NGINX App Protect®

DAS GEHEIMNIS DER MODERNEN ANWENDUNGSSICHERHEIT

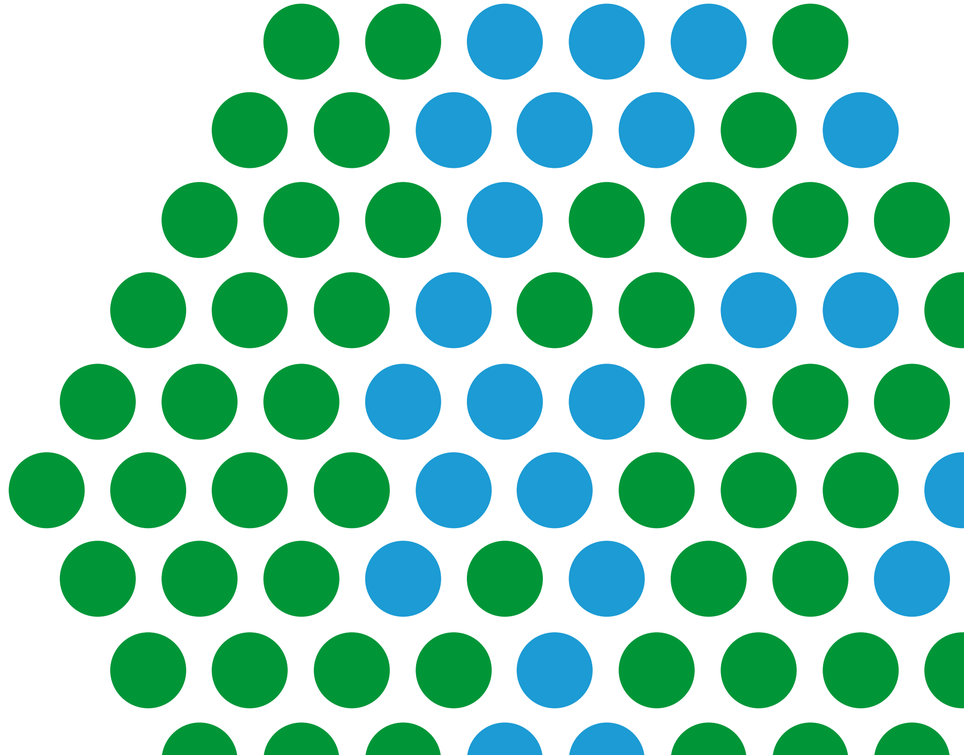
NGINX App Protect verhindert durch den Schutz Ihrer
modernen Apps und APIs Ausfallzeiten und Sicherheitslücken

NGINX ist ein Teil von F5

INHALT

NGINX App Protect.

Die Bedeutung von Geschwindigkeit in der modernen Anwendungsentwicklung	3
Traditionelle Sicherheitsmaßnahmen führen zu einem Dilemma	4
Tradition vs. Wandel	5
Eine moderne Lösung für moderne Anwendungen	6
Harmonie dank NGINX App Protect	8
Verbesserte Sicherheit und Compliance	9
Steigerung der Sicherheit und Leistung mit NGINX App Protect	11



DIE BEDEUTUNG VON GESCHWINDIGKEIT IN DER MODERNEN ANWENDUNGSENTWICKLUNG

Jedes Unternehmen strebt nach Agilität. Um mit der Konkurrenz mitzuhalten sowie den Kunden und Mitarbeitenden einen besseren Service zu bieten, müssen sich Unternehmen schnell an die neuesten Trends anpassen. Geschwindigkeit ist also wichtiger als je zuvor.

Möglich wird dies durch moderne Anwendungen und APIs, die bereits von vielen Unternehmen genutzt werden.

Tatsächlich werden 85 % der neuen Workloads in Containern bereitgestellt. Und 83 % des Internetverkehrs bestehen aus API-Calls.[3]

Eine Microservices-Architektur ermöglicht das Schritthalten mit dem Tempo moderner Unternehmen. Und mithilfe von DevOps können Anwendungen schnell entwickelt, bereitgestellt und bei Bedarf neu definiert werden. Diese agile Softwareentwicklung mit kontinuierlicher Integration und Bereitstellung beruht auf einer weitaus stärkeren Abhängigkeit von der Automatisierung. Um geschäftliche Innovationen in einem dem Markt entsprechenden Tempo zu liefern, sind adaptive Anwendungen dieser Art so konzipiert, dass sie schnell und häufig verändert werden können. Auf diese Weise werden ein optimales Benutzererlebnis ohne Kaufbarrieren und eine hohe Kundenbindung erreicht.

Auf dem immer härter umkämpften Markt führen negative Benutzererfahrungen mit einer App oder einer Website häufig zur Abwanderung (potenzieller) Kunden. Deshalb sind moderne Methoden der Anwendungsentwicklung so beliebt. Im Hinblick auf die Sicherheit haben sie jedoch auch ihre Schattenseiten.

