Web application firewalls – Laying the myths to rest

A review of how businesses are reconsidering long-standing beliefs about web application firewalls

January 2014
CONTENTS

Executive summary p3
Introduction p3
Application layer security landscape p4
Why the WAF? p6
Technical performance of WAFs p7
Business perceptions of WAFs p8
Limit your exposure p8
WAFs and the cloud p9
Conclusion p11
About the sponsor, Riverbed p12
Web application firewalls – Laying the myths to rest

Executive summary

Ever-increasing customer expectations, and the need to deliver richer web applications (apps), means that the challenge of securing applications becomes more complex every year. Consequently, web apps have become a popular attack vector in recent years. Components of the traditional security infrastructure – network firewall, intrusion detection systems (IDS) or intrusion prevention systems (IPS), content security, etc. have proven ineffective in preventing these attacks.

What was needed was the ability to examine all inbound/outbound web traffic at the application level. The web application firewall (WAF) market has grown strongly in recent years, driven by the regulatory environment and the huge growth in the volume of attacks against web apps.

However, WAFs are sometimes viewed as complicated and only partially effective in preventing the kind of attack that they exist to prevent. Computing surveyed 100 IT decision makers to establish their views on how their WAF deployments have performed and thus to see whether the negative beliefs that some organisations still hold about WAFs are justified today. The paper also looks at how organisations are getting the best out of their WAFs and optimising their investment.

Introduction

As web apps are deployed and utilised in ever increasing numbers so they have become an increasingly popular attack vector. Such has been the rush to build and deliver web apps that code security has been sacrificed in varying degrees for operational efficiency, and attackers have ruthlessly exploited any weaknesses.

The automated hacking tools available so freely on the internet have increased exponentially the scale and volume of attacks. This is why the huge volume of web app attacks such as SQL injections and cross-site scripting (XSS) that really took off in 2008 shows no sign of slowing up. SQL injection attacks in particular have been ongoing for years now yet they are still brutally effective.

The prizes are bigger than ever for criminals attacking the vulnerabilities in web app code – the petabytes of valuable data such as credit card details, shopping habits and other financial data. The threat landscape has become increasingly targeted in the last eighteen months, with industries holding high value information, such as finance and retail, the focus of cyber-criminals’ activities. Attacks are now often multi-layered such as those targeting the US banking system earlier this year. These attacks began with massive scale network level attacks by means of DDoS. These were followed up months later with attacks on the applications which control electronic money transfers.

The security infrastructure that many businesses deployed five years ago is simply not up to the job of securing web apps. Traditional network firewalls are effective (or should be) in preventing network level attacks such as DDoS but lack the ability to examine application specific protocols such as HTTP and XML. Even next generation firewalls are ill suited to protecting the application layer. Another problem occurring at the same time for many businesses was the need to demonstrate compliance with government and industry regulations on data control – in particular the Payment Card Industry Data Security Standard (PCI DSS).
This combination of circumstances has led to many business organisations adding a WAF appliance, software or service to their security infrastructure. The WAF market has grown steadily in the last five years and analysts have predicted a growth of 18.34 percent for the global WAF market for the period 2012-2016. However, many organisations are still unconvinced of the need for a WAF or are concerned about the complications that they believe they may cause.

Application layer security landscape

The first big surprise of our survey was how few of our respondents had a WAF in place. Only 48 percent of those surveyed stated that they did so, with approximately 32 percent not having one in place and 20 percent being unsure. This is a worrying finding. The implications for organisations of compromised web apps can be severe – Facebook, Apple and Twitter have all found themselves explaining why confidential data has been compromised this year. Even if adverse publicity can be contained, the cost of detecting and remediying a breach can be enormous. A recent study placed the cost of a data security breach at $136 per record. This can include the loss of existing business, the impact on future business acquisition and the cost of compensating affected customers.

The cost of a breach can also include a hefty fine from a regulatory body. Regulatory regimes differ globally but few countries have no data security controls in place be they industry or legislative requirements. All members of the EU are subject to the Data Protection Directive of 1995 which regulates the processing of personal data. The Data Protection Act 1998 is a UK law that was enacted to comply with the EU directive. This law is enforced by the Information Commissioners Office with every organization processing personal data required by law to register with the ICO. The ICO has already exercised its ability to fine organisations failing to comply with data protection laws. In theory, fines up to £500,000 can be levied and whilst the public sector has been the main target of fines to date, the private sector is catching up.

