Was lehren uns vergangene Angriffe auf Schwachstellen?

CLOUDFLARE®

Zu Beginn des Jahres 2020 wurde ein „schwerwiegender“ Cyberangriff gegen die Vereinten Nationen bekannt, der im September 2019 stattgefunden und 42 Core-Server kompromittiert hatte. Dabei nutzten die Angreifer eine bekannte Schwachstelle in einem mit dem Internet verbundenen Microsoft SharePoint-Server aus. SharePoint ist eine webbasierte, mit Microsoft Office kombinierbare Zusammenarbeitsplattform. Erfolgreich war der Angriff nur deshalb, weil die Infrastruktur der UNO nicht gepatcht worden war, obwohl Microsoft bereits im März 2019 Fixes für diese Schwachstelle herausgegeben hatte.

Bekannte Schwachstellen einer Infrastruktur anzugreifen, ist unter Cyberkriminellen gängige Praxis. Die UNO ist dabei nicht das einzige Opfer. Es gibt zahlreiche Beispiele, darunter der Angriff auf Equifax im Jahr 2017, bei dem Schwachstellen in Apache Struts und bei der Remote-Codeausführung von vBulletin ausgenutzt wurden. Etliche Unternehmen waren davon betroffen. Firmen und Organisationen bemühen sich nach Kräften, ihre Infrastruktur und Daten zu schützen. Doch Sicherheitsmaßnahmen sind betrieblich nur schwer umsetzbar, auch wenn heute jede Lücke potenziell zum Einfallstor werden kann.

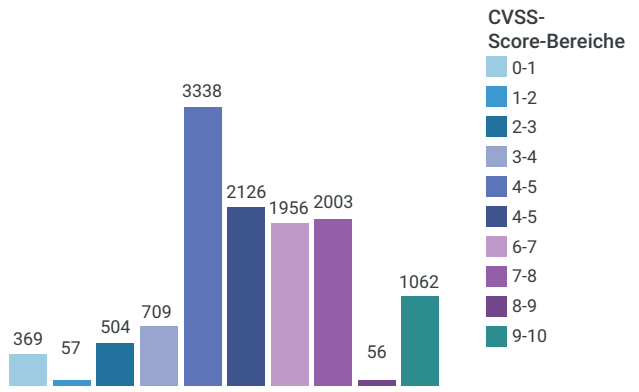
Um solche Angriffe zu vereiteln, muss der Fokus auf der Lösung der grundlegenden Probleme liegen.

Vor allem kommt es auf das Patchen der Infrastruktur an, was allerdings alles andere als einfach ist.

Immer mehr Sicherheitsbeauftragte investieren einen Großteil ihrer Ressourcen in eine gute „Cyberhygiene“ für ihre Infrastruktur. Für eine gut gepflegte Präsenz im Cyberspace ist es äußerst wichtig, die Infrastruktur laufend mit Patches auf dem neuesten Stand zu halten.

Das ist jedoch keine leichte Aufgabe. Angesichts der schieren Menge an Patches und der Häufigkeit, mit der die zahlreichen Anbieter immer wieder neue Korrekturen ausliefern, gelingt dies selbst den größten Sicherheitsteams in der Regel nur für Teile der Infrastruktur. Im Jahr 2019 wurden insgesamt 12.174 gängige Schwachstellen und Gefährdungen öffentlich, von denen 1.062 (8,7 %) mit einem CVSS-Score zwischen 9 und 10 als kritisch eingestuft wurden.

Schwachstellenverteilung nach CVSS-Scores



Quelle: Schwachstellen-Verteilung 2019 nach CVSS-Scores

Die herkömmliche Herangehensweise an dieses Problem besteht darin, Schwachstellen nach bestimmten organisatorischen Risikokennzahlen zu priorisieren und zu patchen. Sie werden in die Schwachstellen-Kategorien P0, P1, P2 usw. eingeteilt, wobei jeder Kategorie ein SLA zugeordnet ist. Die Abwägung zwischen den einzusetzenden Fixes und den verfügbaren Ressourcen ist ein Drahtseilakt – und diese Unsicherheit wird von Angreifern ausgenutzt.

