GDV Gesamtverband der Versicherer

FOKUS I DIGITALISIERUNG

Quanten-computing vor dem Sprung

Ein weiterer Baustein der IT-Transformation für die Versicherungswirtschaft

Ausgabe

№ 12 • APRIL 2025

GDV

Quantencomputing vor dem Sprung

Herausgeber
Gesamtverband der Deutschen Versicherungswirtschaft e. V.
Wilhelmstraße 43 / 43 G, 10117 Berlin
Postfach 08 02 64, 10002 Berlin
Tel.: +49 30 2020–5000, Fax: +49 30 2020–6000
www.gdv.de, berlin@gdv.de

Verantwortlich
Patrik Maeyer
Leiter Betriebswirtschaft, Prozesse und IT
Tel.: +49 30 2020–5452
E-Mail: p.maeyer@gdv.de

Autoren
Mario Heinemann

Publikationsassistenz
Nadine Luther

Redaktionsschluss dieser Ausgabe
25.03.2025

Bildnachweis
Titel: AA+W – stock.adobe.com

Disclaimer
Die Analyse stellt eine allgemeine, unverbindliche Information dar. Die Inhalte wurden mit der erforderlichen Sorgfalt erstellt. Gleichwohl besteht keine Gewährleistung auf Vollständigkeit, Richtigkeit, Aktualität oder Angemessenheit der darin enthaltenen Angaben oder Einschätzungen. Eine Verwendung liegt in der eigenen Verantwortung des Lesers.

© GDV 2025

Einführung

2022
US-Cybersec. Preparedness ACT

2023
EU-Deklaration Quanten-technologie

2023
BReg D-Handlungs-konzept Quanten-techn.

2024
Quantum Data-Center IBM

2025
Quantum-jubiläumsjahr der Vereinten Nationen

Die Quantentechnologie[1] gilt weltweit als eine Schlüsseltechnologie mit enormen Potenzialen. Vielfältige Entwicklungen und Maßnahmen sowie die jüngsten technischen Fortschritte deuten darauf hin, dass sich demnächst konkrete Auswirkungen bemerkbar machen werden:

- Ende 2022 wurde in den USA der Quantum Computing Cybersecurity Preparedness Act erlassen. Dieser zielt darauf ab, die nationale US-Sicherheit im Hinblick auf zukünftige Bedrohungen durch Quantencomputing zu stärken.

- 26 EU-Mitgliedsstaaten haben Ende 2023 zur strategischen Bedeutung für die Wissenschaft und Wettbewerbsfähigkeit eine Deklaration zur Quantentechnologie unterzeichnet – dies mit dem erklärten Ziel, in Europa ein „quantum valley“ zu errichten.

- Ebenfalls in 2023 hat die Bundesregierung das „Handlungskonzept Quantentechnologie“ verabschiedet. Quantentechnologien werden hier als Zukunftstechnologien mit disruptivem Potenzial und besonders vielversprechenden Anwendungsperspektiven beschrieben. Für die Sicherung der technologischen Souveränität ist ein Finanzrahmen in Höhe von 3 Milliarden Euro vorgesehen – inklusive der der Entwicklung eines universellen Quantencomputers. Deutschland ist nach China weltweit der zweitgrößte öffentliche Geldgeber.[2]

- Mitte 2024 wurde bei Stuttgart das erste Quantum Data Center der IBM außerhalb der USA eröffnet. Das europäischen Quantennetzwerk mit mehr als 80 Unternehmen, Universitäten und Forschungseinrichtungen wird zukünftig auf mehrere Systeme zugreifen können, um quantenbasierte Anwendungen und Algorithmen zu erforschen.[3]

- Die Vereinten Nationen haben das Jahr 2025 zum Internationalen Jahr der Quantenwissenschaft und Quantentechnologie ausgerufen. Deren Perspektiven sollen unter dem Motto „Quantum2025 – 100 Jahre sind erst der Anfang …“ einer breiten Öffentlichkeit sichtbar gemacht werden.

