Schutz vor Quantencomputer-Angriff: EU-Projekt in Graz gestartet

23. Jänner 2018, 16:31

posten

Forschungsprojekt, um den Übergang zu "Post-Quantum-Kryptografie" voranzutreiben

Digitale Daten, die heute noch gut gesichert sind, könnten schon in zehn bis 15 Jahren von Quantencomputer-Experten entschlüsselt werden. Weltweit wird daher an sogenannten quantenresistenten (QR) Sicherheitskomponenten (TPM) geforscht. Europäische Experten aus Industrie und Forschung haben sich am Dienstag im Zuge eines EU-Projektes erstmals in Graz getroffen, teilte Infineon Austria mit.

"Post-Quantum-Kryptografie"

Kryptografie-Anbieter stehen vor der Herausforderung, dass zurzeit noch sichere Verschlüsselungsverfahren schon bald mit Hilfe zukünftiger Quantencomputer knackbar sein dürften. Dem Infineon-Konzern ist es im Vorjahr gelungen, einen Verschlüsselungs-Algorithmus, der auch vor künftigen Quantencomputern sicher sein soll, auf einem kontaktlosen Sicherheitschip unterzubringen. Entwickelt wurde das von Forschern aus dem Infineon-Kompetenzzentrum in Graz sowie von Experten aus München. Mit Jahresbeginn hat der Chip-Konzern mit rund einem Dutzend hochkarätiger industrieller und akademischer Partner ein neues Forschungsprojekt gestartet, um den Übergang von heutigen Sicherheitsprotokollen auf die "Post-Quantum-Kryptografie" weiterzutreiben.

Nächste 36 Monate

Das europäische Projekt "FutureTPM" hat sich innerhalb der nächsten 36 Monate die Entwicklung von QR-Kryptoalgorithmen, die mit den TPM (Trusted Platform Moduls) kompatibel sind, zum Ziel gesetzt. "Um besser auf künftige Sicherheitsbedrohungen reagieren zu können, arbeiten wir kontinuierlich mit Wissenschaftern, Kunden und Partnern zusammen", betonte Stefan Rohringer, Leiter des Infineon Entwicklungszentrums in Graz, wo am Dienstag das Kick-Off Meeting stattgefunden hat.

Drei Anwendungsfälle

Das Konsortium versammelt Partner aus neun europäischen Ländern. Koordiniert wird das Projekt von der in Villach ansässigen Technikon Forschungs- und Planungsgesellschaft mbH. Die Technische Leitung wurde in die Hände von Thanassis Giannetsos und Liqun Chen von der britischen

angesiedelt. Von Industrieseite findet sich u.a. auch Huawei Technologies Düsseldorf unter den Konsortialpartnern. Das Design der quantenresistenten Sicherheitskomponenten wird für drei Anwendungsfälle getestet: Im Bereich von Wearables (Activity tracking), bei zentral verwalteten Business Laptops und PC sowie für Anwendungen im Finanzsektor (Secure mobile payment), wie Infineon bekannt gab. (APA, 23.1.2018)