Cyber Security Coursework - Essay

James Donohue - james.donohue@bbc.co.uk

Contents

1 Introduction

The paper to be evaluated is Web Application Firewalls: Enterprise Techniques by Jason Pubal (2015), as published in the SANS Institute Reading Room.

2 Executive Summary of Paper

The domain of the paper is the use of Web Application Firewalls (WAFs) to monitor web application traffic for the purpose of detecting or preventing malicious activity. WAFs are a relatively new category (Scarfone and Hoffman 2009) of security product specifically designed to apply various rule sets to

HTTP/HTTPS traffic, including those designed to prevent common web application vulnerabilities such as SQL injection or cross-site scripting (XSS) (Conklin et al. 2016).

The paper reports an increase in the prevalence of web applications and attacks against them, and says that organisations can manage risks around Internet-facing web applications by using a WAF both to block malicious traffic and perform 'virtual patching' when a new vulnerability is discovered. The author contrasts WAFs with 'traditional' network intrusion and prevention systems (IDS/IPS), which he says are less able to prevent such attacks. WAFs work by inspecting HTTP requests and responses and comparing them to attack 'signatures', either blocking such attacks or raising alerts. He describes 'positive' and 'negative' security models, analogous to the possible *default policy* of a packet filtering firewall described by Stallings and Brown (2015). The author suggests that negative security models are easier to set up and have a lower maintenance burden than those using positive models, but may offer lower protection.

Various approaches to deploying a WAF in a network environment are described. In a 'Reverse Proxy' configuration the WAF sits inline between a web server and the network's external firewall (what Scarfone and Hoffman (2009) call the *ingress point*), proxying inbound requests to the server, while a 'Layer 2 Bridge' WAF is also inline but operates at a lower network layer, blocking traffic as required by simply dropping packets. An 'Out-of-Band' WAF is not inline but receives a copy of network traffic which it monitors passively, interrupting malicious connections where possible. The 'Server Resident' configuration means that WAF software is installed on the web server itself, while 'Internet Hosted/Cloud' deployments rely on software as a service (SaaS) from a third-party cloud provider, with the WAF conceptually inline.

In the next section the author covers the main motivations behind the use of WAFs in organisations. The benefit given for 'production' applications, even those developed using a secure software development lifecycle (SDLC) is that the cost of rectifying security issues in live production applications is reduced. This is shown as particularly relevant to legacy applications developed in house and commercial off-the-shelf (COTS) software, where the organisation's ability to fix underlying code may be restricted due to loss of development skills or lack of vendor cooperation. The author situates this approach as part of a vulnerability management process, specifically the need to 'shield' a vulnerable application from attacks while the affected code is fixed or updated. The accuracy of a WAF is said to increase if it can import results from a dynamic application security testing (DAST) tool.

Another motivation given for WAF adoption is compliance, such as with the Payment Card Industry Data Security Standard (2016) for handling payment card information. This standard's requirement to review web applications using vulnerability assessment tools after any changes, and the high fines for which organisations are liable, make WAFs an attractive alternative route to compliance. Next the paper describes the role of WAFs as sensors within a larger intrusion detection system (IDS). Data from a WAF can be sent to an organisation's security incident and event management (SIEM) system for correlation with other data, which the author says expands such a system's ability to detect attacks on the organisation's web properties. A brief depiction of major WAF vendors at the time of writing is then given.

The rest of the paper describes a lab environment created by the author to demonstrate how a WAF can be used to support virtual patching and security monitoring. Using the 'server-resident' model, the open-source ModSecurity WAF is installed on the same Linux virtual machine as an application designed to exhibit common security vulnerabilities, Damn Vulnerable Web App (DVWA). The OWASP Core Rule Set (CRS) is imported into ModSecurity, while on a separate virtual server the log management tool AuditConsole is installed to illustrate the handling of audit logs. Lastly a Windows host running a DAST tool called Burp Suite is deployed, and another tool, ThreadFix, that aggregates re-

sults from various security testing tools including Burp Suite and uses them to generate WAF rules that ModSecurity can import.

