Quantum Computing

Cybersecurity – Herausforderungen für die politische Schweiz

Stand der Dinge

Der Bau eines voll funktionsfähigen Quantencomputers ist eine der spannendsten wissenschaftlichen und technischen Herausforderungen unserer Zeit. Die Verwirklichung dieses lang ersehnten Ziels würde sich sehr positiv auf Wissenschaftsbereiche wie künstliche Intelligenz und Bioinformatik auswirken. Quantencomputer werden in der Lage sein, bestimmte leistungsfordernde Probleme viel schneller zu lösen als herkömmliche Computer. Es wird jedoch nicht erwartet, dass sie als Allzweckcomputer eingesetzt werden, die traditionelle Computer ersetzen.

Die Quantencomputertechnologie hat sich in den letzten Jahren rasant entwickelt. Erste Quantencomputer sind bereits heute im Internet verfügbar, so dass jede und jeder Interessierte neue Quantenalgorithmen entwickeln und ausprobieren kann.

Während Quanten Computing ein neues Paradigma für die Lösung komplexer Rechenprobleme schafft, schafft es leider auch ein neues Sicherheitsrisiko. Viele der heutigen kryptographischen Algorithmen mit öffentlichen Schlüsseln basieren auf Problemen, die von traditionellen Computern schwer zu lösen sind, aber von Quantencomputern effizient angegangen werden können.

Empfehlungen

1. Auch wenn leistungsstarke Quantencomputer noch nicht verfügbar sind, wird Organisationen empfohlen, die Sicherheitsanforderungen von Datenbeständen und Systemen, die eine lange Lebensdauer haben, zu prüfen. Die Bewertung sollte den Plan bestimmen, wie und wann der sich entwickelnde quantensichere Kryptographiestandard übernommen werden soll.
2. Bei der Entwicklung oder der Anschaffung neuer Software-Lösungen sollten kryptographische Agilitätsprinzipien eingehalten werden, so dass die eingesetzten kryptographischen Algorithmen leicht durch quantensichere ersetzt werden können.

Herausforderungen

Es kann nur spekuliert werden, wann Quantencomputer verfügbar sein werden, die in der Lage sind, aktuelle Kryptosysteme zu durchbrechen. Die Schätzungen reichen von 10 Jahren bis zu 30 Jahren und mehr. Ein Mass zur Beurteilung der Leistung eines Quantencomputers ist die Anzahl der Qubits. Ein Qubit kann als das quantenmechanische Analogon eines klassischen Bits angesehen werden. Es wird zwischen logischen und physikalischen Qubits unterschieden. Ein logisches Qubit benötigt etwa 1000 physikalische Qubits, um Stabilität, Fehlerkorrektur und Fehlertoleranz zu gewährleisten, wie sie für eine zuverlässige Berechnung erforderlich sind. Es wird angenommen, dass mehrere tausend logische Qubits erforderlich sind, um die heutigen Kryptosysteme zu durchbrechen. In der Praxis würde man also Quantencomputer mit Millionen von physikalischen Qubits benötigen. Aktuelle experimentelle Quantencomputer verfügen «nur» über zwischen 50 und 100 physikalischen Qubits.

Obwohl es noch einige Zeit dauern wird, bis leistungsfähige Quantencomputer zur Verfügung stehen, gibt es bereits heute mehrere kryptographische Schemata, die als quantensicher gelten, d.h. als sicher gegen Angriffe von Quantencomputern. Sie basieren auf schwierigen Problemen, für die keine effizienten Quantenlösungen bekannt sind.

Gegenwärtig sind verschiedene Bestrebungen im Gange, die quantensichere Kryptographie zu standardisieren. Am bemerkenswertesten ist der vom National Institute of Standards and Technology (NIST) initiierte Standardisierungsprozess. Die Standardisierung ist ein anspruchsvoller und zeitraubender Prozess. Es ist zu erwarten, dass innerhalb der nächsten drei bis fünf Jahre ein Standard zur Verfügung stehen wird.

Handlungsbedarf

Es gibt IT-Systeme, wie etwa Geräte, die z.B. in Kraftwerken oder Produktionsfabriken eingesetzt werden, die eine lange Lebensdauer haben. Systeme, die heute eingesetzt werden, sind möglicherweise noch in Gebrauch, wenn leistungsfähige Quantencomputer zur Verfügung stehen. Dasselbe gilt für Daten. Einige Datenbestände müssen aus Gründen der Einhaltung gesetzlicher Vorschriften 10 und mehr Jahre lang archiviert werden und könnten anfällig für Quantencomputer-Angriffe werden.

Referenzen

National Institute of Standards and Technology (NIST): Post-Quantum Cryptography. https://csrc.nist.gov/Projects/post-quantum-cryptography.

Computing Community Consortium: Identifying Research Challenges in Post Quantum Cryptography Migration and Cryptographic Agility, CCC Workshop, Feb. 2019: https://cra.org/ccc/wp-content/uploads/sites/2/2018/11/CCC-Identifying-Research-Challenges-in-PQC-Workshop-Report.pdf

w

Kontakt

Nicole Wettstein
Leiterin Schwerpunktprogramm Cybersecurity
+41 44 226 50 13

https://www.satw.ch/cybersecurity-herausforderungen

Impressum
Schweizerische Akademie der Technischen Wissenschaften SATW
Expertenbeiträge
Karl Aberer, EPFL | Umberto Annino, InfoGuard | Alain Beuchat, Banque Lombard Odier & Cie SA | Matthias Bossardt, KPMG | Adolf Doerig, Doerig & Partner | Stefan Frei, ETH Zürich | Roger Halbheer, Microsoft | Pascal Lamia, MELANI | Martin Leuthold, Switch | Hannes Lubich, Verwaltungsrat und Berater | Adrian Perrig, ETH Zürich | Raphael Reischuk, Zühlke Engineering AG | Riccardo Sibilia, VBS | Bernhard Tellenbach, ZHAW | Daniel Walther, Swatch Group Services | Andreas Wespi, IBM Research Lab
Redaktion und Grafik
Beatrice Huber; Claude Naville, Adrian Sulzer, Nicole Wettstein

www.satw.ch
September 2020