



USP CORE WAAP

App-centric Security



Datum: 20. März 2024
Version: 0.12

United Security Providers AG
Telefon +41 31 959 02 02
info@united-security-providers.ch
www.united-security-providers.ch

Besuchsadresse:
Hauptsitz
Stauffacherstrasse 65/15, 3014 Bern
Zürich
Baslerpark, Baslerstrasse 60, 8048 Zürich



USP Core WAAP App-centric Security



Core WAAP ist eine umfassende, in CI/CD-Pipelines integrierbare Sicherheitslösung, die die Agilität und Sicherheit moderner IT-Umgebungen durch tiefgehende Transparenz und Kontrolle sowie einen containernativen Ansatz erhöht.

TRADITIONELLE WAFS

Traditionell schützen Unternehmen ihre Webanwendungen mit Web Application Firewalls (WAFs) am Perimeter, um Datenverkehr zu filtern und Angriffe von aussen abzuwehren. Bei monolithischen Anwendungen ist eine solche Sicherheitsarchitektur geeignet, da es hauptsächlich darum geht, externe Angriffe vom Rechenzentrum und der Webanwendung fernzuhalten. Die Sicherheitsteams konzentrieren sich hauptsächlich auf den "Nord-Süd"-Verkehr. Dadurch wird die Überprüfung interner Kommunikation (Ost-West) vernachlässigt und passt daher nicht in eine Zero-Trust-Architektur.

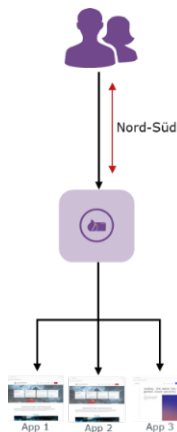


Abbildung 1: Traditionelle WAFs

Der Einsatz von traditionellen WAFs in Software-Projekten erfolgt meist in der Wasserfall Projektmethodik. Dabei erfolgen Entwicklung und Deployment in sequenziellen Schritten: Zuerst wird die Software entwickelt ohne WAF, dann erfolgt das Deployment und die Prüfung

durch Sicherheitsexperten. Diese Herangehensweise unterstützt zwar eine klare Trennung der Zuständigkeiten, ist jedoch weniger geeignet für agile Entwicklungsprozesse oder die Anwendung in Continuous Integration / Continuous Deployment (CI/CD)-Pipelines. Zudem werden Fehler und Sicherheitslücken oft erst spät im Entwicklungsprozess entdeckt. Das erschwert schnelle Iterationen und Anpassungen.

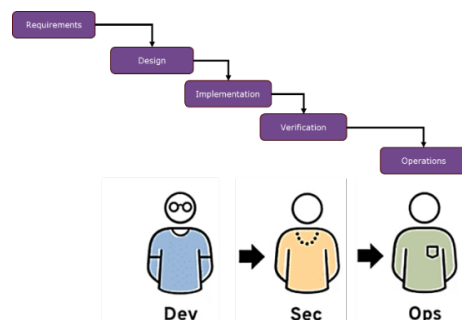


Abbildung 2: Traditioneller Entwicklungsprozess

MODERNE ANFORDERUNGEN

Moderne IT-Abteilungen stehen vor der Herausforderung, ihr Anwendungsspektrum zu erweitern, ohne das Personal aufzustocken. Die Aufteilung von grossen, monolithischen Anwendungen in kleinere Komponenten und der vermehrte Einsatz von Microservices bringt Vorteile mit sich insbesondere in Bezug auf agile Entwicklungsvorgehen, erhöht durch die vielen Schnittstellen aber auch die Angriffsfläche der Anwendung.



USP Core WAAP App-centric Security

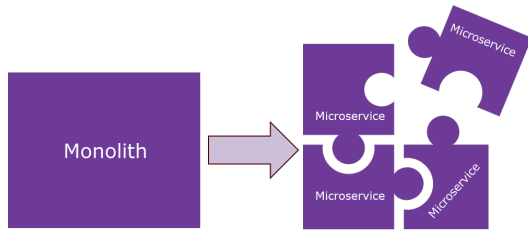


Abbildung 3: Aufspaltung vom Monolithen in Microservices

Jährlich erleben über 85% der Unternehmen Angriffe auf der Anwendungsebene, die versuchen ihre WAF umgehen¹. Dies wird besonders kritisch, da Anwendungen immer komplexer und vielfältiger werden, die Entwicklungszyklen immer kürzer sind und die Migration in die Cloud – ob privat oder öffentlich – weiter zunimmt.

Entwickler und Operationsteams nutzen immer häufiger Container-Frameworks wie Docker, OpenShift und Kubernetes, um durch agile Methoden eine höhere Flexibilität und Effizienz bei der Entwicklung und Bereitstellung von Anwendungen zu erreichen. Diese Container-Umgebungen verbessern die Ressourcennutzung im Vergleich zu traditionellen virtuellen Maschinen. Sie nutzen einen gemeinsamen Betriebssystemkernel und reduzieren dadurch den Overhead. Darüber hinaus bieten sie architektonische Flexibilität und unterstützen eine Automatisierung von bis zu 100%. Dadurch wird eine schnelle Bereitstellung und Entfernung von Diensten begünstigt und trägt zu einer effizienteren und agileren IT-Infrastruktur bei.



