

Hintergrundartikel

Konvergenz bei Webapplikationssicherheit

Die intelligente Kombination von Schutzmechanismen ist entscheidend bei der Sicherheit

*Von Cyrill Osterwalder**

Angriffe auf Webapplikationen erfolgen heute nicht mehr nach dem Zufallsprinzip, sondern sind sehr zielgerichtet. Dies macht den fortwährenden und umfassenden Schutz von Web-Applikationen und -Diensten unumgänglich und dringlicher denn je. Nur eine ausgereifte Lösung, welche verschiedene Sicherheitsmassnahmen kombiniert, kann selbst unbekannte Angriffsmethoden frühzeitig erkennen, verhindern und so den Schutz nachhaltig gewährleisten.

In vielen Unternehmen werden die Massnahmen im Bereich Webapplikationssicherheit aus historischen oder Hersteller-getriebenen Gründen immer noch zu separiert behandelt. Dies führt unmittelbar zu unnötiger Komplexität und weniger Effektivität. Um auf applikatorischer Ebene die richtigen Sicherheitsentscheidungen fällen zu können, müssen verschiedene Informationen zum richtigen Zeitpunkt am richtigen Ort verfügbar sein. Durch punktuelle, verzettelte Massnahmen in einzelnen Teilbereichen wird dies erheblich erschwert. Damit erhöht sich automatisch die Chance für den Angreifer. Im Fall von Web Application Firewalls gilt dies insbesondere für die Themen Authentisierung, Zugriffskontrolle, SSL-Terminierung, Filterung, Protokollvalidierung und Monitoring.

Frage nach dem Wer und Was steht im Zentrum

Ähnlich wie bei physischen Sicherheitsmassnahmen am Flughafen, wo Ticket, Pass, Gepäck und Personen überprüft werden, bevor sie ins Flugzeug gelangen, ist es bei Webapplikationssicherheit entscheidend, sich mit beiden Fragen – also

erstens, wer jemand ist, und zweitens, was er tut – vorgelagert zu beschäftigen. Im Fall einer Web-Applikation oder -Umgebung mit registrierten Benutzern sollte die vorgelagerte Authentisierung im Vordergrund stehen. Für öffentlich zugängliche Web-Applikationen und -Seiten hingegen ist die Filterung von Protokollen, Anfragen und Daten am wichtigsten. Da heutige Webapplikationen meistens beides beinhalten, sind technische Lösungen gefragt, die beide Themen effizient und umfassend abdecken.

Das einfachste Beispiel sind Applikationen mit registrierten Benutzern, die sich authentisieren müssen, wie dies beispielsweise beim E-Banking oder Portalen von Versicherungen, Behörden oder Lieferanten üblich ist. Die Login-Seite ist öffentlich zugänglich und dementsprechend von überall her angreifbar. Zum Schutz der Login-Seite sind deshalb strenge Filterkriterien von entscheidender Bedeutung. Für den Rest der Applikation hingegen ist es viel wichtiger, dass wirklich nur korrekt authentifizierte Benutzer überhaupt zugreifen dürfen. Diese zwei Herausforderungen lassen sich durch vorgelagerte Authentisierung und umfassende Filterung in einer Web Application Firewall (WAF) ideal kombinieren.

Vorgelagerte Authentisierung als integrierter Bestandteil im Sicherheitskonzept

Bei den meisten Unternehmen werden die Entscheidungen für die Art der Authentisierung aufgrund wirtschaftlicher und betrieblicher Gründe gefällt. Zudem gibt es bei mittleren und grösseren Unternehmen oft nicht nur eine einzige Art der Authentisierung, sondern verschiedene – also zum Beispiel starke Authentisierung für externen Zugriff, mittlere Authentisierung für internen Zugriff oder separate Variante für den B2B-Kanal.

Eine Web Application Firewall wie beispielsweise phion Airlock bietet die Möglichkeit, die Authentisierung vorgelagert zu erzwingen (Authentication Enforcement) und die Prüfung selbst an den jeweiligen Authentisierungsdienst zu delegieren. Dies geschieht völlig unabhängig von der konkreten Art der Authentisierungstechnologie. Es können verschiedenste Authentisierungsvarianten und Benutzerverzeichnisse parallel und flexibel

angesprochen werden, auch kundenspezifische IAMs (Identity Access Management).

