Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Kryptografie quantensicher gestalten

Dr. Heike Hagemeier, BSI, Referat TK 21

Omnisecure 2022, Berlin, 22.06.22

Wie viel Zeit bleibt für die Migration auf quantensichere Kryptografie?

Das hängt von folgenden Faktoren ab:

- Wie lange sollen Ihre Daten sicher bleiben? (X Jahre)
- Wie lange dauert die Umstellung Ihrer Systeme auf quantensichere Kryptografie? (Y Jahre)
- Wie lange wird es dauern, bis leistungsstarke Quantencomputer gebaut werden? (Z Jahre)

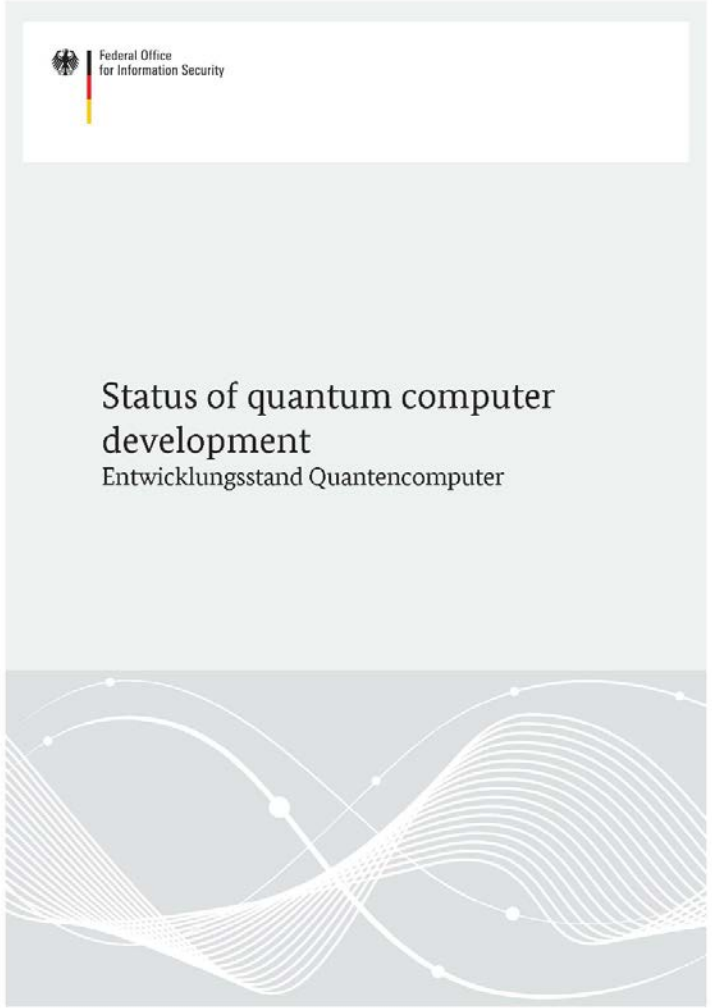
Theorem (Mosca): Wenn X + Y > Z, dann haben Sie ein Problem!

Wie groß ist Z?

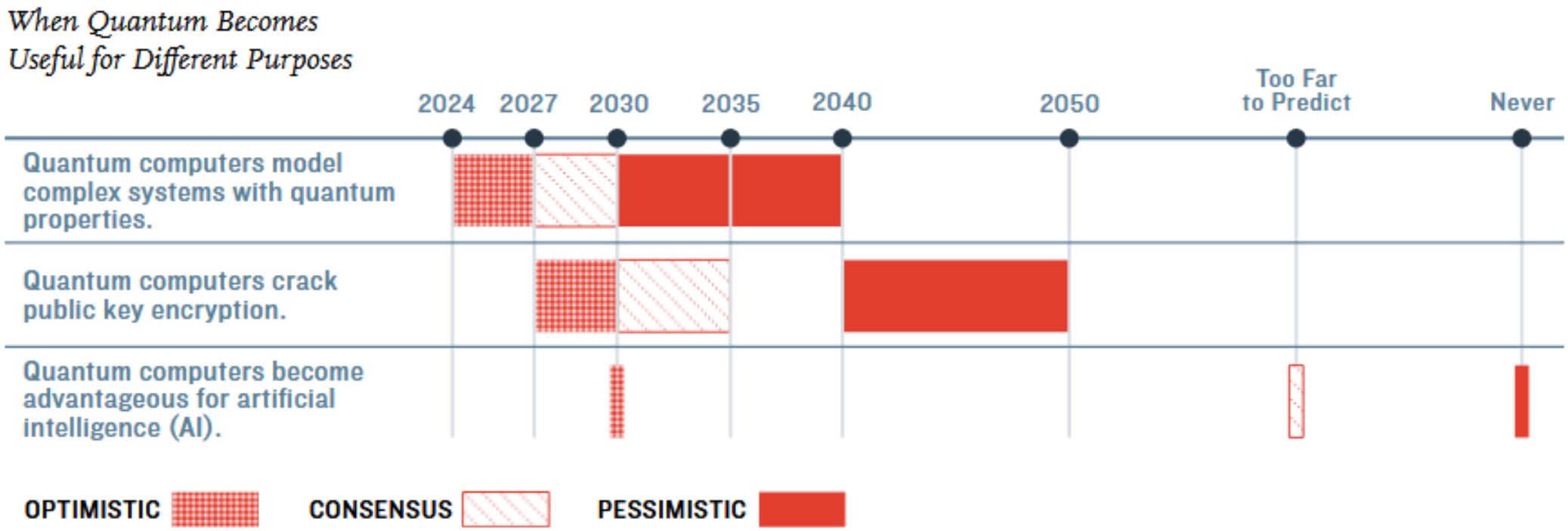
(Wie lange wird es dauern, bis ein leistungsfähiger Quantencomputer zur Verfügung steht?)

