

Quantencomputing: Die unterschätzte Gefahr für den Finanzsektor

Von Jens Bläser und Armin Reinhardt

Das Thema „Quantencomputing“ gewinnt mehr und mehr an Bedeutung. Doch neben zahlreichen Chancen und neuen Möglichkeiten, welche die Technologie eröffnet, stellt sie auch eine wesentliche Bedrohung für alle Unternehmen und Sektoren dar – insbesondere im Kontext der Cybersicherheit. Dass der Handlungsdruck bereits heute gesehen wird, zeigt eine Marktumfrage: Mehr als 95 Prozent der Befragten bewerten die Bedeutung von Quantencomputing für die Sicherheit kryptografischer Verfahren als „hoch“ oder „sehr hoch“.¹

Der Finanzsektor im Fokus

Der Finanzsektor ist von der Bedrohung durch Quantencomputer besonders betroffen. Banken und Versicherungen verarbeiten große Mengen sensibler Daten – von Zahlungs- und Kontodaten bis hin zu Informationen zur Bonitätsbewertung oder Gesundheitsdaten. Viele Sicherheitsmechanismen zum Schutz dieser Daten basieren auf kryptografischen Verfahren, deren Schutzwirkung durch leistungsfähige Quantencomputer künftig gefährdet sein wird.

Zudem findet derzeit in der Praxis vermehrt eine Vernetzung verschiedener Finanzökosysteme statt. Dazu gehören etwa Anwendungen, die Konten mehrerer Banken bündeln oder die Verknüpfung von Bank- und Versicherungsleistungen. Dadurch werden sensible Daten aus verschiedenen Quellen an einer Stelle gebündelt und stellen somit ein attraktives Angriffsziel dar. Zugleich muss jeder beteiligte Akteur kryptografische Maßnahmen einrichten und deren Schutzwirkung sicherstellen.

Hinzu kommt: Finanzinstitute sind aufgrund des hohen Werts ihrer Daten bereits heute ein attraktives Angriffsziel für Cyberkriminelle. Das bestätigt die Agentur der Europäischen Union für Cybersicherheit (ENISA) in ihrem Bericht zur Lage der Bedrohungslandschaft innerhalb der EU. Rund 4,5 Prozent aller Informationssicherheitsvorfälle in der EU entfallen auf den Finanzsektor. Damit ist er, ohne die nicht zugeordneten Vorfälle, der viertmeist betroffene Sektor.²

Der Faktor Zeit: „Harvest Now, Decrypt Later“

Die Möglichkeit der Entschlüsselung bestehender Verfahren ist bereits mathematisch bewiesen. Offen ist nur noch der Zeitpunkt: Der Tag, an dem ein Quantencomputer die dafür erforderliche Leistungsfähigkeit erreicht, wird Q-Day genannt. Expertenschätzungen, wann dieser Q-Day eintritt, unterliegen jedoch einer großen Spannweite (siehe auch Abbildung 1).

Dennoch ist die Post-Quanten-Kryptografie (PQC) bereits heute – völlig unabhängig vom

Was erwartet Sie in diesem Special?

Die Bedrohung durch Quantencomputer beginnt nicht erst, wenn der erste leistungsfähige Quantencomputer verfügbar ist. Schon heute müssen Unternehmen wissen, welche Daten und Systeme gefährdet sind und wie sie ihre Kryptografie zukunftssicher machen. Denn Daten, die heute sicher erscheinen, müssen aufgrund von „Harvest Now, Decrypt Later“ schon jetzt geschützt werden.

Lesen Sie:

- › wo die größten Risiken liegen und welche kryptografischen Verfahren besonders gefährdet sind,
- › was Unternehmen jetzt tun können: von der Bestandsaufnahme über die Priorisierung kritischer Systeme bis zur Migration auf Post-Quanten-Kryptografie (PQC),
- › was das für die Unternehmenssteuerung bedeutet: von DORA und Risikomanagement bis zu Notfallvorsorge und Resilienz.

Dieses Special liefert Impulse für die Umsetzung und konkrete Entscheidungs- und Handlungsempfehlungen für die Unternehmenspraxis.

Jens Bläser und Armin Reinhardt

Quantencomputing: Die unterschätzte Gefahr für den Finanzsektor Seiten 1-2

Udo Würtz

Quantencomputer verstehen: Warum klassische Kryptografie unter Druck gerät Seite 3

Prof. Dr. Dennis-Kenji Kipker

Die Antwort auf das Quantenrisiko: PQC wird zur Pflicht. Seiten 4 - 5

Andreas Breunig

Von der Risikoanalyse zur Umsetzung: Eine Roadmap zur Quantensicherheit. Seiten 6 - 7

Michael Ehrnsperger

Quantenresilienz als Führungsaufgabe: Wie Vorstände heute die Weichen stellen Seite 8

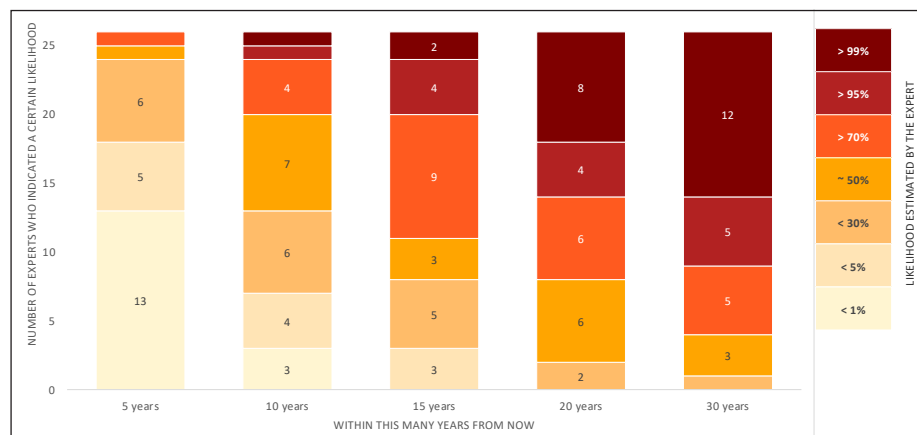


Abbildung 1: Expertenschätzungen zur Wahrscheinlichkeit eines kryptografisch relevanten Quantencomputers nach Zeithorizont. Quelle: Mosca, Michele; Piani, Marco: Quantum Threat Timeline Report, Global Risk Institute, 2024

Impressum

Verlag: Reif Verlag GmbH · Alfred-Jost-Straße 11 · 69124 Heidelberg
Peter Reif · peter.reif@reifverlag.de · www.manager-wissen.com

Redaktion: Christian Deutsch · info@deutsch-werkstatt.de
Regina Gödde, E-Mail: regina.goedde@reifverlag.de
Layout: metropolmedia, 69245 Bammental · Druck: ColorDruck Solutions, 69181 Leimen

Q-Day – hochrelevant. Der Grund ist das sogenannte „Harvest Now, Decrypt Later“-Prinzip (HNDL): Angreifer fangen verschlüsselte Daten schon jetzt ab, um sie später zu entschlüsseln.

Deshalb müssen Informationen mit langfristigem Schutzbedarf schon jetzt durch quantensichere Verfahren abgesichert werden. In der Finanz- und Versicherungswirtschaft betrifft dies eine Vielzahl von Prozessen. So sind beispielsweise Gesundheitsdaten im Rahmen einer Krankenversicherung oft über Jahrzehnte hinweg hochgradig schützenswert. Kryptografische Verfahren sind hier essenziell, um diese sensiblen Daten vor Cyberangriffen, unbefugter Einsicht und Manipulation zu schützen.

Das Thema Kryptografie muss neu gedacht werden

Dabei existieren verschiedene Ansätze. Kryptografische Verfahren dienen dazu, Daten während der Speicherung, Übertragung und auch bei der Verwendung zu verschlüsseln. Dadurch wird sichergestellt, dass ausschließlich berechtigte Personen Zugriff auf die Informationen haben. Zudem können digitale Signaturen bei der Übertragung eingesetzt werden, um die Authentizität des Senders oder Empfängers zu bestätigen. Zusätzlich besteht die Möglichkeit, Hash-Funktionen einzusetzen, um Inhalte in einen einzigartigen Hashwert umzuwandeln. Wird der Inhalt verändert, entspricht er nicht mehr dem einzigartigen Hashwert, wodurch Manipulationen festgestellt werden können.