The author discusses virtual patching in more detail, illustrating it with the example of a (deliberate) XSS vulnerability in DVWA. DAST tools identify such web vulnerabilities by recursively checking pages in the application. Burp Suite is used to test DVWA and identifies the XSS vulnerability above. The Burp Suite results for DVWA, including the XSS vulnerability, are imported into ThreadFix, which generates ModSecurity rules. After deployment, the XSS vulnerability is manually re-tested and is blocked by the WAF. The author states that it may not always be possible to remediate vulnerabilities entirely using virtual patching and it should be viewed as temporary risk reduction.

The author describes how a Network Security Monitoring (NSM) shifts the goal to detecting and reacting appropriately to (inevitable) security incidents. The phases are broken down into collection, in which sensors (including WAFs) collect data, detection, in which alerts are generated, and analysis, when a human interprets the alerts and takes any action. The author states that the importance of WAF NSM sensors depends on how critical web applications are to the organisation. He demonstrates using ModSecurity as an NSM sensor sending logs and alert data to the AuditConsole management tool.

In conclusion, the author re-emphasises the importance of web applications today and mentions again the particular value of WAFs in shielding vulnerable legacy/COTS web applications. He suggests that WAFs have visibility into application traffic that no other monitoring tool is capable of. Finally, he points out the specialist skill set required for application security monitoring as opposed to 'general' network monitoring, and recommends that suitable training is provided.

3 Organisational impact of topic for BBC News

The first security management question to answer is what the organisation wants to protect (Stallings and Brown 2015). BBC News receives 28m monthly unique visitors in the UK alone (DCMS 2016) and has a 30% share of Britain's market for online news (The Guardian 2016), making it a valuable asset.

3.1 Threat characteristics

Several classes of intruder might consider the BBC website an appealing target. Although it does not process financial information, the organisation's current drive to serve more personalised content (BBC 2016) entails gathering more user data, which could attract cyber criminals focused on identity theft. Because of its reputation as a trustworthy news source, BBC News could be targeted by 'hacktivist' groups motivated by a political cause (Stallings and Brown 2015). Most concerning of all are highly-skilled Advanced Persistent Threats (APTs) backed by foreign governments, which are reported to be increasingly targeting the UK (Independent 2016). The Verizon 2016 Data Breach Investigations Report (2016), which Pubal also cites, shows that public or government targets were the largest victims of cyber espionage breaches. BBC web infrastructure has suffered numerous distributed denial-of-service (DDoS) attacks over recent years, some of which have caused major outages (BBC 2015).

Also important is the rise in web applications as an attack vector. The ENISA Threat Landscape report (2016) lists web application attacks as the third-most significant threat, with a 15% yearly increase, while the Verizon report (2016) shows that web application attacks are growing across almost all industries, suggesting one reason for this is that web applications may be the only route in to sensitive data in storage. This indicates that web application attacks are particularly in need of attention.

3.2 Transition to cloud computing and DevOps

Recently the BBC has started migrating some of its online services from a centrally-managed application stack running on co-located server hardware to a heterogeneous cloud-based model in which products (such as News) provision their own cloud hosting. This will enable a significant reduction in data centre costs, however the transitional 'hybrid' cloud model results in an increased network attack surface (shown in Figure 1).

