Commoditized Software Requires Protection

Don MacVittie, 2010-13-10

"Don't worry about doing the business taxes, my cousin Vinnie is taking care of it." Is not the type of statement that inspires confidence.

But you're doing it every day. Or at least some of you are.

Picture this: A small vertical market, most of them using a variety of hosting services, all see their web stores hacked in a six or eight week period.

Investigation shows that nearly all of them shared a single piece of software, and nearly all of them used that software on a hosted platform. To make matters worse, as a vertical it was easy to get Google listings of them, and they often linked to each other right on their sites.

The problem is simple, and one you've thought of in terms of specific bits of software but not in terms of commodity software as a whole. For example, you are no doubt taking extra precautions when utilizing Microsoft SharePoint, because it is a highly complex web application that has many attack vectors built into its basic function (as do most CMS systems, this isn't a Microsoft problem, it's a "complex, prepackaged software" issue – SharePoint is just one of a class of applications that present a broad attack front). But protecting a single application only does the job if you are certain the others are beyond attack. And you can't be, if they are publicly exposed.

With millions of sites on the web and literally thousands in most vertical industries, attackers are starting to look to verticals that are not so well protected and attack software specific to that vertical. Not a ton yet, but it is starting to happen.

Cousin Vinnie

If you deploy in-house, a Web Application Firewall like our BIG-IP ASM can help protect them – it could with a hosted service too, provided your hosted service offers a Web Application Firewall as an optional add-on. For those whose hosting provider don't offer a Web App Firewall, old-fashioned web security may be your only option. Of course, if you don't have access to the source code of the application, that's going to be tough. As I mention below, it is possible to do some architectural wizardry to protect your off-site web applications with a Web Application Firewall, but I've not thought that one out clearly, so I'll just mention it until I have time to research further.

That leaves you counting on your hosting provider – be they Saas, Cloud, or straight up web hosting – to protect your application. I'd get assurances baked into the contract. Once a vulnerability is discovered in a piece of software – as we've seen with larger commodity software like OS's, Joomla, Mambo, and a host of others – it will be exploited, and finding your vertical and the application that most of your vertical uses may be all a ne'er-do-well needs to start a campaign against a vertical market's software.

In the case above – I didn't recognize it for what it was, a commoditized software hack until it was over, so I'm missing some critical data and will only talk of it vaguely here because of that – the site owners had a business to run, most of them small businesses, and they trusted their hosting providers to take care of security. The question must be asked if the hosting providers took reasonable precautions, and I guess I'd have to say yes, since there were several, in several countries, that were attacked in a short time-period. But the site owners still had downtime that they felt they could ill afford. Best to understand how this will go before hand rather than end up in an acrimonious relationship because you didn't plan for a successful attack. For example, even if they're responsible for maintaining a Web Application Firewall, how often is it updated? Is the update automatic or does their staff have to do it? These things can matter at the speed of attacks these days.

One thing you can do is provide your hosting service with your security requirements – the same ones you use internally – and tell them you expect them to meet those requirements. There are some architecture hoops you can jump through to protect a remote web app with a Web Application Firewall in your datacenter too, which I suppose is where more and more people will end up as time goes on. I'll research that topic for a future blog, if one of my co-workers hasn't already done all the work. If they have I'll point you at it in a follow-up blog.

The more commoditized web applications get – how many shopping carts, content management systems, and web portal applications does the market need – the more this becomes a problem. It makes sense to hand off applications that are not critical to the business to a third party that specializes in them so that your IT staff can focus on what IS critical to the business, but make sure you don't forget security along the way. For most enterprises that choose hosting, security will be shared between the hosting provider and enterprise IT. Make sure you know where that line in the sand is, and what you're responsible for. Make sure you have a system in place to validate that your provider is doing their part of the security, and if at all possible, put a Web Application Firewall in front of the application, because the protection they offer is better than going without, by a long shot.


F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com