SEGURANÇA NA INTERNET
Hilton Andrade de Mello

O presente trabalho apresenta um resumo dos principais aspectos relacionados com a segurança dos computadores conectados à Internet, procurando estabelecer de forma simples, as ferramentas disponíveis para uma proteção eficaz. Não se trata de nenhum trabalho original, mas apenas uma compilação de trabalhos já publicados. Para evitar dúvidas sobre os termos utilizados, um pequeno glossário foi acrescentado no final do trabalho.

1-O que é exatamente a INTERNET?

É interessante dar uma rápida explicação sobre a Internet, porque ficará mais fácil entender a sua dimensão e vulnerabilidade.

A INTERNET é uma rede mundial de computadores, que se originou de uma rede do Departamento de Defesa dos Estados Unidos (ARPANET), e cujo objetivo principal era descentralizar as informações, de forma a que o sistema fosse virtualmente indestrutível, pois a destruição de qualquer elemento do sistema não impediria que as comunicações continuassem sendo feitas por caminhos paralelos.

Com o passar dos anos redes particulares de Empresas, Universidades, Centros de pesquisa, etc. foram sendo interligadas a essa rede, constituindo atualmente um gigantesco acervo de informações e de negócios.

Na prática o que ocorre é que computadores individuais e pequenas redes de computadores, se ligam a redes maiores, que finalmente se ligam a troncos de altíssima velocidade de transmissão, os chamados "***backbones"*** (espinha dorsal).

A Embratel disponibiliza, atualmente, o maior "backbone" Internet da América Latina, tanto em termos de abrangência, atingindo mais de 300 localidades em todo o país, como em capacidade de circuitos de transmissão de dados, em nível nacional e internacional *.

Para dar um exemplo, um desses "links" da Embratel liga o Brasil aos Estados unidos com uma velocidade de 20 Gbps (20 bilhões de bits por segundo), velocidade muito maior que a oferecida pelos sistemas de banda larga ao usuário comum no Brasil, de 8, 12 ou 16 Mbps (16 milhões de bits por segundo)!

O fato é que não existe um ente físico chamado de Internet, mas sim uma gigantesca rede de computadores interligados, de forma que estabelecido um protocolo, possam ser trocadas informações entre os usuários. No caso da Internet o protocolo usado é o **TCP/IP (Transmission Control Protocol/Internet Protocol).**

Quando do Brasil mandamos um E-mail para a China, o sistema escolhe o melhor caminho para que esse E-mail atinja o seu destino. Isto pode significar passar por vários computadores espalhados pelo mundo, por meio de cabos, fibras óticas e "links" de satélites, devidamente interligados.

Bem, com milhões de computadores interligados, como o sistema identifica cada computador? Toda vez que acessamos a internet recebemos um endereço, que é chamado de endereço **IP,** e que nos identifica na rede, de modo que o sistema sabe exatamente como chegar ao nosso computador.

****Extraído do "site" da Embratel (***http://www.embratel.com.br/***)***

2-Afinal, de que problema de segurança estamos falando?

Cientistas, engenheiros e técnicos conseguiram viabilizar um sistema barato, prático e rápido para a troca de informações, utilizando computadores interligados em uma grande rede; mas como sempre acontece existe a face negra dessa idéia maravilhosa, pois imediatamente os gênios do mal ("Hackers") iniciaram os seus trabalhos, alguns visando destruir dados e componentes físicos, e outros criando potentes ferramentas para invadir a vida dos usuários, rastreando "sites" visitados, captando senhas de acesso bancário e dados pessoais, enfim criando sérios problemas de segurança. Centenas de usuários já foram vítimas de golpes praticados na Internet, de forma que é absolutamente imprescindível que todos os que utilizam a grande rede, principalmente os que a utilizam para efetuar compras e realizar operações bancárias, estejam a par dos mecanismos de proteção necessários para uma navegação ***razoavelmente*** segura

3-Um pouco de nomenclatura

As palavras "HARD**WARE"** e "SOFT**WARE",** referem-se respectivamente aos componentes físicos de um sistema e aos programas utilizados nos computadores; assim são itens de hardware a CPU, o Monitor, o Teclado, o Mouse, etc.; já o Internet Explorer, o Skype, e o WORD, são exemplos de "software".

Mais recentemente foi introduzida a palavra MAL**WARE,** para designar qualquer "software" **mal**icioso, projetado para se infiltrar em um sistema computacional sem o conhecimento do usuário e exercer alguma ação nociva.