Die Leistung zählt

Untersuchungen von Google haben ergeben, dass die Erwartungen der Kunden an einen Online-Dienst drastisch steigen. Wenn dieser nicht die optimale Benutzererfahrung bietet, wandern sie zur Konkurrenz ab.

Eine Seitenladezeit von einer bis drei Sekunden beispielsweise erhöht die Wahrscheinlichkeit, dass eine Website verlassen wird, um

32 %.

Ein bis fünf Sekunden Verzögerung hat Absprungwahrscheinlichkeit von

90 %

zur Folge.[1]

Wohingegen

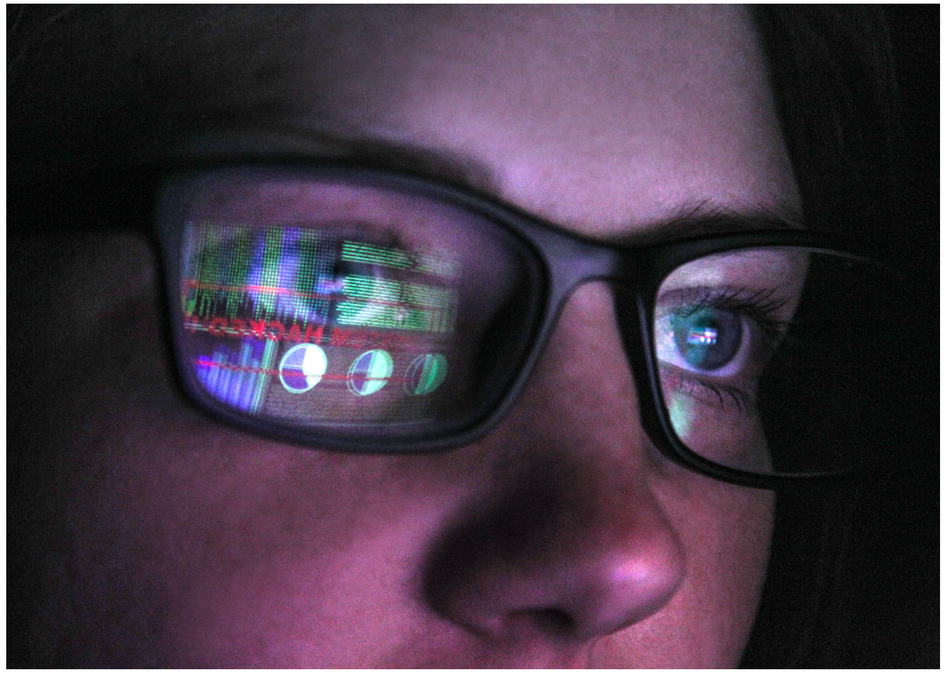
53 %

der Besucher eine mobile Website verlassen, wenn diese **nicht innerhalb von drei Sekunden geladen wird.**[2]

Da sich die Antwortzeit ihrer Anwendungen direkt auf die Benutzererfahrung und den Umsatz auswirkt, sind diese Informationen für Unternehmen von entscheidender Bedeutung.

TRADITIONELLE SICHERHEITSMASSNAHMEN FÜHREN ZU EINEM DILEMMA

Bei der herkömmlichen Anwendungsentwicklung werden erst am Ende des Prozesses die Sicherheitsmaßnahmen angewendet und Kontrollen durchgeführt. Das aktuelle Tempo der Anwendungsentwicklung macht dies jedoch unmöglich. **Amazon** als extremes Beispiel erreichte im Jahr 2015 insgesamt **50 Millionen Produktionsbereitstellungen.**[4] Im Durchschnitt also mehr als eine Bereitstellung pro Sekunde. Wie können herkömmliche Schutzmaßnahmen mit diesem rasanten Tempo mithalten? Die Unternehmen stehen vor einer schwierigen Entscheidung: Verlangsamen Sie die Entwicklung in den modernen Umgebungen, in die Sie viel investiert haben, um einen angemessenen Schutz für Ihre Anwendungen zu gewährleisten? Oder machen Sie mit unzureichenden Sicherheitsmaßnahmen weiter? Angesichts der aktuellen Bedrohungslage kann letzteres ein erhebliches Risiko darstellen.



Was beunruhigt die Entwickler am meisten?*

Sicherheit
50 %

Verfügbarkeit und Verlässlichkeit
39 %

Systemausfälle
39 %

Leistung
34 %

Skalierbarkeit
27 %

Komplexität
24 %

Automatisierung
23 %

Quelle: NGINX, The State of Modern App Delivery 2020

*Die Befragten konnten mehrere Optionen gleichzeitig wählen.