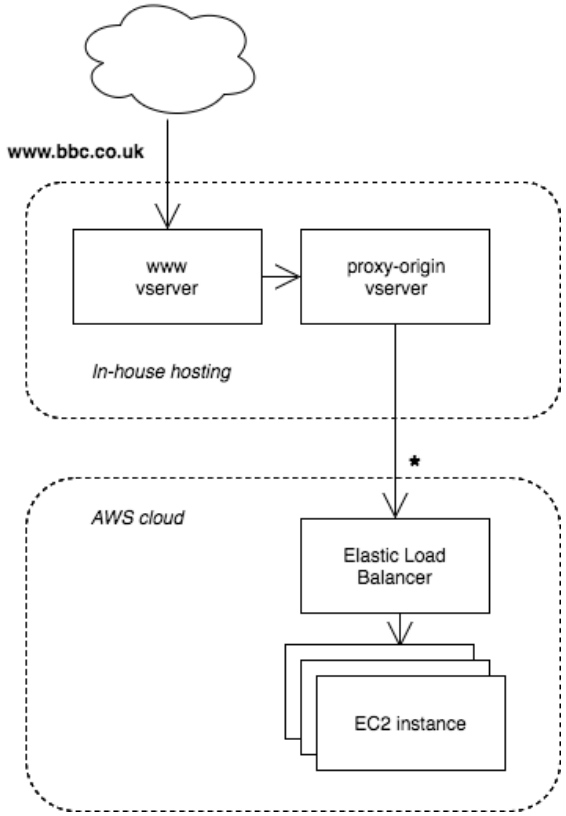

Figure 1: BBC hybrid cloud architecture (most vulnerable point marked with an asterisk)

With the move to the cloud, the development of online services at the BBC is embracing a 'DevOps' philosophy based around continuous delivery (Daniels and Davis 2016). Where in the past developers wrote software that was then handed over to a specialised operations team for deployment, these traditional operational siloes are changing, with responsibility for deployments being shared. Developers therefore need understanding of the production environment, including operating system and networks, and therefore of the information security challenges unique to these areas.

3.3 Stakeholder attitudes and responses

In order to conduct an informal risk analysis for BBC News (and recognising the limitations of such an approach) it is useful to identify key stakeholders, that is, groups that may be concerned about or affected by the topic.

End users – UK audiences perceive the BBC website as the most trustworthy, accurate and impartial source of news (DCMS 2016). Any threat action that compromises the data integrity of BBC News (for example, through deception arising from *falsification* (Shirey 2007) of news reports), will have an impact on public perceptions and therefore support for the BBC. End users also have an expectation of *availability*, i.e. that BBC News services are available when they want them.

Web application developers – These should be aware of the most critical web application weaknesses, such as the OWASP Top 10 (2013), and mitigate them when writing code. Developers are increasingly expected to have a broader range of 'DevOps' skills, but may lack confidence in some areas. They have a unique understanding of application internals and are able to specify, for example, valid input patterns. They may wish to learn more about using WAFs to supplement protections in application code.

Network administrators – They are aware of the security benefits of WAFs over lower-level packet filtering. However they may be concerned about the processing overhead of inspecting higher-level protocols and the potential impact on network throughput (Cheswick et al. 2003). They may have concerns about adding to an already complex set of controls - i.e. another set of ingress rules to be understood and maintained. They may be particularly interested in using WAFs to perform 'virtual patching' on vulnerable systems.

Information Security officers – As Maiwald and Sieglein (2002) point out, the role of the Information Security department is not to guarantee security, but to help the organisation manage risks. Given the BBC's constrained level of funding, these staff would want to evaluate the potential opportunities and costs of using WAFs in the context of the organisation's overall risk appetite. They would be involved in issuing any policy or plan around use of WAFs.

Note: The BBC is currently regulated by the BBC Trust, which sets high-level policies for the running of the organisation, including the way that 'key operating risks' must be reported (BBC Trust 2015). Information security policies need to consider this supervisory framework, corresponding to the *legislation* policy management layer identified by Hare (2001).

Senior management – Managers at the BBC see the benefit of continuous delivery in getting new features into production faster. They are also most aware of the potential consequences of any harm to the BBC's reputation caused by a loss of service availability or data integrity. They are keen to reduce hosting costs by driving cloud migration but do not want to increase the organisation's risk exposure to unacceptable levels. They are likely to have a general understanding of the idea of a 'firewall' but not the specific characteristics or benefits of WAFs.

Table 1 gives an excerpt from a risk register (Stallings and Brown 2015) for this context.

Table 1: Risk register of WAF-related threats for BBC News

Asset	Threat/ Vulnerability	Exiting Controls	Likelihood	Consequence	Level of Risk	Priority
News website	Content modified or defaced	Policies	Possible	Major	High	1
News website	Site unavailable or slow	Policies, CDNs	Possible	Moderate	High	2

4 Example security plan

If the BBC wishes to implement a security plan around the above, it should first identify controls that could help to reduce each risk to acceptable levels (NIST 2013). These controls can be broadly classified as management, operational or technical (Stallings and Brown 2015). Table 2 shows some examples.