Studie „Entwicklungsstand Quantencomputer“

- Studie im Auftrag des BSI
- Durchgeführt 2018 unter Leitung von Prof. Wilhelm-Mauch (Universität des Saarlandes)
- Zwei Revisionen: 2019, 2020
- Aktueller Stand verfügbar unter www.bsi.bund.de/qcstudie
- Aktuelles BSI-Projekt: Erneute Aktualisierung
- Leitung wieder Prof. Wilhelm-Mauch (jetzt FZ Jülich)
- Themenschwerpunkte:
  - NISQ
  - Fehlerkorrektur
  - „Rahmenbedingungen“



Report von Booz Allen Hamilton (Januar 2022)



Wie groß ist X?

(Wie lange müssen Ihre Daten vertraulich bleiben?)

Verschiedene Bedrohungsszenarien

Vertraulichkeit

- „Store now, decrypt later“ **Bedrohung**

➢ Verschlüsselung und Schlüsseleinigung(!) muss so lange sicher sein, wie die zu schützenden Daten vertraulich bleiben sollen.

Authentizität

- Signaturen müssen meist nur kurzfristig sicher sein, Problem bei langen Laufzeiten von Zertifikaten
- Migration der Systeme voraussichtlich sehr aufwändig

➢ rechtzeitiger Umstieg notwendig

Wie groß ist Y?

(Wie lange dauert die Umstellung auf quantensichere Kryptografie?)

NIST-Standardisierung

"A long and winding road"

Weitere notwendige Schritte für …

… **die Migration zu Post-Quanten-Kryptografie**:

- Erweiterung kryptografischer Protokolle
- Anpassung digitaler Zertifikate und von PKIen
- Implementierung in Kryptobibliotheken
- Implementierung in Produkten
- ….

… **die Einsatzreife von Quantum Key Distribution**:

- Sicherheitsuntersuchungen
- Standardisierung von Protokollen
- Erarbeitung zugehöriger Sicherheitsbeweise
- Zertifizierung von Produkten