Viele der derzeit verwendeten Algorithmen zur Sicherstellung kryptografischer Methoden, die meist auf bisher ungelösten mathematischen Problemen beruhen, können durch Quantencomputer aufgelöst werden, wodurch sie unwirksam werden. Die Wissenschaft und verschiedene nationale Behörden (z. B. das Bundesamt für Sicherheit in der Informationstechnik (BSI) oder das National Institute of Standards and Technology (NIST)) haben bereits verschiedene Verfahren und Ansätze für kryptografische Algorithmen gezeigt, die auch Angriffen durch Quantencomputer standhalten können. Eine technische Konkretisierung, warum Quantencomputer einen so starken Einfluss auf die Kryptografie haben, wird u. a. in den tiefergehenden Folgebeiträge erörtert.

Regulatorischer Druck durch DORA und NIS-2

Die Konsequenz ist: Finanzinstitute müssen alle Systeme, die langfristig schützenswerte Daten speichern, verarbeiten oder übertragen, zeitnah auf quantensichere kryptografische Verfahren umstellen.

So können regulatorische Verstöße vermieden werden. Finanzinstitute sind insbesondere durch den Digital Operational Resilience Act (DORA), ein EU-weites Gesetz, an alle Arten von Finanzinstituten mit Vorgaben zur Informationssicherheit, dem Business Continuity Management und dem Management von Drittdienstleistern, zu einer Risikobewertung und dem Stand der Technik angemessen kryptografischen Verfahren verpflichtet. Verstöße z. B. gegen die Datenschutzgrundver-

ordnung oder NIS-2 können auch weitere Sektoren betreffen. Zusätzlich können Vorfälle zu einem Vertrauensverlust der Kundinnen und Kunden führen, was insbesondere für Finanzinstitute von großer Bedeutung ist. Es ist also wichtig, die Entwicklung zu verfolgen und zeitnah mit der Migration quantensicherer kryptografischer Verfahren zu beginnen. Insgesamt können durch einen frühen Start sensible Daten geschützt, Reputations-, Informations- und Kommunikationsrisiken (IKT-Risiken) verringert sowie Kosten gesenkt werden.

Um einen effizienten Start zu ermöglichen, sollten die Identifikation der betroffenen Systeme, die Priorisierung der Systeme, die zuerst auf PQC-Algorithmen migriert werden sollen, sowie auch eine Zeitleiste für die Umsetzung im Vordergrund stehen. Für die Identifikation aller betroffenen Systeme ist ein Informationsverbund als Mittelpunkt der Governance essenziell. Hier wird die Verknüpfung zwischen den verwendeten Informationen und Prozessen, Anwendungen, Technologiekomponenten und Räumlichkeiten (im Folgenden IKT-Komponenten) hergestellt, die diese Informationen verarbeiten. Danach wird für die Informationen der Schutzbedarf für die Schutzziele (Verfügbarkeit, Vertraulichkeit, Integrität und Authentizität) und die Prozesse die Geschäftskritikalität bestimmt, welche auf die unterstützenden IKT-Komponenten vererbt werden. Einen Teil dieses Informationsverbunds stellen auch IDV-Anwendungen oder sogenannte Schatten-IT dar. IDVen sind individuelle Datenverarbeitungsverfahren außerhalb der IT, die mit Mitteln der bereitgestellten Office-IT-Landschaft umgesetzt werden, beispielsweise Programmierungen in Tabellenkalkulationen. Zur Priorisierung können die Art der verarbeiteten Daten sowie die Dauer einer Migration herangezogen werden.

Ebenso unerlässlich ist es, die Leitungsebene einzubinden und das Thema fest in der Unternehmensstrategie zu verankern. Dies sollte mit einer angemessenen Ressourcenzuweisung sowie regelmäßigen Berichten zum Umsetzungsstand einhergehen. So macht das Management die hohe Priorität und Relevanz des Themas deutlich.

Unternehmen – insbesondere in der Finanzwirtschaft – müssen das Thema Quantensicherheit ab sofort als strategische Managementaufgabe begreifen und jetzt handeln, da sensible Daten durch das „Harvest Now, Decrypt Later“-Prinzip bereits heute akut gefährdet sind.

Fazit

Die Bedrohung durch Quantencomputer ist real. Unternehmen müssen sich bereits heute darauf vorbereiten, die etablierten kryptografischen Verfahren anzupassen. Denn mit „Harvest Now, Decrypt Later“ können langfristig schützenswerte Daten schon heute zum Ziel werden. Für Finanzinstitute und vernetzte Finanzökosysteme, die besonders attraktive Ziele für Cyberangriffe sind, bedeutet das: Kritische Systeme und Daten müssen frühzeitig identifiziert und priorisiert werden, um die Migration auf quantensichere Algorithmen rechtzeitig einzuleiten.

Diese Aufgabe ist nicht allein eine technische Fragestellung. Für eine erfolgreiche Umsetzung müssen technische und organisatorische Anforderungen zusammengeführt und verschiedene Stakeholder eingebunden werden – von CISO und CIO bis zu CRO und CPO. Die folgenden Beiträge vertiefen diese Perspektiven: Sie erklären die technischen Grundlagen, zeigen die Herausforderungen der Einführung von Post-Quanten-Kryptografie (PQC) und ordnen das Thema aus Managementsicht ein. Der abschließende Beitrag richtet den Blick auf Resilienz und Notfallmanagement und zeigt, warum Quantenresilienz zunehmend zu einer strategischen Managementaufgabe wird.

Quellenangaben:

¹ Vgl. Fischer, Hans-Peter, Hagemeyer, Heike et al, Marktumfrage Kryptografie und Quantencomputing, S. 7, Marktumfrage Kryptografie und Quantencomputing, zuletzt abgerufen am 05.08.2026 um 15:18

² ENISA Threat Landscape 2025

Die Autoren



Jens Bläser ist Partner bei Deloitte und einer der profiliertesten Experten für Cybersecurity und digitale Resilienz im Finanzsektor. Seit mehr als 15 Jahren begleitet er Banken und Versicherer bei der Absicherung kritischer Infrastrukturen, der Modernisierung komplexer IT-Landschaften und der Umsetzung regulatorischer Anforderungen wie DORA oder MaRisk. Sein Schwerpunkt liegt auf der Frage, wie Finanzinstitute ihre Sicherheitsarchitektur strategisch weiterentwickeln, um den Herausforderungen des Quantenzeitalters zu begegnen – von quantensicherer Kryptografie über Payment-Security bis zur Resilienz globaler Ökosysteme. Er arbeitet an der Schnittstelle von Technologie, Risiko und Regulierung und ist regelmäßiger Sprecher zu Themen wie Post-Quantum-Security, Cyber-Resilienz und der Zukunft der Finanz-IT.



Armin Reinhardt ist Senior Manager bei Deloitte und Experte für Resilienz und Informationssicherheit insbesondere im Kontext KI und Quantencomputing. Seit über 8 Jahren begleitet er Banken und Versicherer beim Aufbau von Managementsystemen sowie der Etablierung von Governance-Strukturen zur Umsetzung von regulatorischen Anforderungen wie DORA oder dem AI Act. Sein Fokus liegt auf der Herausforderung, die Sicherheits- und Kontrollstrukturen von Finanzinstituten so auszugestalten, dass neuartige Technologien und daraus entspringende Risiken und Bedrohungen berücksichtigt und angemessen behandelt werden können.

Quantencomputer verstehen: Warum klassische Kryptografie unter Druck gerät

Von Udo Würtz

Quantencomputer sind keine schnelleren klassischen Computer. Durch eine veränderte Rechenlogik hebeln sie die mathematischen Fundamente heutiger Verschlüsselungsverfahren systematisch aus. Für Unternehmen bedeutet das: Die Bedrohung ist kein Zukunftsszenario, sondern verlangt eine sofortige Risikoanalyse und die langfristige Transformation hin zu einer quantensicheren Infrastruktur.

