Vírus: mitos e verdades

"Alguns sistemas não possuem vírus". Esta é sem dúvida uma das declarações que mais ouvimos no mundo de TI. Porém, se observarmos os objetivos dos propagadores de vírus, descobriremos que todos os sistemas operacionais estão no alvo, inclusive os softwares livres.

Os grandes focos de propagação de pragas virtuais hoje em dia são: a Internet e os emails. Em todas as empresas, existem usuários que acessam a Internet e recebem emails, independente da plataforma utilizada. Portanto, são passíveis de serem contaminadas.

Existem vários tipos de pragas digitais, cada uma com característica própria:

Vírus - São programas que se inserem dentro do código de outros programas, ou áreas específicas de um software, como por exemplo, a área de boot. Neste caso, nem será notada sua presença, pois parte do código legal do programa é descartado para dar espaço ao código do vírus. Um vírus pode excluir arquivos do computador ou abaixar as configurações de segurança, atraindo novos ataques.

Worms - Os worms diferem dos vírus por copiar a si mesmos de sistema para sistema. Eles podem copiar-se de uma unidade de disco para outra, usando a rede local ou email. Os worms comprometem a segurança do computador, pois não necessitam contaminar outros programas ou mesmo de intervenção do usuário para se propagarem.

Trojans - São programas que tentam se passar como "bonzinhos", mas que realizam ações mal-intencionadas. Geralmente é recebido pela Internet por meio de downloads ou por anexos de emails, em forma de proteção de tela, fotos entre outros.

Parando para analisar friamente as definições acima, chegamos à conclusão de que todos os sistemas operacionais podem ter algum tipo de contaminação. Seja por compartilhamento da rede, de anexos de emails, de downloads de "programinhas da Internet" ou de sites de conteúdo duvidoso. Entretanto, algumas regras gerais - que incluem mudanças no comportamento dos usuários - podem ajudar na prevenção e correção do problema.

1. Mantenha sistemas operacionais, navegadores e programas de e-mail atualizados

A Microsoft possui o Windows Update, que verifica quais atualizações são necessárias para cada sistema. O serviço é gratuito e basta clicar no ícone Windows Update do computador ou acessar o site:http://v4.windowsupdate.microsoft.com/ptbr/default.asp
[http://v4.windowsupdate.microsoft.com/ptbr/default.asp]

2. Use anti-vírus e mantenha-o constantemente atualizado

Tenha sempre um antivírus instalado em sua máquina. As atualizações de todos os fabricantes são dinâmicas, basta você acessar a Internet para ele se atualizar. Programe varreduras freqüentes no disco e tenha sempre um disco de recuperação guardado para qualquer eventualidade.

3. Use firewall pessoal

Um firewall pode bloquear conexões indesejadas, prevenindo a propagação dessas pragas digitais. O Windows XP possui um firewall pessoal gratuito. Caso tenha alguma dúvida quanto à configuração, instruções passo a passo são encontradas em:http://www.microsoft.com/brasil/security/protect/windowsxp/firewall.mspx
[http://www.microsoft.com/brasil/security/protect/windowsxp/firewall.mspx]
Lembre-se que no Service Pack 2 (SP2) do Windows XP, teremos ainda mais recursos no firewall.

4. Não abra e-mails não esperados

É complicado dizer isso, mas infelizmente, é necessário. Mesmo que as mensagens pareçam vir de pessoas conhecidas, não abra as que você não está esperando. Se for o caso, telefone ou envie um e-mail para seu amigo e confirme a razão de ele ter enviado algo que vocês não tinham combinado.

5. Cuidado com e-mails de conhecidos

Esta também é difícil. Muitos programas maliciosos são transmitidos acidentalmente entre conhecidos. Inclusive, alguns e-mails que parecem ter sido enviados por conhecidos podem ter sido, na verdade,

enviados por ação de algum vírus ou worm e estarem identificados como vindos de um endereço de e-mail que você conheça. Siga a recomendação acima.

6. Não abra e-mails contendo anexos não solicitados

Se o e-mail contém este tipo de anexo, o melhor mesmo é não abri-lo, principalmente se forem arquivos executáveis. Adicionalmente, jamais faça download em sites desconhecidos.

7. Cuidado com as aparências

Alguns sites e e-mails anunciam programas que prometem a cura para a contaminação. Ao invés disso, servem para propagar outros vírus e programas maliciosos, podendo agravar a situação do usuário.

8. Procure correções para o problema

Se o problema já ocorreu, procure orientações e ferramentas para remoção no site dos fabricantes de sistemas operacionais e anti-vírus.

É fácil reparar que, além do uso de tecnologia, a segurança também inclui mudanças de atitude nas pessoas. A consciência do usuário é fundamental, mesmo com várias ferramentas disponíveis.

Inicio da pagina