Bundesamt
für Sicherheit in der
Informationstechnik

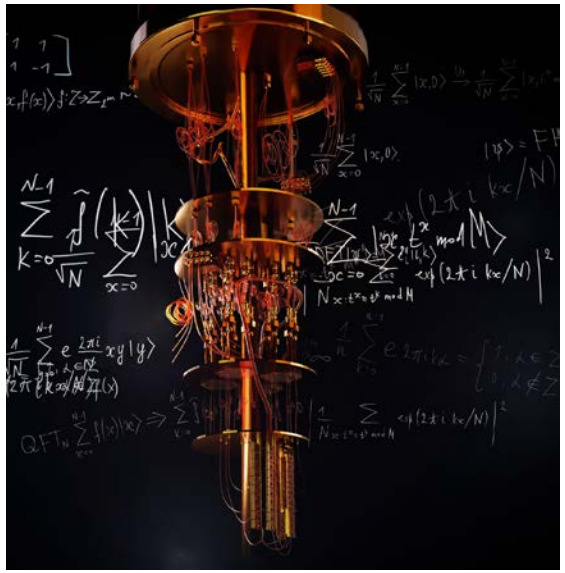
Deutschland
Digital•Sicher•BSI•

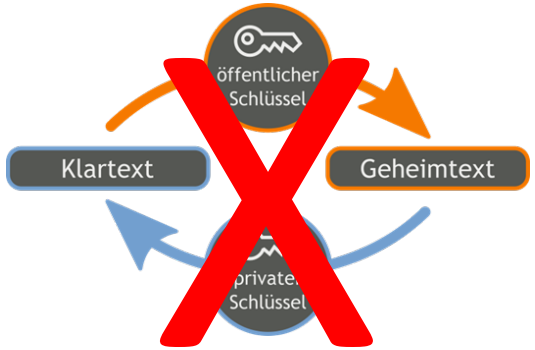
Kryptografie und Quantencomputing

Dr. Heike Hagemeier
Bundesamt für Sicherheit in der Informationstechnik, Referat TK 21
OMNISECURE 2023, 24. Mai 2023

Motivation

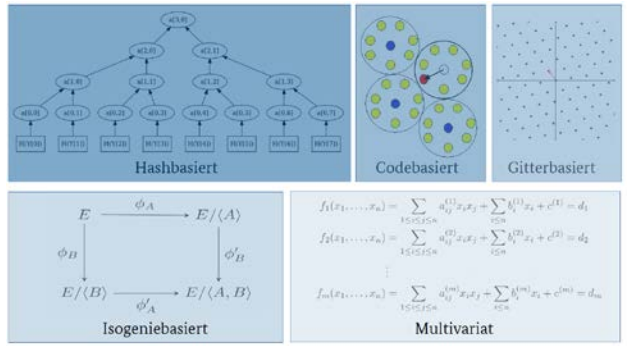
Motivation



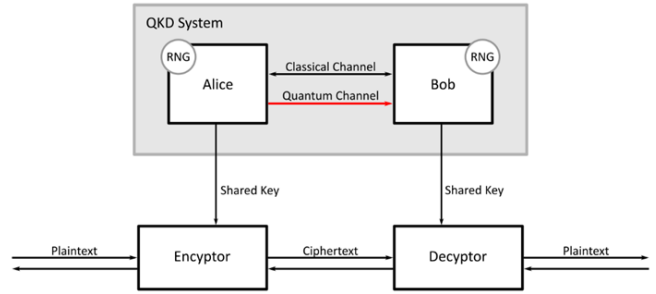


Derzeit eingesetzte Public-Key-Kryptografie

Post-Quanten-Kryptografie



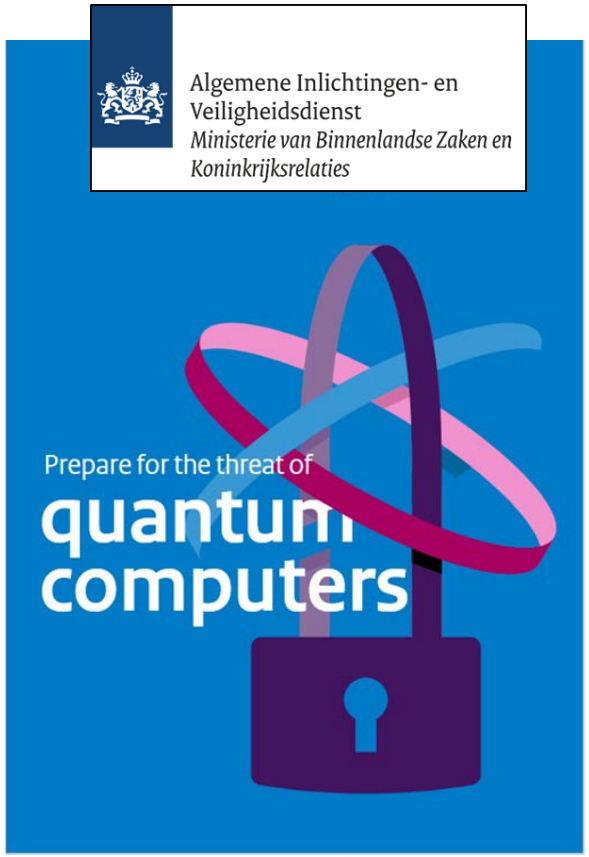
Quantensichere Kryptografie



Quantum Key Distribution

Was passiert in anderen Ländern?

Motivation II



THE WHITE HOUSE
WASHINGTON

MAY 04, 2022

National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems

BRIEFING ROOM › STATEMENTS AND RELEASES

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

THE DIRECTOR

November 18, 2022

M-23-02

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Shalanda D. Young
Director

SUBJECT: Migrating to Post-Quantum Cryptography

Government of Canada | Gouvernement du Canada

COMPANIES | EMERGING TECH | FINANCIAL | GOVERNMENT & PUBLIC SECTOR

Government of Canada invests $360 million in new National Quantum Strategy

ASHEE PAMMA

JANUARY 13, 2023

Handlungskonzept Quantentechnologien

Die Bundesregierung

Ziele der Bundesregierung im Bereich Post-Quanten-Kryptografie

- Erstellung einer Strategie der Bundesregierung für die Migration zu Post-Quanten-Kryptografie in Deutschland.
- Weiterführung der Migration zu Post-Quanten-Kryptografie für den Hochsicherheitsbereich.
- Einleiten der Migration zu Post-Quanten-Kryptografie in weiteren sicherheitskritischen Bereichen.
- Integration von Post-Quanten-Kryptografie-Verfahren in praxistaugliche IT-Sicherheitslösung

Deutscher Bundestag — Drucksache 20/6610
20. Wahlperiode — 28.04.2023

Unterrichtung
durch die Bundesregierung

Handlungskonzept Quantentechnologien der Bundesregierung

Inhaltsverzeichnis

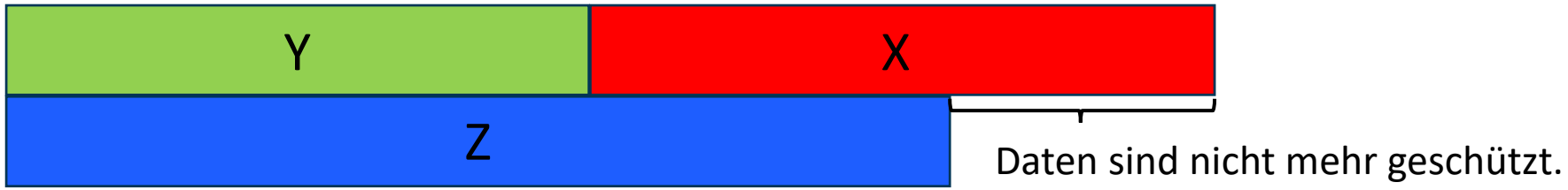
Zugeleitet mit Schreiben des Bundesministeriums für Bildung und Forschung vom 26. April 2023.

