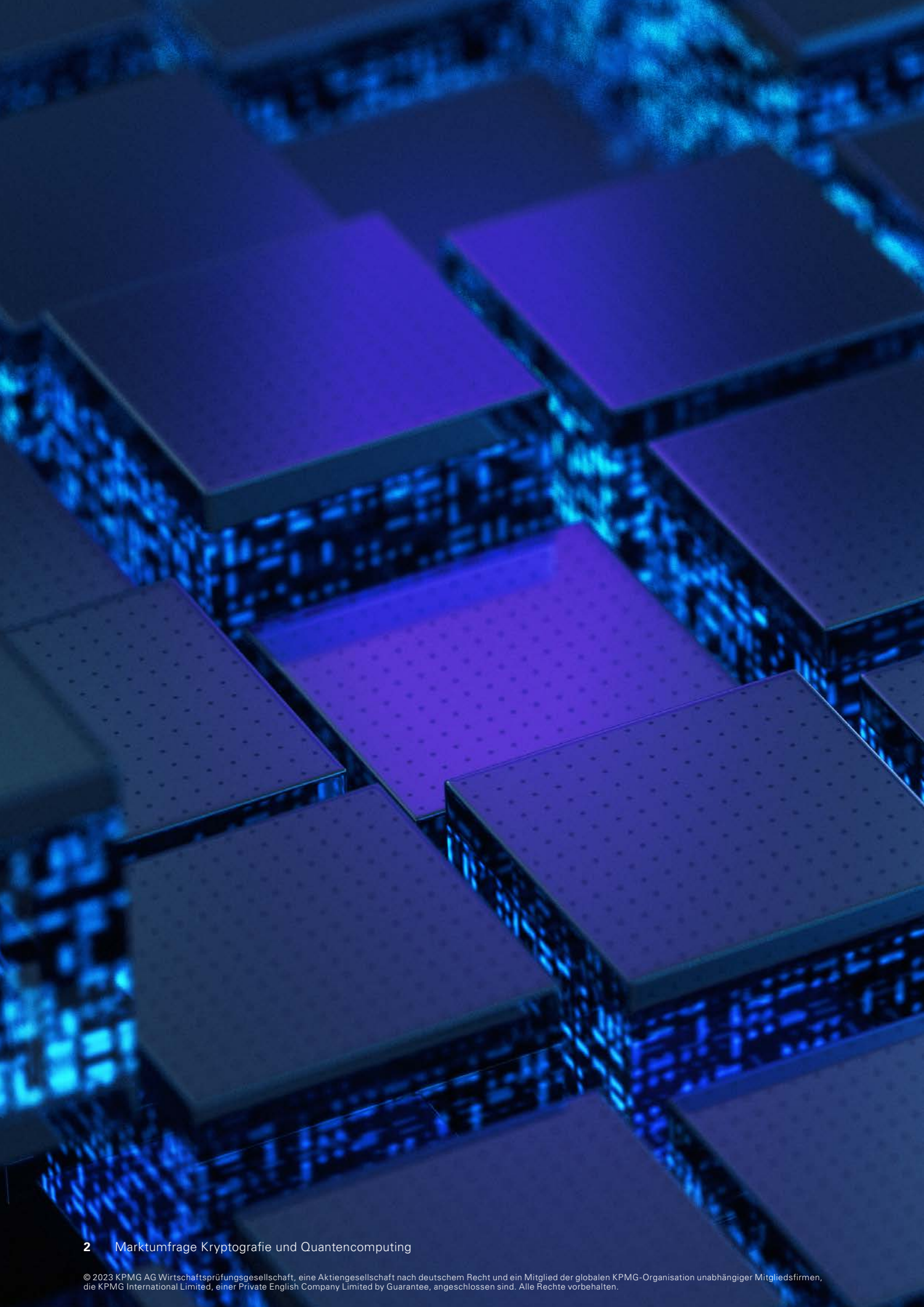
KPMG

Bundesamt
für Sicherheit in der
Informationstechnik

Marktumfrage Kryptografie und Quantencomputing



Inhalt

1. Einleitung

Durch die fortschreitende Digitalisierung wird ein immer größerer Anteil unserer Daten in elektronischer Form gespeichert, verarbeitet und übertragen. Dieser Trend eröffnet uns beachtliche neue Möglichkeiten, macht uns aber gleichzeitig immer abhängiger von Technologie. Kryptografie ist dabei essenziell, um die Authentizität, Integrität und Vertraulichkeit von Informationen sicherzustellen. Vielfach unbemerkt, ist Kryptografie im digitalen Zeitalter geradezu omnipräsent.

Mit Quantencomputing wird eine Technologie entwickelt, die sich die spezifischen Gesetze der Physik der kleinsten Teilchen (Quantenmechanik) zunutze macht, um effiziente Berechnungen durchzuführen. Es ist unklar, wann die Reife zur praktischen Anwendung erreicht ist, jedoch existiert die Technologie bereits und wird von Monat zu Monat leistungsfähiger. Von Biotechnologien bis zur Städteplanung bietet Quantencomputing das Potenzial für enorme Fortschritte, gleichzeitig entstehen aber auch neue Risiken für die Informations- und Kommunikationssicherheit.

Wir dürfen daher nicht nur auf die Möglichkeiten dieser aufkommenden, revolutionären Technologie schauen, sondern müssen auch für die Risiken gewappnet sein, denn die Bedrohung ist groß und geht tief. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat dazu Ende letzten Jahres den Leitfaden „Kryptografie quantensicher gestalten – Grundlagen, Entwicklungen, Empfehlungen“ veröffentlicht.

Kryptografische Verfahren, die heute als sicher gelten und fest in unseren digitalen Infrastrukturen integriert sind, können in Zukunft mit Quantencomputern gebrochen werden und müssen daher bald durch neue, quantensichere Methoden, wie beispielsweise die sogenannte Post-Quanten-Kryptografie, ersetzt und ergänzt werden.

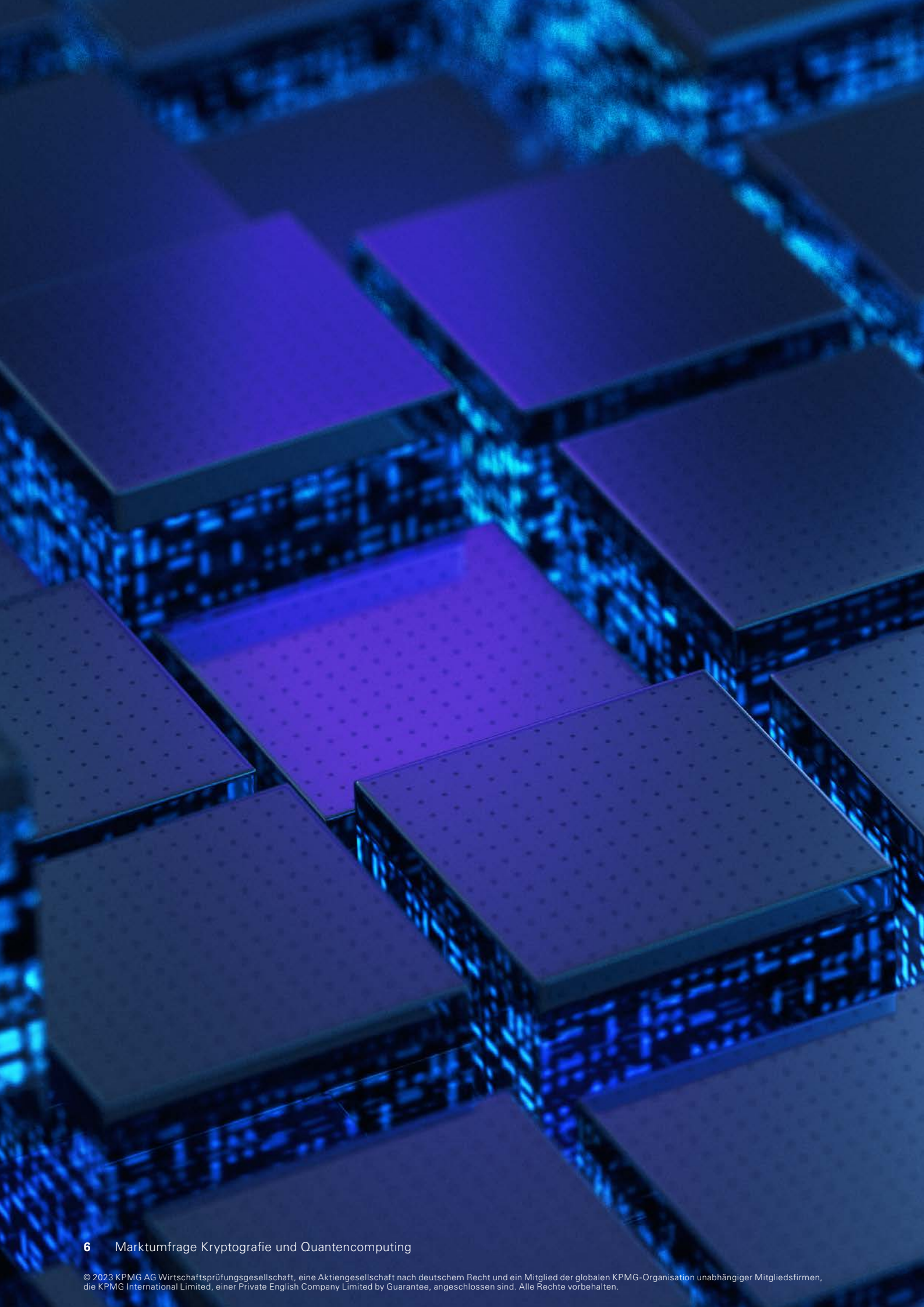
Um Staat, Wirtschaft und Gesellschaft bei diesem Thema bestmöglich unterstützen zu können, haben das BSI und KPMG in Deutschland eine gemeinsame Umfrage unter Organisationen verschiedener Art durchgeführt. Mittels dieser Umfrage und der vorliegenden Auswertung der Ergebnisse möchten wir den aktuellen Stand in verschiedenen Branchen darstellen und besser verstehen. Zudem sollen die notwendige Aufmerksamkeit auf das Thema gelenkt und Handlungsempfehlungen gegeben werden.

Vorgehen:
Diese Marktumfrage entstand in einer Kooperation zwischen dem BSI und KPMG in Deutschland. Expertinnen und Experten beider Organisationen haben gemeinsam einen Fragebogen entworfen, um das Bewusstsein und den Kenntnisstand zu den möglichen Auswirkungen von Quantencomputing auf die Kryptografie sowie den Stand bei der Migration zu quantensicheren Alternativen in den Unternehmen abzufragen. Der Fragebogen beinhaltete außerdem Fragen zum Unternehmen (z. B. Branche, Größe) sowie zur Stellung der Ausfüllenden in deren Organisation. An der Marktumfrage haben 28 Unternehmen und Organisationen[1] teilgenommen. Die Rücklaufquote war im Vergleich zu anderen Studien dieser Art geringer.

[1] Daher entspricht eine Rückmeldung rund 4% der Teilnehmenden.

Abb. 1: Befragte Unternehmen und Organisationen

Quelle: KPMG in Deutschland, 2022



2. Das Wichtigste in Kürze

Relevanz

Über 95 % der Teilnehmenden bewerteten die generelle Relevanz von Quantencomputing für die Sicherheit von kryptografischen Verfahren als „hoch“ oder „eher hoch“.

