Sperrfrist: 24.07.2025, 09:00 Uhr

Pressemitteilung

Cryptomator ebnet den Weg in die post-quantensichere Zukunft

Open-Source-Verschlüsselungslösung setzt auf neue Standards gegen Bedrohungen durch Quantencomputer

Bonn, 24. Juli 2025 – Die **Skymatic GmbH**, Entwickler der Open-Source-Verschlüsselungssoftware **Cryptomator**, kündigt heute ihren Plan an, die eigene Software vollständig **gegen Bedrohungen durch Quantencomputer abzusichern**. Im Zentrum steht dabei die Integration von **post-quantensicheren Kryptografieverfahren**, darunter die neuen NIST-Standards ML-KEM und ML-DSA, sowie eine Kombination aus klassischen und post-quantensicheren Verfahren, die sich X-Wing nennt.

„Obwohl Quantencomputer heute eingesetzte Schlüssellängen noch nicht knacken können, ist die Zeit zu handeln trotzdem jetzt. 'There is no glory in prevention' gilt auch in der IT-Sicherheit.“ – Sebastian Stenzel, CTO von Skymatic

Die Herausforderung: Quantencomputer und Kryptografie

Während symmetrische Algorithmen wie AES durch ausreichend große Schlüssel weiterhin als sicher gelten – insbesondere bei Verwendung von AES-256 – geraten asymmetrische Verfahren wie RSA oder ECDH durch neue Algorithmen wie **Shor-Algorithmus** ins Wanken. Diese Entwicklung erfordert neue kryptografische Standards.

Die Lösung: Post-Quanten-Kryptografie

Cryptomator Hub, die Collaboration-Lösung zur Verwaltung verschlüsselter Cloud-Daten, wird künftig eine **hybride Verschlüsselung** einsetzen: klassische Verfahren werden mit post-quantensicheren Algorithmen kombiniert – ähnlich wie zwei Schlösser an einer Tür. Die **neue Technologie basiert unter anderem auf dem Algorithmus X-Wing**, der bereits von Apple und Google in Hardware implementiert wird.

Zudem arbeitet das Cryptomator-Team an der **Integration des Standards HPKE** (Hybrid Public Key Encryption) auf Basis von X-Wing und der **Umstellung des Formats JWE** (JSON Web Encryption), mit dem verschlüsselte Nutzdaten übertragen werden. Dies soll für maximale Kompatibilität und kryptografische Agilität sorgen.

Standardisierung als Grundpfeiler

Ein weiteres Ziel ist die **Standardisierung des sogenannten Tresor-Formats**, das die Struktur verschlüsselter Verzeichnisse definiert. In Zusammenarbeit mit anderen Open-Source-Projekten wie **Cyberduck, gocryptfs und rclone** arbeitet Cryptomator an einem einheitlichen Format für verschlüsselte Ordner – für mehr Interoperabilität und Benutzerfreundlichkeit.

Open Source und Transparenz

Wie bei allen Entwicklungen setzt Skymatic auf vollständige Transparenz: **Der gesamte Code bleibt Open Source**, die Community ist eingeladen, die neuen kryptografischen Komponenten zu prüfen und zu kommentieren.

Sperrfrist: 24.07.2025, 09:00 Uhr

„Der Open Source Gedanke ist bei uns tief verankert, entsprechend haben wir schon immer auch Code zu anderen Projekten beigetragen. Derzeit stehen wir in engem Austausch mit den RFC-Autoren zukünftiger Standards wie X-Wing und implementieren diese u.a. für das OpenJDK oder JWT-Bibliotheken.“ – Sebastian Stenzel, CTO von Skymatic

Verfügbarkeit

Die neuen kryptografischen Verfahren werden **schrittweise in Cryptomator Hub integriert**. Erste experimentelle Releases mit X-Wing und HPKE sind noch für **2025** geplant.

Über Skymatic und Cryptomator

Skymatic ist ein in Bonn ansässiges Unternehmen mit dem Ziel, Datenschutzlösungen für alle zugänglich zu machen. Mit Cryptomator bietet das Unternehmen eine vielfach ausgezeichnete Open-Source-Software zur clientseitigen Verschlüsselung von Cloud-Daten, die weltweit millionenfach genutzt wird.

Weiterführende Links

- Post-Quantum Roadmap: https://cryptomator.org/de/blog/2025/07/24/post-quantum-roadmap/
- Cryptomator: https://cryptomator.org/de/
- Pressemappe: https://cryptomator.org/de/presskit/
- Skymatic: https://skymatic.de

Pressekontakt

Kerstin Steiner
kerstin.steiner@skymatic.de