Universidade Presidente Antônio Carlos - UNIPAC

Riscos e métodos de segurança na Internet

Por:

Francisco de Almeida Magalhães Neto

BARBACENA – MG.
DEZEMBRO DE 2005.

UNIVERSIDADE PRESIDENTE ANTÔNIO CARLOS - UNIPAC

RISCOS E MÉTODOS DE SEGURANÇA NA INTERNET

POR:

FRANCISCO DE ALMEIDA MAGALHÃES NETO

Monografia apresentada à Universidade Presidente Antônio Carlos – UNIPAC, como requisito para conclusão do Curso de Ciência da Computação.

ORIENTADOR: Prof. Gustavo Campos Menezes

BARBACENA – MG.
DEZEMBRO DE 2005.

Francisco de Almeida Magalhães Neto

Riscos e Métodos de Segurança na Internet

Monografia apresentada à Universidade Presidente Antônio Carlos – UNIPAC, como requisito para conclusão do Curso de Ciência da Computação

Aprovada em _____/_____/_____

BANCA EXAMINADORA

Prof .Gustavo Campos Menezes
Orientador do Trabalho

Prof. Frederico de Miranda Coelho
Membro da Banca Examinadora

Prof. Reinaldo S. Fortes
Membro da Banca Examinadora

AGRADECIMENTOS

Agradeço a Deus, pois acalmou meu coração nessa caminhada, nas alegrias, medos, dúvidas e angústias. À minha família e amigos por ter me dado força, principalmente nos momentos que mais necessitei.

Dedico este trabalho aos meus pais,
pelo incentivo e apoio nos momentos
importantes de minha vida.

SUMÁRIO

I – INTRODUÇÃO

O homem, um ser comunicativo por excelência, cedo demonstrou possuir uma capacidade ilimitada de se relacionar com os outros recorrendo a um conjunto de signos culturais propositadamente concebidos para o efeito.

Primeiro, com o próprio corpo,depois, com a escrita, depressa desenvolveu meios cada vez mais eficazes que lhe permitiram ultrapassar não só as barreiras físicas como atingir um número cada vez maior de destinatários. O ato de comunicar e o de construir dispositivos com essa intenção são, de fato, características antropológicas verificáveis em todos os povos ao longo dos tempos.

Nesse sentido, as sociedades humanas têm sido sempre "sociedades de comunicação". As diferenças são marcadas essencialmente pelo grau de complexidade das técnicas de comunicação.

Dificilmente poderíamos hoje imaginar a nossa vida sem o telefone, a rádio, a televisão ou o computador. Uma coisa parece clara, vivemos na Era da Informação, a substituição do átomo pelo bit, do físico pelo virtual, a um ritmo exponencial, vai converter o *homo sapiens* em *homo digitalis*. Não que esta designação (Era da Informação e/ou Sociedade da Informação) seja livre de polemica. Os teóricos da comunicação social consideram que a sociedade de

informação é um grande contra-senso. Isto, porque a sociedade não conta com a participação de todos, mas também porque a comunicação é mediada pelas

técnicas, nomeadamente pela internet, tornando-se a diferença entre o sonho de uma sociedade em que todos se falam e uma realidade em que as trocas são controladas por sistemas de técnicas interativas. Ninguém, contudo, parece duvidar de que vivemos numa sociedade cuja construção foi influenciada pelo desenvolvimento das telecomunicações e da informática. Desenvolvimento que permite a coexistência de diferentes contextos de trabalho e de vida. (RAMOS,2000)

Por fim, quando ligado a outros computadores numa rede mundial (ou num sistema de redes), como a Internet, que permite aos milhões de usuários a oportunidade de procurar informação, participar em grupos de debate, transferir arquivos, trocar correio eletrônico. (GATES,1995)

A rede é hoje um dos fenômenos de comunicação de maior popularidade, um meio universal de procura de informação a baixo custo.

A questão do quanto são valiosos os dados de uma determinada companhia sempre estará sendo discutida, mas dificilmente alguém consegue respondê-la. Poucas companhias, caso houver alguma, conhecem o valor de seus dados, embora muitas delas estejam, agora, percebendo que seus dados estão se transformando em seu patrimônio mais importante e que sua sobrevivência depende deles.(GATES,1995). Por exemplo, é impossível determinar o real valor dos dados que estão sendo gerados como resultado do projeto de pesquisa sobre o genoma humano, uma vez que seu impacto está apenas começando a fazer efeito e que este não se manifestará totalmente ainda

por muitos anos. Além disso, a quantidade de informações reunidas a respeito de terroristas, em apenas alguns dias, depois do dia 11 de setembro, foi surpreendente; e não teria sido possível sem o papel fundamental que foi representado pelos sistemas de computação. De agora em diante, a TI representará um papel crucial na busca mundial pela segurança. Portanto, precisamos dar maior ênfase à segurança, à recuperação a partir de desastres e à disponibilidade.

Objetivo:

Reconhecer riscos que se podem encontrar ao entrar em um site. Os usuários serão capazes de entender os problemas de invasão na internet, as formas de ataque e os principais processos de defesa para ampliar a segurança.

Objetivo Geral:

- Mostrar os riscos na internet
- Métodos de segurança

Objetivos Específicos:

- Identificar problemas de invasão
- Formas de ataque
- Técnicas de defesa

Este trabalho está dividido na seguinte forma: o capítulo I apresenta a Introdução, o II o Surgimento da Internet no Brasil, o III Conceitos Básicos de Segurança para Internet , o IV Comércio Eletrônico e a Certificação Digital e o V Considerações Finais

II – A Internet no Brasil e o surgimento de um mercado comercial

A Internet nasceu praticamente sem querer. Foi desenvolvida nos tempos remotos da Guerra Fria com o nome de ArphaNet para manter a comunicação das bases militares dos Estados Unidos, mesmo que o Pentágono fosse riscado do mapa por um ataque nuclear.

Quando a ameaça da Guerra Fria passou, ArphaNet tornou-se tão inútil que os militares já não a consideravam tão importante para mantê-la sob a sua guarda. Foi assim permitido o acesso aos cientistas que, mais tarde, cederam a rede para as universidades as quais, sucessivamente, passaram-na para as universidades de outros países, permitindo que pesquisadores domésticos a acessarem, até que mais de 5 milhões de pessoas já estavam conectadas com a rede. Atualmente, não é mais um luxo ou simples questão de opção uma pessoa utilizar e dominar o manuseio e serviços disponíveis na Internet, pois é considerado o maior sistema de comunicação desenvolvido pelo homem.

Com o surgimento da World Wide Web, esse meio foi enriquecido. O conteúdo da rede ficou mais atraente com a possibilidade de incorporar imagens e sons. Um novo sistema de localização de arquivos criou um ambiente em que cada informação tem um endereço único e pode ser encontrada por qualquer

usuário da rede.

Em síntese, a Internet é um conjunto de redes de computadores interligadas que tem em comum um conjunto de protocolos e serviços, de uma forma que os usuários conectados possam usufruir de serviços de informação e comunicação de alcance mundial.

A história da Internet no Brasil começou em 1991 com a RNP (Rede Nacional de Pesquisa), uma operação acadêmica subordinada ao MCT (Ministério de Ciência e Tecnologia). Até hoje a RNP é o "backbone" principal e envolve instituições e centros de pesquisa (FAPESP, FAPEPJ, FAPEMIG), universidades e laboratórios.