Alle 39 Sekunden wird ein Hackerangriff gestartet. Pro Tag werden über 30.000 Websites gehackt.[5] Dabei handelt es sich nicht nur um Angriffe auf den Code.
Über 20 % der im letzten Jahr aufgedeckten Sicherheitslücken waren auf Codefehler zurückzuführen. Und über 40 % dieser Angriffe zielten auf Webanwendungen ab.[6] Allerdings stellt jede Schwachstelle innerhalb der gesamten Anwendungsarchitektur ein potenzielles Risiko dar. Und die dezentrale Natur moderner Anwendungen bietet eine weitaus größere Angriffsfläche. Anwendungen und die damit verbundenen Microservices werden an immer mehr verteilten Orten, auch bei Drittanbietern, ausgeführt. Das eröffnet Hackern mehr Möglichkeiten und Angriffspunkte. Im Gegensatz zu den Anfängen des Internets, als ein Perimeterschutz noch die Bösewichte von einem internen Netzwerk fernhielt, bilden moderne Anwendungen die neue Frontlinie. Dort treffen Netzwerk und Benutzer aufeinander. Und nicht jeder dieser Benutzer hat positive Absichten.

TRADITION VS. WANDEL

Gegensätzliche Methoden sind die Wurzel des Problems: der moderne, schnelle DevOps-Ansatz steht der standardmäßigen, behäbigen Sicherheitsimplementierung, die eher für die Entwicklung älterer Software geeignet ist, gegenüber. Traditionelle Sicherheitsansätze müssen aufgrund von Microservices, die in Containern laufen, über APIs kommunizieren und über automatisierte CI/CD-Pipelines bereitgestellt werden, angepasst werden. So können sie nicht nur Engpässe im Workflow begrenzen, sondern auch in der modernen Welt effektiv sein.

In solchen Fällen werden Open Source Web Application Firewalls wie ModSecurity und Cloud-native Sicherheitstools oft als zusätzlicher Schutz in Betracht gezogen. Häufig erweisen sich diese Lösugnen jedoch als nicht schnell oder umfassend genug.

Für den Erhalt ihrer Wettbewerbsfähigkeit investieren Unternehmen viel in moderne Anwendungen und Infrastrukturen. Alles, was diese Geschwindigkeit drosselt, wird als Gefahr angesehen. Die Entscheidung für mehr Sicherheit auf Kosten der Leistung empfinden viele als kontraproduktiv und daher als nicht vertretbar. Es ist so, als würde man ein Sportauto zum Ziehen eines Wohnwagens einsetzen.

Um sowohl Schutz als auch Geschwindigkeit zu gewährleisten, müssen DevOps und SecOps ihre Kräfte effektiv bündeln, dies wird auch als „DevSecOps“ bezeichnet. Auf diese Weise wird die Sicherheit früher und stärker in Prozesse und Tools eingebettet („Shift left“). DevSecOps klingt zwar in der Theorie gut, gestaltet sich in der Praxis jedoch schwieriger. Nur 14 % der Unternehmen integrieren die Sicherheit vollständig in den gesamten Lebenszyklus der Softwareentwicklung.[7]

Wie lässt sich dieses Ungleichgewicht zwischen Sicherheit und Bereitstellungsgeschwindigkeit auf wirksame und kostengünstige Weise überwinden? Durch Automatisierung.

EINE MODERNE LÖSUNG FÜR MODERNE ANWENDUNGEN

NGINX App Protect

NGINX App Protect ist eine Anwendungssicherheitslösung, die die Effizienz der Advanced Web Application Firewall-Technologie (Advanced WAF) von F5 mit der Agilität und Leistung von NGINX kombiniert. Moderne Anwendungen laufen nach einmaliger Bereitstellung einfach überall. Diesen Komfort bietet die Automatisierung in NGINX App Protect in Bezug auf Sicherheitsrichtlinien: **einmal bereitgestellt, genießen Sie umfassenden Schutz („build once, run anywhere“)**. Diese schlanke, moderne Lösung reduziert Konflikte zwischen den Teams, spart Zeit und Geld und stellt sicher, dass die Security-Best-Practice überall eingehalten wird. So steht einer effektiven und harmonischen Arbeit zwischen DevOps und SecOps und damit auch einer schnellen Bereitstellung, ohne Kompromisse bei der Sicherheit, nichts mehr im Wege.

NGINX APP Protect unterstützt eine Vielzahl von Umgebungen

Cloud
- Amazon Web Services (AWS)
- Google Cloud Platform (GCP)
- Microsoft Azure
- VMware

Container
- Docker
- Kubernetes
- OpenShift

CPUs
- ARM (64 Bit)
- PowerPC (64 Bit)
- x86 (64 Bit)

Betriebssysteme
- CentOS
- Debian
- Ubuntu

App-zentrierte Sicherheit

Die Sicherheitskontrollen von NGINX App Protect werden – anders als Community-unterstützte Lösungen wie ModSecurity – direkt aus der Advanced WAF-Technologie von F5 portiert.