Das durchschnittliche Risiko für die Sicherheit der Daten in der eigenen Organisation schätzen über 65 % der Teilnehmenden als „hoch“ oder „eher hoch“ ein.

Zeitskalen

Die Teilnehmenden erwarten im Mittel, dass aktuell verwendete kryptografische Verfahren in zehn Jahren gebrochen werden.

Allerdings erwarten 89 % der Teilnehmenden, dass die Umstellung ihrer Organisation zu quantensicherer Kryptografie nicht rechtzeitig abgeschlossen wird, um die Vertraulichkeitsanforderungen für ihre Daten zu erfüllen.

Behandlung

Lediglich 25 % der Teilnehmenden gaben an, dass die Gefährdung der Kryptografie durch Quantencomputing im Risikomanagement ihrer Organisation berücksichtigt wird.

96 % der Teilnehmenden gaben an, dass Investitionsentscheidungen für quantensichere Kryptografie durch regulatorische Vorgaben begünstigt würden. Die Existenz von Standards wird von 89 % der Teilnehmenden als begünstigend eingestuft.

Rücklauf

An der Umfrage haben sich 18,3 % der angeschriebenen Unternehmen und Organisationen beteiligt.

Dabei decken sich die Einschätzungen von 71 % mit der gängigen Expertenmeinung, was die Auswirkungen von Quantencomputing auf die Kryptografie betrifft.

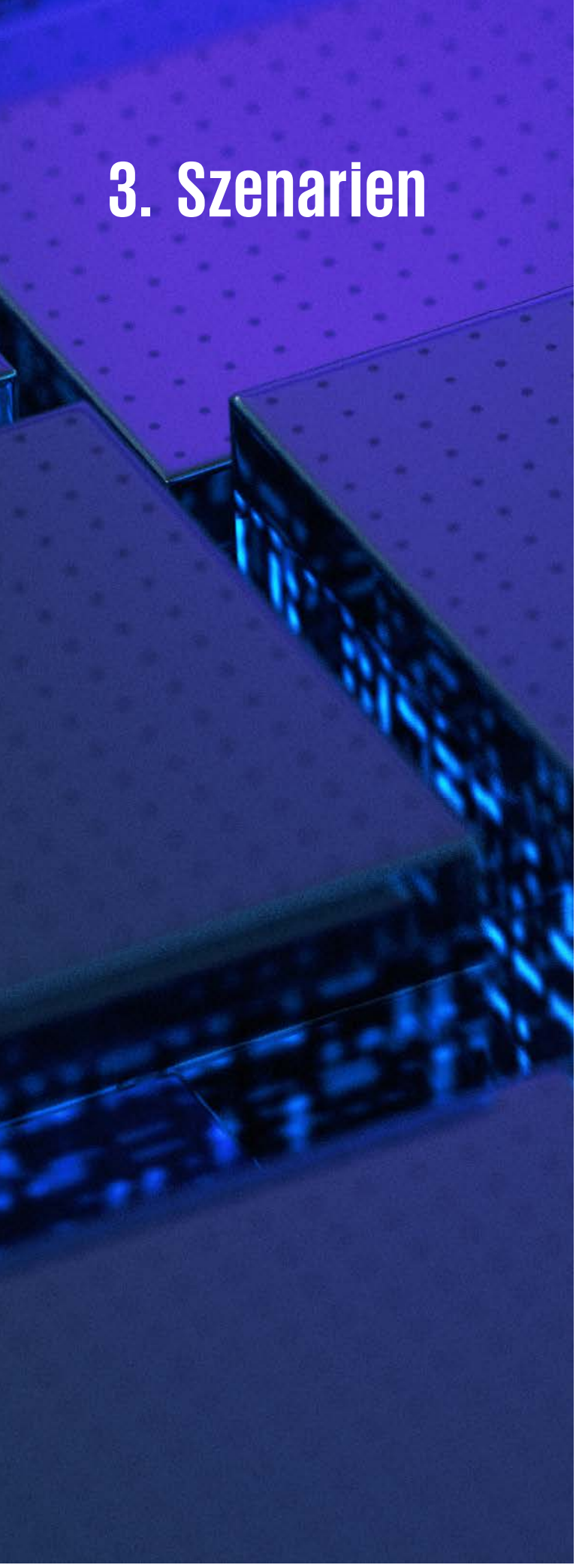
Die Teilnehmenden gaben an, mit den genannten Themen im Durchschnitt „eher vertraut“ zu sein.

Die durchgeführte Umfrage konnte feststellen, dass die vertraulichen Daten der teilnehmenden Organisationen nach eigener Einschätzung jahrelang durch Quantencomputer verwundbar sein werden.

Obwohl es Gegenmaßnahmen gibt, die heute schon durchgeführt oder begonnen werden können, erfolgt dies noch nicht im ausreichenden Maße. Ein wichtiger erster Schritt scheint zu sein, das nötige Risikobewusstsein herzustellen und Methoden zur Behandlung der Risiken zu vermitteln.

Es ist sehr besorgniserregend, dass nur 11 % der Teilnehmenden eine Chance sehen, rechtzeitig quantensicher zu werden.

Hans-Peter Fischer
KPMG in Deutschland
Partner



3. Szenarien

In zwei konkreten Szenarien soll vereinfacht, aber deutlich dargestellt werden, welche Konsequenzen zu befürchten wären, wenn kryptografische Verfahren gebrochen werden, und warum das Thema Quantenresistenz bearbeitet werden muss:

Szenario 1 (Vertraulichkeit):

Ein herstellendes Unternehmen von komplexen Maschinen hat Standorte in mehreren Ländern und auf mehreren Kontinenten. Die Produktentwicklung in der europäischen Entwicklungszentrale sendet die hochvertraulichen Produktionspläne über vertrauliche Telekommunikationsverbindungen an die Produktion in mehreren anderen Ländern. Für die vertrauliche Kommunikation wird die sogenannte Public-Key -Kryptografie verwendet. Quantencomputer können einem Angreifenden durch das Brechen der Public-Key-Kryptografie zukünftig das Mitlesen der vertraulichen Nachrichten im Klartext ermöglichen. Das herstellende Unternehmen bemerkt dies nicht. Dem Angreifenden ist es mit den Produktionsunterlagen möglich, Kopien der komplexen Maschinen herzustellen. Nach kurzer Zeit erscheint auf dem Markt ein kopiertes Konkurrenzprodukt zu einem günstigeren Preis. Das herstellende Unternehmen verliert einen großen Marktanteil an den neuen Wettbewerber. Dies kann über das Store-now-decrypt-later-Vorgehen auch Produktionspläne betreffen, die vor der Verfügbarkeit des Quantencomputers verschickt worden sind.

Szenario 2 (Authentisierung):

Ein Unternehmen, das Kommunikationskomponenten in Konsumentenprodukten anbietet, wie zum Beispiel ein Zulieferunternehmen von Schließsystemen, verwendet in seinen Produkten zum Zweck der Authentisierung Public-Key-Kryptografie. Die dabei verwendeten öffentlichen Schlüssel werden mittels digitaler Zertifikate an die zugehörigen Komponenten (beispielsweise eine Zugangskarte) gebunden; die Zertifikate selbst werden über eine Public-Key-Infrastruktur (PKI) verifiziert. Quantencomputer können durch das Brechen der Public-Key-Kryptografie zukünftig die Sicherheit der Schließsysteme beeinträchtigen, da ein Angreifender mittels Quantencomputern an den privaten Schlüssel einer Root-Zertifizierungsinstanz gelangen könnte. Damit ist der Angreifende in der Lage, mit diesem Schlüssel signierte Zertifikate nach Belieben auszustellen. Er kann somit beispielsweise auch gefälschte Zugangskarten herstellen, die von den Prüfsystemen als gültig erkannt werden. Ein ähnliches Angriffsszenario ist auch in vielen weiteren Anwendungen denkbar, beispielsweise in kritischen Infrastrukturen. Das Problem hierbei ist insbesondere, dass Root-Zertifikate eine lange Lebenszeit und eine hohe Reichweite haben können, dementsprechend lohnen sich in Zukunft unter Umständen auch kostspielige Angriffe mit einem Quantencomputer auf eine Root-Zertifizierungsinstanz.

Bei allen Szenarien muss zur Vermeidung einer konkreten Gefährdung quantensichere Kryptografie eingebaut werden, bevor ein Quantencomputer die eingesetzte Kryptografie brechen kann. Die dafür notwendige Zeit setzt sich zusammen aus der Entwicklungsdauer für ein Produkt mit quantenresistenter Kryptografie sowie der Dauer, um die Neuentwicklung in die bestehenden Produkte bzw. Komponenten zu implementieren. Weiter muss unter Umständen die Zeit, für die Informationen vertraulich bleiben müssen, berücksichtigt werden (siehe „Moscas Theorem“ auf Seite 17).

4. Ergebnisse

Im Folgenden beschreiben wir die wesentlichen Ergebnisse der Umfrage. Dabei haben wir die Antworten unter folgenden Leitfragen eingeordnet:

1. Wie gut sind die Teilnehmenden mit dem Thema vertraut?

2. Wie stark sind die teilnehmenden Organisationen betroffen?

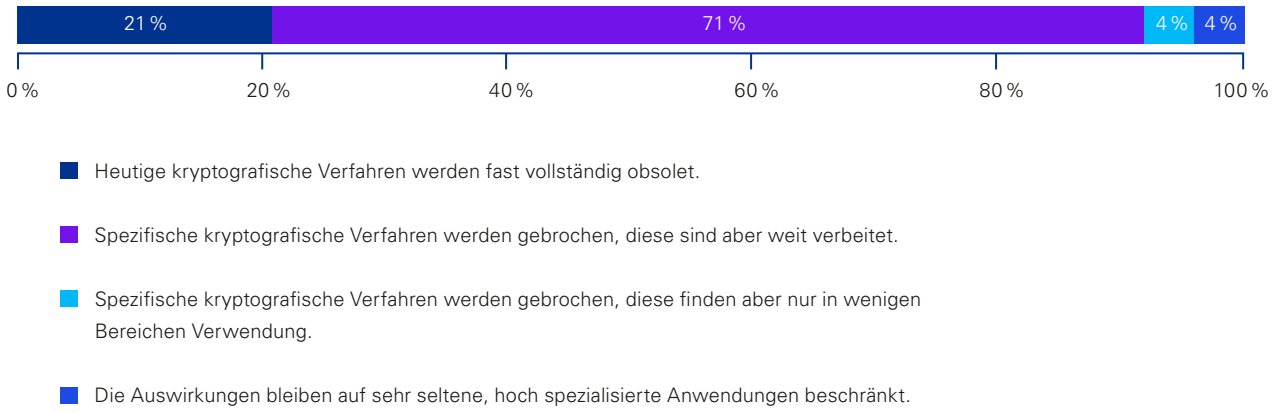
3. Schaffen die Organisationen rechtzeitig die Migration zu quantensicherer Kryptografie?

4. Was wird in den Organisationen unternommen?

5. Welche Unterstützung benötigen die Organisationen für weitere Schritte?

4.1 Wie gut sind die Teilnehmenden mit dem Thema vertraut?

Abb. 2: Wie sehen Sie die Auswirkungen von Quantencomputing auf die Kryptografie?



