

In vielen Unternehmen werden die Maßnahmen im Bereich Web-Applikationssicherheit aus historischen oder herstellergetriebenen Gründen immer noch getrennt voneinander behandelt. Dies führt unmittelbar zu unnötiger Komplexität und weniger Effektivität. Um auf Applikations-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 Authentifizierung, Zugriffskontrolle, SSL-Terminierung, Filterung, Protokollvalidierung und Monitoring.

Ähnlich wie bei physischen Sicherheitsmaßnahmen am Flughafen, wo Ticket, Pass, Gepäck und Personen überprüft werden, bevor sie ins Flugzeug gelangen, ist es bei Web-Applikationssicherheit entscheidend, sich mit zwei 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 Authentifizierung im Vordergrund stehen. Für öffentlich zugängliche Web-Anwendungen und -Seiten hingegen ist die Filterung von Protokollen, Anfragen und Daten am wichtigsten.

Da heutige Web-Applikationen meistens beides beinhalten, sind technische Lösungen gefragt, die beide Themen effizient und umfassend abdecken. Eine Web Application Firewall (WAF) wie beispielsweise Airlock von Phion bietet die Möglichkeit, die Authentifizierung vorgelagert zu erzwingen (Authentication Enforcement) und die Prüfung selbst an den jeweiligen Authentisierungsdienst zu delegieren. Dies geschieht völlig unabhängig von der konkreten Art der Authentifizierungstechnologie. Es können verschiedenste Varianten und Benutzerverzeichnisse parallel und flexibel angesprochen werden, auch kundenspezifische IAM (Identity Access Management).

Mit der vorgelagerten Authentifizierung erreicht ein Unternehmen zwei 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 authentifizierten Applikationen entscheidend reduziert. Zweitens ist die einmalige Anbindung der Authentifizierung an die WAF viel effizienter und flexibler. Das Unternehmen kann jederzeit über die Art der Authentifizierung entscheiden, ohne dabei alle Applikationen anpassen zu 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.