Outside of the EU, the picture varies, but the vast majority of countries still have specific data protection laws in place. Hong Kong for example has a Personal Data Ordinance enforced by the Office of the Privacy Commissioner for Personal Data and Canada also has an Office of the Privacy Commissioner to enforce its own data protection laws. One of the few countries not to have a statutory body in place for data privacy is the United States. The US has been slower to recognise data privacy concerns than other countries and this remains a source of tension between the US and Europe (exacerbated by recent revelations by Edward Snowden.) Guidelines have been issued by the Government on card data but any legislation is industry specific with the preference being to encourage industries to regulate themselves. The Gramm-Leach-Bliley Act for example requires financial institutions to safeguard sensitive data.

Wherever you are in the world, the need to protect customer data is paramount. The low levels of WAF deployment found by our survey are therefore surprising. These businesses could have been deterred by some of the problems that occurred with earlier WAF deployments such as high false positive rates and levels of threat detection lower than expected. There is also a management overhead associated with WAFs that some organisations do not like the look of. These reasons will be discussed in more detail when this paper looks at existing WAF deployments. In the meantime, Computing asked those organisations who did not have a WAF in place which other web security measures they had in place. Respondents could choose as many answers as applied (Fig. 1).

1 http://www.researchandmarkets.com/research/vq9j7g/global_web
2 http://www.ponemon.org/news-2/23
Fig. 1: If you don’t have a WAF please state what other web application security measures you have in place

- Premise based web content security: 47%
- Intrusion prevention system: 40%
- We don’t have specific application layer security in place: 26%
- Secure coding products/services: 14%
- Cloud web content security: 9%
- Other / don’t know: 14%

*Question answered by those without a WAF; respondents could select multiple answers.

Again, the standout finding from this question was that slightly more than one quarter of respondents to this question simply did not have application layer security in place. This is a surprising and downright alarming finding given nearly a decade of publicity about application layer attacks.

The largest proportion of those responding (47%) stated that they had a premise-based web security appliance/software in place and nine percent had the same web content security product but as a cloud service. Forty percent had an IPS. Fourteen percent had opted to secure their code properly with a specific secure coding product.

Each of the approaches set out above are components of a mature web security infrastructure but none can or should be used in isolation. Web content security can certainly prevent content from dubious websites being downloaded by employees (provided that they have been categorised correctly and that category blocked accordingly) and can stop sites with embedded malware being visited so this certainly does reduce risk to a significant degree.

However, content security is just part of the picture – effectively it secures websites external to the organisation, not the organisations’ own web apps. Secure coding is another part of security strategy which integrates secure coding techniques into the application development lifecycle. However, it is legacy apps that are often a weak link in security strategy simply because they are old and less likely to have been securely coded in the first place. Remedying this after the fact is usually not cost effective yet many users claim such apps are mission critical.

Intrusion prevention systems are used by some organisations as, effectively, a WAF. However, this either/or thinking is not a component of best practice security. An IPS will block traffic that it deems threatening but this is based on signature identification and sometimes, anomaly testing.
Web application firewalls – Laying the myths to rest

This makes IPS vulnerable to zero-day attacks and also the identification of false positives. It also means that if an attack happens frequently enough it might well cease to become an anomaly. These drawbacks can be mitigated to some degree by combining with other tools and filters but an IPS’s inability to understand the business logic of web applications makes it insufficient as a standalone device.

Furthermore, whilst both IPS and WAFs can both provide effective protection against application layer attacks, neither are effective on their own with just baseline tuning. Ultimately the effectiveness of both solutions depends on how they are deployed.

Why the WAF?

In order to establish whether organisations are making the most of their WAFs it is first necessary to understand why they bought them in the first place. We have discussed the growth of the WAF market – what has been driving it? A large majority (62%) of those responding to this question gave us a resounding answer – regulatory compliance. Compliance with data security regulations such as PCI DSS have been a huge driver of the WAF market. In order to become compliant with PCI DSS organisations have to demonstrate the security of apps processing card data. Many business looked at the cost of securely coding the app and the cost of a WAF and plumped for the latter.

Forty-six percent also stated that their vulnerability to application layer attacks had enabled them to present a compelling business case for a WAF and an honest 23 percent told us that penetration testing had alerted them to some serious vulnerabilities in their web apps. Eighteen percent of respondents stated that there was simply no other cost effective way of securing legacy apps.

The reasons that businesses put WAFs in place are important because they show us what organisations expect to gain from them. The next logical step is to look at whether or not those expectations have been fulfilled.

Technical performance of WAFs

As we touched on earlier, some of the concerns that businesses have about WAFs are that they slow things down, break important applications, stop legitimate web traffic and generally get in the way. These concerns were based on product versions now nearly a decade old. Our survey has told us that these concerns are, in the majority of cases, no longer founded. Computing asked, “Are you happy with the way that your WAF has performed technically?” The results are shown in Fig. 2 on page 7 and are generally positive.

Thirty-seven percent described themselves as “completely happy,” with their WAFs. A further 55 percent described themselves as “reasonably happy,” with some niggles such as false positives being tuned over a period of time. Fewer than eight percent of respondents described themselves as unhappy with the management overhead and operational issues overshadowing threat protection.

