FORSCHUNGSFORUM DER ÖSTERREICHISCHEN FACHHOCHSCHULEN 2024

FERDINAND PORSCHE FERNFH

University of Applied Sciences

Quantum Computing: Bedrohungsszenario für die State of the Art Informationssicherheit?

Mag. Michael Kirchmair, MA;

Christoph Jungbauer, BA MA MA

Ferdinand Porsche FernFH

Abstract

Quantencomputer haben das Potenzial, durch nie dagewesene Rechenkraft, bedeutende mathematische und wirtschaftliche Probleme zu lösen und die digitale Transformation zu beschleunigen. Gleichzeitig kann diese Rechenkraft dazu verwendet werden, heutzutage in nahezu allen IT-Infrastrukturen tief verankerte asymmetrische Verschlüsselungsverfahren zu knacken.

In dieser Forschungsarbeit wird die Funktionsweise von Quantencomputern und deren aktueller technischer Reifestand evaluiert und die Bedrohung durch theoretische Angriffsmodelle dargestellt. Ziel des empirischen Teils dieser Arbeit war es, gemeinsam mit Expert_Innen zu evaluieren, ob sich österreichische Unternehmen der Angriffsszenarien durch Quantencomputer bewusst sind. Darüber hinaus wurden potenzielle Maßnahmen dagegen sowie deren Implementierung diskutiert.

Die Arbeit kommt zu dem Schluss, dass sich facheinschlägige Führungskräfte durchaus mit Quantencomputern befasst haben und sich auch dem Risiko bewusst sind. Da diese Expert_Innen aktuell jedoch dringlichere Bedrohungen zu bewältigen haben, sind aktuell noch keine Maßnahmen wie die Implementierung von Post-Quanten-Kryptographie geplant.

1. Einleitung

Quantencomputer werden in vielen Bereichen als Disruptoren für bedeutende wirtschaftliche und gesellschaftliche Probleme gesehen: Begonnen mit neuen Möglichkeiten in der künstlichen Intelligenz über die Lösung von Simulations- und Optimierungsproblemen bis hin zur Identifikation noch unbekannter Ansätze zur Bekämpfung des Klimawandels – die Technologie hinter Quantencomputern bringt viele bedeutsame Chancen mit sich (1,2,6).

Doch gleichzeitig birgt die Technologie auch Risiken: So wird vor der Rechenkraft von Quantencomputern gewarnt, da sie eine Gefahr für State of the Art Verschlüsselungstechnologien darstellt. Diese basieren auf mathematischen Einwegfunktionen wie beispielweise der Primfaktorenzerlegung und sind durch gängige Angriffsszenarien praktisch nicht zu knacken. Durch die grundlegend neue Funktionsweise von Quantencomputern ist es deren Recheneinheiten jedoch möglich, mehrere Zustände gleichzeitig einzunehmen, mehrere Berechnungen parallel durchzuführen und dadurch Einwegfunktionen umzukehren. Auf diese Art und Weise könnte es in naher Zukunft

realistisch sein, aktuell als sicher geltende Verschlüsselungstechnologien von Regierungen, Banken, kritischer Infrastruktur, Privatpersonen u.v.m. mit geringem Zeitaufwand zu entschlüsseln (7,9,11).
Genau aus diesem Grund beschäftigen sich Wissenschaftler_Innen rund um die Welt mit der Entwicklung von Verschlüsselungstechnologien, die auch von Quantencomputern nicht geknackt werden können. Auch wenn leistungsstarke Quantencomputer aus Sicht der Forschung noch weit in der Ferne liegen, stellt sich bereits jetzt die Frage, wie Organisationen früh genug ihre Daten, Passwörter und Geheimnisse vor dem Zeitalter der Quantencomputer schützen können (4,5,9).
Zielsetzung der Arbeit war es herauszufinden, inwieweit sich österreichische Unternehmen der Bedrohung durch Quantencomputer bewusst sind und mithilfe welcher Maßnahmen sie sich für diese technologische Transformation rüsten.

2. Methodik

Die methodische Herangehensweise erfolgte zunächst in Form einer Literaturrecherche, in der Grundlagen der Quantenphysik, von Quantencomputern und vom Informationssicherheitsmanagement beleuchtet wurden. Anschließend wurde die Funktionsweise von Kryptographie näher erläutert und Angriffsszenarien mittels Quantencomputern herausgearbeitet. Schlussendlich wurden einige Handlungsempfehlungen des aktuellen Forschungsstands, wie das Standardisierungsverfahren für Post-Quanten-Kryptographie vom NIST (3) zusammengefasst.

Anschließend wurde auf Basis der Grundlagenrecherche ein Interviewleitfaden erstellt, in den der rote Faden der Arbeit übernommen wurde und mit dessen Unterstützung strukturierte Expert_Inneninterviews mit Entscheidungsträger_Innen aus den Bereichen IT-Security, Risikomanagement und IT-Leitung durchgeführt wurden. Die Auswahl der Expert_Innen erfolgte gezielt aus KMUs, Beratungsunternehmen, Industrie und kritischer Infrastruktur. Nach Durchführung der Interviews wurde eine qualitative Inhaltsanalyse nach Mayring (10) durchgeführt und die Ergebnisse nach mehreren Qualitätssicherungsiterationen zu insgesamt 7 Kategorien zusammengefasst.