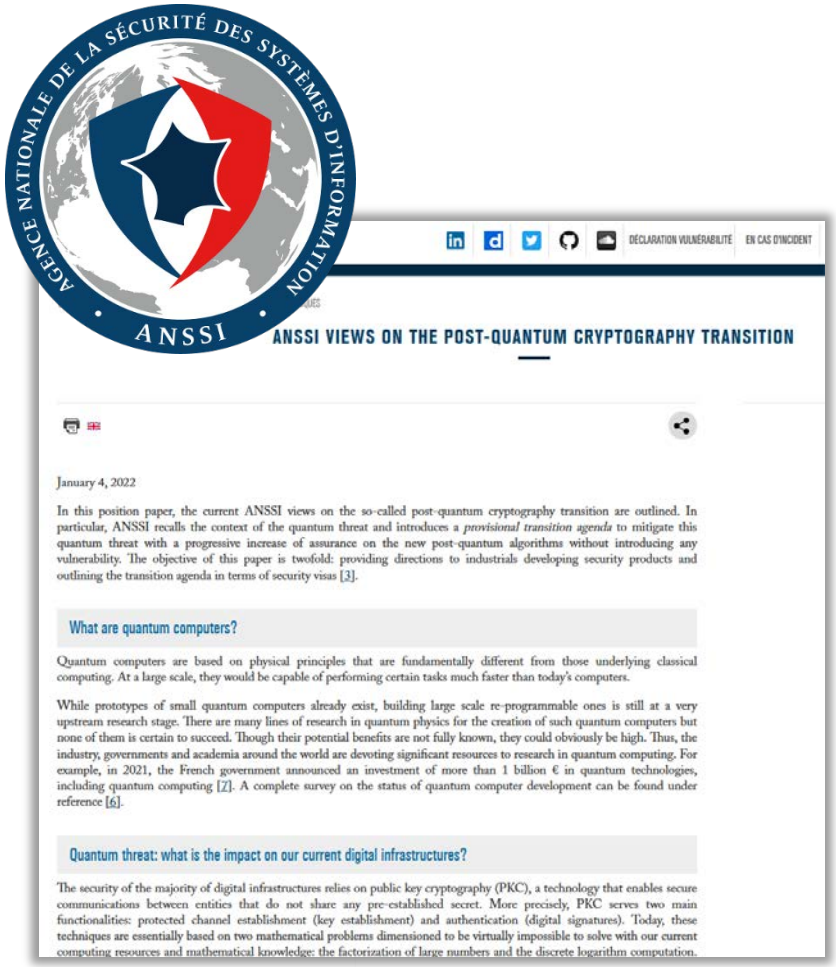
Empfehlungen und Aktivitäten des BSI

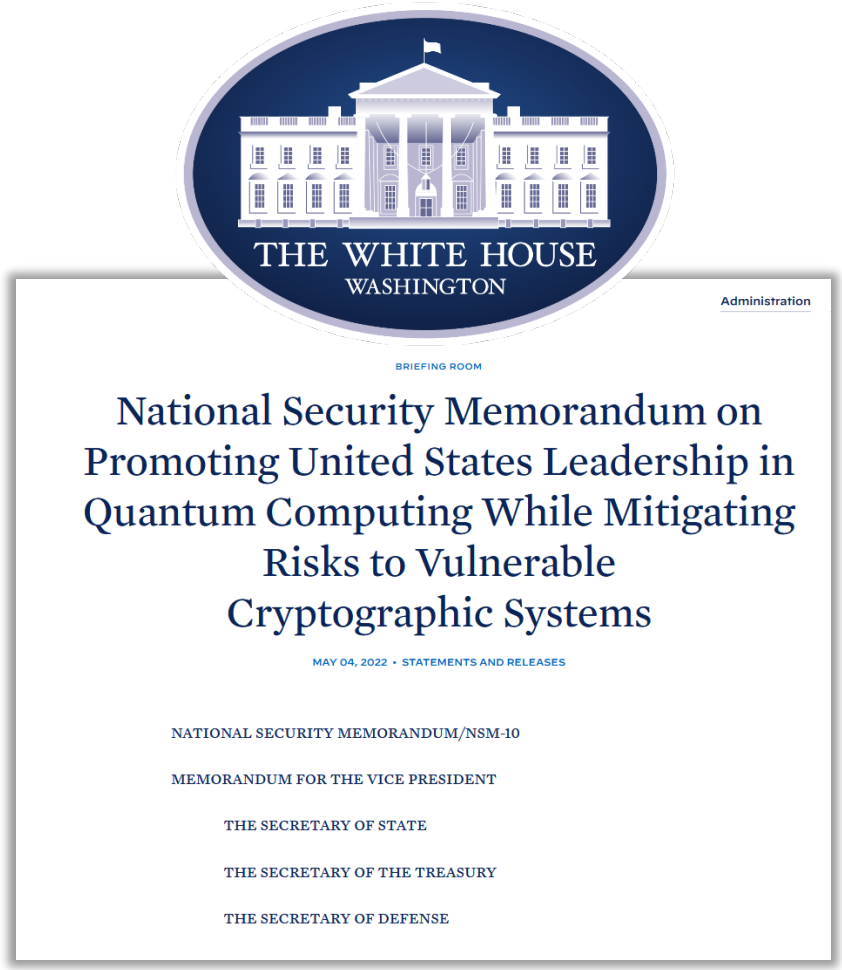
BSI-Leitfaden „Kryptografie quantensicher gestalten“

- Aktualisiert und erweitert die Handlungsempfehlungen „Migration zu Post-Quanten-Kryptografie“
- Hintergründe zu Quantencomputern, Post-Quanten-Kryptografie und Quantum Key Distribution
- Empfehlungen u.a.
  - Rechtzeitige Risikoanalyse
  - Kryptoagilität
  - Hybride Lösungen
  - Vorrang Migration zu Post-Quanten-Kryptografie vor Quantum Key Distribution
  - Weitere Forschung und Dialog notwendig!

Verfügbar unter www.bsi.bund.de/PQ-Migration

Internationale Aktivitäten und Empfehlungen



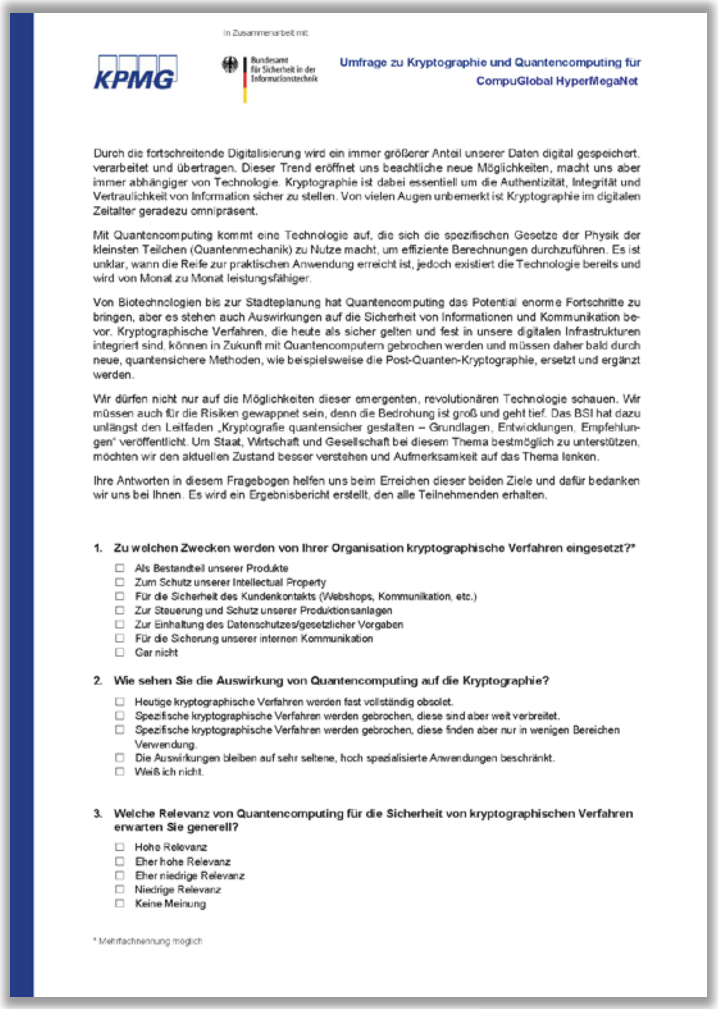


Umfrage „Kryptografie und Quantencomputing“

Umfrage von KPMG, Deutschland und BSI zu Kryptografie und Quantencomputing

- Basiert auf dem BSI-Leitfaden "Kryptografie quantensicher gestalten".
- Richtet sich an alle interessierten Unternehmen und Organisationen (insb. an das Produktmanagement für Sicherheitsfunktionen, CISO's oder CIO's).
- Jede teilnehmende Organisation erhält einen individualisierten Ergebnisbericht.
- **Ziel: Erhöhung der Awareness zum Thema quantensichere Kryptografie und einen Überblick über die Lage in Deutschland erhalten.**

Allianz für Cyber-Sicherheit



In Zusammenarbeit mit:

KPMG

Bundesamt für Sicherheit in der Informationstechnik

Umfrage zu Kryptographie und Quantencomputing für CompuGlobal HyperMegaNet

Durch die fortschreitende Digitalisierung wird ein immer größerer Anteil unserer Daten digital gespeichert, verarbeitet und übertragen. Dieser Trend eröffnet uns beachtliche neue Möglichkeiten, macht uns aber immer abhängiger von Technologie. Kryptographie ist dabei essentiell um die Authentizität, Integrität und Vertraulichkeit von Information sicher zu stellen. Von vielen Augen unbemerkt ist Kryptographie im digitalen Zeitalter geradezu omnipräsent.

