universidade Federal de Santa Catarina.

BUENO, Rosângela Ignácio, **Uma avaliação do uso do Comércio Eletrônico em empresas do setor de confecções na região Noroeste do Paraná**, 2000. 78f.. Monografia (Especialização em “Desenvolvimento de Sistemas para Web”) – Programa de Pós Graduação em Informática, Universidade Estadual de Maringá, Departamento de Informática.

Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. **Cartilha de Segurança para Internet** - Comitê Gestor da Internet no Brasil. São Paulo, 2006. Versão 3.1, 117f.. Disponível em: <<http://cartilha.cert.br/livro>>. Acessado em: 10 de fevereiro de 2007.

\_\_\_\_\_. **Estatísticas dos Acidentes reportados ao cert.br** - Gestor da Internet no Brasil. São Paulo, 2007. Disponível em: <<http://www.cert.br/stats/incidentes/>>. Acessado em: 10 de novembro de 2007.

\_\_\_\_\_. Cartilha de segurança para Internet. **Conceitos de Segurança**. Gestor da Internet no Brasil. São Paulo, 2007. Disponível em: <<http://cartilha.cert.br/conceitos/sec9.html>>. Acessado em: 27 de julho de 2007.

ECOMMERCEORG. **Dicionário de Ecommerce**. Disponível em: <<http://www.e-commerce.org.br/dicionario.htm>>. Acessado em: 12 de setembro de 2007.

\_\_\_\_\_. **Dados Estatísticos sobre a Internet e Comércio Eletrônico**. Disponível em: <<http://www.e-commerce.org.br/stats.html>>. Acessado: em 26 de outubro de 2007.

FEBRABAN - **Federação Brasileira de Bancos**. Disponível em: <[http://www.febraban.org.br/seguranca\\_site/seg\\_investimento\\_seguranca\\_2007.asp](http://www.febraban.org.br/seguranca_site/seg_investimento_seguranca_2007.asp)>. Acessado em: 10 de agosto de 2007

FREITAS, Francisco. **Segurança na Informática**. Disponível em: <[http://www.sebraesp.com.br/principal/abrindo%20seu%20neg%C3%B3cio/produtos%20sebrae/artigos/listadeartigos/seguranca\\_eletronica.aspx](http://www.sebraesp.com.br/principal/abrindo%20seu%20neg%C3%B3cio/produtos%20sebrae/artigos/listadeartigos/seguranca_eletronica.aspx)>. Acessado em: 10 de fevereiro de 2007.

FERRETTO Luiz Filipe Fagundes; FREIRE, Rute Helena Maia; ALMEIDA, Andréa Vilas Boas; OLIVEIRA Ednaldo Francisco. **Implementações Básicas de Segurança Para Ambientes com Processamentos Críticos**. Brasília/DF – 2002. 118f. Monografia (Especialista em Rede de Computadores) – Programa de Pós-Graduação e Extensão (COPEX), da União Educacional de Brasília (UNEB)

ICP BRASIL: Infra-estrutura de Chaves Públicas Brasileira. Disponível em: <<http://www.icpbrasil.gov.br>>. Acessado em: 10 de outubro de 2007.

GONÇALVES, Alberto, BARROS, António Carlos, RIBEIRO, David, COSTA, Luis. *Comércio Eletrónico*. Universidade do Minho, 1999.

KALAKOTA, R. & ROBINSON, M. **E-business: Estratégias para alcançar o sucesso**

**no mundo digital**. 2. ed. Porto Alegre: Bookman, 2002.

MITNICK, Kevin D. & SIMON, Willian L. *A Arte de Invadir – as verdadeiras histórias por trás das ações de hackers, intrusos e criminosos eletrônicos*. São Paulo 2006, editora Pearson Prentice Hall.

SANTOS, Luciano Alves Lunguinho. **O Impacto da Engenharia Social na Segurança da Informação**. Aracaju, 2004. 83f. Monografia (em redes de computadores) - Pós-Graduação, Universidade Tiradentes. Pg 16

SILVA, Antonio Alvino Filho. **Comércio Eletrônico: Marketing, Segurança, aspectos legais e logísticas**. Mossoró, 2000. 225f.. Dissertação (Mestrado em Engenharia da Produção) - Programa de Pós-graduação do Departamento de Engenharia da Produção, Universidade Federal de Santa Catarina.

RICARTE, Ivan & MAGALHÃES, Leo Pini. **Segurança: tendências**. Unicamp, 1999.  
Disponível em: <<http://www.dcc.unicamp.br/~972314/ARTIGO2.html>>. Acessado em: 24 de outubro e 2007

TVC Oeste Paulista Ltda. **Manual de Segurança na Internet**. Disponível em: <<http://www.tvcmarilia.com.br/index.php?pag=seguranca>>. Acessado em: 23 de fevereiro de 2007.

THOMSON, Laura; WELLING, Luke. **PHP e MySQL Desenvolvimento Web**. Tradução da 2ª ed. Rio de Janeiro: Elseiver, 2003. (ver numero de paginas)

TURBAN, E. ET ALLI. **Electronic commerce a managerial perspective**. New Jersey: Prentice-Hall Inc., 2000.