Warum es bereits jetzt von großer Bedeutung ist, sich mit Quantum Cybersecurity zu beschäftigen

CYBERSICHERHEIT FÜR DAS QUANTENCOMPUTER-ZEITALTER

Bild: Savinus - stock.adobe.com

Durch die Entwicklung und Nutzung von Quantencomputern steht die Cybersicherheit vor einem dramatischen Kipppunkt. Die heutige Standardverschlüsselung wird in naher Zukunft einfach nicht mehr ausreichend sicher sein. Vor dem Hintergrund exponentiell gestiegener politischer Spionage und kommerziell motivierter Cyberangriffe steigt das Risiko ins Unermessliche. Es ist daher von höchster Bedeutung, dass Politik, Wirtschaft und Gesellschaft für die Relevanz von Quantum Cybersecurity sensibilisiert werden und entsprechende Gegenmaßnahmen vorbereitet und umgesetzt werden.

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.

DAS POTENZIAL VON QUANTENCOMPUTERN

Quantencomputing verbindet die Quantenphysik mit der Informatik und verspricht eine bislang für unmöglich gehaltene Rechenleistung. Statt mit klassischen Bits arbeiten Quantencomputer mit Quantenbits, auch Qubits genannt. Im Gegensatz zu den klassischen Bits der Binärinformatik, welche die Zustände 1 oder 0 annehmen können, können Qubits eine Überlagerung dieser beiden Zustände darstellen. Dadurch ermöglichen sie (eine bestimmte Art von) parallelen Rechenoperationen, welche die Rechenleistung exponentiell mit der Anzahl der verfügbaren Qubits steigern.

Die Begeisterung für Quantencomputing und Quanteninformatik ist deutlich spürbar. Die Quanteninformatik birgt ein enormes Potenzial zur Lösung komplexer Herausforderungen, beispielsweise in Bereichen wie Klimamodellen oder dem Gesundheitswesen. Forschende möchten die Wechselwirkungen von Molekülen oder deren mögliche Zustände simulieren, was zu einem Durchbruch bei der Entwicklung neuer Medikamente führen könnte. 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, da Quantensimulationen gleichzeitig Millionen von Variablen – vergangene, gegenwärtige und sogar zukünftige – in die Berechnung einbeziehen können.

CYBERRISIKEN DURCH QUANTENCOMPUTER

Die Entwicklung von Quantencomputern birgt zweifellos viele Vorteile, aber es dürfen auch die möglichen Nachteile nicht außer Acht gelassen werden. Der Einsatz von Quantencomputern bringt die Bedrohung der Cybersicherheit auf ein deutlich höheres Niveau.

Heutzutage nutzen wir asymmetrische Verschlüsselung (Kryptografie) zum Schutz sensibler Daten und zur sicheren Übertragung von Informationen. Doch in der Ära der Quantencomputer wird dieses Verfahren mit einem öffentlichen und einem privaten Schlüssel nicht mehr ausreichend sicher sein. Die bisherige „Standardsicherheit" wird ausgehebelt, da Quantencomputer private Schlüssel innerhalb weniger Minuten entschlüsseln können. Das bedeutet, dass der Zugriff auf Bankkonten, persönliche Gesundheitsakten oder vertrauliche Firmeninformationen nicht mehr geschützt ist.

Daher ist es dringend erforderlich, Politik, Wirtschaft und Gesellschaft für dieses Thema zu sensibilisieren und jetzt schon in Verfahren für quantensichere Kommunikation zu investieren. Die USA haben bereits 2022 eine Roadmap für den Übergang zu neuen Verschlüsselungsverfahren angekündigt und damit eine Vorreiterrolle eingenommen.

Auch in Europa werden sichere Schlüssel und eine abhörsichere Schlüsselverteilung auf Basis innovativer Kommunikationstechnologien benötigt, insbesondere in Bereichen wie kritische Infrastruktur, Gesundheitswesen und Verwaltung. Es ist wichtig, dass wir frühzeitig Maßnahmen ergreifen, um uns vor den potenziellen Sicherheitsrisiken zu schützen, welche die Quantencomputertechnologie mit sich bringt.

