InfoGuard
SWISS CYBER SECURITY

WAF AS A SERVICE — WEB APPLICATION FIREWALL

Cloud-basierte Web Application Firewall as a Service für umfassenden Schutz Ihrer Web-Anwendungen und Portale

- Skalierbare State-of-the-Art WAF zu fixen Kosten
- Reduziert das Risiko von Ausfällen, Defacement und Datenverlust
- Schutz vor unerwünschtem Bot-Traffic, Backdoors, DDoS-Attacken
- Echtzeit-Schutz vor versteckten Bedrohungen in Anwendungen
- Kontrolle über den Zugriff auf Anwendungen und Funktionen

Architektur und Funktionalität der Lösung

Sämtliche Anfragen auf durch WAF geschützte Applikationen erfolgen über eine Schweizer Rechenzentrum-Infrastruktur. Die Backend-Anfragen erfolgen entweder mit HTTP über einen VPN-Tunnel (IPSec) oder direkt mittels HTTPS. Die InfoGuard Basis-Infrastruktur beinhaltet Next-Generation Firewalls mit Intrusion Detection and Prevention Systems (IDPS) sowie einen dedizierten DDoS-Schutz, welcher insbesondere auf Low-Volume-Attacken (bspw. Slowloris) ausgelegt ist.

Die InfoGuard WAF validiert sämtliche Layers einer Anfrage. Zudem besteht die Möglichkeit, die Antwort vom Backend-Servern (Headers und Inhalt) zu modifizieren. Falls gewünscht, kann die WAF zudem das Failover und Load-Balancing zum Kunden-Backend übernehmen.

Deployment / Integration

Initial wird je ein VPN-Tunnel von den InfoGuard Rechenzentren zum Rechenzentrum oder Rechenzentren des Kunden aufgebaut. Dies ermöglicht es, im Backend auf Applikationsebene (HTTP) unverschlüsselt zu kommunizieren und somit Ressourcen auf den Backend-Servern zu schonen (SSL-Offloading) sowie den Overhead seitens Backend-Verbindung über das Internet zu optimieren. Falls benötigt, kann selbstverständlich für einzelne oder alle Applikationen auch SSL resp. HTTPS für die Backend-Verbindungen verwendet werden.

Die Integration von neuen Applikationen benötigt die Änderung der entsprechenden DNS A-Records sowie die Freischaltung der Cloud-WAF IP-Adressen auf den involvierten Perimeter-Firewalls für den Backend-Zugriff über den VPN-Tunnel oder für den direkten, mittels SSL verschlüsselten Zugriff. Für die Konfiguration der Applikation auf der WAF muss zudem vorgängig ein Template ausgefüllt werden, in welchem Informationen über die Applikationsinfrastruktur sowie die Applikation wie etwa Backend IP-Adressen, Ports, Filter Settings usw. erfasst werden.

Servicebeschreibung

Sämtliche Komponenten der Infrastruktur sind redundant ausgelegt, um Hochverfügbarkeit gewährleisten zu können. Es besteht die Möglichkeit, in Zusammenarbeit mit dem Kunden vorgelagerte Authentisierung umzusetzen. Die nachfolgende Tabelle zeigt die verschiedenen Service-Modelle sowie die dazugehörigen Optionen:

	SERVICE LEVEL	
WAF LEISTUNGSUMFANG	**BASIC**	**ADVANCED**
Sicherheitsfunktionalitäten		
+ DDoS-Schutz	X	X
+ Protocol Validation & Rebuilding	X	X
+ Whitelist- & Blacklist-Filtering	X	X
+ Cookie Protection	X	X
+ Response Content Filtering & Content Rewriting	X	X
+ Failover & Load-Balancing Backend Infrastructure	X	X
+ URL Encryption		X
+ Smart Form Protection		X
Support & Wartung		
+ SOC Servicezeit	**5x10**	**5x10**
+ Online-Portal	X	X
+ Incident Response & Alerting	X	X
+ Patch & Release Management	X	X
Optionen		
+ SOC Servicezeit 7x24	**7x24**	**7x24**
+ Vorgelagerte Authentisierung	X	X
+ Zusätzliche Bandbreite	**20/50/100 Mbps**	**20/50/100 Mbps**

Ihre Vorteile mit dem InfoGuard WAF as a Service

Expertenschutz

Entfernt die Komplexität des WAF Managements, beschleunigt die Richtlinienbereitstellung und reduziert die Betriebskosten.

DDoS-Schutz

Kontinuierliche Verfügbarkeit der Website dank DDoS-geschütztem Netzwerk von höchster Enterprise-Qualität.

Automatische WAF-Updates

Neu identifizierte Bedrohungen werden in unserem Netzwerk blockiert.

App-Sicherheit & Compliance

Schutz vor Layer-7 & Zero-Day-Angriffen, OWASP Top 10, SQL-Injection, DDoS-Attacken, Cross-Site Scripting usw.

Jetzt online Offerte anfordern!
www.infoguard.ch/waf-as-a-service

InfoGuard AG

Lindenstrasse 10
6340 Baar/Schweiz
Telefon +41 41 749 19 00

INFOGUARD.CH