Mit Quantencomputing kommt eine Technologie auf, die sich die spezifischen Gesetze der Physik der kleinsten Teilchen (Quantenmechanik) zu Nutze 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 hat Quantencomputing das Potential enorme Fortschritte zu bringen, aber es stehen auch Auswirkungen auf die Sicherheit von Informationen und Kommunikation bevor. Kryptographische Verfahren, die heute als sicher gelten und fest in unsere digitalen Infrastrukturen integriert sind, können in Zukunft mit Quantencomputern gebrochen werden und müssen daher bald durch neue, quantensichere Methoden, wie beispielsweise die Post-Quanten-Kryptographie, ersetzt und ergänzt werden.

Wir dürfen nicht nur auf die Möglichkeiten dieser emergenten, revolutionären Technologie schauen. Wir müssen auch für die Risiken gewappnet sein, denn die Bedrohung ist groß und geht tief. Das BSI hat dazu unlängst den Leitfaden „Kryptografie quantensicher gestalten – Grundlagen, Entwicklungen, Empfehlungen“ veröffentlicht. Um Staat, Wirtschaft und Gesellschaft bei diesem Thema bestmöglich zu unterstützen, möchten wir den aktuellen Zustand besser verstehen und Aufmerksamkeit auf das Thema lenken.

Ihre Antworten in diesem Fragebogen helfen uns beim Erreichen dieser beiden Ziele und dafür bedanken wir uns bei Ihnen. Es wird ein Ergebnisbericht erstellt, den alle Teilnehmenden erhalten.

1. **Zu welchen Zwecken werden von Ihrer Organisation kryptographische Verfahren eingesetzt?***
   - ☐ Als Bestandteil unserer Produkte
   - ☐ Zum Schutz unserer Intellectual Property
   - ☐ Für die Sicherheit des Kundenkontakts (Webshops, Kommunikation, etc.)
   - ☐ Zur Steuerung und Schutz unserer Produktionsanlagen
   - ☐ Zur Einhaltung des Datenschutzes/gesetzlicher Vorgaben
   - ☐ Für die Sicherung unserer internen Kommunikation
   - ☐ Gar nicht
2. **Wie sehen Sie die Auswirkung von Quantencomputing auf die Kryptographie?**
   - ☐ Heutige kryptographische Verfahren werden fast vollständig obsolet.
   - ☐ Spezifische kryptographische Verfahren werden gebrochen, diese sind aber weit verbreitet.
   - ☐ Spezifische kryptographische Verfahren werden gebrochen, diese finden aber nur in wenigen Bereichen Verwendung.
   - ☐ Die Auswirkungen bleiben auf sehr seltene, hoch spezialisierte Anwendungen beschränkt.
   - ☐ Weiß ich nicht.
3. **Welche Relevanz von Quantencomputing für die Sicherheit von kryptographischen Verfahren erwarten Sie generell?**
   - ☐ Hohe Relevanz
   - ☐ Eher hohe Relevanz
   - ☐ Eher niedrige Relevanz
   - ☐ Niedrige Relevanz
   - ☐ Keine Meinung

* Mehrfachnennung möglich

Bundesamt für Sicherheit in der Informationstechnik

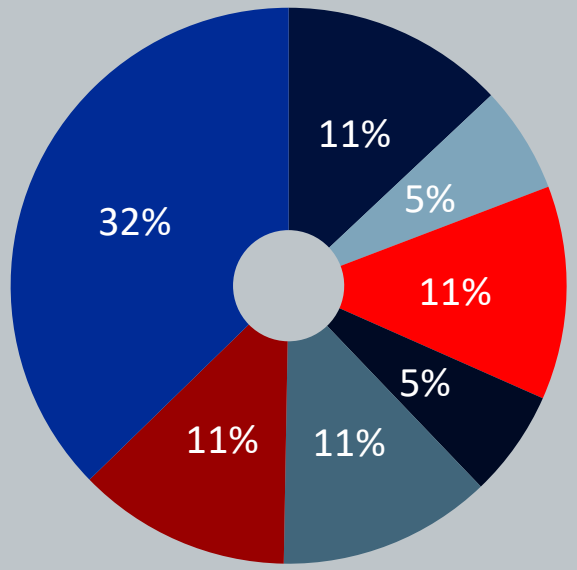
Kontakt: kryptoawareness@bsi.bund.de

Deutschland Digital•Sicher•BSI•

Erste vorläufige(!) Ergebnisse

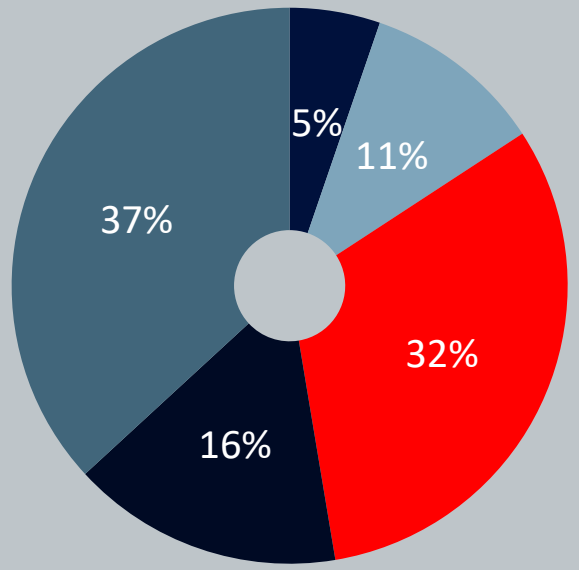
Übersicht – Demografische Daten (Stand 17.6.22)