Von Bits zu Qubits

Klassische Computer verarbeiten Bits als 0 oder 1. Quantencomputer arbeiten mit Qubits, die sich in einer quantenmechanischen Überlagerung befinden können. Erst die Messung erzeugt ein klassisches Ergebnis: Superposition.¹

Bei der Verschränkung bilden mehrere Qubits einen gemeinsamen Zustandsraum, der mit ihrer Zahl stark wächst. Quantencomputer probieren dabei nicht einfach „alle Lösungen gleichzeitig“ aus. Algorithmen verändern vielmehr Wahrscheinlichkeitsamplituden gezielt: Unerwünschte Rechenpfade werden abgeschwächt, relevante Ergebnisse verstärkt. Aus der Messverteilung ergibt sich das wahrscheinlichste Ergebnis.¹

Diese Unterscheidung erklärt, warum Quantencomputer heutige IT-Aufgaben nicht pauschal ersetzen, bei bestimmten mathematischen Problemklassen aber zur Bedrohung werden. Moderne Verschlüsselung beruht darauf, dass Aufgaben wie Faktorisierung oder diskrete Logarithmen mit klassischen Computern praktisch nicht lösbar sind. Ihre Sicherheit liegt im enormen Zeitaufwand.^{1,2}

Warum Quantencomputer klassische Kryptografie bedrohen

Shors Algorithmus kann große Zahlen effizient faktorisieren und diskrete Logarithmen lösen – die Grundlage vieler Public-Key-Verfahren wie RSA, Diffie-Hellman und elliptischer Kurven. Noch fehlt ein hinreichend großer, fehlertoleranter Quantencomputer. Wird eine solche Maschine verfügbar, kippt jedoch die Sicherheitsannahme: Nicht mehr Rechenleistung, sondern ein anderer Algorithmus für eine andere Computerart wird entscheidend.^{2,3}

Grovers Algorithmus wirkt anders. Er kann unstrukturierte Suchprobleme quadratisch beschleunigen. Für symmetrische Verschlüsselung und Hashfunktionen bedeutet das meist keine Entwertung, wohl aber eine Verringerung des Sicherheitsniveaus, der sich häufig durch größere Schlüssel begegnen lässt. Die größere Verwundbarkeit liegt bei asymmetrischen Verfahren, weil Shors Algorithmus deren mathematische Basis direkt angreift. Für Finanzinstitute ist diese Differenzierung zentral.^{3,4}

Wo steht die Technologie heute?

Leistungsfähige Quantencomputer bleiben eine anspruchsvolle ingenieurwissenschaftliche Aufgabe. Qubits reagieren empfindlich auf Störungen;

Quantenzustände müssen lange genug kohärent bleiben; Fehler müssen korrigiert werden. Deshalb sagt die reine Zahl physischer Qubits wenig über die tatsächliche Leistungsfähigkeit aus. Entscheidend sind Fehlerraten, Kohärenzzeiten, Konnektivität, Steuerbarkeit und robuste logische Qubits.¹

Das Rennen um die Hardwarearchitektur ist offen. Erprobt werden supraleitende Qubits, Ionenfallen, neutrale Atome, photonische Systeme und Spin-Qubits. Keine Plattform hat sich durchgesetzt; jede verbindet Vorteile mit technischen Hürden. Aus Managementsicht zählt vor allem, wie schnell Hardware, Fehlerkorrektur, Algorithmen und Systemintegration zusammenfinden.⁵

Die Forschung zeigt, dass sich Hardwareentwicklung und Ressourcenabschätzungen dynamisch annähern. Eine 2026 veröffentlichte Arbeit argumentiert, dass Shors Algorithmus unter bestimmten Annahmen mit deutlich weniger physischen Qubits ausgeführt werden könnte als frühere Schätzungen nahelegten. Zugleich bleiben erhebliche Engineering-Herausforderungen.²

Warum Kryptografie unter Druck gerät

Quantencomputer könnten künftig verbreitete asymmetrische Verschlüsselungsverfahren wie RSA brechen.

Da heute gestohlene Daten später entschlüsselt werden könnten („Harvest Now, Decrypt Later“), müssen Unternehmen ihre Kryptografie bereits jetzt überprüfen und die Migration vorbereiten.

Denn: Die Verschlüsselung von heute muss auch gegen die Rechenleistung von morgen bestehen.

Warum die Gefahr bereits heute besteht

Wie im Leitartikel von Jens Bläser und Armin Reinhardt bereits erläutert, ist die Bedrohung, losgelöst vom Q-Day, durch „Harvest Now, Decrypt Later“ schon heute relevant. Zusätzlich sind Finanzinstitute durch die Art ihrer verarbeiteten Daten besonders exponiert.

Entscheidend ist nicht nur, wann ein kryptografisch relevanter Quantencomputer verfügbar wird, sondern auch, wie lange die Migration dauert und wie langfristig der Schutzbedarf ist. Übersteigen Schutz- und Migrationsdauer zusammen die Zeit bis zur Bedrohung, besteht bereits heute Handlungsbedarf. Aus einer technischen Zukunftswette

wird so eine konkrete Risiko- und Investitionsentscheidung.

Fazit:

Der Weg zur Krypto-Agilität

Die Antwort ist Post-Quanten-Kryptographie (PQC), die in den Folgebeiträgen vertieft wird. PQC ist keine Quantenkryptografie: Sie nutzt klassische Computer und mathematische Verfahren, für die keine effizienten Quantenangriffe bekannt sind. NIST veröffentlichte 2024 erste Standards, darunter ML-KEM, ML-DSA und SLH-DSA. Die Herausforderung liegt nun darin, sie in gewachsene Finanzarchitekturen zu überführen.⁴

Die Rolle eines Quantencomputing-Entwicklers besteht nicht darin, einen exakten „Q-Day“ vorherzusagen. Seriös ist vielmehr, Entwicklungen nüttern einzuordnen, Hype von belastbarer Forschung zu trennen und notwendige Vorbereitungsschritte klar zu benennen. Die Gefahr entsteht nicht erst, wenn ein Quantencomputer ein produktives Kryptosystem bricht. Sie entsteht bereits heute, wenn Daten mit langer Schutzdauer gesammelt werden und Organisationen ihre kryptografischen Abhängigkeiten nicht kennen.^{2,6}

Für die Finanzindustrie ist Quantencomputing Innovationsfeld und Resilienzthema. Es kann langfristig Optimierung, Simulation und Risikoanalyse verbessern, zwingt Institute aber zugleich, ihre digitalen Vertrauensinfrastrukturen zu prüfen. Gefragt sind weder Alarmismus noch Abwarten, sondern Aufklärung, Bestandsaufnahme und frühzeitige Vorbereitung. Entscheidend ist, ob die eigene Organisation rechtzeitig bereit ist.

Quellenangaben:

¹ Auer, R.; Dupont, A.; Gambacorta, L.; Park, J. S.; Takahashi, K.; Valko, A. Quantum computing and the financial system: opportunities and risks. BIS Papers No. 149, 2024.

² Cain, M. et al. Shor's algorithm is possible with as few as 10,000 reconfigurable atomic qubits. arXiv:2603.28627, 2026.

³ Scrivano, A. A Comparative Study of Classical and Post-Quantum Cryptographic Algorithms in the Era of Quantum Computing. arXiv, 2026.

⁴ NIST Computer Security Resource Center. Post-Quantum Cryptography, aktualisiert am 05.08.2026.

⁵ AbuGhanem, M. IBM Quantum Computers: Evolution, Performance, and Future Directions. arXiv:2410.00916, 2024.

⁶ Mascelli, J.; Rodden, M. Harvest Now Decrypt Later: Examining Post-Quantum Cryptography and the Data Privacy Risks for Distributed Ledger Networks. Federal Reserve FEDS, 2025, aktualisiert am 30.01.2026.

Der Autor



Udo Würtz ist Chief Technology Officer (CTO) von Fsas Technologies Europe, dem Plattformgeschäft von Fujitsu. Er berät das Top-Management führender Unternehmen zu IT-Strategien, Technologien und aktuellen Branchentrends.

Die Antwort auf das Quantenrisiko: PQC wird zur Pflicht

Von Prof. Dr. Dennis-Kenji Kipker

Quantencomputer werden die kryptografischen Verfahren angreifbar machen, auf denen Zahlungsverkehr und IT-Sicherheit der Finanzbranche heute beruhen. Mit der Post-Quantum-Kryptografie (PQC) stehen die technischen Gegenmaßnahmen jedoch bereits weitgehend zur Verfügung, sodass die eigentliche Herausforderung nicht mehr in der Forschung, sondern in der systematischen Migration komplexer, historisch gewachsener Finanz-IT-Landschaften liegt. Wer jetzt mit der Bestandsaufnahme beginnt, verschafft sich einen entscheidenden Vorsprung für diese mehrjährige Transformation.