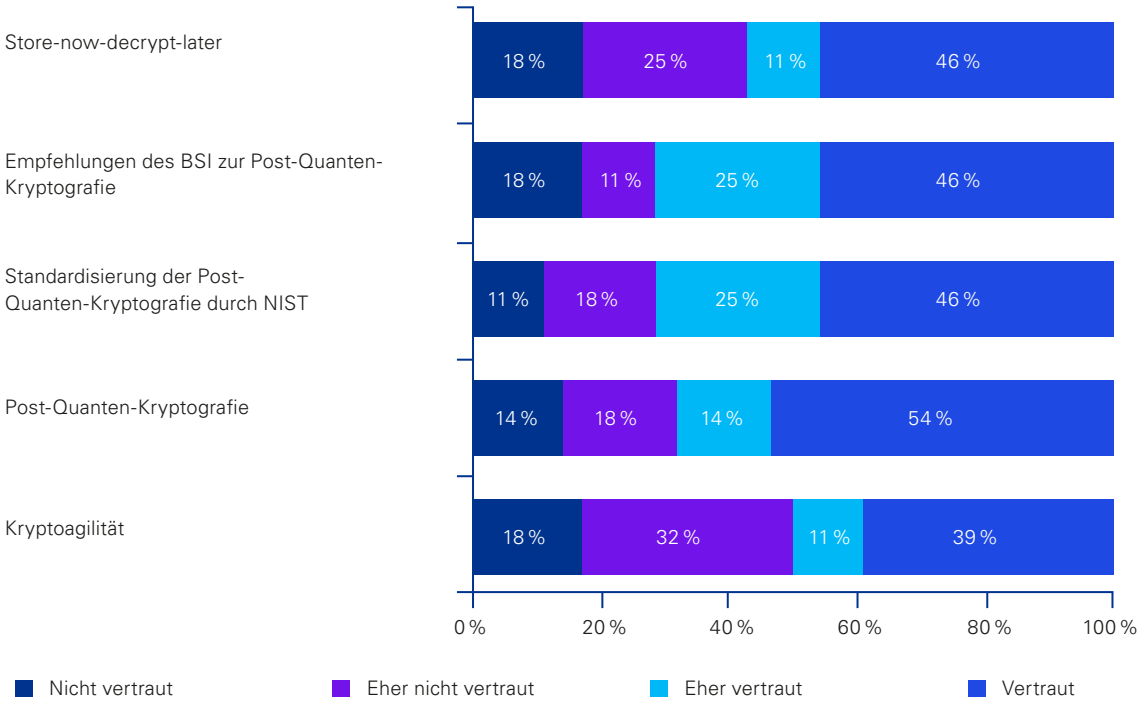
Quelle: KPMG in Deutschland, 2022; Angaben in Prozent, Rundungsdifferenzen möglich

Um die weiteren Angaben besser einschätzen zu können, wurden die Teilnehmenden zunächst gefragt, wie sie die Auswirkungen von Quantencomputing auf die Kryptografie sehen. 71 % gaben an, dass spezifische, aber weit verbreitete kryptografische Verfahren gebrochen werden. Dies deckt sich mit der gängigen Expertenmeinung, dass insbesondere die sogenannte Public-Key-Kryptografie gefährdet ist.

Einschätzung

Diese hohe Übereinstimmung kann als erstes Indiz dafür gesehen werden, dass die Teilnehmenden überwiegend bereits vor der Umfrage an dem Themenkomplex um Quantencomputing und Kryptografie interessiert waren.

Abb. 3: Wie vertraut sind Sie mit den folgenden Themen?



Quelle: KPMG in Deutschland, 2022; Angaben in Prozent, Rundungsdifferenzen möglich

Zusätzlich wurden die Teilnehmenden gebeten, ihre Vertrautheit mit verschiedenen Begriffen aus dem Themenbereich einzuschätzen. Am meisten vertraut (hier: gaben an „eher vertraut“ oder „vertraut“ zu sein) waren die Teilnehmenden mit dem laufenden Standardisierungsverfahren des NIST und den Empfehlungen des BSI zur Post-Quantum-Kryptografie (je 71 %), gefolgt von der Post-Quanten-Kryptografie selbst (68 %) und dem Konzept von Store-now-decrypt-later (57 %). Mit 50 % befindet sich Kryptoagilität an letzter Stelle. Über alle Themen und Rückmeldungen gemittelt, schätzen sich die Teilnehmenden als „eher vertraut“ ein.

Generell ist zu bemerken, dass die Anzahl der Teilnehmenden, die angaben, mit den fünf betrachteten Themen „nicht vertraut“ zu sein, niedrig ist.

Store-now-decrypt-later

Store-now-decrypt-later bezeichnet die Praxis, verschlüsselte Informationen, die lange vertraulich bleiben müssen, gemeinsam mit den öffentlichen Schlüsseln und den bei der Schlüsselaushandlung ausgetauschten Informationen jetzt zu speichern und diese zu entschlüsseln, sobald Quantencomputing eine ausreichende Reife erreicht hat. Dies kann auch im Rahmen von sogenanntem Data Harvesting passieren, dem großflächigen und ungezielten Abfangen, Speichern und Auswerten von über öffentliche Netzwerke gesendeten Daten. Diese Möglichkeit sollte mitbedacht werden, wenn langfristig vertrauliche Daten über einen zugänglichen Kanal gesendet werden.

Kryptoagilität

Kryptoagilität bedeutet, kryptografische Mechanismen beim Design von Kryptosystemen „möglichst flexibel zu halten, um auf Entwicklungen reagieren, kommende Empfehlungen und Standards umsetzen und möglicherweise in Zukunft Algorithmen, die nicht mehr das gewünschte Sicherheitsniveau garantieren, austauschen zu können[2].“ Dies ist in Bezug auf Quantencomputing insofern von großer Relevanz, da die Standardisierung von quantensicheren Algorithmen und Protokollen noch nicht abgeschlossen ist. Kryptoagile Systeme allerdings können nach Bereitstellung standardisierter Verfahren schnell und ohne wesentliche Reibungsverluste quantensicher gemacht werden. Die eigene Kryptografie agil zu gestalten, kann und sollte schon heute angegangen werden, beginnend mit der Erstellung eines umfänglichen Inventars der eingesetzten Kryptografie. Es sei noch erwähnt, dass Kryptoagilität auch unabhängig von Quantencomputing ein wichtiges Designkriterium sein sollte. Auch mit klassischen Computern kann der schnelle Austausch von Kryptografie notwendig werden (ein Beispiel hierfür ist zum Beispiel die OpenSSL-Schwachstelle, die 2022 entdeckt wurde).

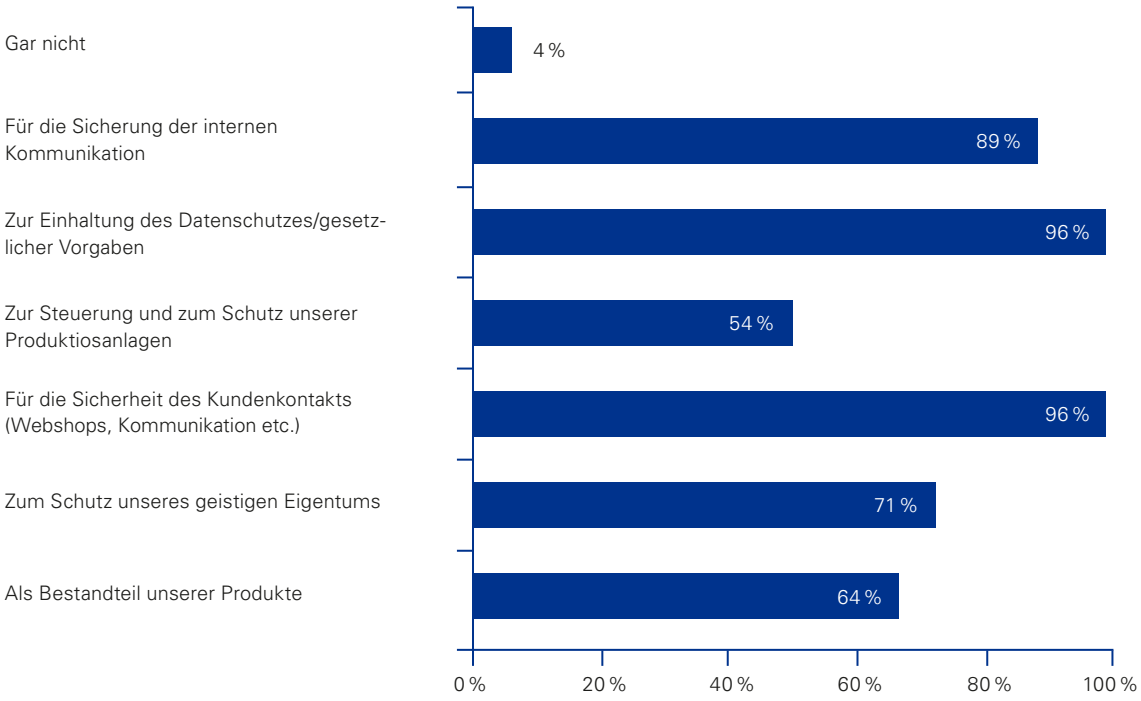
Das Store-now-decrypt-later-Szenario zeigt deutlich, dass die Auswirkungen von Quantencomputing auf die Kryptografie kein Zukunftsproblem sind. Die Bedrohung ist akut und muss bereits jetzt angegangen werden.

Thomas Caspers
Abteilungsleiter Technik-Kompetenzzentren, BSI

[2] „Kryptografie quantensicher gestalten – Grundlagen, Entwicklungen, Empfehlungen“ BSI, Oktober 2021; https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Kryptografie-quantensicher-gestalten.pdf?

4.2 Wie stark sind die teilnehmenden Organisationen betroffen?

Abb. 4: Zu welchen Zwecken werden von Ihrer Organisation kryptografische Verfahren eingesetzt?



Quelle: KPMG in Deutschland, 2022; Angaben in Prozent, Rundungsdifferenzen möglich

Um diese Frage zu beantworten, sollte zunächst die Verbreitung von Kryptografie in den befragten Organisationen eingeschätzt werden. Hierbei gaben fast alle Teilnehmenden an, dass Kryptografie in ihrer Organisation an mehreren Stellen eingesetzt wird. Die meistgenannten Verwendungszwecke sind die Sicherung des Kundenkontakts (96 %), die Einhaltung von gesetzlichen Vorgaben und des Datenschutzes (96 %) sowie die interne Kommunikation (89 %). Andere Auswahlmöglichkeiten wurden mit Nennungen zwischen 54 % und 71 % deutlich seltener gewählt. Weniger häufig wurden „als Bestandteil unserer Produkte“ (64 %) und „zur Steuerung und zum Schutz unserer Produktionsanlagen“ (54 %) genannt. Im Gegensatz zu den Aspekten, die öfter genannt wurden, sind die letztgenannten stärker branchenabhängig, da sich Produkte und Produktionsanlagen stark unterscheiden können. So schwankt die Nennung von „Sicherung des Kundenkontaktes“ branchenabhängig zwischen 87,5 % und 100 %, während „als Bestandteil unserer Produkte“ je nach Branche zwischen 33 % und 100 % der Teilnehmenden nannten. Es erscheint daher wahrscheinlich, dass seltene Nennungen in dieser Kategorie zumindest teilweise auf branchenspezifische Aspekte zurückgehen.

Kryptografie ist überall und aus unserer heutigen Welt nicht mehr wegzudenken. Es ist gut, dass sich die Teilnehmenden dessen bewusst sind.

