Collaborative Discussion 2 – Peer Response 2 – Zihaad Khan

Thank you Zihaad for your post. As a supplement to the Web Application Firewall (WAF), the WAF work on two different types of detection, blacklisted or whitelisted.

The blacklist detection works with a list of known attack types. If any HTTP request is blacklisted, the WAF will block the request. The blacklist model therefore works with the approach that every request that is not on the blacklist is accepted. It only detects known generic web application attacks and saves the IP addresses and user accounts (Takahashi et al., 2011). A major problem for blacklist WAF systems are zero days attacks, as the newly discovered security gaps are not anchored in the blacklist and can therefore be exploited until they are implemented in the blacklist.

In contrast to this is the whitelisted WAF model. In this model, the WAF only allows requests that are noted in the whitelist to pass. In addition to a much greater protection against zero days attacks, as well as the lack of known generic web application attacks in the list, the disadvantage here is the effort involved in implementation (Auxilia & Tamilselvan, 2010). Since only whitelisted requests are allowed to pass, every authorized access must be noted in the whitelist. This means a lot of effort for the first implementation of this model of WAF.

References:

Auxilia, M. and Tamilselvan, D. (2010) "Anomaly detection using negative security model in web application," *2010 International Conference on Computer Information Systems and Industrial Management Applications (CISIM)*, pp. 481-486, doi: 10.1109/CISIM.2010.5643461.

Takahashi, H., Ahmad, H. F. and Mori, K. (2011) "Application for Autonomous Decentralized Multi Layer Cache System to Web Application Firewall," 2011 Tenth International Symposium on Autonomous Decentralized Systems, pp. 113-120, doi: 10.1109/ISADS.2011.20.