



Standpunkt

Der Weg zur
quanten-
sicheren IT

CGI

Quantenrisiken frühzeitig verstehen

Leistungsfähige Quantencomputer werden derzeit noch vor allem in der Forschung und Entwicklung eingesetzt. Trotzdem gibt es bereits Risiken: Verschlüsselte Daten können gespeichert und zu einem späteren Zeitpunkt entschlüsselt werden – eine Vorgehensweise, die man als „Harvest now, decrypt later“ bezeichnet.

Der langfristige Schutz digitaler Kommunikation, Identitäten und sensibler Unternehmensdaten wird daher immer dringender.

Mit dem CGI Quantum Risk Assessment helfen wir Unternehmen, kryptografische Abhängigkeiten sichtbar zu machen, Gefährdungspotenziale zu bewerten und den Übergang zur quantensicheren IT einzuleiten.

Quantum Readiness beginnt jetzt

Bereits heute müssen Unternehmen entscheiden, welche Systeme, Prozesse und Daten es langfristig zu schützen gilt und welche Anforderungen sich daraus für die Kryptografie ergeben.

Unser Standpunkt erklärt die Hintergründe der Quantenbedrohung, zeigt die Auswirkungen auf bestehende Sicherheitsarchitekturen und beschreibt, wie ein strukturierter Transformationsansatz Unternehmen bei der Umstellung auf quantensichere Verfahren hilft.

Abschließend veranschaulicht ein Fallbeispiel aus dem Hafen Rotterdam, wie sich Quantum Readiness in der Praxis umsetzen lässt.



Von der Technologie zur Transformation

Immer mehr Organisationen beschäftigen sich mit der Frage, welche Auswirkungen zukünftige Quantenangriffe auf ihre Systeme, Daten und Geschäftsprozesse haben könnten.

Im Fokus stehen dabei die kryptografischen Verfahren, die seit vielen Jahren die Grundlage einer sicheren digitalen Kommunikation bilden. Mit der Post-Quanten-Kryptografie (Post-Quantum Cryptography, PQC) stehen bereits geeignete Ansätze zur Verfügung, um die bestehenden Sicherheitsarchitekturen schrittweise auf die Zukunft vorzubereiten. In ausgewählten Anwendungsfällen können spezialisierte Technologien wie Quantum Key Distribution (QKD) zusätzliche Anforderungen erfüllen.

Die Herausforderung besteht jedoch selten in der Technologie selbst. Die Unternehmen müssen verstehen, welche Systeme betroffen sind und wie sich eine sinnvolle Transformationsstrategie entwickeln lässt.

Die folgenden Abschnitte zeigen, warum Unternehmen möglichst schnell handeln sollten und wie ein strukturierter Ansatz dabei helfen kann, Risiken frühzeitig zu erkennen und gezielt zu reduzieren.

PQC wird zum Standard

In den vergangenen Jahren hat sich die Entwicklung von Quantencomputing deutlich beschleunigt. Gleichzeitig beschäftigen sich Technologieunternehmen, Forschungseinrichtungen und Standardisierungsgremien zunehmend mit der Umstellung auf quantensichere Kryptografie und veröffentlichen entsprechende Roadmaps und Handlungsempfehlungen.

Mit der Veröffentlichung der ersten Standards für PQC im Jahr 2024 hat das US-amerikanische National Institute of Standards and Technology (NIST) einen wichtigen Schritt vollzogen. Auch Organisationen wie die European Union Agency for Cybersecurity (ENISA) und das Bundesamt für Sicherheit in der Informationstechnik (BSI) empfehlen Unternehmen, die Umstellung auf quantensichere kryptografische Verfahren vorzubereiten.

Die zunehmende Standardisierung und die Empfehlungen führender Sicherheitsbehörden zeigen klar, dass die Vorbereitung auf quantensichere Kryptografie längst über den Bereich der Forschung hinausgeht und zu einer strategischen Aufgabe für Unternehmen und öffentliche Organisationen geworden ist.