Branche



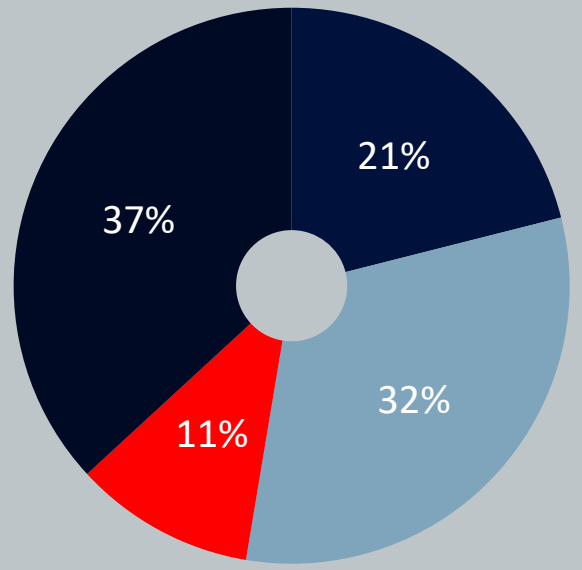
- Chemicals & Pharmaceuticals
- Technology
- Energy & Natural Resources
- Telecommunications
- Government
- Industrial Manufacturing
- Transport & Logistics/Leisure
- Banking

Anzahl Mitarbeitende



- Weniger als 100
- Zwischen 100 und 1000
- Zwischen 1000 und 10000
- Zwischen 10000 und 50000
- Mehr als 50000

Gesamtumsatz



- Bis 1 Mrd. Euro
- Zwischen 1 und 10 Mrd. Euro
- Zwischen 10 und 50 Mrd. Euro
- Mehr als 50 Mrd. Euro

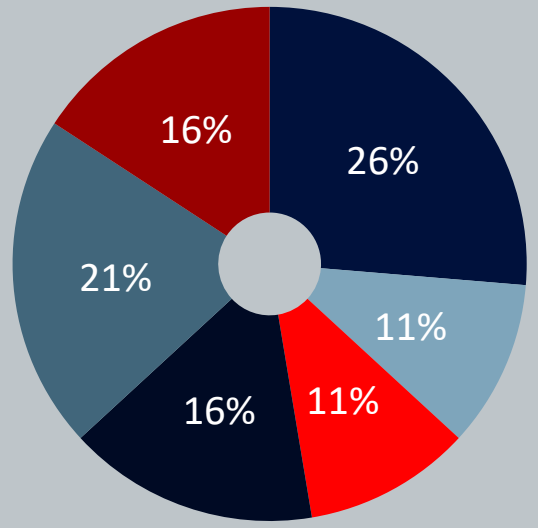
© [year] [legal member firm name]. a [jurisdiction] [legal structure] and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited. a private English company limited by guarantee. All rights reserved.

Einschätzung zur zeitlichen Entwicklung (Stand 17.6.22)

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

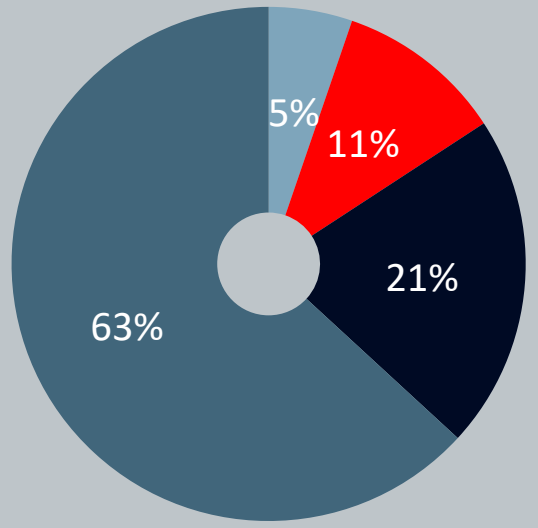
- <1 Jahr
- 1 Jahr
- 3 Jahre
- 5 Jahre
- >5 Jahre
- nicht anwendbar/relevant