Bei dem Angriff auf die UNO haben sich die Angreifer die Tatsache zunutze gemacht, dass die Organisation den Patch für die bekannte Schwachstelle ihrer Infrastruktur noch nicht angewandt hatte.

Grundlegendes mit einem mehrschichtigen Verteidigungsansatz sichern

Mit einem mehrschichtigen Verteidigungsansatz können Sicherheitsexperten einen starken Schutz vor solchen Angriffen aufbauen. Eine wichtige Komponente der aktuellen mehrschichtigen Verteidigungsstrategie ist eine cloudbasierte Web Application Firewall (WAF). Als separate Geräte ausgeführte Hardware-WAFs sind angesichts der aktuellen Bedrohungslage eine extrem veraltete Lösung. Anwendungen und Daten befinden sich heute meist sowohl in der lokalen Infrastruktur als auch in der Cloud.

Im Gegensatz zu Hardware-WAFs können cloudbasierte WAFs Angriffe auf Schwachstellen abwehren – unabhängig davon, ob sich Anwendung und Infrastruktur vor Ort oder in der Cloud befinden bzw. Bestandteil einer Hybridlösung sind.

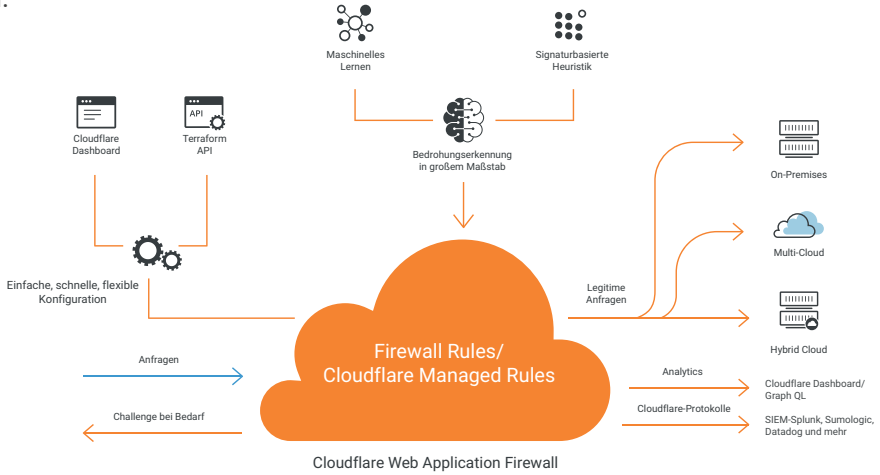
Für Sicherheitsexperten gilt es, mehrere wichtige Aspekte der cloudbasierten WAF zu berücksichtigen.

Der WAF-Markt wächst, insbesondere aufgrund der zunehmenden Verbreitung von Cloud-WAF-Diensten. Wenn Sicherheitsteams von Unternehmen WAFs daraufhin bewerten, ob sie verbesserte Sicherheit bieten können, einfach zu verwenden und zu verwalten sind und gleichzeitig die Datenschutzanforderungen erfüllen, sollten sie diese Studie heranziehen.

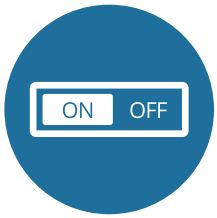
– Gartner-Bericht „Magic Quadrant for WAF“

Eine WAF-Lösung für heute und morgen

In ihrem jüngsten Bericht „The Future of Network Security Is in the Cloud“ (Die Zukunft der Netzwerksicherheit liegt in der Cloud) aus dem Jahr 2019 stellt die Firma Gartner fest: „Der Unternehmensperimeter hat keinen festen Standort mehr, sondern besteht aus einer Reihe dynamischer Edge-Funktionen, die bei Bedarf als Dienst aus der Cloud bereitgestellt werden.“ Mit der cloudbasierten WAF steht und fällt das aktuelle und zukünftige Sicherheitsniveau.

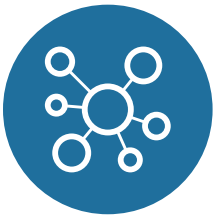


Die folgenden Aspekte sind bei der Auswahl einer cloudbasierten WAF zum Schutz Ihrer Anwendungen, Daten und Infrastruktur von enormer Bedeutung.