Der Dual-Use-Charakter der Technologie beinhaltet die prinzipielle Verwendbarkeit der Technologie für positive wie negative Zwecke. Einerseits ist eine mögliche Erweiterung von Anwendungsfällen und Geschäftsfeldern denkbar und andererseits ist eine erhöhte Vulnerabilität von IKT-Systemen zu erwarten, was erheblichen Anpassungsbedarf bei der IT-Sicherheit auch in der Versicherungswirtschaft zur Folge haben wird.

---

1 Zu den weiteren Feldern der Quantentechnologie neben dem Quantencomputing gehören die Quantensensorik und die Quantenkommunikation, auf die hier aufgrund der Unterschiedlichkeit und technischen Komplexität nicht näher eingegangen werden kann.

2 Bundesministerium für Bildung und Forschung, Handlungskonzept Quantentechnologien 2023, https://www.quantentechnologien.de/fileadmin/public/Redaktion/Dokumente/PDF/Publikationen/Handlungskonzept-Quantentechnologien-2023_bf_C1.pdf, letzter Zugriff 28.01.2025

3 IBM, 2024, https://de.newsroom.ibm.com/quantum-datacenter, letzter Zugriff 28.01.2025

© GDV 2025

Quantencomputing als Enabler in der Versicherungswirtschaft

Mit der Nutzung einsatzfähiger Quantencomputer lassen sich sehr komplexe Modelle aufbauen, die in der Lage sind, sehr präzise die Prozesse in Natur, Technik und Wirtschaft zu analysieren. Optimierungen und Simulationen können gegenüber klassischen Systemen exponentiell schneller durchgeführt werden. Versicherungsunternehmen profitieren davon in unterschiedlichen Geschäftsfeldern.

Als potenzielle Supercomputer können Quantencomputer dazu beitragen, die erwartungsgemäß zunehmend komplexer werdenden KI-Modelle in bereits bestehenden Anwendungsfeldern zu optimieren und das maschinelle Lernen zu fördern, das sogenannte „quantum machine learning“. In den aktuellen Modellen können bereits heute Teilprozesse durch Quantencomputer deutlich beschleunigt werden. Für die volle Ausnutzung des Potentials müssen jedoch neue, speziell auf Quantencomputer ausgerichtete, Algorithmen entwickelt werden.

Definition Quantencomputer

Ein Quantencomputer basiert auf einem Prozessor, der die Gesetze der Quantenmechanik nutzt, um komplexe Berechnungen auszuführen. Im Unterschied zu klassischen Computern arbeitet er nicht auf Basis elektronischer Schaltkreise mit klar definierten elektrischen Zuständen. Quantencomputer nutzen vielmehr die Wechselwirkung quantenmechanischer Zustände, die mittels Wahrscheinlichkeiten beschrieben werden. Theoretische Studien und erste praktische Implementierungen zeigen, dass bestimmte Fragestellungen mittels speziell für Quantencomputer ausgelegter Algorithmen schneller gelöst werden können. Darüber hinaus werden bislang nicht effizient durchführbare oder klassisch unmögliche (exakte) Simulationen von komplexen Vorgängen in der Natur oder künstlich geschaffenen Systemen ermöglicht.

Darüber hinaus ist zu erwarten, dass mithilfe von Quantencomputern versicherungsrelevante Use Cases umgesetzt werden können, die bislang aufgrund mangelnder Rechnerleistung noch nicht angegangen werden konnten bzw. heute noch nicht denkbar sind. Eine indirekte Betroffenheit von Versicherern ist auch in Folge bahnbrechender Innovationen möglich, die aufgrund des erfolgreichen Einsatzes von Quantencomputern in