Wilhelm Dolle
KPMG in Deutschland
Partner, Head of Cyber Security

Zusätzlich wurde gefragt, welche Relevanz für die Sicherheit von kryptografischen Verfahren die Teilnehmenden von Quantencomputing generell erwarten. Dabei gaben über alle Branchen hinweg 96 % der Teilnehmenden an, die Relevanz als „hoch" (54 %) oder „eher hoch" (43 %) einzustufen. Bemerkenswert ist, dass keiner der Teilnehmenden die Relevanz als „niedrig" oder „eher niedrig" einschätzte. Ein Teilnehmender gab an, hierzu keine Meinung zu haben.

Einschätzung

Zusammengenommen deuten diese zwei Ergebnisse darauf hin, dass die Teilnehmenden schwerwiegende Auswirkungen erwarten, wenn Quantencomputer in der Lage sein werden, heutige kryptografische Verfahren zu brechen, ohne dass adäquate neue Technologien eingesetzt werden. Andererseits könnte die Einstimmigkeit unter den Teilnehmenden auch darauf hindeuten, dass die Teilnehmenden aus einer homogenen Gruppe stammen, die ein besonderes Interesse an Quantencomputing und Kryptografie mitbringt.

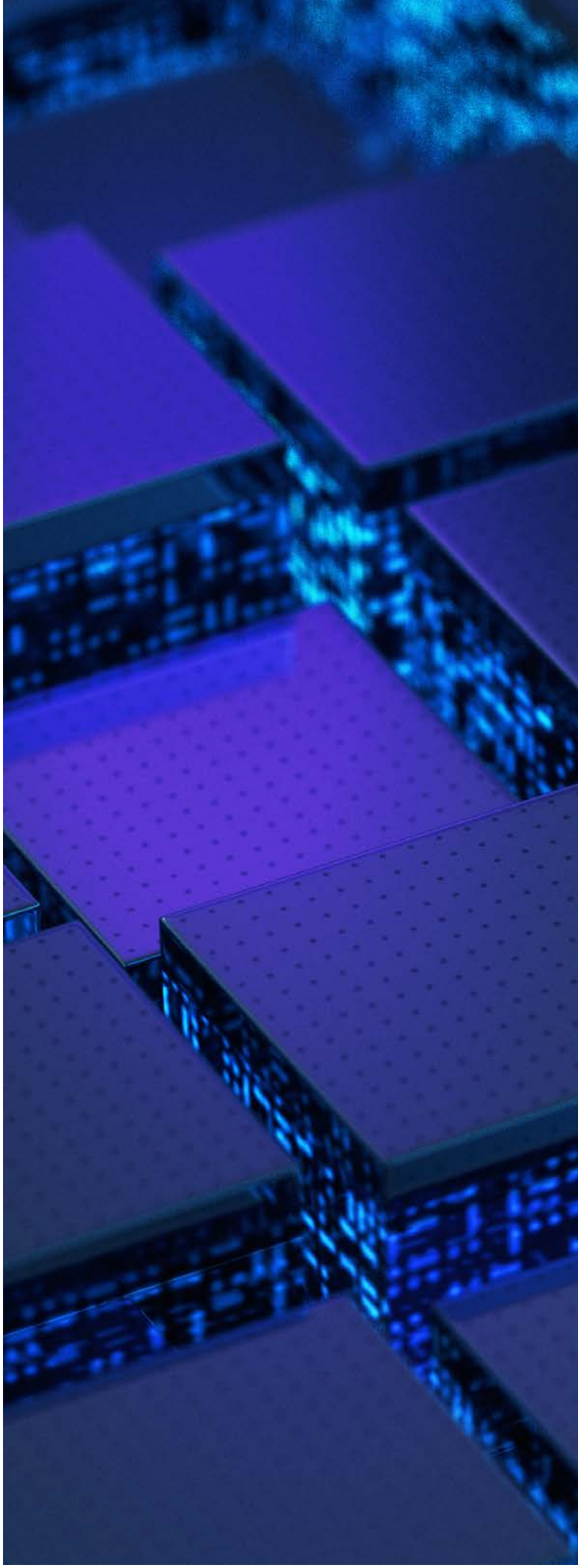
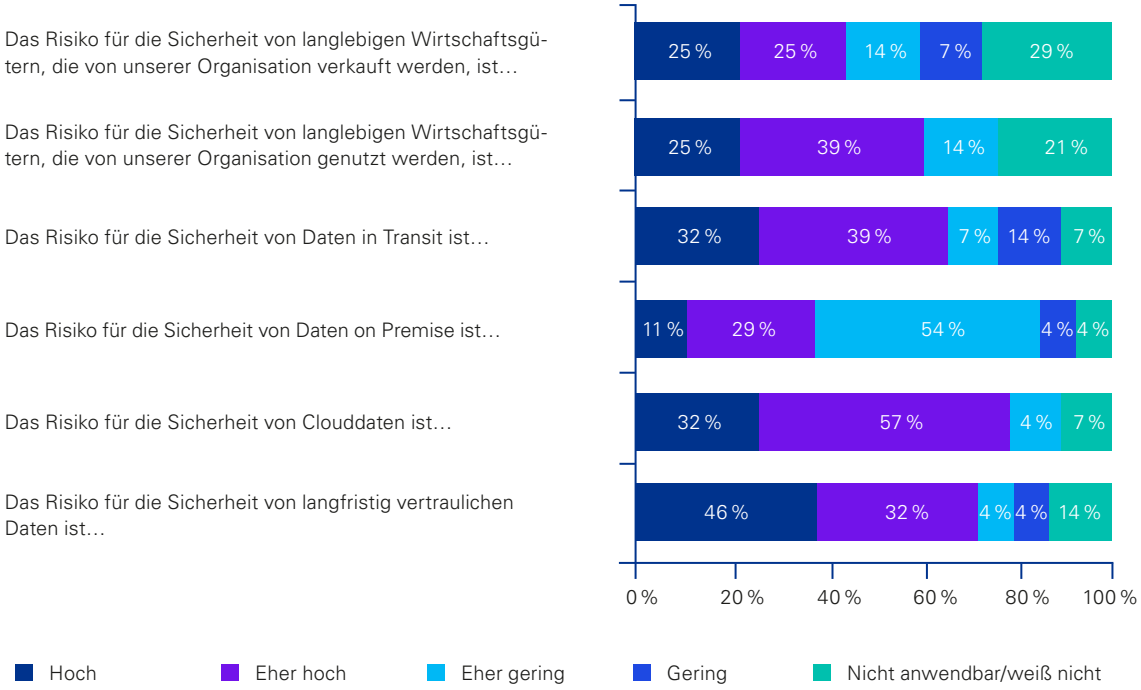


Abb. 5: Wie schätzen Sie die Risiken für Ihre Organisation durch Quantencomputing ein?



Quelle: KPMG in Deutschland, 2022; Angaben in Prozent, Rundungsdifferenzen möglich

Zu den Risiken für die eigene Organisation befragt, gaben 89 % der Teilnehmenden an, das Risiko für Clouddaten als „hoch" oder „eher hoch" einzuschätzen. Etwas geringer wird das Risiko für langfristig vertrauliche Daten (78 %) und von Daten in Transit (71 %) eingeschätzt. Die Sicherheit langlebiger Wirtschaftsgüter wurde als weniger bedroht angesehen: 64 % für die von den Organisationen genutzten langlebigen Wirtschaftsgütern, 50 % für diejenigen, die von den Organisationen verkauft werden. Für am wenigsten bedroht halten die Teilnehmenden Daten on Premise; nur 50 % erwarten hier ein erhöhtes Risiko.

Einschätzung

Bei der Einordnung dieser Zahlen ist zu bedenken, dass die abgefragten Datentypen sich zum Großteil nicht gegenseitig ausschließen. So können sich beispielsweise langfristig vertrauliche Daten in Transit zu einer Cloud befinden. Des Weiteren ist zu beachten, dass spezifisch nach den Risiken für die eigene Organisation gefragt wurde und nicht unbedingt alle Organisation langlebige Wirtschaftsgüter verkaufen. Es erscheint wahrscheinlich, dass dies zumindest ein Faktor ist, der die relativ niedrigen Zahlen beeinflusst.

Nachdem der Trend, dass Organisationen ihre IT-Infrastruktur immer stärker weg von eigenen Datacentern und hin zu Cloud- oder Edge-Lösungen bewegen, anhält, deuten auch diese Ergebnisse auf ein hohes Gefahrenpotenzial hin.

Die Antworten der Teilnehmenden weisen eine Korrelation zwischen den Angaben zur eigenen Vertrautheit mit den aufgeführten Themen und der Risikoeinschätzung auf. Das heißt, umso vertrauter sich die Teilnehmenden mit den verschiedenen Aspekten rund um Quantensicherheit in der Kryptografie fühlen, umso größer schätzen sie tendenziell das Risiko ein. Diese Erkenntnis könnte als zusätzliche Motivation für breite Aufklärungs- und Awarenesskampagnen aufgefasst werden.

4.3 Schaffen die Organisationen rechtzeitig die Migration zu quantensicherer Kryptografie?

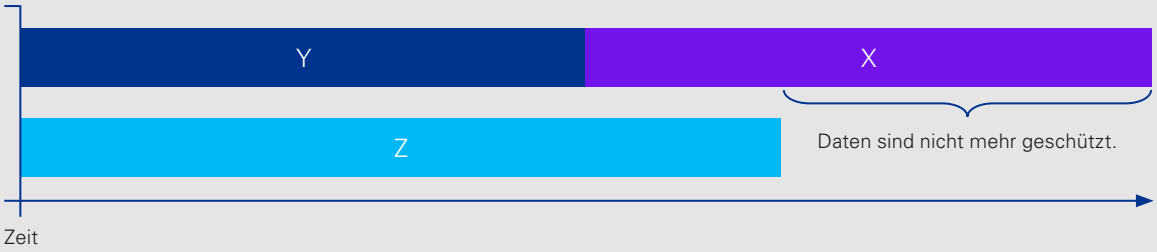
Das „Theorem“ von Mosca

Um abzuschätzen, wann die Migration zu quantencomputerresistenter Kryptografie notwendig ist, ist die folgende Überlegung des theoretischen Physikers Michele Mosca sehr anschaulich.

Sei dafür

- x die Anzahl der Jahre, die die zu schützenden Daten abgesichert bleiben müssen,
- y die Anzahl der Jahre, die man benötigt, um das entsprechende System auf quantencomputer-resistente Kryptografie umzustellen, sowie
- z die Anzahl der Jahre, die es noch dauert, bis Quantencomputer existieren, die die aktuell verwendete Kryptografie gefährden.

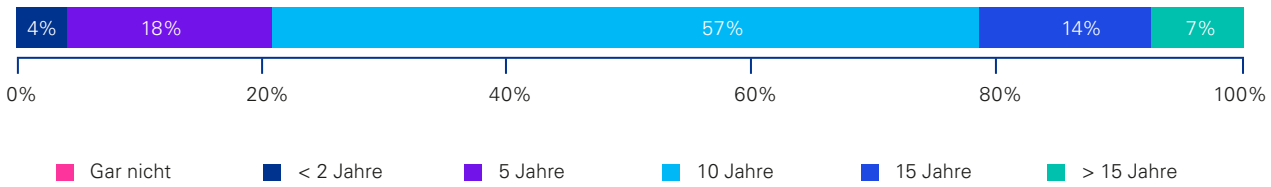
Dann gilt: Falls y+x > z ist, haben Sie ein Problem.



