

PRESSEMITTEILUNG

Zürich, 15. Dezember 2025

Web Application Security bereit für die Quantencomputer-Ära

Airlock Gateway 8.5 setzt neue Massstäbe in der Absicherung digitaler Infrastrukturen und integriert erstmals Post-Quanten-Kryptografie zum Schutz sensibler Daten

Mit Version 8.5 erweitert Airlock Gateway seine Web Application und API Security Plattform um Post-Quanten-sichere Kryptografie. Die neue Version ermöglicht den Einsatz hybrider Verfahren, die klassische Verschlüsselungstechnologien mit quantensicheren Algorithmen wirksam kombinieren. Ergänzt wird das Release des renommierten Security-Anbieters Airlock mit Sitz in Zürich durch zahlreiche Verbesserungen in den Bereichen Sicherheit, Automatisierung und Betrieb.

Jetzt Post Quantum ready!

Quantencomputer gelten als eine der bedeutendsten Entwicklungen unserer Zeit. Gleichzeitig stellen sie eine erstzunehmende Bedrohung für die digitale Sicherheit dar. Im Zentrum der Risikodiskussionen stehen sogenannte Cryptographically Relevant Quantum Computers, welche in naher Zukunft viele der heute genutzten kryptographischen Verfahren wie RSA und ECC gefährden bzw. brechen könnten. Hacker-Szenarien wie «Harvest now, decrypt later» stellen bereits heute eine reale Bedrohung dar. Dabei werden verschlüsselte Daten abgefangen und gespeichert, um sie zu einem späteren Zeitpunkt mithilfe leistungsfähiger Quantencomputer zu entschlüsseln. Unternehmen stehen daher vor der Aufgabe, ihre sensiblen Informationen und Identitätsdaten frühzeitig auf quantensichere Verfahren vorzubereiten.

Airlock Gateway adressiert diese Herausforderung mit innovativer Post-Quanten-Kryptografie (PQK) zur Absicherung von Webanwendungen und Schnittstellen. Die Plattform setzt dabei auf algorithmische Agilität und unterstützt hybride Ansätze, bei denen klassische und quantensichere Algorithmen kombiniert werden. So können Unternehmen neue Verschlüsselungsstandards schrittweise einführen, ohne bestehende Systeme zu gefährden. Die Umsetzung orientiert sich an internationalen Empfehlungen und Standards, etwa des NIST und ETSI. Das US-amerikanische National Institute of Standards and Technology (NIST) empfiehlt, spätestens bis 2030 Post-Quanten-Kryptografie produktiv einzusetzen, um langfristige Sicherheitsrisiken zu vermeiden. Mit Airlock Gateway 8.5 können Unternehmen diese Anforderungen bereits heute angehen und ihre Web- und API-Sicherheit frühzeitig auf kommende regulatorische und technologische Vorgaben ausrichten. «Seit 2024 erproben Airlock-Spezialisten die Funktionalitäten der Post-Quanten-Kryptografie gemeinsam mit unseren Kunden und Partnern in unterschiedlichsten Szenarien. Die Erkenntnisse stehen mit dem neuen Release der gesamten Airlock-Community zur Verfügung», so Stefan Dietiker, Product Manager Airlock Gateway.

PRESSEMITTEILUNG

Technische Basis für PQK-Fähigkeit

Mit dem Upgrade auf OpenSSL 3.5 schafft Airlock Gateway das technische Fundament für die PQK-Fähigkeit. Dazu gehören modernste Kryptografie und optimierte Performance auf Basis der aktuellsten OpenSSL Library. Auch das automatisierte Zertifikatsmanagement der angepassten ACME-Services stellt einen entscheidenden Schritt hin zur notwendigen Crypto-Agilität dar: Sicherheitsrisiken durch abgelaufene Zertifikate werden minimiert und der administrative Aufwand deutlich reduziert.

Die Highlights der Post-Quanten-Kryptografie (PQK) von Airlock Gateway

- Secure by default: PQK-fähige KEM-Gruppen (Key Encapsulation Mechanisms) sind standardmäßig aktiv.
- Klassische und Post-Quantum-Algorithmen werden kombiniert. Dank der sogenannten «Hybride Key Exchanges» bleibt die Verbindung auch dann sicher, wenn ein einzelnes Verfahren künftig gebrochen werden sollte.
- Ein transparentes Reporting zeigt auf einen Blick, welche Clients bereits PQK-fähige Gruppen verwenden.
- Die Einführung der Post-Quanten-Kryptografie von Airlock führt zu keinen relevanten Performance-Einbussen.
- Eine Vielzahl an marktgängigen Browsern unterstützt derzeit schon die Post-Quanten-Kryptografie und Airlock kann die PQC-Funktionalität breit ausspielen.

Vertiefende Informationen zur Bedrohung durch Quantencomputer und zur Vorbereitung auf Post-Quanten-Kryptografie finden sich im Airlock Blog:

[Quantencomputer und Sicherheit: Wie Unternehmen langfristig geschützt bleiben](#)

Weitere Verbesserungen von Airlock Gateway 8.5

- Das integrierte Anomaly Shield verfügt nun über eine automatische IP-Reputation, die verdächtige Zugriffe schneller erkennt und False Positives reduziert.
- Der Add-on Tomcat steht in Version 11 für aktuelle Java-Anwendungen bereit und erlaubt den Parallelbetrieb mit Tomcat 9.
- Die neue PXE-basierte Installation ermöglicht ein vollständig automatisiertes Ausrollen neuer Gateways, was insbesondere bei grossen Umgebungen, verteilten Standorten oder für Managed Security Service Provider eine schnelle, fehlerfreie und konsistente Provisionierung sicherstellt.

PRESSEMITTEILUNG

Bildmaterial:



Stefan Dietiker, Product Manager für
Airlock Gateway bei Ergon Informatik

Das Bildmaterial finden Sie in unserem Medienportal press-n-relations.amid-pr.com zum Download (Suchbegriff «Stefan Dietiker»). Selbstverständlich schicke ich Ihnen die Datei auch gerne per E-Mail zu. Kontakt: rh@press-n-relations.de

Weitere Informationen:

Airlock

Ergon Informatik AG
Michaela Zellnig
Michaela.zellnig@ergon.ch
+41 763069701
Merkurstrasse 43
CH-8032 Zürich

Press'n'Relations GmbH

Rebecca Horn
rh@press-n-relations.de
+49 731 146 156-75
Magirus-Deutz-Str. 14
D-89077 Ulm

Über Airlock

Der Airlock Secure Access Hub vereint seit 20 Jahren die kritischen 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 Applikationssicherheit ab: von einer durch Fachjournalisten ausgezeichneten Web Application and API Protection (WAAP), über ein Microgateway für Sicherheit in Kubernetes-Umgebungen, hin zu einem Identitäts- und Zugriffsmanagement (IAM) mit integrierter starker Authentifizierung. Die IT-Sicherheitslösung Airlock schützt mehr als 30 Millionen aktive, digitale Identitäten und 30.000 Back-Ends von über 600 Kunden auf der ganzen Welt. Weitere Informationen unter <https://www.airlock.com>.

Airlock ist eine Security Innovation des Schweizer Softwareunternehmens Ergon Informatik AG. Das Unternehmen wurde 1984 gegründet, zählt rund 450 Mitarbeiter und wurde wiederholt als einer der beliebtesten Arbeitgeber der Schweiz ausgezeichnet.