Post-Quantum Migration

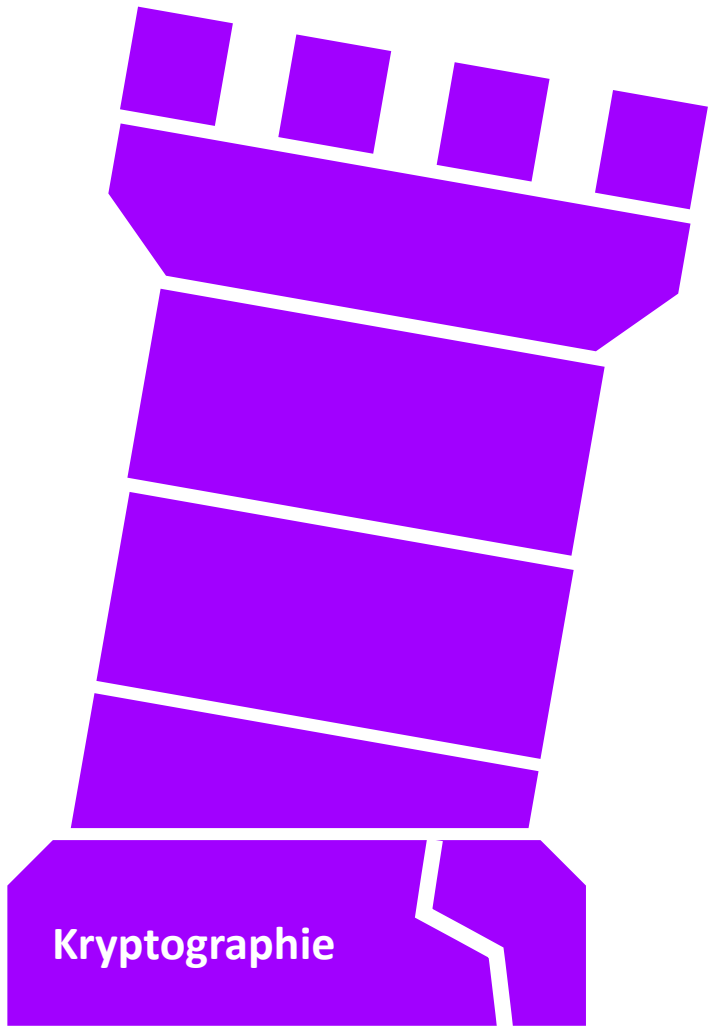
Episode 1 - Die dunkle Bedrohung

Freitag, 02.10 2026
ITSecX – St.Pölten

Viktor Zelezny

Copyright © 2026 Accenture. All rights reserved.

Die Quantenbedrohung



Ein ausreichend leistungsfähiger Quantencomputer wird heute eingesetzte Verschlüsselungsverfahren brechen.



Abhören



Identitätsdiebstahl

Copyright © 2026 Accenture. All rights reserved.

Agenda

Wir durchleuchten die technischen Hintergründe der Quantenbedrohung, gehen auf PQC-Strategien ein und finden heraus, was ein Kryptoinventar ist.

01 Quantumcomputing

02 Quantenrisiko & HNDL

03 Die Perspektive des Gesetzgebers

04 Die Quantenbedrohung im Detail

05 PQC-Strategie

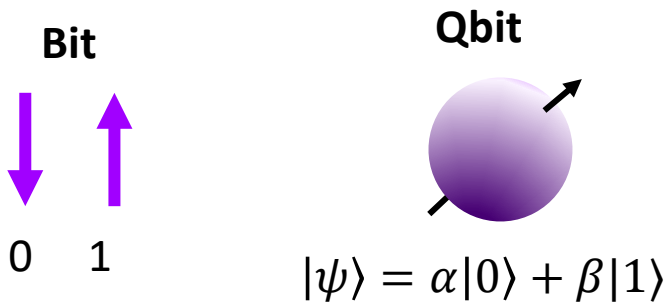
06 Das Kryptoinventar

Copyright © 2026 Accenture. All rights reserved.

Quantumcomputing

Wann krieg‘ ich meinen Quantenlaptop?

