Airlock Web Application Firewall 7.2 integriert den Threat Intelligence Service von Webroot

Ergon Informatik veröffentlicht die Version 7.2 der beliebten Airlock WAF. Ein Ausbau des API Gateways und eine Partnerschaft mit Webroot erhöhen die Sicherheit für Anwender deutlich und vereinfachen die Handhabung

Zürich, 21. Mai 2019 – Ergon Informatik AG, ein Schweizer Anbieter von IT-Sicherheitslösungen, aktualisiert seine beliebte Airlock Web Application Firewall (WAF). Das Update 7.2 konzentriert sich besonders auf den Ausbau des API Gateways, um die Sicherheit weiter zu steigern. Zu den Maßnahmen gehört eine Partnerschaft mit dem Sicherheitsanbieter Webroot. Die Airlock-Sicherheitslösungen werden mit dem BrightCloud Threat Intelligence Service ausgestattet, um gefährliche Clients in Echtzeit erkennen und blockieren zu können. So will Airlock der wachsenden Anzahl global koordinierter Angriffe und dem zunehmenden Einsatz von Bot-Netzen entgegenwirken.

Der BrightCloud Threat Intelligence Service ist ein IP-Reputation Service. Er liefert globale Bedrohungsdaten höchster Güte in Echtzeit an die WAF. Alle verdächtigen IP-Adressen landen auf einer Blacklist. Beispiele für verdächtiges Verhalten sind, wenn Angriffe über sie durchgeführt werden, sie zu Botnetzen gehören, mit Malware infiziert sind, Spam verschicken, Phishing-Angriffe ausführen oder über das TOR-Netzwerk und andere Proxys kommunizieren. Die Prüfung passiert automatisch und im Hintergrund, weil Airlock als OEM Integrator der Webroot-Lösung fungiert und somit der Kunde nicht zusätzlich Hand anlegen muss. Die IP Reputation-Daten werden laufend aktualisiert. Auf Knopfdruck können zusätzlich bösartige IP-Adressen selbstständig blockiert werden, bevor sie überhaupt auf geschützte Services zugreifen können.

Webroot kategorisiert schädliche IP-Adressen außerdem nach bestimmten Kriterien, um die Art der Angriffe übersichtlich darstellen zu können. Das vereinfacht die Überwachung der Netzwerke durch die IT-Sicherheitsverantwortlichen eines Unternehmens ungemein, weil angezeigt wird, für welche Art von Angriff die jeweilige IP bereits bekannt ist. „Die Infos zu IPs können im cIAM ausgewertet und bei Zugriffskontrollen berücksichtigt werden, z.B. für Adaptive Authentisierung. Damit ist eine einfache, zentrale Verwaltung der IP-Adresslisten für die Zugriffssteuerung der Airlock WAF 7.2 möglich und das Produkt auf alle Szenarien vorbereitet: Eigene IP Blacklists, von Drittanbietern bezogene Sperrlisten, oder abgebildete, interne Netzwerk-Bereiche“, erklärt Dr. Martin Burkhart, Head of Product Management bei Airlock.

Das IP-List Management erhält zudem ein neues, wesentlich einfacher gestaltetes Werkzeug zur Verwaltung, das die vorhandenen Threat Intelligence Feeds von Airlock optimal ergänzt. Es erlaubt die Integration vorhandener IP-Blacklists umstandslos und in wenigen Arbeitsschritten. „Hat man bereits Webroot im Einsatz und Listen definiert, können diese einfach integriert werden. Das gilt auch für andere Listen, die zum Beispiel vom Branchenverband der Banken erstellt werden. Mit wenig Aufwand können diese von unserem Secure Access Hub übernommen“, führt Burkhart aus. Zudem erlauben die neuen Funktionen der Version 7.2 eine einfache Erfassung der IP-Listen mittels CIDR Notation. Die IP-Listen können dann für Whitelist- und Blacklist-Regeln, aber auch für Ausnahmen, wie beim Schutz vor DoS-Attacken, verwendet werden. Über REST API können die IP-Listen automatisch aktualisiert werden. Das ist auch nötig, „da Cyber-Kriminelle täglich mehr als 100.000 IP-Adressen für bösartige Aktivitäten nutzen. Daher sind Echtzeit-Bedrohungsinformationen, die automatisch unerwünschten Datenverkehr blockieren und sich selbst gegen eingehende Bedrohungen schützen, wichtiger denn je“, erläutert Michael Neiswender, Vice President of Worldwide OEM Sales bei Webroot.

Die API Gateway-Funktion der Airlock Sicherheitslösung wird außerdem um ein fortschrittliches Access Control Feature basierend auf JSON Web Tokens (JWT) erweitert: Zusätzlich zum OpenAPI Support, wird das API Security Gateway künftig Tokens für Access Control-Entscheidungen auswerten können. Das macht Airlock API, eine neue Komponente des Airlock Secure Access Hubs, bereit für die Zukunft, denn viele Apps und moderne Anwendungen nutzen diese Tokens zur Zugriffsregelung. Konkret heißt das: Die JSON Web Tokens (signiert, verschlüsselt oder beides) können bezüglich Gültigkeit und Signatur validiert werden. Restriktionen auf Claims können überprüft und sogar Zugriffsrollen aus verifizierten Tokens extrahiert werden. Der Zugriff lässt sich somit auch feingranular anhand der verwendeten HTTP-Verben kontrollieren, um anonymen Clients nur Lesezugriff auf eine API zu erlauben. Künftig ist also nicht nur die Definition fester Rollen für den kontrollierten Zugriff auf die APIs möglich, sondern eine feingranulare Einrichtung: Verschiedene Rollen in unterschiedlicher Zahl je Funktion können für Identitäten festgelegt werden, um den Zugriff zu regeln.

Über Airlock – Security Innovation by Ergon Informatik AG

Der Airlock Secure Access Hub vereint die wichtigen IT-Sicherheitsthemen der Filterung und Authentisierung zu einem gut abgestimmten Gesamtpaket, das Maßstäbe in Sachen Bedienbarkeit und Services setzt. Der Secure Access Hub deckt alle wichtigen Funktionen der modernen IT-Sicherheit in diesem Bereich ab: von einer durch Fachjournalisten ausgezeichneten Web Application Firewall (WAF), über ein Customer Identitäts und Access-Management (cIAM), dem Schweizer Banken vertrauen, hin zu einem API-Security Gateway, das neueste Anforderungen erfüllt. Die IT-Sicherheitslösung Airlock schützt mehr als 20 Millionen aktive, digitale Identitäten und 30.000 Back-Ends auf der ganzen Welt. Weitere Informationen unter www.airlock.com. Airlock ist eine Security Innovation des Schweizer Softwareunternehmens Ergon Informatik AG.