PCI DSS Deadline Looming Large While Debate Continues - WAF vs VA

Lori MacVittie, 2008-14-05

According to a recent ComputerWorld article, most retailers aren't ready for the forthcoming June deadline for PCI DSS compliance.

> From ComputerWorld :: Few expected to make June 30 PCI deadline for Web application security
> Most retailers will not meet the June 30 deadline for complying with new Payment Card Industry Data Security Standard (PCI-DSS) requirements for securing web applications. Companies can achieve compliance with either a specialized firewall or web application software code review, which entails finding vulnerabilities and fixing them. **Many retailers appear to be opting for firewalls, which are "quick fixes," according to Gartner analyst Aviva Litan**. "Application firewalls are a reactive measure. You have a lot of vulnerable applications that still need to be fixed," she added, and noted that scanning for vulnerabilities and fixing them should take precedence over firewalls, and that firewalls should be used in addition to scanning, not instead of it.

PCI DSS affects retailers more than any other business owing to their acceptance of credit cards online for purchases.

The quote in question references section 6.6, a somewhat controversial requirement that allows for vulnerability scans and code review or the implementation of a web application firewall as a means of meeting compliance.

There are several good reasons for implementing a web application firewall aside from meeting PCI DSS compliance. I agree with Aviva's assessment that both vulnerability scanning *and* web application firewalls together are a good idea, but disagree that firewalls are simply reactive measures and "quick fixes". This perception seems to assume that we're looking at the problem from the viewpoint of a new application, not one that is running in production *right now.*

Web application firewalls are your first line of defense against new and existing web application threats. They are generally capable of preventing even emerging attacks, and are quickly updated when new threats are discovered. Those deployed in conjunction with or on an extensible application delivery platform provide additional value in the capability to dynamically create policies to address emerging threats or custom threats against your application.

They can CYA (cover your apps) while you find and fix the vulnerabilities, a process that requires development, testing, and redeployment. And while you're going through that process - what's going on with your application? Have you taken it offline because it's vulnerable? Were you aware of the specific attack vector when you developed the application?

No, you probably haven't, especially not if you're in the retail business because if your application is down then you are losing revenue and that's not acceptable. And no, you probably weren't aware of that attack when the app was developed because it hadn't been discovered yet.

But if you've got a web application firewall (WAF) you are likely able to continue running your application, secure in the knowledge that the WAF is going to be able to thwart a wide variety of known attacks while you scan, find, and fix the vulnerabilities in your application whether those are emerging threats or existing ones.

Deploying a WAF doesn't make an organization short-sighted or imply that they aren't going to address any vulnerabilities found in their applications. On the contrary, it implies that an organization is ***realistic;*** that it understands that no matter how many vulnerabilities their application is secure against today that a new one ***is*** going to appear. Maybe not tomorrow or next week or even next month, but it will appear. And they know their application is not likely to be protected against that brand new attack, neither will they likely be able to address that new attack fast enough to protect their application. They know that a WAF, however, is likely to updated very quickly, or at least have the means by which a fix can be put into place while they go about updating their application.

Deploying a WAF isn't reactive, it is proactive defense against existing and future threats. It isn't replacing the security sought through vulnerability scanning, it's augmenting and enabling that process while protecting the business' investment in its web presence. That's risk management and proactive security.

Imbibing: Coffee

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

F5 Networks, Inc.	F5 Networks	F5 Networks Ltd.	F5 Networks
Corporate Headquarters	Asia-Pacific	Europe/Middle-East/Africa	Japan K.K.
info@f5.com	apacinfo@f5.com	emeainfo@f5.com	f5j-info@f5.com