Technology in general is a world of its own that will never stand still, so too are security technologies continuously evolving. Two security technologies namely packet filtering firewalls as well as Web Application Firewalls (WAF’s) were discussed in an Initial Post by the writer. Packet filtering firewalls are still being used in organisations today and in some cases tightly integrated with network devices (Melanson, 2014), despite its inability to store state information or inspect the payload of a packet (Andress, 2014). WAF’s also play a vital role in protecting organisations publicly accessible assets, a view agreed by Callaghan (2021), Mundy (2021) and Onyeemeosi (2021).

Clincy and Shahriar (2018) suggests that the benefits of WAF’s certainly outweigh the disadvantages, making WAF’s paramount in protecting internet facing applications of the 21st century. Gieger (2021) highlights the importance of WAF’s and their types of detection i.e., blacklist and whitelist as well as contrasting each of them, a perspective the writer appreciates and agrees with.

In contrast, Chan (2021) mentions that WAF’s cannot offer protection to all layer 7 type attacks referencing the use case of blind-SQL injection. According to Dhiraj (2019) blind-SQL injection attacks can bypass a WAF’s regular expression, a viewpoint the writer agrees with. This is supported by Dorai and Kannan (2011) who believe that writing secure code is one way of preventing SQL injection attacks.

Biljon (2021) recommends that access to WAF’s should be integrated with Active Directory Federation Services (ADFS) as well as Multifactor Authentication (MFA) making it difficult for attackers to brute force, an excellent suggestion the writer agrees with. Furthermore, organisations should strive to implement these integrations in an automated way sooner rather than later.

Implementing security technologies in organisations has become imperative to protect network and information assets. A holistic approach should be considered when implementing security technologies which include mandatory security training and awareness i.e., a branch of the human factor in cybersecurity.

List of References

Andress, J. (2014). *The Basics of Information Security, Understanding the Fundamentals of InfoSec in Theory and Practice*. 2nd ed. Massachusetts: Syngress Publishing. Available from: https://doi.org/10.1016/C2013-0-18642-4 [Accessed 30 September 2021]

Biljon, V, E. (2021). ’Collaborative Learning Discussion 2’. Peer response submitted to University of Essex Online for [LCYS\_PCOM7E August 2021] Initial Post by Zihaad Khan. Available from: https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=275575 [Accessed 30 September 2021].

Callaghan, J. (2021). ’Collaborative Learning Discussion 2’. Peer response submitted to University of Essex Online for [LCYS\_PCOM7E August 2021] Initial Post by Zihaad Khan. Available from: https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=275575 [Accessed 30 September 2021].

Chan, Y. (2021). ’Collaborative Learning Discussion 2’. Peer response submitted to University of Essex Online for [LCYS\_PCOM7E August 2021] Initial Post by Zihaad Khan. Available from: https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=275575 [Accessed 30 September 2021].

Dhiraj, M. (2019) SQL Injection Bypassing WAF. *OWASP*. Available from: https://owasp.org/www-community/attacks/SQL\_Injection\_Bypassing\_WAF [Accessed 30 September 2021].

Dorai, R. & Kannan, V. (2011) SQL injection-database attack revolution and prevention. *Journal of International Commercial Law and Technology* 6(4): 224-231. Available from: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.994.1257&rep=rep1&type=pdf [Accessed 01 October 2021]

Gieger, M. (2021). ’Collaborative Learning Discussion 2’. Peer response submitted to University of Essex Online for [LCYS\_PCOM7E August 2021] Initial Post by Zihaad Khan. Available from: https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=275575 [Accessed 30 September 2021].

Melanson, T J. (2014) Firewall Evolution from Packet Filter to Next Generation. Available from: https://www.juniper.net/documentation/en\_US/learn-about/LA\_FIrewallEvolution.pdf [Accessed 30 September 2021]

Mundy, A. (2021). ’Collaborative Learning Discussion 2’. Peer response submitted to University of Essex Online for [LCYS\_PCOM7E August 2021] Initial Post by Zihaad Khan. Available from: https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=275575 [Accessed 30 September 2021].

Onyeemeosi, K. (2021). ’Collaborative Learning Discussion 2’. Peer response submitted to University of Essex Online for [LCYS\_PCOM7E August 2021] Initial Post by Zihaad Khan. Available from: https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=275575 [Accessed 30 September 2021].

Clincy, A & Shahriar, H. (2018) ‘Web Application Firewall: Network Security Models and Configuration’,*42nd Annual Computer Software and Applications Conference (COMPSAC)*. Tokyo, 23-27 July 2018. USA: IEEE. Available from: https://ieeexplore.ieee.org/document/8377769 [Accessed 01 October 2021]