Verfügbar unter https://dserver.bundestag.de/btd/20/066/2006610.pdf

Wie viel Zeit bleibt für die Migration auf quantensichere Kryptografie?

Das hängt von folgenden Faktoren ab:

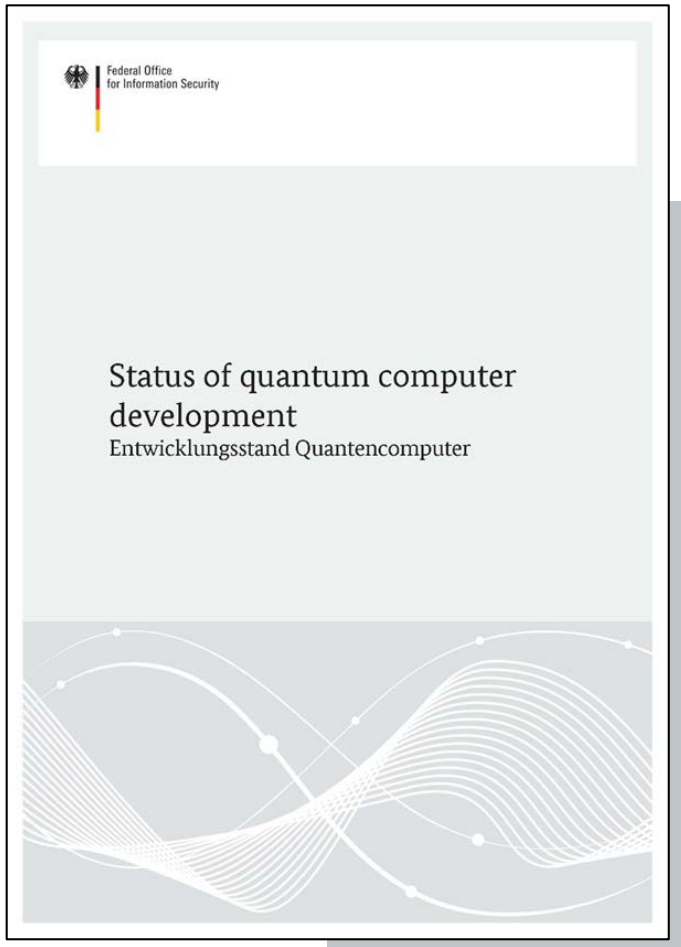
- Wie lange sollen Ihre Daten sicher bleiben? (X Jahre)
- Wie lange dauert die Umstellung Ihrer Systeme auf quantensichere Kryptografie? (Y Jahre)
- Wie lange wird es dauern, bis kryptografisch relevante Quantencomputer existieren? (Z Jahre)



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

Studie „Entwicklungsstand Quantencomputer“

- Aktueller Stand verfügbar unter www.bsi.bund.de/qcstudie
- Aktuelles BSI-Projekt: Aktualisierung der Studie
- Projektleiter Prof. Wilhelm-Mauch (FZ Jülich)
- Ergebnis der 1. Aktualisierung:
  - Fülle neuer Entwicklungen bei
    - Algorithmen im NISQ-Bereich
    - Fehlerkorrektur und -mitigation
    - Hardware
  - Kein echter Durchbruch
  - Aber: Die Entwicklung kann sich deutlich beschleunigen, sollten sich heuristische Ergebnisse verfestigen.



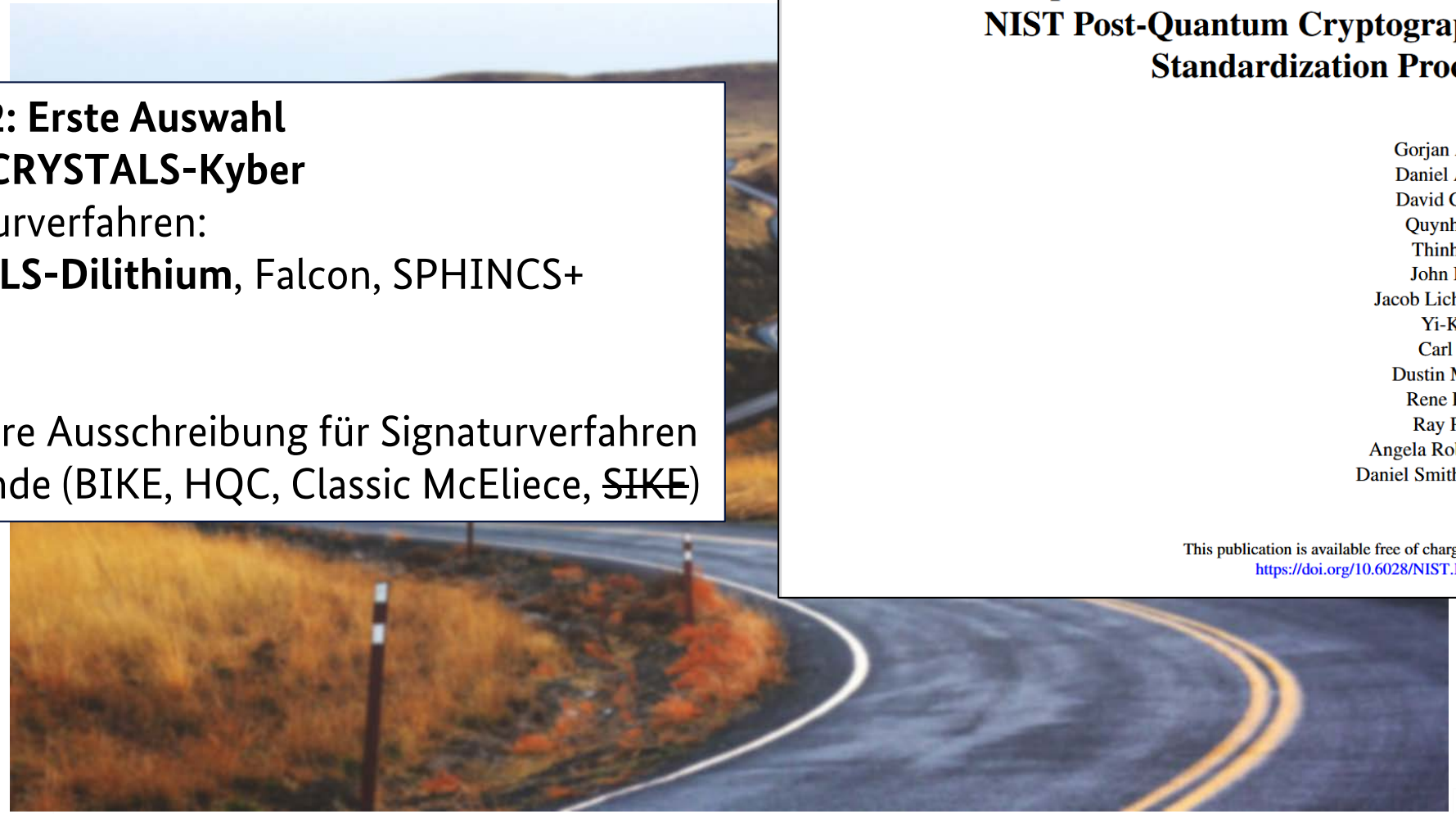
Post-Quanten-Kryptografie

Standardisierung: NIST-Prozess („A long and winding road“)

Standardisierung: NIST

Juli 2022: Erste Auswahl
1 KEM: **CRYSTALS-Kyber**
3 Signaturverfahren:
CRYSTALS-Dilithium, Falcon, SPHINCS+

