COLUNA

Meu servidor foi invadido: e agora?

Augusto Campos

Saiba o que fazer após desconectar a máquina da rede, antes de decidir que a formatação é a única saída.

Um dos meus livros preferidos na área de administração de sistemas é o *Linux System Administration*, que tem como um de seus co-autores Jim Dennis, que muitos fãs antigos de Linux devem conhecer como o titular por muitos anos da coluna "The Answer Guy", da *Linux Gazette*. Ele foi publicado em 2000 (com prefácio de Eric Raymond), mas consegue se manter atual por não se fixar tanto nos procedimentos da administração de sistemas, mas sim nos métodos, técnicas e mesmo na filosofia que permeia toda essa arte e ciência. Se você encontrar alguma edição à venda por um preço camarada, definitivamente vale a pena.

> *Nossa vida seria muito mais fácil se pudéssemos saber que está tudo ok sem ter de ler o email inteiro, e se pudéssemos saber rapidamente quais emails de relatório ler primeiro e quais simplesmente arquivar, certo?*

Os conselhos do livro são diretos e sólidos. Alguns itens até parecem óbvios, mas freqüentemente não são atendidos, como o conselho de que todo script de monitoramento que mande resultados por email deve colocar no campo de assunto um resumo de seu resultado, e não apenas a identificação do script, data e servidor. Nossa vida seria muito mais fácil se pudéssemos saber que está tudo ok sem ter de ler o email inteiro, e se pudéssemos saber rapidamente quais emails de relatório ler primeiro e quais simplesmente arquivar, certo?

Mas o livro tem um capítulo – extremamente curto – que cai como uma luva para o tema desta edição da Linux Magazine: o que fazer quando um servidor é invadido. Embora muito já se tenha escrito a respeito, as pessoas continuam cometendo os mesmos erros quando descobrem esse que é um dos piores pesadelos dos administradores de rede — e isso às vezes as leva a um ciclo sem fim de formatações, reinstalações e novas invasões.

O procedimento proposto leva um pouco mais de tempo, mas evita os atos impensados e os círculos viciosos. Começa por uma decisão: haverá interesse em usar o servidor invadido como prova em algum processo? Em caso positivo, não há outra forma de ação possível: você terá que colocá-lo de lado (desconectado da rede, é claro) e fazer uma nova instalação em outro equipamento, no qual retornará o backup mais recente de todos os seus dados.

Depois verifique a natureza da falha, usando inclusive um detector de rootkits. Se a invasão se limitou a contas de usuários comuns, é possível (embora raro) que baste restaurar os dados, educar o usuário cuja senha foi descoberta e ativar um monitoramento mais estrito das conexões a essa máquina no futuro próximo. Mas, se há suspeita de invasão com acesso de superusuário, de modo geral será necessária a reinstalação em um sistema de arquivos limpo, seguida de um procedimento que corrija a falha usada para a invasão (antes de recolocar o equipamento na rede). Mas antes de reinstalar, vale a pena preservar todas as informações que podem ser importantes para identificar o que houve: logs, históricos de comandos etc. Muitas vezes eles são removidos ou "limpos" pelo invasor, mas às vezes há pistas suficientes para compreender o que foi feito e de que forma. Uma dica importante é investigar também os logs de outras máquinas da mesma rede, que não tenham sido invadidas.

Mas a parte mais importante, e mais freqüentemente negligenciada, vem depois que tudo está reinstalado e funcionando: a revisão geral dos procedimentos e políticas de segurança. Se não houver pessoas habilitadas para fazer essa análise, isso é um sinal claro de problemas – e você deve considerar a idéia de procurar um profissional habilitado e de confiança. Não leve a política de segurança a se tornar um obstáculo ao trabalho dos usuários, mas, ao mesmo tempo não abra mão de procedimentos mais seguros em nome da simples conveniência: o sucesso está no equilíbrio. ■

O autor

Augusto César Campos é administrador de TI e, desde 1996, mantém o site BR-linux.org, que cobre a cena do Software Livre no Brasil e no mundo.