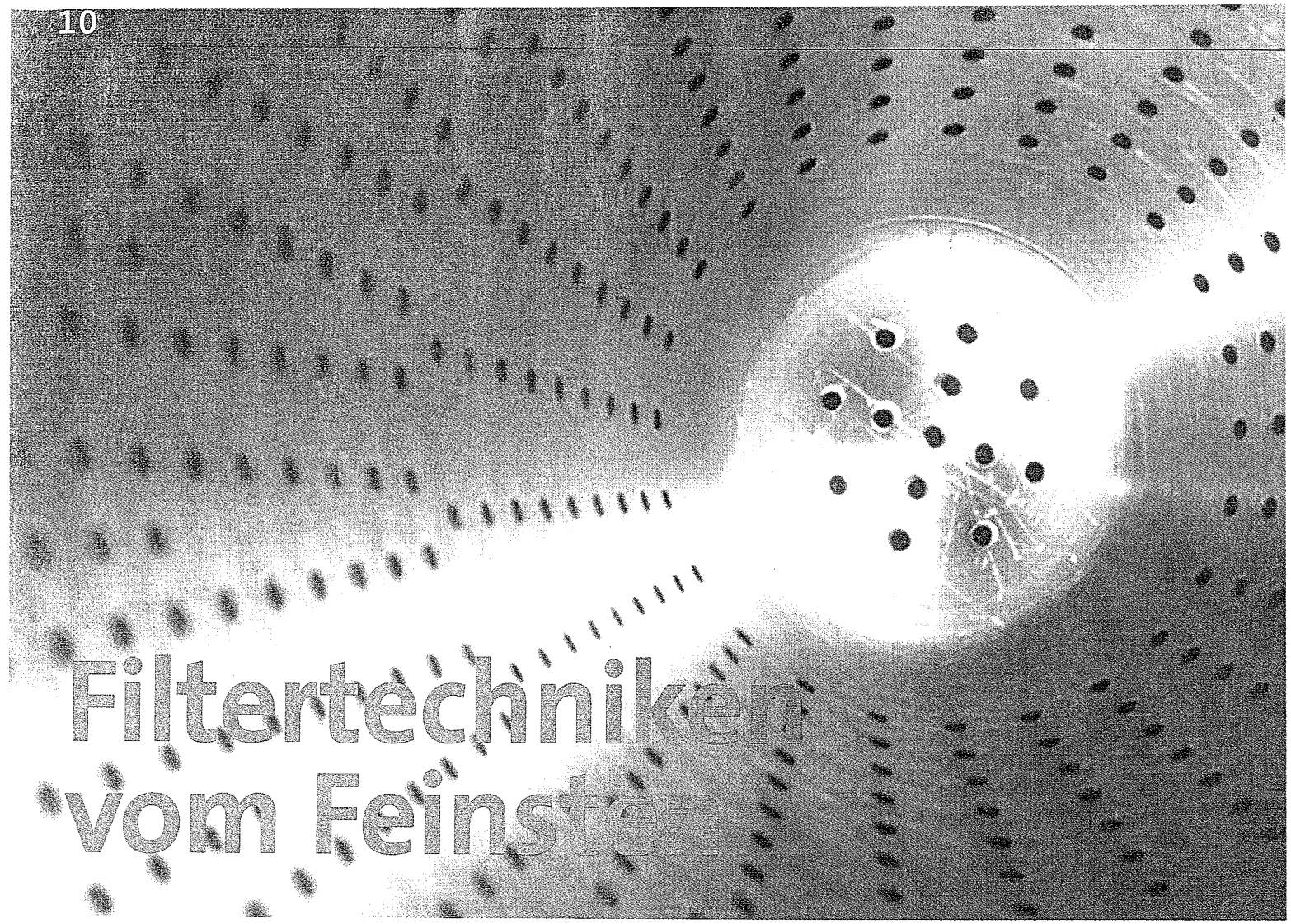


Filtertechniken vom Feinsten

Bei Webanwendungen können die unvermeidlichen Programmierfehler besonders desaströs werden. Schutzmechanismen wie Web Application Firewalls filtern Schmutzcode aus. Eine glatte Lösung für alle Wünsche wird es allerdings wohl nie geben.