O exército dos "malware" é muito vasto e poderoso e está exigindo dos usuários e autoridades um enorme esforço para amenizar os danos por eles causados, e punir os responsáveis por sua utilização. Os Vírus, Cavalos de Tróia, Worms, Spyware, e diversos tipos maliciosos de Adware, são exemplos dessa tropa maléfica.

4-As portas de entrada de um computador

Apenas para exemplificar imaginemos uma das ações básicas que fazemos na Internet, o recebimento e envio de E-mails; É claro que quando um E-mail é enviado para nós, e é recebido no nosso computador, esse E-mail caminhou de alguma forma pela rede, e chegou ao nosso computador. Para que isso seja possível, o computador possui o que chamamos de portas. Em um computador normalmente existem 65536 portas, numeradas de 0 a 65535, que possibilitam esse acesso.

Algumas dessas portas tem sua utilização padronizada; por exemplo, quando acessamos um 'site' da internet é utilizada a porta 80 do servidor. Já o software MSN MESSENGER utiliza as portas de 6891 a 6900 para a transferência de arquivos, e a 6901 para as comunicações de voz.

É claro que o usuário normalmente nem toma conhecimento da existência e uso dessas portas, mas a pergunta óbvia, que deve ter se formado na mente do nosso leitor, é como o acesso a essas portas é controlado. Esse é de fato um grande problema de segurança, pois normalmente essas portas estão disponíveis, de modo que um "hacker" pode descobrir isso e utilizá-las para invadir o nosso computador e nele instalar um "malware".

Na realidade os "Hackers" ficam continuamente vasculhando a Internet, e quando descobrem um computador cujas portas estão abertas, a festa está feita!!!

Daí surge a primeira ferramenta indispensável no mundo da Internet, o chamado **FIREWALL** (Parede de fogo), que pode ser o embutido no windows XP, ou qualquer outro disponível no mercado.

O que o Firewall faz? Como o nome sugere o firewall funciona como uma parede, um escudo de proteção, se interpondo entre a Internet e o nosso computador: ele controla todas as portas, somente permitindo o acesso se assim o desejarmos.

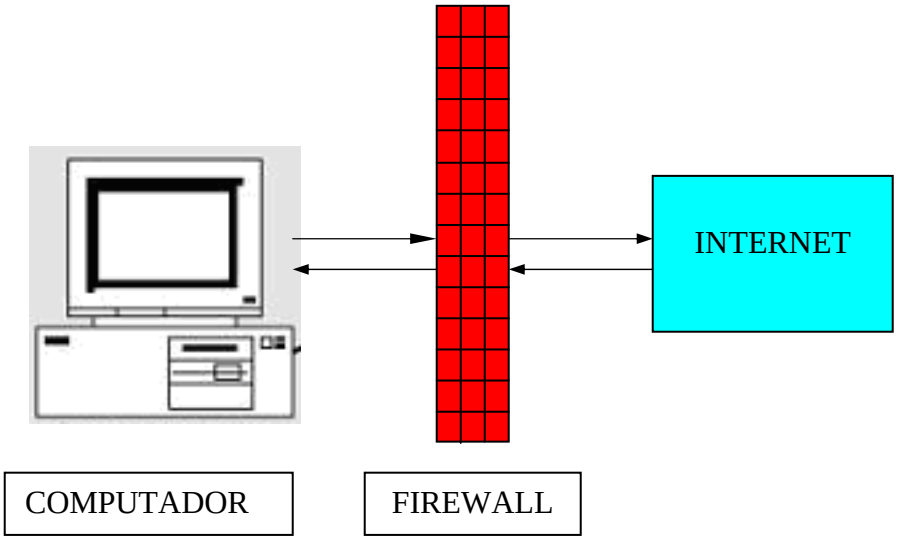

Fig. 2-A proteção do FIREWALL

Normalmente quando um "site" tenta estabelecer uma conexão pela primeira vez com o nosso computador, o firewall perguntará se permitimos ou não o acesso, e se queremos que essa informação seja gravada; caso indiquemos que sim, da próxima vez o firewall não fará a consulta.

REGRA NÚMERO 1
ATIVE O FIREWALL DO WINDOWS OU UTILIZE UM BOM FIREWALL DISPONÍVEL NO MERCADO.