Der Q-Day und seine Bedeutung für Unternehmen

Weltweit investieren Staaten und Technologieunternehmen erhebliche Mittel in die Entwicklung von Quantencomputern. Neben den wirtschaftlichen Chancen, die sich damit verbinden, spielen strategische Aspekte wie die nationale Sicherheit, die technologische Souveränität und die Informationsgewinnung eine große Rolle.

Durch die intensive Beschäftigung mit der Materie rückt auch der sogenannte Q-Day näher. Dieser bezeichnet den Moment, an dem leistungsfähige Quantencomputer weit verbreitete Verfahren wie RSA oder Elliptic Curve Cryptography (ECC) in praktikabler Zeit überwinden können. Auch wenn Wissenschaftlerinnen und Wissenschaftler über das wahrscheinliche Datum des Q-Days weiterhin diskutieren, ist eines sicher: Die verbleibende Vorbereitungszeit wird immer kürzer.

Welche Bedeutung der Q-Day für eine bestimmte Branche hat, hängt davon ab, welche Rolle Kryptografie in den jeweiligen Geschäftsprozessen spielt. Im Finanzsektor bildet sie die Grundlage für sichere Transaktionen und digitale Identitäten. Betreiber kritischer Infrastrukturen schützen damit ihre Kommunikations- und Steuerungssysteme. Im Verteidigungs- und Sicherheitsumfeld müssen Informationen häufig über sehr lange Zeiträume vertraulich bleiben.

Für Unternehmen dieser und anderer Branchen stellt sich daher nicht mehr die Frage, ob sie sich mit PQC beschäftigen sollten, sondern wann und mit welcher Priorität sie die Vorbereitung beginnen.



„Harvest now, decrypt later“ – ein aktuelles Risiko

Viele Unternehmen verbinden die Quantenbedrohung vor allem mit dem Q-Day. Tatsächlich beginnt die Gefahr jedoch deutlich früher.

Schon heute werden weltweit verschlüsselte Daten gesammelt und gespeichert – mit dem Ziel, sie zu einem späteren Zeitpunkt zu entschlüsseln. Dieses Szenario wird als „Harvest now, decrypt later“ bezeichnet. Angreifer müssen die Daten dabei gar nicht sofort lesen können. Es genügt, sie heute zu stehlen und auf zukünftige technologische Entwicklungen zu warten.

Besonders kritisch ist dies für Informationen mit langfristigem Schutzbedarf. Dazu zählen beispielsweise Forschungs- und Entwicklungsdaten, Konstruktionspläne, geistiges Eigentum, Finanzinformationen oder sensible Kundendaten. Viele dieser Informationen behalten über Jahre oder sogar Jahrzehnte hinweg ihren Wert. Werden sie künftig entschlüsselt, können erhebliche wirtschaftliche Schäden, strategische Nachteile oder regulatorische Konsequenzen entstehen.

Bestehende Systeme erschweren die Transformation

Die Herausforderung beschränkt sich aber nicht auf Daten und neu entwickelte Systeme: Die Anwendungen, industrielle Steuerungen, Geräte und Kommunikationsplattformen werden oft deutlich länger betrieben als ursprünglich geplant. Die darin verwendeten kryptografischen Verfahren wurden jedoch zu einer Zeit implementiert, in der Quantencomputing noch kein praktisches Risiko darstellte. Für Unternehmen bedeutet dies, dass sie nicht nur zukünftige Systeme schützen müssen. Es gilt auch, bestehende kryptografische Abhängigkeiten frühzeitig zu erkennen und zu bewerten.

Doch je komplexer die IT-Landschaft ist, desto schwieriger wird es, die betroffenen Systeme, Datenflüsse und eingesetzten kryptografischen Verfahren vollständig zu erfassen. Umso wichtiger ist eine strukturierte Analyse, die die Risiken sichtbar macht und die Bereiche identifiziert, die langfristig geschützt werden müssen.

