

Quantencomputer im Vormarsch: Revolutioniert sicherheitsrelevante Technologien?

Entdecken Sie, wie Quantencomputing 2025 verschiedene Branchen revolutioniert und Zukunftsherausforderungen in der Cybersicherheit angeht.



Es gibt keinen spezifischen Ort oder Adresse im Text. - Die Zukunft der Technologie, insbesondere der Versuch, das Potenzial der Quanteninformatik zu nutzen, ist bereits heute ein heiß diskutiertes Thema. Im Jahr 2025 wird deutlich, wie diese Technologie nicht nur die digitale Kommunikation revolutionieren könnte, sondern auch Bereiche wie die Arzneimittelentwicklung und die Cybersicherheit maßgeblich beeinflusst. Laut **Anewz** werden Quantencomputer durch die Verwendung von Qubits, die gleichzeitig 0 und 1 darstellen können, in der Lage sein, Informationen erheblich effizienter zu verarbeiten als herkömmliche Computer, die nur mit Bits

operieren.

Was macht das Besondere an Qubits? Dank der Superposition können sie mehr Informationen speichern sowie mehrere Möglichkeiten gleichzeitig verarbeiten. Dies ermöglicht es Quantencomputern, komplexe Probleme viel schneller zu lösen. Zudem führt das Prinzip der Verschränkung dazu, dass die Veränderung eines Qubits die anderen beeinflusst, egal wie weit sie voneinander entfernt sind. Damit ergeben sich viele potenzielle Anwendungen aus dieser Technologie: von einer schnelleren Medikamentenentwicklung über verbesserte Herstellungsverfahren bis hin zu optimierten Verkehrs- und Routenplanungen.

Die Bedrohung durch Quantencomputer

Doch während die Technologie viele Vorteile verspricht, birgt sie auch Risiken, besonders im Bereich der Cybersicherheit. Quantencomputer könnten bestehende Verschlüsselungsmethoden, die unsere digitalen Daten schützen, schnell knacken. Laut **PostQuantum** sind Cryptographically Relevant Quantum Computers (CRQCs) potenziell in der Lage, moderne kryptographische Algorithmen, die für die Sicherheit von Systemen wie RSA und ECC verantwortlich sind, zu brechen. Experten schätzen, dass wir binnen der nächsten 15-20 Jahre mit der Entwicklung solcher Computer rechnen können, die langfristig für ernsthafte Sicherheitsprobleme sorgen könnten.

Ein erhebliches Risiko dabei ist die Rückwärtsdekodierung sensibler Kommunikation und das Fälschen digitaler Signaturen. Im Zuge dieser Entwicklungen sprechen Fachleute bereits über die Notwendigkeit, sich auf Post-Quanten-Kryptographie (PQC) vorzubereiten. Diese neuen Algorithmen sollen gegen Angriffe durch Quantencomputer resistent sein und in Zukunft verlässlich eingesetzt werden können. Wichtige Ansätze in diesem Bereich sind lattice-basierte, code-basierte und hash-basierte Verfahren.

Die Rolle von Quantencomputern und deren Entwicklung

Angeblich gibt es bis heute keinen Quantencomputer, der bemerkenswert besser ist als seine konventionellen Pendanten, aber das Querformat von Quantencomputern entwickelt sich rasant weiter. Deshalb investiert die Welt zunehmend in diese Technologie; bis 2030 wird ein globales Investment von etwa 9,1 Milliarden Dollar erwartet, was die Wichtigkeit und Dringlichkeit in der Forschung unterstreicht. Technologien wie IBM und Google bieten Cloud-Services an, die es Nutzern ermöglichen, die Quantenprogrammierung auszuprobieren, ohne dass sie selbst ein eigenes Labor benötigen.

Wie wirken sich diese Fortschritte auf bestehende Industriepraktiken aus? Sektoren wie Gesundheitswesen, Fertigung, Finanzen und Klimawissenschaften erkunden alle die Möglichkeiten von Quantencomputing. Gleichzeitig müssen Unternehmen auch die Herausforderungen berücksichtigen, die mit der Migration zu Post-Quanten-Kryptographie verbunden sind, einschließlich der Standards, der Interoperabilität und der Leistung.

Abschließend lässt sich sagen, dass die Weiterentwicklung der Quanteninformatik sowohl immense Chancen als auch erhebliche Risiken birgt. Die Zeit drängt, denn das Umfeld der digitalen Sicherheit muss sich schnell anpassen, um gegen die Herausforderungen gewappnet zu sein, die die Quantenrevolution mit sich bringt.

Details	
Ort	Es gibt keinen spezifischen Ort oder Adresse im Text.
Quellen	• anewz.tv • postquantum.com

Besuchen Sie uns auf: wom87.de