- Quantencomputer verwenden fundamental neue Hardware
- **Spezielle Berechnung** können weitaus schneller ausgeführt werden
- Quantencomputer verwenden Qbits anstelle von Bits

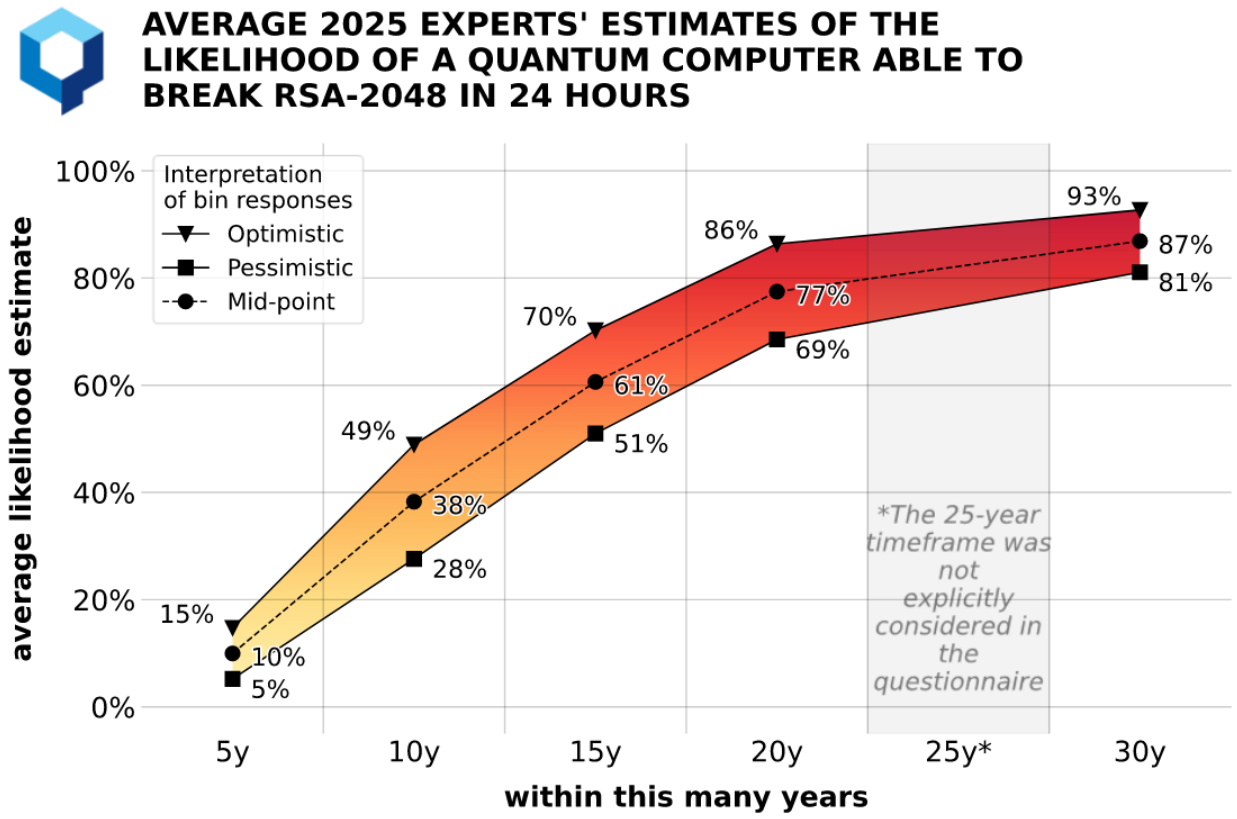


- Die größte Challenge ist die Kontrolle der sensiblen Quanteninformation und die Skalierung:
  - Physische Qbits mit hoher Stabilität
  - Fehlerkorrektur & logische Qbits
  - Architekturen und Algorithmen



Quantum Risk – Was sagen die Experten?

Das Global Risk Institute & evolutionQ haben 27 Meinungsführer befragt.