Em 1994, no dia 20 de dezembro é que a EMBRATEL lança o serviço experimental a fim de conhecer melhor a Internet.

Somente em 1995 é que foi possível, pela iniciativa do Ministério das Telecomunicações e Ministério da Ciência e Tecnologia, a abertura ao setor privado da Internet para exploração comercial da população brasileira.

A RNP fica responsável pela infra-estrutura básica de interconexão e informação em nível nacional, tendo controle do backbone (Coluna dorsal de uma rede, backbone representa a via principal de informações transferidas por uma rede, neste caso, a Internet).

2.1 O SURGIMENTO DE UM MERCADO COMERCIAL

Em meados dos anos 80, havia interesse suficiente em relação ao uso da Internet no setor de pesquisas, educacional e das comunidades de defesa, que justificava o estabelecimento de negócios para a fabricação de equipamentos

especificamente para a implementação da Internet. Empresas tais como a Cisco Systems, a Proteon e, posteriormente, a Wellfleet (atualmente Bay Networks) e a 3Com, começaram a se interessar pela fabricação e venda de *roteadores,* o equivalente comercial dos *Gateway* criados pela BNN nos primórdios da ARPANET.

Outro fator primordial que existe por trás do recente crescimento da Internet é a disponibilidade de novos serviços de diretório, indexação e pesquisa que ajudam os usuários a descobrir as informações de que precisam na imensa Internet. A maioria desses serviços surgiu em função dos esforços de pesquisa das universidades e evoluíram para serviços comerciais, entre os quais se incluem o WAIS (Wide Area Information Service), o Archie (criado no Canadá), o YAHOO, de Stanford, o The McKinley Group e o INFOSEEK, que são empresas privadas localizadas no Vale do Silício.

2.2 - O Comércio Eletrônico

Este é um tema moderno e ao mesmo tempo tradicional envolvendo televendas e tele-atendimento. A principal questão está centralizada na nova filosofia de percepção de compra eletrônica, na definição de um internauta e sua percepção de realização da compra através de um novo canal de comunicação, a Internet.

Para compreender a filosofia do comércio eletrônico é necessário entender o mecanismo de televendas e tele-atendimento como sendo a primeira tentativa de venda "virtual" que surgiu no início da década de 80 e procura incorporar os seguintes conceitos:

1. *Desmaterialização:* substituição do movimento e contato físico por informação telefônica ou via catálogos e um contato virtual.

2. *Desintermediação:* eliminação de um ou mais intermediários na cadeia de venda do produto.

3. *Grupo de afinidades:* são produtos e serviços que possuem similaridades (em termo de divulgação e consumo) e que oferecem ao consumidor soluções apenas visuais, cujas características são inquestionáveis em termo de qualidade, preços e garantias.

Algumas empresas implementam o conceito e a infra-estrutura necessária para operar um centro de atendimento ao cliente, os chamados call-centers. Surgiram os sistemas de informação, os banco de dados, sistemas de telefonia com unidade de respostas audíveis, profissionais de tele-atendimento e a interação entre comandos, dados e voz, que representa o ponto máximo de evolução do atendimento virtual. [1]

Os recursos de telefonia integrados com sistemas de banco de dados aliados a uma filosofia de televendas proporcionam o início do comércio eletrônico que "acoplou" os recursos de Internet, home page, browser, servidor Web e provedor de acesso.(COMITÊ GESTOR DA INTERNET NO BRASIL.2005)

Este "mundo" virtual, com filosofias de consumo próprias ainda não claramente estabelecidas e compreendidas, envolve basicamente a facilidade de manipulação de um browser inter-relacionando às necessidades do cliente e a oferta de produtos e serviços até a efetivação da compra segundo:

[1] E-BRASIL.Câmara Brasileira de Comércio Eletronico. Disponivel em: <<http://www.ebrasil.org.br/contexto/index.shtml>> acesso em 26/04/2005

- Learn: Como os clientes aprendem e adquirem informações gerais e institucionais sobre a empresa, que são necessariamente informações correntes e consistentes, com foco e direcionamento nas necessidades dos usuários do browser.

- Shop: Como os clientes consultam e escolhem as ofertas de produtos e serviços, ou seja, informações baseadas nas preferências do consumidor e na seqüência de ações no browser, auxiliando o consumidor a tomar decisões.

- Buy: Como os clientes efetivam as transações de compras, ou da facilidade do consumidor de preencher um pedido de compra onde não existe a necessidade de um contato do tipo face a face. Essas transações são suportadas por múltiplas formas de pagamento, devendo ser ágil e livre de erros no processamento do pedido de compras.

- Support: Como os clientes poderão ter um suporte técnico e um serviço de atendimento no pós-vendas, considerando-se o atendimento 24 horas por 7 dias de vital importância, e também, toda a comunicação interativa (do tipo pergunta/resposta escrita), além de contar com uma organização de processos e profissionais que identificam um problema e encaminhamento da solução com agilidade.

III– Conceitos básico de Segurança para Internet

Três conceitos básicos importantes na Internet sobre segurança relativos a informações são:

- Confidenciabilidade
- Integridade
- Disponibilidade

Outros conceitos importantes para pessoas que usam essas informações são:

- Autenticação
- Autorização
- Não-repudiação

Quando a informação é lida e copiada por alguém não autorizado para fazê-lo, o resultado é entendido como perda de confidenciabilidade. Para vários tipos de informação confidenciabilidade é essencial. Exemplos disso são dados de pesquisa, médicas, novas especificações de um produto, estratégias de investimentos corporativos. Em alguns lugares há a obrigação de se respeitar e

proteger a privacidade dos indivíduos. Isso é particularmente verdade para bancos, financiadoras, corretoras; negócios que lidam com crédito ao consumidor ou cartões de créditos; hospitais, consultórios médicos, laboratórios médicos; pessoas e empresas que oferecem serviços psicológicos ou tratamentos médico e agências de coleta de impostos.

As informações podem ser corrompidas quando estão disponíveis numa rede insegura. Quando elas são modificadas por meios não esperados, o resultado é conhecido como perda de integridade. Isso levará a um acesso não autorizado a troca de informações, seja por erros humanos ou interferência intencional. Integridade é particularmente importante para segurança crítica ou para dados financeiros usados para atividades como fundos eletrônicos de investimentos, controle de tráfego aéreo e contas financeiras, além disso, podem ser apagadas ou postas inacessíveis, resultando no que podemos chamar na perda de disponibilidade. Isso quer dizer que pessoas que são autorizadas para manipular com certas informações não poderão usá-las.

Disponibilidade é sempre uma característica importante em empresas de prestações de serviço que dependem de informações (ex.: agendas de companhias aéreas, sistemas de investimento online). Disponibilidade da rede é importante para qualquer um que tenha o negócio ou informações dependendo da conexão de rede. Quando um usuário não pode acessar a rede ou algum serviço específico da rede eles passam por algo chamado "negação de serviço"(do inglês, "denial of service").