Aktuell:
- Weitere Ausschreibung für Signaturverfahren
- 4. Runde (BIKE, HQC, Classic McEliece, ~~SIKE~~)



NIST IR 8413

Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process

Gorjan Alagic
Daniel Apon*
David Cooper
Quynh Dang
Thinh Dang
John Kelsey
Jacob Lichtinger
Yi-Kai Liu
Carl Miller
Dustin Moody
Rene Peralta
Ray Perlner
Angela Robinson
Daniel Smith-Tone

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8413

Post-Quanten-Kryptografie

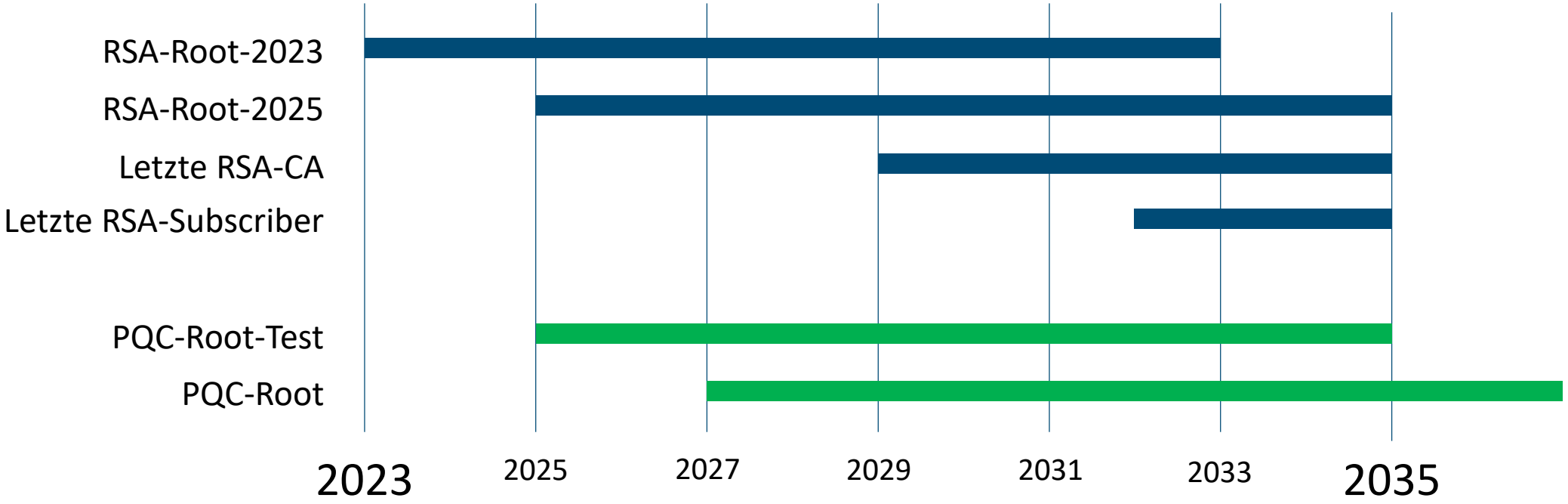
- BSI hat bereits 2020 (konservative) Algorithmen empfohlen (TR-02102-1):
  - FrodoKEM und Classic McEliece
  - hashbasierte Signaturen
- 2021: erweiterte Empfehlungen und Hintergrundinformationen zu PQC und QKD
- Handlungsempfehlungen (Auszug):
  - **Vorbereitung / Inventarisierung**
  - **Agilität**
  - **Hybride Lösungen**

BSI-Aktivitäten (Auszug)

Kryptobibliothek Botan	Integration von Post-Quanten-Kryptografie in den E-Mail Client Thunderbird	Quantensichere Verwaltungs-PKI
• Botan 3.x • Implementierung von Post-Quanten-Kryptografie in Botan, insb. auch FrodoKEM, Classic McEliece, SPHINCS+ • Hybride Schlüsseleinigung in TLS 1.3 • Krypto-Dokumentation	• PQC+ECC für E-Mail-Verschlüsselung und -Signatur • Standard-Entwurf für PQ in OpenPGP: https://datatracker.ietf.org/doc/draft-wussler-openpgp-pqc/	• BSI betreibt Root-CA • Migration durch parallelen Betrieb • Hybride Lösung (PQC+ECC) für Subscriber-Zertifikate • Root-CA: BSI prüft Einsatz von hashbasierten Signaturverfahren

Wie groß ist Y?

Beispielhafter Migrationsplan V-PKI



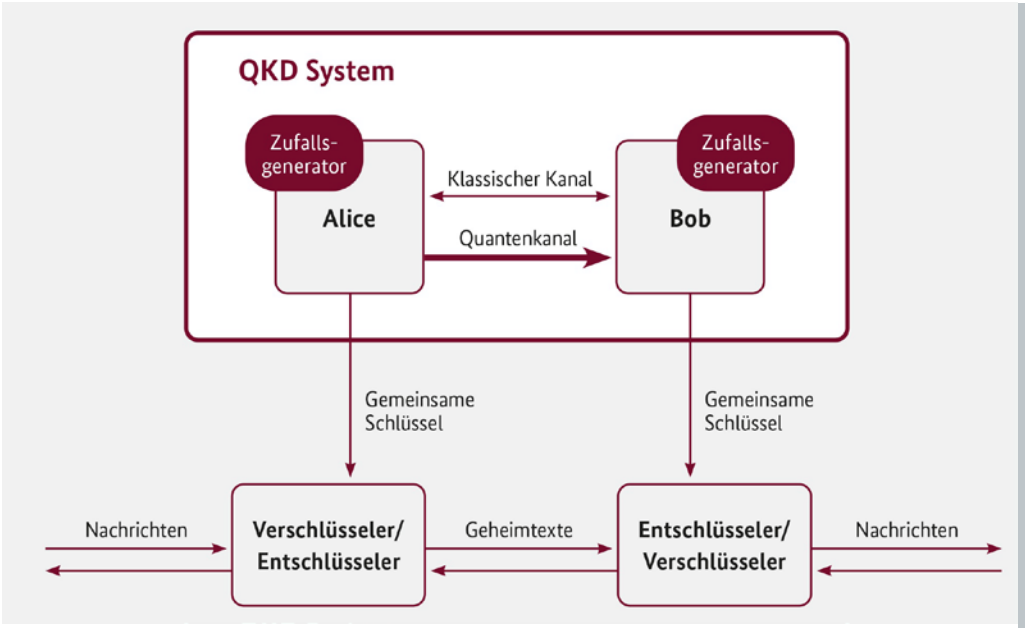
Quantum Key Distribution

Alternativer Vorschlag: Quantum Key Distribution

- QKD kann Post-Quanten-Kryptografie in hybriden Lösungen ergänzen

→ **Fokus auf Migration zu Post-Quanten-Kryptografie**

- BSI-Aktivitäten
  - Studie zu Seitenkanalangriffe auf QKD-Systeme (Ende 2023)
  - CC Protection Profile zu QKD-Devices (mit ETSI)
  - Koordination des BMBF-geförderten Schirmprojekt Quantenkommunikation Deutschland (SQuaD, mit PTB)



