O Perigo no Mundo Virtual

Jordano Fernandes Cordeiro

Mateus Fonseca dos Reis

Augusto César Alves

Resumo: *O aumento da troca de informações via internet e dispositivos portáteis tem demonstrado a necessidade de sistemas/procedimentos de segurança cada vez mais rigorosos. Um grande erro é julgar que somente as pessoas que utilizam a internet para operações comerciais ou bancárias estão sujeitas ao perigo virtual, pois existem vários outros crimes, cometidos na internet, que possuem finalidades diversas. Outro grande problema vinculado à internet são os sítios de relacionamentos, uma vez que os usuários disponibilizam informações valiosas, facilitando a ação dos criminosos.*

Palavras chave: *Internet; Crimes virtuais; Segurança na internet.* Dimitri Araújo Soares

1. INTRODUÇÃO

Atualmente, é praticamente impossível viver afastado da internet. O número de usuários com acesso à internet tem crescido de forma espantosa, o que tem forçado cada vez mais o desenvolvimento de novas tecnologias de acesso e transmissão de dados. E assim, o uso cada vez maior de tecnologias diferentes com essa finalidade torna a missão de manter uma rede segura uma tarefa mais complicada.

Ao se falar em segurança na internet, a imagem que aparece rapidamente na mente das pessoas é a imagem dos hackers. Hacker é o indivíduo que tem a habilidade de enganar os mecanismos de segurança de sistemas de computação e conseguir acesso não autorizado aos recursos destes. E um grande erro é pensar que somente as pessoas que utilizam a internet para operações comerciais ou bancárias são os alvos dos hackers. Mas então, por que alguém teria interesse invadir máquinas de usuários domésticos, que não possuem arquivos valiosos, ou mesmo estações de trabalho que são usadas apenas para editar textos e enviar e-mails? A questão principal nem sempre são as informações armazenadas, mas sim a banda e o poder de processamento das máquinas. Ter vários computadores sob seu controle significa poder.

A pergunta agora é: como manter uma rede segura? Segundo Morimoto (2008), o comportamento do usuário é o que mais afeta na segurança do sistema. Assim, o objetivo deste artigo é apresentar os principais erros cometidos pelos usuários e sugerir algumas ações para melhorar a segurança na internet.

2. METODOLOGIA

Para o desenvolvimento deste artigo, foram pesquisados quais são os erros mais comuns dos usuários da internet que comprometem a sua segurança. Em seguida, foram apresentadas algumas ações que ajudam a tornar uma rede mais segura.

3. PRINCIPAIS ERROS QUE AFETAM A SEGURANÇA DE UMA REDE

Pode-se dizer que um computador ou um sistema computacional é seguro se ele atende a três requisitos básicos relacionados aos recursos que o compõem: confidencialidade, integridade e disponibilidade. Porém, alguns procedimentos dos usuários podem comprometer a segurança deste

sistema.

Os usuários estão tão acostumados e familiarizados com o ambiente da internet que às vezes não percebem que estão se descuidando da segurança. Um grande erro cometido é na visualização de *e-mails*. Grande parte dos problemas de segurança envolvendo *e-mails* está relacionada ao seu conteúdo e/ou às características de determinados programas leitores de *e-mails*, que permitem abrir arquivos ou executar programas anexados às mensagens automaticamente, sem prévia análise de sua confiabilidade pelo destinatário.

Outro problema que afeta a segurança de um computador ou de uma rede de computadores está vinculado a sítios não seguros, acessados pelos usuários em busca de jogos, programas, vídeos, dentre outras necessidades e se descuidam dos *plug-ins* e *pop ups* destes sítios. Geralmente, os *pop ups* contêm *links* "atraentes" que podem redirecionar os internautas à páginas fraudulentas ou induzi-lo a instalar *softwares* maliciosos. Já os *plug-ins* tem acesso irrestrito ao sistema, podendo buscar informações do disco local ou introduzir um *trojan horse* (cavalo de tróia), que é um programa utilizado para liberar acessos para uma invasão. *browsers* passaram a receber código ativo pela rede, e o simples fato de visitar uma página de um sitio na *Internet já o suficiente para receber um código malicioso que possa ter acesso a qualquer parte do sistema ou da rede. Internet; Crimes virtuais; Segurança na internet.*

A segurança de qualquer rede ou sistema começa pela senha de acesso, porém a maioria dos usuários comete um erro freqüente, às vezes por comodidade, que é a utilização de uma senha para todas as ocasiões e senhas consideradas fáceis, como datas especiais. E de forma geral, disponibilizam em sítios de relacionamentos ou *blogs* todas essas datas e informações pessoais, facilitando a dedução da senha.

Dentre os erros que afetam a segurança de uma rede, estes são os principais. Contudo, deve-se ter consciência que não são os únicos, pois a não utilização de *firewall* e antivírus ou a utilização de antivírus desatualizado e a utilização em demasia de programas de mensagens instantâneas e compartilhamento de pastas em rede podem trazer transtornos bem grandes. **5. CONCLUSÕES**

4. AÇÕES QUE PROMOVEM A SEGURANÇA

Dentre as diversas atitudes que podemos tomar para promover a segurança, se destacam algumas simples atitudes que, muitas das vezes, passam despercebidas, como:

- atualizar o antivírus diariamente, fazendo o escaneamento de tempos em tempos;
- não clicar em links recebidos por e-mail, sem análise prévia;
- não executar arquivos recebidos por e-mail ou via serviços de mensagem instantânea, sem análise prévia;
- manter os programas, como o navegador, atualizados;
- utilizar, além de antivírus, *firewall* e *anti-spyware*;
- somente habilitar o *javascript*, *cookies* e *popup windows* ao acessar sites confiáveis;
- nas senhas, não utilizar dados pessoais e procurar usar letras, números e símbol
- evitar colocar dados pessoais em páginas Web, blogs ou sites de redes de relacionamentos.

Portanto, apesar da internet ser muito atrativa e conectar todas as pessoas à praticamente todos os assuntos relacionados à suas vidas, deve-se tomar bastante cuidado no uso desta ferramenta, talvez a mais importante atualmente. Isto porque com um simples clique o internauta pode se tornar vítima de algum golpe ou crime. Os usuários devem se cercar de todos os meios possíveis de segurança, seja ele a nível de *hardware*, pois existem equipamentos para fraude com funções diversas, passando pelo nível de *software*, que talvez seja onde existam mais ferramentas e artifícios para se obter informações e aplicar golpes, e chegando ao nível do usuário, que precisa se reeducar para não

cometer pequenos erros como os citados anteriormente, de forma a estar atento a todas as atitudes, observando sempre o que acontece a sua volta para não ser enganado.

Os crimes virtuais são caracterizados não somente por ocorrer em um meio que não seja físico, porque, muitas das vezes, suas conseqüências são sentidas no mundo real. Através de determinadas informações conseguidas no mundo virtual, esses crimes podem se desdobrar em seqüestros, furtos, roubos, atentados ao pudor, atentados a honra e outros, ocasionando transtornos diversos pelo simples compartilhamento de dados e detalhes da vida pessoal com estranhos.

No mundo virtual, deve-se manter as informações pessoais de forma muito mais sigilosa do que no mundo real, pois muitas das vezes não se conhece a pessoa que está te observando.

REFERÊNCIAS BIBLIOGRÁFICAS

MORIMOTO, Carlos E. ***Redes, Guia Prático*****. Ed. GDH Press e Sul Editores, 2008. 560 p.**
CERT.br, ***Cartilha de Segurança para Internet.*** **Versão 3.1, 2006**