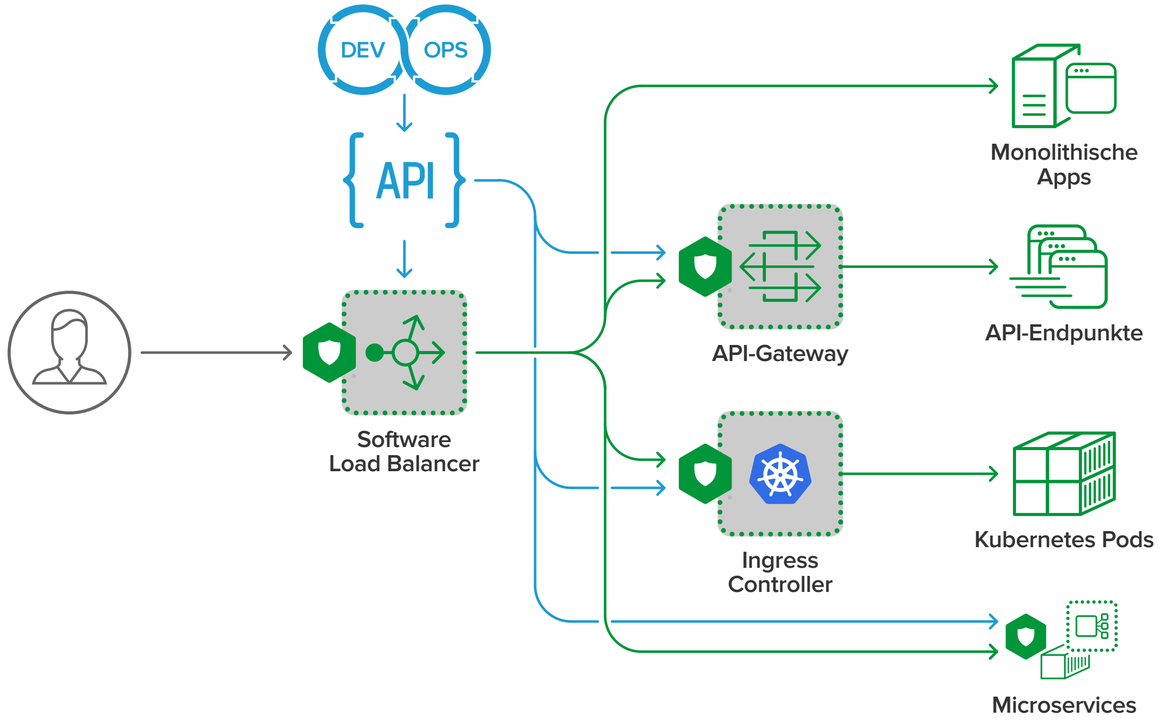
Der umfassende Satz von WAF-Angriffssignaturen hat sich nach ausgiebigen Tests in der Praxis bewährt und erzeugt praktisch keine Fehlalarme. NGINX App Protect schützt vor den OWASP Top 10 – den zehn größten Risiken für die Anwendungssicherheit –, es erzwingt die Einhaltung von Protokollstandards und wehrt gängige Umgehungstechniken ab. Darüber hinaus bietet NGINX App Protect Denylisting, prüft Cookies, schützt APIs und verhindert mit dem Data Guard von F5 den Verlust sensibler Daten.

EINE MODERNE LÖSUNG FÜR MODERNE ANWENDUNGEN

NGINX App Protect.

Entwickelt für moderne Anwendungen

Es ist nicht zielführend, strenge Sicherheitskontrollen aufzustellen, wenn sie nicht in der Betriebsumgebung einer Anwendung implementiert werden können. Aus diesem Grund wurde NGINX App Protect so konzipiert, dass es moderne Topologien für die Anwendungsbereitstellung unterstützt, wie z. B. die gängigen Bereitstellungsmodi für NGINX Plus. Dazu gehören Load Balancer, API-Gateway, Ingress Controller für Kubernetes Pods und Per-Pod Proxies für Microservices. Da NGINX App Protect speziell für die moderne Welt und die erforderlichen Tools entwickelt wurde, bietet es die nötige Sicherheit, um in einer solchen Umgebung erfolgreich zu bestehen.



Geschwindigkeit und Sicherheit in einem

Mit NGINX App Protect gehören Geschwindigkeitseinbußen aufgrund von Sicherheitsmaßnahmen der Vergangenheit an, ohne dabei Kompromisse bei der Leistung einzugehen – und andersherum. ModSecurity zum Beispiel beinhaltet die Auswertung regulärer Ausdrücke. Das bedeutet, dass jede zusätzliche Kontrolle die Anwendungsleistung direkt beeinträchtigt. Infolgedessen implementieren viele Administratoren bewusst nur eine sehr geringe Anzahl von Kontrollen, um die Geschwindigkeit – auf Kosten der Sicherheit – aufrechtzuerhalten. Kontrollen durch NGINX App Protect hingegen werden zu Bytecode kompiliert. So wird der Datenverkehr, unabhängig von der Anzahl an angewandten Angriffssignaturen, blitzschnell verarbeitet. Im Vergleich zu einer Implementierung von ModSecurity mit eingebundenem Core Rules Set v3 erhöhen sich Durchsatz und Anfragen pro Sekunde um das bis zu Zwanzigfache.