Umfrage „Kryptografie und Quantencomputing“

Umfrage „Kryptografie und Quantencomputing“

Umfrage von KPMG, Deutschland und BSI zu Kryptografie und Quantencomputing

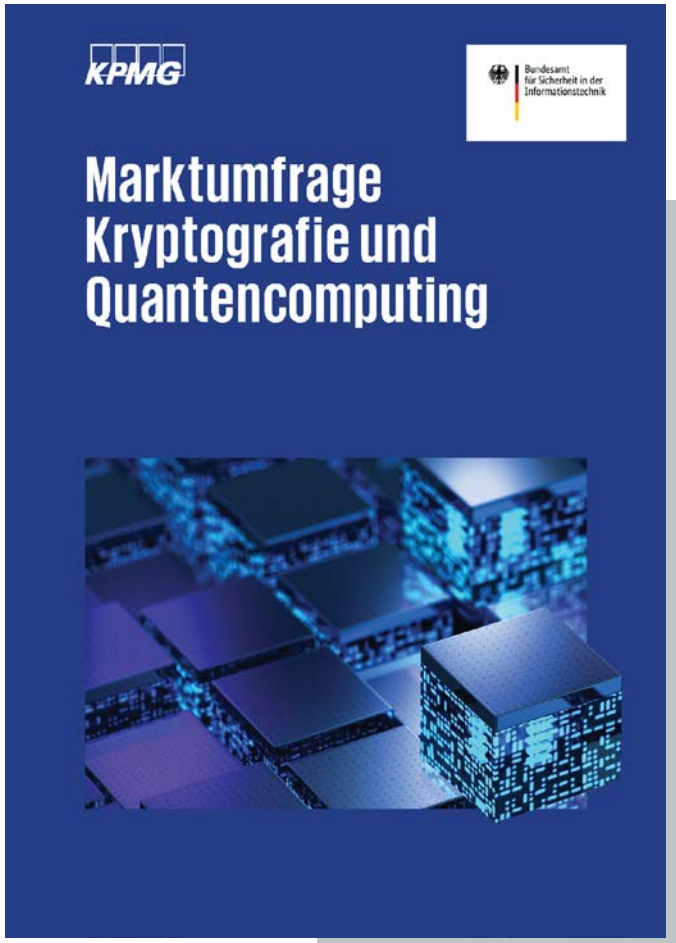
- Basiert auf dem BSI-Leitfaden "Kryptografie quantensicher gestalten".
- Richtet sich an alle interessierten Unternehmen und Organisationen (insb. an das Produktmanagement für Sicherheitsfunktionen, CISO's oder CIO's).
- Jede teilnehmende Organisation erhält einen individualisierten Ergebnisbericht.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

Allianz für Cyber-Sicherheit

Umfrage Quanten-sicherheit

- Hohe Relevanz von Quantencomputing für die Sicherheit von kryptografischen Verfahren.
- Teilnehmende erwarten im Mittel, dass aktuell verwendete kryptografische Verfahren in zehn Jahren gebrochen werden.
- 89 % erwarten, dass die Umstellung ihrer Organisation zu quantensicherer Kryptografie nicht rechtzeitig abgeschlossen wird.
- Gefährdung der Kryptografie durch Quanten-computing wird von wenigen Organisationen im Risikomanagement berücksichtigt.

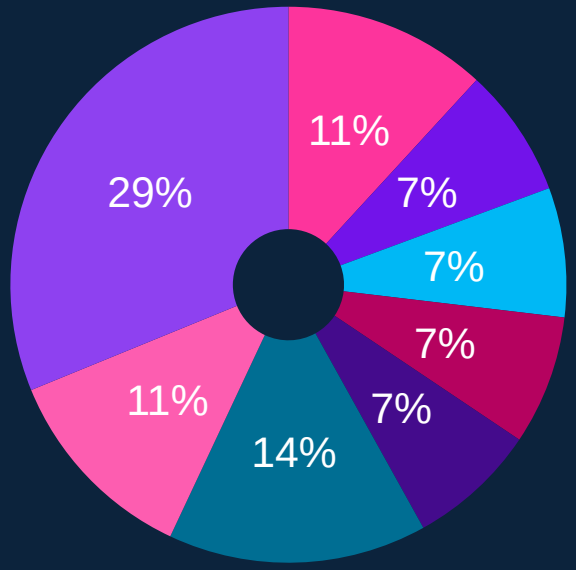
Bundesamt für Sicherheit in der Informationstechnik



Ergebnisse verfügbar unter: https://www.bsi.bund.de/dok/umfrage-pqc

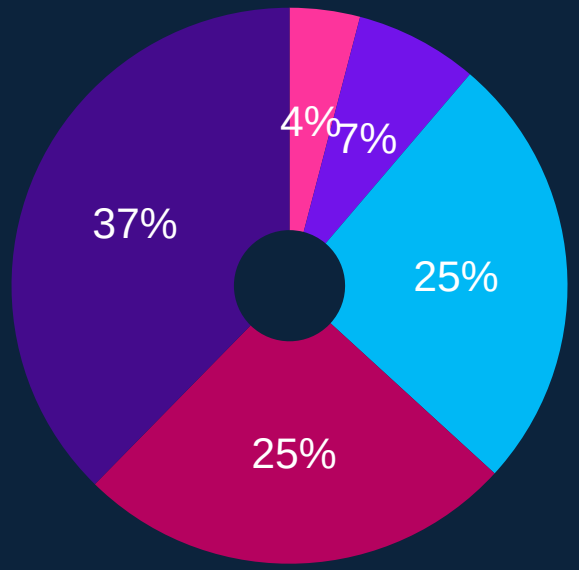
Übersicht – Demografische Daten

Branche



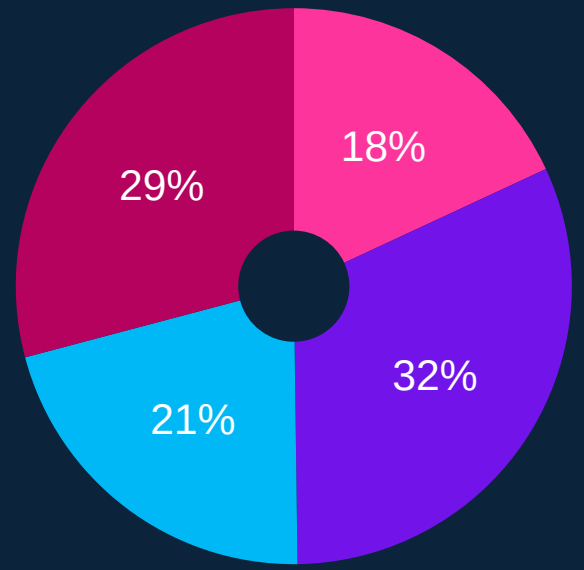
- Chemicals & Pharmaceuticals
- Technology
- Energy & Natural Resources
- Telecommunications
- Government
- Industrial Manufacturing
- Transport & Logistics/Leisure
- Banking

