THREEMA

PRESSEMITTEILUNG

Pfäffikon SZ, 25. Februar 2026

Threema und IBM arbeiten zusammen an Post-Quanten-Kryptografie für Instant Messaging

Obwohl Quantencomputer derzeit noch kein Risiko in Sachen Cybersicherheit darstellen, gehen Experten davon aus, dass sie in den kommenden Jahren zu einer grossen Herausforderung für die heutigen Sicherheitsstandards werden. Um sich frühzeitig gegen diese Risiken zu wappnen und den Austausch sensibler Daten und Informationen zu sichern, arbeitet Threema, Pionier und Marktführer im Bereich sicherer Kommunikation, gemeinsam mit Teams von IBM an der Integration von Post-Quanten-Kryptografie in Threemas Messaging-Dienst.

Quantencomputer funktionieren grundlegend anders als herkömmliche Rechner: Anstelle von klassischen Bits, die nur die Werte 0 oder 1 annehmen können, nutzen sie Quantenbits oder «Qubits». Dank quantenphysikalischer Phänomene wie Überlagerung und Verschränkung können Qubits mehrere Rechenzustände gleichzeitig annehmen, wodurch ein Rechenraum zugänglich wird, der selbst die Fähigkeiten von Supercomputern übersteigt. Folglich könnte ein leistungsfähiger Quantencomputer die aktuellen Verschlüsselungsstandards aushebeln.

Allerdings gibt es noch keine modernen, leistungsfähigen und fehlertoleranten Quantencomputer mit potenziell Tausenden von logischen Qubits, die in der Lage wären, die heutigen Sicherheitsprotokolle zu knacken. Nichtsdestotrotz wird derzeit eine Post-Quanten-Kryptografie (PQC) entwickelt, die vor einem solchen zukünftigen Risiko schützen soll.

Zusammenarbeit für langfristige Sicherheit

Um auf die zukünftigen Risiken vorbereitet und auch langfristig gegen neue Angriffsmethoden gewappnet zu bleiben, setzt Threema auf die schrittweise Implementierung von PQC in sein Messaging-System. Dazu arbeitet das Schweizer Unternehmen gemeinsam mit dem renommierten Kryptografie-Forschungsteam von IBM an der Transformation hin zu quantensicherer Verschlüsselung.

Threema schützt die Kommunikation seiner Kunden derzeit durch Ende-zu-Ende-Verschlüsselung, Zero-Knowledge-Architektur, einen Privacy-by-Design-Ansatz, Vertrauensstufen für Kontakte und vieles mehr. In Zusammenarbeit mit IBM untersucht das Unternehmen, wie PQC-Algorithmen wie ML-KEM (Module-Lattice-Based Key-Encapsulation Mechanism) integriert werden können. Dieser Algorithmus wurde von IBM mitentwickelt und vom US-amerikanischen National Institute of Standards and Technology (NIST) 2024 als einer von drei PQC-Standards veröffentlicht.

«Wir freuen uns auf diese spannende Zusammenarbeit. Die Wissenschaftler von IBM verfügen über eine enorme Expertise im Bereich der quantensicheren Kryptografie und haben massgeblich bei zwei der drei veröffentlichten Post-Quanten-Kryptografie-Standards des NIST mitgewirkt», erläutert Robin Simon, CEO von Threema. «Diese Zusammenarbeit und die Bündelung unseres Know-hows legen den Grundstein für die quantensichere Kommunikation von morgen – und verkörpern das, was Threema ausmacht: kompromisslose Sicherheit und modernste Technologie.»

Über Threema

Die Threema GmbH ist eine Pionierin und Marktführerin im Bereich geschützter Kommunikation. Mehr als 12 Millionen Nutzer in Europa und darüber hinaus vertrauen bereits auf die Kommunikationslösung aus der Schweiz, die konsequent auf Datenschutz und Datenvermeidung ausgelegt sind. Unter ihnen sind drei Millionen Nutzer der Business-Anwendung Threema Work in über 8’000 Unternehmen, Behörden, Schulen und Verbänden. Das 2014 in Pfäffikon SZ bei Zürich gegründete Unternehmen betreibt – anders als die meisten Wettbewerber – seine eigenen Server in der Schweiz und garantiert damit höchste Datenschutz-Standards.

Text und Bild sind zur Verwendung frei.

Pressekontakt

Micha Harris
Carta GmbH
Strategie & Kommunikation
Iggelheimer Str. 26
67346 Speyer
E-Mail harris@carta.eu
Tel. +49 (0) 6232 / 100111-20