PRESSEMITTEILUNG

Kryptografie von Cloud-Daten hält auch Quanten-Computern stand

Ein Statement von Andreas Steffen, CEO bei eperi

Pfungstadt, 9. April 2024 – Kryptografie ist seit geraumer Zeit eines der besten Mittel, um digitale Informationen vor unberechtigtem Zugriff zu schützen – beispielsweise, um gesetzliche Bestimmungen wie die DSGVO oder branchenbezogene Regeln einzuhalten. Es geht aber auch um den Schutz vertraulicher Daten vor Diebstahl durch Cyberkriminelle. Eine vergleichsweise neue Diskussion wirft allerdings Fragen bezüglich der Zuverlässigkeit von kryptografischer Sicherheit auf: Sind kryptografische Verfahren, wie beispielsweise mit dem RSA Kryptosystem, auch mit der Verfügbarkeit von extrem leistungsfähigen Quantencomputern noch sicher? Um die Sicherheit von verschlüsselten Daten zu gewährleisten, ist es wichtig, jetzt die Stärke der verwendeten Verschlüsselungsmechanismen zu überprüfen und bei Bedarf auf sicherere Algorithmen oder längere Schlüssellängen zu migrieren. Um das potenzielle Risiko durch Quanten-Computer zu adressieren, gewährleistet die Post-Quantum-Kryptografie die Zuverlässigkeit einer Datenverschlüsselung. Sie stellt sicher, dass die Verschlüsselung selbst unter Verwendung von Quanten-Computern nicht zu knacken ist.

Die Entwicklung und Nutzung der Post-Quantum-Kryptografie nimmt in Unternehmen und Organisationen hinsichtlich der schützenswerten Daten in der Cloud eine besondere Rolle ein. Sensible Daten, die beispielsweise in Microsoft 365, Teams, Salesforce oder beliebig anderen Cloud-Umgebungen gespeichert sind, sollten grundsätzlich durch Verschlüsselung geschützt werden. Dabei ist der durchgängige Verschlüsselungsschutz dann gewährleistet, wenn die Daten nicht erst beim Cloud-Anbieter verschlüsselt werden, sondern bereits im Unternehmen. Erst damit liegt die Datenhoheit inklusive der kryptografischen Schlüssel allein in den Händen des Dateneigentümers.

Doch wie sicher sind die Daten in der Cloud trotz der besten Krypto-Strategie im Zeitalter von Quanten-Computern? Die künftige Sicherstellung des Datenschutzes hängt unter anderem von den Fähigkeiten der eingesetzten Verschlüsselungslösung ab. Diese sollte Post-Quantum-Ready sein, damit sie rechtzeitig und ohne große Umstände auf kryptografische Verfahren umgestellt werden kann, die der massiven Computing-Leistung der Quanten-Computer etwas entgegenzusetzen hat. Gitter- oder

hashbasierte Kryptografie bietet geeignete Verfahren, um auch in Zukunft die angestrebte Sicherheit zu gewährleisten.

Das National Institute of Standards in Technology (NIST) und die European Telecommunications Standards Institute (ETSI) arbeiten an allgemeingültigen Standards, um wirkungsvolle Post-Quantum-Standards zu identifizieren und als Best Practice zu empfehlen. Hersteller von Verschlüsselungslösungen und Unternehmen erhalten dadurch aktive Unterstützung, um ihre Verschlüsselung auf dem sichersten Standard zu halten.

Für Unternehmen, deren Verschlüsselungslösungen nicht problemlos auf neue und sichere Kryptografieverfahren umgestellt werden können, ist es jetzt an der Zeit, geeignete Migrationskonzepte auszuarbeiten – bevor Quanten-Computer eine Reife und Verbreitung erreichen, mit der sie den bestehenden Verschlüsselungsverfahren gefährlich werden können. Im Idealfall entscheiden sich Unternehmen und Organisationen für Verschlüsselungslösungen, die nicht nur den nächsten Schritt in der Sicherheit der Quanten-Computing-Ära sicherstellen, sondern auch langfristig in der Lage sind, künftige Verschlüsselungsverfahren nahtlos, ohne Migrationsaufwand sowie unter Beibehaltung der Such- und Sortierfunktionen zu integrieren.

Über die Eperi GmbH:

Wir bei eperi® sind der festen Überzeugung, dass Datenschutz ein grundlegendes Menschenrecht ist. Unser Ziel ist es, dass Menschen und Unternehmen zu jeder Zeit die Kontrolle über ihre Daten behalten. Ohne Kompromisse und mit der besten Technologie. Mit dem Fokus auf die Sicherheit unserer Kunden haben wir eine Lösung geschaffen, die für den Benutzer unsichtbar ist und gleichzeitig die höchsten Sicherheitsstandards erfüllt.
Mit der eperi® Lösung profitieren unsere Kunden von allen Vorteilen der Cloud-Nutzung, wie beispielsweise einer effizienten unternehmensweiten Kollaboration, und bleiben dabei rechtssicher gemäß weltweiten Datenschutzgesetzen. Wir besitzen mehrere internationale Patente für unsere innovative Multi-Cloud-Technologie, die einen konkurrenzlosen Datenschutz für SaaS Anwendungen, individuelle Applikationen und Dateien bietet. Unsere Kunden behalten die alleinige Kontrolle über alle sensiblen Daten, da keine unverschlüsselten Daten in die Cloud gesendet werden.
Wir ermöglichen die Cloud – einfach, sicher, individuell, DSGVO-konform.

Pressekontakt eperi
Eperi GmbH
Sabine Jost
Gutenbergstraße 4-6
64319 Pfungstadt
Tel: +49 (0)6157 95639 16
E-Mail: sabine.jost@eperi.com
Web: www.eperi.com

Pressekontakt Agentur
TC Communications
Thilo Christ
Tel: +49 171 6220610
Alexandra Schmidt
Tel: +49 170 3871064
E-Mail: eperi@tc-communications.de