Anzahl Mitarbeiter



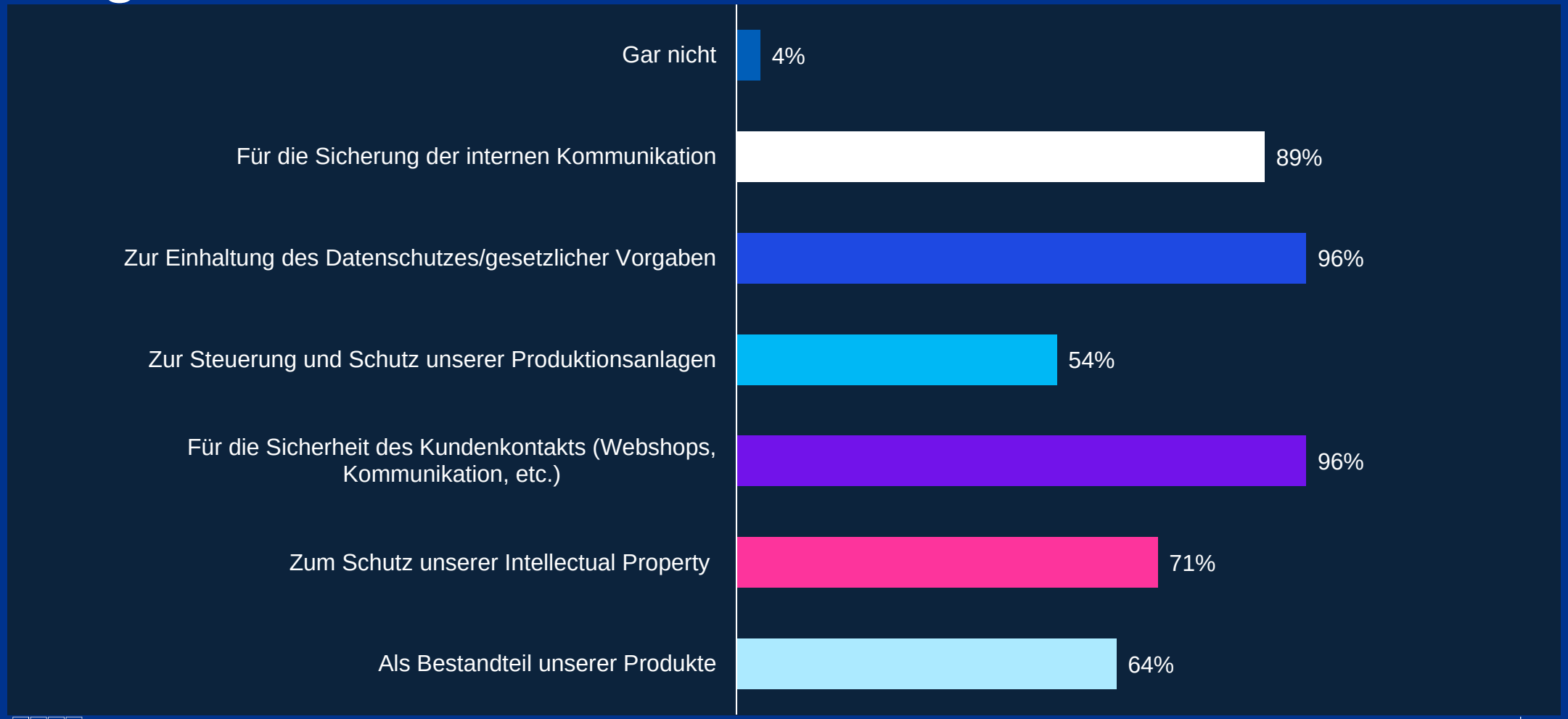
- Weniger als 100
- Zwischen 100 und 1000
- Zwischen 1000 und 10000
- Zwischen 10000 und 50000
- Mehr als 50000

Gesamtumsatz

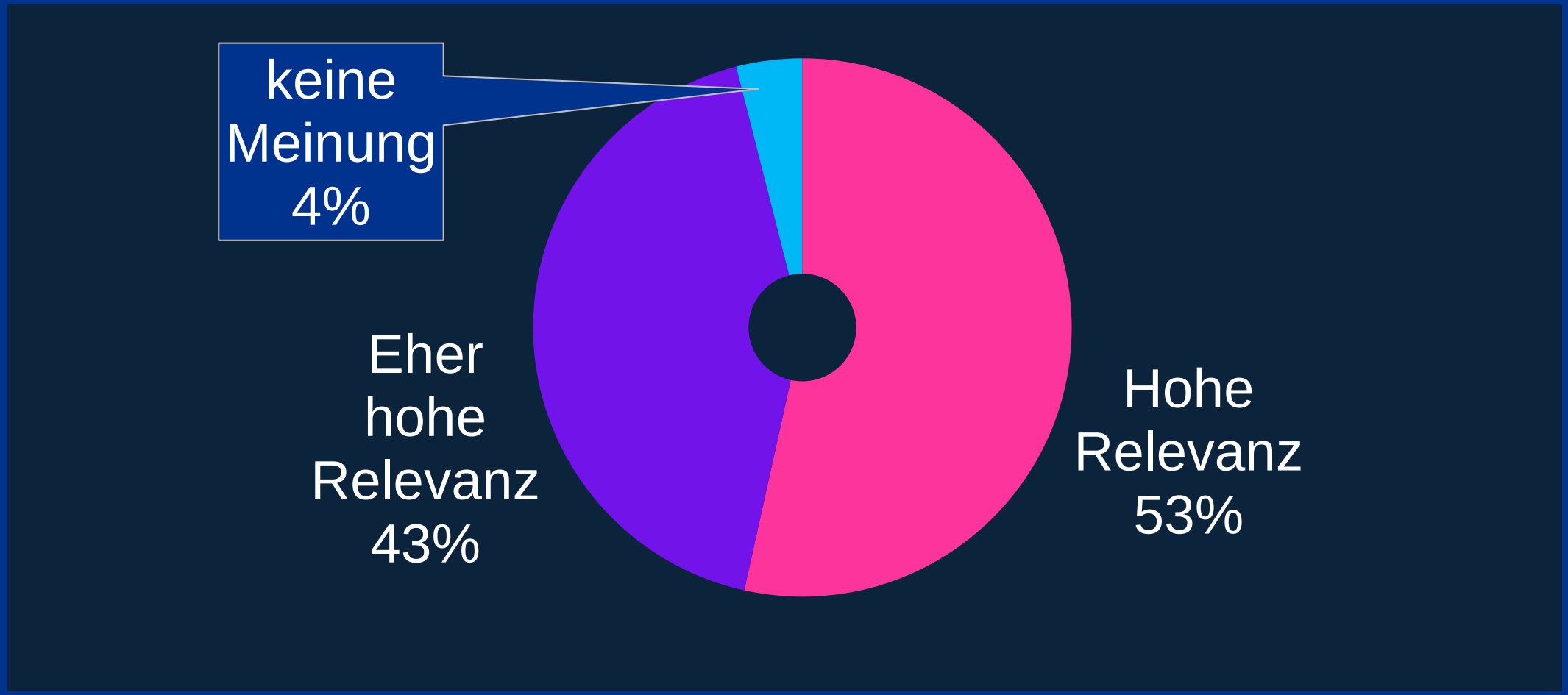


- Bis 1 Mrd. Euro
- Zwischen 1 und 10 Mrd. Euro
- Zwischen 10 und 50 Mrd. Euro
- Mehr als 50 Mrd. Euro