Table 2: Controls for risk 'Content modified or defaced'

Control	Class	Instance of (NIST 2013)
Vulnerability scan cloud origin servers	Management	RA-5 Vulnerability Scanning
Detect and block attacks using a WAF	Operational, Technical	SI-3 Malicious Code Protection, SC-7 Boundary Protection
Ensure all input validated in application code	Operational	SI-10 Information Input Validation

Cost-benefit analysis suggests that implementing a WAF control may reduce the likelihood and severity of web application attacks with relatively low costs. The appropriate security policy layer is 'standard', since it will include "mandatory activities, actions, rules or regulations" (Hare 2001, p 19). The target audience for the BBC WAF standard will be technical architects, web application developers and network administrators. The likely proponent of the standard would be the BBC information security function (Howard 2002).

An outline WAF standard is given below with some of the key information it should include.

4.1 Purpose

The purpose of this standard is to increase the security of BBC web services hosted in the cloud by requiring all new applications to include a Web Application Firewall (WAF) into their proposed architecture.

4.2 Background

(Refer to threat landscape description in previous section.)

4.3 Scope

This standard applies to all new public cloud-hosted web applications regardless of domain, cloud provider (AWS, Google, etc.) or product (e.g. News, iPlayer). It does not apply to web applications for internal use, or to applications deployed within private cloud platforms, or existing live applications.

4.4 Policy

In addition to complying with existing BBC policies [link] around common web application weaknesses (e.g. OWASP Top 10, CWE/SANS Top 25), it is mandatory for cloud-hosted web applications to be pro-

tected against common attacks through the deployment of a WAF or equivalent component.

This standard does not specify the use of a specific WAF product or architecture. However, the following mandatory requirements must be observed:

- The WAF should be 'inline' at all times
- All traffic through the WAF should be logged for auditing purposes
- Products must assess WAF options using the Web Application Firewall Evaluation Criteria 1.0 (WASC/OWASP 2015)

4.5 Compliance

The information security department is responsible for ensuring compliance with this standard and may request evidence from product teams that their WAF is in place and operational, and perform periodic vulnerability scans to verify WAF capabilities.

Non-compliance with this standard will be handled through the BBC disciplinary procedure [link].

4.6 Relevant dates

This standard is effective from DD/MM/YYYY. It is due for review after two years, on DD/MM/YYYY.

Other features removed for brevity here but that may be useful in a standard are a glossary, references, a change log (SANS Institute 2014), and contact details for the author/and or authorising officer (Hare 2001).

5 Evaluation of paper

The main strength of the paper is its detailed proof-of-concept using a WAF within an enterprise by integrating it with other tools into a vulnerability scanning and 'virtual patching' workflow. By using the ModSecurity OWASP Core Rule Set (CRS) as initial input, the approach used validates the capabilities of WAFs to detect and mitigate vulnerabilities found in the OWASP Top 10 (2013), which is referenced by standards such as the PCI DSS (2016) as an example of best practice in vulnerability management. This therefore suggests that WAFs could form part of a 'baseline approach' to implementing generic, industry-standard security controls against common threats (Stallings and Brown 2015). However, the author does not reflect on the relative complexity of the model used and the challenges in integrating and managing so many separate components, or contrast it with simpler deployment options such as unified threat management (UTM) products (Stallings and Brown 2015).

5.1 Terminology and classification of controls

Pubal states that WAFs can prevent attacks that "network firewalls and intrusion prevention systems cannot" (p.3), but these terms are used flexibly in vendor marketing and there is often overlap between the capabilities of each system. WAFs can be seen as a specialised type of application gateway, one of the three categories of firewall (along with packet filters and circuit gateways) identified by Cheswick et al. (2003), but as they point out, the protocol levels analysed by each category is not clear-cut. More recently, Scarfone and Hoffman (2009) use a broad application of the term 'firewall' and more precisely

compare their capabilities by determining which level(s) of the TCP/IP stack the firewall is able to operate on.

