63 - Janeiro de 2005

A paranóia da segurança chegou ao usuário final.

Demorou mas chegou ao usuário final o comportamento paranóico da segurança da informação. Para os profissionais de tecnologia da informação, há muito o assunto é conhecido e fator de motivação, sendo também o principal responsável pelo desenvolvimento de uma síndrome de medo ou digamos, respeito pelos agentes eletrônicos de risco.

Muito antes da Internet virar realidade, quando os computadores ainda eram ilhas de processamento ou quando somente trocavam mensagens através de Boletim Board Systems, a percepção dos riscos de segurança para programadores, administradores de sistemas e profissionais de TI em geral já era elevada. Seja durante a troca de programas de computador usando os velhos discos de 3 ½, seja na utilização de programas residentes em memória ou ainda durante o desenvolvimento de uma rotina em linguagem de programação, já existia uma preocupação com o acesso indevido aos dados, com a potencial indisponibilidade de um trecho de código fonte ou ainda com a corrupção de uma base de dados.
Era um comportamento praticamente restrito aos profissionais da área por conta de seu profundo envolvimento com a tecnologia e pela possibilidade de enxergar as "engrenagens" dos bastidores que faziam toda a mágica funcionar. Já o usuário final, procurava no meio de tanta complexidade, encontrar aplicabilidade para os sistemas de informação, planilhas de cálculo e editores de texto, que já requeriam grande desenvoltura por conta das interfaces pobres e principalmente por conta das confusas linhas de comando e seu velho prompt C:>.

Ocorre que tudo mudou muito rapidamente. O poder de processamento dos computadores cresceu exponencialmente acompanhado de seu barateamento relativo. As interfaces de hardware se multiplicaram e diversificaram-se assim como as interfaces de software que ganharam agentes inteligentes levando praticamente o usuário no colo para ensiná-lo a colar uma imagem, gerar um vídeo e customizar sua área de trabalho.
Como fator alavancador desse desenvolvimento, surgiram rapidamente os conceitos de rede local que por sua vez, se conectaram à redes regionais e globais aumentando sobremaneira o volume de informações trocadas pelos usuários e ao mesmo tempo, reduzindo quase que na mesma proporção, o tempo de disseminação do conhecimento.

A realidade atual imposta pelo progresso é formada por múltiplos dispositivos computacionais que se conectam sem sequer requerer meio físico, trocam dados em alta velocidade através de interfaces cada vez mais amigáveis, quase automaticamente e sem intervenção humana. Por traz de toda a facilidade de uso que os fabricantes prometem e os usuários procuram, se escondem praticamente as mesmas "engrenagens" de antigamente, mas agora invisíveis e muito mais lubrificadas. E o usuário também não é mais o mesmo. O grau de penetração da tecnologia em sua vida é muito maior e mais intenso. A dependência dos sistemas de informação, dos serviços de correio eletrônico e da Internet de uma

maneira geral, é enorme, o que motivou o desenvolvimento da paranóia da segurança em todo e qualquer usuário.

A melhor maneira de comprovar esta percepção é avaliar os softwares comercializados em grande escala, em todo o lugar e para todos os perfis de usuário. Em 1987, por exemplo, Peter Norton e seu conjunto de aplicativos para manutenção de sistemas operacionais, eram conhecidíssimos, mas somente para os profissionais de TI, mesmo assim, só para aqueles mais modernos. Dez anos depois, em 1997, os firewalls eram produtos sofisticados e conhecidos especialmente pelos administradores de rede e especialistas em conectividade e segurança.
Atualmente, podemos comprar até pelos canais de compras das TVs, toda a sorte de hardware e programas de proteção para o usuário final. São antivírus que além dos vírus bloqueiam spyware, pop-up e spam. Programas que desabilitam todos os serviços não utilizados pelo usuário e protegem sua privacidade impedindo a coleta de informações pessoais em seu computador. Programas que bloqueiam a execução de agentes Java ou Active X, programas que varrem o conteúdo de seu e-mail à procura de códigos maliciosos e ainda o impedem de visualizar imagens inseridas que não tenham sido anexadas ao e-mail e representam links externos.

A realidade é mesmo dura. Os usuários estão paranóicos. As tão amigáveis interfaces já não dão tanta liberdade de movimento, bloqueando tudo antes de perguntar ou simplesmente pressupondo que aquele email de família é a ameaça mais devastadora que pode existir, colocando-o em quarentena para nunca mais ser lido. As pessoas não querem mais trocar tantas informações, pois os certificados digitais que assinam digitalmente as mensagens deixam seu cliente de email muito lento, travando-o esporadicamente. As pessoas enviam cartões eletrônicos de Natal e Aniversário fingindo que seus destinatários irão lê-los e eles, por sua vez, também fingem que o fizeram, mas todos estão com muito medo de tudo. Clicar virou uma ação de risco. Qualquer movimento provoca um alerta do firewall, do antivírus, do detector de intrusos, do sistema anti-spam ou ainda do controle de conteúdo, transferindo quase sempre o risco para o usuário, que terá de autorizar ou desautorizar aquele movimento. Os computadores descobriram o som e para tudo existe um sinal sonoro, o que torna difícil é decifrar o ocorrido. Terá sido um ataque ou foi simplesmente um sinal de bateria fraca? Sendo mesmo um ataque, terá sido bem sucedido ou mal sucedido? Estaria a base de dados de ameaças atualizada? Derrubo a conexão Internet ou permaneço atônito esperando ver os efeitos do ocorrido?

Isso é paranóia! Estamos todos pisado em ovos e envoltos por mais aplicações de segurança do que de programas de produtividade que justificam a existência de um computador sobre a mesa. É certo que a percepção dos riscos de segurança deve existir e que o comportamento dos usuários deve ser ajustado às suas sensibilidades e à importância de suas aplicações e informações, mas também é certo que deve existir um ponto de equilíbrio. Todos os dispositivos que mencionei têm uma razão de existir, afinal, as ameaças também são uma realidade, mas nem todos devem se justificar para todos e configurados da mesma maneira. Proteger é preciso, mas ter saúde para usufruir tudo que a tecnologia ainda nos reserva é prioritário.

Marcos Sêmola *é South America Security Consulting Manager da multinacional Atos Origin, Consultor Sênior em Gestão de Segurança da Informação, profissional certificado CISM – Certified Information Security Manager pelo ISACA, BS7799 Leader Auditor pelo BSI, Membro do Computer Security Institute, Professor de Segurança da Informação da FGV – Fundação Getúlio Vargas, MBA em Tecnologia Aplicada, Bacharel em Ciência da Computação, autor do livro Gestão da Segurança da Informação – uma visão executiva, Ed.Campus e eleito pelo prêmio SecMaster, Profissional de Segurança da Informação de 2003 cat4.*
marcos@semola.com.br