3. Ergebnisse

Die Ergebnisanalyse zeigt, dass das Bewusstsein für die durch Quantencomputer verursachten Bedrohungen in der Praxis noch unterentwickelt ist. Obwohl der Einsatz asymmetrischer Kryptographieverfahren in Zukunft ein Sicherheitsrisiko darstellen wird, ist die Kenntnis und Bereitschaft zur Implementierung von Post-Quanten-Kryptographie noch nicht weit genug verbreitet. Viel mehr fokussieren sich Unternehmen auf akutere Bedrohungen der IT-Sicherheit wie Ransomware, Phishing und Angriffe mit Cloud-Ressourcen. Aus ihrer Sicht nehmen diese Angriffe neue Ausmaße an und werden nicht mehr weniger werden. Zusätzlich ist davon auszugehen, dass leistungsstarke Quantencomputer zunächst im Verborgenen operieren und damit zum Beispiel Wettbewerbsvorteile für Technologiegiganten generieren oder für Spionagetätigkeiten eingesetzt werden.

Zwar ist bekannt, dass die Notwendigkeit zur frühzeitigen Auseinandersetzung mit der Thematik besteht, allerdings sind auch noch keine aus der Forschung bekannten Maßnahmen zur Umrüstung für das Post-Quanten-Zeitalter geplant. Zudem halten die Expert_Innen aktuelle, quantenresistente Verschlüsselungsverfahren für noch nicht ausreichend erprobt und teilweise sogar für ein zusätzliches Sicherheitsrisiko.

Somit bekommt der ISO/IEC 27000-Standard einen immer höheren Stellenwert, indem er durch regelmäßige Risikobewertungen für eine laufende technologische Beobachtung von Quantencomputern sorgt (8).

4. Conclusio & Ausblick

Die Implementierung von Post-Quanten-Kryptographie stellt einen komplexen Prozess dar, da im Grunde genommen alle Geräte in einem Netzwerk aktualisiert, ersetzt oder in Quarantäne verschoben werden müssen. Dazu existieren zwar bereits Migrationsfahrpläne von diversen öffentlichen Einrichtungen wie der ENISA oder dem BSI, die Dauer des Umstiegs wird je nach Größe der Organisationen aber mehrere Jahre dauern.

So stellt sich weiterhin die grundlegende Frage, ab welchem Zeitpunkt Quantencomputer eine Bedrohung für State-of-the-Art Verschlüsselungsverfahren darstellen. Nach aktuellem Stand liegt dieser Zeitpunkt zwar noch 5 bis 10 Jahre in der Ferne, allerdings könnten Angreifer schon heute verschlüsselte Daten abfangen und speichern, mit dem Ziel, sie zu einem späteren Zeitpunkt mit einem leistungsstarken Quantencomputer zu entschlüsseln („Store now decrypt later“).

Außerdem hat auch die jüngste Vergangenheit gezeigt, dass technologische Durchbrüche oft sehr plötzlich und überraschend eintreten können. Ein ähnlich rapider Durchbruch wie im Bereich der künstlichen Intelligenz hätte jedenfalls katastrophale Folgen und würde Milliarden von IT-Systemen auf einen Schlag für Angreifer öffnen. Ob alle wichtigen Systeme bis dahin gerüstet sind, bleibt ebenfalls offen. Es ist auf jeden Fall noch ein langer und intensiver Weg.

5. Literaturverzeichnis

(1) BSI, 2021a. Migration to Post Quantum Cryptography.
(2) BSI, 2021b. Quantum-safe cryptography – fundamentals, current developments and recommendations.
(3) Chen, L., Jordan, S., Liu, Y.-K., Moody, D., Peralta, R., Perlner, R., Smith-Tone, D., 2016. Report on Post-Quantum Cryptography (No. NIST IR 8105). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8105
(4) ENISA, 2021. Post-quantum cryptography: current state and quantum mitigation. Publications Office, LU.
(5) ETSI, 2020. Migration strategies and recommendations to Quantum Safe schemes.
(6) IST Austria, 2021. Dossier - Quantencomputer.
(7) Joseph, D., Misoczki, R., Manzano, M., Tricot, J., Pinuaga, F.D., Lacombe, O., Leichenauer, S., Hidary, J., Venables, P., Hansen, R., 2022. Transitioning organizations to post-quantum cryptography. Nature 605, 237–243. https://doi.org/10.1038/s41586-022-04623-2
(8) Kirchmair, M. 2023. Quantum Computing: Bedrohungsszenario für die State of the Art Informationssicherheit? Ferdinand Porsche FernFH.
(9) KPMG, 2019. Sicherheitsrisiko Quantencomputer. KPMG.
(10) Mayring, P., 2015. Qualitative Inhaltsanalyse: Grundlagen und Techniken, 12., überarb. Aufl. ed. Beltz, Weinheim Basel.
(11) Mosca, M., 2018. Cybersecurity in an Era with Quantum Computers: Will We Be Ready? IEEE Security & Privacy 16, 38–41. https://doi.org/10.1109/MSP.2018.3761723