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



- <1 Jahr
- 1 Jahr
- 3 Jahre
- 5 Jahre
- >5 Jahre
- nicht anwendbar/relevant

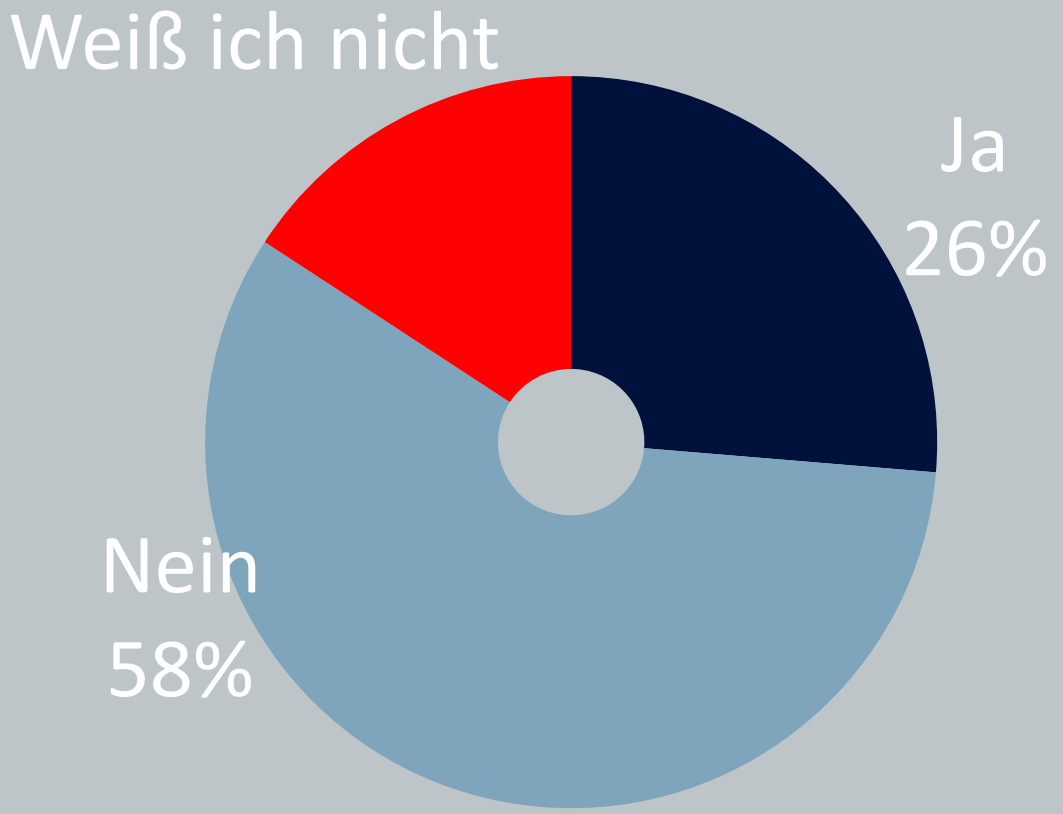
Wie lange wird Ihrer Meinung nach Ihre Organisation für die Realisierung der Quantenresistenz benötigen?



- <1 Jahr
- 1 Jahr
- 3 Jahre
- 5 Jahre
- >5 Jahre
- nicht anwendbar/relevant

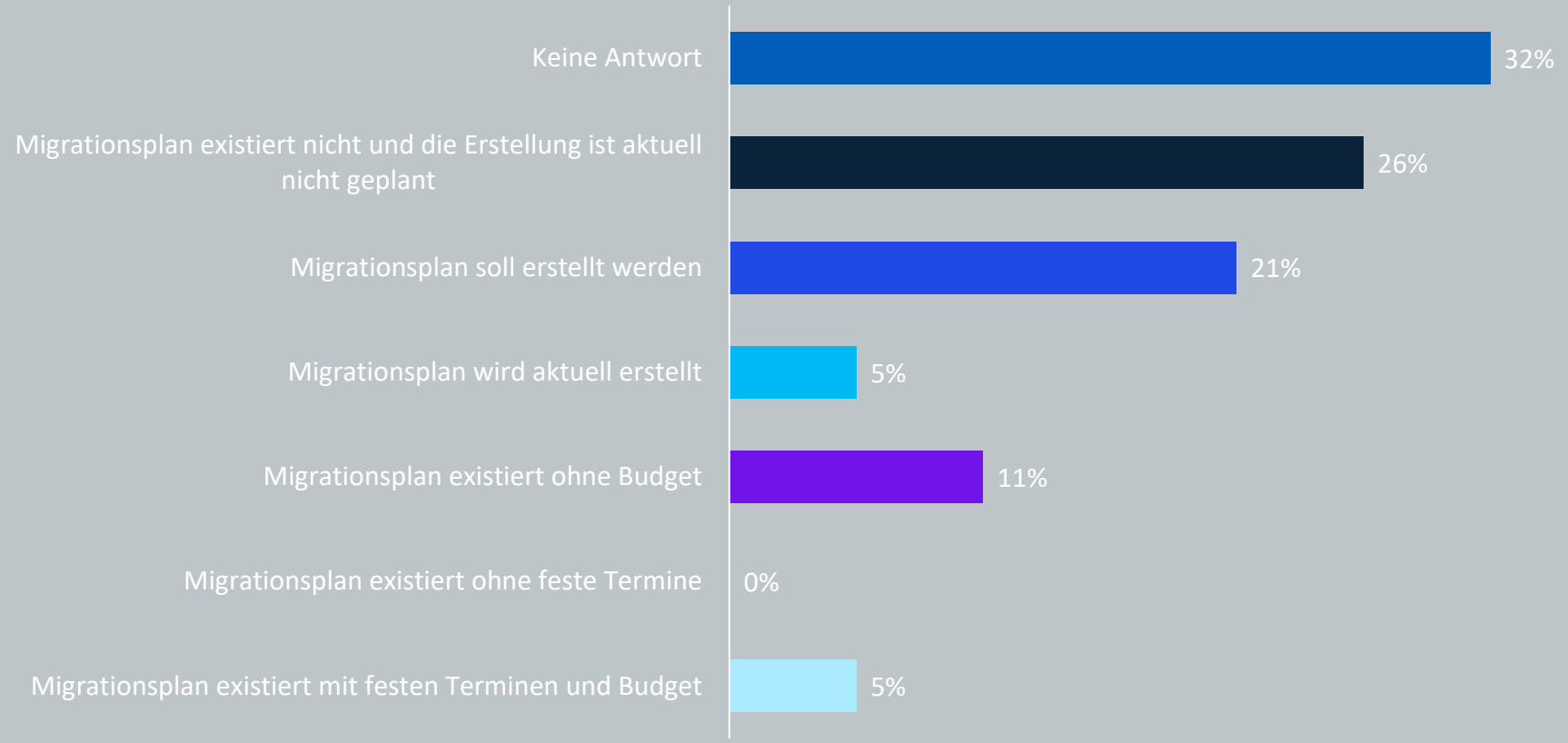
© [year] [legal member firm name]. a [jurisdiction] [legal structure] and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited. a private English company limited by guarantee. All rights reserved.

