

Webvorkoster

Datenströme inspizieren

Webapplikationen ermöglichen einer großen Anzahl Anwender den einfachen Zugang zu IT-Ressourcen. Zum Schutz der über sie zugänglichen Informationen haben sich Web Application Firewalls durchgesetzt.

Online-Shops oder die Service-Portale von Finanzdienstleistern sind typische Webapplikationen, mit denen fast jeder Anwender von Zeit zu Zeit in Berührung kommt. In Unternehmen existieren darüber hinaus webgestützte Anwendungen, die der internen Organisation dienen, zum Beispiel Zeitbuchungssysteme, spezielle Teamkalender, Frontends für Warenwirtschafts- und Customer-Relationship-Management-Software. Gemeinsam ist all diesen Systemen, dass sie auf der einen Seite einen möglichst einfachen Zugriff übers Internet oder Intranet gewähren sollen, auf der anderen Seite aber die Brücke zu Datenbanken mit wichtigen und zum Teil vertraulichen Informationen darstellen. Der Webshop etwa muss über eine Schnittstelle zur Kundendatenbank verfügen, und das interne Zeitbuchungssystem verwaltet

zwangsläufig zumindest einen Teil der Personaldaten.

Dieser Brückenfunktion wegen sind Webapplikationen durchaus lohnende Ziele für Angreifer mit verschiedenen Interessen. Darunter können Spione sein, die Betriebsgeheimnisse ausforschen möchten, aber auch Diebe von Identitätsinformationen oder Saboteure. Damit sind also alle drei Standard-Schutzziele der Informationssicherheit betroffen: Vertraulichkeit, Verfügbarkeit und Integrität.

Dass die erwünschte Sicherheit nicht leicht herzustellen ist, liegt dabei nicht allein an der primären Ausrichtung der Webapplikationen auf eine einfache Kommunikation der Anwender mit internen Ressourcen. Vielmehr kommt erschwerend dazu, dass diese Anwendungen oft Eigenentwicklungen sind, die nicht in größerem Umfang auf Sicherheitslücken getestet

und entsprechend optimiert werden. Darüber hinaus verfügen die Hintergrund-Datenbanken als Systeme für den internen Betrieb nicht immer über ausgefeilte Schutzmechanismen.

Web Application Firewalls (WAF) stellen ein bewährtes Mittel dar, auch in dieser Situation die Informationssicherheit auf ein akzeptables Niveau zu heben. Sie verlagern den Schutz auf eine Ebene vor der eigentlichen Webanwendung, um deren Konzeption und Betrieb von den hohen Sicherheitsanforderungen zu entlasten. WAF-Systeme inspizieren die Datenströme von und zur Webapplikation und reagieren, wenn sie darin Sicherheitsrisiken erkennen – etwa Eingaben, die auf Manipulationsversuche schließen lassen, oder unbeabsichtigt ausgehende Informationen. Web Application Firewalls existieren als Servermodule, klassische Softwaresysteme, Hardware-Appliances und in jüngerer Zeit auch als virtuelle Appliances.

Auf den ersten Blick mag es inkonsequent erscheinen und nach „Bastelei“ aussehen, den Schutz in eine zweite Instanz zu verlagern, statt die Webapplikationen selbst optimal zu härten. Organisatorisch und personell aber hat dies durchaus Vorteile: Die Anwendungsentwickler können sich bei diesem Kon-

strukt weiter auf die Funktionsfähigkeit konzentrieren und die Sicherheitsverantwortlichen auf den Bereich Security. Außerdem lässt sich ein spezialisiertes und standardisiertes Sicherheitssystem vergleichsweise leicht und schnell und mit der Unterstützung des Anbieters auf neue Bedrohungen wie aktuelle Hacker-Tricks einstellen, während eine derartige Modifikation bei einer komplexen Webapplikation erheblich aufwendigere Eingriffe erfordern würde.