von jürgen höfling |
juergen.hoefling@informationweek.de

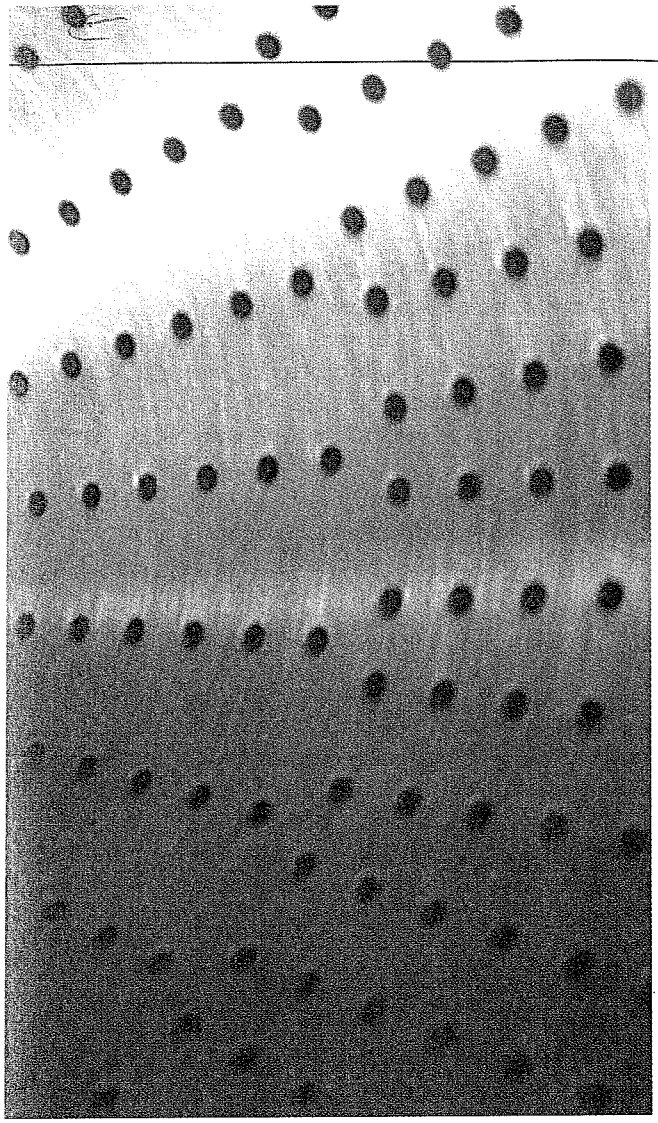
Die digitale Ökonomie hat Hochkonjunktur. Immer mehr Anwendungen sollen webfähig und damit Teil eines weltweiten Selbstbedienungsladens werden. Aber mit der Selbstbedienung ist das so eine Sache. Durch die »Webifizierung« werden Programme nicht nur öffentlich bedienbar, sondern auch klammheimlich angreifbar. Auf den ersten Blick scheinen die Schattenseiten der Selbstbedienung behebbar zu sein. Man muss einfach böse Absichten vorherahnen und durch geschickte Programmierung vereiteln. Eine stetige Codekontrolle sollte eventuell doch entstandene Fehler schnell eliminieren.

Doch solche Gedanken sind nur graue Theorie. Banken zum Beispiel haben in der Regel 600 bis 1000 verschiedene Anwendungen in Betrieb, die auf insgesamt 80 bis 100 Datenbank-Systeme zugreifen und zwischen sechs und zehn Middleware-Systeme erfordern, um reibungsfrei betrieben werden zu können. Allein diese Zahlen deuten an, dass vermutlich die Qualität mit der Quantität nicht Schritt halten kann. Mehr noch: »Bei vielen großen Webprojekten, beispielsweise bei der Anbindung von gekauften SAP-Anwendungen, kann man den Code schon deshalb nicht prüfen, weil man nicht an ihn herankommt«, sagt Dr. Georg Heß, Geschäftsführer der Firma »Art of Defence« in Regensburg.

Statische und dynamische Komponenten

Das Regensburger Unternehmen ist einer der Anbieter von Schutzsoftware, die Lücken in Webanwendungen aufspürt und neutralisiert. Diese unter dem etwas unglücklichen Begriff »Web Application Firewall« (WAF) angebotenen Instrumente blockieren beispielsweise Versuche, in Browser-Eingabefenster Code einzugeben, der Systeme im Hintergrund (Datenbanken) manipuliert. Oder sie verhindern, dass sich jemand auf eine fremde http-Session »durch das Kapern von Cookies und ähnlichem aufschaltet«. Gängige Schutzinstrumente sind auch das Erstellen von Positiv- und Negativlisten, in denen aufgeführt ist, was erlaubt

Foto: Demirman_photocase



»Auch Konstrukte mit einem dynamischen Lernmodus können in manchen Kontexten Probleme bereiten.«
Stefan Strobel, Geschäftsführer von Cirosec

»Bei vielen großen Webprojekten, beispielsweise bei der Anbindung von gekauften SAP-Anwendungen, kann man den Code schon deshalb nicht prüfen, weil man nicht an ihn herankommt.«
Dr. Georg Heß, Geschäftsführer von »art of defence«

was verboten ist. Auch die Verschlüsselung von Webadressen, SSL-Terminierung und SSL-Dechiffrierung sowie spezielle Authentisierungsverfahren gehören zu den Schutzmechanismen. Im Grunde versuchen die beschriebenen Schutzsysteme die Semantik der Applikation nachzuempfinden, also zu verstehen, was die Applikation will und damit gleichermaßen aufzudecken, was sie nicht wollen darf.