Para tornar informações disponíveis para quem precisa e quem é confiável, organizações usam autenticação e autorização. Autenticação é provar que um usuário é quem ele diz que é. Isso utiliza-se de algo que o usuário sabe (uma

senha), algo que o usuário tenha (um smartcard), ou algo sobre o usuário que ele prove sua identidade (como a impressão digital). Autorização é o ato de determinar aquilo que um usuário particular (ou sistema de computadores) tem o direito de utilizar: qual atividade ele tem o direito de desenvolver. A segurança é considerada forte quando o significado de autenticação não pode ser contestado a posteriore - o usuário não pode negar posteriormente que ele fez alguma atividade. Isso é entendido como não-repudiação.

É notável perceber a facilidade de se ganhar acesso não autorizado a informações num ambiente de rede inseguro e a dificuldade de detectar os verdadeiros intrusos. Sempre que os usuários não tenham nada gravado em seus computadores que considerem importante, os computadores podem ser chamados de ponto vulnerável, aceitando acesso não autorizado para o sistema da organização e informações subseqüentes.

Informações inócuas claramente podem expor um sistema de computadores. As informação que os intrusos possam considerar úteis incluem quais hardwares e softwares são usados, configurações do sistema, tipo de conexão de rede, números de telefone e acesso a métodos de autenticação. Informações relativas a segurança podem habilitar indivíduos não autorizados a obter acesso a importantes arquivos e programas que comprometam a segurança do sistema. Exemplos importantes disso são senhas, arquivos de controle de acesso, chaves, informações pessoais e algoritmos de encriptação.

Nos últimos tempos, computadores e sistemas inteiros tem sido invadidos e casos são divulgados na mídia. A conseqüência dos ataques e invasões cobrem uma enorme gama de possibilidades: a menor é a perda de tempo recuperando a situação anterior, uma queda de produtividade, uma perda significante de

dinheiro, horas de trabalho, devastação de credibilidade ou oportunidades de marketing, um negócio não habilitado para competir, legalidade real e a perda de uma vida.

3.1- Os Riscos e os Métodos de Segurança na Internet

A Internet tem se tornado o maior meio de difusão de informações e troca generalizada de dados até hoje conhecido. A cada dia que se passa, milhares do novos computadores ou entidades computacionais são adicionados a Internet como parte da mesma. Pouca gente sabe, mas quando você disca para seu provedor de acesso e recebe um endereço Internet (endereço IP), você na verdade está se tornando um nó, ou "node" (em inglês), da Internet.

Como nó da Internet, seja seu computador um provedor de serviços ou apenas mais uma máquina para "navegar na Web", ela está conectada a um grande meio de comunicação que permite à informação transitar em ambas as direções. Assim como você pode transmitir dados, alguém pode recuperar ou acessar dados do seu computador.(STAIR,1996).

Este fato tem assustado os especialistas em segurança, e tem tirado a noite de sono de muitos provedores de acesso e, têm se tornado comum em empresas que estão conectando suas redes à internet. Desta forma, estas empresas estão abrindo na verdade uma porta para que usuários ou pessoas alheias ao meio de sua corporação, acessem informações confidenciais. O protocolo utilizado na Internet não ajuda muito, pois não oferece muita segurança: diversos são os modos que existem para entrar nestas redes corporativas através

da Internet.

A melhor maneira de descobrir se um computador está infectado é através dos programas antivírus. É importante ressaltar que o antivírus deve ser sempre atualizado, caso contrário poderá não detectar os vírus mais recentes.

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

- Instalar e manter atualizado um bom programa antivírus;
- Desabilitar no seu programa de e-mail a auto-execução de arquivos anexados às mensagens;
- Não executar ou abrir arquivos recebidos por e-mail, mesmo que venham de pessoas conhecidas, mas caso seja inevitável, certifique-se que o arquivo foi verificado pelo programa antivírus;
- Não abrir arquivos ou executar programas de procedência duvidosa ou desconhecida e mesmo que você conheça a procedência e queira abrí-los ou executá-los, certifique-se que foram verificados pelo programa antivírus:
- Procurar utilizar, no caso de arquivos de dados, formatos menos suscetíveis à propagação de vírus, tais como RTF, PDF ou PS;
- Procurar não utilizar, no caso de arquivos comprimidos, o formato executável. Utilize o próprio formato compactado, como por exemplo ZIP ou GZ.

O cavalo de tróia, na maioria das vezes, irá instalar programas para possibilitar que um invasor tenha controle total sobre um computador. Estes

programas podem permitir que o invasor possa ver e copiar todos os arquivos armazenados no computador, bem como, descubrir todas as senhas digitadas pelo usuário ou que cause estragos consideráveis como a formatação do disco rígido do computador. Normalmente o cavalo de tróia procura instalar programas, para realizar uma série de atividades maliciosas, sem que o usuário perceba.

A utilização de um bom programa antivírus (desde que seja atualizado freqüentemente) normalmente possibilita a detecção de programas instalados pelos cavalos de tróia. É importante lembrar que nem sempre o antivírus será capaz de detectar ou remover os programas deixados por um cavalo de tróia, principalmente se estes programas forem mais recentes que a sua versão de antivírus. Atualmente, novas funcionalidades têm sido adicionadas aos programas antivírus, de modo que alguns procuram detectar e remover cavalos de tróia, barrar programas hostis e verificar e-mails.

Um bom antivírus deve:

- Identificar e eliminar a maior quantidade possível de vírus;
- Analisar os arquivos que estão sendo obtidos pela Internet;
- Verificar continuamente os discos rígidos (HDs), flexíveis (disquetes) e CDs de forma transparente ao usuário;
- Procurar vírus e cavalos de tróia em arquivos anexados aos e-mails;
- Criar, sempre que possível, um disquete de verificação (disquete de boot) que possa ser utilizado caso o vírus desative o antivírus que está instalado no computador;

- Atualizar a lista de vírus conhecidos, pela rede, de preferência diariamente

. Alguns antivírus permitem verificar e-mails enviados, podendo detectar e barrar a propagação por e-mail de vírus e worms.

Detectar a presença de um worm em um computador não é uma tarefa fácil. Muitas vezes os worms realizam uma série de atividades, incluindo sua propagação, sem que o usuário tenha conhecimento. Embora alguns programas antivírus permitam detectar a presença de worms e até mesmo evitar que eles se propaguem, isto nem sempre é possível.

Portanto, o melhor é evitar que seu computador seja utilizado para propagá-los. Normalmente um worm procura explorar alguma vulnerabilidade disponível em um computador, para que possa se propagar. Portanto, as medidas preventivas mais importantes são aquelas que procuram evitar a existência de vulnerabilidades.

Algumas versões de antivírus são gratuitas para uso pessoal e podem ser obtidas pela Internet. Mas antes de obter um antivírus pela Internet, verifique sua procedência e certifique-se que o fabricante é confiável. Um antivírus não é capaz de evitar o acesso não autorizado a um backdoor instalado em um computador.