Die Bedeutung von Kryptografie für die Vertrauensbildung

Die Auswirkungen der Quantenbedrohung gehen weit über den Verlust einzelner vertraulicher Informationen hinaus. Auf Kryptografie basieren heute nahezu alle digitalen Geschäftsprozesse. Sie schützt die Kommunikation, bestätigt Identitäten, sichert Software-Updates und ermöglicht vertrauenswürdige Interaktionen zwischen Systemen, Anwendungen und Benutzerinnen bzw. Benutzern.

	Verbindungen			unsicher	
	Identitäten			nicht vertrauenswürdig	
	Software- und Firmware-Updates			manipulierbar	
	Systeme			nicht verifizierbar	

Verlieren etablierte kryptografische Verfahren ihre Schutzwirkung, gefährdet dies nicht nur die Vertraulichkeit der Daten. Auch die zentralen Mechanismen, die die Vertrauenswürdigkeit der digitalen Prozesse absichern, geraten unter Druck: Digitale Zertifikate verlieren ihre Aussagekraft, sichere Verbindungen lassen sich nicht mehr zuverlässig aufbauen und die Herkunft von Software- oder Firmware-Updates kann nicht mehr zweifelsfrei überprüft werden.

Besonders kritisch ist dabei, dass viele Systeme weiterhin scheinbar normal funktionieren. Die Anwendungen bleiben verfügbar, die Prozesse laufen weiter und über die Schnittstellen wird wie gewohnt kommuniziert. Gleichzeitig kann jedoch das Vertrauen in die zugrunde liegenden Mechanismen für Authentifizierung und Integrität schrittweise verloren gehen.

Für Unternehmen bedeutet dies, dass die Herausforderung nicht auf einzelne Anwendungen oder Infrastrukturbereiche begrenzt ist. Die zentrale Frage lautet, welche geschäftskritischen Prozesse und digitalen Abhängigkeiten auf kryptografischen Verfahren beruhen, die künftig ersetzt werden müssen.

Um diese Frage fundiert beantworten zu können, benötigen Unternehmen einen guten Überblick über ihre kryptografischen Abhängigkeiten, Zertifikatsstrukturen, Kommunikationswege und Vertrauensketten. Erst eine gründliche Untersuchung zeigt, welche Bereiche besonders betroffen sind und welche Prioritäten sich daraus ergeben.

Wie Verschlüsselung heute funktioniert

Um die Quantenbedrohung richtig einordnen zu können, lohnt sich ein Blick auf die Funktionsweise moderner verschlüsselter Kommunikation. Heute basiert ein Großteil des Austauschs digitaler Informationen auf dem Zusammenspiel mehrerer kryptografischer Verfahren.



Abbildung 1: Grundprinzip heutiger sicherer Kommunikation: Advanced Encryption Standard (AES) schützt die Daten, RSA/ECC den Schlüsselaustausch innerhalb des TLS-Prozesses.

Bei einer typischen TLS-gesicherten Verbindung übernimmt TLS die Organisation des gesamten sicheren Kommunikationsprozesses zwischen Sender und Empfänger. Die eigentlichen Daten werden dabei durch das symmetrische Verschlüsselungsverfahren AES geschützt. AES gilt als äußerst leistungsfähig und wird voraussichtlich auch in der zukünftigen Quantenwelt eine wichtige Rolle spielen.

Wo Quantencomputer kryptografische Verfahren angreifen

Das Problem ist nicht die Datenverschlüsselung selbst. Damit beide Kommunikationspartner sicher denselben AES-Schlüssel verwenden können, kommen heute häufig klassische Public-Key-Verfahren wie RSA oder ECC zum Einsatz. Sie ermöglichen den sicheren Schlüsselaustausch und die Authentifizierung der Kommunikationspartner – und genau hier liegt das Risiko.

Leistungsfähige Quantencomputer könnten künftig Algorithmen wie RSA und ECC mit Verfahren wie dem Shor-Algorithmus angreifen. Wird der Schlüsselaustausch kompromittiert, sind Angreifer in der Lage, nachträglich auf geschützte Kommunikationsinhalte zuzugreifen, obwohl die eigentliche Datenverschlüsselung durch AES weiterhin stark ist.