Quelle: Paper des BSI (Co-Autor): „Kryptografie quantensicher gestalten – Grundlagen, Entwicklungen, Empfehlungen“ BSI, Oktober 2021; https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Kryptografie-quantensicher-gestalten.pdf?

Die folgenden Fragen zielten darauf ab, von den befragten Organisationen eine Einschätzung der Werte x, y und z aus dem Theorem von Mosca (siehe Box) zu erhalten. Dabei wird die Einschätzung für z gegeben durch die Antwort auf die Frage: „Wann, schätzen Sie, werden Quantencomputer in der Lage sein, relevante, heute eingesetzte kryptografische Verfahren zu brechen?“. Für x ergibt sich die Einschätzung aus den Antworten auf die Frage: „Wie hoch ist die maximale Dauer, für die Informationen durch Ihre Organisation vertraulich bleiben?“. Die Frage nach der Migrationszeit y ist zweigeteilt: Sie setzt sich zusammen aus dem voraussichtlichen Beginn („Wann plant Ihre Organisation, mit der Umstellung auf Post-Quanten-Kryptografie zu beginnen?“) und der Dauer der Migration („Wie lange wird, Ihrer Meinung nach, Ihre Organisation für obige Umstellung benötigen?“).

Abb. 6: Wann, schätzen Sie, werden Quantencomputer in der Lage sein, bestimmte, heute eingesetzte Verfahren zu brechen?

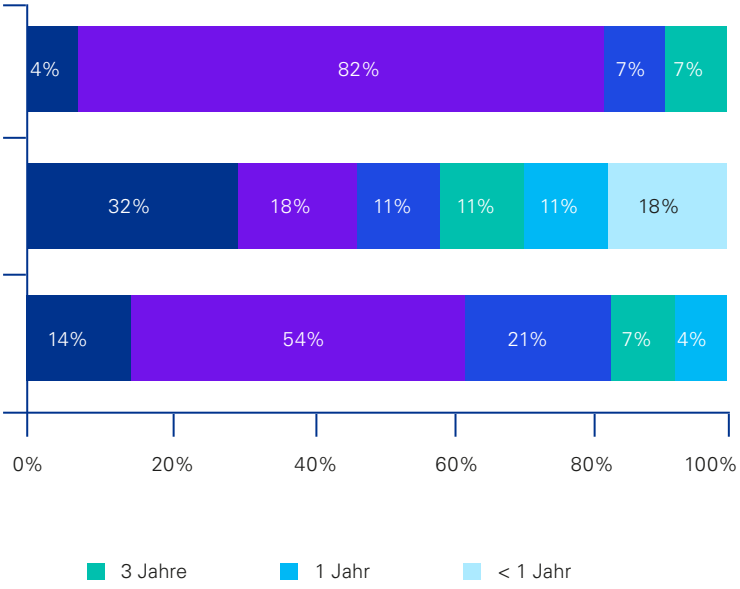


Quelle: KPMG in Deutschland, 2022; Angaben in Prozent, Rundungsdifferenzen möglich

Wie hoch ist die maximale Dauer, für die Informationen durch Ihre Organisationen vertraulich gehalten werden müssen?

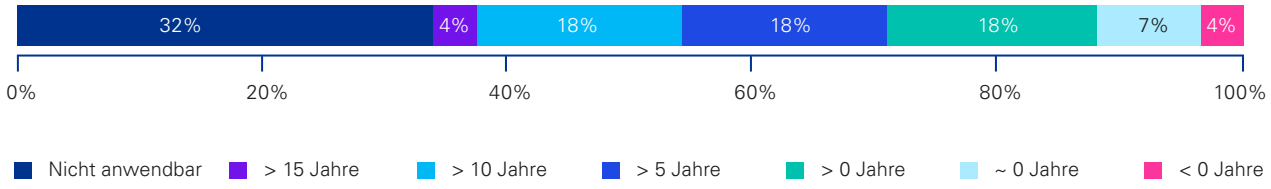
Wann plant Ihre Organisation, mit der Umstellung auf quantensichere Kryptografie zu beginnen?

Wie lange wird, Ihrer Meinung nach, Ihre Organisation für die Realisierung der Quantenresistenz benötigen?



Quelle: KPMG in Deutschland, 2022; Angaben in Prozent, Rundungsdifferenzen möglich

Abb. 7: Geschätzte Zeit, um die der Grenzwert zur sicheren Umstellung auf Post-Quanten-Kryptografie verfehlt wird.



Quelle: KPMG in Deutschland, 2022; Angaben in Prozent, Rundungsdifferenzen möglich

Bei den Antworten zeigt sich, dass 79 % der antwortenden Organisationen damit rechnen, dass Quantencomputer in spätestens zehn Jahren in der Lage sein werden, heute eingesetzte kryptografische Verfahren zu brechen. Und keine Organisation sieht es als ausgeschlossen an, dass dies überhaupt passieren wird.

Zudem legt eine große Mehrheit der Teilnehmenden (89 %) die Dauer, für die Informationen vertraulich bleiben sollen, auf mindestens fünf Jahre fest. Insgesamt ergibt sich so ein Bild, nach dem die antwortenden Organisationen nach eigener Einschätzung die Migration auf quantensichere Kryptografie im Mittel 6,5 Jahre zu spät abgeschlossen haben werden.[3] Wenn vertrauliche Informationen, möglicherweise unbemerkt, jahrelang lesbar sind, kann das dramatische Folgen haben.

Einschätzung

Die Antwort auf die Frage, wann Quantencomputer eine reale Bedrohung für die Public-Key-Kryptografie sein werden, ist eine subjektive Einschätzung der Befragten. Die Bundesregierung und das BSI gehen für den Hochsicherheitsbereich von der Annahme aus, dass mit signifikanter Wahrscheinlichkeit Anfang der 2030er Jahre kryptografisch relevante Quantencomputer verfügbar sein werden. Auch dies ist nicht als Prognose zu verstehen, sondern ist eine Arbeitshypothese für das Risikomanagement. Diese Einschätzung entspricht ungefähr einem Zeitraum von zehn Jahren und wird von einem Großteil der Teilnehmenden (57 %) geteilt. Legt man diesen Wert für z bei allen antwortenden Organisationen an, erhöht sich die Zeit, die die Teilnehmenden zu spät sind, entsprechend zum oben genannten Wert nur unwesentlich auf 7,16 Jahre. Allerdings zeigt sich, dass unter dieser Annahme in keinem der hier betrachteten Fälle Quantensicherheit rechtzeitig erreicht werden würde.

Bei den Antworten zum voraussichtlichen Beginn fällt zudem auf, dass 32 % der Teilnehmenden angegeben haben, dass die Frage „nicht anwendbar/relevant“ sei. Dies steht im Gegensatz dazu, dass nur eine einzelne Organisation angab, keine kryptografischen Verfahren einzusetzen (siehe Abschnitt 4.2). Dies ist bemerkenswert, da die Antwort „nicht anwendbar/relevant“ darauf schließen lässt, dass in den jeweiligen Unternehmen kein Handlungsbedarf in Richtung Migration von Post-Quanten-Kryptografie gesehen wird. Da es eher unwahrscheinlich ist, dass in den entsprechenden Organisationen nur symmetrische Kryptografie eingesetzt wird, werden sie aber voraussichtlich dennoch von der Bedrohung durch Quantencomputing betroffen sein.

[3] Diese Schätzung geht davon aus, dass die Ungleichheitszeichen einer Abweichung von 50 % entsprechen, also geht die Antwort „< 1 Jahr“ als 0,5 Jahre und die Antwort „> 5 Jahre“ als 7,5 Jahre in die Rechnung ein.

4.4 Was wird in den Organisationen unternommen?

Abb. 8: Wird das Thema „Gefährdung der Kryptographie durch Quantencomputing“ im Risikomanagement berücksichtigt?

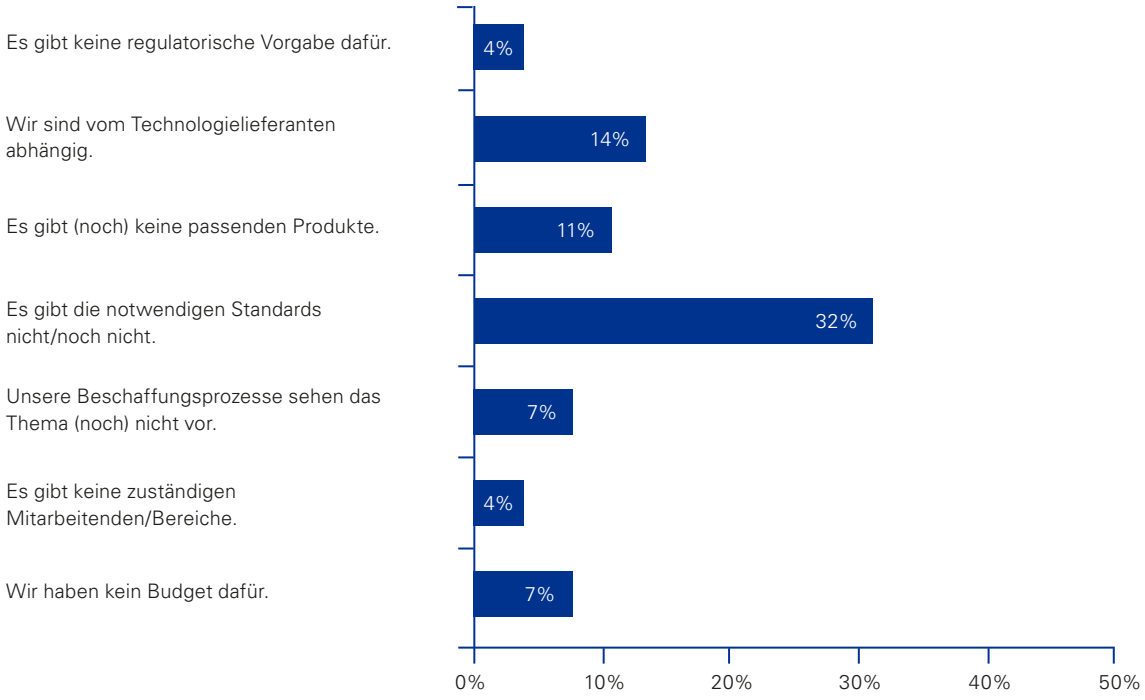
Quelle: KPMG in Deutschland, 2022; Angaben in Prozent, Rundungsdifferenzen möglich

Obwohl, wie in Abschnitt 4.3 beschrieben, die zeitlichen Prognosen mehrheitlich negativ ausfallen, wird das Thema „Gefährdung der Kryptografie durch Quantencomputing“ in einem Großteil der Organisationen (61 %) nicht im Risikomanagement berücksichtigt. Als Hauptgrund werden mehrheitlich die bisher fehlenden Standards (32 %), eine Abhängigkeit von Technologielieferanten (14 %) oder fehlende Produkte (11 %) genannt. Interessant ist, dass die naheliegenden Antworten („Wir haben dafür kein Budget“ und „Es gibt keine zuständigen Mitarbeitenden/Bereiche“) nur selten der Hauptgrund für eine fehlende Betrachtung des Themas im Risikomanagement sind; ersteres wurde von zwei der teilnehmenden Organisationen, letzteres nur von einer einzigen berichtet. Dies könnte ein zusätzliches Zeichen dafür sein, dass jene Befragten, die an der Studie teilgenommen haben, aus einer eher homogenen Gruppe stammen, die sich bereits mit den Gefahren von Quantencomputing für die Kryptografie auseinandergesetzt hat.