Existem sites na Internet que mantém listas atualizadas de vulnerabilidades em softwares e sistemas operacionais. Além disso, fabricantes também costumam manter páginas na Internet com considerações a respeito de possíveis vulnerabilidades em seus softwares. Portanto, a idéia é estar sempre atento aos sites especializados em acompanhar vulnerabilidades, aos sites dos fabricantes,

às revistas especializadas e aos cadernos de informática dos jornais, para verificar a existência de vulnerabilidades no sistema operacional e nos softwares instalados em seu computador. A melhor forma de evitar que o sistema operacional e os softwares instalados em um computador possuam vulnerabilidades é mantê-los sempre atualizados. Entretanto, fabricantes em muitos casos não disponibilizam novas versões de seus softwares quando é descoberta alguma vulnerabilidade, mas sim correções específicas (patches). Estes patches, em alguns casos também chamados de hot fixes ou service packs, têm por finalidade corrigir os problemas de segurança referentes às vulnerabilidades descobertas. Assim, é extremamente importante que você, além de manter o sistema operacional e os softwares sempre atualizados, instale os patches sempre que forem disponibilizados.

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

- Execução de Javascript ou de programas Java hostis;
- Execução de programas ou controles ActiveX hostis;
- Obtenção e execução de programas hostis em sites não confiáveis;
- Realização de transações comerciais ou bancárias via Web, sem qualquer mecanismo de segurança.

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

Normalmente os browsers contém módulos específicos para processar programas Java. Apesar de estes módulos fornecerem mecanismos de

segurança, podem conter falhas de implementação e, neste caso, permitir que um programa Java hostil cause alguma violação de segurança em um computador.

O JavaScript é bem mais utilizado em páginas Web do que os programas Java e, de modo geral, constitui uma versão bem "enxuta" do Java. É importante ressaltar que isto não quer dizer que não existam riscos associados à sua execução. Um Javascript hostil também pode acarretar a violação da segurança de um computador.

Antes de receber um programa ActiveX, o seu browser verifica sua procedência através de um esquema de certificados digitais (vide partes I e IV desta cartilha). Se você optar por aceitar o certificado, o programa é executado em seu computador.

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

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

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

Portanto, é muito importante que você, ao realizar transações via Web, certifique-se da procedência dos sites, se estes sites são realmente das instituições que dizem ser e se eles fornecem mecanismos de segurança para evitar que alguém conectado à Internet possa obter informações sensíveis de

suas transações, no momento em que estiverem sendo realizadas.

Algumas medidas preventivas para o uso de browsers são:

- Manter o seu browser sempre atualizado;
- Desativar a execução de programas Java na configuração de seu browser. Se for absolutamente necessário o Java estar ativado para que as páginas de um site possam ser vistas, basta ativá-lo antes de entrar no site e, então, desativá-lo ao sair;
- Desativar a execução de Javascripts antes de entrar em uma página desconhecida e, então, ativá-la ao sair. Caso você opte por desativar a execução de Javascripts na configuração de seu browser, é provável que muitas páginas Web não possam ser visualizadas;
- Permitir que programas ActiveX sejam executados em seu computador apenas quando vierem de sites conhecidos e confiáveis;
- Manter maior controle sobre o uso de cookies, caso você queira ter maior privacidade ao navegar na Internet;
- Certificar-se da procedência do site e da utilização de conexões seguras ao realizar transações via Web.

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

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

- Acesso não-autorizado: o programa de distribuição de arquivos pode permitir o acesso não autorizado ao computador, caso esteja mal configurado ou possua alguma vulnerabilidade;
- Softwares ou arquivos maliciosos: os softwares ou arquivos distribuídos podem ter finalidades maliciosas. Podem, por exemplo, conter vírus, ser um cavalo de tróia, ou instalar backdoors em um computador;
- Violação de direitos autorais (Copyright): a distribuição não autorizada de arquivos de música, filmes, textos ou programas protegidos pela lei de direitos autorais constitui a violação desta lei.

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

- Manter seu programa de distribuição de arquivos sempre atualizado e bem configurado;
- Ter um bom antivírus instalado em seu computador, mantê-lo atualizado e utilizá-lo para verificar qualquer arquivo obtido, pois eles podem conter vírus ou cavalos de tróia;
- Certificar-se que os arquivos obtidos ou distribuídos são livres, ou seja, não violam as leis de direitos autorais.

Os riscos envolvidos na utilização de recursos compartilhados por terceiros são:

- Abrir arquivos ou executar programas que contenham vírus;
- Executar programas que sejam cavalos de tróia.

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

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

Algumas medidas preventivas para o uso do compartilhamento de recursos do Sistema Operacional são manter um bom antivírus instalado em seu computador, atualizado e utilizá-lo para verificar qualquer arquivo ou programa compartilhado, pois eles podem conter vírus ou cavalos de tróia. Deve-se estabelecer senhas para os compartilhamentos, caso seja estritamente necessário compartilhar recursos do seu computador.

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

As cópias de segurança podem ser simples como o armazenamento de arquivos em CDs, ou mais complexas como o espelhamento de um disco rígido inteiro em um outro disco de um computador. Atualmente, uma unidade

gravadora de CDs e um software que possibilite copiar dados para um CD são suficientes para que a maior parte dos usuários de computadores realize suas cópias de segurança.

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

A freqüência com que é realizadas uma cópia de segurança e a quantidade de dados armazenados neste processo depende da periodicidade com que o usuário cria ou modifica arquivos. Cada usuário deve criar sua própria política para a realização de cópias de segurança.(BRENTON,1992)

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

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

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

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

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

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

- Cópia em outro local: cópias de segurança podem ser guardadas em locais diferentes. Um exemplo seria manter uma cópia em casa e outra no escritório. Também existem empresas especializadas em manter

áreas de armazenamento com cópias de segurança de seus clientes. Nestes casos é muito importante considerar a segurança física de suas cópias, como discutido no item anterior;

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

3.2 - AMEAÇAS MAIS COMUNS

As ameaças mais comuns na Internet se baseiam em um princípio bastante simples: se passar por outra pessoa. Isto pode ser conseguido em diversos níveis: por exemplo, a coisa mais fácil do mundo e mandar um e-mail se passando por outra pessoa. Quando você manda uma correspondência via Internet, não existe certificação nenhuma da autenticidade de quem a envia. Tal fato pode ser amplamente comprovado através de um "TELNET" (utilitário para emulação de terminais e comandos remotos), para a porta do soquete do servidor de correspondência (geralmente 25). TELNET <nome_servidor.nome_ dominio.nome_dominio> 25 (por exemplo, TELNET www.meudominio.com.br 25).

Tal comando irá abrir uma sessão de comunicação via TELNET para o endereço especificado (deve ser o endereço do servidor de mail), para a porta 25 do mesmo (porta do serviço de mail SMTP). O servidor de mail do outro lado, irá simplesmente responder ao seu pedido e aguardar seus comandos. Torna-se fácil

desde que você saiba os comandos necessários para interagir com o servidor de mail SMTP.(STAIR,1996)

Sendo assim, uma falha de segurança que não pode ser consertada a curto prazo (tal falha é resultado da natureza da suíte de protocolos utilizados na Internet), a única maneira de se certificar sobre a autenticidade de uma mensagem é via uma assinatura digital, criptografada, pessoal e intransferível, que o usuário pode adicionar ao mail.

Outro método utilizado é o IP spoofing. Através deste método, pode-se alterar o conteúdo de um pacote da Internet sem alterar o endereço de fonte e de destino. Seria o equivalente a capturar uma carta enviada por você a um amigo seu e colocar dentro qualquer dado que quiser, sem alterar o endereço de remetente e destino.