Dass dies ein ambitioniertes Unterfangen ist und allenfalls zum Teil gelingen kann, wird jeder einsehen. Webanwendungen sind vielfältig und mit vorweg definierten Positiv- oder Negativlisten wird man vielen dieser Anwendungen nicht gerecht werden können.

Schon von Anfang an enthielten deshalb einige Web Application Firewalls neben den statischen, also vordefinierten Richtlinien, auch eine dynamische Komponente (so das Produkt von Sanctum, das heute samt Firma vom Markt verschwunden ist). De facto handelt es dabei um einen Lernmodus, bei dem quasi automatisch das tatsächliche Verhalten eines berechtigten Nutzers mit bestimmten Anwendungen analysiert und daraus resultierende Gebote oder Verbote dem bestehenden statischen Regelsatz hinzugefügt werden.

Lernmodi können Probleme bereiten

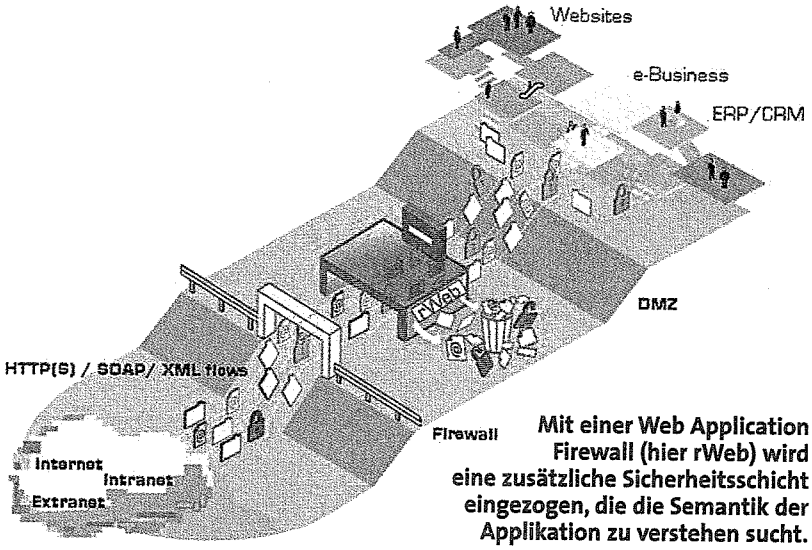
Dass das Schlagwort »Lernmodus« im Leistungskatalog eines Produkts durchaus noch wenig besagt, darauf weist Stefan Strobel hin, Geschäftsführer des Heilbronner Sicherheitsspezialisten Cirosec, der sich schon seit Jahren mit den verschiedenen WAF-Produkten beschäftigt. Je nach Art der zu schützenden Anwendung benötigt man in der Praxis verschiedene Lernmodi. Produkte, die gänzlich ohne eine dynamische Komponente, etwa zur Sessionverfolgung, arbeiten, sieht Strobel als nicht zeitgemäß und wenig zielführend für viele Problemlösungen an: »Bei dem quelloffenen Tool mod-security für den Apache Webserver beispielsweise würde ich nicht von einer Web Application Firewall sprechen, weil fast alles händisch konfiguriert werden muss. Damit lassen sich viele der heutigen Angriffsszenarien nicht abwehren und der Betriebsaufwand ist immens«, sagt Strobel.

Im Übrigen betont der Cirosec-Geschäftsführer, dass auch Konstrukte mit einem dynamischen Lernmodus in manchen Kontexten stumpf bleiben beziehungsweise Probleme bereiten: »Dynamische Verfahren lassen beispielsweise bestimmte Handlungen nur zu, wenn vorher schon andere Seiten aufgerufen wurden. Das kann dann dazu führen, dass ein gesetztes Bookmark, das Sie vierzehn Tage später aufrufen wollen, von der Web Application Firewall als nicht erlaubt eingestuft wird. Und auch der Aufruf von Suchmaschinen aus kann zu Problemen führen. Ein gutes Produkt muss deshalb mehrere Lernmodi beziehungsweise Lösungswege anbieten.«

