

Holger Reibold

Q-Day im Anflug

Warum Post-Quantum-Readiness
zur strategischen Pflicht wird –
und wie Unternehmen jetzt
handeln müssen

BRAIN-MEDIA.DE

Alle Rechte vorbehalten. Ohne ausdrückliche, schriftliche Genehmigung des Verlags ist es nicht gestattet, das Buch oder Teile daraus in irgendeiner Form durch Fotokopien oder ein anderes Verfahren zu vervielfältigen oder zu verbreiten. Dasselbe gilt auch für das Recht der öffentlichen Wiedergabe. Der Verlag macht darauf aufmerksam, dass die genannten Firmen- und Markennamen sowie Produktbezeichnungen in der Regel marken-, patent- oder warenrechtlichem Schutz unterliegen.

Verlag und Autor übernehmen keine Gewähr für die Funktionsfähigkeit beschriebener Verfahren und Standards.

© 2026 Brain-Media.de

ISBN: 978-3-95444-349-9

Cover: Freepik

Brain-Media.de

Dr. Holger Reibold – Huber-Müller-Str. 52c – 66113 Saarbrücken

info@brain-media.de – www.brain-media.de

Inhaltsverzeichnis

Inhaltsverzeichnis	I
Vorwort	1
1 Q-Day – Mythos, Realität und Zeitachse	5
1.1 Definition Q-Day und Abgrenzung	6
1.2 Stand der Technologie	8
1.3 Bedrohungsmodell	12
1.4 Zeitachsen und Szenarien	15
1.5 Komplexitätsbruch.....	17
1.6 Management Summary	21
2 Grundlagen der Quantenbedrohung.....	23
2.1 Quantenmechanische Prinzipien.....	24
2.2 Shor- und Grover-Algorithmus im Kontext.....	27
2.3 Angriffsszenarien auf heutige Kryptografie	30
2.4 Branchenabhängige Risikoexposition	33
2.5 Nationale Sicherheit und KRITIS	35
2.6 Management Summary	37

3	Post-Quantum-Kryptografie	39
3.1	Zielbild und Definition PQC.....	40
3.2	Algorithmusklassen	43
3.3	Standardisierung durch NIST	45
3.4	Auswahlkriterien	48
3.5	Aktuelle Standards und Roadmaps.....	50
3.6	Management Summary	53
4	Krypto-Agilität als Schlüsselkompetenz.....	55
4.1	Definition und strategische Bedeutung	56
4.2	Architekturprinzipien	58
4.3	Herausforderungen in Legacy-Systemen	61
4.4	Hybrid-Ansätze	63
4.5	Governance-Modelle	66
4.6	Management Summary	69
5	Post-Quantum-Readiness	71
5.1	Reifegradmodelle und Assessments	72
5.2	Crypto Inventory: Transparenz schaffen.....	75
5.3	Risikoanalyse und Priorisierung	77
5.4	Roadmap zur PQC-Transformation	79
5.5	Budgetierung und Ressourcenplanung	81
5.6	Ressourcenkonkurrenz	84

5.7	Management Summary	87
6	Technische Umsetzung und Migration	89
6.1	Integration in bestehende Systeme	90
6.2	Anpassung zentraler Protokolle.....	92
6.3	Teststrategien und Pilotierung	95
6.4	Performance- und Skalierungsaspekte	98
6.5	Hardware- und Infrastruktur-Risiken	100
6.6	Interoperabilität und Legacy-Systeme	104
6.7	Management Summary	106
7	Regulierung, Standards & Supply Chain	107
7.1	Globale Regulierungslandschaft	108
7.2	Anforderungen von Behörden & Aufsicht.....	111
7.3	Branchenstandards.....	113
7.4	Auditierbarkeit und Zertifizierung	115
7.5	Datenschutz und rechtliche Aspekte	117
7.6	Supply Chain und Anbietersteuerung	119
7.7	Management Summary	122
8	Zukunftsperspektiven.....	123
8.1	Markt- und Technologieentwicklung	124
8.2	Wettbewerbsvorteile durch frühe Adoption.....	125
8.3	Risiken verspäteter Migration.....	128

8.4	Ökosysteme und Partnerschaften	130
8.5	Change Management	133
8.6	Handlungsempfehlungen für Entscheider.....	135
8.7	Management Summary	137
	Zum Schluss	139
	Anhang.....	V
	PQC-Scorecard.....	VI
	PQC Maturity Levels.....	XII
	Weitere Downloads.....	XVII
	Glossar	XIX
	Abkürzungsverzeichnis.....	XXI
	Literatur- und Quellenverzeichnis	XXIII
	Stichwortverzeichnis	XXV
	Mehr von Brain-Media.de	XXIX

Vorwort

Warum die Quantenbedrohung heute schon relevant ist

Der „Q-Day“ ist kein klar datierbares Ereignis. Er ist kein Stichtag, der im Kalender markiert werden kann, kein Moment, an dem die Welt abrupt von „sicher“ auf „unsicher“ kippt. Und doch ist er real. Der Q-Day beschreibt den Zeitpunkt, an dem Quantencomputer in der Lage sein werden, die heute eingesetzten kryptografischen Verfahren effektiv zu brechen – insbesondere jene, auf denen nahezu die gesamte digitale Vertrauensinfrastruktur basiert.