Was Post-Quantum-Kryptografie leistet und wie sie sich von klassischen Verfahren unterscheidet

Die Bedrohung durch Quantencomputer betrifft im Kern zwei für die heutige IT-Sicherheit entscheidende mathematische Probleme: nämlich die Faktorisierung großer Zahlen und die Berechnung diskreter Logarithmen. Beide Probleme lassen sich mit klassischen Rechnern praktisch nicht lösen, wohl aber mit einem ausreichend leistungsfähigen Quantencomputer und dem sogenannten Shor-Algorithmus, der RSA- und ECC-Verfahren in überschaubarer Zeit aushebeln würde. Deshalb setzt Post-Quantum-Kryptografie auf vollkommen andere mathematische Grundlagen, insbesondere auf Gitterprobleme, hashbasierte Signaturen sowie code- und multivariate Verfahren, die nach heutigem Kenntnisstand auch für Quantencomputer nicht effizient lösbar sind.

Ein wesentlicher Unterschied zur klassischen Kryptografie liegt darin, dass Post-Quantum-Verfahren vollständig auf klassischer Hardware laufen und sich in bestehende Protokolle wie TLS, IPsec oder Signaturformate integrieren lassen, ohne dass ein Institut selbst Quantentechnologie betreiben müsste. Genau diese Eigenschaft ist der entscheidende praktische Vorteil, denn sie erlaubt eine Migration über Software-Updates und Zertifikatserneuerungen, während die physische Infrastruktur weitgehend erhalten bleibt.

Das Risiko langlebiger Daten: „Harvest Now, Decrypt Later“

Besonders deutlich wird die Dringlichkeit bei langlebigen Daten. Kreditverträge, Kundendossiers und aufsichtsrechtlich vorgeschriebene Archive müssen häufig zehn bis dreißig Jahre lang vertraulich bleiben. Deshalb stellen bereits heute abgegriffene, verschlüsselte Daten selbst dann ein Risiko dar, wenn ein leistungsfähiger Quantencomputer erst in zehn Jahren verfügbar sein wird. Dieses Prinzip, das unter dem Begriff „Harvest Now, Decrypt Later“ bekannt ist, verändert die Priorisierung erheblich. Denn nicht die unmittelbare Angreifbarkeit eines Systems entscheidet heute über die Dringlichkeit, sondern die Vertraulichkeitsdauer der jeweils verarbeiteten Daten.

Abgrenzung: Post-Quantum-Kryptografie vs. Quantum Key Distribution

Post-Quantum-Kryptografie wird zudem häufig mit Quantum Key Distribution verwechselt. Tat-

sächlich handelt es sich jedoch um zwei grundverschiedene Ansätze. Quantum Key Distribution nutzt physikalische Eigenschaften einzelner Photonen, um Schlüssel über dedizierte Glasfaserstrecken auszutauschen, benötigt dafür spezialisierte Hardware und bleibt auf begrenzte Distanzen sowie Punkt-zu-Punkt-Verbindungen beschränkt. Für die breite Absicherung von Kernbankensystemen, Zahlungsverkehr und Kundenschnittstellen ist dieser Ansatz weder wirtschaftlich noch technisch praktikabel. Instituten wird deshalb regelmäßig empfohlen, ihre IT-Investitionen auf Post-Quantum-Kryptografie zu konzentrieren und Quantum Key Distribution allenfalls für einzelne, hochsensible Verbindungen in Betracht zu ziehen.

Die neuen Standards geben die Richtung vor

Mit der Veröffentlichung von FIPS 203, FIPS 204 und FIPS 205 hat das US-amerikanische National Institute of Standards and Technology im August 2024 erstmals verbindliche Standards für die Post-Quantum-Kryptografie festgelegt. ML-KEM, abgeleitet aus dem Verfahren Kyber, dient dem quantensicheren Schlüsselaustausch, während ML-DSA und SLH-DSA, basierend auf Dilithium und SPHINCS+, für digitale Signaturen vorgesehen sind. In einem Entwurf zur Übergangsplanung sieht NIST außerdem vor, quantenverwundbare Public-Key-Verfahren schrittweise zurückzunehmen: Verfahren mit nur 112 Bit Sicherheitsstärke sollen nach 2030 als überholt gelten, und nach 2035 sollen die heute gebräuchlichen quantenverwundbaren Public-Key-Verfahren grundsätzlich nicht mehr zugelassen sein. Zusätzlich bereitet das NIST mit HQC einen weiteren Algorithmus für die Schlüsselsenkapselung vor, um für den Fall abzusichern, dass sich bei gitterbasierten Verfahren im Zeitverlauf unerwartete Schwächen zeigen sollten.

Die Notwendigkeit kryptografischer Agilität

Damit dieser Rahmen in der Praxis tragfähig bleibt, kommt der kryptografischen Agilität eine Schlüsselrolle zu, denn kein Standard wird für alle Zeit gültig bleiben. Systeme sollten Verschlüsselungsalgorithmen daher nicht fest verdrahtet nutzen, sondern sie über zentral steuerbare Bibliotheken und Konfigurationen einbinden. Dadurch lassen sich Verfahren austauschen, sobald neue Erkenntnisse vorliegen oder Schwachstellen dies erfor-

Wie Security-Architekturen quantensicher werden

Entscheidend sind:

- **Kryptoagilität und „quantum-secure-by-design“:**
Kryptografische Funktionen müssen flexibel austauschbar sein. Neue Systeme sollten nach dem Prinzip „quantum-secure-by-design“ entwickelt werden.
- **Abhängigkeiten und Organisation:**
HSMs, Cloud- und API-Landschaften sowie Dienstleister müssen frühzeitig in die Planung einbezogen werden. PQC braucht klare Governance, Budget, Zeitplan und Verantwortlichkeiten.
- **Inventur und Priorisierung:**
Algorithmen, Schlüssel, Zertifikate, Schnittstellen sowie Dienstleisterabhängigkeiten erfassen und nach Sensitivität, Aufbewahrungsdauer und externer Exponierung priorisieren.
- **Hybride Verfahren:**
Klassische und Post-Quantum-Verfahren sollten in der Übergangsphase kombiniert werden. So lässt sich der Schutz schrittweise erhöhen, ohne auf eine vollständige Ablösung bestehender Verfahren zu warten.
- **Security-by-Design:**
Quantensicherheit sollte bereits bei neuen Systemen und in Beschaffungsprozessen berücksichtigt werden. Anbieter und Dienstleister sollten frühzeitig verbindliche Roadmaps für PQC-Unterstützung vorlegen.

dern. Genau dieser Aspekt wird in vielen Projekten unterschätzt, weil Legacy-Anwendungen kryptografische Parameter oft tief im Quellcode verankert haben. Ein Austausch bedeutet daher weit mehr als eine reine Konfigurationsänderung.

Risikominimierung durch hybride Verfahren in der Übergangsphase

Für die Übergangsphase, die je nach System mehrere Jahre andauern dürfte, empfehlen sich hybride Verfahren. Diese kombinieren klassische Algorithmen wie RSA oder ECC mit einem Post-Quantum-Verfahren im selben Handshake. Solange eines der beiden Verfahren hält, bleibt die Verbindung sicher – das federt Implementierungsrisiken neuer Algorithmen ab und erfüllt zugleich regulatorische Anforderungen bereits heute. TLS 1.3 unterstützt hybride Schlüsselaustauschverfahren inzwischen produktiv, und große Cloud-Anbieter sowie Browser-Hersteller haben die entsprechende Unterstützung bereits ausgerollt. Institute sollten daher hybride Pilotprojekte an exponierten Schnittstellen zeitnah starten, statt auf die finale Marktreife zu warten.

Regulatorischer Druck für den Finanzsektor: NIS-Roadmap und DORA

Für Banken und Versicherer kommt zu diesen technischen Fristen ein regulatorischer Zeitplan hinzu, der die Dringlichkeit zusätzlich unterstreicht. Die

europäische NIS-Kooperationsgruppe hat im Juni 2025 gemeinsam mit der Europäischen Kommission eine koordinierte Roadmap veröffentlicht. Demnach sollen alle Mitgliedstaaten bis Ende 2026 mit Kryptografie-Inventuren und nationalen Migrationsstrategien beginnen. Systeme mit hohem Risiko, wozu weite Teile der Finanzinfrastruktur zählen, sollen bis Ende 2030 auf Post-Quantum-Kryptografie umgestellt sein. Der Digital Operational Resilience Act (DORA) verstärkt diesen Druck zusätzlich: denn die Verordnung verlangt von Finanzunternehmen bereits seit Januar 2025 ein Verschlüsselungs- und Kryptografiemanagement, das den gesamten Lebenszyklus kryptografischer Schlüssel abdeckt und regelmäßig an den Stand der Technik angepasst werden muss. Wer diese Anforderung ernst nimmt, kommt an einer Post-Quantum-Roadmap kaum vorbei, auch wenn die Verordnung den Begriff selbst nicht ausdrücklich nennt.

