Deklarative Web Application Firewall in einem Softwarebereitstellungsprozess

Studiengang: MAS Cyber Security

Durch die Automatisierung werden Applikationen immer schneller im Internet bereitgestellt. Um die Sicherheit dieser Applikationen zu gewährleisten, sollte die Bereitstellung einer Web Application Firewall (WAF) zeitgleich geschehen. Der Betrieb einer WAF erfordert jedoch viel Zeit und Expertise und beisst sich mit den Praktiken in der agilen Softwareentwicklung. Diese Differenz soll sich klären, wenn die WAF in den Softwarebereitstellungsprozess aufgenommen wird.

Einführung

Zurzeit nehmen die Applikationsentwickelnden mit dem Team Kontakt auf, welche für die Application Delivery Controlling (ADC) Infrastruktur zuständig ist. Dieses Team versucht zu verstehen, wie die Applikation funktioniert und konfiguriert dementsprechend die WAF Policy. Später durchläuft die Konfiguration der WAF Policy die Test-, Integration- und die Produktionsinstanz, wo das Ganze möglich akkurat getestet werden soll.

Probleme

Dabei können je nach Fortschritt des Projektes mehrere Wochen vergehen, ohne dass die WAF auch nur einen einzelnen schädlichen Request blockiert hat. Sensitive Daten oder kritische Infrastrukturen können während dieser Zeit einem hohen Sicherheitsrisiko ausgesetzt sein. Zu oft werden dabei die Prozesse nicht korrekt eingehalten oder schlecht getestet, was sich negativ auf den korrekten Betrieb einer WAFs auswirkt. Es werden Störungstickets eröffnet und die Kundschaft erhält einen negativen Eindruck über die Firma, welche diese Applikation betreibt.

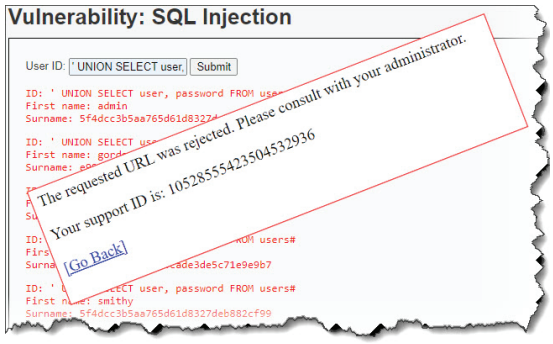
Ziele

Die WAF Konfiguration wird zusammen mit der Applikation deklariert und soll mit der Applikation wachsen. Wie bei jedem neue Softwarerelease soll auch die WAF Konfiguration den Softwarebereitstellungsprozess durchleben. Es wird erhofft, dass das Verständnis im Umgang mit einer WAF verbessert und dadurch den Schutz der Applikation langfristig gesteigert wird.
Zusätzlich wird beschrieben, wie eine WAF Policy Prüfung aussehen könnte. Mit so einer Prüfung soll den Applikationsentwickelnden aufgezeigt werden, wo potenziell die WAF Policy noch verbessert werden muss. Dies basierend der Frage: «Was» kann «Wovor» geschützt werden und «Wie» wird dies gemacht?

Simeon Jordi

Ergebnis

Es ist möglich, mit modernen Tools wie Jenkins, Ansible und Bitbucket die Bereitstellung der WAF zu beschleunigen, ohne dass sich dabei die Sicherheit bemerkbar verschlechtert. Dabei kann die WAF Konfiguration von Beginn an die schädliche Anfragen blockieren und den Applikationsentwickelnden eine transparente Sicht auf die WAF Konfiguration gegeben werden. Es bedarf aber vielen Abklärungen, um ein solches Produkt anderen DevOps Engineers als Selfservice anzubieten. Zum einem benötigt es spezifisches Wissen, welches sich zuerst aneignet werden muss. Zum anderen müssen viele Abklärungen und Tests gemacht werden, um die hohen Anforderungen wie Verfügbarkeit, Stabilität und Sicherheit von Web Applikationen zu gewährleisten.
DevOps Engineers, welche sich mit Netzwerk und Sicherheit auf Anwendungsebene auskennen, sollten die nötige Voraussetzung jedoch besitzen, sich mit zu erstellenden Richtlinien und Dokumentationen in die Thematik einzuarbeiten.



SQL Injection ? Bestmöglich unterbinden!