Diese Infrastruktur ist allgegenwärtig. Sie schützt Kommunikationskanäle, sichert Finanztransaktionen, gewährleistet die Integrität von Software und bildet das Fundament moderner Identitäts- und Zugriffssysteme. Verfahren wie RSA und elliptische Kurvenkryptografie gelten seit Jahrzehnten als verlässlich – jedoch unter der Annahme klassischer Rechenmodelle. Genau diese Annahme wird durch das Quantencomputing infrage gestellt.

Die Herausforderung liegt nicht allein in der technologischen Entwicklung, sondern in ihrer zeitlichen Unschärfe. Niemand kann mit Sicherheit sagen, wann leistungsfähige Quantencomputer verfügbar sein werden. Gleichzeitig existiert bereits heute ein reales

Bedrohungsszenario: „Harvest now, decrypt later“. Angreifer sammeln verschlüsselte Daten mit langfristigem Wert – in der Erwartung, diese zu einem späteren Zeitpunkt entschlüsseln zu können. Damit wird die Bedrohung in die Gegenwart verlagert.

Vor diesem Hintergrund stellt sich eine strategische Frage: Wann beginnt Handlungsdruck? Die klare Antwort lautet: jetzt.

Gleichzeitig stehen Organisationen unter massivem Transformationsdruck durch andere Technologien – insbesondere im Bereich der Künstlichen Intelligenz. Große Teile der verfügbaren Budgets und Ressourcen fließen aktuell in Generative AI, Datenplattformen und Automatisierung. Diese Entwicklung ist nachvollziehbar und wirtschaftlich sinnvoll. Doch sie erzeugt einen blinden Fleck.

Denn genau die Datenbestände, die heute für KI-Systeme aufgebaut, kuratiert und monetarisiert werden, sind langfristig nur dann wertvoll, wenn ihre Vertraulichkeit und Integrität auch in einer Post-Quantum-Welt gewährleistet ist. Ohne geeignete kryptografische Schutzmechanismen droht ein paradoxes Szenario: Unternehmen investieren heute massiv in datengetriebene Geschäftsmodelle – und riskieren gleichzeitig, dass diese Daten in wenigen Jahren kompromittiert werden können.

Post-Quantum-Readiness ist daher kein isoliertes IT-Thema. Sie ist eine strategische Absicherung bestehender und zukünftiger Geschäftsmodelle. Sie ist die Versicherungsschicht unterhalb von Digitalisierung, Cloud-Transformation und Künstlicher Intelligenz.

Dieses Buch verfolgt ein klares Ziel: Es übersetzt ein hochkomplexes, technisch geprägtes Thema in eine strukturierte Entscheidungsgrundlage für Unternehmen und Organisationen. Es richtet sich bewusst nicht nur an Kryptografie-Experten, sondern insbesondere an Entscheider – an C-Level, IT-Leitung, Sicherheitsverantwortliche und Governance-Funktionen.

Der Aufbau folgt dabei einer klaren Logik. Zunächst wird die Bedrohung eingeordnet: Was ist der Q-Day, und warum ist er relevant? Anschließend werden die technologischen Grundlagen und die Ansätze der Post-Quantum-Kryptografie erläutert. Darauf aufbauend rückt die organisatorische Umsetzung in den Fokus: Krypto-Agilität, Migrationsstrategien, Budgetierung und Governance. Ergänzt wird dies durch regulatorische Perspektiven sowie die zunehmende Bedeutung der Lieferkette – insbesondere im Kontext von Cloud- und Software-Anbietern.

Ein besonderer Schwerpunkt liegt auf der praktischen Umsetzbarkeit. Post-Quantum-Readiness ist kein kurzfristiges Projekt, sondern ein Transformationsprogramm mit einem Zeithorizont von fünf bis zehn Jahren. Entsprechend werden neben technischen Aspekten auch organisatorische und psychologische Faktoren adressiert – etwa die Herausforderung, über Jahre hinweg Priorität, Budget und Aufmerksamkeit für ein Thema aufrechtzuerhalten, dessen Eintrittszeitpunkt nicht exakt bestimmbar ist.

Der Anhang dieses Buches ist bewusst als Werkzeugkasten konzipiert. Er enthält konkrete Hilfsmittel, Checklisten und

Bewertungsmodelle, die Organisationen dabei unterstützen, ihren eigenen Reifegrad zu bestimmen und nächste Schritte abzuleiten.