Wie Security-Architekturen quantensicher werden

Die architektonische Basis: Zentralisierung und Entkopplung

Auf Architekturebene lässt sich kryptografische Agilität nur erreichen, wenn Schlüssel- und Zertifikatsverwaltung zentralisiert und von der einzelnen Anwendung entkoppelt werden. In Projekten zeigt sich regelmäßig, dass genau diese Entkopplung fehlt. Der Grund hierfür: Über Jahre gewachsene Systemlandschaften haben kryptografische Funktionen dezentral und uneinheitlich implementiert. Eine belastbare Public-Key-Infrastruktur (PKI) mit klar definierten Verantwortlichkeiten und automatisierter Zertifikatsrotation bildet deshalb das Fundament jeder quantensicheren Architektur.

Risikominimierung durch Zero-Trust-Prinzipien

Zero-Trust-Prinzipien gewinnen in diesem Zusammenhang zusätzlich an Bedeutung, da sie ohnehin jede Sitzung und jede Transaktion einzeln authentifizieren, statt sich auf einen vermeintlich sicheren Netzwerkperimeter zu verlassen. Gerade langlebige Zugangsdaten und Signaturschlüssel zählen zu den bevorzugten Zielen – unter anderem für das eingangs beschriebene Vorgehen des Abgreifens verschlüsselter Daten auf Vorrat. Zero-Trust-Architekturen und quantensichere Verfahren ergänzen sich daher sinnvoll und senken das Restrisiko spürbar.

Zukunftsfähige Beschaffung und Herstellerabhängigkeiten

Neue Systeme sollten von Beginn an nach dem Prinzip „quantum-secure-by-design“ entwickelt werden, damit während der laufenden Migration kein neuer technischer Rückstand entsteht. Für Beschaffungsprozesse bedeutet das, von Softwareanbietern und Dienstleistern verbindliche Roadmaps zur Unterstützung von Post-Quantum-Verfahren einzufordern, bevor neue Verträge geschlossen werden. In der Praxis ist das hochrelevant, denn in einem Kernbankensystem werden Transaktionen häufig über ein Hardware-Sicherheitsmodul signiert, dessen Hersteller womöglich noch keinen konkreten Fahrplan für Post-Quan-

Das Quantenrisiko steuern:

Warum PQC eine strategische Migrationsaufgabe ist

➤ Das Quantenrisiko ist keine Zukunftsfrage mehr, sondern eine Migrationsaufgabe:

Quantencomputer könnten die heute eingesetzten Public-Key-Verfahren wie RSA und ECC brechen. Gleichzeitig müssen Finanzinstitute Daten schützen, deren Vertraulichkeit noch Jahrzehnte relevant ist. Das macht eine frühzeitige Vorbereitung auf Post-Quantum-Kryptografie (PQC) erforderlich.

➤ Die technische Lösung steht weitgehend bereit – die Herausforderung liegt in der Migration:

Gewachsene IT-Landschaften, Legacy-Systeme, HSMS, Cloud- und API-Schnittstellen sowie Abhängigkeiten von Dienstleistern machen den Austausch kryptografischer Verfahren zu einer mehrjährigen Transformation. Kryptografische Agilität wird deshalb zum zentralen Architekturprinzip.

➤ Für Vorstände bedeutet das:

PQC ist kein isoliertes IT-Projekt. Institute brauchen eine systematische Kryptografie-Inventur, eine risikobasierte Priorisierung, klare Verantwortlichkeiten und eine mehrjährige Migrations-Roadmap. Hybride Verfahren können dabei den Übergang absichern. Wer jetzt mit der Bestandsaufnahme beginnt und kritische Abhängigkeiten früh identifiziert, schafft die Grundlage für eine kontrollierte Migration statt eines späteren Technologiewechsels unter Zeitdruck.

tum-Algorithmen vorlegen kann. Da sich solche Abhängigkeiten nicht kurzfristig auflösen lassen, sollten sie so früh wie möglich identifiziert und in die Beschaffungsplanung eingesteuert werden.

Sicherheitsanforderungen an Cloud- und API-Landschaften

Besondere Aufmerksamkeit verdienen zudem Cloud- und API-Landschaften, denn Zahlungsverkehrsschnittstellen nach ISO 20022, Open-Banking-APIs und die TLS-Terminierungspunkte großer Cloud-Anbieter bilden oft die am stärksten exponierten und zugleich am schwierigsten zu überblickenden Teile der Infrastruktur. Institute sollten deshalb von ihren Cloud- und API-Gateway-Anbietern verlangen, hybride TLS-Konfigurationen und quantensicheres Schlüsselmanagement als Dienstleistung bereitzustellen, statt diese Aufgabe vollständig intern zu lösen.

Organisatorische Governance und Kompetenzaufbau

Eine der größten Herausforderungen ist dabei häufig weniger technischer als organisatorischer Natur. In mehreren Projekten hat sich regelmäßig gezeigt, dass Sicherheitsarchitektur, Anwendungsentwicklung und Fachbereiche zunächst unterschiedliche Prioritäten setzen und ein gemeinsames Verständnis für die Dringlichkeit erst erarbeitet werden muss. Bewährt hat sich deshalb

ein bereichsübergreifendes Programm mit klarer Governance, das Budget, Zeitplan und Verantwortlichkeiten über mehrere Jahre hinweg sichtbar macht, statt Post-Quantum-Kryptografie als Aufgabe einzelner IT-Teams zu behandeln. Ebenso wichtig ist der gezielte Aufbau eigener Kryptografie-Kompetenz, denn Fachkräfte mit praktischer Erfahrung in Post-Quantum-Verfahren sind am Markt knapp und lassen sich nur begrenzt einkaufen.

Der Migrationspfad: Kryptografie-Inventur und Priorisierung

Deshalb sollte jede Migration mit einer vollständigen Kryptografie-Inventur beginnen, in der sämtliche Algorithmen, Schlüssellängen und Zertifikatslaufzeiten sowie APIs, andere Schnittstellen und Abhängigkeiten von Dienstleistern systemübergreifend erfasst werden.

Auf dieser Grundlage lässt sich eine Priorisierung ableiten, die sich an zwei Kriterien orientiert: der Sensitivität und der Aufbewahrungsdauer der verarbeiteten Daten einerseits sowie dem Grad der externen Exponierung eines Systems andererseits. Internetseitige Schnittstellen mit langlebigen Kundendaten, etwa im Zahlungsverkehr oder bei Vertragsarchiven, sollten daher vor internen Back-office-Systemen migriert werden, während tief integrierte Komponenten wie Hardware-Sicherheitsmodule aufgrund ihrer Abhängigkeit von Herstellerzyklen typischerweise die längste Vorlaufzeit benötigen und entsprechend früh eingeplant werden sollten.

Fazit: eine mehrjährige Transformation, kein bloßes IT-Projekt

Post-Quantum-Kryptografie lässt sich nicht als abgeschlossenes Technologieprojekt behandeln, da sie Architektur, Governance, Beschaffung und Personalentwicklung gleichermaßen betrifft und sich über mehrere Jahre und Budgetzyklen erstreckt. Die Transformation gelingt dort am besten, wo sie von Vorstand, CIO, CISO und CRO gemeinsam getragen und in bestehende Programme wie die DORA-Compliance, das Risikomanagement und laufende IT-Modernisierungsvorhaben eingebettet wird, anstatt als isolierte Initiative parallel dazu zu laufen.

Wer jetzt mit der Kryptografie-Inventur beginnt, kryptografische Agilität als Architekturprinzip verankert und hybride Verfahren pilotiert, schafft die Grundlage, um die eigene Organisation rechtzeitig und beherrschbar auf das Quantenzeitalter vorzubereiten.

Der Autor



Prof. Dr. Dennis-Kenji Kipker studierte Rechtswissenschaft und Informatik. Als Gründer und wissenschaftlicher Direktor des *cyberintelligence.institute* forscht er an der Schnittstelle von Recht und Technik in den Bereichen Cybersicherheit, Konzernstrategie und digitale Resilienz im Kontext globaler Krisen.

