Blogueiros correm riscos com falta de segurança em provedores de conteúdo

Você ou sua empresa certamente utilizam algum serviço nas nuvens para divulgar informações? Muitas empresas adotam os blogs como canais de interação com o cliente e os instalam no mesmo *host* onde está hospedado o site corporativo. Pois saiba que esta pode ser a porta de entrada para um ataque de imensas proporções em seus sites.

No WordPress por exemplo, falhas de segurança são notificadas a cada semana e quanto mais *plugins* se tem no blog, maior deve ser a atenção para com falhas que os explorem especificamente. Temos falhas publicadas desde uma simples manutenção de *html*, que pode gerar o *"defacing"* do blog ou a delação de posts a falhas que permitem a exploração por *"spam link injection"* principalmente em códigos *wp_footer() e wp_head()* , onde o criminoso utilizará o servidor da vítima para aplicar outros golpes.

Plugins são recursos adicionais que são instalados no blog para fazê-lo possuir novas funcionalidades. Realmente, eles deixam um blog com a interface de portal profissional, mas é preciso cuidado, pois muitos *softwares* em fase beta ainda não passaram pela revisão da segurança de Código.

Não bastassem as falhas de segurança dos *plugins*, outro risco passa a integrar a lista de cuidados de empresas e usuários que acessam ou visitam Blogs: o risco de plugins invasivos. Selecionamos "plugins" do bem e do "mal" existentes no mundo WordPress para alertar nossos leitores.

Imagine se você instalasse um plugin em seu Blog e todos os usuários que o acessassem passassem a ser monitorados? Pois é, isto já uma realidade com o recurso *"WordPress Massup Plugin"*. Segundo o criador, é possível ao titular do blog rastrear seus visitantes em tempo real e garante ainda que podemos saber "quase tudo sobre o que nossos usuários estão fazendo". O plugin já vem com um Spy feito em Ajax parecido com o Digg Spy.

Assim, basta um usuário desavisado navegar no seu Blog, para que o espião lhe passe a rastrear, coletando diversas informações como localização geográfica, ip de conexão, palavras buscadas, sistema operacional e browser, dentre outras informações.

Já se pode imaginar os problemas legais que o uso desta ferramenta poderá trazer nos blogs, considerando que existe nítida invasão de privacidade. O próprio WordPress.org, embora liste o plugin em seu toolkit, deixa claro que ele pode ser considerado ilegal e que não se responsabiliza pela utilização.

Em contrapartida, temos inúmeros plugins que reforçam a segurança dos Blogs e que devem ser implementados por profissionais de segurança, onde citamos o *"HTML Purified"* , que filtra a linguagem WordPress *html* para *html* puro, impedindo a execução de ataques XSS e o *"Chap Secure Login"*, que permite que seu login no site seja criptografado.

Mas, dois plugins de segurança merecem total atenção, o *"WP Secruity Scam"*, que varre os arquivo em busca de vulnerabilidades e já sugere as correções, realizando inúmeros testes de vulnerabilidade, e o *"Secure WordPress"*, que faz procedimentos básicos mas úteis como por exemplo adicionar um

“index.html” no diretório de plugins, impedido que terceiros o acesse.

Como se vê, temos inúmeras proteções para quem mantém ou administra um blog, mas, e para usuários que os acessam? Tem-se um vácuo. Está na hora de pensarmos em plugins para browers que evitem invasão de privacidade e violação de outros direitos digitais.

Seja como for, somente implemente os plugins de segurança neste citados em seu site se realmente conhecer tecnicamente os mesmos, do contrário, poderá ter problemas ainda maiores. Ainda, melhor que conhecer plugins que realizam tarefas, é desenvolver o seu próprio e confiável código, razão pela qual sugiro um link sobre “Wordpress Hardening” ou “Blindagem de WordPress” onde é possível descobrir as técnicas para aprimorar a segurança de blogs, cada vez mais comuns na vida de pessoas e empresas.

E para as empresas, fica a questão: Você já auditou o código do seu Blog hoje?

Date Created
03/10/2009