Zuverlässigerer Schutz von Webanwendungen und APIs

Es werden immer mehr cloudnative Anwendungen in Containern, serverlosen Funktionen und Microservices in diversen Technologielösungen bereitgestellt und die Verbreitung dieser komplexen Architekturen wird in Zukunft sogar noch zunehmen. Der Schutz der Webanwendungen und APIs, auf denen die Architekturen aufsetzen, ist seit jeher eine Herausforderung für Anwendungssicherheits- und DevOps-Teams. Webanwendungen und APIs verändern sich kontinuierlich und die vorhandenen Websicherheitslösungen bieten keinen ausreichenden Schutz.

Daher bietet Palo Alto Networks auf seiner Prisma Cloud-Plattform jetzt das branchenführende WAAS-Modul (Web Application and API Security). In diesem Whitepaper präsentieren wir eine quantitative Analyse des Moduls und den Vergleich mit anderen verfügbaren Lösungen der Branche. Das Ziel war, die größere Genauigkeit des WAAS-Moduls von Prisma Cloud nachzuweisen.

Kurze Einführung zu Messungen: Genauigkeit von Cybersicherheitslösungen

Die grundlegende Anforderung an eine Lösung zum Schutz von Webanwendungen und APIs ist die Abwehr webbasierter Angriffe wie SQL-Injektion, Cross-Site Scripting und Local File Inclusion. Cybersicherheitslösungen sollten allerdings nicht allein an der Tatsache gemessen werden, wie gut sie Angriffe abwehren können. Andernfalls wäre die beste Cybersicherheitslösung vermutlich ein ausgestöpseltes Ethernetkabel – ohne jegliche Verbindungen. Bei einer solch drastischen Maßnahme würde allerdings wohl ein Großteil des Geschäfts wegbrechen.

Die besten Vergleichstests berücksichtigen mehrere Genauigkeitsfaktoren der standardmäßigen binären Klassifikation zur Cybersicherheit. In diesem Whitepaper betrachten wir die folgenden Messwerte:

- **False Positives (FP)**: Legitime Aktivitäten werden fälschlicherweise als schädlich gemeldet.
- **False Negatives (FN)**: Schädliche Aktivitäten werden nicht erkannt.
- **True Positives (TP)**: Schädliche Aktivitäten werden korrekt erkannt.
- **True Negatives (TN)**: Legitime Aktivitäten werden korrekt erkannt.

Bei jeder Analyse, bei der die Genauigkeit von Cybersicherheitslösungen ermittelt und verglichen werden soll, müssen alle vier Faktoren berücksichtigt werden, damit Benutzer und Käufer die beste Lösung für ihren individuellen Anwendungsfall wählen können. Denn es gelten nicht immer die gleichen Anforderungen. Eventuell werden in einigen Fällen die Geschäftskontinuität und das erforderliche Maß an Sicherheit unterschiedlich gewichtet.

Diese vier Genauigkeitsfaktoren lassen sich mithilfe von zwei statistischen Konzepten ermitteln, und zwar Präzision und Sensitivität:

- **Präzision** (Precision) ist der Anteil (oder Prozentsatz) der gemeldeten Anforderungen, die tatsächlich schädlich waren. Anders gesagt: Präzision beschreibt, wie stark eine Sicherheitsfunktion zu False Positives neigt. Ein hoher Präzisionswert bedeutet, dass die Lösung weniger False Positives generiert.
- **Sensitivität** (Recall) ist der Anteil (oder Prozentsatz) der Angriffe, die korrekt gemeldet wurden. Ein hoher Sensitivitätswert bedeutet, dass die Lösung die Angriffe wie erwartet erkennt.

