Segurança na Internet: Qual a nossa Vulnerabilidade?

Thiago Domingos de Souza Silva

Hoje em dia qualquer usuário conectado a internet, independentemente do objetivo e da tarefa a ser realizada, está sujeito a ataques e invasões de vírus e pessoas de mal intencionadas. Este artigo irá mostrar quais os maiores riscos que um usuário pode correr ao utilizar a internet e quais tipos de ataques cada perfil de usuário está mais sujeito a sofrer, oferecendo também dicas de como se proteger e se tornar menos vulnerável.

Os motivos pelos quais alguém tentaria invadir seu computador são inúmeros, entre eles o seu computador pode ser utilizado para alguma atividade ilícita, para ler e enviar emails em seu nome, furtar senhas de banco e contas de usuário, disseminar vírus, utilizar seu computador para lançar ataques contra outros computadores, etc.

Cada perfil de usuário está mais sujeito a um tipo de ataque do que outro. Usuários domésticos, que buscam entretenimento e utilizam redes sociais estão muito sujeitos a ataques que utilizam um método denominado engenharia social, que se baseia na ingenuidade ou confiança do usuário para obter informações que podem ser utilizadas para ter acesso não autorizado a computadores ou informações. Um exemplo são mensagens postadas em redes sociais (Orkut, Twitter, Facebook) ou enviadas via programas de mensagem instantânea (MSN, ICQ, Yahoo Messenger) que contém mensagens de propaganda ou se faz passar por alguma empresa conhecida (cartões virtuais, álbum de fotos), solicitando acessos através de links, que na verdade contém algum vírus ou instala programas maliciosos para captura de informações do computador ou para permissão de acesso de algum invasor. Este tipo de mensagem maliciosa também é muito comumente enviada via e-mail.

Quanto à utilização de blogs, a disponibilização de informações como seus dados pessoais (e-mail, telefone, endereço), informações sobre seus familiares e amigos, dados sobre seu computador e informações sobre seu cotidiano podem ser utilizados por pessoas mal intencionadas para lançar ataques de engenharia social ou até mesmo ataques à integridade física do usuário.

Por último, o acesso a sites de pornografia, jogos e programas de compartilhamento de arquivos podem conter diversos tipos de malware (vírus, worms, backdoors, cavalos de tróia, spywares), que colocam em xeque a segurança do computador.

Usuários corporativos também estão muito vulneráveis a ataques de engenharia social, principalmente através de e-mails que se fazem passar por bancos, instituições e empresas conhecidas e órgãos governamentais (Receita Federal, SPC, Serasa, Polícia Federal), e assim se utilizam da confiança do usuário para capturar senhas de banco, informações para utilização em atividades ilícitas em seu nome, para ter acesso não autorizado a seu computador, roubar informações, entre outras. Ataques desta natureza são conhecidos como “phishing”.

Este tipo de usuário também sofre muito com e-mails do tipo “spam”, que são arquivos de correio não solicitados e que geralmente são enviados para um grande número de usuários. Este tipo de e-mail pode causar diversos transtornos, como:

- Não recebimento de 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 antispam ineficientes, por exemplo, classificando como spam mensagens legítimas.

- Gasto desnecessário de tempo: Para cada spam recebido, o usuário necessita gastar um determinado tempo para ler, identificar o e-mail como spam e removê-lo da caixa postal.

- Aumento de custos: Independentemente do tipo de acesso a Internet utilizado, quem paga a conta pelo envio do spam é quem o recebe. Por exemplo, para um usuário que utiliza acesso discado a Internet, cada spam representa alguns segundos a mais de ligação que ele estará pagando.

- Perda de produtividade: Para quem utiliza o e-mail como uma ferramenta de trabalho, o recebimento de spams aumenta o tempo dedicado à tarefa de leitura de e-mails, além de existir a chance de mensagens importantes não serem lidas, serem lidas com atraso ou apagadas por engano.

- Conteúdo impróprio ou ofensivo: Como a maior parte dos spams são enviados para conjuntos aleatórios de endereços de e-mail, é bem provável que o usuário receba mensagens com conteúdo que julgue impróprio ou ofensivo.

- Prejuízos financeiros causados por fraude: O spam tem sido amplamente utilizado como veículo para disseminar esquemas fraudulentos, que tentam induzir o usuário a acessar e-mails do tipo "phishing".

Para se prevenir dos ataques de engenharia social, nos casos em que receber mensagens procurando lhe induzir a executar programas ou clicar em um link contido em um e-mail ou página da web, é extremamente importante que você, antes de realizar qualquer ação, procure identificar e entrar em contato com a instituição envolvida para certificar-se sobre o caso. Procure não fornecer muita informação e não forneça, sob hipótese alguma, informações sensíveis, como senhas ou números de cartões de crédito. Sites de comércio eletrônico ou Internet Banking confiáveis sempre utilizam conexões seguras, quando dados pessoais e financeiros de usuários são solicitados. Caso a página não utilize conexão segura, desconfie imediatamente. Caso a página falsificada utilize conexão segura, um novo certificado (que não corresponde ao site verdadeiro) será apresentado e, possivelmente, o endereço mostrado no browser será diferente do endereço correspondente ao site verdadeiro.

Outras medidas de segurança são a utilização de um bom programa antivírus, que esteja sempre atualizado, o uso de firewall, que bloqueia tentativas de invasão ao seu computador, a utilização de um filtro antispam em seu servidor de e-mail e principalmente que o usuário tenha bom senso e desconfie de mensagens e e-mails que solicitem informações pessoais ou que contenham anúncios mirabolantes. Deve-se ter cuidado também com links não solicitados enviados por e-mail ou mensagens, mesmo que sejam de pessoas conhecidas, pois o remetente pode ser facilmente falsificado ou até estar infectado por algum malware.

Ou seja, estando bem informado e disciplinando um pouco sua postura, o usuário pode se manter livre de ataques ou riscos de infecções, já que a grande maioria destes ataques só são possíveis se o usuário abrir as portas para o invasor.