Como o único método para garantir a segurança de um pacote da Internet é verificar de onde o mesmo veio, então, com tal técnica, eu poderia por exemplo, me fazer passar por uma máquina confiável.

Outra ameaça comum, principalmente para as grandes instituições de acesso a Internet, são os serviços que vêm instalados nos servidores por padrão. Máquinas UNIX possuem diversos Daemons, ou serviços, que ficam rodando no servidor, à espera de alguém para utilizá-los. Existem daemons por exemplo, que habilitam um usuário via Internet, copiar arquivos, deletar arquivos e até executar aplicações no servidor, tudo remotamente.

Outro ponto são os protocolos adicionais que trafegam através do TCP/IP. Um exemplo é o NetBIOS (utilizado em redes Microsoft). O TCP/IP por padrão carrega informações NetBIOS nas portas de 135 a 139. Isto quer dizer que posso, através deste protocolo e destas portas, acessar uma máquina Microsoft (ou uma

máquina UNIX com Samba, produto que torna máquinas UNIX compatíveis com NetBIOS) que esteja conectada a Internet como se estivesse conectada a mesma via uma rede local (LAN), utilizando a Internet apenas como meio de comunicação. (LEAL,2001).

De todas as ameaças que podem ser exploradas para conseguir acesso a uma rede Intranet, através da Internet, talvez a técnica do Packet Sniffing seja a mais insólita.

Serviços da Internet como FTP, Telnet e E-mail, fazem sua senha trafegar pela Internet (ou linha telefônica) sem nenhum tipo de criptografia. Isto quer dizer que, se alguém estiver utilizando um software de análise de pacotes na rede (Packet Sniffing), poderá capturar um pacote seu, para seu provedor de acesso, que seja justamente o pacote de autenticação. Naturalmente, sua senha estará lá, para quem quiser ler. Trocar suas senhas periodicamente é a única solução. Se sua conta é pessoal sem nada a esconder, troque sua senha pelo menos uma vez por mês. A maioria dos provedores Internet possuem um serviço de troca de senhas online, via TELNET.

Além destas ameaças comuns, existe a utilização não autorizada do protocolo de gerência, mais conhecido como SNMP (Simple Network Management Protocol). Através deste protocolo, é possível verificar dados estatísticos de equipamentos que provém a conectividade à rede, como roteadores, hubs, switches e etc., permitindo a visualização do status das portas do equipamento e até desativação de portas bem como a desativação de todo o equipamento. O SNMP trabalha com comunidades de segurança e implementa segurança através de senhas de acesso. Porém, a maioria não configura o serviço, simplesmente o deixa no mesmo estado em que foi fornecido junto com o

equipamento. A grande porção das implementações do SNMP tem por padrão a comunidade PUBLIC, e como senha, coisas como PUBLIC, PASSWORD ou ADMINISTRATOR, isto quando sequer é fornecido com alguma senha. Poderia portanto, via Internet, construir um mapa completo do sistema de conectividade de uma empresa, realizar a monitoração dos equipamentos e desativá-los / reiniciá-los. Para impedir tal ameaça, basta configurar um nome de comunidade diferente do padrão e, obviamente, modificar a senha.

3.3- ENGENHARIA SOCIAL: UM MÉTODO ANÁLOGO EM UM MUNDO DIGITAL

A engenharia social é um método bastante simples de se obter informações. A grande maioria dos mal-intencionados utilizam-se da psicologia, para conseguir informações de cunho restrito. Tal técnica é chamada de engenharia social. Consiste em convencer alguém de dentro de uma empresa de que você é confiável, e que pode receber informações restritas. O caso típico de engenharia social: Ás 18h00min da sexta-feira, o CPD recebe um telefonema. Neste horário, geralmente, está presente somente o operador de plantão ou o pessoal de suporte de emergência. Tais funcionários trabalham em sua grande maioria em turnos noturnos, fora da agitação do dia-a-dia, e fora, por conseqüência das informações mais atualizadas. Um destes funcionários atende ao telefonema de uma pessoa que se diz ser um alto executivo da empresa e que precisa de uma conta temporária para atualizar dados vitais da empresa. O funcionário cria a conta, com direitos de dial-in (acesso remoto). A pessoa desliga com ar satisfeito. Porém, 15 minutos depois, esta mesma pessoa liga, alegando

que não está conseguindo atualizar os arquivos / banco de dados porque não possui direitos para tal. Então, o funcionário despreparado dá acesso equivalente de administração, para não ter mais problemas. A porta então está aberta. Na melhor das situações, o funcionário se negará a realizar tal tarefa, e a pessoa no telefone o ameaçará, alegando que, se não for atendido, o chefe do CPD receberá uma comunicação oficial na segunda às 8 da manhã.

Para evitar tal situação, deve-se ter sempre à mão uma lista de telefones onde tal informação de segurança possa ser certificada. Implementar na empresa uma política de autorização de segurança centralizada, onde somente uma/algumas pessoas de confiança tenham acesso à modificação dos direitos dos usuários. Se tal filosofia for implementada, todos saberão quando e como solicitar serviços como o descrito acima.

3.4 - PROXY E FIREWALLS

Existem diversas tecnologias para impedir acessos não autorizado. Uma das técnicas mais comuns de segurança é a implementação de um Servidor de Proxy, ou de procuração. Tal técnica consiste em conectar uma máquina a Internet que agirá como agente de comunicação. Tal máquina terá tanto uma interface de comunicação com a Internet como outra interface de comunicação com a rede local. Quando um usuário de sua rede local requisita um documento ou um dado na Internet, este o faz ao Servidor de Proxy, que "aparece" para a Internet e realiza a requisição. Uma vez o dado recuperado da Internet, este é repassado para a máquina na rede interna. A segurança reside no fato de que as

máquinas da sua rede interna não estão disponíveis para a Internet, somente uma máquina estará, esta sendo o Servidor de Proxy. Portanto, somente uma máquina estará vulnerável aos ataques dos "hackers". Outra vantagem do Servidor de Proxy é a facilidade em prover o acesso à Internet para uma rede local. Apenas uma conexão com a Internet e necessária, para abastecer toda uma empresa (claro, a velocidade do canal de comunicação deve ser cuidadosamente dimensionada, para impedir que o serviço se torne sobrecarregado). Um bom exemplo de Servidor de Proxy, é o Microsoft Proxy Server, uma solução de Servidor de Proxy para Servidores Windows NT. (STAIR,1996).

Porém, tal técnica impede que os computadores da rede local desempenhem funções mais avançadas, qualquer coisa além de serviços como FTP, WWW, IRC e e-mail. Ou seja, existirão determinadas situações onde um computador na rede interna terá de acessar a Internet como nó, e não através de um servidor de Proxy.

Assim sendo, a utilização do Servidor de Proxy é limitada. Para tais situações, existe outra técnica o Firewall , que são dispositivos constituídos pela combinação de software e hardware, utilizados para dividir e controlar o acesso entre redes de computadores.

O firewall pessoal é um software ou programa utilizado para proteger um computador contra acessos não autorizados vindos da Internet, e constitui um tipo específico de firewall.