App-zentrierte Sicherheit

Die Implementierung vertrauenswürdiger Sicherheitsrichtlinien von F5 in der Nähe Ihrer Apps schützt vor umsatzschädigenden Angriffen, Datendiebstahl, Rufschädigung und Rechtsverstößen.

Entwickelt für moderne Apps

Die leistungsstarke, skalierbare Sicherheit auf den NGINX ADCs ermöglicht konsistente Sicherheitskontrollen für Webanwendungen, Microservices, Container und APIs.

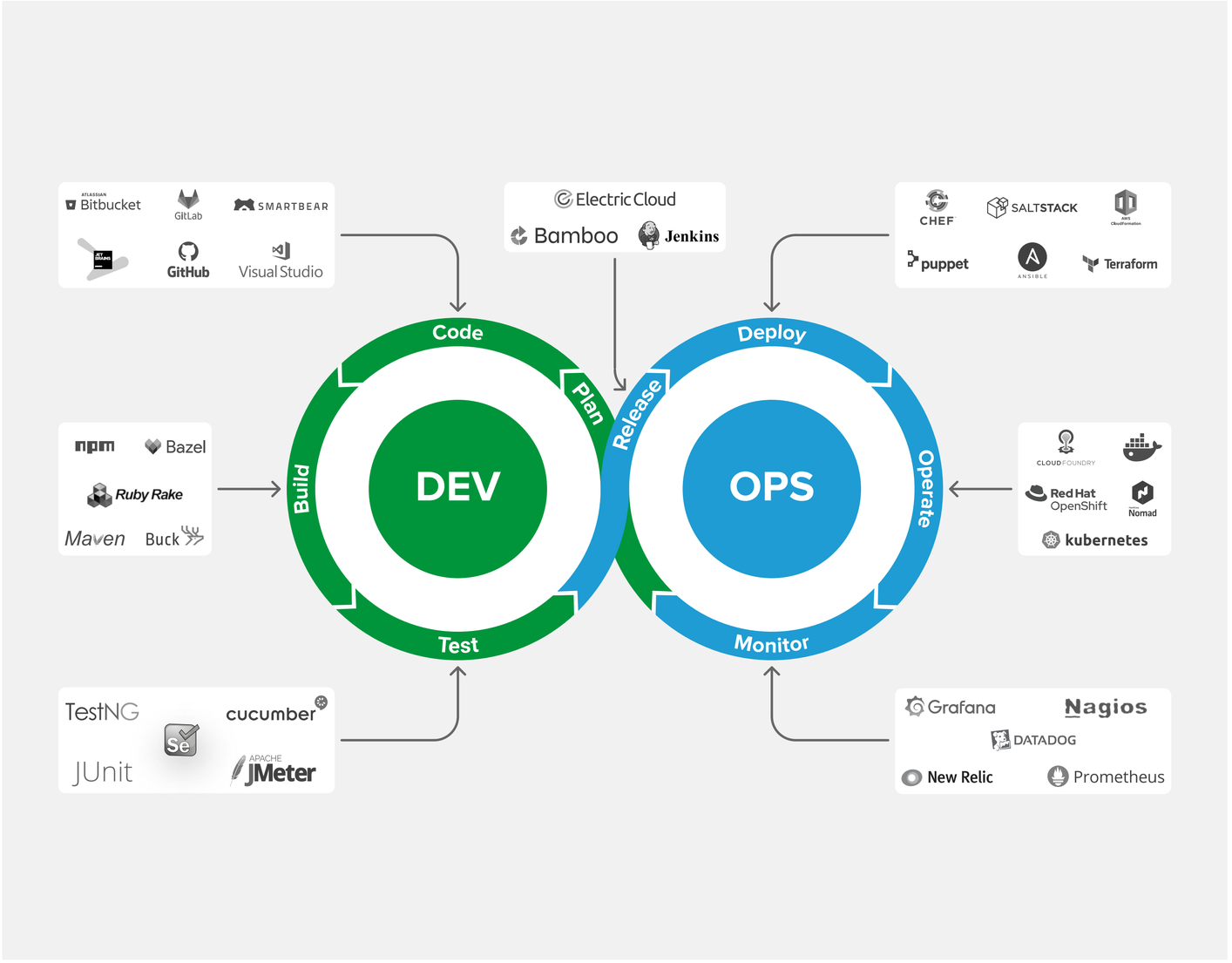
CI/CD-freundlich

Das zentrale Management und die Automatisierung genehmigter Sicherheits-kontrollen beseitigen Engpässe im Workflow und unterstützen „Shift left“ bei DevOps-Initiativen.