Dieses Buch versteht sich nicht als abschließende Antwort, sondern als strukturierte Orientierung in einem sich dynamisch entwickelnden Feld. Die Technologien werden sich weiterentwickeln, Standards werden angepasst, und Prognosen werden sich verschieben. Der Handlungsdruck jedoch bleibt bestehen.

Der Q-Day kommt nicht plötzlich. Aber er rückt näher.

Herzlichst

Holger Reibold

1 Q-Day – Mythos, Realität und Zeitachse

Der Angriff beginnt, bevor jemand ihn bemerkt

Der Begriff „Q-Day“ beschreibt einen potenziellen Wendepunkt in der IT-Sicherheit: den Moment, ab dem Quantencomputer in der Lage sind, heute eingesetzte kryptografische Verfahren effizient zu brechen. Trotz seiner häufigen Darstellung als singuläres Ereignis handelt es sich jedoch weniger um einen klar definierten Zeitpunkt als vielmehr um eine Entwicklungsschwelle. Zwischen theoretischer Möglichkeit und praktischer Angreifbarkeit liegt eine Phase technologischer Reifung, die schwer exakt zu terminieren ist.

Aktuelle Fortschritte im Quantencomputing – unter anderem durch Unternehmen wie IBM und Google – zeigen, dass sich die Forschung zunehmend in Richtung skalierbarer Systeme bewegt. Gleichzeitig existiert bereits heute ein relevantes Bedrohungsmodell: Angreifer sammeln verschlüsselte Daten mit langfristigem Wert, um diese zu einem späteren Zeitpunkt zu entschlüsseln („Harvest now, decrypt later“).

Damit verschiebt sich der Q-Day konzeptionell in die Gegenwart. Die eigentliche Herausforderung liegt nicht nur im möglichen Bruch etablierter Verfahren wie RSA oder ECC, sondern im fundamentalen Komplexitätsbruch, den Quantenalgorithmen ermöglichen. Dieses Kapitel

ordnet den Q-Day zwischen Hype und Realität ein, analysiert technologische Fortschritte und entwickelt belastbare Szenarien für Entscheidungsträger.

1.1 Definition Q-Day und Abgrenzung

Der Begriff „Q-Day“ wird häufig verkürzt und teilweise missverständlich verwendet. In seiner präzisesten Form beschreibt er den Zeitpunkt, ab dem ein ausreichend leistungsfähiger Quantencomputer in der Lage ist, heute weit verbreitete asymmetrische Kryptografieverfahren – insbesondere RSA und elliptische Kurvenkryptografie (Elliptic Curve Cryptography, ECC) – praktisch zu brechen. „Praktisch“ bedeutet in diesem Kontext: innerhalb eines Zeitrahmens und mit Ressourcen, die für staatliche oder wirtschaftlich motivierte Angreifer realistisch sind.

Wichtig ist dabei die klare Abgrenzung zu einem rein theoretischen Bruch. Die zugrunde liegenden Algorithmen, insbesondere der Shor-Algorithmus, sind seit den 1990er-Jahren bekannt. Ihre Existenz allein definiert jedoch keinen Q-Day. Erst die Kombination aus algorithmischer Reife, ausreichend vielen stabilen Qubits, niedrigen Fehleraten und skalierbarer Fehlerkorrektur führt zu einem Zustand, in dem kryptografische Verfahren tatsächlich angreifbar werden.

Der Q-Day ist daher kein binärer Schalter, sondern eine operative Schwelle. Er markiert den Übergang von „kryptografisch sicher“ zu „kryptografisch verwundbar“ unter realen Bedingungen. Diese

Schwelle kann je nach Anwendungsfall unterschiedlich verlaufen. Hochsensible Daten mit langen Schutzfristen – etwa im Bereich staatlicher Kommunikation, geistigen Eigentums oder Gesundheitsdaten – sind bereits dann betroffen, wenn ein zukünftiger Bruch plausibel erscheint. Für kurzlebige Daten hingegen kann das Risiko deutlich später relevant werden.

Ein weiterer zentraler Aspekt ist die zeitliche Entkopplung von Angriff und Auswertung. Durch das Szenario „Harvest now, decrypt later“ verliert der Q-Day seinen Charakter als zukünftiges Ereignis. Daten, die heute verschlüsselt übertragen oder gespeichert werden, können bereits jetzt abgegriffen und archiviert werden. Der eigentliche Bruch erfolgt dann retrospektiv. In dieser Logik beginnt die Verwundbarkeit nicht erst mit der Verfügbarkeit leistungsfähiger Quantencomputer, sondern bereits mit der Existenz wertvoller, langfristig schützenswerter Daten.