O portal de entrada mais comum para explorações de segurança são bugs ou "backdoors" em produtos, que permitem aos hackers entrar no sistema da rede ou mesmo adquirir poderes além dos designados. A maior fonte de informação sobre bugs de segurança e a mais atualizada é a Internet. Se alguém ou algum

programa suspeito tentar se conectar ao seu computador, um firewall bem configurado entra em ação para bloquear tais tentativas, podendo barrar o acesso a backdoors, mesmo se já estiverem instalados em seu computador.

Alguns programas de firewall permitem analisar continuamente o conteúdo das conexões, filtrando cavalos de tróia e vírus de e-mail antes mesmo que os antivírus entrem em ação. Também existem pacotes de firewall que funcionam em conjunto com os antivírus, provendo um maior nível de segurança para os computadores onde são utilizados.

É comum observar relatos de usuários que acreditam ter computadores seguros por utilizarem apenas programas antivírus. O fato é que a segurança de um computador não pode basear-se apenas em um mecanismo de defesa. Um antivírus não é capaz de impedir o acesso a um backdoor instalado em um computador. Já um firewall bem configurado pode bloquear o acesso a ele. Além disso, um firewall poderá bloquear e permitir que o usuário identifique as tentativas de explorar vulnerabilidades em seu computador e as possíveis origens de tais ataques.

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

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

3.5 - SENHAS

Um dos pontos de maior ataque, obviamente, são as senhas. Através de uma senha, qualquer usuário pode ser autenticado em sistemas de segurança. Ao identificar-se como administrador de um servidor e fornecer a senha correta, conseguirá poderes de administração. Sendo assim, existem algumas diretrizes que devem ser observadas para minimizarmos as vulnerabilidades:

1. Trocar a senha sempre que puder (para um usuário comum, 1 vez por mês; para um Administrador, 1 vez / semana);
2. utilizar senhas sem significado (não usar nomes próprios, substantivos e etc.);
3. utilize no mínimo 8 caracteres como senha;
4. utilize senhas randômicas, ou seja, com caracteres alfanuméricos (letras e números);
5. não utilize a conta do Administrador; utilize sua conta pessoal;
6. não dê a senha do administrador ou equivalente para ninguém. Se for o caso, dê direitos ao usuário de administração, mas nunca a senha do administrador. Isto possibilita a realização de auditoria posterior;
7. nunca, em hipótese alguma, passe sua senha de acesso PARA NINGUÉM, mesmo que DEVIDAMENTE autorizado. Se for completamente inevitável, mude-a imediatamente, em seguida;
8. sempre observe se o seu mIRC não está com o servidor de arquivos ligado. Se sim, desative-o imediatamente. Isto possibilita que um usuário recupere do seu sistema o seu arquivo de senhas;
9. Tenha sempre paranóia com senhas. Sempre que suspeitar de algo, mude-a imediatamente.

IV – COMÉRCIO ELETRÔNICO E A CERTIFICAÇÃO DIGITAL - SEGURANÇA POSSÍVEL

> "Na próxima década, os negócios vão mudar mais do que mudaram nos últimos cinqüenta anos."
> (Bill Gates - A Empresa na Velocidade do Pensamento)

A Internet tornou-se uma formidável ferramenta para a realização do comércio, sobretudo porque traz a vitrine dos objetos de consumo para dentro de nossas casas. Produtos e serviços podem ser adquiridos ou contratados rapidamente, de maneira simplificada, sem que o consumidor tenha que se locomover ou sequer ter contato pessoal com alguém. No entanto, o comércio eletrônico traz inúmeras conseqüências e a principal preocupação é com a segurança dos negócios. São intensos os debates sobre a validade dos documentos digitais e os riscos da sua manipulação, o que torna a implementação de tecnologias de segurança o grande desafio na busca da confiabilidade.

Os especialistas em contratos eletrônicos, explicam que o tratamento digital da informação (necessário para a transmissão de dados por computador), traz como conseqüência a desmaterialização do documento, que deixa de ser

representado no suporte clássico de papel, passando a ser registrado em suporte magnético.

O fato de os documentos serem representados por um meio completamente diferente, libertando-se do formato que tiveram durante séculos de desenvolvimento, tem imensa implicação no relacionamento comercial, pois nossa tradição negocial está alicerçada no uso do papel como suporte material das declarações de vontade. Entretanto, atualmente já existem técnicas capazes de conferir segurança e integridade, além de atestar a autenticidade dos documentos produzidos e armazenados em meio digital. Isto é possível graças ao desenvolvimento da criptografia, que funciona pela aplicação de um padrão secreto de substituição dos caracteres, de maneira que a mensagem se torne ininteligível para quem não conheça o padrão criptográfico utilizado. (BRASIL,2005)

A criptografia moderna utiliza conceitos matemáticos avançados e abstratos, que servem como padrão para cifrar ou decifrar mensagens. Este padrão criptográfico é também denominado chave. A utilização da criptografia simétrica, também conhecida como "de chave privada", por exemplo, exige que o destinatário da mensagem conheça o algoritmo utilizado para criptografar a mensagem (deve possuir a chave utilizada pelo remetente), caso contrário, não poderá decifrar o conteúdo.

Já a criptografia assimétrica ou "de chave pública", funciona a partir de complexos métodos matemáticos, onde são gerados dois códigos, duas chaves diferentes. Uma delas fica em poder do proprietário do sistema, que terá exclusividade no seu uso. A outra poderá ser distribuída a todos aqueles com

quem o proprietário precisa manter uma comunicação segura ou identificada.

Qualquer uma delas pode ser utilizada para cifrar uma mensagem, que somente a outra chave será capaz de decifrar e vice-versa. Portanto, a chave usada para cifrar a mensagem não consegue decifrá-la, o que só pode ser realizado pela outra chave.

A partir da tecnologia da criptografia assimétrica foi desenvolvido o mecanismo da assinatura digital, que tem a função de identificar o autor do documento e garantir a sua autenticidade. Esta assinatura é gerada pelos bits contidos no próprio documento assinado, tendo validade apenas para este, assim, qualquer modificação feita nestes bits originários, mesmo que seja a simples inclusão de uma vírgula, invalidará automaticamente a assinatura.

Quando a distribuição da chave pública é feita em larga escala, como ocorre com o comércio eletrônico, para se evitar fraudes instituiu-se a autenticação digital, que significa que a identificação do proprietário das chaves foi verificada previamente por uma entidade certificadora oficial, que credita a validade da mesma. A autenticação é provada por um certificado, formado por um conjunto de dados que vinculam a assinatura e a sua respectiva chave pública a uma determinada pessoa, identificada como proprietária das chaves, com base em registros que devem ser mantidos pela autoridade certificadora em local seguro e a salvo de adulteração.

De acordo com o Projeto de Lei nº 1.589/99, em tramitação no congresso nacional, a autoridade certificadora será exercida pelos tabeliães. Este é o mais completo dos projetos em estudo, pois regula o comércio eletrônico, a validade jurídica do documento eletrônico, a assinatura digital e outras providências e foi elaborado pela comissão de informática da Ordem dos Advogados do Brasil

(OAB) e encampado por todos os partidos políticos. (BRASIL,2005)

No Congresso Nacional existem mais de 40 projetos em tramitação que objetivam estabelecer novos tipos de normas para o comércio eletrônico, como a tipificação de crimes virtuais e a criação de novos tipos de documentos e identificadores. Há, por exemplo, o Projeto de Lei do Senado de nº 672/99, que dispõe sobre o comércio eletrônico inspirado na Lei Modelo da UNCITRAL (Comissão das Nações Unidas para o Direito Comercial Internacional)[2] que, ao contrário do projeto da OAB, não trata da certificação digital, assim como vários outros que se mantiveram neutros em relação a essa tecnologia.