Filter oder Stellvertreter

WAF-Systeme haben mit üblichen Firewalls wenig zu tun. Eine klassische Firewall regelt, über welche Ports von ihr geschützte Systeme erreicht werden können, und überwacht die IP-Adressen der Kommunikation. Typische Angriffe auf Webapplikationen finden aber grundsätzlich über legitime *http*- und *https*-Verbindungen statt, also über bereits explizit freigegebene Kommunikationswege. Web Application Firewalls müssen deshalb auf der Anwendungsebene (OSI-Schicht 7) die Datenströme auf ihren Inhalt hin kontrollieren und haben somit eher eine Filterfunktion. Um diesen Zweck zu erfüllen, können sie sich auf unterschiedliche Art in die Verbindung



9.990,- €
inkl. 12 Monate
Security Updates

Greenbone Security Manager Schwachstellenanalyse für Ihr Netzwerk

- Erkennt über 21.000 Schwachstellen
- BSI-Grundschutzkatalog und PCI-DSS Überprüfung
- Automatisierte Überwachung der Security Compliance
- Konfigurierbare Scanpläne und umfangreiche Reports



7.490,- €
inkl. 12 Monate
Energize Updates

Barracuda WAF 360 Web Application Firewall

- Schutz vor SQL-Injections, Cross-Site-Scripting
- Website Cloaking, Response Control
- HTTP/HTTPS/FTP Protocol Validation
- SSL Offloading, PCI-DSS Compliance-Checks

Security Consulting Audits, Konzeptionen, ISMS Aufbau

- ISMS und Security Audits auf ISO 27001 Basis
- Security Konzeptionierung und Implementierung
- Kurz- und Langzeitprojektunterstützung

solvotec
IT-Services GmbH

Heesfeld 1a | 38112 Braunschweig
Tel.: +49 (0) 531 / 60 94 97 40
www.solvotec.de | info@solvotec.de



Preise inkl. MwSt.
Bestellbar unter:
<https://shop.solvotec.de>
vertrieb@solvotec.de

zwischen Browser und Webapplikation einklinken: als WAF im Bridge-Modus oder als Reverse Proxy.

WAFs im Bridge-Modus sind wie ein Switch in die Datenleitung eingebunden und lesen die Kommunikation mit. Der Anwender greift in diesem Fall weiterhin direkt auf die Webapplikation zu. Findet eine Bridge-WAF verdächtige Kommunikation, kann sie zumindest Alarm schlagen und Kommunikationsströme blockieren. Ein Reverse Proxy dagegen bricht die Verbindung zur Anwendung auf. Bei diesem häufiger gewählten Konzept kommuniziert der Anwender, ohne dies zu merken, zunächst nur mit dem WAF-System – seine *http*- oder *https*-Verbindung endet dort.

Von der Webapplikation nimmt das WAF-System die Webseiten mit den zu transferierenden Informationen entgegen und präsentiert sie dem Anwender. Zugleich analysiert es den eingehenden Datenstrom und damit die Eingaben des Anwenders und reicht nur geprüfte und für risikofrei befundene Eingabedaten und Uploads an die Applikation weiter.

Schwarze und weiße Listen

Ein zentraler Schutzmechanismus, auf den nahezu alle WAF-Systeme bauen, ist die gleichzeitige Arbeit mit White- und Blacklists. Eine weiße Liste dokumentiert, welche Eingaben bei der Arbeit mit einer Webapplikation erlaubt sind – in welche Felder etwa Zahlen welcher Größe und welchen Formats eingegeben werden, wo nur Text erlaubt ist, welche URLs aufgerufen werden können und so weiter. Dies verhindert, dass ein böswilliger Anwender Systeme durch unerwartete Eingaben in einen instabilen Betriebsmodus bringt oder beispielsweise Programmcode einschleust.

Über Whitelists lässt sich also jede Eingabe unterbinden, die

nicht explizit zugelassen ist. Dazu allerdings ist eine durchaus aufwendige Abstimmung der WAF auf die zu schützende Applikation notwendig. Moderne Systeme können dazu in einem Lernmodus arbeiten. Darin speichern sie über einen gewissen Zeitraum legitime Kommunikationsströme und leiten daraus selbst ab, was Anwender beispielsweise in bestimmte Felder eingeben dürfen und was nicht.