Potentiale des Quantencomputings für die Versicherungswirtschaft

Abbildung 1 · Mögliche Anwendungsbereiche in der Versicherungswirtschaft

	**Analyse von Klimaveränderungen in der Rückversicherung**
	**Naturgefahrenabschätzungen, z. B. für Hochwasser in der Elementarschadenversicherung**
	**Analyse der Auswirkungen von Katastrophen auf Morbidität und Mortalität (z. B. Pandemien)**
	**Risikobewertungen in der Kreditversicherung**
	**Finanzmodellierungen zur Portfoliooptimierung (Monte-Carlo-Simulation) und Einschätzung von Marktrisiken**
	**Bewertung von Produktionsprozessen und Lieferketten in der Industrieversicherung (Risk-Engineering)**

Quelle: GDV

© GDV 2025

anderen Branchen ermöglicht werden. In der Medizin- und Medikamentenforschung könnten fundamentale Anwendungen zur Marktreife gelangen, die großen Einfluss auf die menschliche Gesundheit und Lebenserwartung haben, mithin auf die Kalkulation und Produktgestaltung in der Kranken- und Lebensversicherung.

Grundsätzlich stellt sich die Frage, wann klassische Rechner an ihre Grenzen kommen und Quantencomputer einen deutlichen Zusatznutzen stiften oder bedeutende Innovationen herbeiführen können. Derzeit wird eine Vielzahl von Anwendungsfällen erforscht bzw. als Proof of Concepts demonstriert.

Quantencomputer – Risiken und Schutzmaßnahmen

Mit der rasanten Entwicklungsgeschwindigkeit der Quantencomputertechnologie rücken auch die Gefahren infolge einer kriminellen Nutzung näher. So sind Quantencomputer durch ihre immense Rechenleistung in der Lage, bestehende Verschlüsselungstechnologien – z.B. traditionelle Verfahren wie RSA und ECC – zu brechen. Angriffe auf bislang sichere Kommunikationsleitungen und Systeme werden dadurch deutlich erleichtert.

Die meisten Versicherer haben sich mit dem Thema Quantencomputing und deren Gefahren bereits in Teilbereichen befasst. Aktuelle Verbandszahlen zur Priorisierung verschiedener Digitalisierungsprojekte zeigen jedoch, dass die Technologie – bedingt durch ihre Neuartigkeit und den Reifegrad – für zwei Drittel der teilnehmenden Unternehmen noch keine bzw. eine nur geringe Relevanz genießt.[4]

Allerdings dürfte eine baldige industrieweite Umstellung auf quantensichere Verfahren im Interesse der Branche sein, um weiterhin die Versicherbarkeit bestimmter Risken zu gewährleisten. Andernfalls könnten beispielsweise in krimineller Absicht durch eine nicht quantensichere Verschlüsselung erlangte Steuerungsdaten zukünftig Diebstähle von Fahrzeugen vereinfachen und das Herbeiführen schwerer Unfälle fördern.

Allerdings sind alle Unternehmen diesen Bedrohungen bereits heute ausgesetzt. Durch „Store now, decrypt later"-Angriffe können heute erbeutete, nicht quantensicher verschlüsselte Daten in Zukunft mit leistungsfähigen Quantencomputern entschlüsselt werden. Dieses Risiko besteht grundsätzlich für alle Branchen.

Zeitlicher Horizont der neuen Bedrohungslage

Über den Zeitpunkt, ab dem Quantencomputer voll einsatzfähig sein werden, sind sich die Experten uneinig. Die Mehrheit geht jedoch davon aus, dass in 15 Jahren die Wahrscheinlichkeit der Verfügbarkeit einsatzfähiger Systeme bei über 50% liegt. Demnach ist davon auszugehen, dass die in zahlreichen Anwendungen eingesetzte Public-Key-Kryptografie in den 2030er-Jahren durch Quantencomputer gebrochen werden kann.