Außerdem ist es hilfreich, mithilfe der oben aufgeführten Genauigkeitsfaktoren einen übergeordneten Genauigkeitswert zu berechnen, der die Leistung der Lösung insgesamt beziffert. Ein solcher Wert ist der Matthews-Korrelationskoeffizient (Matthews Correlation Coefficient, MCC), auch Phi-Koeffizient genannt. Mit der MCC-Formel lässt sich ein einziger MCC-Wert berechnen.

$$MCC = \frac{TP \times TN - FP \times FN}{\sqrt{(TP \times FP)(TP + FN)(TN + FP)(TN + FN)}}$$

Abbildung 1: Formel zur Berechnung des Matthews-Korrelationskoeffizienten

Ein MCC-Wert von **+1,0** bedeutet, dass die Lösung immer richtig liegt – sie erkennt zuverlässig schädliche Aktivitäten und lässt legitime Aktivitäten stets zu. Ein MCC-Wert von **-1,0** bedeutet, dass die Lösung immer falsch liegt – legitime Aktivitäten werden immer und schädliche Aktivitäten nie blockiert. Ein MCC-Wert von **0,0** bedeutet wiederum, dass die Lösung fast nach dem Zufallsprinzip vorgeht.

Nach der Klärung der Begriffe sehen wir uns jetzt die Ergebnisse für unsere WAAS-Lösung an.

Messung der Genauigkeit: Schutz von Webanwendungen und APIs

In Bezug auf den Schutz von Webanwendungen bedeutet ein False Positive, dass eine legitime HTTP-Transaktion (zum Beispiel die legitime Übermittlung eines Benutzerformulars) von einem Schutzmechanismus fälschlicherweise blockiert wurde. Ein False Negative bedeutet, dass ein webbasierter Angriff wie eine SQL-Injektion von dem Schutzmechanismus nicht gemeldet wurde. True Positives beziehen sich auf webbasierte Angriffe, die korrekt gemeldet wurden, und True Negatives entsprechend auf legitimen Benutzerdatenverkehr, der an die Webanwendung oder den API-Endpunkt weitergeleitet wurde.

Präzision beschreibt in diesem Zusammenhang, wie viele False Positives die Sicherheitsfunktion generiert. **Sensitivität** beschreibt wiederum, wie effektiv die Sicherheitslösung Angriffe erkennt.

Wir hoffen natürlich, dass die Präzisions-, Sensitivitäts- und MCC-Werte möglichst hoch sind. Für einen echten Nachweis müssen wir diese Werte in einem Test ermitteln.

Messung von False Negatives und True Positives

Um festzustellen, wie gut eine Lösung in Bezug auf False Negatives und True Positives abschneidet, müssen wir zahlreiche Angriffsfälle vorbereiten, die alle bekannten Angriffsvektoren abdecken. Ein solches Arsenal kann durch Techniken aus realem Angriffsverkehr, Automatisierungstools von Hackern und Inhalten von Hackerwebsites zusammengestellt werden.

Für den Test müssen dann nur die Schutzmechanismen vor einer Webanwendung implementiert und anschließend die Angriffstechniken ausgelöst werden. Jeder abgewehrte Angriff zählt als True Positive, jeder übersehene Angriff als False Negative.

Messung von False Positives und True Negatives

Dieser Fall ist etwas komplizierter. Zur Messung von False Positives können beispielsweise Schutzfunktionen für eine Webanwendung eingerichtet werden. Anschließend wird überprüft, ob sie bei legitimem Benutzerdatenverkehr reagieren. In diesem Fall muss allerdings festgelegt werden, welche Menge an Datenverkehr für einen solchen Test ausreicht. Außerdem sind die erfassten Daten nur für diese spezifische Webanwendung relevant.

Eine andere Methode wäre die Aufzeichnung großer Mengen an legitimem Datenverkehr von möglichst vielen realen Webanwendungen und APIs sowie diversen Anwendungsarten (zum Beispiel Backend-APIs für mobile Apps, E-Commerce-Websites, CRM-Systeme und Marketingwebsites). Nachdem möglichst vielfältiger legitimer Datenverkehr erfasst wurde, wird dieser über den getesteten Schutzmechanismus geleitet. Jede Reaktion der Sicherheitslösung gilt dann als False Positive und jede Anforderung, die an die Anwendung weitergeleitet wird, als True Negative.

Nachdem alle vier Genauigkeitsfaktoren ermittelt wurden, kann der MCC-Wert berechnet und die Genauigkeit der Lösung insgesamt bestimmt werden.

Dieser Ansatz ist allerdings nicht neu. Er wurde zum Testen der Genauigkeit von WAF (Web Application-Firewalls) im Jahr 2013 entwickelt und auf der NYC OWASP-Konferenz im selben Jahr vorgestellt.

