Cybersicherheit für das Quantencomputer-Zeitalter

Die besondere Gefährdung von kritischen Infrastrukturen

Das Thema Quantencomputing ist aktueller denn je. Weltweit liefern sich Universitäten, Spitzenlabors und Weltkonzerne einen intensiven Wettbewerb bei der Entwicklung leistungsfähiger Quantencomputer. Insbesondere nach dem öffentlichkeitswirksamen Aufschwung von künstlicher Intelligenz (KI) zählen führende Unternehmen die Tage, bis auch das Quantencomputing „Mainstream" wird.

Foto: iStock.com/audioundwerbung

Gleichzeitig stehen wir durch die Entwicklung und Nutzung von Quantencomputern vor einem Tipping Point in der Cybersicherheit. Heutige Standardverschlüsselung wird mit Einführung von leistungsfähigen Quantencomputern schlichtweg nicht mehr sicher sein. Gerade vor dem Hintergrund exponentiell gestiegener politischer Spionage und kommerziell motivierter Cyberangriffe steigt hiermit das Risiko von erfolgreichen Cyber-Angriffen massiv.

Besonders der Bereich der kritischen Infrastruktur (KRITIS) ist von dem erhöhten Risiko betroffen. Kritische Infrastrukturen stellen Strom und Wasser zur Verfügung, sichern den Verkehr und die medizinische Versorgung. Sie umfassen all die Einrichtungen und Systeme, die ein Gemeinwesen braucht, um zu funktionieren. Fallen sie aus, kann das zu erheblichen akuten Problemen bei der Versorgung und im Kontext der öffentlichen Sicherheit führen.

Weltweit sind kritische Infrastrukturen immer stärker durch Cyber-Angriffe bedroht. Allein für das Jahr 2022 beläuft sich der durch sie verursachte Schaden in deutschen Unternehmen geschätzt auf mehr als 200 Milliarden Euro (Quelle: tagesschau.de).

Cyber-Risiken durch Quantencomputer

Bei allen Potenzialen, die Quantencomputer aufgrund ihrer unvorstellbar vielen parallelen Rechenoperationen mit sich bringen, wollen wir hier die Risiken für die Cyber-Sicherheit in den Fokus rücken.

Heutzutage wird der Schutz sensibler Daten sowie die sichere Übertragung unserer Informationen im

AUTOR

OLIVER WEIMANN

FOUNDER & CEO DER
QUANTUM CYBERSECURITY GROUP

Wesentlichen durch asymmetrische Verschlüsselung (Kryptografie) realisiert. Dieses Verfahren mit einem privaten und einem öffentlichen Schlüssel hat sich bewährt und ist Grundlage sicheren Austausches. Gerade die parallelen, voneinander losgelösten Rechenoperationen eines Quantencomputers führen zur quasi Echtzeit-Entschlüsselung der privaten Schlüssel. Somit kann bisherige „Standardsicherheit" nicht mehr gewährleistet werden. Das bedeutet auch, dass der Zugang zu Bankkonten, persönlichen Krankenakten, Geheimrezepturen oder geheimen Firmeninformationen zukünftig nicht mehr geschützt ist.

Quantencomputer – eine Zukunftsvision?

Quantencomputing verbindet die Quantenphysik mit der Informatik und verspricht somit eine bislang nicht für möglich gehaltene Rechenleistung. Damit birgt die Quanteninformatik ein enormes Potenzial im Kontext der Lösung von komplexen Herausforderungen, wie beispielsweise in Systemen wie Klimamodellen oder dem Gesundheitswesen. Forschende wollen die Wechselwirkungen von Molekülen oder deren mögliche Zustände simulieren, was zu einem Durchbruch bei der Entwicklung neuer Medikamente führen kann. Anwendungen der künstlichen Intelligenz und die Verarbeitung von Big Data könnten mit Quantencomputern einen gewaltigen Sprung nach vorn machen. Krankheiten oder das Wetter könnten langfristig vorhergesagt werden, weil Quantensimulationen gleichzeitig Millionen von Variablen – vergangene, gegenwärtige und sogar zukünftige – in die Berechnung einbeziehen können.

Bei so unterschiedlichen Anwendungsoptionen fehlt es nicht an Finanzierungsbereitschaft sowohl von Regierungen (China und die USA sind an der Spitze) als auch globalen Konzernen wie Google, IBM und Amazon. Aktuell liegt die angewandte Forschung zeitlich sogar vor dem Plan, sodass momentan ab 2027/28 mit ausreichend leistungsfähigen Quantencomputern gerechnet wird.

Quantum Cybersecurity

Gleichzeitig kann ironischerweise gerade ein anderes Feld der Quantentechnologie für den Aufbau leistungsfähiger Verschlüsselung genutzt werden. Mit Hilfe der Quantentechnologie ist es zum Beispiel erstmals möglich, mathematisch beweisbare, nicht hackbare Verschlüsselungstechnologien zu entwickeln - sowohl gegen heutige Standardcomputer als auch gegen zukünftige Quantencomputer.