HARMONIE DANK NGINX APP PROTECT

Wie bereits in diesem E-Book beschrieben, möchten viele Unternehmen Sicherheitspraktiken bereits in der Entwicklungsphase einbeziehen. Doch das ist leichter gesagt als getan. **Zwar berichten 65 % der Sicherheitsteams von „Shift-left“-Initiativen, nachweisen kann dies jedoch nicht einmal ein Fünftel.**[8] Schlimmer noch, **fast die Hälfte der Unternehmen gibt zu, aus Zeitgründen wissentlich anfälligen Code in Produktion zu bringen.**[9]

Solche Kompromisse in Bezug auf die Sicherheit sind häufig auf die Trägheit und Störungsanfälligkeit herkömmlicher Sicherheitsprozesse zurückzuführen. Statische Anwendungssicherheitstests (SAST) und Software Composition Analysis (SCA) können beispielsweise Sicherheitsmängel in einem frühen Stadium der Entwicklung aufdecken. Aber was passiert, wenn Schwachstellen erst nach der Veröffentlichung der Anwendung entdeckt werden? Das Zurückschicken einer App an die Entwicklung erhöht nicht nur die Kosten und schadet der Produktivität, sondern führt auch zu Konflikten zwischen DevOps- und SecOps-Teams. Denn **48 % des technischen Fachpersonals glauben, dass die Sicherheit ein wesentliches Hindernis für die schnelle Bereitstellung von Software darstellt.**[10] NGINX App Protect hilft, solche Unstimmigkeiten zu vermeiden. Durch die Integration in gängige Entwicklungspipelines können Konflikte beseitigt und die sichere Bereitstellung beschleunigt werden. Dank der deklarativen Konfigurationsmöglichkeiten kann die Sicherheit Teil der CI/CD-Automatisierung der DevOps werden und wie jeder andere Teil der Funktionsspezifikation einer Anwendung getestet werden. Im Wesentlichen werden die Sicherheitsrichtlinien und die Konfiguration als „Code“ konsumiert, der aus einem Quellcode-Repository gezogen wird. Das SecOps-Team erstellt und pflegt diese Sicherheitsrichtlinien, um die zum Schutz des Unternehmens erforderlichen Kontrollen sicherzustellen.



VERBESSERTE SICHERHEIT UND COMPLIANCE

NGINX App Protect.

Leistungsstarke Perimetersicherheit

Vor der Einführung des Zero-Trust-Modells grenzte man das als sicher geltende Intranet mithilfe eines Perimeters vom Extranet ab. Doch die Hacker fanden schnell Wege, diesen Perimeter zu umgehen. Deshalb setzt man nun auf eine kontinuierliche Bewertung aller Zugriffe und des Datenverkehrs - standardmäßig wird niemandem vertraut.

Neue App-Architekturen bringen ihre eigenen Sicherheitsherausforderungen mit sich. Da sie an verschiedenen Orten z. B. in der Cloud oder auf lokalen Servern vorgehalten werden, stehen die Anwendungen nicht mehr unter der Kontrolle eines lokalen Administrators. NGINX App Protect wird zu einem Gatekeeper. Zum Schutz moderner Anwendungen nimmt es eine kontinuierliche Bewertung innerhalb eines Perimeters vor, um einzelne Anwendungen oder Anwendungsgruppen herum. Dabei prüft es den eingehenden Datenverkehr und setzt Sicherheitsrichtlinien durch. Dazu zählen Anwendungen, die vor Ort, in der Cloud oder in einer Hybrid-Cloud bereitgestellt werden, sowie containerisierte Architekturen wie das Kubernetes-Framework.

Abdeckung von Kubernetes-Clustern

NGINX App Protect arbeitet mit dem NGINX Plus Ingress Controller als Gatekeeper für ein gesamtes Kubernetes-Cluster, verwaltet den Zugriff von externen Clients und leitet Anfragen an die Kubernetes-Services im Cluster weiter. Die Sicherheitsrichtlinien können allerdings auch feingranular innerhalb des Clusters durchgesetzt werden, entweder pro Pod oder pro Service. Bei der Absicherung der Pods definiert der Pod den Perimeter, der eine App oder eine App-Komponente in einem oder mehreren Containern enthält. Bei der Absicherung des Services stellt ein Service die Instanzen einer App-Bereitstellung über einen oder mehrere Pods zur Verfügung. Der Perimeter wird hinter dem Service um die Pods herum errichtet.

Mit NGINX App Protect werden Bedrohungen durch Überprüfung des Datenverkehrs und Zugriffskontrollen beseitigt, bevor sie den Perimeter passieren. Als letzten Schritt vor den Apps können Sie hier die Art und Anzahl der Bedrohungen für Ihre Anwendungen am besten erkennen.