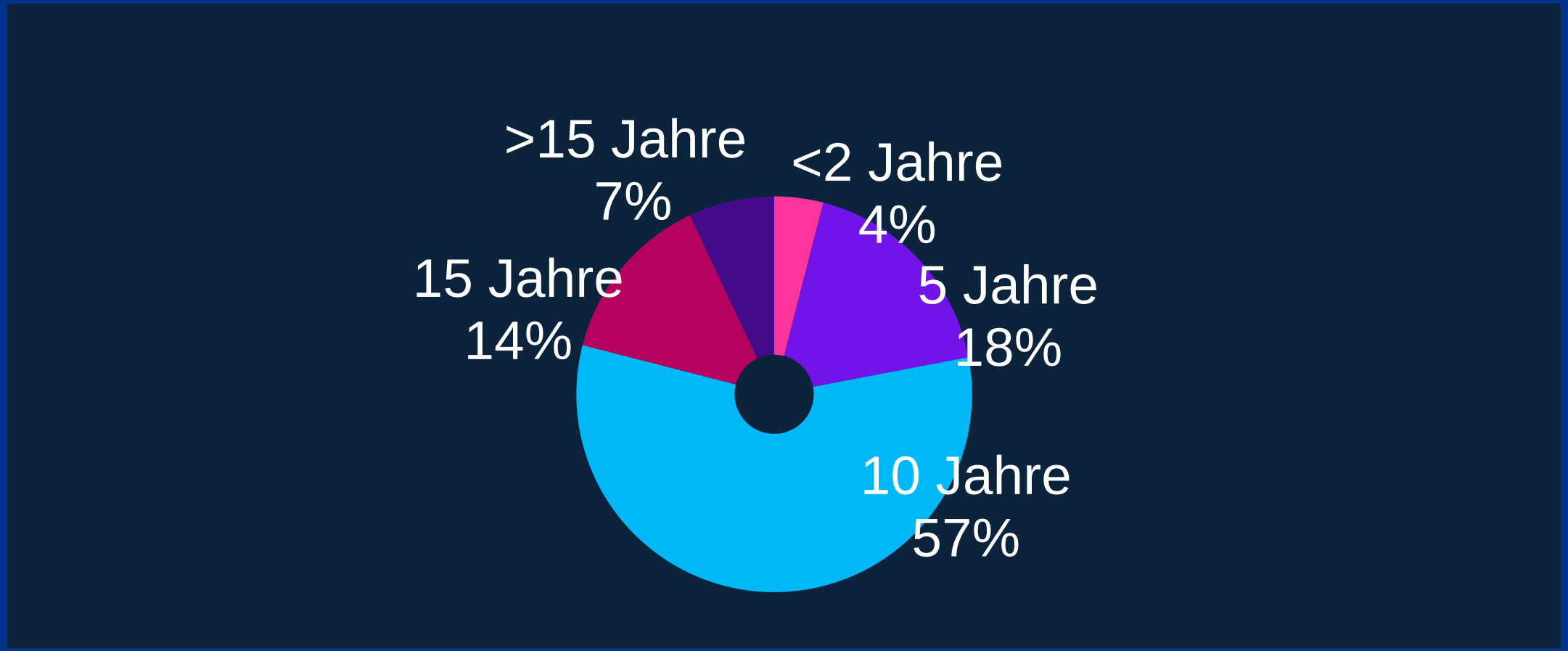
Zu welchen Verwendungszwecken werden von Ihrer Organisation kryptographische Verfahren eingesetzt?



Welche Relevanz von Quantencomputing für die Sicherheit von kryptographischen Verfahren erwarten Sie generell?

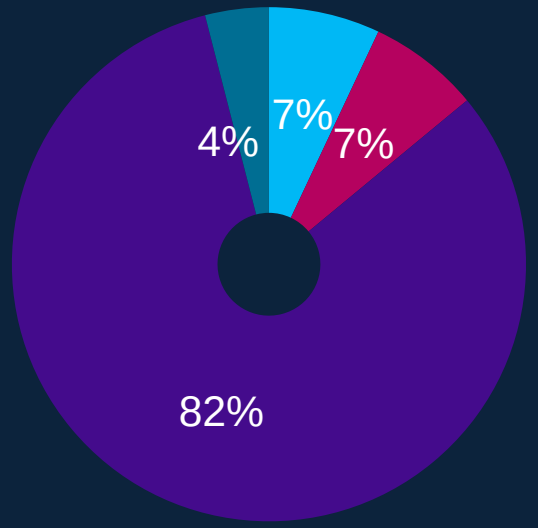


Wann schätzen Sie werden Quantencomputer in der Lage sein, bestimmte, heute eingesetzte kryptographische Verfahren zu brechen?

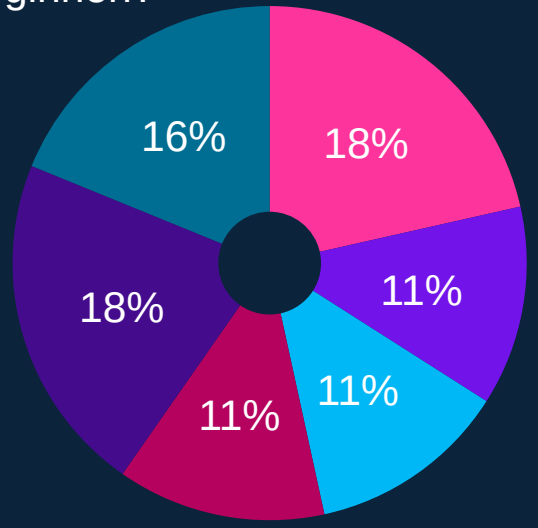


Bitte geben Sie uns Ihre Einschätzung zur zeitlichen Entwicklung

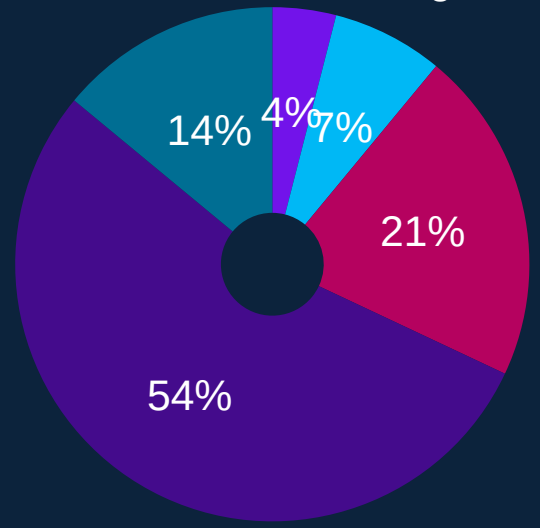
Maximale Dauer, für die Informationen durch Ihre Organisation vertraulich gehalten werden müssen?



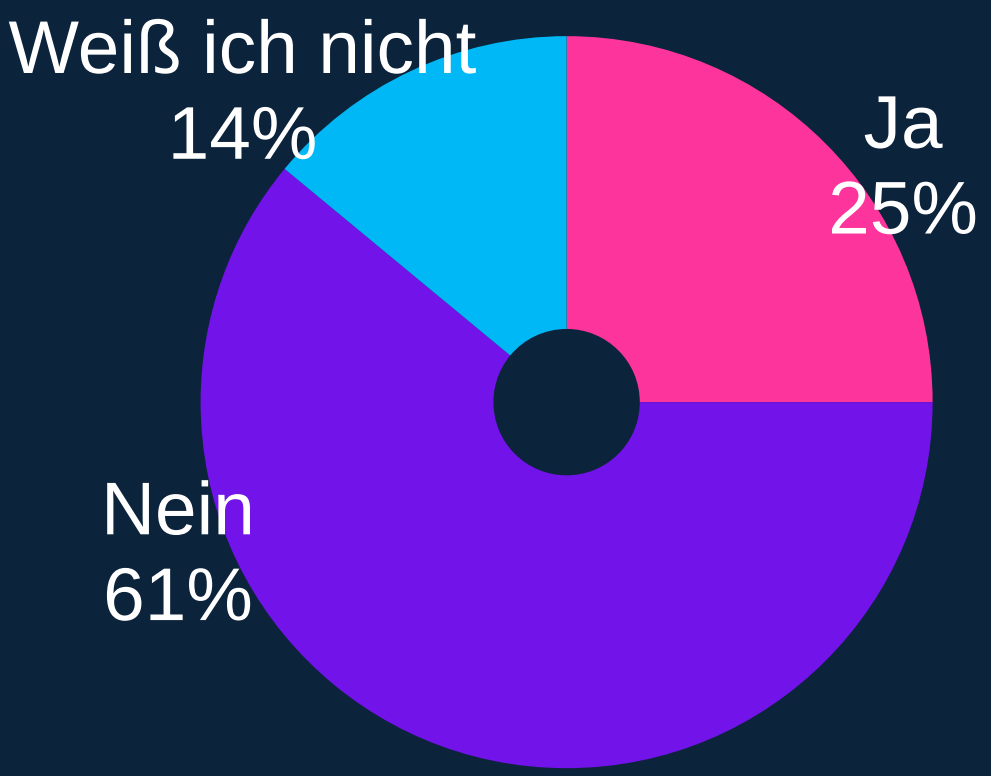
Wann plant Ihre Organisation mit der Umstellung auf quantensichere Kryptographie zu beginnen?