Abbildung 4: Vorteile von Container-Deployment

Die Containerisierung und die damit verbundene Microservices-Architektur steigern den Geschäftswert von Anwendungen, indem sie Entwicklungszyklen beschleunigen und die Skalierbarkeit verbessern. Sie bieten Plattformunabhängigkeit und ermöglichen die Portabilität von Anwendungen zwischen verschiedenen Cloud-Umgebungen und lokalen Servern ohne Codeänderungen. Diese Flexibilität unterstützt DevOps-Teams bei der schnellen Bereitstellung und Qualitätssicherung von Anwendungen. Sie reduziert Ausfallzeiten und Kosten.

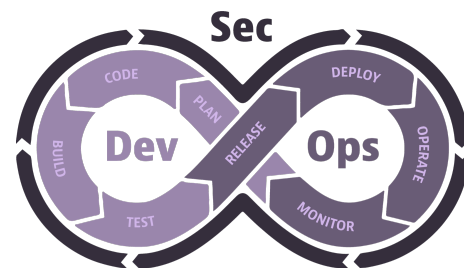


Abbildung 5: SecDevOps

Kubernetes ist der De-facto-Standard für die Orchestrierung von Microservices. Da Unternehmen zunehmend Kubernetes einsetzen, besteht die Gefahr, dass sie unbeabsichtigt Sicherheitslücken einführen. Anstatt die Sicherheit um die Plattform herum zu implementieren, müssen DevOps-, Sicherheits- und Plattfortmteams darauf achten, dass die

¹ Ponemon Institute, The State of Web Application Firewalls



USP Core WAAP

App-centric Security



Verteidigung durch die Plattform durchgesetzt wird (SecDevOps).

SOLUTION

In einer Zeit, in der traditionelle Sicherheitsperimeter an Bedeutung verlieren, erfordert der Schutz von Webanwendungen und APIs in Kubernetes-Clustern einen revolutionären Ansatz. Im Zentrum dieses Wandels steht unsere Workload-basierte Web Application and API Protection (WAAP), die tief in die Struktur von Kubernetes-Clustern eingreift. Der HTTP-Datenverkehr, der die Lebensader moderner RESTful APIs und Microservice-Kommunikation darstellt, fließt durch die Kubernetes-Cluster und erfordert ein neues Mass an Überwachung und Sicherheit. Dieser Ansatz ermöglicht eine umfassende Sichtbarkeit des gesamten Datenverkehrs, unabhängig von seiner Herkunft und Richtung, und ist damit eine adäquate Antwort auf die Herausforderungen der digitalen Transformation. Er passt sich auch nahtlos an die spezifischen Anforderungen jeder Anwendung an (App-centric), um ein optimales Gleichgewicht zwischen Sicherheit und Nutzbarkeit zu gewährleisten.

Unsere Core WAAP ist ein zentrales Element in Defense-in-depth-Sicherheitsarchitekturen. Sie ermöglicht die Integration von WAF-Regeln direkt in Kubernetes-orchestrierte Pipelines, bietet detaillierte Sichtbarkeit bis auf Pod-Ebene und unterstützt effektive Sicherheitsmassnahmen sowohl lokal als auch in der Cloud. Die nahtlose Kompatibilität mit gängigen Deployment- und Test-Tools erfüllt die Anforderungen an Automatisierung, Flexibilität und Ausfallsicher-

heit. Diese hohe Integration fördert effektive Sicherheitsmassnahmen und unterstützt die Umsetzung von Zero-Trust-Strategien durch identitätsbasierte Mikrosegmentierung und robuste Sicherheitsrichtlinien, die vor den häufigsten Sicherheitsbedrohungen wie SQL-Injection und Cross-Site Scripting schützen.

Weiter ermöglicht Core WAAP eine schnellere Bereitstellung durch vordefinierte Templates, vereinfacht das Richtlinienmanagement und ermöglicht die Implementierung von Zero-Trust-Regeln für Workloads innerhalb des Clusters. Diese fortschrittliche Sicherheitslösung erhöht die Agilität und Transparenz der Anwendungsentwicklung und -bereitstellung durch einen Container-nativen Sicherheitsansatz, der speziell für die Anforderungen moderner Container- oder Cloud-nativer Anwendungslandschaften entwickelt wurde.

HIGHLIGHTS

- Schützt nahtlos sowohl Cloud- als auch Legacy-Apps und APIs
- Vereint Vorzüge von Positive- und Negative-Security Model OWASP Top 10 Protection (OWASP Core Rule Set)
- Auto-Learning zur Verringerung falsch-positiver Request-Blocks
- Schnelle & einfache Implementierung
- gut integrierbar in CI/CD Prozesse, Infrastructure as Code
- Virtuelles Patching schützt Anwendungen vor einem Angriff aufgrund einer Schwachstelle, für die es noch keinen Patch gibt oder deren Patch noch nicht angewendet wurde
- Ressourcen-schonend, skalierbar