The technical performance of existing WAFs was analysed further with the question, “Do you consider your WAF effective?” Again, a significant majority (58%) stated that they did. However, 37 percent told us that whilst their WAF had proven reasonably effective, penetration testing had managed to evade it.
This is not wholly surprising. The fact that penetration testers are sometimes able to evade WAFs has contributed to the perception among some businesses that benefits of WAFs do not justify the costs. However, the fact that skilled pen testers are sometimes able to get around a WAF is often due to the configuration of the WAF itself rather than weaknesses inherent in the technology. WAF evasion is a real black art and techniques evolve continually.

You may not be able to make it impossible to evade a WAF but you can make it hard enough to deter all but the most sophisticated, targeted attack. As we have established, many WAFs exist because of compliance requirements, they may not have been secured properly and/or kept up to date. Compliance and security are most definitely not the same thing. The fact that a very honest five percent of respondents stated that they did not have the necessary skills or time to devote to ongoing tuning gives some indication of the resources required to optimise investment in a WAF.

The issue of ongoing management was probed again with the question, “Would you say that your WAF rule base has been kept up to date, including older rules being consolidated when no longer required? In keeping with the survey so far, approximately 74 percent of respondents said that the rule base was up to date.

This is a key finding. Because many WAFs were purchased with a compliance mandate in mind, they were deployed with “out of the box,” policies and then left, updated purely via vendor push outs or updated sporadically with new rules without consolidation of existing ones. This has had two main effects. The first is that newer threats can come around or through the WAF. The second is that legitimate traffic down is slowed down as the rules pile up. Both will contribute to some very negative perceptions of WAFs.
Web application firewalls – Laying the myths to rest

Business perceptions of WAFs

As we have seen, there are a number of reasons why a business may view WAFs negatively from an operational point of view. However, these adverse perceptions were not held by many respondents to our survey, indicating perhaps that many Computing readers reside some way up the WAF maturity curve.

A huge 71 percent stated that the business as a whole was happy with their WAF performance. Only slightly fewer than 11 percent of respondents stated that this was not the case. Reasons cited were false positives, high management overhead, an underestimation of the skills required to effectively manage the device and issues with the effectiveness of the WAF is blocking threats. These issues underline the message that a WAF is for life – not just for compliance. Underestimating these requirements will seriously limit how much businesses will gain from a WAF.

Limit your exposure

Having established respondents’ views around the management and performance of WAFs, our survey now turns to the apps themselves. Computing asked which of our respondents apps were covered by their WAF. As would perhaps be expected, 51 percent covered external, customer facing apps, slightly fewer (43%) email, calendar and IM collaboration apps and (37%) covered internal business operations apps.

A full breakdown of results is shown in Figure 3 on page 9, but tellingly, only 27 percent of respondents chose the “all of the above,” option. The fact is that choosing to leave apps such as business intelligence (BI) or finance/human resources/legal apps open as some of our respondents have done, creates a way for a skilled attacker to access that organisation’s data assets. It is also an interesting finding that it is these sorts of apps that tend to be unprotected. Part of the calculation for establishing the, “attack surface” of an application is the value of the data used in the app. BI and finance apps are going to be full of business critical data. Leaving them out of a WAF deployment seems risky.

However, it is understandable to a certain extent. If organisations have hundreds of apps as some do, writing and maintaining individual rules would require man hours disproportionate to the risks posed from vulnerabilities in web apps in the first place. Prioritising apps is a logical approach. Again, compliance mandates only that apps processing credit card data are secure – apps for internal use only simply do not fall into the remit.

Computing asked those who did not specify that “all of the above,” were covered why this was the case. The two most popular reasons given were related. The first was that there were too few users of the app to make it worthwhile and the second was simply too much cost thus no business case. Whilst prioritising apps is a logical approach if you have huge numbers of apps, ideally a WAF should cover all apps – both public and private.
Fig. 3: Please indicate what is protected by your WAF

- **External, customer facing apps**: 51%
- **Email, calendar, IM collaboration apps**: 43%
- **Internal business operations apps**: 38%
- **IT management systems**: 27%
- **Finance/Legal/HR apps**: 22%
- **Outsourced applications**: 16%
- **Cloud apps**: 16%
- **Business intelligence apps**: 11%
- **All of the above**: 27%
- **Don’t know**: 5%

*Respondents could select multiple answers.

**WAFs and the cloud**

Hybrid apps are also now part of the equation. Over the last three years, applications have grown in size and are increasingly being moved from physical hardware to virtual machines. Businesses are connecting apps hosted in data centres and linking them to others in the private cloud. There are third party elements in all of these deployments and bespoke coding. Some is on physical hardware (e.g. Oracle) some is on third party dedicated hosted hardware, some is in the public cloud. All of this must be secured. More apps are also being built on web services. Whether the agility of the web app environment has been reflected in security practices is debatable.

