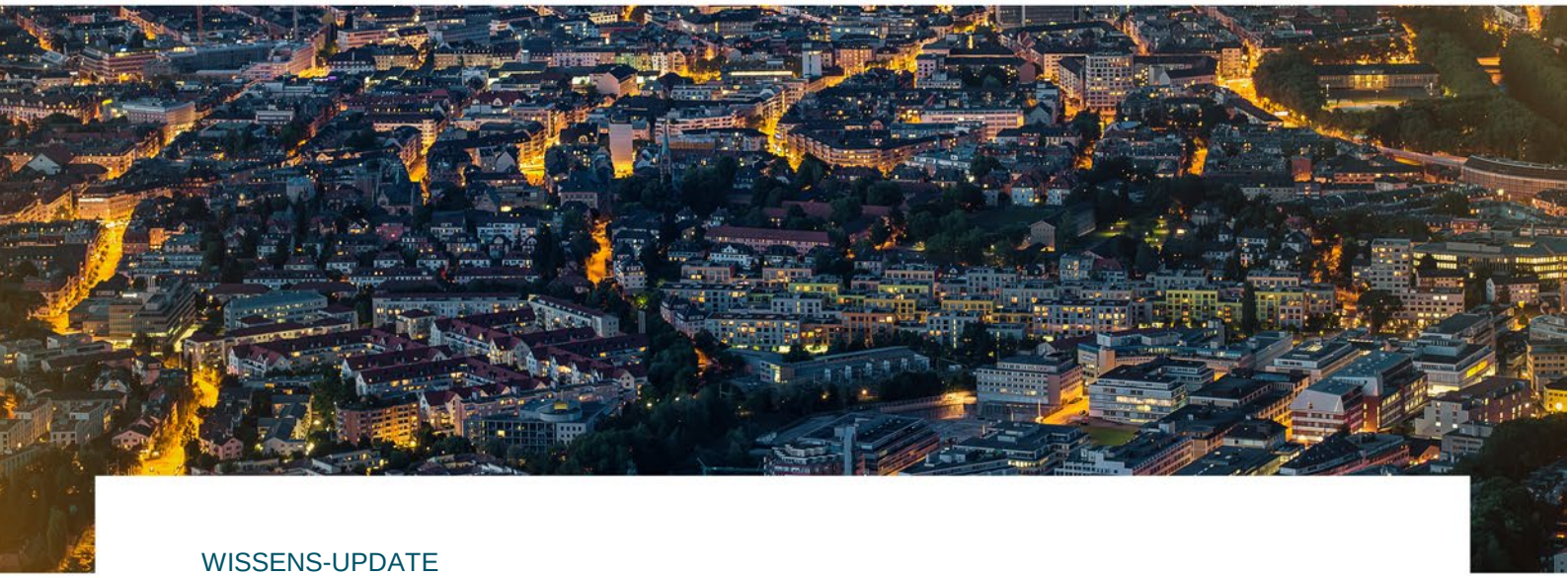
CyOne Security AG
Hinterbergstrasse 18
6312 Steinhausen

Telefon +41 41 748 85 00
info@cyone.ch
cyone.ch



WISSENS-UPDATE

Quantencomputer – In der Kryptografie bricht eine neue Ära an

Dr. Markus Stadler | CTO | Steinhausen, 2. April 2019

Quantencomputer stehen möglicherweise kurz vor dem Durchbruch. Die leistungsstarken Rechner bieten neue Möglichkeiten, bedrohen gleichzeitig aber die altbewährten Public Key-Verfahren. Damit IT-Systeme auch in Zukunft sicher sind, braucht es «Post-Quantenkryptografie».

Der Quantencomputer war lange mehr Fantasie als Realität. Als theoretisches Konzept geistert er schon seit 1982 durch die Wissenschaft. Damals formulierte Physik-Nobelpreisträger Richard Feynman erstmals die Idee für einen Computer, der die Prinzipien der Quantenmechanik nutzt, um schwer zugängliche Eigenschaften von Festkörpern, Flüssigkeiten und Gasen zu simulieren.

Nun mehren sich die Anzeichen, dass die Theorie in der Praxis funktioniert. Den Beweis dafür hat IBM im Januar 2019 auf der Technologie-Messe CES in Las Vegas präsentiert: «Q System One» ist der erste kommerziell verfügbare Quantencomputer. Interessierte Unternehmen und Forschungsinstitutionen sollen per Cloud Zugriff erhalten. ExxonMobil und das CERN sind bereits mit an Bord. An vergleichbaren Systemen arbeiten Konzerne wie Google, Intel, Toshiba und Microsoft. Sie alle setzen grosse Hoffnungen in den Quantencomputer, der gängige Rechner früher oder später in den Schatten stellen soll.

In Europa wird die Entwicklung der neuen Technologie ebenfalls vorangetrieben. Im letzten Jahr fiel der Startschuss für ein EU-Forschungsprojekt, das den Bau eines Quantencomputers bis 2021 zum Ziel hat. Er soll die Simulation von Prozessen in Chemie und Materialwissenschaft beschleunigen und für die Forschung an künstlicher Intelligenz eingesetzt werden.