Die Sicherheitsbehörden in der europäischen Union sind deutlich vorsichtiger. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat Ende 2024 gemeinsam mit Partnern aus 17 EU-Mitgliedsstaaten die Industrie, die Betreiber kritischer Infrastrukturen und die öffentliche Verwaltung dazu aufgerufen, zur Post-Quanten-Kryptografie (PQC) überzugehen. Anwendungen mit besonders sensiblen Daten seien dabei so schnell wie möglich, spätestens jedoch bis Ende 2030 zu schützen.[5]

Ein wesentliches, noch ungelöstes Problem beim Quantencomputing ist die physikalisch bedingte inhärente Fehleranfälligkeit. Diesem begegnet man in der Forschung mit der Entwicklung effektiver Fehlerkorrektur- und -mitigationsmechanismen. Eine weitere wesentliche Herausforderung ist die Skalierbarkeit, die für komplexe Berechnungen notwendig ist. Die aktuellen Systeme weisen auch hierfür eine noch zu geringe Leistungsfähigkeit auf. Die Entwicklungs-Roadmap eines auf dem Gebiet der Quantencomputertechnologie führenden IT-Unternehmens deutet allerdings darauf hin, dass die genannten Barrieren bereits 2029 abgebaut sein könnten.[7]

[4] s. GDV (2024): Digitalisierung…aber sicher: Resilienz und IT-Transformation in unsicheren Zeiten, https://www.gdv.de/gdv/themen/digitalisierung.

[5] https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2024/241127_PQC-Joint-Statement.html, letzter Zugriff 27.01.2025

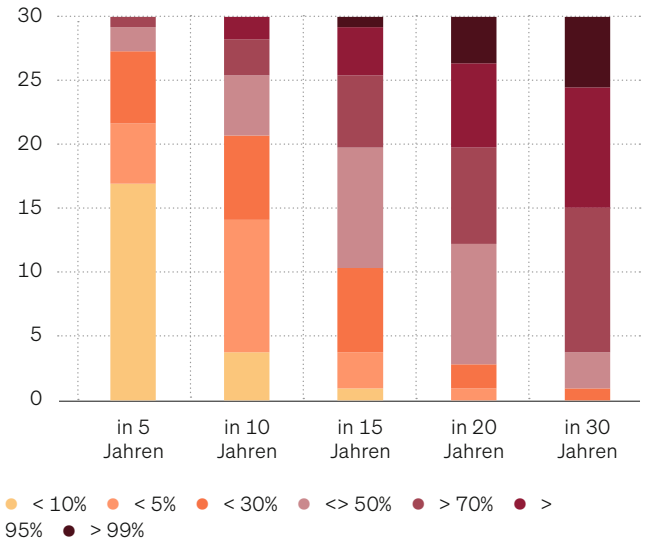
[6] Die Quantum Key Distribution (QKD) ist eine weitere Methode zur quantensicheren Verschlüsselung, auf die aufgrund noch vieler Limitierungen in diesem Beitrag jedoch nicht explizit eingegangen wird.

[7] https://www.ibm.com/quantum/blog/ibm-quan-

© GDV 2025

Schätzung der Wahrscheinlichkeit, mit der Quantencomputer den Code RSA-2024 innerhalb von 24 Stunden brechen könnten

Abbildung 2 · Anzahl der Expertenschätzungen je Jahreshorizont in der Zukunft ab 2024



Quelle: Mosca/Piani (2024): Quantum threat timeline report 2024, Global Risk Institut, S. 21

Mitigierung von Quanten-Risiken

Unternehmen stehen zukünftig vor der Herausforderung, ihre Systeme quantenresistent aufzustellen und Maßnahmen zu ergreifen, die zur Realisierung einer vollumfänglichen „Post-Quanten-Kryptografie" führen.

In den USA hat das National Institute of Standards and Technology (NIST) eine Ausschreibung zur Standardisierung von quantenresistenten Algorithmen im Jahr 2016 begonnen. In einem mehrstufigen Verfahren wurden unter Beteiligung von Forschern, Institutionen und der IT-Community nach umfangreichen Prüfungen 2024 drei Standards bekanntgeben, die für PQC sofort einsatzbereit sind.[8] Sicherheitsbehörden weltweit nehmen in ihren Empfehlungen Bezug auf die Ergebnisse der NIST.