VERBESSERTE SICHERHEIT UND COMPLIANCE

Entscheiden Sie sich für den PCI-DSS

Um den Payment Card Industry Data Security Standard (PCI-DSS) zu erfüllen und Ihre Apps gegen die ständig wachsende Zahl von Sicherheitslücken zu schützen, benötigen Sie eine moderne WAF-Lösung wie NGINX App Protect. Die allererste Anforderung des PCI-DSS[11], um Daten von Karteninhabern zu schützen, lautet: **„Installation und Wartung einer Firewall-Konfiguration zum Schutz der Karteninhaberdaten."** Außerdem müssen Eigentümer von öffentlichen Webanwendungen diese schützen, indem eine automatische technische Lösung (z. B. eine Web Application Firewall) implementiert wird, „um webbasierte Angriffe zu erkennen und zu verhindern". Das ist jedoch nicht so einfach, wie es klingt. Angesichts der Vielzahl möglicher Angriffe und sich ständig ändernder Angriffsmethoden ist die Einhaltung des PCI-DSS eine der größten Herausforderungen für moderne Anwendungen.

Zusätzlicher Schutz

NGINX App Protect deckt 6.000 Signaturen ab und prüft darüber hinaus auch HTTP-Protokolle und Umgehungstechniken für jede einzelne Anfrage, um Fehler wie unzulässige Metazeichen in der HTTP-Nachricht oder eine ungültige Länge zu erkennen. Solche Anomalien können auf einen möglichen Angriff hinweisen, der noch nicht bekannt ist (Zero-Day-Angriff). Und ihre Anwesenheit verstärkt mögliche andere Anzeichen im Datenverkehr. Es verarbeitet JSON- und XML-Inhalte und kann die Nutzdaten auf potenziell bösartige Eingriffe prüfen. Außerdem verhindert es mittels Datenmaskierung (auch Response Scrubbing genannt), dass Antworten sensible Informationen preisgeben.

Anwendungsschutz in der Praxis: reifen.com

Ein führender Multi-Channel-Anbieter von Reifen, Rädern und Reifenservices, **reifen.com**, stand vor einer ganz besonderen Herausforderung. Für die höchstmögliche Einstufung als vertrauenswürdiger und sicherer Online-Händler verlangte der Prüfdienstleister TÜV die Installation einer WAF. Da Verbraucher großen Wert auf TÜV-Zertifizierungen legen, wurde dies zu einer wesentlichen Priorität.

Reifen.com nutzte bereits seit einigen Jahren NGINX-Webserver, um eine leistungsstarke Bereitstellung von Inhalten zu ermöglichen. Zunächst zog das Unternehmen NGINX Plus mit ModSecurity in Betracht – eine Lösung, die die TÜV-Anforderungen erfüllt hätte. Nach Gesprächen mit den Teams von F5 und NGINX fiel die Wahl jedoch auf NGINX App Protect. Ausschlaggebend für die Entscheidung war zum einen die überragende Leistung. In Anbetracht der Tatsache, dass sich Angriffsvektoren weiter verbreiten werden, war zum anderen die Fähigkeit, Angriffe z. B. auf ihre APIs abzuwehren, ein weiteres überzeugendes Argument.

„Wir haben uns für App Protect entschieden, weil es die beste Performance bietet. Im Zusammenspiel mit der Expertise von NGINX und F5 ist es langfristig die beste Lösung", so Sascha Petranka, E-Commerce-Berater von reifen.com. „Auch wenn die Kosten etwas höher waren als bei ModSecurity, war es eine klare Entscheidung."

Mithilfe von NGINX Plus und NGINX App Protect konnte reifen.com nicht nur die Anforderung in Bezug auf Compliance und für die TÜV-Zertifizierung erfüllen. Das Unternehmen hat nun auch einen besseren Einblick in seine Performance, kann Probleme schneller erkennen und flexibler auf Wettbewerber reagieren.

Da NGINX App Protect für moderne Infrastrukturen entwickelt wurde und überall installiert werden kann, fügt es sich „als Code" direkt in Ihre CI/CD-Pipeline ein. Indem es näher an Ihren Anwendungen ist als herkömmliche WAFs, können Sie Sicherheitsrichtlinien schnell aktualisieren. Da NGINX App Protect auf allen Plattformen (darunter Public und Private Clouds, VMs, Container) und in allen Tools (einschließlich API-Gateway und Kubernetes Ingress Controller) eingesetzt werden kann, erhalten Sie eine konsistente Leistung und das gleiche Maß an Schutz für Ihre gesamte Infrastruktur. Darüber hinaus umfasst NGINX App Protect mehr als 6.000 Signaturen, die mindestens alle zwei Monate aktualisiert werden, um die neuesten bekannten Angriffe abzudecken. Kurzum: NGINX App Protect erfüllt nicht nur, sondern übertrifft die Anforderungen des PCI-DSS.

SICHERHEITS- UND LEISTUNGSSTEIGERUNG MIT NGINX APP PROTECT

NGINX App Protect

NGINX App Protect ermöglicht Unternehmen, die stark in neue Anwendungsarchitekturen und agile Praktiken investiert haben, eine Steigerung ihres ROI und gewährleistet gleichzeitig Anwendungssicherheit und die bestmögliche Performance. Durch die Einbindung in Entwicklungspipelines kollidiert NGINX APP Protect nicht mit den Prozessen der DevOps-Teams, sondern arbeitet im Einklang mit ihnen. Auf diese Weise können Anwendungen schnell und optimal geschützt bereitgestellt werden. Es optimiert die Anwendungssicherheit und Compliance. Sie erhalten eine hohe Performance bei einer extrem niedrigen Fehlalarmquote – ein weiterer Wettbewerbsvorteil für Ihr Unternehmen.