Von der Risikoanalyse zur Umsetzung: Eine Roadmap zur Quantensicherheit

Von Andreas Breunig

Quantensicherheit in der Finanzwirtschaft ist primär eine organisatorische, erst nachgelagert eine technische Aufgabe. Langfristig schutzbedürftige Informationen, kryptografische Abhängigkeiten und Verantwortlichkeiten müssen früh identifiziert und gesteuert werden. Eine erfolgreiche PQC-Migration erfordert zeitabhängigen Schutzbedarf, ein unternehmensweites Kryptoinventar sowie einen mandatierten Transformationsprozess mit klaren Zuständigkeiten, Budget und Governance.

Banken und Versicherungen, insbesondere die Erstversicherer, bieten Schutz und finanzielle Sicherheit gegen Risiken auf Zeit. Sie geben heute ein Versprechen ab, das oft erst Jahrzehnte später eingelöst wird, beispielsweise bei Lebens-, Kranken- oder Pflegeversicherungen. Wie im Leitartikel dargestellt, können jedoch bereits heute langfristig schutzbedürftige Daten durch „Harvest Now, Decrypt Later“-Angriffe gefährdet sein. Für Erstversicherer ist dies aufgrund der Art der verarbeiteten Daten besonders relevant.

Die zeitliche Perspektive des Informationsverbundes

Wie bereits im Beitrag von Prof. Dr. Kipker ausgeführt, wird die Debatte über PQC noch zu häufig als rein technisches Problem gesehen. Im ersten Schritt geht es weniger um die Auswahl neuer kryptografischer Verfahren als darum, den Informationsverbund um eine zeitliche Perspektive zu erweitern.

Ausgangspunkt sind dabei die kritischen Geschäftsprozesse und Funktionen sowie die Informationen, Anwendungen und Systeme, von denen sie abhängen. Damit wird die Geschäftskritikalität mit dem Schutzbedarf der jeweils unterstützenden Informationen und IKT-Komponenten verbunden. Neben dem heutigen Schutzbedarf muss bewertet werden, welche Informationen und Funktionen auch morgen oder in vielen Jahren noch hohe Anforderungen an Vertraulichkeit, Integrität, Authentizität und Nichtabstreitbarkeit stellen werden.

Für die PQC-Roadmap müssen deshalb Geschäftskritikalität, Schutzziel und Schutzfrist gemeinsam betrachtet werden. Dabei ist die zeitliche Risikologik nicht für alle Schutzziele identisch: So können langfristig vertrauliche Informationen bereits heute durch „Harvest now, Decrypt later“-Angriffe gefährdet sein, während bei digitalen Nachweisen, Identitäten und anderen kryptografisch abgesicherten Funktionen insbesondere relevant ist, wie lange Integrität, Authentizität und Nichtabstreitbarkeit gewährleistet bleiben müssen und wie viel Zeit für ihre Migration benötigt wird.¹

Erst diese Betrachtung schafft das Fundament, um risikoreiche Bereiche zu identifizieren und in der PQC-Roadmap zu priorisieren. Das Verständnis des Informationsverbundes bildet die zentrale

Grundlage risikobasierter Informationssicherheit. Es macht sichtbar, von welchen Informationen, Anwendungen und Systemen kritische Geschäftsprozesse abhängen und übersetzt damit technisches Risiko in Geschäftsrelevanz.

Seine Einführung vor rund 20 Jahren war ein langwieriger Kulturwandelprozess. Die Erweiterung um zeitliche Aspekte sowie die wachsende Bedeutung von Authentizität und Nichtabstreitbarkeit wird einen ähnlichen langwierigen Prozess erfordern. Die PQC-Roadmap beginnt daher mit einem erweiterten Verständnis des Informationsverbundes.

Das Kryptoinventar ermöglicht risikobasierte Entscheidungen zum Aufbau der PQC-Roadmap

Die Erstellung eines Kryptoinventars zur Identifikation bereits etablierter kryptografischer Verfahren und Schnittstellen ist eine wesentliche Grundlage für die Priorisierung der Migration auf quantensichere Verfahren (siehe Beitrag Prof. Dr. Kipker).

Herausforderungen bei der Inventarisierung

Das Inventar muss erkennen lassen, welche Assets quantengefährdet sind, welche Alternativen bestehen und welche Abhängigkeiten ihre Migration bestimmen. Besondere Aufmerksamkeit erfordern Legacy-Systeme, eingeschränkt gepflegte Anwendungen, Schatten-IT und ältere IDVen, da historisch gewachsene Strukturen häufig nur mit erheblichem Aufwand verändert werden können.²

Kryptografie ist dabei vielerorts noch in Anwendungscode, Bibliotheken, Appliances oder Schnittstellen eingebettet, ohne durchgängig transparent steuerbar zu sein.

Für PQC müssen kryptografische Komponenten deshalb transparent inventarisiert, modular eingebunden und kontrolliert austauschbar werden. Automatisierte Discovery-Werkzeuge und Software-QS-Scanner (wie GitHub CodeQL) unterstützen die Analyse von Quellcode, Systemen und Netzwerkcommunication, erfassen Nutzungskontext und Abhängigkeiten jedoch nicht vollständig. Entwickler und Systemverantwortliche müssen die Ergebnisse daher fachlich validieren und ergänzen.³

Quantensicherheit: Vier Fragen für Entscheider

Quantensicherheit ist keine reine IT-Aufgabe. Entscheidend ist, ob das Unternehmen Schutzbedarf, technische Abhängigkeiten und Verantwortlichkeiten bereits so steuert, dass eine rechtzeitige Migration möglich wird.

1. Was müssen wir langfristig schützen?

Welche Informationen und kritischen Funktionen haben einen langfristig hohen Schutzbedarf?

2. Wo setzen wir heute Kryptografie ein?

Welche Systeme, Anwendungen, Schnittstellen und externen Abhängigkeiten sind betroffen?

3. Was muss zuerst migriert werden?

Wo treffen hohe Quantenverwundbarkeit, hohes Schadenspotenzial und lange Migrationszeiten aufeinander?

4. Wer steuert die Transformation?

Sind Verantwortung, Risikoappetit, Budget und Governance verbindlich festgelegt?

Die zentrale Managementfrage lautet:

Sind wir heute in der Lage zu entscheiden, was wann migriert werden muss und wer diese Entscheidung verantwortet?

Die PQC-Roadmap integriert alle Teilnehmer der digitalen Supply-Chain

Crypto Discovery muss auch APIs und andere Schnittstellen, externe Kommunikationsverbindungen sowie kryptografische Abhängigkeiten zu Cloud-Diensten, Standardssoftware, Hardware-Sicherheitsmodulen (HSM) und IT-Dienstleistern erfassen.

Es muss transparent sein, welche Kryptografie eingesetzt wird, welche Gegenpartei beteiligt ist, wer Änderungen veranlassen kann und wann externe Anbieter PQC-fähige Lösungen bereitstellen.⁴

Die Roadmap externer Partner bestimmt unmittelbar die eigene Migrationsfähigkeit des Instituts. Auf dieser Grundlage werden Quick Wins, kritische Systeme und Abhängigkeiten identifiziert, die die tatsächliche Reihenfolge der PQC-Migration bestimmen.

Agile Priorisierung bedeutet, nicht auf Vollständigkeit zu warten

Ein vollständiges Kryptoinventar bleibt das Ziel. Im Sinne einer agilen Steuerung darf dessen Vollständigkeit jedoch nicht zur Voraussetzung für erste Entscheidungen werden.

Die Inventarisierung kann sich zunächst auf Komponenten mit identifiziertem oder vermutetem PQC-Risiko konzentrieren. Parallel werden Schutzdauer, Quantenverwundbarkeit, Schadenspotenzial, Migrationsaufwand und Abhängigkeiten bewertet. Abhängigkeiten sind ein relevanter Faktor, der gerne übersehen wird.

In ersten Ansätzen wird aus Quantenverwundbarkeit, potenziellen Schäden sowie Aufwand

Das PQC-Rollenmodell

Das Rollenmodell sollte Informationssicherheit, IT, Risiko, Compliance, Einkauf und Fachbereiche verbinden:

CISO: Verantwortet die Methodik der PQC-Risikobewertung und führt Schutzbedarf, Kryptoinventar und Risiken zu einer steuerbaren Gesamtsicht zusammen.