MIT QUANTUM CYBERSECURITY DAGEGENHALTEN

Dennoch ist die Quantentechnologie natürlich nicht per se ein „Gegner" der Cybersicherheit, sondern kann ebenso zur Generierung leistungsfähiger Verschlüsselung genutzt werden. Mithilfe der Quantentechnologie ist es zum Beispiel erstmals möglich, mathematisch be-

weisbare, nicht hackbare Verschlüsselungstechnologien zu entwickeln - sowohl gegen heutige Standardcomputer als auch gegen zukünftige Quantencomputer. Dabei wird zwischen Quantenkryptografie und Post-Quanten-Kryptografie unterschieden:

Die *Quantenkryptografie* nutzt quantenmechanische Effekte, um Informationen sicher zu verschlüsseln. Im Gegensatz zu bisherigen kryptografischen Verfahren bilden also physikalische Effekte und nicht mathematische Annahmen sowie Algorithmen die Grundlage für die Verschlüsselung von Daten.

Die Quantenkryptografie mit Quantum-Key-Distribution (QKD) nutzt Elementarteilchen und Photonen, um mit ihren wesentlichen Eigenschaften ein nicht hackbares Verschlüsselungssystem zu schaffen. Dies ist darauf zurückzuführen, dass der Quantenzustand eines Systems nicht gemessen werden kann, ohne es zu beeinflussen. Folglich werden sowohl Abhör- als auch Manipulationsversuche immer erkannt.

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 National Institute of Standards and Technology (NIST) erforscht und bereits standardisiert wurden. Zu diesen Verfahren gehören:

- komplexe mehrdimensionale mathematische Gitternetze
- multivariante Polynome (zum Beispiel quadratische Gleichungssysteme mit mehreren Variablen)
- kollisionssichere Hash-Funktionen
- Isogenesen zwischen elliptischen Kurven
- symmetrische Verfahren mit langen Schlüsseln

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 Quantenkryptografie geschützt werden. Die heutige mobile Datenübertragung und die klassische Kommunikation können sich auf die Post-Quanten-Kryptografie stützen, welche heutige Infrastrukturen nutzt.

WARUM ES NOTWENDIG IST, JETZT IN DIE QUANTEN-CYBERSICHERHEIT ZU INVESTIEREN

Obwohl Quantencomputer derzeit nur etwa zehn Prozent der benötigten Menge an Qubits erreichen, um die heutige Kryptografie zu knacken, ist es von großer Bedeutung, bereits jetzt geeignete Maßnahmen im Bereich der Quantum Cybersicherheit zu ergreifen und zu testen.

Diese Projekte führen zu einer erhöhten Sensibilisierung und einem erfahrenen Umgang mit der innovativen Technologie. Sie beschleunigen auch die technologische Entwicklung in Deutschland und Europa und steigern die Produktqualität erheblich. Zudem 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 langfristig relevant sind, später entschlüsselt werden.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) empfiehlt ebenfalls, sich jetzt auf die Quantensicherheit vorzubereiten. Allerdings ist die Bedeutung des Themas in Deutschland noch nicht ausreichend erkannt, und dringendes Handeln ist erforderlich.

Deutschland sollte sich im internationalen Diskurs positionieren und sich stärker in die Europäische Quantenkommunikationsinfrastruktur Initiative (EuroQCI) einbringen. Das Ziel sollte sein, eine starke Rolle für Deutschland und Europa zu übernehmen, um einerseits die richtigen Weichen zu stellen und andererseits wettbewerbsfähig zu bleiben und zu werden. ■

OLIVER WEIMANN,
Founder & CEO der Quantum Cybersecurity Group (www.qscgroup.io)

PROF. MARCIN PAWŁOWSKI,
Experte für Quantum Cybersecurity an der Universität Danzig sowie Founder der Quantum Cybersecurity Group (www.qscgroup.io)