Auch das BSI hat technische Richtlinien herausgeben, die Empfehlungen für kryptografische Algorithmen und Schlüssellängen enthält.[9]

Definition PQC

Die Post-Quanten-Kryptografie (hier englisch abgekürzt: PQC) befasst sich mit der Entwicklung und Standardisierung sicherer Verschlüsselungsverfahren, die unter Einsatz von Quantencomputern und wirtschaftlich begrenzter Ressourcen nach aktuellem Stand nicht zu brechen sind. PQC-Verfahren benötigen keine Quantenkryptografie auf Basis entsprechender physikalischer Prinzipien und können auf einem vergleichbaren Sicherheitsniveau in bestehenden klassischen Systemumgebungen implementiert werden.[6]

Einige Experten sowie das BSI empfehlen den Einsatz hybrider Lösungen, d.h. eine Kombination von klassischen und quantenresistenten Verfahren[10]. Dieser Ansatz hat zwar seine eigenen Herausforderungen, er gewährleistet jedoch Schutz, solange die jeweiligen klassischen und kryptografischen Post-Quantum-Verfahren nicht gleichzeitig gebrochen werden.

Operations

Die Einführung der PQC erfordert neben dem kryptografischen Basiswissen auch geeignete administrative Regelungen und Vorgehenskonzepte. Experten verschiedener Institutionen haben zu diesen Aspekten bereits Veröffentlichungen in Form von Leitfäden und Handbüchern publiziert.[11]

Als erster Schritt wird in den vielzähligen Empfehlungen zum Vorgehen dazu geraten, eine kryptografische Landkarte zu erstellen. Diese sollte neben den internen Systemen auch diejenigen der externen Kommunikationspartner einschließen, inkl. der staatlichen Institutionen, mit denen ein Datenaustausch besteht. Um effektiv zu sein, müssen sich Maßnahme zu PQC auf die gesamte Prozesskette der Datenkommunikation und -speicherung beziehen, um das Ziel eines harmonisierten PQC-Ökosystems zu erreichen. Dies erfordert ein konzertiertes und koordiniertes Vorgehen, national und überregional.

tum-roadmap-2025, letzter Zugriff 28.01.2025

[8] https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards

[9] s. BSI TR-02102 (2023), https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr02102/tr02102_node.html

[10] BSI, Migration zu Post-Quanten-Kryptografie, August 2020, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Post-Quanten-Kryptografie.pdf?__blob=-publicationFile&v=1, letzter Zugriff 28.01.2025

[11] Neben den Handlungsempfehlungen des BSI sehr aktuell und umfassend: AIVD, CWI, TNO (2024) – The PQC Migration Handbook, s. https://www.tno.nl/en/newsroom/2024/12/renewed-handbook-quantum-safe-crypto/, letzter Zugriff 14.01.2025

© GDV 2025

Eine grundlegende Anforderung an Organisationen ist die sogenannte Krypto-Agilität. Sie bringt zum Ausdruck, dass der stetige Wettlauf zwischen neuen Angriffsrisiken und Schutzmaßnahmen stets mitbedacht werden sollte, um genutzte kryptografische Verfahren bei Bedarf flexibel austauschen oder anpassen zu können. Weniger relevant wird diese Eigenschaft, wenn Unternehmen überwiegend oder ausschließlich Systeme externer Hersteller bzw. Cloud-Infrastrukturen nutzen. In diesen Fällen sollte jedoch ein strategisch passender PQC-Fahrplan bekannt sein bzw. eingefordert werden.

Governance

Gesetzliche Vorgaben könnten für die Herstellung eines umfänglichen Postquanten-Ökosystems die Planbarkeit und Verbindlichkeit unter Umständen deutlich verbessern. Weltweit existiert bislang noch keine allgemeine, verpflichtende Einführung von Post-Quanten-Kryptografie (PQC). Allerdings sind Entwicklungen und Initiativen sichtbar, die auf mögliche Vorgaben hinweisen.