Relevanz von Risikomanagement

Um wirtschaftliche und technische Risiken frühzeitig identifizieren, messen, bewerten, dokumentieren und abmildern zu können, wird das Risikomanagement in Unternehmen als zentraler Baustein eingesetzt. Im Interesse des Unternehmens können so Umsatzverluste und hohe Kosten frühzeitig verhindert werden. Erforderliche Prozesse werden im Rahmen des strategischen Controllings etabliert, um die benötigten Daten und Fakten zu erheben und Entscheidungstragenden die notwendigen Informationen zu liefern.

Abb. 9: Falls in Ihrer Organisation keine Initiativen/Vorhaben zu diesem Thema existieren – warum nicht?



Quelle: KPMG in Deutschland, 2022; Angaben in Prozent, Rundungsdifferenzen möglich

Um den aktuellen Fortschritt und mögliche Pläne der Teilnehmenden im Hinblick auf die Migration zur Post-Quanten-Kryptografie zu ermitteln, wurden sie zu einzelnen Handlungsempfehlungen aus dem Ende 2021 veröffentlichten Leitfaden „Kryptografie quantensicher gestalten" des BSI befragt.

Es zeigt sich, dass sich das Thema „Kryptoagilität" schon recht gut durchgesetzt hat, obwohl bei einer anderen Frage die Teilnehmenden angaben, mit dem Begriff eher weniger vertraut zu sein (siehe Abschnitt 4.1): Über ein Drittel der antwortenden Unternehmen gibt an, bereits jetzt darauf zu achten, dass kryptografische Mechanismen möglichst flexibel gestaltet werden, ein knappes Drittel arbeitet daran und von dem restlichen Drittel hat es über die Hälfte zumindest vor. Auch die Mindestlänge von 192 Bit für symmetrische Schlüssel scheint sich durchzusetzen.

Außerdem bereiten fast 50 % der Teilnehmenden den Einsatz von hashbasierten Signaturverfahren für Soft-/Firmwareupdates vor oder setzen diese bereits heute ein.

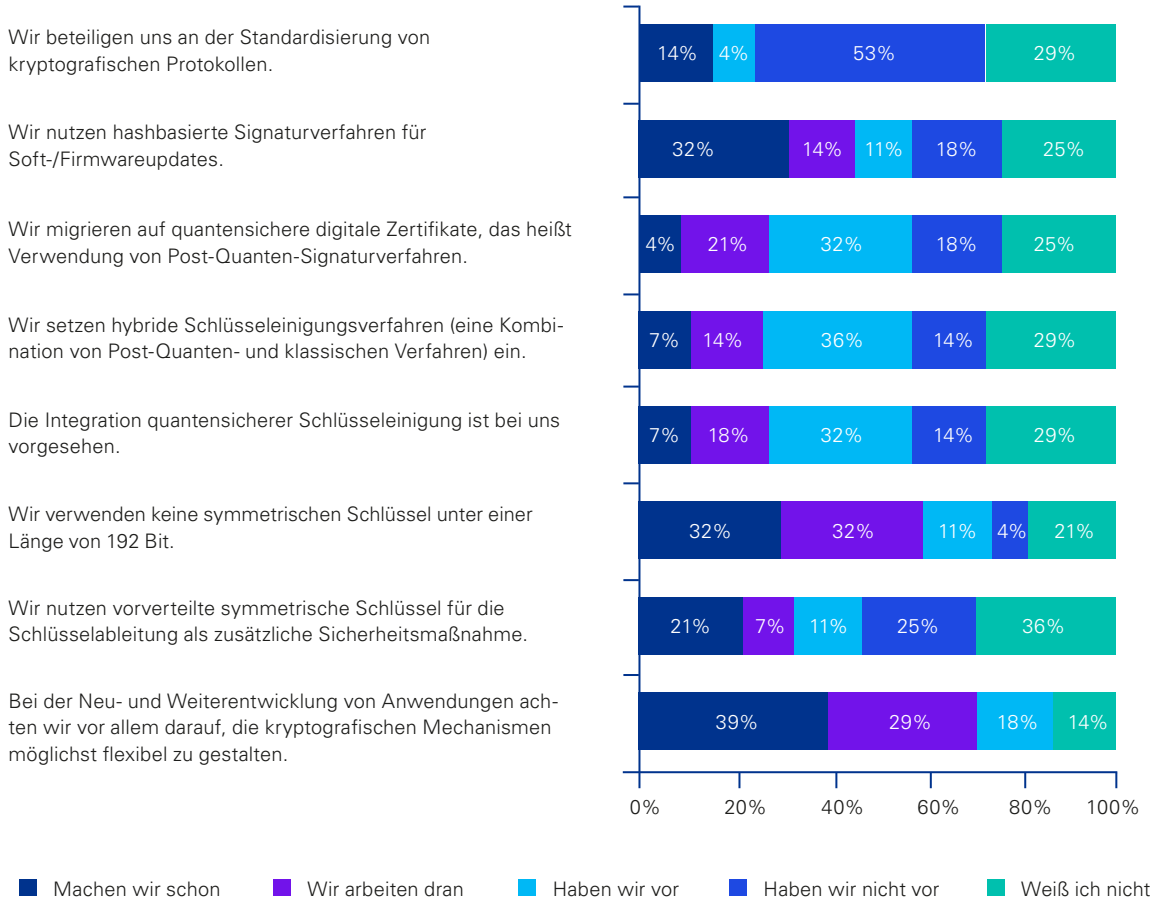
Etwas anders sieht es bei den Empfehlungen zur Public-Key-Kryptografie aus: Quantensichere (hybride) Schlüsseleinigung setzen bisher nur 7 % der Teilnehmenden ein, die Hälfte arbeitet aber daran oder hat es zumindest vor. Auf quantensichere digitale Zertifikate migriert nur ein einzelner.

Eine Mitwirkung bei der Standardisierung von kryptografischen Verfahren haben die meisten Unternehmen zum aktuellen Zeitpunkt außerdem nicht geplant: Über die Hälfte der antwortenden Organisationen gab an, sich nicht an entsprechenden Prozessen zu beteiligen.

Einschätzung

Es stimmt natürlich, dass zurzeit noch kaum Standards (mit Ausnahme hashbasierter Signaturverfahren) zur Post-Quanten-Kryptografie existieren und dementsprechend nur sehr wenige Produkte diese implementiert haben. Dennoch ist eine Vorbereitung und Auseinandersetzung mit dem Thema auch jetzt schon möglich. Dies wird weiter unten vertieft.

Abb. 10: Das BSI hat im Dezember 2021 den Leitfaden „Kryptografie quantensicher gestalten – Grundlagen, Entwicklungen, Empfehlungen" veröffentlicht. Darin werden auch die folgenden Handlungen für die Migration zur Post-Quanten-Kryptografie empfohlen.



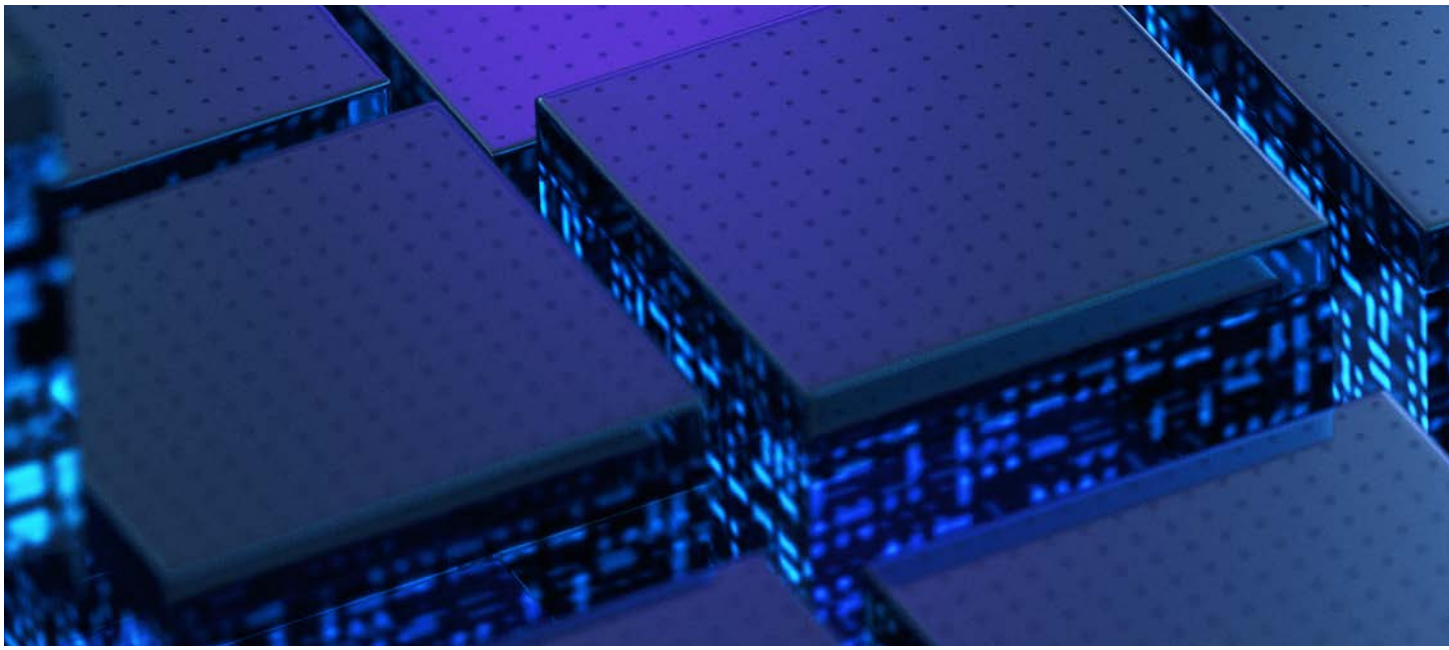
Quelle: KPMG in Deutschland, 2022; Angaben in Prozent, Rundungsdifferenzen möglich

Einschätzung

Die Ergebnisse legen nahe, dass sich ungefähr die Hälfte der antwortenden Unternehmen bewusst ist, welche Schritte für die Migration zur Post-Quanten-Kryptografie notwendig sind. Eine Umsetzung der Handlungsempfehlungen des BSI steht, bis auf einige Ausnahmen, allerdings noch aus.

