Airlock Web Application Firewall 7.3 mit umfangreichen Neuerungen

Zürich, 30. September 2019 – Ergon Informatik AG kündigt einen neuen Release seiner Airlock Web Application Firewall (WAF) an. Die Version 7.3 baut den umfangreichen Schutz um Bot Detection aus, erweitert die API-Gateway-Funktionen und verbessert die Cloud-Unterstützung. Hinzu kommen Security Level für Logging, um die Integration von Blacklist Regeln zu vereinfachen.

Die Abwehr von bösartigen Bot-Anfragen erfolgt nun auf zwei Arten: Auf eine dynamische, interne IP-Blacklist geraten IP-Adressen, wenn sie innerhalb eines frei konfigurierbaren Zeitfensters zu viele bösartige Anfragen schicken. Sie werden daraufhin über einen gewissen Zeitraum blockiert, was Sand ins Getriebe automatisierter Angriffs-Tools, wie z.B. sqlmap, streut. Als zweite Möglichkeit kann vom Client verlangt werden, dass er Cookie Handling unterstützt, wodurch viele automatisierte Scripts und Botnet Clients ausgeschlossen werden. Um keine gutartigen Bots, wie Suchmaschinen, abzulehnen, stehen umfangreiche Möglichkeiten zur Verfügung, wie die Prüfung des User Agents oder der Domain hinter den Bots mit Hilfe von IP Reverse Lookup. Diese neuen Features ergänzen den mit Version 7.2 eingeführten Service, Webroot Threat Intelligence, der auf eine globale Echtzeit-Datenbank bösartiger IP-Adressen zurückgreift.

Der Airlock API Gateway ist nun in der Lage die ID von technischen Clients, wie Mobile Apps oder SPAs, aus JSON Web Tokens auszulesen. Die Client IDs werden in die Logs geschrieben, um Ereignisse, wie Sicherheitsvorfälle, eindeutig einem Client zuordnen zu können. Außerdem kann der Airlock API Gateway nun einzelne Pfadsegmente, anstatt des gesamten Pfades, gegen die festgelegten Regeln prüfen.

Außerdem verbessert die Version 7.3 die Cloud-Unterstützung, wodurch das Airlock Cloud Image, neben Amazon Web Service und Google GCP, auch kompatibel zu Microsoft Azure ist. Mit wenigen Kicks lässt sich die Airlock Sicherheitslösung damit in einer Public Cloud aktivieren. Bestehende Lizenzen können zudem für den Betrieb in der Google Cloud benutzt werden (BYOL). Der API-Gateway geht auch hier den Weg der Digitalisierung mit und fügt dem REST API einige Endpunkte hinzu, um den Cloud-Betrieb zu erleichtern. Darunter fallen Nodes, Routes, Network Services, Lizenz-Verwaltung und Session Settings. Der Status von Back-end Hosts wird ebenfalls ausgelesen.

Die bewährten Security Levels Basic, Standard und Strict erlauben es, das Sicherheits-Niveau schnell und einfach anzupassen. Für die Blacklist Regeln lassen sich nun zwei Level auswählen, getrennt nach Enforcement der Richtlinien und Logging der Ereignisse. Letzteres ermöglicht ein Policy Learning und Testen eines Security Levels, bevor es tatsächlich über Enforcement durchgesetzt wird. Das macht sich bezahlt, wenn alte Regeln durch die neuen Levels ersetzt werden, aber ohne Lücken übernommen werden sollen. Die laufende Applikation wird bei den Testläufen nicht beeinträchtigt.

Weitere Verbesserungen runden das große WAF-Paket 7.3 ab, wie die Unterstützung von SNMPv3, einfache Konfiguration von http und JSON Limits, Mapping Templates für MS Exchange 2019 und Sharepoint 2019, Unterstützung für Kerberos-Cross-Domain-Szenarien und ein großes Update von Elasticsearch und Kibana.

Einen vollständigen Überblick der Neuerungen und eine detaillierte Auflistung der Änderungen finden Sie im offiziellen Datenblatt zur WAF 7.3 in der Airlock-Techzone.

Viele weitere Ideen und Innovationen zur IT-Sicherheit erfahren Sie zusätzlich auf dem Airlock-Kongress während der it-sa 2019 und an der Messe-Präsenz in Halle 9, Stand 403. Informationen zum Kongress-Programm – wo auch die Partner eperi, SHE und Deloitte Deutschland Vorträge halten – sowie Möglichkeiten, sich anzumelden, finden Sie hier: https://www.airlock.com/itsa

Wie die IT-Sicherheit zum Beschleuniger von innovativen Geschäftsprozessen wird, können Sie abschließend im aktuellen Whitepaper nachlesen: https://www.airlock.com/whitepaper/whitepaper-digitalisierung-beschelunigen

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.