Nahtlose Integration mit NGINX, der führenden Plattform für Webanwendungen

- Ermöglicht starke Sicherheitskontrollen, die nahtlos in NGINX Plus integriert sind.
- Übertrifft andere WAFs durch eine verbesserte Benutzererfahrung.
- Reduziert Komplexität und die Zahl der benötigten Tools und unterstützt gleichzeitig moderne Apps.

Schnelle Abwehr von Bedrohungen und umfassende Sicherheitsanalysen

- Bietet erweiterte Sicherheit über grundlegende Signaturen hinaus, um angemessene Kontrollen zu gewährleisten.
- Nutzt die App-Sicherheitstechnologie von F5, deren Effizienz ModSecurity und anderen überlegen ist.
- Baut auf bewährtem Know-how von F5 auf, sodass Sie während der Entwicklung sicher im „Blocking“-Modus arbeiten können.
- Bietet hochgradig zuverlässige Signaturen für eine extrem niedrige Anzahl von Fehlalarmen.
- Erhöht die Sichtbarkeit durch Integration mit Analyselösungen von Drittanbietern.

Anwendungssicherheit – genauso agil wie Ihre DevOps-Prozesse

- Integriert Sicherheit und WAF nativ in die CI/CD-Pipeline.
- Bereitgestellt als schlankes Softwarepaket, das unabhängig von der zugrundeliegenden Infrastruktur ist.
- Ermöglicht deklarative Richtlinien für „Sicherheit als Code“ und die Integration mit DevOps-Tools.
- Verringert den Entwickleraufwand und schafft eine Feedbackschleife für eine schnelle Wiederherstellung der Sicherheit.
- Beschleunigt die Markteinführung und senkt die Kosten durch DevSecOps-automatisierte IT-Security.

Entdecken Sie die Vorteile von NGINX App Protect. Einmal installiert, genießen Sie umfassenden Schutz und bringen Sie Ihre Apps schneller auf den Markt.

Übersicht Partner

Liefern Sie schnell und erfüllen Sie die Kundennachfrage mit flexiblen IT-Lösungen von techmatrix.

In der sich schnell entwickelnden Geschäftswelt von heute ist der Kunde König. Egal, ob Sie einzelne Apps erstellen oder komplette Lösungen bereitstellen, die komplexe geschäftliche Herausforderungen lösen, Ihre Kunden müssen an erster Stelle stehen, um zu überleben.

Wir bei techmatrix sind bestrebt, Ihnen dabei zu helfen, Dienstleistungen schnell, sicher und mit größerer Agilität bereitzustellen. Seit über 20 Jahren unterstützen wir unsere Kunden mit kompetenter Beratung, Planung und Umsetzung und bieten flexible und maßgeschneiderte IT-Lösungen.

Als einer der wenigen Partner mit tiefgehenden technischen NGNIX-Kenntnissen sind wir in den letzten zehn Jahren mit NGNIX für jedes unserer Lösungspakete aufgewachsen. Unsere 20-jährige Erfahrung umfasst NGNIX-Integrationen in bestehende Umgebungen für Identitäts- und Zugriffsmanagement sowie für DevOps. Ob Sie Hilfe bei der Softwareentwicklung oder beim Datenmanagement, bei der Konfiguration oder beim Monitoring benötigen, wir unterstützen Sie dabei, flexibler auf die Bedürfnisse Ihrer modernen Kunden einzugehen.

techmatrix CONSULTING GMBH

https://www.techmatrix.de/ sales@techmatrix.de +49 89 121 914 55

Referenzen

[1] https://www.thinkwithgoogle.com/marketing-strategies/app-and-mobile/mobile-page-speed-new-industry-benchmarks/

[2] https://www.thinkwithgoogle.com/consumer-insights/consumer-trends/future-of-marketing-mobile-micro-moments/

[3] https://www.nginx.com/wp-content/uploads/2020/05/2020-05-21-NGINX-App-Protect.pdf

[4] https://www.allthingsdistributed.com/2014/11/apollo-amazon-deployment-engine.html

[5] https://techjury.net/blog/how-many-cyber-attacks-per-day

[6] https://enterprise.verizon.com/resources/reports/dbir/

[7] https://www.whitesourcesoftware.com/forrester-state-of-application-security-report/

[8] https://about.gitlab.com/developer-survey/

[9] https://www.prnewswire.com/news-releases/devsecops-study-finds-that-nearly-half-of-organizations-consciously-deploy-vulnerable-applications-due-to-time-pressures-301107632.html

[10] https://snyk.io/wp-content/uploads/dso_2020.pdf

[11] https://www.pcisecuritystandards.org/doibrary