Genauigkeitstest: WAAS-Modul von Prisma Cloud

Für unseren Genauigkeitstest haben wir mehr als 200.000 legitime HTTP-Transaktionen von verschiedenen gängigen Webanwendungen, Websites und Web-APIs zusammengestellt. Außerdem haben wir ein umfangreiches Arsenal aus über 5.000 spezifischen Webangriffsvektoren erstellt, die alle OWASP Top-10-Kategorien und weitere Bedrohungen abdeckten. Anschließend wurden das WAAS-Modul eingerichtet und die Angriffe ausgeführt.

Der MCC-Wert insgesamt für das WAAS-Modul von Prisma Cloud lag bei **0,956**.

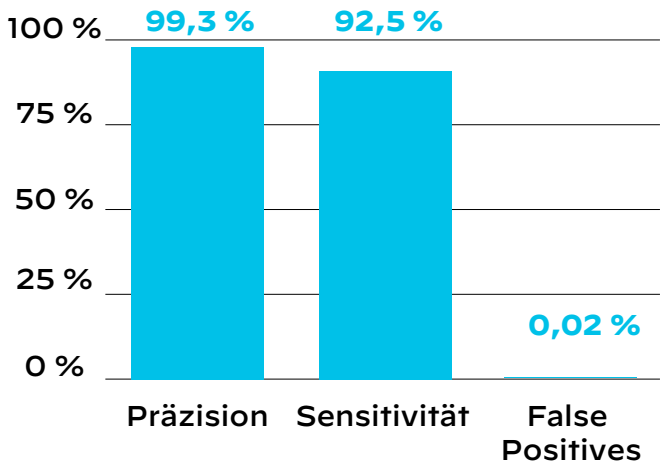

Abbildung 2: WAAS-Modul von Prisma Cloud: Präzision, Sensitivität und False Positives

Branchenvergleiche

Diese Zahlen sind zwar interessant, aber wirklich aussagekräftig sind sie erst, wenn man die Genauigkeit des Moduls mit anderen branchenführenden Lösungen vergleicht. Wir haben dieselben Tests mit denselben Methoden für sechs andere Lösungen durchgeführt:

- Zwei führende WAF-Lösungen und -Services (Web Application-Firewall)
- Eine Open Source WAF-Lösung
- Zwei führende WAF-Lösungen von Cloud-Serviceanbietern (Cloud Service Provider, CSP)
- Eine RASP-Lösung (Runtime Application Self-Protection)

In Tabelle 1 sind die Ergebnisse der Vergleiche des WAAS-Moduls von Prisma Cloud mit diesen Lösungen zu sehen.

Tabelle 1: Vergleich des WAAS-Moduls von Prisma Cloud mit ähnlichen Lösungen

Lösung	Präzision	Sensitivität	False Positives	MCC
WAAS-Modul von Prisma Cloud	**99,3 %**	**92,5 %**	**0,02 %**	**0,956**
WAF-Lösung 1	65,5 %	91,1 %	1,61 %	0,764
WAF-Lösung 2	87 %	85,9 %	0,43 %	0,866
Open Source WAF-Lösung	91,3 %	91 %	0,29 %	0,908

Tabelle 1: Vergleich des WAAS-Moduls von Prisma Cloud mit ähnlichen Lösungen (Fortsetzung)				
Lösung	**Präzision**	**Sensitivität**	**False Positives**	**MCC**
WAF-Lösung des CSP 1	57,6 %	83,5 %	2 %	0,681
WAF-Lösung des CSP 2	61,4 %	91,3 %	0,85 %	0,729
RASP-Lösung	79,9 %	50,1 %	0,85 %	0,614

WAAS-Modul von Prisma Cloud: Nachweislich überragende Genauigkeit

Wir haben nach der optimalen Methodik zum Testen der Genauigkeit einer Lösung zum Schutz von Webanwendungen und APIs gesucht. Dabei haben wir gelernt, dass es nicht ausreicht, eine Lösung unter den Gesichtspunkten der strikten Richtlinien oder der Anzahl der abgewehrten Angriffe zu betrachten. Es müssen immer auch ihr Verhalten bei legitimem Datenverkehr und die Anzahl der False Positives berücksichtigt werden. Mithilfe der beschriebenen Testmethoden haben wir die Genauigkeit für das WAAS-Modul von Prisma Cloud mit anderen führenden Lösungen verglichen. Die Daten sprechen für sich und beweisen eindeutig die überragende Genauigkeit unserer Lösung.