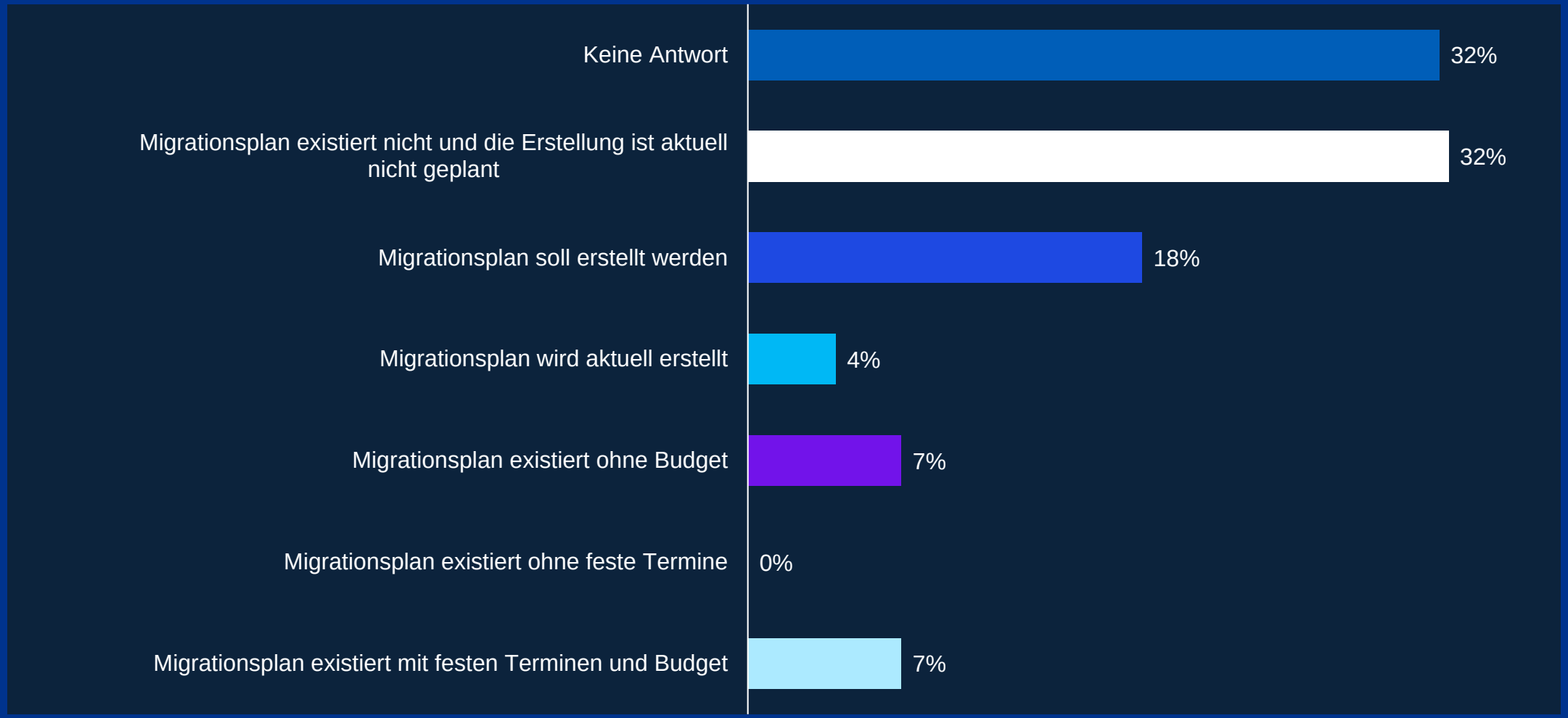
Wie lange wird Ihrer Meinung nach Ihre Organisation für die Realisierung der Quantenresistenz benötigen?



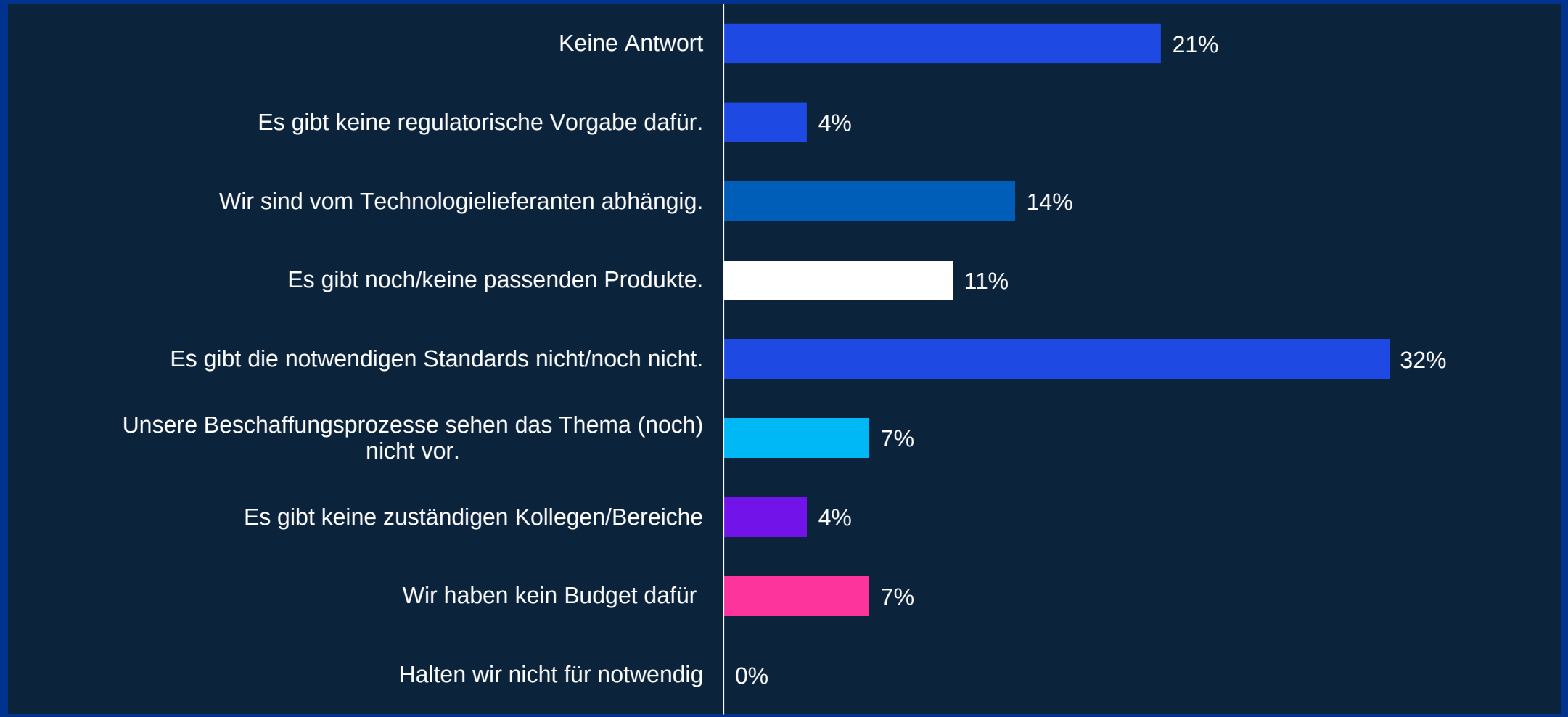
Wird das Thema „Gefährdung der Kryptographie durch Quantencomputing“ im Risikomanagement berücksichtigt?