Teilweise geringe Einsatzerfahrungen

Die Zwecke einer WAF können sehr allgemein mit »Sicherung von transaktionsorientierten Webanwendungen« angegeben werden. Auf diese Definition können sich sicher alle Anbieter einigen. Es fragt sich nur, ob eine solche Definition dem Anwender→

Fotos: Cirosec, Art of Defence



Quelle: Deny All

Mit einer Web Application Firewall (hier rWeb) wird eine zusätzliche Sicherheitsschicht eingezogen, die die Semantik der Applikation zu verstehen sucht.

bei der Auswahl konkreter Produkte am Markt viel bringt. Denn tatsächlich sind die »technischen Ansätze« der einzelnen Produkte sehr verschieden und die Aussagen der einzelnen Protagonisten über den Konkurrenten zeugen nicht selten von purer Unwissenheit oder sie fälschen bewusst. Erschwerend kommt für den Anwender, der vor der Qual der Wahl steht, hinzu, dass über einige Produkte nur relativ wenige Einsatzerfahrungen vorliegen. Einer dieser »Unbekannten« ist das Produkt Airlock der schweizerischen Firma Visonys (früher: Seclusion). Man könnte aber auch Hyperguard von Art of Defence oder F5 nehmen. Letztere sind zwar in der Lastverteilung und in der Netzverkehrsbeschleunigung gut im Geschäft, in der WAF-Ecke haben sie zumindest in Deutschland nie ein Bein auf die Erde gekriegt. Hyperguard und Airlock wiederum sind insgesamt noch zarte Pflänzchen. Beide haben einige neue technische Ansätze. Bei Airlock beispielsweise ist die digitale Signierung der URL interessant, für Anwendungen, die vom Nutzerkreis her sinnvoll eingrenzbar sind, sicher auch die vorgelagerte Authentisierung. Durch die URL-Signierung muss eine zulässige Webadresse nicht im Hauptspeicher gehalten werden, sondern wird je nach Signatur als gültig oder ungültig erkannt.

Qual der Wahl

Wir haben hier leider nicht den Platz, auf die speziellen Vorzüge und Nachteile der einzelnen Produkte einzugehen. Überdies hat niemand in der Branche, auch so erfahrene Leute wie Stefan Strobel, einen wirklichen Gesamtüberblick, sodass er alle Systeme »gerecht« beurteilen könnte. Auch stehen legitime Geschäftsinteressen oft einer solchen abstrakten Gerechtigkeit im Wege. In der Tabelle auf dieser Seite wollen wir wenigsten alle uns bekannten Protagonisten namentlich erwähnen und – mit aller Vorsicht – mit einer beschreibenden Bemerkung versehen, die nicht als Schulnote aufgefasst werden sollte. Letztlich kann nur ein längerer Praxiseinsatz zeigen, ob die WAF im Webshop Ordnung schafft und Schmutzcode rigoros aussiebt. ■

Schutzmechanismen für Webanwendungen

Produkt	Hersteller	Charakteristik
NC1100, NC2000	Barracuda (ex Netcontinuum)	eingeführtes Produkt, mittlerweile auf Barracuda-Boxen portiert
Defiance	Protegrity (ex Kavado)	gegen den Trend ein reines Software-Produkt, keine Beschleunigung, keine Lastverteilung
Traffic Shield	F5 (ex Magnifire)	zusammen mit dem Lastverteiler und Beschleuniger interessantes Produkt; wenig Anwender in Deutschland
rWeb	Deny All	Hardware-Appliance, kooperiert mit Herstellern wie Corisecio in Darmstadt in puncto eines kompletten Webservice-Schutzes
AirLock	Visonys	Software-Appliance; URL-Verschlüsselung, Authentisierungs-Komponente. Wenige Installationen in Deutschland
Citrix Application Firewall	Citrix (ex Teros)	in bestehende Citrix Netscaler-Architektur (Lastverteilung und Beschleunigung) integriert
SecureSphere	Imperva (ex Webcohort)	eingeführtes Produkt, besonderes Augenmerk auf Schutz der Backend-Systeme
Mod-security	Open Source	kein Lernmodus (fast alles muss manuell in eine Konfig-Datei eingetragen werden). Kein reifes WAF-Produkt
Hyperguard	Art of Defence	Plug-In in Webserver. Firma kooperiert mit gut etablierten Netzwerk-Firewall-Herstellern wie Genua, insofern auch Appliance
Reactivity	Cisco	eher nur ein XML-Filter. Anwendungen in Maschine-zu-Maschine-Kommunikation
DataPower	IBM	eher nur XML-Filter