55 – Fevereiro de 2004

Vírus: como estar 100% seguro

Deixe de usar o computador. Esta parece ser a melhor solução, senão a única, que realmente elimina os riscos de uma contaminação por vírus de computador em 100%. No mundo já são mais de 50 mil programas de computador desenvolvidos para provocar prejuízo, perda de informação, vazamento ou qualquer dano à operação de um computador. Eles se multiplicam em uma velocidade absurda e vem ganhando inteligência com o passar dos anos. Lembro-me dos vírus ping-pong, sexta-feira 13 ou o madonna que tiraram o sono ou fizeram rir muitos dos usuários de computador na década de 80. Eram perigosos se considerarmos seus objetivos de atrapalhar o usuário, apagando um arquivo e até engraçados ao embaralharem a tela do velho monitor de fósforo verde, fazendo as letras caírem ao pé da tela. Os programadores desses programas repugnantes, por mais criativos que pudessem ser, estavam limitados pelo poder de processamento, pelo espaço em disco e principalmente pelos escassos recursos de conectividade que tornavam o computador uma ilha incomunicável na maioria do tempo.

Mas de lá para cá muita coisa mudou, a começar pela popularização das redes, primeiro em perímetros privados e fisicamente definidos, depois por perímetros lógicos remotos e logo em seguida pela conexão através da rede mundial de computadores. O poder de processamento dos equipamentos cresceu muito, os dispositivos de comunicação seguiram o mesmo caminho, o email se tornou ferramenta individual e indispensável para qualquer um em praticamente qualquer atividade e a comunidade digital também cresceu proporcionalmente. Os vírus ganharam recursos novos que permitem a auto-replicação, a geração automática de variantes, a mutação comportamental com base em variáveis externas e até mesmo, o poder de decidir o alvo e o melhor momento para entrar em ação. Isso nos leva a concluir que os potenciais programadores de vírus estão em muito maior número, com uma quantidade infinitamente maior de recursos, agora disponíveis mundialmente e pior, com muito mais usuários acessíveis que possam servir de vítima voluntária ou involuntária.

Este conceito de voluntariado não está associado à vontade explícita de um usuário de computador em ser contaminado, mas sim por sua atitude imprudente e muitas vezes por seu comportamento negligente que o torna vítima. Já o involuntário pode ser considerado aquele que tomou todas as providências dentro das suas limitações, como instalar e manter atualizado o anti-vírus e não abrir arquivos suspeitos, mas foi surpreendido por uma falha do sistema operacional que o expôs à ação de um novo vírus.

Parece que estamos todos encurralados. Se estamos conectados à Internet, temos o mundo inteiro como potencial candidato a experimentar o poder de proteção do meu computador. Se me limito à rede corporativa sem Internet, posso não estar diretamente ligado ao potencial destrutivo da grande rede, mas ser um alvo de segundo nível, contaminado por outro computador da mesma rede privada que em algum momento manteve uma conexão suspeita e se tornou o hospedeiro e replicador de um agente virótico. Se radicalizo e desconecto a pobre máquina das tradicionais redes, posso ainda ser alvo de um vírus que

chega através da leitura de um cdrom, um disquete ou ainda um dispositivo usando infra-vermelho que insiste em estabelecer uma conexão sem fio e me transferir qualquer arquivo.

A comunidade digital está sem saída. É optar pelo isolamento, reduzir drasticamente o risco e também perder todos os benefícios que a tecnologia e o poder de conectividade nos oferece, ou ceder aos seus encantos e "tentar" se cercar de tudo que encontrar para reduzir os riscos a níveis aceitáveis. Tudo indica que as empresas já estão em estágio bem avançado de proteção da máquina do usuário final. Empregam antivírus automáticos e atualizados de forma transparente sempre que uma nova ameaça surge, treinam os funcionários e os orientam a não adotar comportamentos de risco no manuseio das informações, apertam os processos de permissão de acesso e filtram os recursos da rede privada e da Internet. Porém, os fatos têm demonstrado que estes procedimentos não são suficientes. Trata-se de uma malha muito veloz e super conectada onde um único usuário despreparado pode comprometer a segurança do grupo e principalmente dos serviços e informações disponibilizadas na rede. É preciso fazer mais. É preciso ser pró-ativo, monitorar o movimento da rede e dos usuários, definir índices de normalidade e acompanhá-los regularmente, de preferência em tempo real, para perceber situações que sinalizem a proximidade do caos. Como contramedida de contingência, já que risco zero inexiste, é preciso adotar mecanismos inteligentes de segmentação de perímetro, isolamento dinâmico de segmentos da rede e até mesmo de computadores específicos que aparentam ser suspeitos. Caso contrário, se nada disso for feito e se sua empresa não quiser vivenciar a amarga experiência de perder informações valiosas, interromper os serviços e experimentar o prejuízo, talvez a melhor solução seja abandonar o computador.

Marcos Sêmola *é Security Practice Manager da multinacional Atos Origin, Consultor Sênior em Gestão de Segurança da Informação, CISM – Certified Information Security Manager, Professor de Segurança da Informação da FGV – Fundação Getúlio Vargas, MBA em Tecnologia Aplicada, Bacharel em Ciência da Computação e autor do livro Gestão da Segurança da Informação – uma visão executiva, Ed.Campus 2003.*
marcos@semola.com.br