Even within the application layer, it may be helpful to distinguish between WAF functionality focused on the HTTP protocol itself and that protecting against weaknesses in web application code. The data sheet for one market-leading WAF (Imperva 2015) shows it "enforces HTTP standards compliance". This is a firewall behaviour termed 'RFC compliance' (Scarfone and Hoffman 2009) which protects against weaknesses in the protocol implementation (for example, a 'cookie' that does not conform to the standard could be used as an attack against an insecure HTTP parser). By contrast, guidelines such as the OWASP Top 10 normally focus on weaknesses web application that are built on top of HTTP.

Additionally, the 'out-of-band' configuration described in the paper does not strictly fulfil the requirement for a firewall that all traffic must past through it (Cheswick et al. 2003).

5.2 Other benefits of WAF controls

Pubal identifies a number of important reasons to consider WAF controls, including detecting and blocking malicious traffic, 'virtual patching' of legacy/COTS software, and their role within a broader network security monitoring infrastructure. However he only briefly mentions their ability to assist with the creation of security audit trails (Shirey 2007). Cheswick et al. (Cheswick et al. 2003) list the ability to log and control all traffic passing through them as a key advantage of the application gateway category of firewall. Scarfone and Hoffman (2009) also suggest that application-layer firewalls are able to provide provide user-oriented services such as enforcing authentication or logging events associated with a system user. For example, a suitably-configured WAF could be used to audit failed login attempts for a given user account, which is listed as a security event that should be audited by standards such as X.816 (ITU 1999). This could be especially useful where a legacy/COTS web application does not provide its own security audit trail. Some high-end commercial WAF products such as BIG-IP (2016) even include 'stateful' rules that can automatically detect and block brute-force login attacks by inspecting application traffic, going well beyond the feature set of the example WAF (ModSecurity) discussed in the paper.

The paper focuses on using WAFs for 'shielding' applications in production that have identified weaknesses, without considering the role they have to play in managing web application risk more generally. Implementing multiple, overlapping layers of security is the well-established principle of *defence in depth*, and as Stallings and Brown (2015) point out may address people and operational concerns as well as technology. In the case of the BBC, the need to educate and support web developers in developing more secure applications and for a robust InfoSec review of possible weaknesses does not preclude adding WAFs as a supplementary layer of protection.

Similarly, the inclusion of centralised WAF protection at the edge of the BBC network, through which all traffic would pass (currently under consideration) does not mean that origin servers should not also include WAF components. The use of multiple layers of firewalls is a common way of providing defence in depth (Scarfone and Hoffman 2009), and where different firewall products or configurations are used the software attack surface may be reduced even further. Moreover, the reduced amount of traffic reaching origin servers (due to centralised caching) makes it more practical to apply types of application layer inspection that are more costly in terms of processing time (such as the 'stateful' rules described above) at this level. By contrast the large volume of requests hitting the edge of the network could make such rules cost-prohibitive, application gateways being "poorly suited to high-bandwidth or real-time applications" (Scarfone and Hoffman 2009, pp. 2–6).

5.3 Downsides and arguments against WAF usage

WAFs add additional level of complexity to the organisation's infrastructure and increase the maintenance burden on network administrators. As Scarfone and Hoffman (2009) point out, having multiple layers of firewalls make debugging problems more difficult, since potentially multiple sets of logs have to be checked. This problem is made worse in WAFs, since each layer may modify the HTTP messages, and if the WAF is stateful (for example, applies rules based on a sequence of requests) it becomes even more challenging.

There is also the related argument that many of the protections afforded by WAFs (for example, against XSS) are most appropriately enforced in web application code itself, where set of possible valid inputs can be known with certainty and the risk of false positives (where legitimate user behaviour is incorrectly identified as malicious) is therefore lowest. At the higher level, the downside of blocking repeated login attempts at the WAF level is that if the WAF is ever bypassed all protection is lost. Protection may also be weakened if a WAF is replaced with an alternate product that employs different heuristics. Web developers typically mitigate such risks using a test-driven development (TDD) approach which makes it easier to catch regressions (Beck 2002), but this methodology is not yet widely supported for validating WAF behaviour.