Abzugrenzen ist der Q-Day zudem von verwandten Konzepten wie „Quantum Advantage“ oder „Quantum Supremacy“. Diese beschreiben den Punkt, an dem Quantencomputer bestimmte Aufgaben schneller lösen als klassische Systeme – jedoch nicht zwingend kryptografisch relevante Probleme. Ein System kann also bereits einen quantentechnischen Vorteil besitzen, ohne unmittelbar eine Bedrohung für bestehende Kryptografie darzustellen.

Ebenso ist der Q-Day nicht gleichbedeutend mit dem vollständigen Zusammenbruch aller Sicherheitsmechanismen. Symmetrische Verfahren wie AES gelten weiterhin als vergleichsweise robust,

wenngleich sie durch Grover-ähnliche Ansätze eine reduzierte effektive Sicherheit aufweisen. Der primäre Bruch betrifft die asymmetrischen Verfahren, die für Schlüsselaustausch, digitale Signaturen und Zertifikatsinfrastrukturen essenziell sind. Damit wird nicht die gesamte Kryptografie obsolet, wohl aber deren tragende Säulen.

Für Organisationen ergibt sich daraus eine entscheidende Implikation: Der Q-Day ist kein fernes, hypothetisches Ereignis, sondern ein strategischer Planungsparameter. Er definiert nicht nur einen zukünftigen Zustand, sondern wirkt bereits heute auf Entscheidungen in Architektur, Datenhaltung und Risikomanagement. Wer den Q-Day ausschließlich als zukünftigen Stichtag interpretiert, unterschätzt seine operative Relevanz.

1.2 Stand der Technologie

Die Entwicklung des Quantencomputings hat in den vergangenen Jahren einen deutlichen Übergang von theoretischer Forschung hin zu industriell getriebenen Innovationsprogrammen vollzogen. Insbesondere große Technologieunternehmen wie IBM und Google prägen aktuell die Roadmaps, investieren massiv in Hardware, Software und Ökosysteme und setzen damit den Takt für die gesamte Branche. Dennoch ist der aktuelle Stand der Technologie differenziert zu betrachten: Fortschritt ist sichtbar, Durchbruchsfähigkeit jedoch noch nicht erreicht.

Gegenwärtige Quantencomputer befinden sich im sogenannten NISQ-Zeitalter („Noisy Intermediate-Scale Quantum“). Diese Systeme verfügen über einige Dutzend bis wenige hundert physische Qubits, sind jedoch durch hohe Fehlerraten, begrenzte Kohärenzzeiten und starke Umwelteinflüsse eingeschränkt. Die Folge ist eine geringe Rechenstabilität, die komplexe, tief verschachtelte Algorithmen – wie sie für kryptografische Angriffe erforderlich wären – derzeit praktisch unmöglich macht.

IBM verfolgt eine klar strukturierte Skalierungsstrategie. Im Zentrum steht die kontinuierliche Erhöhung der Qubit-Anzahl bei gleichzeitiger Verbesserung der Konnektivität und Reduktion von Fehlern. Darüber hinaus setzt IBM stark auf Modularisierung: Künftig sollen mehrere Quantenprozessoren miteinander verbunden werden, um größere, logisch zusammenhängende Systeme zu schaffen. Parallel dazu baut das Unternehmen ein umfassendes Software-Ökosystem auf, das über Cloud-Plattformen zugänglich ist. Ziel ist es, Quantencomputing frühzeitig in reale Entwicklungs- und Testumgebungen zu integrieren und so eine Lernkurve bei Anwendern zu erzeugen.

Google verfolgt einen stärker auf Durchbrüche fokussierten Ansatz. Der viel beachtete Nachweis der „Quantum Supremacy“ markierte einen wichtigen Meilenstein: Ein speziell konstruiertes Problem wurde schneller gelöst als auf klassischen Supercomputern möglich. Auch wenn dieses Experiment keine direkte Relevanz für kryptografische Anwendungen hatte, demonstrierte es prinzipiell die Leistungsfähigkeit quantenbasierter Systeme. Der strategische Fokus von

Google liegt seitdem auf der Entwicklung fehlertoleranter Qubits und skalierbarer Fehlerkorrekturverfahren – beides zentrale Voraussetzungen für den Übergang von experimentellen Systemen zu praktisch einsetzbaren Maschinen.

Die größte technische Herausforderung besteht derzeit in genau dieser Fehlerkorrektur. Physische Qubits sind extrem störanfällig. Um stabile, sogenannte logische Qubits zu erzeugen, müssen viele physische Qubits redundant kombiniert werden. Schätzungen gehen davon aus, dass für einen einzigen logisch nutzbaren Qubit mehrere tausend physische Qubits erforderlich sein können. Für das Brechen kryptografisch relevanter Schlüssel – etwa im Kontext von RSA (Rivest–Shamir–Adleman) – wären somit nicht nur tausende, sondern potenziell Millionen physischer Qubits notwendig. Diese Größenordnung ist mit heutigen Systemen noch weit entfernt, bildet jedoch das zentrale Ziel der aktuellen Forschungs- und Entwicklungsprogramme.