*Computing* asked “To what extent does your organisation place infrastructure in the cloud?
The picture was mixed. The largest proportion of respondents (35%) had a true hybrid environment including IaaS and SaaS. Only slightly fewer (32%) used some SaaS but only on a small scale. A further 11 percent were working towards greater use of the cloud. Only 22 percent of respondents remained wedded to an on-premise infrastructure with no plans to utilise cloud services at all.
Web application firewalls – Laying the myths to rest

The fact that approximately two thirds of respondents were using the cloud to deliver infrastructure services underlines its importance. However, some (possibly earlier) WAF deployments have not kept pace with changing infrastructure. Whilst 73 percent of respondents were happy that their WAF could deploy with virtual as well as physical apps, 27 percent however stated that it had not kept pace. This will either hamper innovation by impeding the delivery of new applications and/or increase their vulnerability to an application layer attack.

A best practice WAF deployment will protect all applications – physical, virtual and hybrid. This can be achieved by means of an on-premise deployment and also a WAF delivered as a cloud service. A cloud service WAF may be suitable for smaller organisations who may not have the resource or in-house skills necessary for running a high-availability deployment.

However, a WAF delivered as a cloud service cannot be closely integrated with the application itself, and can potentially be bypassed if attackers can target the application directly. Hence there is a third model – virtual/software-based WAF solutions - which combines the advantages of closer application integration and lower latency, and the ability to scale on-demand, by being deployed in the cloud adjacent to the application itself.

Both types of cloud models provide a degree of resiliency that is impossible to replicate with point solutions, and can be instantly scaled in the event of a massive attack.

Organisations are also increasingly developing apps in the cloud using services such as AWS. In this instance, WAFs and application optimisation software can be purchased by the hour in a true, pay-as-you-go format with no prohibitive, up-front licensing costs.

Some early WAFs have not kept pace with the changing ways that businesses deliver web apps, but many have, and businesses can now choose from several ways of protecting their web apps from layer 7 attacks.
**Conclusion**

Web apps have become a popular, lucrative attack vector yet traditional network firewalls do not have the ability to actually look inside web traffic – hence the huge volume of successful SQL injection and cross-site scripting attacks in recent years. Even though these types of attack have been around for some years they are still carried out successfully with relentless regularity. Web application firewalls can examine web application protocols and hence block attacks on the application layer. This has led to wide deployment of WAFs, yet many organisations (around one half of our respondents) remain unconvinced.

Early WAFs were hampered by a high rate of false positives and a level of threat detection which did not justify the problems generated by the blocking of legitimate traffic. This may have led many organisations to conclude that they weren’t worth the trouble and that a network firewall, IPS and decent web content security would suffice. Whilst all of these are components of a mature and well layered security infrastructure, the missing link is an ability to look at web traffic specifically in depth. Only a WAF can deliver this.

Many of the WAF deployments were put in place by companies keen to demonstrate their compliance with government and industry regulations – PCI DSS in particular. This has led to some WAFs not being managed and tuned properly as organisations deployed them, displayed their compliance credentials, and then paid insufficient management attention to them until problems occurred. Respondents to our survey have dispelled the myth that WAFs are difficult to manage and/or ineffective with over 90 percent stating that they were happy with the technical performance of their WAF.

However, despite a majority of respondents being happy with their WAFs, a significant number were not protecting all of their web apps. Prioritising external, customer facing apps is an understandable approach to protecting hundreds of apps but choosing not to cover apps only used by small numbers of people such as BI or finance apps is a risky path. These are the apps containing some of the most valuable data an organisation will possess and are the kind of apps likely to be the focus of a targeted attack.

Web apps are also being deployed on virtual as well as physical machines – or both. A best practice WAF deployment will protect all applications – physical, virtual and hybrid. Early WAFs have not kept pace with the growth in virtual and hybrid apps but the majority of our respondents stated that their WAFs were very much up to the job.

This paper has conclusively laid to rest some of the myths about WAFs and shown how businesses are optimising their investment in protecting their ever evolving web apps.
About the sponsor, Riverbed

Riverbed® is the leader in Application Performance Infrastructure, delivering the most complete platform for Location-Independent Computing.™ Location-Independent Computing turns location and distance into a competitive advantage by allowing IT to have the flexibility to host applications and data in the most optimal locations while ensuring applications perform as expected, data is always available when needed, and performance issues are detected and fixed before end users notice. Riverbed’s 24,000+ customers include 97 percent of the Fortune 100 and 95 percent of the Forbes Global 100.

For more information:
Visit: www.riverbed.com