# WAF

Weitere Bezeichnungen: Web Application Firewall, Webanwendungs-Firewall, Web Application Firewalls

Rubrik: IT-Sicherheit

Eine WAF (Web Application Firewall) ist eine spezielle Sicherheitslösung, die Webanwendungen vor Angriffen über das Internet schützt. Sie überwacht den Datenverkehr zwischen einem Webbrowser und einem Webserver und kann verdächtige oder schädliche Anfragen erkennen und blockieren. WAFs werden häufig zum Schutz von Webseiten, Onlineshops, Webportalen und webbasierten Anwendungen eingesetzt.

Im Gegensatz zu einer herkömmlichen Firewall, die vor allem Netzwerkverbindungen anhand von IP-Adressen, Ports und Protokollen kontrolliert, untersucht eine WAF die Inhalte von HTTP- und HTTPS-Anfragen. Dazu gehören beispielsweise URL-Parameter, Formulareingaben, Cookies und HTTP-Header. Dadurch kann sie Angriffe erkennen, die über grundsätzlich erlaubte Webverbindungen erfolgen.

Zu den wichtigsten Bedrohungen, vor denen eine WAF schützen soll, gehören SQL-Injection, Cross-Site-Scripting (XSS) und andere Angriffe auf Webanwendungen. Bei einer SQL-Injection versuchen Angreifer beispielsweise, Datenbankabfragen durch manipulierte Eingaben zu beeinflussen. Eine WAF kann solche Angriffsmuster erkennen und die betreffende Anfrage zurückweisen.

Die Erkennung erfolgt häufig mithilfe von Sicherheitsregeln und Angriffssignaturen. Moderne Systeme verwenden zusätzlich verhaltensbasierte Analysen, um ungewöhnliche Zugriffe zu identifizieren. Je nach Konfiguration kann eine WAF Anfragen blockieren, protokollieren oder zur weiteren Überprüfung markieren. Allerdings können zu strenge Regeln auch legitime Zugriffe versehentlich verhindern.

Eine WAF kann als Hardware-Appliance, Softwarelösung oder cloudbasierter Dienst betrieben werden. Besonders verbreitet sind Cloud-WAFs, bei denen der Webverkehr zunächst über die Infrastruktur eines Sicherheitsanbieters geleitet wird. Auch Reverse-Proxys können WAF-Funktionen übernehmen. Bekannte Lösungen sind beispielsweise ModSecurity, Cloudflare WAF und AWS WAF.

Neben der Abwehr typischer Webangriffe unterstützen manche WAFs zusätzliche Schutzfunktionen. Dazu gehören die Begrenzung übermäßig vieler Anfragen (Rate Limiting), die Erkennung automatisierter Zugriffe und bestimmte Maßnahmen gegen DDoS-Angriffe. Der genaue Funktionsumfang hängt vom jeweiligen Produkt und seiner Konfiguration ab.

Eine WAF ist ein wichtiger Bestandteil der Websicherheit, ersetzt jedoch keine sichere Programmierung oder regelmäßige Softwareupdates. Sicherheitslücken in Webanwendungen

sollten weiterhin direkt behoben werden. In Kombination mit anderen Schutzmaßnahmen kann eine WAF das Risiko erfolgreicher Angriffe deutlich verringern.

## Weiterführende Informationen

Firewall, Webserver, Webanwendung, HTTP, HTTPS, SQL-Injection, Cross-Site-Scripting, XSS, DDoS, Reverse-Proxy, ModSecurity, Cloudflare WAF, AWS WAF, Rate Limiting