Em tempos de crises é necessário um

COMPORTAMENTO SAUDÁVEL EM REDE

Em sua origem, o termo hacker vem do verbo em inglês *to hack* que significa "dar golpes cortantes (para abrir caminho)" e era utilizado para os programadores que trabalhavam com tentativa e erro ao forçar a porta do CPD. Essas ações eram normalmente frutos de traquinagem, de uma geração que apenas queria mostrar do que são capazes.

Um famoso programador, Richard Stallman, conhecido mundialmente por ter criado o movimento GNU e pela licença GPL, tem uma forma muito clara, e em alguns momentos até poética, da real definição do termo hacker:

O uso da palavra hacker para se referir ao violador de segurança é uma conclusão que vem por parte dos meios de comunicação de massa. Nós, hackers, nos recusamos a reconhecer este significado, e continuamos usando a palavra para indicar alguém que ama programar e que gosta de ser hábil e engenhoso.

No entanto, infelizmente, hoje o termo hacker é muito utilizado pela mídia na maioria das vezes para referenciar não mais profissionais, mas sim para falar de indivíduos que invadem sistemas e computadores por falsas ideologias e, quase sempre, por motivações escusas. Embora existam termos mais adequados para denominar um criminoso digital, como *"crackers, insider* e *scriptkids"*, a mídia insiste em chamá-los de hackers.

Ataques como os que ocorreram no início deste ano não são novos, mas evidenciam a fragilidade, em alguns contextos, que encontramos na internet. Principalmente no que tange o lado do usuário quando vinculado a proliferação continua e automatizadas de *malware* que amplificam o poder dos invasores, possibilitando-os criar *Botnet* (coleção de agentes de *software* que executam autónomamente e/ou automaticamente) cada vez maiores.

Os primeiros ataques, de origem semelhante, aconteceram no final dos anos 80. Um dos mais famosos é o ataque do Morris Worm, um dos primeiros *worms* (tipo de *malware* que tem em sua engenharia seu vetor de propagação) distribuídos pela internet e também um dos primeiros a receber atenção da mídia. Desde então, os ataques estão cada vez mais automatizados, assim como seus objetivos. Os

A utilização deste artigo é exclusiva para fins educacionais.

ciberataques se tornaram cada vez mais direcionados e o cenário de ameaças evoluiu, incluindo dispositivos que, quando foram desenvolvidos, não eram considerados uma ameaça à segurança. Se no início era uma brincadeira de jovens, hoje virou profissão, seja legal ou não.

Embora se tenha pessoas competentes atuando na manutenção da segurança, há limite de braços para responder a demanda dos atuais problemas, somando a isso o fato de que muitas empresas ainda investem pouco ou de forma não direcionada em segurança, tanto no que diz respeito a *software, hardware* e *peopleware*. Adicionalmente, para o sistema operacional mais utilizado pelos usuários comuns surgem novos *malwares* - como vírus, *trojans* e outros - a todo o momento.

Vale lembrar que, apesar da evolução dos ataques, a multiplicação e propagação não acontecem sozinhas. É sempre necessário um intermediário. Muitas vezes, o personagem multiplicador é o próprio usuário, que não protegeu seu equipamento, mantém comportamento não seguro na rede ou, pior, não tem conhecimento do que é um antivírus e da sua utilização.

Exemplo disso é a pesquisa divulgada em fevereiro pela Symantec, que revela que São Paulo ocupa o 4º lugar de cidade considerada com maior risco em termos de ameaça cibernética na América Latina, está atrás somente de Buenos Aires (1°), San Juan-Porto Rico (2°) e Bogotá-Colômbia (3°).

Para mudar esse cenário, basta que o usuário replique em sua vida virtual as atitudes de segurança que tem em seu dia a dia, como evitar caminhos perigosos, fazer a manutenção do carro e manter um comportamento seguro.

Tudo isso parece fácil, mas o que é, na prática, manter um comportamento seguro na rede?

É simples. Não se deve clicar em qualquer arquivo que é recebido por email, ou mesmo link que leva ao download de um arquivo. Mesmo com um bom antivírus, ainda assim existem riscos que podem ser mitigados se uma cautela seletiva do que executa em seu computador é mantida, pois a possibilidade de um programa malicioso engenhoso em um primeiro momento não ser detectado por um antivírus é factível.

Sandro Melo

Professor titular da Faculdade de Tecnologia do Colégio Bandeirantes

Fonte: Ser Mais, São Paulo, ano 3, n. 31, p. 18-19, 2012.