Great information Zihaad on using Web Application Firewalls (WAF). With attacks happening all the time on various applications such as Microsoft Exchange, Microsoft SQL, Web Application servers and other applications that are exposed to the internet, companies should look at putting a Web Application Firewall (WAF) in front of these applications with proper authentication such as Active Directory Federation Services (ADFS) (Microsoft, 2017), that will not allow an attacker to just gain access by brute force because the authentication method can be linked to user accounts that are using multifactor. An example of this is Barracuda Web Application Firewall (Barracuda, 2016)

A good example of this is F5 (F5, 2021) and having used and supported this product for several years and currently still support it, you will be amazed at what attacks it can block and it gives you the ability to blacklist IP addresses if you see them coming through on the monitoring systems. F5 is not just designed for use with just 1 application like Microsoft Exchange. You can create different partitions with different rules and public IP’s, locking down your environment further.

While no product is 100% fool proof, F5 recently announced attacks (F5, 2021) on their appliances with one of the severities listed as 9.9 also known as a

Common Vulnerabilities and Exposures (CVE) (Redhat, 2020) which means that companies using the equipment where this vulnerability was identified need to upgrade immediately to avoid any attacks.

References

F5. (2021) What is a Web Application Firewall (WAF)?. Available from:<https://www.f5.com/services/resources/glossary/web-application-firewall> [Accessed 25 September 2021].

F5. (2021) K50974556: Overview of F5 vulnerabilities (August 2021). Available from: <https://support.f5.com/csp/article/K50974556> [Accessed 25 September 2021].

Microsoft. (2017) AD FS Overview. Available from: <https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/ad-fs-overview> [Accessed 25 September 2021].

Redhat. (2020) What is a CVE?. Available from: <https://www.redhat.com/en/topics/security/what-is-cve> [Accessed 25 September 2021].

Barracuda. (2016) Barracuda Web Application Firewall: Active Directory Federation Services. Available from: <https://www.barracuda.com/resources/Barracuda_Web_Application_Firewall_Azure_TB_Active_Directory_Federation_Services_US> [Accessed 25 September 2021].