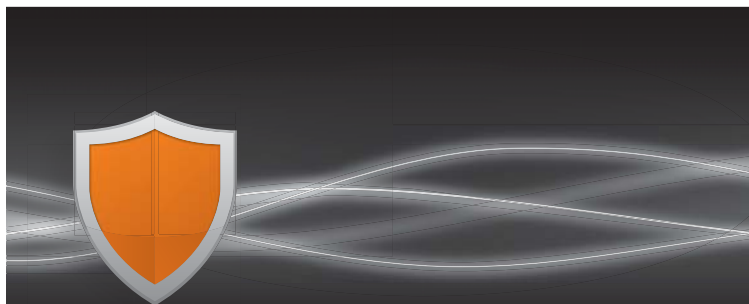
Wichtig ist dies vor allem, wenn WAF-Systeme auch für häufiger modifizierte Webanwendungen eingesetzt werden sollen. Neueste Systeme gehen hier noch einen Schritt weiter: Sie sind in der Lage, Regeln für die legitime Kommunikation mit Webanwendungen dynamisch zu pflegen und Werte- oder Zeichenmengen, die für Eingaben zugelassen sind, flexibel mittels regulärer Ausdrücke zu beschreiben.

Kommen reguläre Ausdrücke zum Einsatz, müssen nicht erst alle zugelassenen Zeichenketten oder Zahlenwerte vom Administrator eingegeben oder von der WAF „erlernt“ werden. Ein wichtiges Qualitätskriterium, das für alle WAF-Systeme mit Whitelists gilt, ist eine möglichst geringe Zahl von „False Positives“ – also fälschlich zurückgewiesener Anwenderkommunikationen – während und nach der Konfigurations- oder Lernphase.

Blacklists unterbinden lediglich Eingaben, die als Teil von Angriffsmustern bereits bekannt sind, etwa als Teil einer SQL-Injection oder des Cross-Site Scripting. Die schwarzen Listen können wie die Pattern-Dateien von Virenschutz-Systemen und die Angriffsmuster-Dateien von Intrusion-Detection-Systemen von den Herstellern der Systeme gepflegt werden.

SSL-Inspektion und Authentifizierung

WAF-Systeme im Reverse-Proxy-Modus lassen sich so einsetzen, dass sie für SSL-Ver-



ASTARO SECURITY GATEWAY ALL-IN-ONE PROTECTION

Alle relevanten Sicherheitsfunktionen unter einer einheitlichen Managementoberfläche. Abgerundet wird das vollständig modular aufgebaute Produktportfolio der Astaro durch starke Management und Reporting Werkzeuge, die auch ein Managed-Services Modell unterstützen.

FLEXIBEL EINFACH

Modulares Lizenzmodell. Komfortable Installation und Administration.

EFFIZIENT

Minimaler Ressourcenaufwand.

Weltweit über 56.000 Installationen.



**30 Tage
kostenlos testen**
www.astaro.com/testen

KOMMERZIELLE UND FREIE WAFs

Anbieter	Produkt	URL
Applicure	dotDefender Web Application Firewall	www.applicure.com
Armorlogic	profense WAF	www.armorlogic.com
art of defence	hyperguard	www.artofdefence.com
Astaro	Web Application Firewall	www.astaro.com
Barracuda Networks	Barracuda Web Application Firewall	www.barracudanetworksag.com
Breach Security	WebDefend	www.breach.com
Cisco	ACE Web Application Firewall	www.cisco.com/web/DE
Citrix	NetScaler Web Application Firewall	www.citrix.com
Deny All	rWeb	www.denyall.com
Ergon	Airlock	www.ergon.ch
F5	BIG-IP Application Security Manager	www.f5.com
Fortinet	Fortiweb	www.fortinet.com
Imperva	SecureSphere Web Application Firewall	www.imperva.com
Radware	AppWall	www.radware.com
secunet	Web Application Firewall	www.secunet.com
SONICWALL	Web Application Firewall	www.sonicwall.com
United Security Providers	USP Secure Entry Server	www.united-security-providers.ch
Zeus	Web Application Firewall	www.zeus.com
IronBee	Web Application Firewall (Open Source)	www.ironbee.com
ModSecurity	ModSecurity (Open Source)	www.modsecurity.org
WebCastellum	Web Application Firewall (Open Source)	www.webcastellum.org