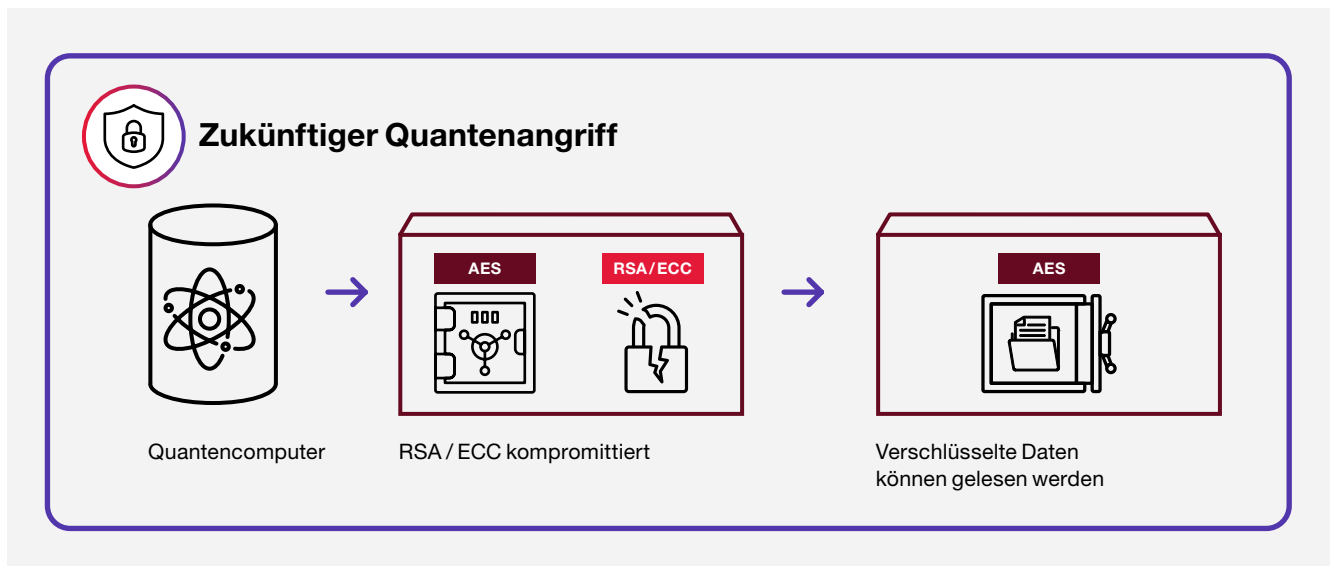


Abbildung 2: Das „Harvest now, decrypt later“-Szenario: Angreifer speichern verschlüsselte Daten bereits heute und nutzen zukünftige Quantencomputer, um die zugrunde liegenden Schlüsselmechanismen zu kompromittieren und die Daten später zu entschlüsseln.

Der Weg zur quantensicheren Kommunikation

Für eine quantensichere Kommunikation müssen Unternehmen ihre bestehende Sicherheitsarchitektur nicht vollständig neu aufbauen. Viele bewährte Komponenten moderner Kommunikationssysteme bleiben auch in der Post-Quantum-Ära erhalten. Der entscheidende Wandel findet vor allem dort statt, wo heute kryptografische Schlüssel ausgetauscht werden.

