Expediente editorial

Diretor Geral
Rafael Peregrino da Silva
rperegrino@linuxmagazine.com.br

Editores
Flávia Jobstraibizer
fjobs@linuxmagazine.com.br
Kemel Zaidan
kzaidan@linuxmagazine.com.br

Editora de Arte
Larissa Lima Zanini
llima@linuxmagazine.com.br

Colaboradores
Alexandre Borges, Alexandre Santos, Augusto Campos, Ben Martin, Daniel Bartholomew, David Berube, David Rupprechter, Ralf Spenneberg, Ron McCarty, Sebastian Kummer.

Tradução
Emersom Satomi, Michelle Ribeiro e Pablo Hess

Editores internacionais
Uli Bantle, Andreas Bohle, Jens-Christoph Brendel, Hans-Georg Eßer, Markus Feilner, Oliver Frommel, Marcel Hilzinger, Mathias Huber, Anika Kehrer, Kristian Kißling, Jan Kleinert, Daniel Kottmair, Thomas Leichtenstern, Jörg Luther, Nils Magnus.

Anúncios:
Rafael Peregrino da Silva (Brasil)
anuncios@linuxmagazine.com.br
Tel.: +55 (0)11 3675-2600

Penny Wilby (Reino Unido e Irlanda)
pwilby@linux-magazine.com

Amy Phalen (América do Norte)
aphalen@linuxpromagazine.com

Hubert Wiest (Outros países)
hwiest@linuxnewmedia.de

Diretor de operações
Claudio Bazzoli
cbazzoli@linuxmagazine.com.br

Na Internet:
www.linuxmagazine.com.br – Brasil
www.linux-magazin.de – Alemanha
www.linux-magazine.com – Portal Mundial
www.linuxmagazine.com.au – Austrália
www.linux-magazine.es – Espanha
www.linux-magazine.pl – Polônia
www.linux-magazine.co.uk – Reino Unido
www.linuxpromagazine.com – América do Norte

Linux Magazine é publicada mensalmente por:

Linux New Media do Brasil Editora Ltda.
Rua São Bento, 500
Conj. 802 – Sé
01010-001 – São Paulo – SP – Brasil
Tel.: +55 (0)11 3675-2600

Impressão e Acabamento: RR Donnelley
Distribuída em todo o país pela Dinap S.A.,
Distribuidora Nacional de Publicações, São Paulo.

Atendimento Assinante

www.linuxnewmedia.com.br/atendimento
São Paulo: +55 (0)11 3675-2600
Rio de Janeiro: +55 (0)21 3512 0888
Belo Horizonte: +55 (0)31 3516 1280

ISSN 1806-9428 **Impresso no Brasil**

INSTITUTO VERIFICADOR DE CIRCULAÇÃO

Atenção redobrada

"Com pista molhada, atenção redobrada. Uma pequena poça pode esconder um grande buraco."

A frase acima, veiculada em diversas estações de rádio atualmente, por mais louvável que seja o propósito que encerra – alertar motoristas para as más condições da pista – mascara um grande problema: o fato de partirmos do pressuposto de que pistas têm buracos. Enquanto que isso (infelizmente) pode ser verdade no Brasil, países de primeiro mundo previnem e dão manutenção o suficiente em suas ruas e estradas para que não haja buracos. E o que isso tem a ver com tecnologia da informação? O óbvio: para que remediar se é possível prevenir? Para que deixar buraco na rua se é factível criar um pavimento bem estruturado, e dar manutenção como manda o figurino? Traduzindo para o mundo da tecnologia: para que deixar servidores e sistemas ao sabor de vulnerabilidades, se é possível estruturar tudo de forma a não permitir que falhas de segurança sejam exploradas?

A primeira coisa a se fazer é deixar o sistema o mais "minimalista" possível, instalando somente aquilo que for imprescindível. Programas têm erros. Quanto mais programas são instalados, mais erros serão instalados também. Depois, sistemas com controle de acesso compulsório (do inglês, *Mandatory Access Control* – MAC), tais como SELinux, AppArmor ou SMACK, permitem que se defina políticas que fornecem um controle granular sobre as permissões do usuário para acessar recursos e modificar permissões. Com isso, mesmo que um aplicativo esteja comprometido por uma vulnerabilidade, não vai ser possível utilizá-lo para realizar a elevação de privilégios – técnica que usa a falha de um programa que está sendo executado com privilégios de administrador, para fornecer acesso root a um invasor. Esse programa terá seu acesso totalmente limitado àquilo que ele foi designado para fazer originalmente. A associação desse tipo de tecnologia com sistemas modernos de detecção e prevenção de intrusões (PDS/IPS, tais como o Prelude, Snort, OSSEC, AIDE, entre outros), contribuem ainda mais para dificultar a vida dos malfeitores digitais de plantão. Junte a isso o uso de sistemas virtualizados como base de todos os servidores, que dispõem assim do mesmo hardware virtual, utilizando ainda um sistema moderno de gerenciamento de correções de segurança (*patch management*), que aplicaria as mesmas atualizações de segurança a todas as máquinas virtuais – o que torna fácil a automatização e reduz a possibilidade de falhas – os sistemas ficarão (com o perdão do trocadilho) virtualmente invulneráveis. Dá até para usar um desses sistemas como *honeypot* e fechar as portas de invasão nos outros sistemas, a partir do que aprendermos com ele.

Para finalizar, a utilização de firewalls em dois níveis, de preferência utilizando tipos diferentes de sistemas operacionais (Linux e OpenBSD, por exemplo) em arquiteturas de hardware diferentes (misturando Intel, ARM, PowerPC). Agora que você já sabe o que fazer com aquele Macintosh G4 velho que estava encostado no canto juntando poeira, feche as portas de vez na cara dos invasores. Afinal, além de ter que dominar dois sistemas operacionais diferentes, será necessário descobrir quais aplicativos estão vulneráveis em cada uma das plataformas.

Agora vá dormir tranquilo. Sua pista está lisa. Pode chover à vontade. ■

Rafael Peregrino da Silva
Diretor de Redação