5-Segurança adicional

E agora será que estamos devidamente protegidos?
É claro que não, pois o Firewall apenas impede que o nosso computador seja acessado ***sem o nosso consentimento***.
O problema é que o uso normal do computador viabiliza a introdução de todos os tipos de "malware".
Os Vírus, que por definição são software maléficos que se reproduzem, podem infectar o computador pelo simples uso de disquetes, "pendrives" ou outros dispositivos que permitam a transferência de arquivos, e que estejam contaminados. Os vírus podem inclusive danificar discos rígidos e outros itens de hardware.

A Instalação de um bom programa ANTIVIRUS é vital para evitar esses problemas de contaminação. Chamamos a atenção que não adianta nada instalar um bom programa antivírus e não mante-lo devidamente atualizado, pois a cada dia novos tipos de vírus são criados e as vacinas para os mesmos são obtidas com as atualizações.

REGRA NÚMERO 2
UTILIZE UM BOM PROGRAMA ANTIVIRUS, E O MANTENHA RIGOROSAMENTE ATUALIZADO.

Além disso, ao navegar na Internet, acessamos "sites" que apresentam assuntos de nosso interesse, e recebemos dezenas de E-mails cuja origem é desconhecida. A simples entrada em alguns "sites" ou a abertura de anexos de E-mails podem gerar sérios problemas de segurança. Até a instalação de alguns "software" gratuitos podem gerar problemas de segurança, pois esses programas quando executados podem introduzir no nosso computador diversos tipos de "malware". Dois tipos bem divulgados de "malware" são os "Spyware" e os "Adware".
Os "Spyware" são programas que espionam o computador, e podem enviar para o seu criador dados pessoais do usuário, contas bancárias, senhas, etc.
Os "Adware" (AD-de advertisement:propaganda) são programas que normalmente estão vinculados a exibição de propagandas no nosso computador; muitas vezes esses "adware" estão embutidos em programas que são oferecidos gratuitamente, e é comum esse fato ser especificamente declarado nas pequenas letras do contrato, que normalmente dizemos "aceito" sem ler com atenção.
De qualquer forma é importante sabermos tudo que foi instalado no nosso computador, seja ou não maléfico.
Há dois excelentes programas para detetar e eliminar esses perigos do seu computador. São o "**Spybot-Search & Destroy**" e o "**Ad-Aware**", ambos grátis e que podem ser obtidos na Internet.

REGRA NÚMERO 3
UTILIZE UM BOM PROGRAMA PARA DETETAR E REMOVER SPYWARE E AD-WARE.

6-Software grátis e comprado

Devemos estar atentos que muitas vezes vale a pena gastar um pouco e facilitar a vida com relação à segurança. O que acontece é que muitos "software" grátis possuem uma versão paga e que pode reunir diversos programas em um só.
Para dar um exemplo, o popular AVG tem uma versão grátis (AVG Anti-Virus free edition) e uma versão paga que na realidade é um pacote completo visando prover uma segurança adequada na Internet (AVG INTERNET SECURITY). Esse tipo de software é também fornecido por outros fabricantes como o NORTON (Symantec), AVAST e outros.

Na realidade esses sistemas que visam uma proteção “completa” na INTERNET, integram no pacote todos os programas necessários para uma proteção adequada, justificando portanto, o investimento realizado.
Por exemplo o AVG INTERNET SECURITY é composto de:
Antivírus, Anti-Spyware, Anti-Spam, Firewall, LinkScanner, Proteção residente, Family Safety, Verificador de E-mail, Proteção Online.
Ou seja, um conjunto de ferramentas que supervisionam completamente o computador.
Ah!!! Eu ia esquecendo de mencionar: será que é razoável confiar nos “software” ilegais, que são vendidos livremente no Brasil? É evidente que sempre há o risco de um programa vendido por um camelô conter algum tipo de “malware”, fato que infelizmente somente é descoberto tarde demais.

7-Armadilhas adicionais

Embora os Bancos, Empresas que prestam serviços (Gás, Luz ,Telefone) e os Órgãos do Governo em geral avisem que não fazem nenhuma solicitação de dados pessoais por meio de E-mail, dezenas de usuários são vítimas desse golpe vulgar:

“Você tem um processo pendente na Receita Federal. “Click” no “link” abaixo para agendar sua ida à Receita Federal”...
“Você tem um dívida com a nossa empresa “Click” no “link” abaixo para evitar que o seu nome seja incluído no SERASA”...

Ou então o apelo à nossa imaginação ou ganância:
“Alô querido! Essa é apenas uma de minhas fotos. Visite o meu “site” no “link” abaixo e se delicie com as minhas fotos sensuais. Te amo!”...
“Você acaba de ganhar 1000 dólares”. “Click” no link baixo para ver como receber o seu premio”...
E dezenas de golpes similares.