Wird das Thema „Gefährdung der Kryptographie durch Quantencomputing“ im Risikomanagement berücksichtigt? (Stand 17.6.22)



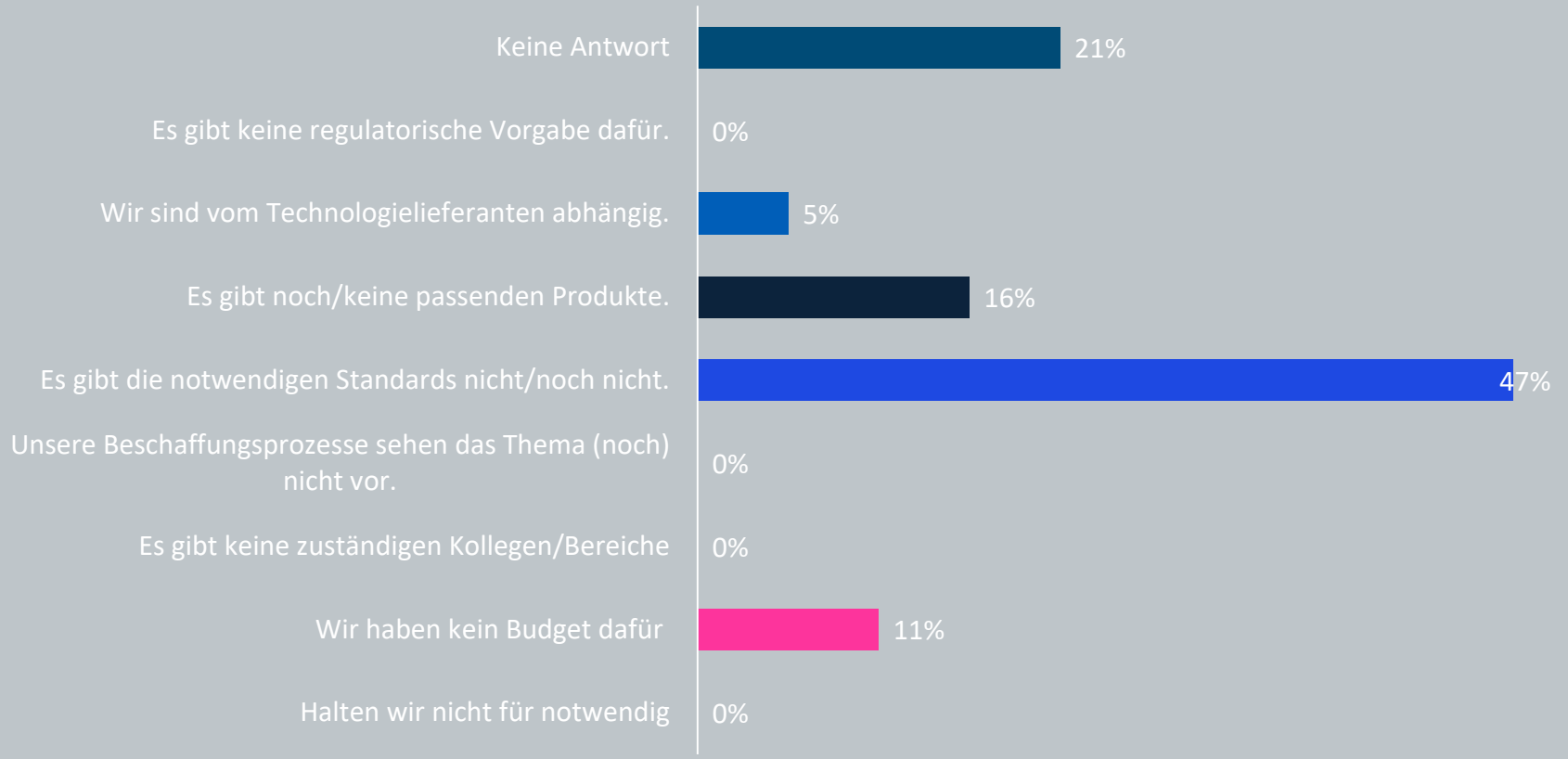
© [year] [legal member firm name]. a [jurisdiction] [legal structure] and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited. a private English company limited by guarantee. All rights reserved.