Dabei wird zwischen Quantenkryptographie und Post-Quanten-Kryptographie unterschieden:

- Die Quantenkryptographie nutzt quantenmechanische Effekte, um eine sichere Übertragung der Schlüssel zu gewährleisten. Im Gegensatz zu bisherigen kryptographischen Verfahren bilden also physikalische Effekte und nicht mathematische Annahmen (Algorithmen) die Grundlage, sodass die synchrone Verschlüsselung gewählt werden kann.

- Die Quantenkryptographie mit Quantum-Key-Distribution (QKD) nutzt Photonen, um mit ihren wesentlichen Eigenschaften die Zusammensetzung des Schlüssels beim Sender und Empfänger zu ermöglichen und so ein nicht hackbares Verschlüsselungssystem zu kreieren. Dies ist darauf zurückzuführen, dass der Quantenzustand eines Systems nicht gemessen werden kann, ohne es zu beeinflussen. Folglich führen sowohl Abhör- als auch Manipulationsversuche jeweils zum direkten Ausschluss des generierten Schlüssels.
- QKD-Protokolle verwenden Zufallszahlen und ihre Sicherheit hängt stark von der Qualität der verwendeten Zufallszahlengeneratoren ab. Diese dürfen zum Beispiel unter keinen Umständen deterministisch sein. In diesem Zusammenhang werden Quantum Random Number Generators (QRNGs) verwendet.
- QRNGs erzeugen Zufälligkeit durch die Messung von Quantenprozessen, die von Natur aus nicht deterministisch sind. Die Vorteile sind vielfältig. Sie liegen beispielsweise in der Nutzung der Quantenunbestimmtheit und vor allem in der Fähigkeit, den Ursprung der Unvorhersehbarkeit zu verstehen und zu verifizieren - was eine wichtige Voraussetzung für die gesamte Cybersicherheitskette ist.
- Die Post-Quantum-Kryptografie beruht auf mathematischen Methoden, um die Kryptografie auch ohne den Einsatz von Quantentechnologie auf das Quantencomputing vorzubereiten.
- Für die Post-Quantum-Kryptografie wurden zahlreiche verschiedene Verfahren und Algorithmen entwickelt, die vom NIST (National Institute of Standards and Technology) erforscht und bereits standardisiert wurden.

AUTOR

PROF. MARCIN PAWŁOWSKI

EXPERTE FÜR QUANTUM CYBERSECURITY AN DER UNIVERSITÄT DANZIG SOWIE FOUNDER DER QUANTUM CYBERSECURITY GROUP

Beide Methoden der quantensicheren Kryptografie bieten ihre Vorteile und es ist wahrscheinlich, dass sich in Zukunft eine Kombination aus beiden durchsetzen wird. Kritische Infrastrukturen, Verbindungsknoten, autarke Netze und Satellitenkommunikation werden tendenziell durch Quantenkryptographie geschützt werden. Die heutige mobile Datenübertragung und die klassische Kommunikation können sich auf die Post-Quanten-Kryptografie stützen, die die heutige Infrastruktur nutzt.

> „Quantencomputing verbindet die Quantenphysik mit der Informatik und verspricht somit eine bislang nicht für möglich gehaltene Rechenleistung."

Warum es notwendig ist, jetzt in die Quanten-Cybersicherheit zu investieren

Auch wenn Quantencomputer derzeit nur eine Leistung von etwa 400 hochwertigen Qubits erreichen - und damit nur etwa 10 % der Menge, die erforderlich ist, um die derzeitige Kryptographie zu knacken - ist es dennoch von größter Bedeutung, bereits jetzt geeignete Maßnahmen im Bereich der Quantum Cybersicherheit zu ergreifen und zu testen.

Zum einen führen diese Projekte zu einer erhöhten Sensibilisierung und einem erfahrenen Umgang mit der innovativen Technologie. Zweitens wird die technologische Entwicklung in Deutschland und Europa in hohem Maße beschleunigt und die Produktqualität massiv gesteigert. Und drittens können heutige Daten und ausgetauschte Informationen zwar noch nicht von Quantencomputern gehackt, aber abgefangen und gespeichert werden. Nach dem Prinzip: „Harvest now, decrypt later" (HNDL) können also Daten, die für Unternehmen langfristig relevant sind, später entschlüsselt werden.

Auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) rät, sich jetzt auf die Quantensicherheit vorzubereiten, da dringend sichere Schlüssel und eine abhörsichere Schlüsselverteilung auf Basis neuartiger Kommunikationstechnologien benötigt werden - insbesondere in den Bereichen der kritischen Infrastruktur, des Gesundheitswesens und der Verwaltung. Allerdings ist in Deutschland die Bedeutung des Themas bei Weitem noch nicht hoch genug und es gibt dringenden Handlungsbedarf, um Politik, Wirtschaft und auch die Gesellschaft zu sensibilisieren. •