Yelling ‘WebApp Firewall’ in a Crowded Data Center

Peter Silva, 2009-19-08

You've probably seen the statistics: As of January 2009, almost 90% of the 100 to 150 million Websites are still critically vulnerable to attack according to SearchSecurity. And Web Application Security Consortium (WASC) reports that 87% of Websites are vulnerable to attack. Reports also indicate that 400+ new vulnerabilities a month are found (and growing) along with the fact that malware on legitimate Websites has doubled in 6 months. WhiteHat Security notes that at least 70% of the websites it scans has at least one critical vulnerability and another 63% have flaws that need attention with Social Networking sites the most vulnerable.

Some additional stats:

Every 1000 lines of code averages 15 critical security defects. (U.S. Department of Defense)

The average security defect takes 75 minutes to diagnose and 6 hours to fix. (5-year Pentagon Study)

The average custom business application has 150,000 to 250,000 lines of code. (Software Magazine)

Average worldwide cost of programmer = $40 per hour (WorldSalaries.org)

Thus, to diagnose defects:

- 15*1.25hrs*150/40 = 70 weeks.
- $40 x 40 hrs. = $1600/week.
- 70 weeks x $1600 = (potentially) $112K per app.
- *WAF = Mitigate now & diagnose when time permits*

And to fix defects:

- 15*6hrs*150/40 = 338 weeks.
- $40 x 40 hrs. = $1600/week.
- 338 weeks x $1600 = (potentially) $540K per app.
- *WAF = Mitigate now & fix when time permits*

There are the numbers, need I say more? But of course, I will. Just installing a Web Application Firewall doesn't mean you are instantly protected. There are WAF solutions that have wizards, templates and pre-built policies to help the administrator enable some baseline protection. BIG-IP Application Security Manager even has Application Ready security policies pre-built for popular applications like OWA, Oracle, PeopleSoft, SharePoint and others. Select the policy and you are on your way. Even after creating your policy, whether it be from scratch, a template, live traffic and so forth, you still need to test it, in a transparent non-blocking mode to make sure no false-positives appear and legitimate visitors are able to use the application. When you are comfortable with the level of protection along with usability, then enable blocking mode.

The challenges can continue. Often IT staff, particularly network gurus (no offense, to those reading this) are not familiar with application security and Layer 7 focused attacks, let alone the intricacies of the back end applications. There will probably need to be some coordination/collaboration amongst the network, security and application experts. Blur the lines between the Compliance minded who look at WAF as an audit pass and the Security minded who really want to stop attacks. Right now, compliance (especially PCI) is the main driver of the WAF market. There can also be some hesitancy in placing a WAF in front of web applications due to the fear of effecting their performance.

Speaking of PCI, we're now seeing WAF integration with application scanning technologies. For PCI 6.6, this merging brings both the WAF requirement AND the code review requirement together as a combined solution. Scan the code with the analysis tool to find vulnerabilities and create/adjust the WAF policy to address them. Best of both worlds as the cliché goes.

Managed WAFs are gaining some traction as many merchants do not have the expertise in house to understand either the types of attacks or ways to protect against them. There is also an emerging 'WAF in the Cloud' trend. It's probably still a little early for mass adoption since Security in the Cloud is such a moving target and companies are wary of putting sensitive data in the cloud. The same data that's bound to regulatory compliance. The real barrier for WAF in the Cloud is performance and bandwidth since that traffic might have to make a few passes back and forth. It eventually will happen (cloud coattails) but with smaller organizations initially.

A couple years back, WAFs were considered new technology. With PCI and many of the highly publicized security breaches, they became a necessity. Today, you need to look at a Web Application Firewall as an essential part of the application lifecycle.

ps

#6 out of 26 Short Topics about Security

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

©2016 F5 Networks, Inc. All rights reserved. F5, F5 Networks, and the F5 logo are trademarks of F5 Networks, Inc. in the U.S. and in certain other countries. Other F5 trademarks are identified at f5.com. Any other products, services, or company names referenced herein may be trademarks of their respective owners with no endorsement or affiliation, express or implied, claimed by F5. CS04-00015 0113