Die Übersicht erhebt keinen Anspruch auf Vollständigkeit.

bindungen vom Browser des Anwenders zur Webanwendung den Endpunkt darstellen. Die Web Application Firewall entschlüsselt dann den Datenstrom, der vom Browser des Anwenders kommt, und verschlüsselt, was die Webapplikation zum Anwender hin liefert. Damit dies funktioniert, installiert der Verantwortliche auf einer entsprechend eingerichteten WAF das Server-Zertifikat für die geschützte Applikation.

Sinnvoll ist dieses Konzept, weil das Sicherheitssystem auf diese Weise vollen Einblick in die verschlüsselte Kommunikation erhält. Ob auch die Verbindung zwischen dem WAF-System und der Webapplikation verschlüsselt werden muss, hängt davon ab, wo die Systeme installiert sind – in einem gut geschützten internen Netzsegment kann diese Verbindung offen bleiben. Gängig ist es außerdem, WAF-Systeme zur Authentifizierung der Anwender einer Webapplikation

heranzuziehen. Je nach Produkt sind dabei alle bekannten Methoden der Benutzererkennung möglich.

Eine weitere Sicherheitsstrategie, die moderne WAF-Systeme bieten, ist die Verschleierung von Informationen

über die interne Struktur einer Webapplikation. Die URLs beispielsweise, die im Code der HTML-Seiten einer Applikation enthalten sind, kann eine Web Application Firewall gegen verschlüsselte Varianten austauschen, bevor sie die Seiten

etwa im Reverse-Proxy-Modus an den Anwender weiterreicht.

Lässt sich dieser den Quellcode einer solchen Seite anzeigen, findet er in den eingebetteten Links anstelle lesbarer Dateinamen und -typen nichtsagende Zeichenketten. Er erhält somit keine Informationen über Ordnerstrukturen, IP-Adressen und Dateien, die die Webanwendung verwendet. Akzeptiert außerdem eine WAF als Eingabe grundsätzlich nur die von ihr selbst verschlüsselten Links, hat ein Angreifer auch keine Möglichkeit, über manipulierte Webcode direkt Dateien oder Ressourcen aufzurufen, deren Existenz er auf dem Server der Webapplikation vermutet („Forceful Browsing“).

Ähnlichen Zwecken dient es, wenn eine WAF Fehlermeldungen von Webservern oder Applikationen abfängt, statt sie den Anwendern weiterzureichen. Solche Meldungen enthalten technische Interna, die ein Hacker missbrauchen könnte. Auch Cookies, die eine Webanwendung auf dem System des Anwenders setzt, lassen sich durch Verschlüsselung gegen Manipulationen sichern. (sf/ur)

*Bettina Weßelmann
ist freie Journalistin.*

In iX extra 8/2011

Storage: SaaS – Public und Private Cloud Storage

Die Aufregung um Cloud Computing hat deutlich den Hype-Gipfel überschritten und nähert sich allmählich der Nullgrenze. Unbestritten ist, dass mit fein abgestimmter Ressourcenzutei-

lung und präzisen Abrechnungsmethoden viele Speicheranforderungen bedarfsgerecht von außen erfüllt werden könnten. Doch was für File Services möglich erscheint, sieht bei

Block-Storage schon wieder ganz anders aus. Ein Situationsbericht.

Erscheinungstermin:
21. 07. 2011

DIE WEITEREN IX EXTRAS:

Ausgabe	Thema	Erscheinungstermin
09/11 Networking	Hochverfügbares Server-Hosting	18. 08. 11
10/11 Embedded Systems	Industrietaugliche I/O-Komponenten	15. 09. 11
11/11 Security	Malware-Trends – die Professionalisierung des Bösen	13. 10. 11