

# Segurança e Linux

Prezado leitor, prezada leitora da Linux Magazine,



no final do mês de Agosto de 2004, durante uma coletiva de imprensa realizada no âmbito da 9ª Conferência Anual sobre o Futuro da TI, o grupo Gartner anunciou o resultado de uma pesquisa de opinião sobre qual área de TI de empresas no Brasil deveria receber atenção (e investimentos) em especial em 2005. Desenvolvida junto aos participantes do evento que ocupam cargos de direção, a resposta da grande maioria foi **segurança**.

Quando se fala em segurança, sistemas baseados em tecnologia de código aberto, como o Linux, são, via de regra, a escolha apropriada. Mas por que o Linux é tão seguro? Ou melhor, por que o Software Livre é, por natureza, normalmente mais seguro que suas contrapartes proprietárias? Não deveria ser o contrário? Afinal, se todo mundo pode ler o código fonte dos programas, é mais fácil encontrar as falhas que podem ser exploradas, não? A resposta a essa última pergunta é um sonoro NÃO! Muito pelo contrário: é justamente porque o código pode ser lido por milhares de desenvolvedores no mundo todo que pode ser auditado e provado em segurança por quem quer que deseje e disponha de conhecimento técnico para fazê-lo. Enquanto alguém está implementando um novo recurso, outros estão corrigindo erros nessa implementação, empresas a estão testando sob cenários de missão crítica e devolvendo “patches” (correções – literalmente, “remendos”) que tornem a execução do programa produzido menos passível de erros e mais eficiente. É, em resumo, por essa razão que o desenvolvimento de Software Livre torna essa modalidade de programas mais eficiente, rápida e segura.

Será que isso é verdade? Ou será que só se trata de retórica? Será que o Linux não é atingido por problemas de segurança com a mesma frequência que, por exemplo, o Windows®, sistema operacional da Microsoft, porque o sistema criado por Linus Torvalds ainda não está tão disseminado quanto o da empresa de Bill Gates & Co.? Afinal, segundo pesquisas, a participação do Linux no

mercado de desktops é de menos de 5%. Não haveria interesse de nenhum “cracker” em criar um vírus para Linux, ou mesmo um worm ou cavalo de Tróia, já que o sistema não seria um alvo realmente apetitoso, certo? Mais uma vez, a resposta é NÃO. O Linux, e outros sistemas de código aberto como o servidor web Apache, constituem hoje o fundamento da Internet. A maioria maciça de servidores web no mundo lá fora é baseada no quarteto de acrônimo LAMP – Linux, Apache, MySQL e PHP, todos projetos livres. Eles são alvos muito mais interessantes que o desktop do João, do José etc., uma vez que guardam informações corporativas que podem valer muito dinheiro. De outro lado, modificar o conteúdo de tais servidores é um excelente modo de se mostrar – coisas que “crackers” sempre apreciam. Aliás, tanto isso é verdade, que basta o administrador de sistemas não ficar atento e deixar de aplicar com frequência as correções de segurança que a sua distribuição Linux torna disponíveis diariamente para que os sistemas sob sua supervisão sejam atacados – infelizmente com sucesso. Há inúmeros casos em que isso ocorreu no passado.

Mas para agradar os céticos, vamos embasar nossa retórica com alguns números: na edição anterior da Linux Magazine, noticiamos que, segundo um estudo realizado desde o ano 2000 no Centro de Pesquisas em Ciência da Computação da Universidade de Stanford, o kernel 2.6 do Linux, em suas 5,6 milhões de linhas, apresentou uma taxa média de erros de implementação da ordem de 0,17 a cada 1000 linhas de código. Estudo semelhante, realizado pela Universidade Carnegie Mellon com softwares proprietários, identificou uma média variando entre 20 e 30 bugs a cada 1000 linhas, o que coloca o kernel do Linux em uma posição absolutamente vantajosa em relação à média de sistemas semelhantes, mas de código fechado, embora comparações específicas devam ser feitas caso a caso.

Para encerrar, gostaríamos de lembrar mais uma característica do Linux – na verdade do Unix – que também contribui para que tais sistemas sejam por padrão mais seguros: a sua arquitetura. No Unix, como no Linux, há uma clara separação de privilégios. Usuários são, normalmente, incapazes de instalar qualquer programa ou mesmo apagar arquivos fora do seu diretório pessoal. Para tanto, é necessário obter privilégios de administrador. Além disso, não basta um arquivo qualquer ter a extensão EXE ou COM para automaticamente ser executado com um clique do mouse. Ele precisa ter atributos especiais que digam ao sistema: “Ei, eu sou executável, mas só o usuário ‘fulano’ é que pode me executar!” Isso dificulta a vida do programador de vírus. Aliado a isso some-se a velocidade com que correções de segurança aparecem para Software Livre – em contraste com o que acontece com o software de código fechado, para o qual às vezes espera-se por meses até que uma correção apareça – e temos um cenário muito mais vantajoso de utilização, o que estimula a adoção de soluções abertas por governos, empresas e vai, inevitavelmente, acabar por chamar a atenção do usuário doméstico.

Não é à toa que o projeto OpenBSD anuncia com orgulho a ocorrência de apenas uma falha de segurança explorável remotamente na instalação padrão em mais de 8 anos! Projetos como Adamanthix (Trusted Debian) e Security-Enhanced Linux (SELinux) seguem a mesma linha. Nesta edição, você vai conhecer algumas das tecnologias de segurança disponíveis em sistemas abertos que, apesar de não serem visíveis, podem constituir a diferença entre a vida e a morte de sua estrutura de TI.

Rafael Peregrino da Silva  
Editor