

87 – Maio 2007

Mais Segurança com Sistema Operacional de Bolso

Programas de computador, sem exceção, possuem falhas de desenvolvimento e codificação, consideradas inerentes a sua natureza, mas algumas dessas falhas podem comprometer a estabilidade do programa ou ainda comprometer direta ou indiretamente a segurança do sistema operacional e afetar a privacidade e os dados do usuário.

Disso todos já sabemos ou ouvimos falar, por isso, o melhor a fazer é conviver com a realidade e, sempre que possível, buscar alternativas que sejam apropriadas ao seu contexto de uso do computador. Atualizações de segurança, firewall, anti-vírus, detectores de intrusos e filtros de malware são algumas alternativas mais conhecidas, contudo, à medida que a mobilidade do usuário e o tele-trabalho se tornam mundialmente uma realidade, surgem alternativas criativas e interessantes com os sistemas operacionais de bolso.

Me refiro especialmente a uma nova modalidade de operação dos sistemas Linux, em geral, chamada Live CD. Existe uma infinidade de sistemas operacionais abertos e “sabores” diferenciados de Linux, mas muitos deles, com a proposta de serem portáteis, enxutos e indolores, já podem ser transportados e executados a partir de simples mídias de CD, DVD ou até Pen Drives USB, de forma que possam entrar em funcionamento rapidamente após iniciar qualquer computador que permita o boot por CD ou USB sem interferir no ambiente de trabalho e sistema operacional originalmente instalado.

Deixando a compatibilidade e outros aspectos funcionais de lado, e focando nossa análise nos aspectos de segurança, essas variantes de Linux podem ser também muito úteis quando é preciso utilizar um computador público ou de terceiros, sem que você interfira no sistema operacional e no ambiente de trabalho originais. Entretanto, o maior benefício está na possibilidade de levar consigo o próprio ambiente de trabalho, no qual você confia e se sente seguro para realizar operações críticas como realizar uma transação no Internet Banking, enviar um email ou ainda qualquer tarefa rotineira que poderia estar em risco caso a executasse em um computador contaminado com um vírus, um trojan horse ou com qualquer outro aspecto de segurança comprometido.

Em geral, os Linux na versão Live CD cabem em um único disco, quando não, podem ser gravadas e executadas em um DVD ou em um generoso Pen Drive USB com mais de 1GB. Este último ainda permite a configuração personalizada do ambiente de trabalho e sua gravação, assim como de qualquer outro arquivo de dados, no próprio dispositivo. Costumam vir acompanhados de muitos aplicativos de código aberto para auxiliar o usuário nas mais comuns tarefas, como acessar a Internet; enviar e receber emails; assistir vídeo; editar um documento ou uma planilha eletrônica e muito mais. E antes mesmo que seu lado conservador condene completamente a iniciativa, vale lembrar que a comunidade Linux tem obtido avanços significativos em relação ao suporte de hardware e especialmente à interface gráfica, podendo entusiasmar até o mais incrédulo usuário.

Popularmente comparando, esta alternativa pode representar para o usuário de computador praticamente o mesmo que um preservativo contraceptivo representa para seu usuário ao se relacionar com múltiplos parceiros, ou seja, independente do estado de saúde do parceiro, ele carrega consigo um mecanismo que o isola do potencial risco, tornando a experiência sempre segura e saudável onde quer que ele esteja.

Infelizmente, esta descoberta não elimina completamente as ameaças e os riscos no uso do computador mesmo que você carregue um ambiente computacional conhecimento e confiável, pois como já disse, conceitualmente todo programa de computador possui falhas e nada impede que um descuido ao abrir um arquivo suspeito ou até mesmo o aparecimento de uma nova ameaça especializada em explorar falhas do seu ambiente de código aberto, não provoque um furo no seu preservativo.

Conhecido o cenário de uso, mapeados os riscos e ponderados os benefícios de possuir uma versão de bolso de um sistema operacional, só resta escolher o sabor de Linux que melhor se alinha ao seu paladar, sem esquecer que também existem ótimas distribuições Brasileiras, e adicioná-lo à bagagem.

Marcos Sêmola é Diretor de Operações de Security & Information Risk da Atos Origin em Londres, Consultor Sênior em Gestão de Segurança da Informação, certificado CISM, BS7799 Lead Auditor, Membro da ISACA, ISSA, CSI e fundador do IISP – Institute of Information Security Professionals of London. Professor da FGV, Pós Graduado em Negociação e Estratégia pela London School, MBA em Tecnologia Aplicada, Pós Graduado em Marketing e Estratégia de Negócios, Bacharel em Ciência da Computação, autor de livros sobre gestão da segurança da informação e inteligência competitiva. Premiado SecMaster® em 2003 e 2004, tornando-se membro da comissão a partir de 2005. Visite www.semola.com.br ou contate marcos@semola.com.br