Mit der vorgelagerten Authentisierung erreicht ein Unternehmen zwei grosse Vorteile: Erstens sind die Applikationen vollständig vor anonymen Zugriffen geschützt (das gilt für alle Ebenen wie TCP/IP, SSL, HTTP, Applikationsserver, Betriebssystem, Bibliotheken; Business-Logik und andere mehr). Somit sind Bedrohung und Angriffsrisiko für die authentisierten Applikationen um Dimensionen reduziert. Zweitens ist die einmalige Anbindung der Authentisierung an die WAF viel effizienter und flexibler. Das Unternehmen kann jederzeit über die Art der Authentisierung entscheiden, ohne dabei alle Applikationen anpassen zu müssen. Bei Bedarf kann zum Beispiel auf diese Art ein Single-Sign-On mit einer PKI-Lösung implementiert werden, ohne dass die damit geschützten Applikationen überhaupt etwas von der PKI-Lösung wissen müssen. Dieser Vorteil spart dem Unternehmen direkt Geld, erhöht die Flexibilität, weil neue Applikationen viel einfacher in die Umgebung integriert werden können, und steigert nachhaltig die Sicherheit.

Gleichzeitiges Monitoring profitiert von kombiniertem Ansatz

Eine zentrale WAF, die sich als sicherer Reverse Proxy sowohl um die Authentisierung als auch um die konsequente Filterung aller Anfragen und Daten kümmert, bietet den Unternehmen zu jeder Zeit alle relevanten Informationen darüber, WER in der gesamten Web-Umgebung WAS getan hat. So ist zum Beispiel bei einem getriggerten Whitelist-Filter innerhalb einer E-Banking-Session sofort auch ersichtlich, wer den auslösenden Request geschickt hat und was dieser Benutzer sonst auf der Applikations-Session getan hat.

Mit diesen Informationen, die nur bei einem kombinierten Ansatz von vorgelagerter Authentisierung, umfassender Filterung, SSL-Terminierung, sicherem Session Handling und weiteren Funktionen in dieser Qualität zur Verfügung stehen, gewinnen Sicherheitsverantwortliche Zeit und können proaktiv handeln.

Vorgelagerte Authentisierung in Kürze

Eine vorgelagerte Authentisierung verhindert, dass Webserver anonymen Verbindungen ausgesetzt sind. Auf diese Weise wird die Menge der potenziellen Angreifer bereits massiv reduziert und die Applikationen werden entlastet. Zudem ermöglicht die vorgelagerte Authentisierung eine zentrale Zugriffskontrolle getrennt von der Business-Logik. Dies erhöht die Sicherheit und reduziert gleichzeitig die Kosten. Nur authentifizierte und autorisierte Verbindungen werden auf die entsprechenden Applikationsserver zugelassen.

* Cyrill Osterwalder ist Experte für Webapplikationssicherheit und Senior Vice President Web Application Security bei der phion AG. Ausserdem ist er Mitglied des Web Application Security Consortium (WASC, www.webappsec.org) und erarbeitet dort Richtlinien und Kriterien für höhere Sicherheit von Webapplikationen.

Über phion:

Die phion AG ist einer der führenden europäischen Anbieter für Lösungen zum Schutz der Unternehmenskommunikation. Mit dem netfence-Produktportfolio bietet phion Lösungen für höchste Ansprüche an Verfügbarkeit, Sicherheit und Management. ‚phion netfence‘ adressiert konsequent sämtliche sicherheitsrelevanten Aspekte: Von der Verteidigung am Perimeter über die sichere und hochverfügbare Anbindung von Filialen bis hin zur Abwehr gefährlicher Inhalte und dem Schutz des internen Netzwerks. Webapplikationen wie e-Banking-Plattformen und Web Services werden von ‚phion Airlock‘ vor Angriffen und Missbrauch geschützt.

Alle phion-Produkte verfügen zudem über ein zentrales Management und zeichnen sich durch besonders günstige TCO aus.

phion ist im mid market Segment der Wiener Börse gelistet (Kürzel: PHIO) und hat seinen Hauptsitz in Innsbruck, Österreich. Zu den Kunden von phion zählen namhafte, international tätige Unternehmen aus allen Branchen.

Weitere Informationen stehen unter: <http://www.phion.com> zur Verfügung.