REGRA NÚMERO 4
NENHUM BANCO, ORGÃO DO GOVERNO OU PRESTADOR DE SERVIÇO PÚBLICO, ENVIA INTIMAÇÕES OU PEDE DADOS PARTICULARES POR E-MAIL. SIMPLESMENTE IGNORE ESSES E-MAILS, OU EM CASO DE DÚVIDA CONSULTE DIRETAMENTE O ORGÃO EM QUESTÃO.
NÃO ACREDITE EM BENESSES OU PREMIOS DADOS PELA INTERNET.
LEMBRE QUE NINGUÉM DÁ NADA DE GRAÇA!!!

8-Comentários finais

O problema de segurança na Internet é extremamente sério e complexo, e caso o leitor não se julgue capacitado a cuidar da sua segurança, acho que não deve efetuar transações bancárias ou compras utilizando a Internet.
O que fizemos foi apenas uma pequena incursão nos aspectos de segurança envolvendo a Internet, mas o leitor pode usar a própria rede para consultar artigos mais completos e obviamente mais complexos.

BOA SORTE

Gostaria de receber os seus comentários

(hamello@unisys.com.br)

GLOSSÁRIO

Backbone – Chamamos de backbone a uma linha de transmissão de dados de alta velocidade, que recebe os dados de outras linhas de menor velocidade; Na Internet há diversos "backbones" interligando regiões diferentes do planeta,

Bit – Nos computadores lidamos com o sistema binário, que usa apenas os dígitos 1 e 0 , ao contrário do sistema decimal que usa os digitos 0 a 9. O fluxo de dados em um computador é feito apenas com esses digitos 0 e 1, que são chamados de "bits". A velocidade de transmissão de dados e é medida em bits por segundo, ou com os multiplos kilobits por segundo(**Kbps**), Megabits por segundo (**Mbps**), Gigabits por segundo (**Gbps**) e Terabits por segundo (**Tbps**).Lembre que os prefixos Kilo, Mega, Giga e Tera correspondem a mil, milhão, bilhão e trilhão).

Byte- O conjunto de 8 bits chamamos de Byte.Por exemplo a seqüência "01000001" corresponde a um byte. Novamente podemos usar os prefixos anteriores para designar quantidades maiores de bytes. Por exemplo 100 Megabytes corresponde a 100 milhões de bytes.

Hacker – O termo hacker originalmente em inglês é aplicado àquelas pessoas que trabalham duramente encima de um objetivo, esmiuçando todos os detalhes; ou seja o próprio "bisbilhoteiro"!!! Atualmente o termo é geralmente usado para designar os programadores que invadem os sistemas de computação alheios sem autorização, e geralmente provocam danos aos usuários, captando senhas de acesso bancários, etc. Na realidade os "hackers" não são todos gênios do mal, pois é graças a muitos deles, que esmiúçam todas as falhas de segurança, por exemplo no windows, permitindo assim que essas falhas sejam corrigidas. Os gênios do mal que realmente causam danos são mais corretamente chamados de "crackers". Mas de um modo quase generalizado se usa o termo "hackers" para todos os casos.

Link – Em inglês "link" significa o meio de ligação entre duas coisas; na Internet o termo link é usado para designar um local onde se deve "clicar" o mouse para entrar em um dado "site". Por exemplo o link abaixo nos conduz ao "site" da Receita Federal:

http://www.receita.fazenda.gov.br/

Protocolo - Para que computadores possam se comunicar é necessário que seja estabelecida uma "linguagem" comum, ou seja um conjunto de regras que estabeleça padrões a serem obedecidos. Essas regras são estabelecidas no que chamamos de protocolo; no caso da Internet o protocolo aplicado é o **TCP/IP** (**T**ransmission **C**ontrol **P**rotocol/**I**nternet **P**rotocol).

Site e Homepage –Em inglês site significa local, lugar; Na internet falamos de “site” do Banco do Brasil, “site” do museu do Louvre, “site” do Yahoo, etc. Muitas vezes esse termo é usado como sinonimo de “home page”, mas a homepage é a primeira página de entrada em qualquer “site”. Na Home page há links para entrada das outras páginas. Por exemplo a Home page do Museu do louvre é “http://www.louvremuseum.com/”. Nessa página de entrada há “links” direcionando para as diversas atividades e conexões do museu.