Neben Hardware-Aspekten spielt auch die Software-Seite eine entscheidende Rolle. Die Entwicklung effizienter Quantenalgorithmen, die Optimierung von Laufzeiten sowie die Reduktion der benötigten Qubit-Tiefe sind aktive Forschungsfelder. Fortschritte in diesen Bereichen können den Hardwarebedarf signifikant beeinflussen und damit den Zeithorizont bis zu praktisch relevanten Angriffsszenarien verkürzen.

Ein weiterer Beschleunigungsfaktor ist die zunehmende Industrialisierung des Quantencomputings. Neben IBM und Google investieren

auch zahlreiche weitere Akteure – darunter Start-ups, Halbleiterhersteller und staatlich geförderte Forschungsprogramme – in unterschiedliche technologische Ansätze, etwa supraleitende Qubits, Ionenfallen oder photonische Systeme. Diese technologische Diversifizierung erhöht die Wahrscheinlichkeit von Durchbrüchen, macht Prognosen jedoch gleichzeitig komplexer.

Für Unternehmen entsteht daraus ein Spannungsfeld zwischen aktueller Realität und zukünftiger Disruption. Einerseits existiert heute noch keine Maschine, die etablierte kryptografische Verfahren praktisch gefährdet. Andererseits sind die technologischen Pfade klar erkennbar, und die zentralen Herausforderungen werden systematisch adressiert. Entscheidend ist daher nicht der heutige Leistungsstand einzelner Systeme, sondern die Geschwindigkeit, mit der sich Skalierung, Fehlerkorrektur und algorithmische Effizienz gegenseitig verstärken.

In der Konsequenz bedeutet dies: Der Q-Day ist kein fernes, spekulatives Szenario mehr, sondern das Ergebnis einer bereits laufenden technologischen Entwicklung, deren Fortschritt sich zunehmend beschleunigt. Für strategische Entscheidungen ist daher weniger relevant, ob aktuelle Systeme ausreichen, sondern ob Organisationen rechtzeitig auf die nächste Technologiegeneration vorbereitet sind.

1.3 Bedrohungsmodell

Das Bedrohungsmodell „Harvest now, decrypt later“ (HNDL) verändert die zeitliche Logik klassischer IT-Sicherheitsüberlegungen grundlegend. Während traditionelle Angriffsmodelle davon ausgehen, dass Daten zum Zeitpunkt ihrer Übertragung oder Speicherung geschützt sein müssen, verschiebt HNDL den Angriff in zwei Phasen: das heutige Sammeln verschlüsselter Daten und deren spätere Entschlüsselung mithilfe leistungsfähigerer Technologien – insbesondere Quantencomputer.

Im ersten Schritt werden Daten abgefangen, gespeichert und langfristig archiviert. Dies betrifft insbesondere Kommunikationsverbindungen, verschlüsselte Backups, Cloud-Datenströme oder auch signierte Softwareartefakte. Der entscheidende Punkt: Für den Angreifer besteht heute keine Notwendigkeit, die Verschlüsselung unmittelbar zu brechen. Es genügt, die Daten vollständig und unverändert zu sichern.

Im zweiten Schritt erfolgt – zu einem späteren Zeitpunkt – die Entschlüsselung. Sobald Quantencomputer in der Lage sind, die zugrunde liegenden kryptografischen Verfahren effizient anzugreifen, können zuvor gesammelte Daten retrospektiv offengelegt werden. Der eigentliche Schaden tritt somit zeitversetzt ein, während die Verwundbarkeit bereits in der Gegenwart entsteht.

Dieses Modell ist insbesondere für Daten mit langer Schutzdauer kritisch. Dazu zählen geistiges Eigentum, strategische

Unternehmensentscheidungen, Forschungsdaten, personenbezogene Informationen oder staatliche Kommunikation. In vielen dieser Fälle übersteigt die notwendige Vertraulichkeitsdauer den erwarteten Zeithorizont bis zur praktischen Verfügbarkeit leistungsfähiger Quantencomputer. Damit wird jede heutige Übertragung potenziell zu einem zukünftigen Risiko.

Für Organisationen ergibt sich daraus eine zentrale Verschiebung in der Risikobewertung: Sicherheit darf nicht mehr ausschließlich im Kontext aktueller Bedrohungen betrachtet werden, sondern muss zukünftige Entschlüsselungsfähigkeiten antizipieren. Klassische Kryptografie bietet zwar heute Schutz gegen konventionelle Angreifer, versagt jedoch perspektivisch gegenüber quantenbasierten Angriffen. Die Folge ist eine schleichende Erosion der Sicherheitsgarantien.