CIO: Verantwortet die technische Inventarisierung (Crypto Discovery), die Zielarchitektur, Releaseplanungen und die Durchführung der Migrationswellen.

CRO: Integriert die PQC-Risiken in das bestehende IKT-Risikomanagement und eskaliert Abweichungen vom Risikoappetit an die Entscheidungsgremien.

Compliance: Übersetzt regulatorische Entwicklungen (z. B. DORA) in Vorgaben für Governance und Nachweisführung.

Einkauf (CPO): Verankert Anforderungen an PQC-Fähigkeit und Kryptoagilität in Ausschreibungen, Verträgen und der Lieferantensteuerung.

Fachbereiche: Bestimmen die Geschäftskritikalität und den zeitachsenspezifischen Schutzbedarf der von ihnen verantworteten Daten und Prozesse.

Entscheidend ist das Zusammenspiel dieser Funktionen:

Erst wenn technische Abhängigkeiten, geschäftliche Kritikalität, regulatorische Anforderungen und der Risikoappetit zusammengeführt werden, lässt sich das Tempo der PQC-Migration fundiert steuern.

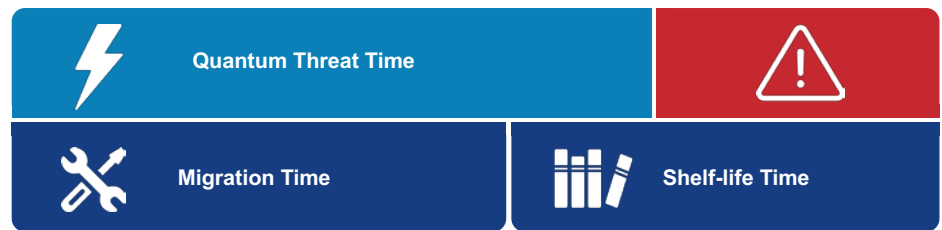
und Dauer der PQC-Migration ein PQC-Risikowert abgeleitet. Hohe Risiken verlangen frühes Handeln.⁵

No-Regret-Maßnahmen: Sofort umsetzbare Schritte

Daraus lassen sich unmittelbare No-Regret-Maßnahmen ableiten: Prioritäre Bereiche inventarisieren, veraltete Protokolle ablösen, Lieferanten nach ihrer PQC-Planung abfragen und Kryptoagilität in Architektur und Beschaffung verankern.⁶

Drei Zeitgrößen bestimmen die Dringlichkeit der PQC-Migration

Die zeitliche Logik lässt sich nach Mosca und Piani auf drei Größen verdichten. Dies sind Schutzdauer („Shelf-Life“), PQC-Migrationszeit („Migration Time“) und der erwartete Zeitraum bis zu einem kryptografisch relevanten Quantencomputer („Quantum Threat Time“). Für die Priorisierung ist daher nicht entscheidend, den Q-Day möglichst genau vorherzusagen. Maßgeblich ist vielmehr das Verhältnis dieser drei Zeitgrößen zueinander.⁷



Drei Zeitgrößen bestimmen die Dringlichkeit der PQC-Migration.

Quelle: Quantum Threat Timeline Report 2024

Die Mosca-Ungleichung als Entscheidungsgrundlage

Diese Entscheidungslogik wird durch die Mosca-Ungleichung beschrieben. Ist der Zeitraum bis zur Quantenbedrohung kürzer als die Summe aus notwendiger Schutzdauer und PQC-Migrationszeit, besteht ein materielles kryptografisches Risiko. Die Ungleichung übersetzt damit einen unsicheren technologischen Zeithorizont in eine organisations- und systemspezifische Risikobetrachtung.⁸

Diese Unsicherheit prägt auch die Umsetzung der PQC-Roadmap. Ihre Phasen überlappen bewusst und sind nicht als starre Sequenz zu verstehen. Deshalb müssen Vorbereitung, Risikobewertung und erste Umsetzungsmaßnahmen parallel erfolgen.

Zu Beginn werden Scope, Verantwortlichkeiten, Bewertungslogik und ein Kryptoinventar für prioritäre Domänen erstellt. Parallel können Lieferantenabfragen, PQC-Risikobewertungen und erste Migrations-Piloten starten. Mit wachsender Transparenz werden Kryptoinventar und Risikobild erweitert und die ersten PQC-Migrationswellen vorbereitet und umgesetzt. Danach verlagert sich der Schwerpunkt auf Skalierung, Legacy-Ablösung und die Überführung in den Regelbetrieb.

Regulatorik und Governance geben den Rahmen für PQC vor

Bestehende Regulatorik schafft einen Rahmen, an den die PQC-Steuerung anknüpfen kann. Für die europäische Finanzwirtschaft ist das insbesondere der Digital Operational Resilience Act (DORA).⁹ Die technischen Regulierungsstandards verlangen, relevante Entwicklungen in der Kryptografie zu verfolgen und kryptografische Bedrohungen – einschließlich solcher, die aus Fortschritten der Quantentechnologie entstehen – mit einem flexiblen Ansatz aus Risikominderung und Überwachung zu begegnen.

Die PQC-Migration sollte deshalb nicht als paralleles Sonderprogramm neben der bestehenden IKT-Risiko- und Resilienzsteuerung behandelt werden, sondern in diese integriert werden. Damit wird die PQC-Risikobewertung zugleich zur Governance-Aufgabe.

Die Geschäftsleitung muss ein entsprechendes Mandat sowie Risikoappetit und Ressourcen festlegen, um die Umsetzung der PQC-Roadmap zu enablen und die Interoperabilität innerhalb der Organisation sicherzustellen (siehe Infobox in der linken Spalte).

Fazit: Langfristigen Schutz frühzeitig absichern

Quantensicherheit beginnt organisatorisch, nicht technologisch. Es muss klar sein, welche Informationen und kritischen Funktionen langfristig geschützt werden, welche kryptografischen Assets dafür eingesetzt werden, welche Abhängigkeiten bestehen und wer entscheidet.

Dafür braucht es vier Voraussetzungen:

1. einen um Schutzdauer erweiterten Informationsverbund,
2. ein unternehmensweites Kryptoinventar,
3. klare Verantwortlichkeiten,
4. sowie ein mandatiertes PQC-Programm mit Budget, Risikoappetit und Steuerung der digitalen Lieferkette.

Diese Grundlagen ermöglichen eine kontrollierte PQC-Migration und stärken bereits heute die Fähigkeit, auf kryptografische Veränderungen zu reagieren.

Quellenangaben:

¹ Algemeen Inlichtingen- en Veiligheidsdienst (AIVD) / CWI / TNO: The PQC Migration Handbook. Guidelines for Migrating to Post-Quantum Cryptography, Den Haag 2024.

² AIVD/CWI/TNO, PQC Migration Handbook (2024)

³ National Institute of Standards and Technology (NIST): Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms, Washington, D.C. 2021; Walker Chablott: Addressing Post-Quantum Cryptography with CodeQL, 2023;

⁴ AIVD/CWI/TNO, PQC Migration Handbook (2024)

⁵ AIVD/CWI/TNO, PQC Migration Handbook (2024)

⁶ AIVD/CWI/TNO, PQC Migration Handbook (2024)

⁷ AIVD/CWI/TNO, PQC Migration Handbook (2024); Mosca, Michele; Piani, Marco: Quantum Threat Timeline Report, Global Risk Institute, 2024.

⁸ AIVD/CWI/TNO, PQC Migration Handbook (2024); Mosca, Michele; Piani, Marco: Quantum Threat Timeline Report, Global Risk Institute, 2024.

⁹ Delegierte Verordnung (EU) /1774, Art. 6 Abs. 3–5, 2024

Der Autor



Bildrechte: ERGO

Andreas Breunig ist seit Mai 2022 Chief Information Security Officer (CISO) der ERGO Group AG. Er verantwortet die internationale Implementierung des konzernweiten Information Security Risk Managements. Zuvor war er unter anderem als CISO bei Henkel tätig.

Quantenresilienz als Führungsaufgabe: Wie Vorstände heute die Weichen stellen

Von Michael Ehrnsperger

Quantencomputing wird in den Chefetagen des Finanzsektors noch kaum als Bedrohung wahrgenommen. Zwar testen erste Institute neue Krypto-Verfahren, doch für echte Quantenresilienz ist ein breiterer Ansatz erforderlich: Neben moderner Verschlüsselung sind ein agiles Risikomanagement, bereichsübergreifende Teams, die Absicherung des laufenden Betriebs und praxiserprobte Krisenszenarien notwendig.