O Projeto 1.589, coloca o Brasil na contramão da tendência mundial de deixar à iniciativa privada a condução do comércio eletrônico em geral, e da atividade de certificação em especial, como instrumento de formação de um mercado aberto e competitivo, criando um sistema caracterizado pelo favorecimento de uns poucos (tabeliães) e insistindo em manter viva essa tradição cartorial, que está mais interessada na manutenção de certos privilégios do que na eficiência dos sistemas públicos de informação.

A Medida Provisória nº 2.200, de 28/06/2001, instituiu a Infra-estrutura de Chaves Públicas Brasileiras (ICP-Brasil)[3], e dá outras providências como a garantia da comunicação com os órgãos públicos por meios eletrônicos e disciplina a questão da integridade, autenticidade e validade dos documentos eletrônicos. Dentre as principais disposições está a figura da Autoridade Certificadora Raiz das Autoridades de Registro e Certificação da cadeia, representada pelo Instituto Nacional de Tecnologia da Informação (órgão do Ministério da Ciência e Tecnologia), bem como o gerenciamento do sistema pelo Comitê Gestor da Internet no Brasil.(BRASIL,2005)

[2] UNCITRAL-United Nations Comissions on International Trade Law. Resoluçaõ nº 51/162. New York ,

[3] USA (UN) Presidência da República. Comitê Gestor de Chaves Públicas

Segundo o entendimento de juristas e estudiosos, a legislação brasileira pode e vem sendo aplicada nos problemas relacionados com a rede, uma vez que as relações virtuais e seus efeitos são realidade. Quando é possível, ocorre uma adequação e adaptação das normas jurídicas a esse novo ambiente. No entanto, o avanço das tecnologias de informação está provocando um grande obsoletismo em muitos institutos jurídicos. Por isso há uma premente necessidade de reformulação do sistema jurídico, onde as questões específicas e controvertidas sejam regulamentadas. O que se condena é a lentidão do andamento desse processo.

O atraso tecnológico no emprego das ferramentas pelo poder público para combater o crime eletrônico é uma questão de vontade política, vontade esta que se estende à promulgação das novas leis que darão combate efetivo ao crime exclusivo eletrônico.

4.1 - A Infra-estrutura de Chaves Públicas Brasileira

A ICP-Brasil - Infra-estrutura de Chaves Públicas Brasileira - é um conjunto de entidades, padrões técnicos e regulamentos, elaborados para suportar um sistema criptográfico com base em certificados digitais.

Foi criada a partir da percepção do Governo Federal da importância de regulamentar as atividades de certificação digital no País, com vistas a inserir

maior segurança nas transações eletrônicas e incentivar a utilização da Internet como meio para realização de negócios.

A ICP-Brasil foi instituída pela Medida Provisória 2.200-2, de 24 de agosto de 2001, que cria o Comitê Gestor da ICP-Brasil, a Autoridade Certificadora Raiz Brasileira e define as demais entidades que compõem a estrutura. A partir dessa medida foram elaborados os regulamentos que passaram a reger as atividades das entidades integrantes da ICP-Brasil, chamados de Resoluções do Comitê Gestor da ICP-Brasil (até o momento foram aprovadas 37 resoluções, que podem ser obtidas no site www.iti.gov.br).

Desde as primeiras Resoluções ficou clara a importância da Auditoria para a ICP-Brasil, como forma de assegurar a aplicação dos normativos por parte de todos os envolvidos. As entidades participantes da ICP-Brasil são auditadas previamente ao credenciamento, para verificar se estão aptas a desenvolver suas atividades conforme os regulamentos, e também anualmente, para verificar se todos os procedimentos previstos foram executados.

A própria AC Raiz foi auditada por uma comissão composta de membros de diversos órgãos do Governo federal, para ter seu funcionamento autorizado pelo Comitê Gestor (ver Resolução 3, de 25 de setembro de 2001, que nomeia a comissão de auditoria e Resolução 5, de 22 de novembro 2001, que publica o relatório da auditoria realizada na AC Raiz).

A quantidade de entidades credenciadas na ICP-Brasil vem aumentando de forma cada vez mais acelerada, dada a percepção, pelos diversos setores, das inúmeras possibilidades de uso dos certificados digitais.

Alguns exemplos de uso são:

- Sistema de Pagamentos Brasileiro – SPB – gerencia o processo de compensação e liquidação de pagamentos por meio eletrônico, ligando as Instituições Financeiras credenciadas ao Banco Central do Brasil. Utiliza certificados digitais da ICP-Brasil para autenticar e verificar a identidade dos participantes em todas as operações realizadas;

- Tramitação e assinatura eletrônica de documentos oficiais, por Ministros e pelo Presidente da República, para publicar no DOU;

- Registro de operações e prestações do ICMS pela Internet, em Pernambuco e outros estados;

- Consulta da situação dos contribuintes na base da Receita Federal e demais serviços providos pelo Receita 222;

- Programa de ampliação do uso de certificados digitais para correntistas (convênio entre ITI, Febraban e Receita Federal);

- Substituição dos certificados do programa Conectividade Social, da Caixa Econômica Federal, por certificados da ICP-Brasil.

VI – CONSIDERAÇÕES FINAIS

A internet é considerado o maior sistema de comunicação desenvolvido pelo homem. A história da internet no Brasil começou em 1991,mas somente em 1995 que a população brasileira teve abertura ao setor privado da internet para exploração comercial. A mesma tornou-se uma ferramenta para realização do comércio, onde produtos e serviços podem ser adquiridos rapidamente, no entanto traz inúmeros riscos, como a falta de segurança. Entretanto já existem técnicas de segurança, graças a criptografia.

A confidenciabilidade, a integridade e a disponibilidade são indispensáveis na internet com relação a informação.

Os ataques e invasões podem acarretar prejuízos de ordem econômica. A melhor maneira para descobrir se o computador está infectado é através do antivírus, que nem sempre é capaz de detectar os mesmos, existindo também o firewall. Talvez a maniera mais insólita para conseguir acessos a uma rede é a técnica do Packet Sniffing.

As notificações associadas a fraudes informadas ao Grupo de Resposta a Incidentes para a Internet Brasileira (NBSO), cresceram 178% no primeiro trimestre de 2005, na comparação com o mesmo período do ano anterior.

Segundo o balanço divulgado pela entidade - que é mantida pelo Comitê Gestor da Internet - os três primeiros meses do ano registraram 2.213

notificações. No último trimestre de 2004 esse número foi de 1.675.

O número de incidentes relacionados a fraudes vem crescendo de maneira notável nos últimos anos. Em 2003, esse gênero de ataque pela internet não passava de 1% das notificações reportadas. Em 2004 passou a 5% e só neste primeiro trimestre de 2005 já alcançou 18%, tendência que deve se manter durante todo o ano. (BRASIL,2005)

As fraudes, entretanto, continuam em terceiro lugar entre os tipos de ataques mais freqüentes no período. Os primeiros colocados neste trimestre foram os scans - varredura nos computadores vulneráveis - com 47% do total.