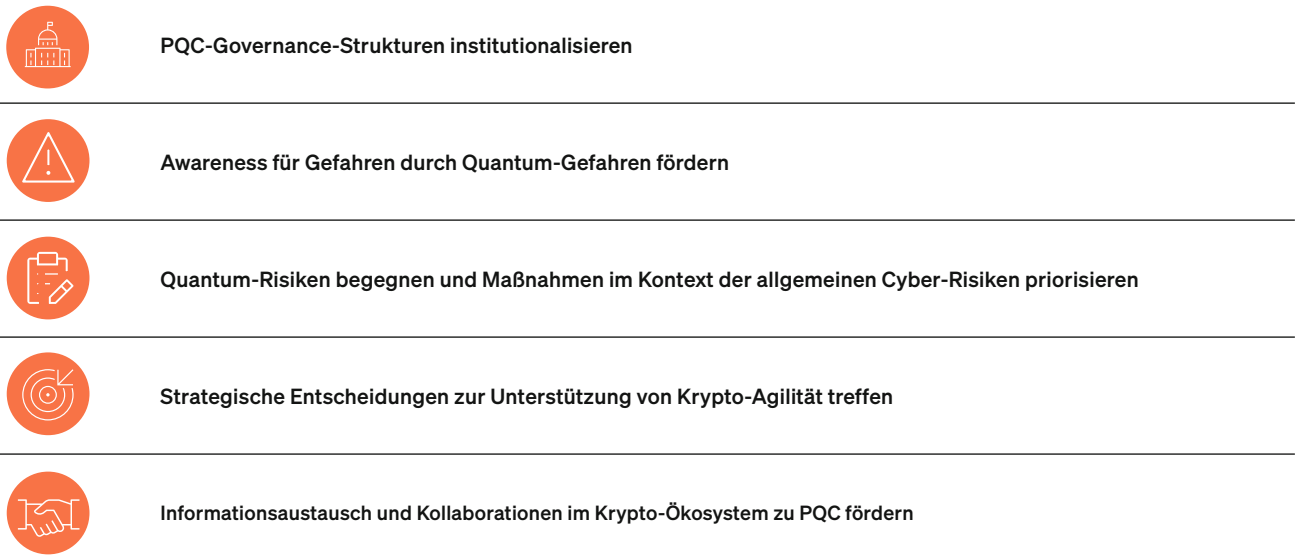
So wurde 2022 in den USA der Quantum Computing Cybersecurity Preparedness Act erlassen. Diese zielt darauf ab, die nationale US-Sicherheit im Hinblick auf zukünftige Bedrohungen durch Quantencomputertechnologien zu stärken. Neben der Forderung einer notwendigen Zusammenarbeit von Regierung, Wissenschaft und Industrie sowie einer umfassenden Untersuchung der Auswirkungen von Quantencomputertechnologien, werden alle Bundesunternehmen verpflichtet, eine Strategie zur Migration von bestehenden Verschlüsselungssystemen auf quantensichere Verfahren vorzulegen.

Auf der Ebene der EU wird noch recht allgemein im Digital Operational Resilience Act (DORA) auf die Bedrohungen durch Quantencomputer verwiesen. In den technischen Standards (RTS) zum IKT-Risikomanagement heißt es in der Gesetzesbegründung mit Blick auf die rasche technologische Entwicklung, dass „...Finanzunternehmen über Entwicklungen in der Kryptoanalyse auf dem Laufenden bleiben und führende Praktiken und Normen berücksichtigen...“ sollen. Die Finanzunternehmen werden aufgefordert „...einen flexiblen Ansatz zu verfolgen, der auf Risikominderung und -überwachung beruht, sodass sie vor dem Hintergrund der Dynamik kryptografischer Bedrohungen in der Lage sind, solche Bedrohungen, einschließlich Bedrohungen aufgrund der Fortschritte im Bereich der Quantentechnologie, zu bewältigen.“

Für die Praxis leitet sich daraus ab, dass mit dem Inkrafttreten der DORA-Verordnung Maßnahmen zur Erlangung von Kryptoagilität vorzubereiten und die Entwicklungsfortschritte auf dem Gebiet der Quantencomputertechnologie regelmäßig zu beobachten sind.