Nur ein Software-Update?

„Wir haben noch keine Cyber-Attacke vom Ausmaß einer Pandemie gesehen, aber wir sollten darauf vorbereitet sein – schon längst!“ Diese Warnung der *Munich Cyber Security Conference* im Februar 2026 rüttelt auf. Spätestens mit dem „Q-Day“ drohen völlig neue Dimensionen von Cyberangriffen.

Wie verwundbar unsere vernetzte Welt ist, zeigte der CrowdStrike-Ausfall im Juli 2024¹, der globale IT-Systeme schlagartig lahmlegte. Der Vorfall offenbarte erhebliche Defizite bei der Krisenvorbereitung der Finanzwirtschaft. Während die Software schnell wieder lief, dauerte die vollständige Wiederherstellung des Geschäftsbetriebs oft Wochen. Laut der britischen Finanzaufsicht FCA fehlte ein ganzheitlicher Blick auf die operationelle Resilienz – insbesondere bei der Verzahnung von Krisenmanagement, Business Continuity und IT-Wiederherstellung.² Die aktuelle Debatte um Quantensicherheit greift hier oft zu kurz: Viele Unternehmen behandeln das Thema wie ein einfaches Software-Update, anstatt es strategisch anzugehen.

Der erweiterte Horizont

Die Bedrohung durch Quantencomputing ist Teil einer zunehmend dynamischen Cyber-Bedrohungslage. Künstliche Intelligenz (KI) katapultiert Angriffe bereits in neue Dimensionen: Von automatisierten KI-Agenten bis hin zur blitzschnellen Suche nach Software-Schwachstellen ist alles möglich. Quantencomputer werden das Training von KI zudem exponentiell beschleunigen, was ein schnelleres Patch-Management und anpassungsfähigere Sicherheitsarchitekturen erfordert.

Auch die neuen Verschlüsselungsmethoden werden erst noch durch den Praxiseinsatz im großen Umfang verprobt, aktives Monitoring und Vorbereitung auf Veränderungen müssen Teil der künftigen Prozesse sein. Dies alles zeigt, dass das jahrzehntelang statische Thema „Verschlüsselung“ künftig einen agilen Ansatz erfordert.

Noch mehr Abhängigkeit?

Die geopolitische Instrumentalisierung von US-amerikanischen IT-Anbietern gefährdet die Souveränität europäischer Finanzdienstleister. Quantensicherheitslösungen von Hyperscalern verschärfen diese Abhängigkeit häufig, da sie an proprietäre Verschlüsselungsdienste ohne Multi-Cloud-Support gebunden sind. Beim Confidential Computing müssen Unternehmen daher genau wissen, wer die Kontrolle über Schlüssel und Sicherheitsfunktionen hat. Die entscheidende Frage lautet: Wird das

Ziel größerer Quantenresilienz am Ende durch eine neue technologische Abhängigkeit konterkariert?

Das neue Horrorszenario: HNDL³

Ein Akronym, das Vorstände kennen sollten: HNDL („Harvest Now, Decrypt Later“) beschreibt eine unmittelbare Bedrohung. Angreifer sammeln bereits heute kryptografisch gesicherte Daten, um sie später zu entschlüsseln. Banken und Versicherungen sind Hauptziele, da Transaktionen, Identitäten und Verträge jahrzehntelang absolute Integrität erfordern.

Die notwendigen Maßnahmen sind jedoch umfangreich und realistischerweise Mehrjahresprogramme. Gleichzeitig sind die verfügbaren Ressourcen begrenzt: Nur 14 Prozent der Organisationen sind überzeugt, über die erforderlichen Mitarbeiter und Fähigkeiten im Bereich Cybersicherheit zu verfügen.⁴ Das Management sollte daher frühzeitig einen klaren Fahrplan mit Prioritäten, Verantwortlichkeiten sowie langfristiger Budget- und Ressourcenplanung einfordern.

Technologie-Migration: Nachhaltige Stabilität statt Aktionismus

Versteht das Management das Problem, werden oft schnelle Lösungen gefordert. Doch Kryptografie ist nicht einfach als Tresorschloss zu verstehen: Sie greift tief in Daten, Prozesse und die Kundeninteraktion ein. Gerade in historisch gewachsenen IT-Infrastrukturen von Banken und Versicherungen birgt eine abrupte Umstellung erhebliche Risiken für die Betriebsstabilität.

Zudem müssen sich neue PQC-Verfahren in der Praxis erst bewähren. Eine sofortige, vollständige Migration ist daher riskant. Die Lösung ist ein hybrider kryptografischer Ansatz: Er kombiniert klassische und quantensichere Algorithmen in einem Prozess – eine Strategie, die auch das BSI ausdrücklich empfiehlt.⁵

Was passiert eigentlich, wenn?

Auch verschlüsselte Daten waren schon immer Ziel erfolgreicher Angriffe – durch technische Fehler, Organisationsversagen oder den Faktor Mensch. Im Post-Quantum-Zeitalter wird das Tandem aus KI und Quantencomputing kleinste Schwachstellen jedoch noch viel schneller und massiver ausnutzen. Da die Finanzbranche einheitliche Standards nutzt, können schon vereinzelt Vorfälle das Vertrauen in das gesamte System erschüttern. Auch Angriffe auf kritische Infrastrukturen (z. B. Strom- und Datennetze) bedrohen den Sektor direkt.

Was Unternehmen jetzt tun müssen

Quantenresilienz entsteht nicht allein durch den Austausch kryptografischer Verfahren. Vorstände sollten deshalb fünf Handlungsfelder aufsetzen:

1. Kryptografische Abhängigkeiten transparent machen, also wissen, welche Systeme, Anwendungen und Prozesse welche kryptografischen Verfahren nutzen und voraussetzen.
2. Kritische Daten und Prozesse priorisieren
3. Eine mehrjährige Migrations-Roadmap etablieren
4. Technologische Abhängigkeiten und Souveränität prüfen
5. Den Ernstfall vorbereiten und testen

Neben der Prävention, dem permanenten Monitoring und der konsequenten Schließung von Schwachstellen muss die Vorbereitung auf Worst-Case-Szenarien Teil des Projekts sein. Business Continuity Management (BCM) und Krisenstäbe müssen extrem schnelle Reaktionen trainieren. Dazu gehört auch das Entwerfen und Testen eines Minimalbetriebs, der die Überlebensfähigkeit des Unternehmens aus einer gesicherten Umgebung heraus garantiert.

Fazit: Quantenresilienz erfordert eine breit angelegte Strategie

Vorausschauendes Management von Banken und Versicherungen bedeutet im Post-Quantum-Zeitalter mehr als die planvolle Transformation der Sicherheitsarchitektur. Vorstände müssen Quantenresilienz als unternehmensweite Aufgabe verstehen: mit klaren Prioritäten, belastbaren Ressourcen, technischer Flexibilität, überprüften Abhängigkeiten sowie einer Betriebs- und Krisenvorsorge, die auch unter neuen Bedrohungsbedingungen funktioniert.

Quellenangaben:

¹ Wikipedia – CrowdStrike-Computerausfall 2024, Link: https://de.wikipedia.org/wiki/CrowdStrike-Computerausfall_2024

² FCA – CrowdStrike outage: lessons for operational resilience, 31.12.2024 – Link: <https://www.fca.org.uk/firms/operational-resilience/crowdstrike-outage-lessons-operational-resilience>

³ HNDL: Harvest Now, Decrypt Later (Jetzt ernten, später entschlüsseln)

⁴ World Economic Forum: Global Cyber Security Outlook 2025, Link: https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf

⁵ BSI: Bundesamt für Sicherheit in der Informationstechnik – „Quantentechnologien und quantensichere Kryptographie“ Link: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Quantentechnologien-und-Post-Quanten-Kryptografie/quantentechnologien-und-quantensichere-kryptografie_node.html

Der Autor



Michael Ehrnsperger leitet seit 2023 den Bereich Group Protection & Resilience sowie den Konzern-Krisenstab der Allianz Gruppe. Er verantwortet global die Themen Unternehmenssicherheit, Security Operations Center, Business Continuity, Vorfalls- und Krisenmanagement sowie Bedrohungsanalyse.