Os casos de worms - programas capazes de se propagar automaticamente, enviando cópias de si mesmos de computador para computador - caíram para o segundo lugar, representando 32% do total. O porcentual restante corresponde a ataques a usuários finais e a servidores.

Neste período, o órgão constatou que o número total de notificações de ataques no Brasil apresentou queda em relação aos trimestres anteriores. Nos primeiros três meses de 2005 foram reportados 12.438 incidentes, contra 23.138 no período anterior, o que representa uma diminuição de 46%.

Segundo os analistas do NBSO, esta redução se deve a queda do número de notificações de worms.

A maior parte dos incidentes reportados (75%) continua sendo originada de cinco países: Estados Unidos (27,62%), Brasil (26,14%), Coréia do Sul (9,94%), China (7,56%) e Taiwan (3,43%). O volume de spams reportados ao Grupo de Resposta a Incidentes para a Internet Brasileira (NBSO) atingiu a marca de 690.721 mensagens entre os meses de janeiro e março de 2005.

De acordo com a organização, controlada pelo Comitê Gestor da Internet

do Brasil, o volume representa de queda de 35% frente a um milhão de spams registrados nos três primeiros meses de 2004. Na comparação com o último trimestre do ano passado, a queda foi de 9%.

Segundo analistas do NBSO, a diminuição reflete provavelmente a queda no número de notificações de spam enviadas por usuários e administradores de redes, e o aumento na eficácia das técnicas anti-spam adotadas por redes e provedores de acesso.

Pelo levantamento, as reclamações concentram-se nas categorias de Spamvertised Website - máquinas que hospedam páginas com produtos e serviços oferecidos no spam, com 38% do total das notificações - e na área de proxy aberto, que reflete abusos em máquinas com serviço de proxy mal configurado, com 31% de participação. No ano de 2004, o NBSO registrou 4,1 milhões de spams.

Como pôde ser verificado neste estudo, a Internet avança rápido. Alguns adjetivos são dados à esta monumental rede digital, tais como avassaladora, supersônica, estonteante, dentre outros.

Acessar a Internet tornou-se um hábito diário na vida de muitas pessoas, mudando seus hábitos, na busca por mais e mais informações e conhecimentos que venham facilitar suas vidas. Não há tempo a perder. A inserção brasileira na era digital já está ocorrendo e não pode seguir adiante de forma tímida. O Brasil terá que se esforçar para fazer parte do elenco principal, debatendo questões importantes que definirão, no enredo da nova economia, sua posição no mercado mundial.

No que se relaciona com as questões do comércio eletrônico, o Brasil deverá se envolver na discussão de um quadro normativo minimalista que

promova um ambiente previsível e livre de restrições ao comércio eletrônico, na tentativa de se encontrar soluções

apropriadas que mantenham a reciprocidade de interesses que deverá sustentar o processo de integração econômica e, leve em consideração as diferenças econômicas e tecnológicas de países em desenvolvimento como o nosso.

No que concerne ao debate sobre infra-estrutura e acesso, parece-nos coerente que o Governo brasileiro continue promovendo o exame da posição do Brasil com relação aos acordos do ITA – Information Tehnology Agreement, de forma a evitar eventuais estrangulamentos na oferta de produtos de tecnologia da informação e de serviços básicos de telecomunicações, ou a elevação de seus níveis de preços por proteção indevida.

A discussão sobre propriedade intelectual apresenta-se mais complexa. Torna-se necessário promover um amplo debate em torno do assunto para se ter absoluta certeza se os mecanismos hoje existentes e, que regulam a propriedade intelectual, são suficientes para simplesmente estendê-los ao ambiente digital. Parece-nos adequada a posição americana de que o “ordenamento deste novo espaço econômico só será ótimo na medida em que um regime rigoroso de propriedade intelectual for estabelecido". Entretanto, é preciso discutir e encontrar uma forma que permita a circulação de informações e conhecimentos, sem prejudicar o inventor e o mercado e, leve em consideração as diferenças regionais dos diversos países do mundo.

VII - Referências Bibliográficas

BARENBOIM, Bia. Conceitos Básicos sobre Segurança. Disponível em << http://olinux.uol.com.br/artigos/291/1.html >> acessado em 26/04/2005

BOGO, kellen Cristina. A História da Internet – Como Tudo Começou... Disponível em << http://kplus.cosmo.com.br/materia.asp?co=11&rv=vivencia>> acessado em 26/04/2005.

BRASIL, A. Bittencourt. O documento físico e o documento eletrônico. Disponível em <<http://jusnavigandi.com.br/doutrina/docuele2.html>>acessado em 26/04/2005.

BRETON, Philippe. A Utopia da Comunicação. Lisboa: Instituto Piaget, Col. Epistemologia e Sociedade. 1992

CORRÊA, Gustavo Testa. Aspectos Jurídicos da Internet. São Paulo: Saraiva. 2000.

DONIZETI, J. A.. A validade jurídica dos documentos digitais. Disponível em http://www1.jus.com.br/doutrina/texto.asp?id=3165. capturado em 25/04/2005.

ELIAS, Paulo Sá. O documento eletrônico, a criptografia e o direito: in*:* Revista Consultor Jurídico. Disponível em <<http:/www.uol.com.br/consultor>> acesso em 25/04/2005.

GATES, B. *A estrada do futuro.* Trad. Beth Vieira; José Rubens Siqueira; Ricardo Rangel. Cia das Letras. 1995.

GRECO, M. A. Internet e Direito*.* São Paulo: Dialética. 2000.

LEAL, G.J. Repensando a Tecnologia da Informação, AXCEL BOOKS, 2001

PAESSONI, L. M. Direito e Internet – Liberdade de Informação, Privacidade e Responsabilidade Civil. São Paulo: Editora Atlas. 2000.

RAMOS, Murilo César. Às Margens da Estrada do Futuro- Comunicações, políticas e tecnologia. Coleção FAC – Editorial Eletrônica.2000. Disponível em << http://www.unb.br/fac/publicacoes/murilo/>>. Acesso em 07/05/2005.

STAIR, R.M. Princípios de Sistemas de informação – Uma Abordagem Gerencial. LTC. Rio de Janeiro, 1996.

WEBOPEDIA - The only online dictionary and search engine you need for computer and Internet technology [on line] <<Disponível em http://webopedia.internet.com>>acesso em 25/04/2005.

_____ BRASIL. Presidência da República. Comitê Gestor de Chaves Publicas. Disponivel em < http://www.icpbrasil.gov.br/> Acesso em 26/04/2005.

_____ Comitê Gestor da Internet no Brasil. Disponível em <<http://www.cg.org.br/ sobre-cg>> acesso em 26/04/2005.

_____ UNCITRAL – United Nations Comissions on International Trade Law. Resolução nº 51/162. New York, USA (UN).

_____E-BRASIL. Câmara Brasileira de Comércio Eletrônico. Disponível em <http://www.e-brasil.org.br/contexto/index.shtml> acesso em 26/04/2005.