CITADEL
INFORMATION GROUP, INC.

Can You Prevent Hackers from Taking Over Websites? Web-Site Security Basics.

I was recently asked if I had any methods to "prevent hackers" from taking over websites.

Alas. I don't. No one does and it's doubtful that we will ever have methods to "prevent hackers from taking over websites" any more than we could develop methods to "prevent car thieves from stealing cars."

But, just like protecting our cars, we can protect our websites, we can make it harder for the hackers, we can improve the odds.

Here are four "basic rules" for protecting your website. They are every bit as fundamental as (i) turn off your engine, (ii) take the keys, (iii) lock the doors. They should be considered the minimum necessary for any website.

Rule 1. Follow security configuration guidelines for WordPress, Drupal or whatever content management system you're using. Do the same for the plug-ins. And make sure the company hosting your web site has configured their server(s) following security configuration guidelines.

Rule 2. Keep your content management system updated. Install patches and new versions when they're released. Make sure the company hosting your web site is doing the same for the server(s) on which your web site is located.

Rule 3. Always use very strong passwords for direct access to your website and the server(s) it's located on. In today's world, "strong" means at least 15 alpha-numeric characters, including lower case, upper case, numbers and special characters.

Rule 4. Always keep a back-up of your web site. Store this off-line, on a computer that you always have access to.

You'll want to do more than this if your website is at all "sensitive." If your website is used for eCommerce, for example. Or you have a special section of your site where you exchange information with customers or where employees can access their 401(k), or your web site server connects with corporate servers where other sensitive information is present; in these circumstances the basics are definitely no longer adequate.

In these more sensitive situations you, first, need to make sure your web site conforms to whatever specific security requirements applies to it. For eCommerce, this means conforming with the Payment Card Industry's Data Security Standard.

Second, you also want to make sure the web site is developed in accordance with a "Secure Systems Development Life-Cycle" methodology. A good starting point is the excellent work being done by the Open Web Application Security Project (OWASP), particularly their Top-10 Project. No sensitive web site should be put into production without, at the very least, testing it against the current OWASP Top-10 list.

www.citadel-information.com
2060 Hercules Drive
Los Angeles, CA 90046
Tel: 323.876.1441
Fax: 323.876.7794

Reprinted from our blog: www.Citadel-information.com/blog

© Copyright 2012. Citadel Information Group, Inc. All Rights Reserved.