bankenverband

Themenbeitrag
Quantencomputer bei Banken

25. August 2020

Nicole Hellmich
Associate, Themengruppe Banktechnologie und Sicherheit
+49 30 1663 2326
nicole.hellmich@bdb.de

Der Einsatz von Quantencomputern

Der Einsatz von Quantencomputern beeinflusst alle bisher eingesetzten kryptografischen Verfahren und Produkte der Deutschen Kreditwirtschaft. Unter anderen müssen Verschlüsselungsverfahren für das Online Banking, Prozesse bei Kartenzahlungen und Geldautomaten, aber auch Technologien, auf der beispielsweise die Blockchain beruhen, angepasst werden, um das gleiche Sicherheitsniveau zu erhalten sowie heutige und zukünftige Daten sicher zu speichern.

Was sind Quantencomputer?

Quantencomputer sind eine technologische Entwicklung auf Basis von Gesetzen der Quantenphysik. Durch ihre physikalischen Eigenschaften können sie eine deutlich größere Datenmenge in wesentlich kürzerer Zeit verarbeiten. Dadurch werden Simulationen und Analysen ermöglicht, die mit heutigen Computern, aufgrund der geringen Rechenleistung, nicht möglich sind. Zudem können präzisere Ergebnisse erzielt und genauere Vorhersagen getroffen werden. Die Sicherheit der heutigen kryptografischen Verfahren in der Bankeninfrastruktur beruht unter anderem auf mathematischen Berechnungen, die von heutigen Computern in Monaten oder Jahren entschlüsselt werden müssen. Passwörter, Schlüssel, gespeicherte Daten, u.ä., können durch Quantencomputer in wesentlich kürzerer Zeit als heute „geknackt“ werden. Im Moment besteht noch die Herausforderung eine stabile und fehlerfreie Funktionsweise von Quantencomputern zu schaffen, aber die Technologie entwickelt sich mit sehr hoher Geschwindigkeit. Voraussichtlich werden die Vorteile von Quantencomputern zunächst in der Pharmazie und der Transportbranche zur Lösung von Optimierungsproblemen und Wirkungssimulationen genutzt, später ist auch ein Einsatz in der Cybersicherheit denkbar.

Was bedeutet Post-Quanten-Verfahren?

Post-Quanten-Verfahren beruhen auf mathematischen Problemen, für deren Lösung heute weder effiziente klassische Algorithmen noch effiziente Quantenalgorithmen bekannt sind. An quantenresistenten Verfahren wird derzeit international geforscht. Bisher hat sich noch kein Verfahren eindeutig durchgesetzt, so dass im Moment kein Verfahren vor dem Jahr 2023 standardisiert werden wird, was eine Migration auf diese Verfahren erschwert.

Wie wirken sich Quantencomputer auf kryptografische Verfahren der Bankeninfrastruktur aus?

- Verschlüsselungsverfahren verlieren an Stärke
  Asymmetrische (z.B. https, elliptische Kurven) und symmetrische (z.B. TDES, AES) Verfahren werden deutlich geschwächt. Asymmetrische Verfahren sind durch ihre mathematische Beschaffenheit stärker betroffen. Bei symmetrischen Verfahren kompensiert eine Schlüsselverlängerung die Schwächung teilweise, bei gleichzeitiger Beeinträchtigung der Performance. Internetprotokolle müssen angepasst werden.
- Ist-Situation prüfen
  Eine Analyse und Prüfung der bestehenden Verfahren auf Quantenresistenz und notwendiger Anpassungsbedarf werden derzeit von der Deutschen Kreditwirtschaft ermittelt und bewertet.
- Kryptoagilität erforderlich
  Eine Kombination aus aktuellen und mehreren Post-Quanten-Verfahren ist für die Sicherheit der Systeme und Daten zwingend erforderlich, trotz hoher Investitions- und Instandhaltungskosten für die Banken.

Position des Bankenverbandes zu Quantencomputern

Nach Auffassung des Bankenverbands hat der Einsatz von Quantencomputern Auswirkungen auf alle derzeit genutzten kryptografischen Verschlüsselungsverfahren. Quantencomputer sind auch Enabler für Teilprozesse, so dass sie zum Beispiel künstliche Intelligenz und Cloud Computing unterstützen können. Vorteile und Gefahren durch die Nutzung sind derzeit für die Bankenbranche gering, steigen aber stetig an. Aufgrund langer Migrationszeiträume in der Deutschen Kreditwirtschaft werden jetzt erste Konzepte für quantenresistente Verfahren erstellt. Zudem wird auf europäischer und internationaler Ebene sowohl an der Entwicklung der Post-Quanten-Verfahren teilgenommen als auch die Zusammenarbeit mit Experten und anderen Stakeholdern verstärkt.