Zeitschrift: Schweizer Soldat : die führende Militärzeitschrift der Schweiz
Herausgeber: Verlagsgenossenschaft Schweizer Soldat
Band: 99 (2024)
Heft: 5

Werbung

Post-Quanten-Kryptografie: gerüstet für den «Q-Day»

Der «Q-Day» rückt näher: Unter Hochdruck arbeiten Cyber Security-Experten weltweit an der Post Quantum Security. Ihr besonderes Augenmerk liegt dabei auf der Kryptografie. Die Verschlüsselungslösungen der CyOne Security sind bereits heute post-quantensicher.

Quantencomputing markiert eine Zäsur im IT-Zeitalter. Anders als herkömmliche Laptops oder Smartphones «denken» Quantenrechner in Qubits und können somit eine enorme Vielzahl an Rechenaufgaben parallel lösen.

Die Kehrseite der Medaille: Die gigantische Rechenleistung von Quantencomputern stellen Cyber Security-Fachleute vor grosse Herausforderungen. Der «Q-Day» – jener Tag, an dem Quantencomputer es schaffen, die kryptographischen Algorithmen heute gängiger Public Key-Systeme in kurzer Zeit zu brechen – rückt näher. Experten gehen davon aus, dass dies bereits in fünf bis zehn Jahren der Fall sein wird. Je früher sichere Verschlüsselungssysteme zur Verfügung stehen, desto besser.

PQC-Entwicklung als Wettbewerb

Deshalb beschäftigt sich die Kryptologie weltweit seit Jahren mit der sogenannten Post-Quanten-Kryptografie (engl. abgekürzt PQC). Diese fokussiert auf asymmetrische Verschlüsselungs- und Signaturverfahren. Dies, da die aktuell weltweit umfassend eingesetzten asymmetrischen Public Key-Verfahren auf mathematischen Problemen – der Schwierigkeit der Primfaktorzerlegung und der Berechnung diskreter Logarithmen – beruhen, welche sich mit Quantencomputern effizient lösen lassen. Daher ist es das Ziel von PQC, neue quantensichere Public-Key Verfahren zu entwickeln, die für die Ära nach Beginn der kommerziellen Nutzung des Quantencomputers zur sicheren Verschlüsselung eingesetzt werden.

2016 startete das National Institute of Standards and Technology (NIST) einen Prozess zur Standardisierung von quantenresistenter Public Key-Kryptografie in Form eines Wettbewerbs. Erste definitive Standards sollen noch in diesem Jahr folgen.

Post-quantensichere Verschlüsselung – bereits heute

Die CyOne Security hat – unabhängig von den Standardisierungsbemühungen – bereits post-quantensichere Verschlüsselungslösungen entwickelt. Grossmehrheitlich kommen dabei symmetrische Chiffrierverfahren mit einem mehrstufigen Sicherheitskonzept zum Einsatz. Die symmetrische Kryptografie gilt als nicht von Quantencomputern bedroht, solange ausreichend lange Schlüssel verwendet und Schlüsselaustausch- und Authentifizierungsmechanismen umfassend geschützt werden.

Ein Beispiel hierfür ist die hochmoderne one Technology Suite: Um höchste Cyber Security für Behördenorganisationen zu erreichen, wurde die post-quantensichere one-Produktefamilie, bestehend aus hard- und softwarebasierten Sicherheitselementen und basierend auf dem «Security by Design»-Ansatz entwickelt. Sie bietet umfassenden und zuverlässigen Schutz – auch vor dem allgemein mit Bangen erwarteten «Q-Day» und den damit verbundenen potenziellen Cyber-Bedrohungen.

Erfahren Sie mehr über die Security Solutions für Schweizer Behörden.

Roland Odermatt
Leiter Verkauf Behörden
Tel. +41 41 748 85 00
roland.odermatt@cyone.ch