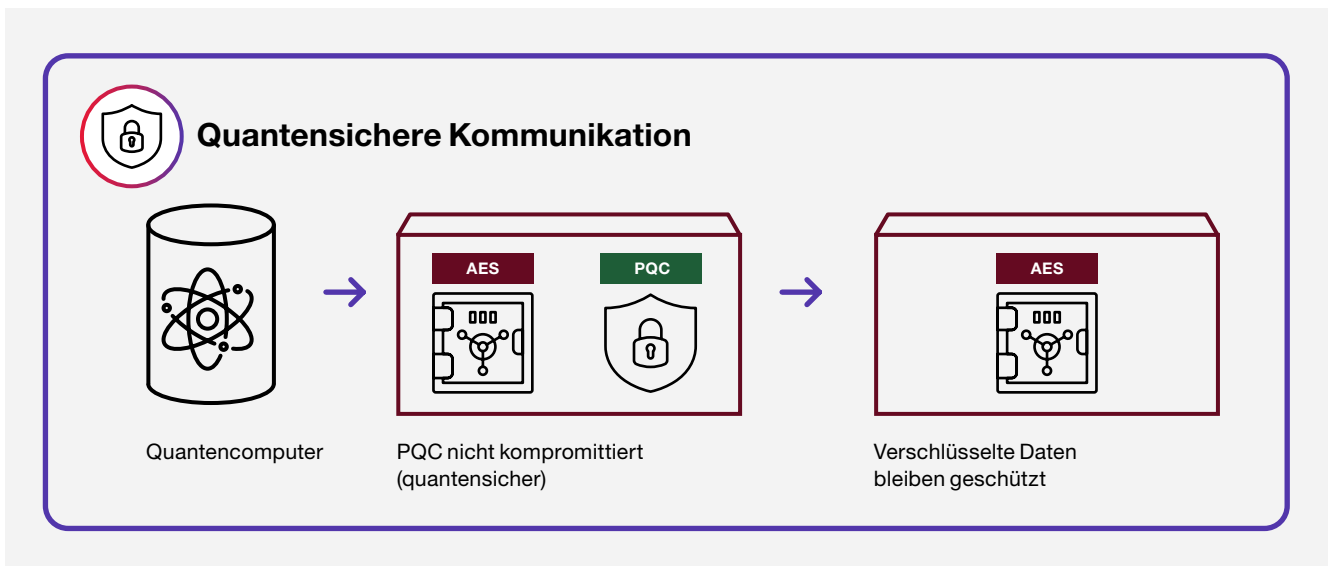


Abbildung 3: PQC verhindert „Harvest-now-decrypt-later“-Angriffe und schützt die Vertraulichkeit von Daten auch gegenüber Quantencomputern.

Auch zukünftig schützt AES die Daten innerhalb einer verschlüsselten Verbindung. Das Verfahren gilt weiterhin als leistungsfähig und bildet nach wie vor die Grundlage moderner Datenverschlüsselung. Auch Protokolle wie TLS bleiben erhalten und sichern weiterhin die Kommunikation zwischen Sendern und Empfängern.

Der wesentliche Unterschied besteht darin, dass klassische Public-Key-Verfahren wie RSA oder ECC durch PQC ersetzt werden. Die neuen Verfahren sind speziell darauf ausgelegt, auch Angriffen durch Quantencomputer standzuhalten.

Damit verändert sich nicht die eigentliche Datenverschlüsselung, sondern vor allem der Mechanismus, mit dem kryptografische Schlüssel ausgetauscht und digitale Identitäten abgesichert werden.

QKD ergänzt PQC in ausgewählten Anwendungsfällen

Bei besonders hohen Sicherheitsanforderungen kann PQC optional durch Quantum Key Distribution (QKD) ergänzt werden. Während PQC auf neuen mathematischen Verfahren basiert, nutzt QKD physikalische Eigenschaften der Quantenmechanik, um Manipulations- oder Abhörversuche während der Schlüsselverteilung aufzudecken.

QKD ersetzt weder AES noch TLS. Die Technologie stellt eine zusätzliche Sicherheitsschicht dar, die besonders in ausgewählten Hochsicherheitsumgebungen eingesetzt werden kann.

Wird während der Schlüsselverteilung ein Abhörversuch erkannt, kann der betroffene Schlüssel verworfen und die Kommunikation unterbrochen werden, bevor vertrauliche Informationen übertragen werden.

Für Unternehmen ergibt sich daraus ein klarer Migrationspfad: Bestehende Kommunikationsarchitekturen können schrittweise um quantensichere Schlüsselmechanismen erweitert werden, ohne dass sie bewährte Sicherheitskomponenten vollständig ersetzen.



Vom Risiko zur Roadmap: das CGI Quantum Risk Assessment

Die meisten Unternehmen haben die Relevanz von Quantencomputing und PQC bereits erkannt. Doch für viele stellt sich die Frage, welche konkreten Maßnahmen erforderlich sind und wo der Einstieg in die Transformation erfolgen sollte.