BENUTZERFREUNDLICHKEIT

Benutzerfreundlichkeit für Onboarding und Verwaltung ist bei der Auswahl einer WAF äußerst wichtig. Das Onboarding einer WAF sollte keine Wochen oder gar Monate in Anspruch nehmen und die Verwaltung der Lösung sollte auch ohne eine Heerschar von Fachleuten möglich sein. Zahlreiche Unternehmen schätzen die leichte Bedienbarkeit der Cloudflare WAF. Über ein intuitives Dashboard können Unternehmen schon mit wenigen Klicks ihr Sicherheitsniveau rasch steigern. Terraform API-Integrationen bieten praktische Methoden zur Erstellung und Verwaltung von WAF-Regeln.



BEDROHUNGSERKENNUNG IN ECHTZEIT

Zu den größten Mankos einer hardwarebasierten WAF zählen die fehlenden Echtzeitinformationen zu Bedrohungen und Angriffen. Selbst wenn man Bedrohungsinformationen in eine hardwarebasierte WAF einspeist, schafft man damit nur eine Lösung, die auf einen laufenden Angriff reagieren kann. Doch angesichts der sich rasant wandelnden Bedrohungslage der heutigen Zeit kommt es darauf an, Erkenntnisse zu Gefahren in Echtzeit zu erhalten. Die WAF von Cloudflare stützt sich auf ein ständig hinzulernendes Netzwerk, das mit den Rechenzentren von Cloudflare in 200 Städten auf der ganzen Welt verbunden ist und über 20 Mio. Internetwebsites weltweit schützt. Die aus der Analyse vielfältiger globaler Datenströme abgeleiteten Erkenntnisse liefern der WAF zusätzliche Echtzeit-Hintergrundinformationen zur Abwehr der neuesten Angriffe.

RUNDUMSCHUTZ

Unabdingbar für jede WAF ist der Schutz vor verbreiteten Schwachstellen wie den OWASP Top 10. Angreifer versuchen natürlich, diese Sicherheitslücken auszunutzen, sind aber vor allem an Zero Day Exploits und anderen kritischen Schwachstellen interessiert. Die Managed Rulesets von Cloudflare werden regelmäßig aktualisiert, damit Angriffe, die Zero Day-Schwachstellen und andere kritische Sicherheitslücken ausnutzen, bereits am Netzwerkrand von Cloudflare vereitelt werden und gar nicht bis zu Ihrer Infrastruktur vordringen. Die Managed Rulesets von Cloudflare können innerhalb der WAF mit nur einem Mausklick aktiviert werden. Mit Firewall Rules können Unternehmen mit wenigen Klicks ihre eigenen benutzerdefinierten Regeln erstellen, testen und einsetzen.

VERWERTBARE ANALYSEN

Kontrolle und Schutz sind wichtig, doch ebenso entscheidend ist es, über alle Angriffsereignisse und relevanten Daten im Bilde zu sein. Cloudflare Analytics bietet Sicherheitsexperten und -teams eine Dashboard-Ansicht zur schnellen und umfassenden Analyse der Daten. Die GraphQL API ermöglicht die Integration mit bereits vorhandenen Firmen-Dashboards. Darüber hinaus können Unternehmen umfassende Cloudflare-Protokolle in gängige SIEMs wie Splunk, Sumologic oder Datadog einspeisen.

AGILITÄT

Mit Bekanntwerden einer Sicherheitslücke, insbesondere einer Zero Day-Schwachstelle, beginnt der Wettlauf zwischen Kriminellen und den Sicherheitsteams der Unternehmen. Mit einem Außenperimeter am Netzwerkrand können sich Firmen schnell vorläufig vor Angriffen schützen, während ihre Sicherheitsteams die Infrastruktur patchen. Die WAF Rulesets von Cloudflare lassen sich weltweit in einer beispiellosen Geschwindigkeit von weniger als 30 Sekunden über unser Anycast-Netzwerk verbreiten.

Mehr erfahren Sie unter:

cloudflare.com/de-de/waf/