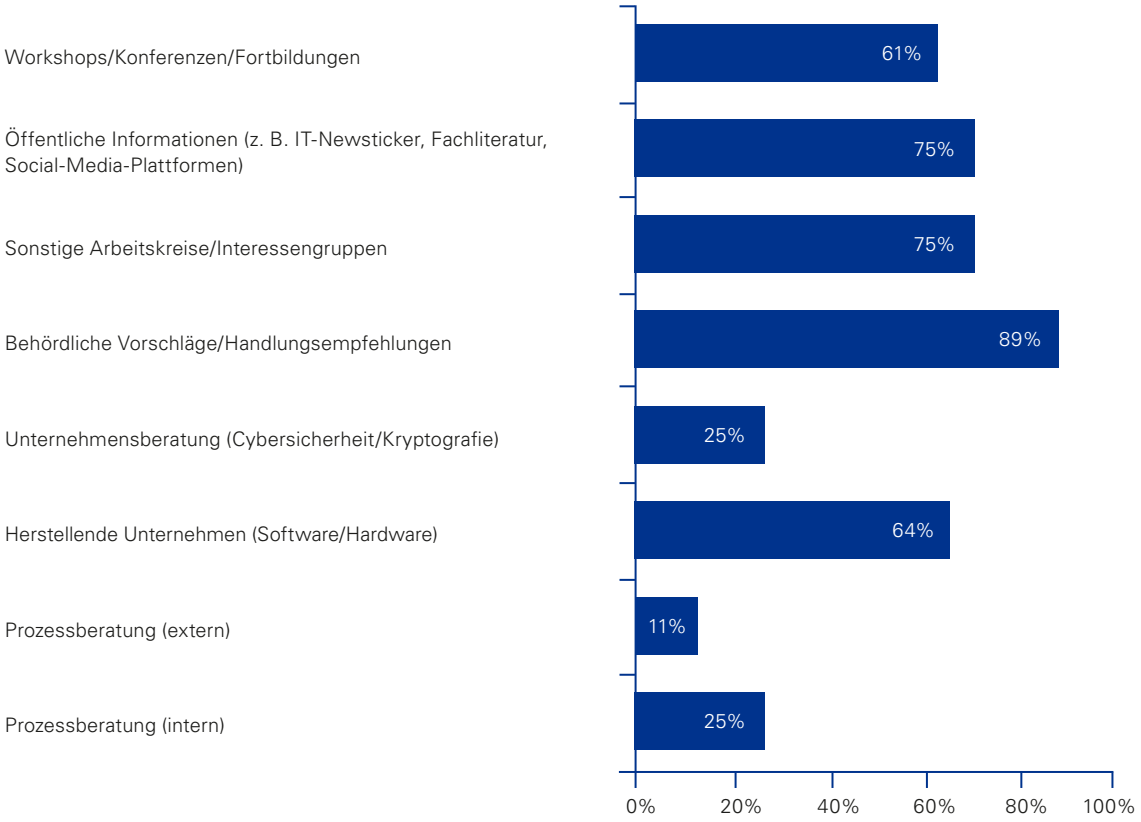
Der BSI-Leitfaden und die Empfehlungen zum Quantencomputing haben ein deutliches Echo erzeugt. Wir sind mit diesem Thema am Puls der Zeit. Lassen Sie uns die Zeit jetzt nutzen, die Grundlagen und Anwendungen weiter voranzutreiben und dafür zu sorgen, dass quantensichere Kryptografie Einzug in die aktive Nutzung findet.

Dr. Günther Welsch
Abteilungsleiter Krypto-Technik und IT-Management, BSI



4.5 Welche Unterstützung benötigen die Unternehmen für weitere Schritte?

Abb. 11: Welche Unterstützung nutzen Sie/planen Sie zu nutzen?



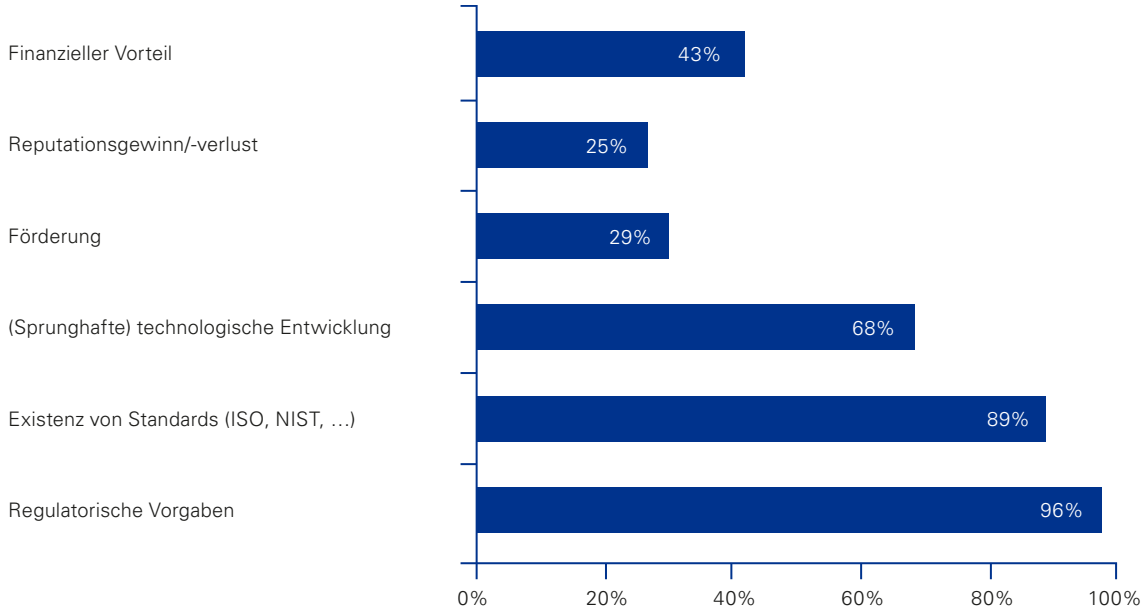
Quelle: KPMG in Deutschland, 2022; Angaben in Prozent, Rundungsdifferenzen möglich

Die bisherigen Ergebnisse legen nahe, dass zur vollständigen Umstellung auf Post-Quanten-Kryptografie noch Arbeit erforderlich ist. Dazu befragt, welche Unterstützung sie dafür nutzen bzw. zu nutzen planen, antworteten die meisten Teilnehmenden (89 %), sich auf behördliche Handlungsempfehlungen zu beziehen. Sonstige Arbeitskreise und Interessengruppen lagen als Unterstützung gleichauf mit öffentlichen Informationen (IT Newsticker, Fachliteratur, Social Media…); beides wurde jeweils von 75 % der Teilnehmenden genannt. Die Hersteller von Hard- und Software sowie das Besuchen von Konferenzen, Workshops und Fortbildungen nannten noch 64 % bzw. 61 %.
Die meisten Teilnehmenden sahen die Verantwortung für die Behandlung des Risikos, das durch Quantencomputing für die Kryptografie entsteht, bei sich selbst; 79 % für die eigenen Produkte, 93 % für die eigenen Prozesse.

Einschätzung

Es ist also konsistent, dass die Teilnehmenden hauptsächlich Interesse an Unterstützungsangeboten bekunden, die sie selbst umsetzen können. Daraus kann man schlussfolgern, dass Aufklärungskampagnen und öffentlich zugängliche Informationen eine nicht zu unterschätzende Rolle in der großflächigen Umstellung auf quantensichere Kryptografie zu spielen haben. Über öffentliche Kanäle sollten die Verantwortlichen in den Organisationen in die Lage versetzt werden, Quantensicherheit bei sich selbst herzustellen. Öffentlich zugängliche und verständliche Leitfäden sowie Best-Practice-Empfehlungen könnten ein wirkungsvolles Mittel sein, diesen Prozess weiter voranzutreiben. Die relativ geringe Vertrautheit mit Store-now-decrypt-later und dem Begriff Kryptoagilität (siehe oben) deutet darauf hin, dass dies schon heute relevant ist.

Abb. 12: Was würde Investitionsentscheidungen Ihrer Organisation begünstigen?



Quelle: KPMG in Deutschland, 2022; Angaben in Prozent, Rundungsdifferenzen möglich

Um weiter einzukreisen, was die Organisationen benötigen, um ihre Kryptosysteme quantensicher zu machen, wurden die Teilnehmenden gefragt, welche Aspekte ihrer Meinung nach Investitionsentscheidungen begünstigen würden. Zwei Antworten stachen dabei besonders hervor: Regulatorische Vorgaben wurden von 96 % der Teilnehmenden genannt, die Existenz von Standards (ISO, NIST,…) von 89 %. Sprunghafte technologische Entwicklungen wurden noch von 68 % der Teilnehmenden angeführt. Klassische Motivatoren, wie finanzielle Vorteile, Reputation oder Förderungen, wurden von weniger Teilnehmenden genannt (43 %, 29 % bzw. 25 %).

Diese Einschätzungen decken sich zum einen damit, dass die Erfüllung von regulatorischen Vorgaben und Datenschutzanforderungen als einer der häufigsten Einsatzzwecke von Kryptografie genannt wurde und zum anderen damit, dass 32 % der Teilnehmenden angaben, dass der Hauptgrund für fehlende Initiativen in ihrer Organisation das Fehlen von Standards sei. Auch, dass mangelndes Budget und Personal sehr selten (von einer bzw. zwei der teilnehmenden Organisationen) als Gründe dafür genannt wurden, dass keine Initiativen zu dem Thema existieren, und die Tatsache, dass finanzieller Förderung nur eine geringe Zugkraft zugetraut wird, erscheinen konsistent.

Einschätzung

Dass klassische wirtschaftliche Faktoren vergleichsweise selten genannt wurden, kann so aufgefasst werden, dass es nicht an Motivation mangelt, sich den Herausforderungen, die mit Quantencomputing einhergehen, zu stellen. Das deckt sich mit der hohen Relevanz, die die Teilnehmenden dem Thema zuschreiben. Allerdings könnte dies auch auf die Vermutung zurückzuführen sein, dass die teilnehmenden Personen möglicherweise aus einer homogenen, grundsätzlich an dem Thema interessierten Gruppe stammen.

Die gute Nachricht ist, dass die Standardisierung von Post-Quanten-Kryptografie vorangeht. NIST hat im Juli eine erste Entscheidung über künftige Standards getroffen und wird bald erste Drafts veröffentlichen. Es ist anzunehmen, dass andere Organisationen diese übernehmen und bald nachziehen werden. Das BSI hat bereits im Frühjahr 2020 erste quantensichere Verfahren zur Schlüsseleinigung empfohlen. Kürzlich wurde in der ISO/IEC SC27 WG2 nach einem Vorstoß des BSI ein Preliminary Work Item für das Projekt „Inclusion of key encapsulation mechanisms for PQC in ISO/IEC standards“ ins Leben gerufen und zu Beiträgen von Expertinnen und Experten aufgerufen. Aus diesem Projekt könnten ISO-Standards für FrodoKEM und Classic McEliece hervorgehen. Laut den Teilnehmenden sind aber auch Regulierungsbehörden gefragt, bei Vorgaben in kritischen und betroffenen Bereichen die Quantensicherheit kryptografischer Lösungen zu bedenken.

Die Ergebnisse dieser Umfrage zeigen mir, dass sich bisher nur wenige Leute mit unserem Thema beschäftigen, diese dann aber die Bedrohung der Kryptografie durch Quantencomputing sehr ernst nehmen. Das lässt für mich nur einen Schluss zu: Wir brauchen mehr Leute, die sich auskennen. Und das muss dringend auch die Entscheidungstragenden mit einschließen.

