Thüringen

Quantenmechanik für IT-Sicherheit

[13.06.2023] Ein wichtiges Element der Kryptographie ist der sichere Austausch so genannter Schlüssel. Am Landesrechenzentrum Thüringen wurde nun erfolgreich ein zukunftssicheres Verfahren erprobt, das auf Quantenmechanik setzt.

Ende Mai 2023 startete ein mehrtägiger Testbetrieb zur Nutzung der Quantenmechanik für den sicheren Schlüsselaustausch zwischen den beiden Standorten des Thüringer Landesrechenzentrums (TLRZ) in Erfurt und Ilmenau. Dieser wurde nach Angaben des Thüringer Finanzministeriums inzwischen erfolgreich abgeschlossen. Durchgeführt wurde der Test von den Firmen Quantum Optics aus Jena und ADVA Network Security mit Sitz in Berlin und Meiningen. Dabei wurde erprobt, wie die digitale Kommunikation auf Glasfaserverbindungen mithilfe einer neuartigen Quantentechnologie – dem Quantenschlüsselaustausch (Quantum Key Distribution, kurz: QKD) – künftig noch besser geschützt werden kann. Das Thüringer Landesrechenzentrum ist laut Ministeriumsangaben der erste öffentliche IT-Dienstleister, der die Quantentechnologie zu Testzwecken vollständig in eine Glasfaserübertragungsstrecke integriert hat.

Basierend auf den physikalischen Gesetzen der Quantenmechanik ermöglicht die neue Lösung die Generierung und sichere Übertragung von geheimen Schlüsseln, mit denen später Informationen verschlüsselt werden. Der Vorteil dieses Quantenschlüsselaustauschs liegt darin, dass die erreichte Sicherheit auf physikalischen Gesetzmäßigkeiten beruht – im Gegensatz zu klassischen Verfahren der Schlüsselverteilung, die auf Annahmen über die Leistungsfähigkeit von Computern und deren Rechenverfahren oder die Vertrauenswürdigkeit von Personen beruhen. Das Konzept des Jenaer Start-ups erlaubt es, dass der Schlüssel selbst nur bei den beteiligten Kommunikationspartnern entsteht. Ein möglicher Angreifer, der die Schlüsselübertragung abhört, kann durch messtechnische Verfahren sofort erkannt werden.

Der Testbetrieb sei ein Meilenstein für die verschränkungsbasierte Quantenverschlüsselungstechnologie, da diese weltweit erstmals vollständig in eine IT-Infrastruktur integriert wurde, so das Thüringer Finanzministerium. Erste Testergebnisse zeigten bereits, dass die Schlüsselübertragung über eine lange Glasfaserstrecke – in Thüringen wurden mehr als 50 Kilometer überwunden – zuverlässig und sicher erfolgen kann.

In der Kryptographie spielt der geheime Schlüsselaustausch eine besonders wichtige Rolle. Die derzeit dafür eingesetzten kryptographischen Verfahren und Algorithmen gelten als sicher. Experten vermuten jedoch, dass mit der Weiterentwicklung des Quantencomputers in den kommenden fünf bis zehn Jahren die Gefahr steigt, dass bestehende Schlüsselaustauschverfahren anfälliger für erfolgreiche Angriffe werden. Dieses Risiko adressiert der Quantenschlüsselaustausch.

(sib)

Stichwörter: IT-Sicherheit, Kryptographie, Landesrechenzentrum, QKD, Quantenmechanik, Thüringen