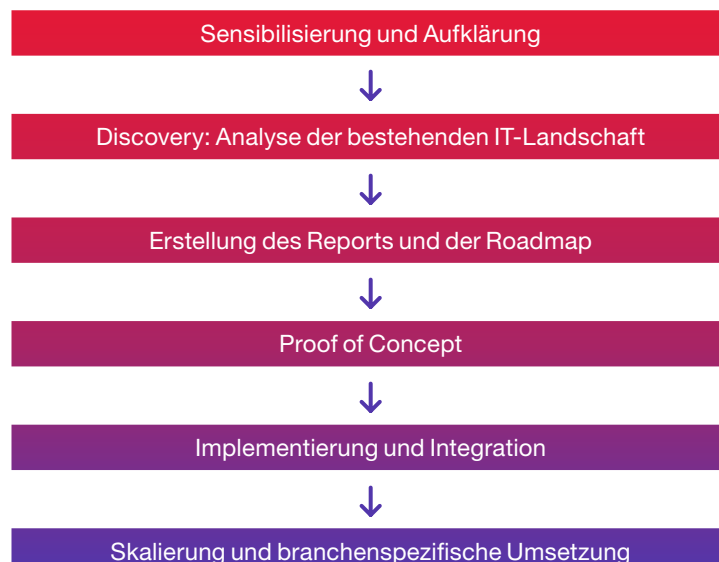
Mit unserem CGI Quantum Risk Assessment unterstützen wir Unternehmen, ihre Ausgangssituation systematisch zu bewerten und einen strukturierten Übergang zur quantensicheren IT zu gestalten.

Gemeinsam klären wir entscheidende Fragen:

- Welche Systeme und Prozesse sind von kryptografischen Verfahren abhängig?
- Welche Daten müssen auch in zehn, fünfzehn oder zwanzig Jahren noch geschützt sein?
- Wo bestehen bereits heute kritische Abhängigkeiten von RSA, ECC oder anderen klassischen Verfahren?
- Welche Geschäftsrisiken ergeben sich daraus?
- Wie gut ist die Organisation auf eine zukünftige Migration vorbereitet?

Gemeinsam analysieren wir kryptografische Abhängigkeiten, bewerten Risiken und untersuchen die geschäftlichen Auswirkungen – immer ausgehend vom individuellen Status quo und den strategischen Zielen der Unternehmen.

Auf dieser Grundlage geben wir dann konkrete Handlungsempfehlungen und erstellen eine Roadmap mit priorisierten Maßnahmen.



Quantum Readiness in der Praxis: der Hafen Rotterdam

Der Hafen Rotterdam zeigt, wie Unternehmen bereits heute konkrete Schritte in Richtung Quantensicherheit gehen können. Gemeinsam mit unserem niederländischen Team und der internationalen CGI Quantum Community haben wir das CGI Quantum Risk Assessment durchgeführt, um die Auswirkungen zukünftiger Quantenangriffe auf die bestehenden Systeme und Prozesse zu bewerten.

