iCyber-Security
SAFEGUARDING YOUR DIGITAL WORLD

Case Study
UK Online Retailer

Web Application Firewall Policy Tuning To Strengthen Ecommerce Website Security

Company Summary

This online retailer origin can be traced as far back as 100 years as a small independent shop employing a handful of staff. The company grew and continues to operate today as a bike retailer with a growing online shopping presence.

Requirement

Our client had a requirement to secure its ecommerce infrastructure against Advanced Persistent Threats (APT) and DDoS. F5 Networks was selected to deliver the Web Application Firewall (WAF) functionality. The main task was to tune the existing F5 ASM (WAF) policy to ensure that the configuration was robust and optimised to protect cardholder's data against information leakage and web based attacks.

Solution

iCyber-Security was selected because of our combined expertise in network and application security as well as our integration expertise with Security Analytics solutions such as Splunk. Having helped several retailers design, secure, and optimised their online web systems, we provided recommendations and practical guidance based on OWASP top 10. By configuring the F5 ASM security features such as L7 DDoS, web scrapping detection, SQL-injection prevention, and Data Guard, our client was able to protect sensitive data against leakage and APT.

Business Benefits

• Increase the availability and security of ecommerce apps

Key Challenges

• F5 ASM policy tuning to enhance the security of web apps used for ecommerce

• Recommendations and best practices for the strongest security to protect cardholders data

• Knowledge transfer to the network and application security teams

iCyber-Security Delivery

• Delivered F5 ASM policy tuning guidelines and practical steps to improve the security of ecommerce apps

• Delivered F5 ASM integration with Splunk for Security Analytics

• Be-spoke training to the network and security team