Besonders problematisch ist, dass HNDL-Angriffe schwer nachweisbar sind. Das passive Mitschneiden verschlüsselter Kommunikation hinterlässt in vielen Fällen keine unmittelbaren Spuren. Es handelt sich nicht um einen aktiven Angriff, sondern um eine vorbereitende Maßnahme. Organisationen können daher kaum erkennen, ob und in welchem Umfang ihre Daten bereits gesammelt wurden.

Ein weiterer kritischer Aspekt betrifft digitale Signaturen und Integritätsschutz. Während häufig der Fokus auf Vertraulichkeit liegt, eröffnet HNDL auch langfristige Risiken für Authentizität und Nachweisbarkeit. Signierte Dokumente oder Software können in Zukunft gefälscht werden, wenn die zugrunde liegenden Signaturverfahren

gebrochen werden. Dies untergräbt nicht nur technische Sicherheit, sondern auch rechtliche und regulatorische Grundlagen.

Das Bedrohungsmodell hat zudem eine geopolitische Dimension. Staaten und staatlich unterstützte Akteure verfügen über die Ressourcen, große Datenmengen systematisch zu sammeln und über Jahre hinweg zu archivieren. Für sie ist HNDL kein hypothetisches Szenario, sondern eine strategische Option. Unternehmen, die international tätig sind oder in sensiblen Branchen operieren, müssen dieses Risiko explizit berücksichtigen.

Die Konsequenz ist eindeutig: Der Q-Day beginnt aus Sicht von HNDL nicht in der Zukunft, sondern wirkt bereits heute. Jede Entscheidung über den Einsatz kryptografischer Verfahren, jede Datenübertragung und jede langfristige Speicherung muss unter der Annahme getroffen werden, dass die verwendete Verschlüsselung in Zukunft gebrochen werden kann.

Damit verschiebt sich auch die Priorität von Post-Quantum-Kryptografie. Sie ist nicht nur eine Reaktion auf zukünftige Technologien, sondern eine präventive Maßnahme gegen bereits laufende Angriffsstrategien. Organisationen, die heute keine Maßnahmen ergreifen, gehen implizit davon aus, dass ihre Daten keinen langfristigen Wert besitzen – eine Annahme, die in den meisten Fällen nicht zutrifft.

1.4 Zeitachsen und Szenarien

Die zentrale Herausforderung im Kontext des Q-Day liegt nicht nur in der technologischen Entwicklung selbst, sondern in der Unsicherheit ihrer zeitlichen Einordnung. Anders als bei klassischen IT-Innovationen lassen sich Fortschritte im Quantencomputing nicht linear prognostizieren. Vielmehr bewegen sich Organisationen in einem Spannungsfeld aus optimistischen und konservativen Szenarien, die jeweils unterschiedliche strategische Implikationen haben.

Optimistische Szenarien gehen davon aus, dass entscheidende Durchbrüche – insbesondere im Bereich der Fehlerkorrektur und Skalierung – schneller erreicht werden als derzeit erwartet. In solchen Projektionen könnten leistungsfähige, fehlertolerante Quantencomputer bereits innerhalb der nächsten 10 bis 15 Jahre verfügbar sein. Treiber hierfür sind exponentielle Investitionen, technologische Diversifizierung sowie mögliche algorithmische Effizienzgewinne, die den Hardwarebedarf reduzieren. Für sicherheitskritische Anwendungen würde dies bedeuten, dass die verbleibende Migrationszeit deutlich kürzer ist als in vielen aktuellen Planungen angenommen.

Konservative Szenarien hingegen betonen die erheblichen physikalischen und ingenieurstechnischen Hürden. Insbesondere die Anforderungen an stabile Qubits, skalierbare Fehlerkorrektur und kontrollierte Umgebungsbedingungen gelten als langfristige Herausforderungen. In dieser Perspektive könnte es mehrere Jahrzehnte dauern, bis Quantencomputer tatsächlich in der Lage sind, kryptografisch

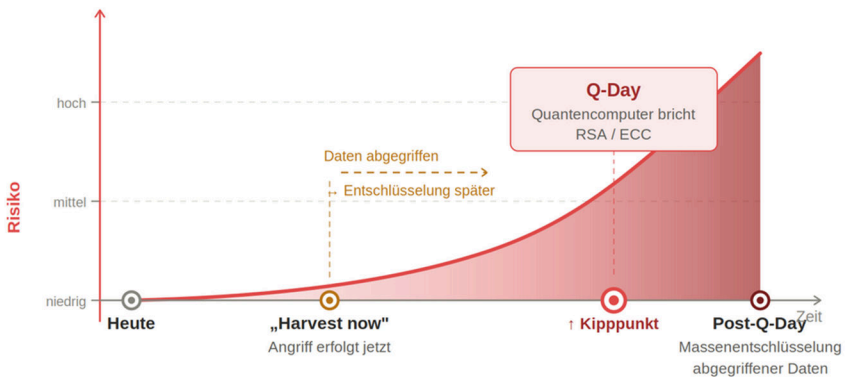
relevante Schlüsselgrößen praktisch zu brechen. Diese Sichtweise wird häufig von der Annahme getragen, dass heutige Fortschritte zwar signifikant, aber nicht unmittelbar disruptiv sind.