Rechnen bei minus 273°C

Herkömmliche Computer rechnen mit Bits und diese kennen nur zwei Zustände: 0 und 1. Quantencomputer überwinden das binäre Entweder-oder. Ihre kleinste Recheneinheit sind Quantenbits, kurz Qubits. Mit ihnen können beliebig viele Überlagerungszustände von Nullen und Einsen verarbeitet werden – und das simultan. Möglich macht dies das quantenmechanische Prinzip der Superposition: Teilchen können verschiedenste Zustände gleichzeitig annehmen. Deshalb können Quantencomputer Operationen simultan durchführen, statt wie normale Computer Rechenschritte nacheinander abzuarbeiten. Dadurch verkürzt sich die Rechenzeit bei komplexen Aufgaben erheblich. Innert kürzester Zeit lassen sich beispielsweise alle möglichen Varianten einer Formel kalkulieren.

Quantencomputer sind ebenso komplex wie fragil. Den Entwicklern stellt sich das Problem, dass Qubits nur unter ganz speziellen Umständen benutzt und gemessen werden können – nämlich nur nahe am absoluten Nullpunkt, bei minus 273,135 Grad Celsius. Hinzu kommt: Qubits dürfen ausschliesslich untereinander interagieren, damit die sogenannte Quantenkohärenz aufrechterhalten bleibt. Deshalb muss das System sowohl vor Erschütterungen als auch vor elektromagnetischer Strahlung geschützt sein. Aufgrund der aufwendigen Kühl- und Schutzmechanismen stecken Quantencomputer in riesigen Gehäusen, obwohl der Prozessor eigentlich nur wenige Millimeter gross ist. IBMs «Q System One» etwa wird mit einem 2,7 Meter hohen Glaskasten vor Umwelteinflüssen geschützt.

Zwei Seiten einer Medaille

Bis heute gibt es Dinge, an denen sich herkömmliche Computer die Zähne ausbeissen. Dazu gehört zum Beispiel das Koffein-Molekül. Es ist so komplex, dass es sich mit gängigen Mitteln nicht simulieren lässt. Ein Quantencomputer könnte diese Aufgabe lösen. Da er nach den Prinzipien der Quantenmechanik arbeitet, lassen sich damit auf mikroskopisch kleiner Ebene Wechselwirkungen von Atomen und Molekülen analysieren. Quantencomputer sind somit prädestiniert, um komplexe Stoffe zu erforschen und könnten deshalb für die Entwicklung neuer Materialien oder Medikamente hilfreich sein.

Das ist jedoch nur die eine Seite der Medaille. Weil Quantencomputer bisher unlösbare Aufgaben lösen können, bedrohen sie die IT-Sicherheit. Betroffen sind insbesondere asymmetrische Verschlüsselungsverfahren. Der US-Mathematiker Peter Shor hat bereits 1994 aufgezeigt, dass mithilfe eines Quantencomputers effiziente Algorithmen zur Primfaktorzerlegung grosser Zahlen und zum Finden diskreter Logarithmen möglich wären. Weil fast alle asymmetrischen Verfahren, sowohl für Verschlüsselung als auch für digitale Signaturen, auf diesen beiden mathematischen Problemen basieren, hätte der Bau eines ausgereiften Quantencomputers fatale Auswirkungen auf die IT-Sicherheit.

Das Unmögliche wird möglich

Bei asymmetrischen Verschlüsselungsverfahren kommen zwei Schlüssel zum Einsatz: Der sogenannte Public Key ermöglicht die Chiffrierung und wird jedem kommunikationswilligen Teilnehmer zugänglich gemacht. Der zweite Schlüssel, mit dem sich die Informationen dechiffrieren lassen, wird hingegen geheim gehalten. Man kann sich diesen Schutzmechanismus als mathematische Einbahnstrasse vorstellen: Die Verschlüsselung ist simpel, denn es ist zum Beispiel sehr einfach, zwei Primzahlen zu multiplizieren. Versucht man die Daten jedoch zu entschlüsseln und den Rechenweg in die andere Richtung zu beschreiten und die Zahl in ihre Primfaktoren zu zerlegen, ist die Aufgabe deutlich komplexer – und für gängige Computer unlösbar.

Auf der Komplexität der Primfaktorzerlegung basiert etwa RSA, der bekannteste aller Verschlüsselungsalgorithmen, der 1977 von Ronald Rivest, Adi Shamir und Leonard Adleman entwickelt wurde. Mit einem Quantencomputer würde das Faktorisierungsproblem plötzlich lösbar. Auch andere Verschlüsselungsverfahren wie das Elgamal-Signaturverfahren und DSA sind von der Technologie bedroht, da Quantencomputer auch das bisher unlösbare Problem des diskreten Logarithmus lösen können.