Stemming from the above is the human issue that using WAFs could give application developers a false sense of security, believing that they can postpone or limit protections against common weaknesses because a WAF is inline. Again, should the WAF be bypassed by an attacker, or accidentally disabled, this leave the application unprotected.

A third area which presents challenges for WAF adoption at the BBC is the increasing pressure to encrypt all web traffic using SSL/TLS. Google is one of the main advocates for this trend, tracking SSL adoption across top sites (Google 2017). By definition WAFs must be able to decrypt such connections in order to inspect the contents, which means that web server SSL certificate(s) must be installed on the WAF system (known as SSL 'offloading'), increasing the complexity of managing certificates across the organisation and encouraging vendor lock-in due to the different approaches handling HTTPS between WAF implementations. Pubal only mentions HTTPS decryption to say that WAFs are more likely to handle it than IPSes.

5.4 Implications for cyber security and scope for future work

In the time since the paper was written, organisations such as the BBC have accelerated their transition to cloud hosting. In late 2015 Amazon Web Services (AWS) launched their own Web Application Firewall product (AWS 2017) which has lowered the barriers to adoption through a simple setup process and a pay-as-you-go pricing model (per-rule and per-request). Pubal does refer to a cloud software-as-a-service (SaaS) deployment option for WAFs but does not evaluate them in detail. It would be interesting to explore the suggestion made by Pfleeger et al. (2015) that one danger of cloud infrastructure is the cloud provider becoming a single point of failure.

The concepts of configuration management and infrastructure automation applied to cloud computing have recently come to be closely associated with DevOps (Daniels and Davis 2016). Most cloud providers allow architects and developers to define their infrastructure requirements as code, which can be managed and audited through a version control system (VCS). The ability to define WAF rule sets as part of this infrastructure creates an opportunity for web application code to be packaged along with a firewall rule set tailored to the application by its developers, for automated deployment. This

follows Maiwald and Sieglein's idea (2002) of security "working within the developers' world" and could also be a fruitful area for further research.

References

AWS, 2017. *AWS WAF - Web Application Firewall* [online]. Available from: https://aws.amazon.com/waf/ [Accessed 25 Feb 2017].

BBC, 2015. *Web attack knocks BBC websites offline* [online]. Available from: http://www.bbc.co.uk/news/technology-35204915 [Accessed 18 Feb 2017].

BBC, 2016. *BBC unveils next stage to make a more personal BBC for everyone* [online]. Available from: http://www.bbc.co.uk/mediacentre/latestnews/2016/a-more-personal-bbc-for-everyone [Accessed 18 Feb 2017].

BBC Trust, 2015. *BBC protocol: Trust oversight of the BBC* [online]. Available from: http://downloads.bbc.co.uk/bbctrust/assets/files/pdf/regulatory_framework/protocols/2015/e1_trust_oversight.pdf [Accessed 19 Feb 2017].

Beck, K., 2002. *Test Driven Development: By Example*. Fourth edition. Boston, MA: Addison-Wesley.

BIG-IP, 2016. *BIG-IP Application Security Manager: Datasheet* [online]. Available from: BIG-IP Application Security Manager [Accessed 25 Feb 2017].

Cheswick, W. R., Bellovin, S. M., and Rubin, A. D., 2003. *Firewalls and Internet Security: Repelling the Wily Hacker*. Second edition. Boston, MA: Addison-Wesley.

Conklin, W. A., White, G., Williams, D., Davis, R., and Cothren, C., 2016. *Principles of Computer Security*. Fourth edition. McGraw-Hill.

Daniels, K. and Davis, J., 2016. *Effective DevOps*. O'Reilly Media.

DCMS, 2016. *BBC television, radio and online services: An assessment of market impact and distinctiveness* [online]. Available from: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/504012/FINAL_-_BBC_market_impact_assessment.pdf [Accessed 18 Feb 2017].

