Responsabilidade dos provedores de hospedagem por invasão: Culpa do sistema ou do provedor?

Você mantém um site rodando sobre o motor wordpress, disponível via painel de controle em uma hospedagem qualquer. Estima-se que 19% dos sites rodem sobre WordPress. Seguiu todos os passos para o hardening, revisou http://codex.wordpress.org/pt-br:Blindando_o_WordPress e mesmo assim está encontrado problemas com injection, file include ou invasões.

Alterou a senha do blog, ftp e do banco de dados. Nada resolve. Alterou os prefixos das tabeas wp_, alterou as permissões, criou um novo usuário administrativo, removeu plugins, criou index.html em diretórios, ocultou a versão do seu CRM, tunou o .htaccess, instalou plugins de scannes de vulnerabilidades e nada…

Então, ao identificar o ip (no Bing, Ip:seu número de IP) para seu site descobre se tratar de um servidor com dezenas de sites. Um servidor compartilhado. Não há hardening de WordPress que resista a um servidor compartilhado comprometido.

Quais as medidas de segurança que o provedor está adotando para proteger seus arquivos? Em servidores compartilhados as permissões de alterações de arquivos pode ser fatal. E o pior, o provedor pode "abafar" sua vulnerabilidade, alegando que não encontrou problema algum. E o usuário, muitas vezes consumidor, se complica para provar pois não tem acesso à infra do provedor.

O grande problema é que diante de tais incidentes, o primeiro

cenário é buscar entender o que aconteceu com o provedor de hospedagem. Lamentavelmente, muitos provedores irão sempre jogar a culpa no código do cliente, nunca no servidor. Em alguns casos, simplesmente dizem que nada aconteceu, mesmo você mostrando para o helpdesk registros na tabela wp_posts cheios caracteres “estranhos” e posts não criados pelo administrador.

Sob o prisma jurídico, não há duvida que o provedor pode ser responsável, sobretudo quando alega que o problema é no seu código. É possível provar com um pentest que não é o código o problema!

O provedor, diante de um incidente, deve restaurar backup anterior a invasão e imediatamente encaminhar os logs (access) e outras informações. O backup deve envolver o banco de dados e é questionável a cobrança pela restauração de backups dos clientes.

Já se decidiu na justiça brasileira que a ausência de backup ou a corrupção do mesmo pelo cracker, pode ensejar responsabilização do provedor de hospedagem.

Mesmo o provedor tendo restabelecido o serviço, é direito do consumidor de serviços descobrir data e hora do acesso indevido, vulnerabilidade explorada e técnica utilizada. Se o provedor alega que se trata de um injection ou uma vulnerabilidade no seu código que permitiria a injeção de um shell, mas não existe nada nos logs, esta afirmação pode não corresponder à realidade, sobretudo se o incidente se repetir.

Cabe, neste caso, a atuação com uma perícia ou auditoria externa, para constatar efetivamente se a afirmação do fornecedor de hospedagem realmente procede. Com a perícia em informática, pode-se identificar, por exemplo, vulnerabilidade no servidor ou serviços desnecessários rodando, não iniciados pelo cliente, sendo o caso de responsabilização do provedor.

Em Minas Gerais, ao julgar o recurso de apelação 433.758-0

(2.0000.00.433758-0/000.), o então Tribunal de Alçada responsabilizou provedor de hospedagem em caso em que defacer invadiu site e anexou fotos pornográficas no site da vítima. Por outro lado, nos termos do inciso II, parágrafo 3o. do Art. 14 do Código de Defesa do Consumidor, o provedor poderá provar culpa exclusiva da vitima, que por exemplo, não protegia o arquivo wp-config.php, permitindo que qualquer um conhecesse a senha para acesso ao banco de dados, ou mesmo mantinha uma senha fraca para seus serviços.

Recentemente, em 2013, um provedor foi condenado por não garantir segurança ao cliente, permitindo a invasão (http://www.ebc.com.br/tecnologia/2013/08/microsoft-e-condenada-a-indenizar-consumidora-que-teve-perfil-invadido)

Outro julgado pode ser encontrado em http://www.migalhas.com.br/arquivo_artigo/art20130828-11.pdf

A controvérsia é técnica e será decidida pela justiça. Vale quem produzir a melhor prova. Mais uma vez a perícia informática é fundamental, desta vez, para o prestador de serviços de hospedagem que pretenderá demonstrar que o problema não era com sua infra.

Seja como for, recomenda-se a ambas as partes o registro de todas as telas e detalhes da invasão, bem como das conversações (suporte, chamados, helpdesk, etc.) envolvendo o incidente. A coleta de evidências dever ser ágil sim, mas sempre preceder qualquer medida para "apagar" o exploit ou arquivos plantados pelo atacante no FTP, pois serão provas em juízo. O contrato deve ser revisto, sempre, pois ele limitará, no que não for nulo ou abusivo, os direitos e deveres entre as partes, diante de um incidente.

Recomenda-se, em caso de servidor aberto ou compartilhado, mediante um ajuste com o prestador de serviços, a utilização do OSSEC (http://www.ossec.net/), que permite a análise de logs rapidamente, permitindo ainda monitorar arquivos quando

os mesmos são alterados, garantindo a possibilidade de uma resposta rápida a um incidente.

Para segurança em WordPress, por fim, recomendamos o ebook http://ithemes.com/wp-content/uploads/downloads/2013/12/WordPress-Security-ebook.pdf