Für die strategische Planung ist jedoch entscheidend, dass beide Szenarien nicht isoliert betrachtet werden dürfen. Die relevante Größe ist nicht der wahrscheinlichste Zeitpunkt, sondern der frühestmögliche Eintritt eines kritischen Zustands. Sicherheitsarchitekturen müssen sich daher am konservativen Risikomanagement orientieren: Es gilt, auf das frühere Szenario vorbereitet zu sein, selbst wenn dieses mit geringerer Wahrscheinlichkeit eintritt.

Hinzu kommt die zeitliche Verzögerung durch organisatorische und technische Umstellung. Die Migration kryptografischer Infrastrukturen – insbesondere in komplexen IT-Landschaften – kann mehrere Jahre in Anspruch nehmen. Systeme müssen identifiziert, Abhängigkeiten analysiert, Protokolle angepasst und Hardware gegebenenfalls ersetzt werden. Diese Transformationsdauer verschiebt den effektiven Handlungsbeginn deutlich nach vorne.

Ein weiterer Aspekt ist die unterschiedliche Betroffenheit von Datenklassen. Während kurzfristige Datenströme möglicherweise erst bei einem tatsächlichen Eintritt des Q-Day relevant werden, sind langfristig schützenswerte Informationen bereits heute exponiert. Damit entsteht eine überlappende Zeitachse: Der technische Durchbruch liegt in der Zukunft, die sicherheitsrelevanten Konsequenzen beginnen jedoch in der Gegenwart.

Aus dieser Perspektive ergibt sich keine klare Deadline, sondern ein Handlungsfenster mit unscharfen Grenzen. Organisationen, die auf eindeutige Signale oder verbindliche Zeitpunkte warten, laufen Gefahr, dieses Fenster zu verpassen. Effektive Post-Quantum-Readiness bedeutet daher, unter Unsicherheit zu planen und Entscheidungen nicht an exakten Prognosen, sondern an robusten Szenarien auszurichten.



Die Abbildung verdeutlicht die zeitliche Entkopplung von Angriff und Wirkung. Sensible Daten können bereits heute abgegriffen werden, während ihre Entschlüsselung erst mit zukünftigen Quantencomputern erfolgt.

1.5 Komplexitätsbruch

Die Bedrohung durch Quantencomputer ist nicht lediglich eine Frage höherer Rechenleistung, sondern Ausdruck eines fundamentalen

Stichwortverzeichnis

A

Adoption	125
Algorithmusklasse	43
Algorithmuslandschaft	45
Angriffsszenario	30
API	91
Architekturprinzip	58, 90
Auditierbarkeit	115
Auswahlkriterium	48

B

Bedrohungsmodell	12
Budgetierung	3, 81

C

Change Management	133
CISO	67
Cloud	114
Codebasierte Kryptografie	44
Continuous Integration	80
Crypto Inventory	75
Crypto-Abstraction	58
Crypto-Inventory	67

D

Datenschutz	117
Deadline	17
Digitale Signatur	30

E

ECC	6
Effektive Post-Quantum-Readiness	17
Elliptic Curve Cryptography	6
Embedded System	89
Entkopplung	90

F

Finanzsektor	113
Framework	111

G

Gesundheitswesen	113
Gitterbasierte Kryptografie	43
Google	5
Governance	3

Governance-Modell.....66
 Grover8

H

Handlungsempfehlungen 135
 Hardware 100
 Hardware Security Module..... 101
 Harvest now, decrypt later7
 HNDL12
 HNDL-Angriff13
 HSM 101
 Hybrid-Ansatz..... 41, 63

I

IBM5
 Incident Response.....92
 Industrie..... 113
 Infrastruktur1
 Integration.....90
 Interoperabilität 104
 IoT..... 49, 89
 Isogeniebasierte Kryptografie.....44

K

KI-System.....2
 Kommunikation36
 Kopplung.....90
 Kostenimplikation 102

KRITIS 35
 Krypto-Agilität 3, 55
 Kryptografie.....6
 Kurvenkryptografie 6, 18

L

Learning With Errors 43
 Legacy-System..... 61
 Lifecycle-Management 67
 LTE 43

M

Migration..... 128
 Migrationsstrategie3
 Monitoring.....92
 Mythos5

N

Nachweispflicht 118
 National Institute of Standards and
 Technology.....45
 Nationale Sicherheit..... 35
 NISQ9
 NIST45
 Noisy Intermediate-Scale Quantum 9