ENISA, 2016. *ENISA Threat Landscape Report 2016* [online]. Available from: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016 [Accessed 18 Feb 2017].

Google, 2017. *HTTPS on Top Sites* [online]. Available from: https://www.google.com/transparencyreport/https/grid/ [Accessed 25 Feb 2017].

Hare, C., 2001. *Information Security Policies, Procedures, and Standards: Establishing an Essential Code of Conduct* [online]. Revision 4. Available from: http://www.ittoday.info/AIMS/DSM/82-10-85.pdf [Accessed 24 Feb 2017].

Howard, P. D., 2002. *The Security Policy Life Cycle: Functions and Responsibilities* [online]. Available from: http://www.ittoday.info/AIMS/DSM/82-01-06.pdf [Accessed 24 Feb 2017].

Imperva, 2015. *Imperva SecureSphere Web Application Firewall: Datasheet* [online]. Available from: https://www.imperva.com/docs/ds_securesphere_web_application_firewall.pdf [Accessed 25 Feb 2017].

Independent, 2016. *Russian hackers pose increasing threat to UK's national security, GCHQ chief warns* [online]. Available from: http://www.independent.co.uk/news/uk/home-news/

russian-hackers-target-uk-claims-gchq-government-cyber-security-chief-fake-news-a7576646.html [Accessed 18 Feb 2017].

ITU, 1999. *X.816 : Information technology - Open Systems Interconnection - Security frameworks for open systems: Security audit and alarms framework* [online]. Available from: https://www.itu.int/rec/T-REC-X.816-199511-I/en [Accessed 25 Feb 2017].

Maiwald, E. and Sieglein, W., 2002. *Security Planning and Disaster Recovery*. Berkley, CA: McGraw-Hill.

NIST, 2013. *NIST Special Publication 800-53: Security and Privacy Controls for Federal Information Systems and Organizations* [online]. Revision 4. Available from: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf [Accessed 23 Feb 2017].

OWASP, 2013. *The Open Web Application Security Project Top 10 -2013* [online]. Available from: https://www.owasp.org/images/f/f8/OWASP_Top_10_-_2013.pdf [Accessed 19 Feb 2017].

PCI, 2016. *Payment Card Industry (PCI) Data Security Standard, v3.2* [online]. Available from: https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2.pdf [Accessed 24 Feb 2017].

Pfleeger, C. P., Pfleeger, S. L., and Margulies, J., 2015. *Security in Computing*. Fifth edition. Upper Saddle River, NJ: Prentice Hall.

Pubal, J., 2015. *Web Application Firewalls: Enterprise Techniques* [online]. Available from: https://uk.sans.org/reading-room/whitepapers/application/web-application-firewalls-35817 [Accessed 5 Feb 2017].

SANS Institute, 2014. *Information Security Policy Templates* [online]. Available from: https://www.sans.org/security-resources/policies [Accessed 24 Feb 2017].

Scarfone, K. and Hoffman, P., 2009. *NIST Special Publication 800-41: Guidelines on Firewalls and Firewall Policy* [online]. Revision 1. Available from: http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=901083 [Accessed 23 Feb 2017].

Shirey, R., 2007. *RFC4949: Internet Security Glossary, Version 2* [online]. Available from: https://tools.ietf.org/html/rfc4949 [Accessed 19 Feb 2017].

Stallings, W. and Brown, L., 2015. *Computer Security: Principles and Practice*. Third edition; Global edition. Harlow, Essex: Pearson.

The Guardian, 2016. *BBC websites dominate the market in online news views* [online]. Available from: https://www.theguardian.com/media/greenslade/2016/feb/09/bbc-websites-dominate-the-market-in-online-news-views [Accessed 18 Feb 2017].

Verizon, 2016. *2016 Data Breach Investigations Report* [online]. Available from: http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/ [Accessed 18 Feb 2017].

WASC/OWASP, 2015. *Web Application Firewall Evaluation Criteria* [online]. Available from: http://projects.webappsec.org/w/page/13246985/Web%20Application%20Firewall%20Evaluation%20Criteria [Accessed 25 Feb 2017].