ModSecurity Kullanım Modelleri

Gömülebilirliğin Avantajları

Çoğu web güvenlik duvarı, cihazlar üzerine monte edilmiş şekildedir ve bu cihazlar ağa dahil edilirler. Fakat gömülebilirliğin avantajları bilinen web güvenlik dubarı cihazlarına göre daha fazladır. Bunu da aşağıda ki şekilde dile getireyim.

ModSecurity gömülebilir bir web güvenlik duvarıdır. Yani hali hazırda çalışır olan web sunucunuzun yapısını bozmadan eklenilebileceğini kastediyoruz. Aynı zamanda istenildiğinde yapıyı bozmadan çıkarılabileceğini. Gömülebilirliğin getirdiği avantajları sıralayacak olursak,

1. Kurulu sunucu yapısında ve network de bir değişiklik yapmanıza gerek kalmadan ModSecurity`i bir kaç dakikada kurup, aynı zamanda kaldırabilirsiniz. Bununla birlikte sadece ihtiyacınız olan özelliklerini kullanabilirsiniz.
2. No single point of failure. Öncelikle SPOF (Single Point Of Failure) den bahsedeyim. Tüm işlerinizi gören, servislerin üzerinde koştuğu bir sunucunuz var. Bu sunucunun ayakta durmasını engelleyecek olaylara SPOF denir. Bunlar elektrik esintileri, işletim sisteminin çökmesi v.s olabilir. ModSecurity kullanımı size yeni bir SPOF kazandırmaz. Herhangi bir sorun anında sistemden basitçe çıkarılır ve eklenir.
3. Mümkün olduğunca az yük bindirmesi yapar. Çünkü web server`ün prosesi içinde çalışmaktadır. Ağ haberleşmesine ek hiç bir yük bindirmez. Sadece parsing ve veri değişikliği yaparken azda olsa bir yük bindirir. ModSecurity kurallarında bu yük bindirimi için parse işlemlerindeki bellek kullanımına dikkat etmek gerekir. Özellikle “?:” PCRE parametresi parse yapılan modelin hafızada tutulmamasını ve işlemlerin daha hızlı yazılmasını sağlar. ModSecurity`nin hız konusu ise auditlog ve debuglog u kullanmanızla doğru orantılıdır. Özellikle auditlog hatırı sayılır yük bindirebilir. Onun için sadece analiz işlemlerinde bunu kullanmanızı tavsiye ederim.
4. Şifrelenmiş ve sıkıştırılmış veri ile bir sorun yaşamazsınız. Bazı WAFlar SSL trafiğini analiz etmede zorlanabilir. Fakat ModSecurity deşifreleme ve sıkıştırılmış verinin açıldığı anda devreye girer. Buda onun gömülü olmasından kaynaklanmaktadır.

Reverse (Ters) Proxy Modeli ve Avantajları

Bu model size bir WAF cihazı yapmanızı sağlıyor. Apache üzerinde mod_proxy ve mod_security ile birlikte kuracağınız bir web güvenlik duvarının arkasında istediğiniz web sunucusunun (IIS, Tomcat etc) güvenliğini sağlamış olursunuz. Avantajlarını sıralayacak olursak;

1. Single Point Of Acces olarak adlandırılan tek noktadan denetimn mekanizmasını sunar. Yani tüm web sunucularınızı bu modeli kullnarak tek noktadan devre dışı bırakabilirsiniz. Kimi zaman avantaj sağladasa dez avantajlarıda çoktur.

2. Performans artışını sağlar. Bilindiği gibi web sunucularında CPU ve RAM büyük önem arzetmektedir. Zararlı isteklerin öndeki güvenlik duvarına takılacak olmalarıyla (mod_proxy+mod_security) arkadaki sunucuların işlemcilerine fazla yük binmemiş olacaktır. Bu nedenle CPU ve RAM kullanımında önemli artışlar olacaktır. Özellikle saldırı zamanlarında CPU kullanımlarının tavan yapması bu özelliği avantajlı kılıyor. Aynı zamanda mod_proxy kullanıldığı için cachele mekanizmasıda devrede olmuş olacak. Son olarakta zararlı isteklerin öndeki güvenlik duvarına takılmaların dan dolayı responseden kaynaklanan bandwith`te gözle görülür kazançlar sağlanır.
3. Bu model ile birlikte arkadaki sunucuların özelliklerini, işletim sistemlerini, sunucu imzalarını saklayabilirsiniz. Bir nevi web sunucularının bulunduğu ağı izole eder diyebiliriz.
4. Güvenlik duvarının arkasında olan ağ topolojisini dış dünyaya kapatır.
5. Aynı zamanda kullandığınız farklı model-marka sunucularında güvenlik açıklarını perdelemiş olursunuz.

Yazan: Bünyamin Demir
İletişim: bunyamin@webguvenligi.org