Dr. Frank Damm
KPMG in Deutschland
Senior Manager

5. Fazit, Handlungsempfehlungen und Ausblick

Zeitskalen

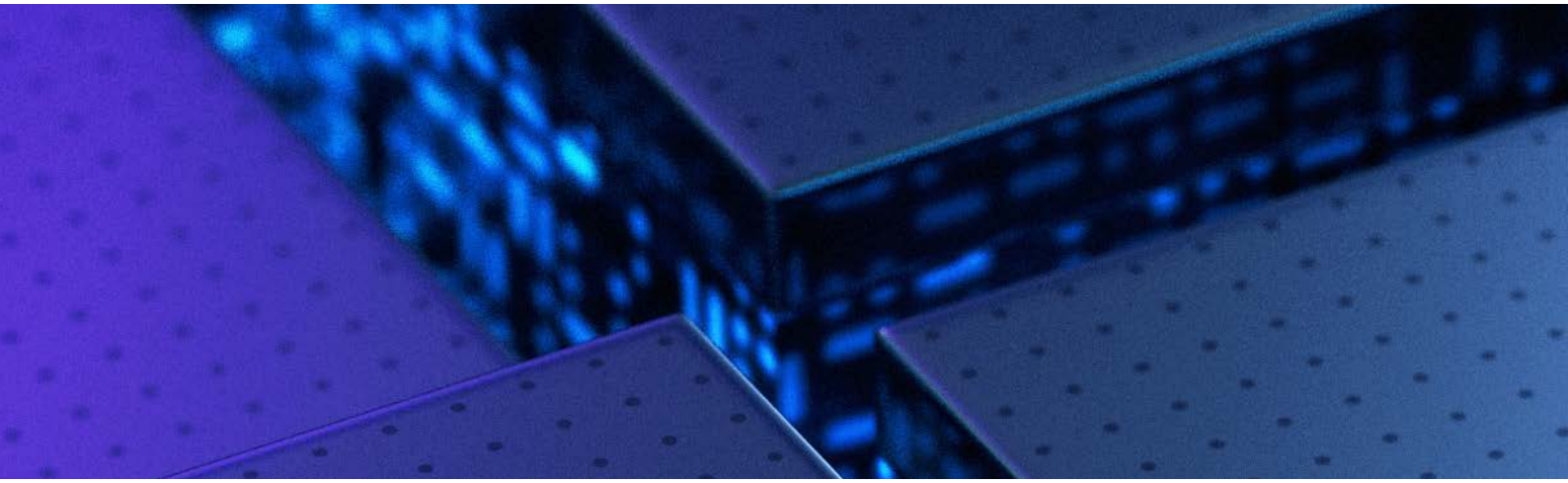
Das BSI warnt schon seit Jahren vor der Bedrohung der Public-Key-Kryptografie durch Quantencomputing und hat für den Hochsicherheitsbereich bereits die Migration zu quantensicheren Lösungen eingeleitet. Grundlage hierfür ist folgende Arbeitshypothese: Im staatlichen Hochsicherheitsbereich wird unter der Hypothese gearbeitet, dass Anfang der 2030er Jahre kryptografisch relevante Quantencomputer zur Verfügung stehen werden[4]. Diese Aussage ist nicht als Prognose zur Verfügbarkeit von Quantencomputern zu verstehen, sondern stellt einen Richtwert für die Risikobewertung dar.

Dieser Richtwert deckt sich mit den Einschätzungen der Teilnehmenden. Im Mittel erwarten diese, dass Quantencomputer in 10,4 Jahren in der Lage sein werden, aktuell eingesetzte kryptografische Verfahren zu brechen; nach eigener Einschätzung würden sie damit – wie in Abschnitt 4.3 beschrieben – die Migration auf quantensichere Kryptografie 6,5 Jahre zu spät abgeschlossen haben. Folgt man Moscas Theorem[5] erkennt man, dass nur 11 % der Teilnehmenden eine Chance sehen, Quantensicherheit zu erreichen, bevor die Vertraulichkeit ihrer Daten verletzt wird.

Beinahe 90 % der Teilnehmenden erwarten, den Gefährdungen der Kryptografie durch die aufkommenden Quantencomputer nicht gewachsen zu sein. Es besteht also ein gravierender Handlungsbedarf, um zu verhindern, dass die Vertraulichkeit von Daten maßgeblich kompromittiert wird.

Dabei bewerteten 97 % der Teilnehmenden die generelle Relevanz von Quantencomputing für die Sicherheit von heute eingesetzten kryptografischen Verfahren als „hoch“ oder „eher hoch“; für das durchschnittliche Risiko der Daten in der eigenen Organisation galt das noch für 65 %.

[4] https://dserver.bundestag.de/btd/19/252/1925208.pdf, abgerufen am 20.03.2023
[5] https://eprint.iacr.org/2015/1075.pdf, abgerufen am 20.03.2023



Behandlung

Dennoch wird die Gefährdung durch Quantencomputing nur von 25 % der antwortenden Organisationen im Risikomanagement berücksichtigt. Zudem gaben 32 % der Teilnehmenden an, dass die Frage, wann ihre Organisation plane, mit der Umstellung zu beginnen, bei ihnen „nicht anwendbar/relevant“ sei. Dies legt nahe, dass in diesen Fällen eine Umstellung noch nicht einmal geplant ist.

Nach Faktoren befragt, die Investitionsentscheidungen für quantensichere Kryptografie begünstigen würden, nannten 96 % regulatorische Vorgaben und noch 89 % die Existenz von Standards.

Auch wenn die notwendigen Standards noch nicht existieren, kann die Umstellung der eingesetzten Kryptografie schon jetzt geplant und begonnen werden. Vernachlässigt man die Zeit bis zum geplanten Beginn der Umstellung in obiger Überlegung, würden immerhin 32 % der Teilnehmenden erwarten, rechtzeitig Quantensicherheit zu erreichen.

Zudem können schon jetzt Maßnahmen getroffen werden, um die Zeit, die für die Umstellung benötigt wird, zu verkürzen. Exemplarisch sei an dieser Stelle die Einführung und Pflege eines Kryptoinventars genannt. Eine detaillierte Aufstellung, welche kryptografischen Verfahren in einer Organisation eingesetzt werden und wo diese Verwendung finden, erlaubt es, die Gefährdung mit relativ wenig Aufwand im Risikomanagement zu berücksichtigen. Der Leitfaden „Kryptografie quantensicher gestalten – Grundlagen, Entwicklungen, Empfehlungen“ des BSI nennt noch weitere Maßnahmen, um solcherlei Bemühungen zu unterstützen. Einige der dort genannten Vorschläge, wie Kryptoagilität und die Nutzung hashbasierter Signaturverfahren, haben laut dieser Umfrage schon eine relativ hohe Durchdringung erreicht. Allerdings weisen die Antworten der Teilnehmenden darauf hin, dass das bisher Erreichte nicht ausreichend ist.

Zusätzlich ist es schon jetzt möglich, Vorkehrungen zu treffen, um damit umzugehen, dass Quantensicherheit nicht rechtzeitig erreicht wird. Auch hier würde ein entsprechendes Risikomanagement dabei helfen, die notwendigen Pläne für den Eventualfall zu entwickeln.

Awareness

Mit 28 Rückmeldungen fiel die Teilnahmequote deutlich geringer aus als beispielsweise bei einer vergleichbaren Studie zum Thema „Schwachstellenmanagement“. Diejenigen, die an der Umfrage teilnahmen, scheinen allerdings über einiges Wissen über Quantencomputing und Kryptografie zu verfügen. Die Einschätzungen von 71 % der Teilnehmenden zu der erwarteten Auswirkung der Verfügbarkeit ausreichend leistungsfähiger Quantencomputer deckt sich mit der gängigen Expertenmeinung. Im Durchschnitt gaben die Teilnehmenden an, mit den abgefragten Teilaspekten des Themas „eher vertraut“ zu sein.

Zusammengenommen zeichnen diese Aspekte das Bild, dass die Teilnehmenden aus einer Personengruppe stammen, die sich von vornherein für die Themen Quantencomputing und Kryptografie interessiert und die Konsequenzen von ausreichend leistungsfähigen Quantencomputern auf die Sicherheit als dramatisch ansieht. Dies ist konsistent mit dem Ergebnis, dass die Risikoeinschätzung der Teilnehmenden mit deren Vertrautheit mit der Materie korreliert.

Dies deutet darauf hin, dass der Aufklärung eine nicht zu unterschätzende Rolle dabei zukommt, die Vertraulichkeit und Integrität von sensiblen Daten und Informationen langfristig zu sichern; angefangen vom Vermitteln eines angemessenen Risikobewusstseins über Vertraulichkeitsanforderungen bestimmter Datentypen bis zu Methoden zur Behandlung der Risiken. Auch das Management sollte entsprechend geschult und mit einem entsprechenden Risikobewusstsein ausgestattet werden. Und schlussendlich kann der Ruf nach Regulatorik in diesem Kontext nur beantwortet werden, wenn auch politische Entscheidungen in dem Bewusstsein einer aufkeimenden Bedrohung getroffen werden.

Politische Vorgaben notwendig?

In den USA gibt es bereits politische Vorgaben zur Quantensicherheit. Im Januar 2022 hat das Weiße Haus ein Memorandum veröffentlicht, in dem die Ministerien und Sicherheitsbehörden aufgefordert wurden, innerhalb von 180 Tagen alle nicht quantensicheren Verschlüsselungsverfahren in Nationalen Sicherheitssystemen (NSS) zu identifizieren und einen Zeitplan zur Migration[6] zu erstellen. Bis 2035 soll in den USA die Migration zu quantensicherer Kryptografie weitestgehend abgeschlossen sein.

In Deutschland und Europa konzentrieren sich die Aktivitäten zum Thema Quantentechnologien zurzeit insbesondere darauf, bei der Entwicklung von Quantencomputern und auch im Bereich Quantenkommunikation den Anschluss an die führenden Nationen zu halten. Aber auch von der deutschen Regierung werden die Auswirkungen von Quantencomputing auf die Kryptografie immer ernster genommen. In seiner Cybersicherheitsagenda hat das Bundesministerium des Inneren und für Heimat (BMI) auch die Investition in Post-Quanten-Kryptografie als Maßnahme für die 20. Legislaturperiode formuliert“[7].

Es bleibt abzuwarten, welche weiteren technischen, wissenschaftlichen und politischen Entwicklungen zu diesem Thema auf uns zukommen werden. Eins aber ist sicher: Post-Quanten-Kryptografie wird über kurz oder lang zum Standard werden. Es ist ratsam, sich rechtzeitig mit der Migration oder zumindest – wenn diese nicht rechtzeitig erfolgt – den möglichen Konsequenzen auseinanderzusetzen.

Wenn ich den Unternehmen und Organisationen drei Dinge raten könnte, um sich schon jetzt auf Quantensicherheit vorzubereiten, wären es diese:

- **Berücksichtigen Sie diese Bedrohung in Ihrem Risikomanagement**
- **Erstellen Sie ein Kryptoinventar**
- **Berücksichtigen Sie Kryptoagilität**

Dr. Gerhard Schabhüser
Vizepräsident, BSI

[6] https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/, abgerufen am 20.03.2023
[7] https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/themen/sicherheit/cybersicherheitsagenda-20-legislatur.pdf?__blob=publicationFile&v=4, abgerufen am 20.03.2023

Kontakt

KPMG AG
Wirtschaftsprüfungsgesellschaft
Klingelhöferstraße 18
10785 Berlin

Bundesamt für Sicherheit in
der Informationstechnik
Postfach 200363
53133 Bonn
T +49 228 99 9582-0
bsi@bsi.bund.de

Hans-Peter Fischer
Partner
T +49 69 9587-2404
hpfischer@kpmg.com

Dr. Heike Hagemeier
Referat TK 21 – Technologie- und Forschungsstrategie
T +49 228 99 9582-5968
heike.hagemeier@bsi.bund.de

Dr. Frank Damm
Senior Manager
T +49 221 2073-5728
fdamm@kpmg.com

Dr. Manfred Lochter
Referat KM 21 – Vorgaben an und Entwicklung von Kryptoverfahren
T +49 228 99 9582-5643
manfred.lochter@bsi.bund.de

www.kpmg.de

www.kpmg.de/socialmedia

www.bsi.bund.de

https://bsi.bund.de/dok/520160