Falls ja, gibt es in Ihrer Organisation einen Migrationsplan zur Post-Quanten-Kryptographie? (Stand 17.6.22)



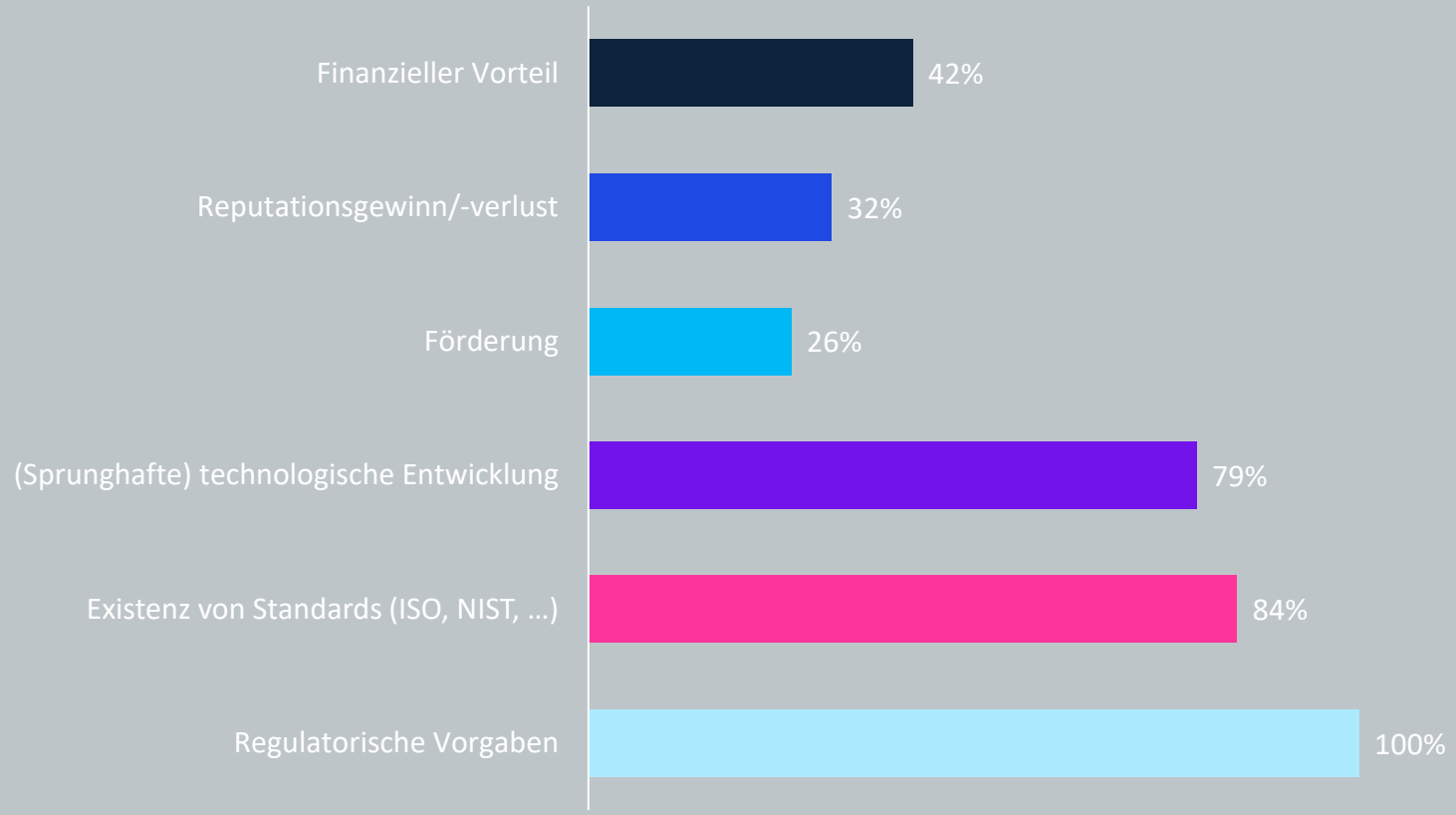
© [year] [legal member firm name]. a [jurisdiction] [legal structure] and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited. a private English company limited by guarantee. All rights reserved.

Falls in Ihrer Organisation keine Initiativen/Vorhaben zu diesem Thema existieren – warum nicht? (Stand 17.6.22)



© [year] [legal member firm name]. a [jurisdiction] [legal structure] and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited. a private English company limited by guarantee. All rights reserved.

Was würde Investitionsentscheidungen begünstigen? (Stand 17.6.22)



© [year] [legal member firm name]. a [jurisdiction] [legal structure] and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited. a private English company limited by guarantee. All rights reserved.

Fragen?

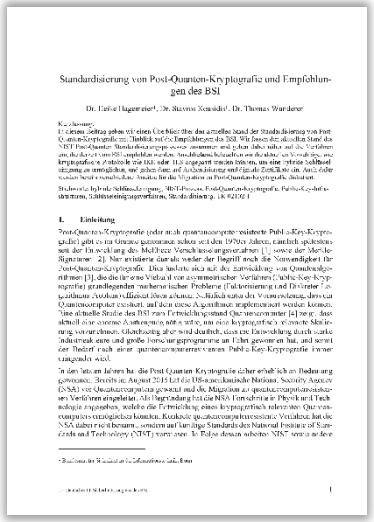
Kontakt

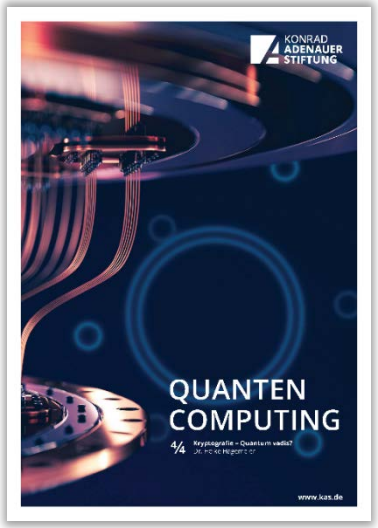
Bundesamt für Sicherheit in der Informationstechnik
Referat TK 21 – Technologie- und Forschungsstrategie

Ansprechpartnerin
Dr. Heike Hagemeier
heike.hagemeier@bsi.bund.de
www.bsi.bund.de/Quanten
Tel. +49 99 9582 5968

Bundesamt
für Sicherheit in der
Informationstechnik

Weiterlesen





Deutschland
Digital•Sicher•BSI•