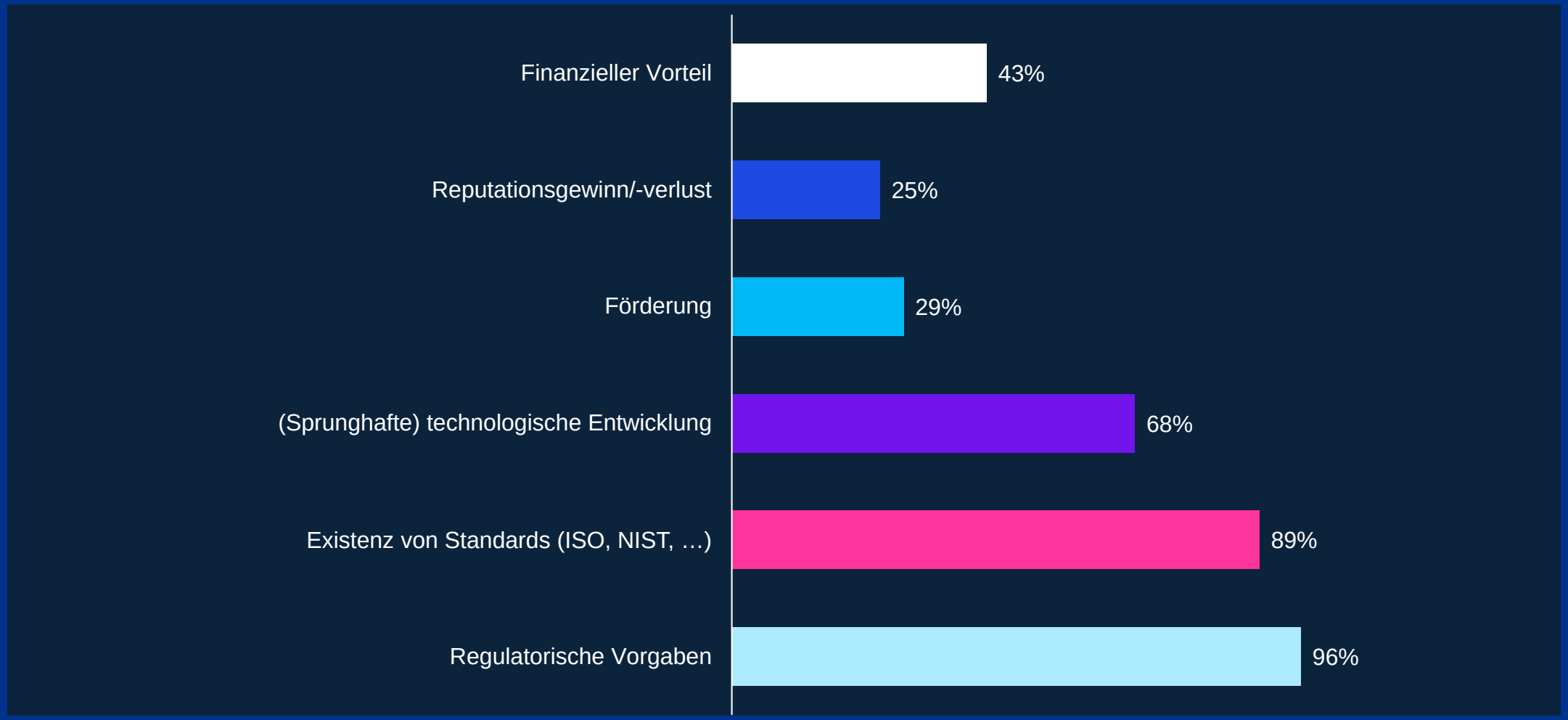
Falls ja, gibt es in Ihrer Organisation einen Migrationsplan zur Post-Quanten-Kryptographie?



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



Was würde Investitionsentscheidungen begünstigen?



Fazit

Deutschland
Digital•Sicher•BSI•

- Der kryptografische Umbruch hat begonnen.
- Die Migration zu quantensicherer Kryptografie ist voraussichtlich noch immer langwierig.
- Inventur, Risikobewertung und Planung sind bereits jetzt möglich.
- Es können sich jederzeit sprunghafte Entwicklungen in der Kryptanalyse ergeben. (Gilt auch unabhängig von Quantencomputern.)
- Kryptoagilität sollte ein Designkriterium sein!

Weitere Informationen: https://bsi.bund.de/Quanten

Vielen Dank für Ihre Aufmerksamkeit!

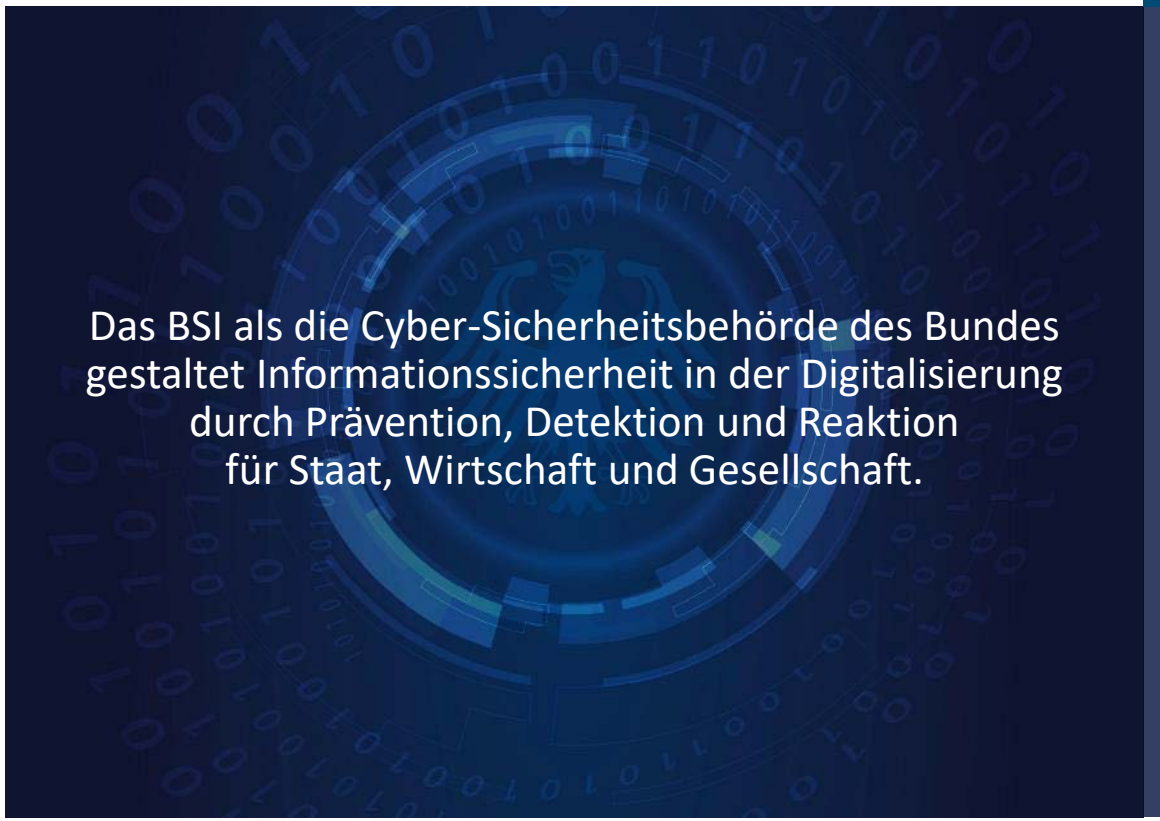
Deutschland
Digital•Sicher•BSI•

Kontakt

Dr. Heike Hagemeier
Heike.Hagemeier@bsi.bund.de

quantum@bsi.bund.de

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 185-189
53175 Bonn
www.bsi.bund.de



Bundesamt
für Sicherheit in der
Informationstechnik