Umsetzung der Postquanten-Kryptografie

Abbildung 3 · Beispiel für PQC-Guidelines



Quelle: Centre for European Policy Studies (CEPS)(2023): Quantum Technologies and Cybersecurity Technology, Governance and Policy Challenges, S. 39

© GDV 2025

Ausblick

Die weitere Entwicklung sowohl hinsichtlich der Gefahren und Einsatzmöglichkeiten muss weiterhin eng in den Blick genommen werden. Mindestens für Neuentwicklungen und Anschaffungen von IT-Systemen sollten bereits heute das Merkmal quantensicherer Verschlüsselungen eine mitentscheidende Rolle spielen. Spannend wird es in den nächsten ein bis zwei Jahren im regulatorischen Umfeld. Ob die Informationen der EU-Kommission und des BSI zur Postquanten-Kryptografie weiterhin lediglich Empfehlungscharakter haben werden, bleibt abzuwarten. Zunehmend werden auch Stimmen laut, die auf die Dringlichkeit der Umstellung hinweisen und kurzfristig den Beginn erster Maßnahmen einfordern.[12]

Nach Auffassung der IT-Verantwortlichen in der Versicherungswirtschaft sind über die derzeitigen Regelungen des DORA hinaus keine zusätzlichen Vorgaben für den Übergang zur Post-Quanten-Kryptografie erforderlich. Die Branche ist bestens informiert und beginnt bereits, die Gefahren für die Sicherheit der jeweils eingesetzten kryptografischen Verfahren zu analysieren und adäquate Maßnahmen im Sinne der Empfehlungen des BSI in Gang zu setzen und bis 2030 abzuschließen. Auch wird bereits darauf geachtet, dass von IT-Dienstleistern genutzte Systeme entsprechende Planungen aufweisen.

Hinsichtlich der Nutzung von Quantencomputern ist aufgrund der komplexen und sehr speziellen Technologie die interdisziplinäre Zusammenarbeit von Experten und Praktikern von elementarer Bedeutung. Dies gilt insbesondere für die kleinen und mittelgroßen Versicherer, für die das Vorhalten von entsprechenden Ressourcen und Expertise nicht wirtschaftlich ist. Dabei könnte eine staatliche Anschubförderung von gemeinsamen Brancheninitiativen in Betracht gezogen werden, um den Zugang zur technischen Infrastruktur von quantenbasierten Computersystemen zu erleichtern.

Die Versicherer befürworten daher die intensive Förderung der Quantencomputertechnologie in Deutschland und in Europa auf allen technologischen Ebenen. Die Entwicklungen und Ergebnisse aus Wissenschaft, Forschung und der Industrie sollen für europäische Unternehmen transparent und regelmäßig zur Verfügung gestellt werden. Dies gilt insbesondere für die Maßnahmen des von der Bundesregierung im Jahr 2023 veröffentlichten Handlungskonzepts zu Quantentechnologien. Die noch in diesem Jahr geplante Entwicklung einer europäischen Quantum-Strategie wird begrüßt und sollte sich auch auf die Potentiale der Quantencomputertechnologie in der Finanzwirtschaft fokussieren.

[12] s. die Rede von Julia Wiens, Exekutivdirektorin der BaFin, zu Pkt. III. vom 06.03.2025 unter https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/RedenInterviews/re_250204_Rede_EDinVA_Neujahrsempfang_Assekuranzclub_Rhein-Main.html, abgerufen am 21.03.2025

GDV

Gesamtverband der Deutschen Versicherungswirtschaft e. V.
Wilhelmstraße 43 / 43 G, 10117 Berlin
Postfach 08 02 64, 10002 Berlin
Tel.: +49 30 2020–5000, Fax: +49 30 2020–6000
www.gdv.de, berlin@gdv.de

© GDV 2025