O

Ökosystem 130

P

Performance98

Performance-Overhead60

Pilotprojekt.....95

Post-Quantum-Kryptografie 3, 39

Post-Quantum-Readiness 3, 71

Post-Quantum-Strategie.....29

Post-Quantum-Transformation.....79

PQC18

PQC Maturity LevelsXII

PQC Scorecard..... VI

Public-Key-Infrastruktur 30, 93

Q

Q-Day.....1

Quantenalgorithmen25

Quantenalgorithmus 10

Quantenbedrohung23

Quantencomputer.....1

Quantenmechanik.....24

Quantum Supremacy9

Quantum-Safe.....73

R

Rechenlast.....99

Regulierungslandschaft..... 108

Reifegradmodell.....72

Ressourcenkonkurrenz..... 84

Risikoanalyse77

Risikobewertung33

Risikoexposition33

Rivest-Shamir-Adleman..... 10

Roadmap79

RSA.....10

S

SaaS 119

Schlüsselaustausch30

Schlüsselmanagement.....92

Schutzdauer.....12

Shor-Algorithmus27

Shortest Vector Problem43

Skalierbarkeit.....99

Skalierungsstrategie.....9

Standardisierung.....45

Superposition.....24

Supply Chain..... 116, 119

SVP43

T

Testumgebung.....	95
tice-based.....	43
TLS.....	49, 51, 93
Token.....	31
Transparenz.....	75
Transport Layer Security.....	93
Trend.....	124

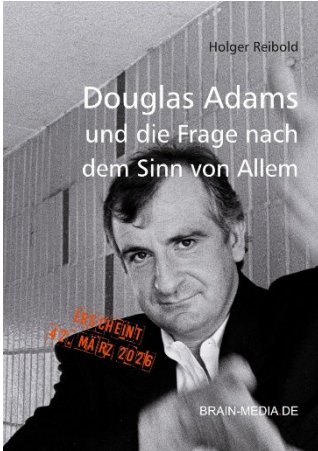
V

Verschlüsselung.....	40
VPN.....	51
VPN-Technologie.....	93

Z

Zeitachse.....	15
Zertifikat.....	31
Zertifizierung.....	115
Zielbild.....	40

Mehr von Brain-Media.de



42 – Douglas Adams und die Frage nach dem Sinn von Allem

Am 11. Mai 2026 ist Douglas Adams 25 Jahre tot. Der Kultautor hat der Welt wunderbar, skurrile Werke geschenkt. Jetzt ist es an der Zeit, den Autor kennenzulernen.

Umfang: 140 Seiten

Preis: 14,99 EUR

Erscheint: 42. März 2026



Towelday, das ultimative Handtuch für alle Fans

An seinem Todestag, dem Towelday, erinnern sich Fans an Douglas Adams und huldigen dem Kultautor.

100 % intergalaktisch geprüfte Baumwolle, nachhaltig Produktion zum Preis von 42 EUR.



**Synergie der Intelligenz –
Das Handbuch für das Design
und die Implementierung von
Multi-Agenten-Systemen**

Dieses Buch zeigt, wie Agenten zusammenarbeiten und wie Sie intelligente, skalierbare Systeme erfolgreich designen und einsetzen.

Umfang: 190 Seiten

Preis: 29,99 EUR



**Lokale KI – Sichere Architektur,
Betrieb und Governance
von GenAI- und RAG-Systemen**

RAG- und LLM-Plattformen mit klarer Architektur, Guardrails, Monitoring und Governance kontrolliert und resilient betreiben.

Umfang: 270 Seiten

Preis: 29,99 EUR



Knowledge as a Service

Personal
Business
Enterprise

IT-Security, Compliance und KI entwickeln sich schneller als jedes gedruckte Buch. Um dieser Dynamik Rechnung zu tragen, hat Brain-Media.de **KaaS – Knowledge as a Service** entwickelt.

Mit KaaS erhalten Sie ein lebendes **Wissenssystem**: Alle Titel als PDF/E-Book, **regelmäßig aktualisierte Living Documents** sowie **exklusive Downloads** – Checklisten, Vorlagen und sofort einsetzbare Templates.

Speziell für **Regulierung und Audits**: Inhalte zu NIS-2, DORA, CRA & AI Act werden laufend gepflegt und helfen Ihnen, Anforderungen strukturiert umzusetzen und auditfähig zu bleiben. Für fortgeschrittene Nutzung stehen Inhalte zusätzlich als **Markdown- und JSON-Rohdaten** bereit – ideal für die Automatisierung und Integration in Ihre Umgebungen.

KaaS ist die wachsende **Bibliothek für**
Praxis, Compliance und Resilienz.