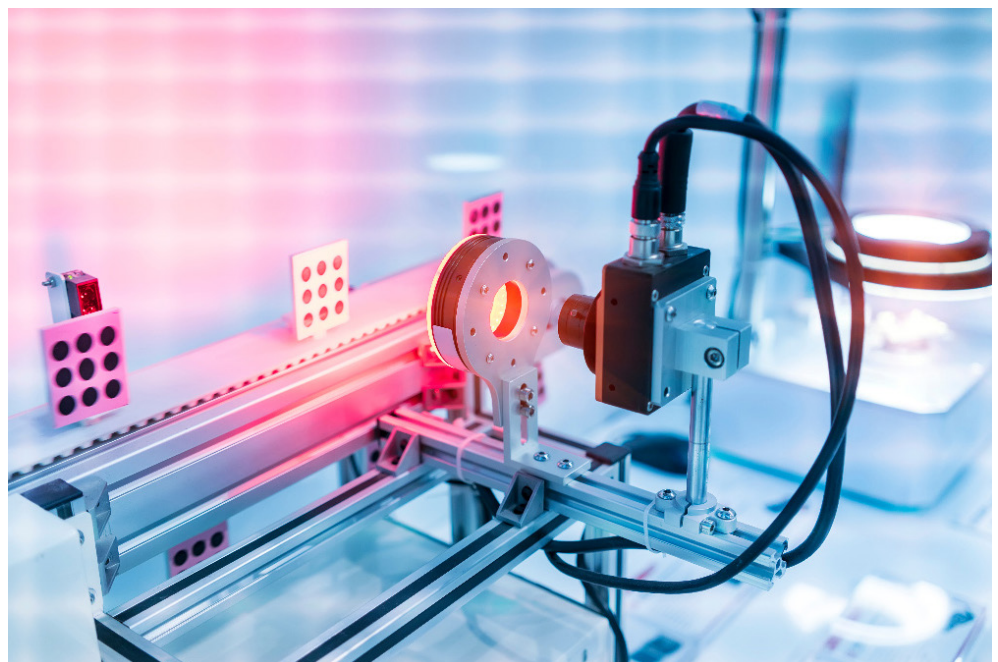
Im Mittelpunkt stand die Analyse der vorhandenen kryptografischen Landschaft. Dabei wurden die kryptografischen Verfahren bewertet, die potenziellen Risiken durch „Harvest now, decrypt later“-Szenarien identifiziert und die Einsatzmöglichkeiten von PQC und QKD untersucht.

Vom Assessment zur Umsetzung

Unser Assessment machte kryptografische Abhängigkeiten sichtbar, half bei der Priorisierung potenzieller Migrationsbedarfe und ermöglichte die Bewertung verschiedener Technologieoptionen im Kontext der bestehenden Infrastruktur. Auf dieser Basis konnte eine Transformationsstrategie entwickelt werden, die sowohl kurzfristige als auch langfristige Maßnahmen umfasst.

Die daraus abgeleiteten Handlungsempfehlungen dienten nicht nur als strategische Orientierung. Ausgewählte Maßnahmen wurden bereits umgesetzt und bilden die Grundlage für die schrittweise Weiterentwicklung der Sicherheitsarchitektur.

Das Projekt zeigt, dass Unternehmen bereits heute die Voraussetzungen schaffen können, um ihre Systeme kontrolliert auf eine quantensichere Zukunft vorzubereiten.



Die richtigen Fragen für die Zukunft stellen

Quantencomputing ist zu einer strategischen Herausforderung für die IT-Sicherheit geworden. Unternehmen müssen heute noch nicht alle Antworten kennen. Entscheidend ist aber, schon die richtigen Fragen zu stellen.

Besonders Systeme mit langen Lebenszyklen, geschäftskritische Anwendungen und Daten mit langfristigem Schutzbedarf sollten frühzeitig betrachtet werden. Je besser Unternehmen ihre kryptografischen Abhängigkeiten verstehen, desto gezielter können sie zukünftige Maßnahmen planen.

Quantum Readiness beginnt nicht mit dem Q-Day, sondern jetzt – mit konkreten Schritten in Richtung einer quantensicheren IT.



Über CGI

Insights you can act on

Wir sind ein globales Dienstleistungsunternehmen für IT- und Geschäftsprozesse mit insgesamt 94.000 Mitarbeitenden. An 400 Standorten bieten wir für mehr als 20 Branchen ganzheitliche, skalierbare und nachhaltige Services, durch die unsere Kunden greifbare Ergebnisse erzielen; unser Portfolio umfasst IT- und Business-Beratung, Systemintegration, Managed IT, Business Process Services und Intellectual Property auf Topniveau. Ein Schwerpunkt unserer strategischen Beratung liegt in der Verbesserung der geschäftlichen Agilität und des Change Managements; unsere IP-basierten Lösungen dienen einer beschleunigten Innovation und nutzen dazu Verfahren wie KI.

Mehr Informationen erhalten Sie auf
www.cgi.com/de oder info.de@cgi.com