Weit weniger kritisch ist die Situation bei der symmetrischen Verschlüsselung. Mithilfe des sogenannten «Grover-Algorithmus» könnte ein Quantencomputer derartige Krypto-Systeme zwar angreifen, allerdings würde sich die Komplexität des Angriffs nur auf die Quadratwurzel reduzieren. Anders ausgedrückt: Ein Algorithmus mit 128 Bit würde nur noch 64 Bit Sicherheit bieten. Die Lösung ist also einfach: Wird die Schlüssellänge verdoppelt, können Quantencomputer symmetrischen Systemen nichts anhaben.

Quantensichere Algorithmen sind gefragt

Da Quantencomputer möglicherweise vor dem Durchbruch stehen, gilt es, rasch Verschlüsselungsverfahren zu entwickeln, die den leistungsstarken Rechnern standhalten. Momentan arbeiten Experten unter der Leitung des US-Standardisierungsgremiums National Institute of Standards and Technology (NIST) an einem Standard für die sogenannte «Post-Quantenkryptografie». Von anfänglich 80 eingereichten Algorithmen sind aktuell noch 26 im Rennen und der Evaluierungsprozess wird noch mindestens drei Jahre in Anspruch nehmen. Bis dahin werden Quantencomputer weitere Fortschritte machen.

Heute sind Quantencomputer herkömmlichen Rechnern zwar noch in keiner Anwendung überlegen, Experten rechnen aber damit, dass dieser als «Quantum Supremacy» bezeichnete Schritt bald erreicht werden könnte. Google will in den nächsten Monaten mit dem 72-Qubit-Chip Bristlecone den Beweis für die Überlegenheit von Quantencomputern antreten. Zum Vergleich: IBMs «Q System One» hat lediglich eine Leistung von 20 Qubits. Der für 2021 geplante EU-Supercomputer hingegen soll bereits über 100 Qubits verfügen.

Der Paradigmenwechsel scheint also absehbar, doch wann genau er eintritt, bleibt ungewiss. Fest steht: In den nächsten Jahren kommt es zu einem Kopf-an-Kopf-Rennen von Entwicklern und Kryptologen. Gefragt ist deshalb «Krypto-Agilität». Für Unternehmen und öffentliche Institutionen geht es darum, die IT-Systeme schrittweise auf die neuen Gefahren auszurichten und so weit wie möglich gegen potenzielle Quantenrechner-Attacken zu wappnen.

Quantenkryptografie löst nur Teilproblem

Zwar bedroht die Quantenphysik die IT-Sicherheit, aber sie bietet auch Wege, um diese zu erhöhen. Die noch junge Quantenkryptografie verspricht eine geschützte Kommunikation in Netzwerken, die mit dem Internet vergleichbar sind. Österreichischen Forschern ist es im Dezember 2018 erstmals gelungen, vier Teilnehmer in einem abhörsicheren Quantennetzwerk zu verbinden.

Quantennetzwerke nutzen ein Phänomen der Quantenphysik, die sogenannte Quantenverschränkung, nach deren Regeln zwei Teilchen einen gemeinsamen Zustand bilden können, auch wenn sie über eine weite Entfernung voneinander getrennt sind. So können Quantenzustände über weite Distanzen teleportiert werden. Die Quantenverschlüsselung verhindert, dass Aussenstehende in das Netzwerk eindringen. Da sich Quanteninformation grundsätzlich nicht kopieren lässt, kann der Schlüssel nicht von Cyber-Kriminellen abgefangen werden.

Somit könnte mit der Quantenkryptografie eine sichere Kommunikation aufgebaut werden, die auch gegen Quantencomputer sicher ist. Aber die Quantenkryptografie löst damit nur ein Problem unter vielen. Denn für die sichere Speicherung und Archivierung von Daten und vor allem für digitale Signaturen liefert sie keine Antworten.

CyOne Security ist der vertrauensvolle Partner dafür

Es gilt, die Schweiz schon heute vor den Risiken durch Quantencomputer zu schützen, auch wenn die reale Bedrohung wohl erst in der Zukunft eintritt. Denn eine moderne und effiziente Informations- und Kommunikationstechnologie bildet das Rückgrat von Staat und Wirtschaft und ist unabdingbar. Agil, skalierbar und mit einer gesicherten Verfügbarkeit trägt sie entscheidend zum nachhaltigen Erfolg und zur Wettbewerbsfähigkeit der Schweiz bei.

Setzen Sie dafür auf die langjährige Erfahrung und die 360°-Sicherheitskompetenz der CyOne Security. Als rein schweizerisches Unternehmen bieten wir den kundenspezifischen Cyber-Risiken angepasste, umfassende Sicherheitskonzepte und -lösungen auf höchstem Niveau für Product Security, System Security sowie Operational Security an.

Beginnen Sie heute, Ihre Organisation und somit die Schweiz vor Quantencomputer-Risiken zu schützen.

Machen Sie den ersten Schritt: Analysieren Sie gemeinsam mit unseren Experten Ihre aktuellen und zukünftigen Cyber-Sicherheitsbedürfnisse und entsprechende Sicherheitslösungen.

Kontaktieren Sie uns für ein kostenloses Expertengespräch.