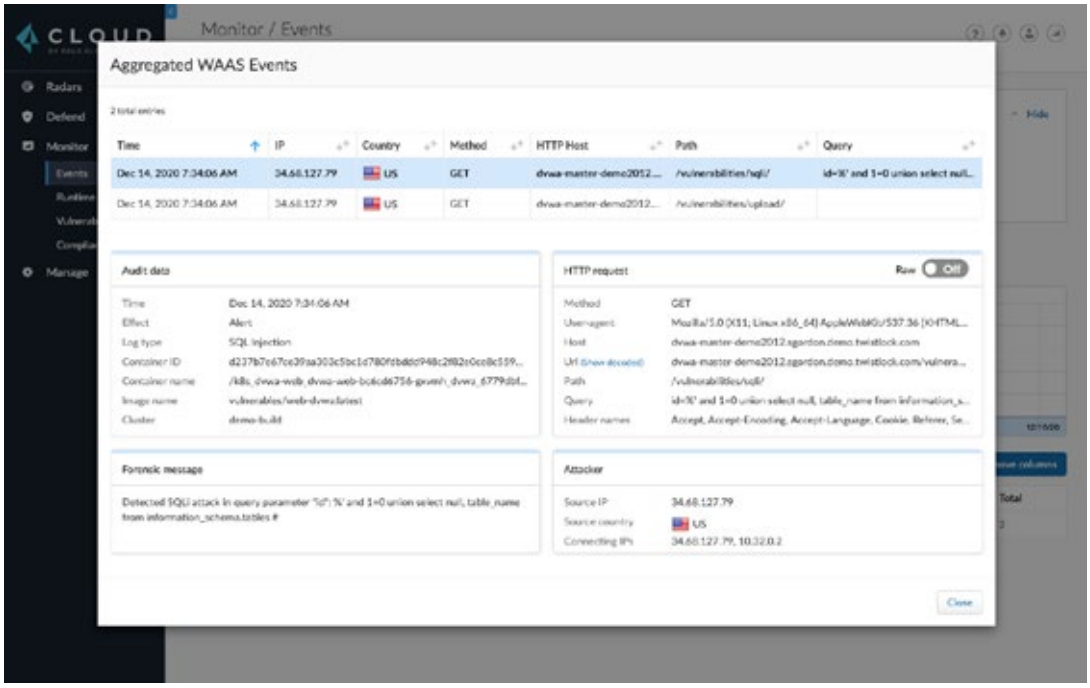

Abbildung 3: Aggregierte Auditdaten für das WAAS-Modul von Prisma Cloud

Prisma Cloud von Palo Alto Networks

Prisma® Cloud ist die branchenweit umfassendste Plattform für den Schutz cloudnativer Anwendungen (Cloud Native Application Protection Platform, CNAPP) und bietet eine beispiellose integrierte Cloud-Sicherheit. So werden Cloud-Umgebungen und cloudnative Anwendungen während des Entwicklungszyklus und in Hybrid- und Multi-Cloud-Umgebungen geschützt.

Mit ihrem integrierten Ansatz überwindet Prisma Cloud die mit cloudnativen Architekturen einhergehenden Einschränkungen bezüglich der Sicherheit, statt sie nur zu maskieren. Im gesamten Anwendungslebenszyklus werden voneinander isolierte Sicherheitsprozesse miteinander verknüpft, sodass DevSecOps- und DevOps-Teams für Anwendungssicherheit sorgen und automatische Sicherheitsfunktionen einrichten können, um die sich ändernden Sicherheitsanforderungen in cloudnativen Architekturen zu erfüllen.

Weitere Informationen finden Sie auf unserer Website und in dieser Demo.

paloalto NETWORKS | Cybersecurity Partner of Choice

Oval Tower, De Entrée 99–197
1101 HE Amsterdam, Niederlande
www.paloaltonetworks.de

Telefon: +31 20 888 1883
Vertrieb: +800 7239771
Support: +31 20 808 4600