„This is the clearest warning that I can offer in public right now about the urgency of migrating to post-quantum cryptosystems, […]“

Scott Aaronson, OG of Quantum Computing

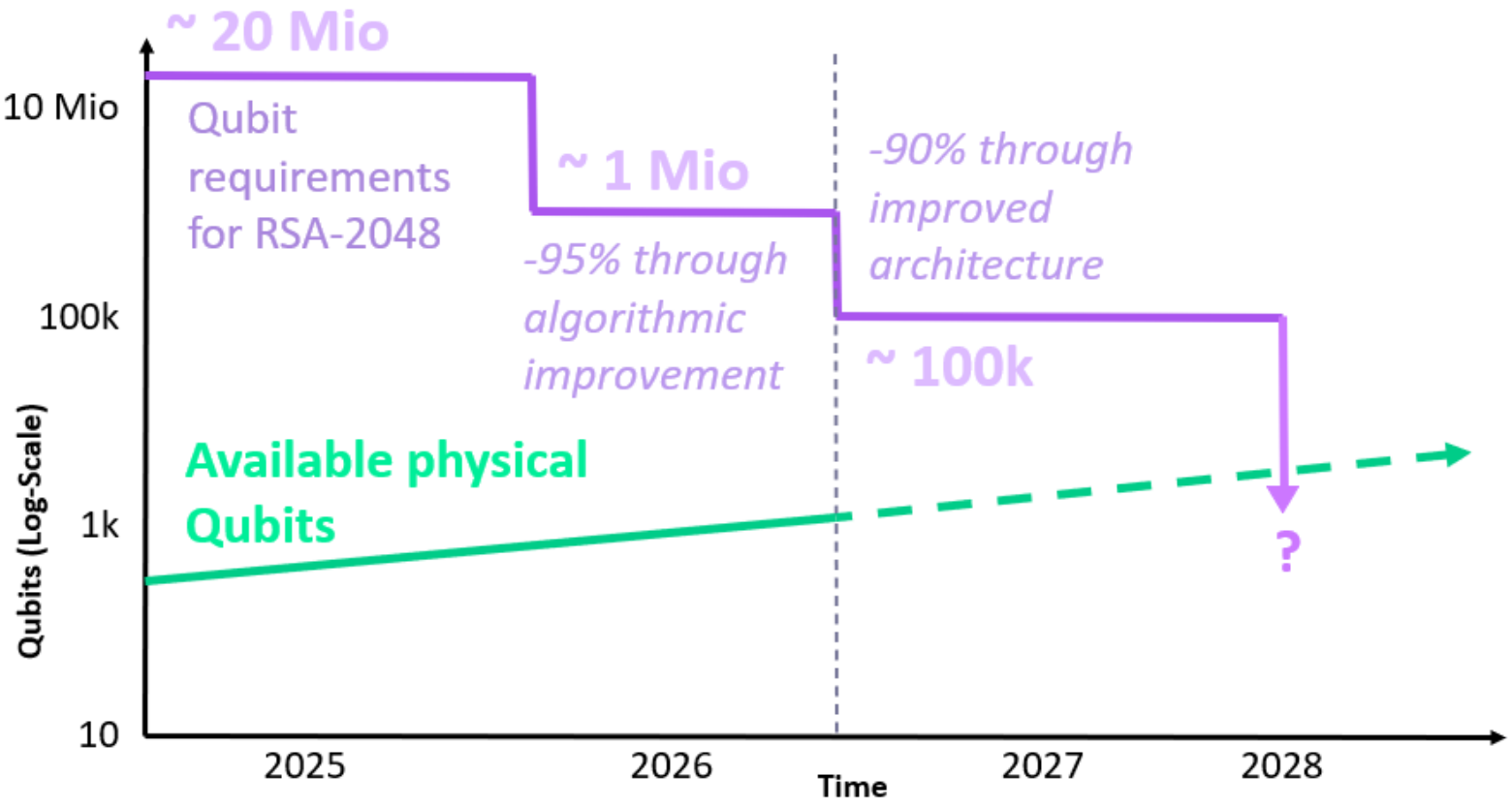
“Unsere konservative Einschätzung ist, dass kryptographisch relevante Quantencomputer in 15 Jahren verfügbar sein werden, […] vielleicht sogar schon in 10.”

Germany’s Federal Office for Information Security (BSI)

Copyright © 2026 Accenture. All rights reserved.

Algorithmen & weitere Risiken

Architektonische Verbesserungen reduzieren die Anzahl notwendiger Qbits, kommen aber mit Drawbacks.



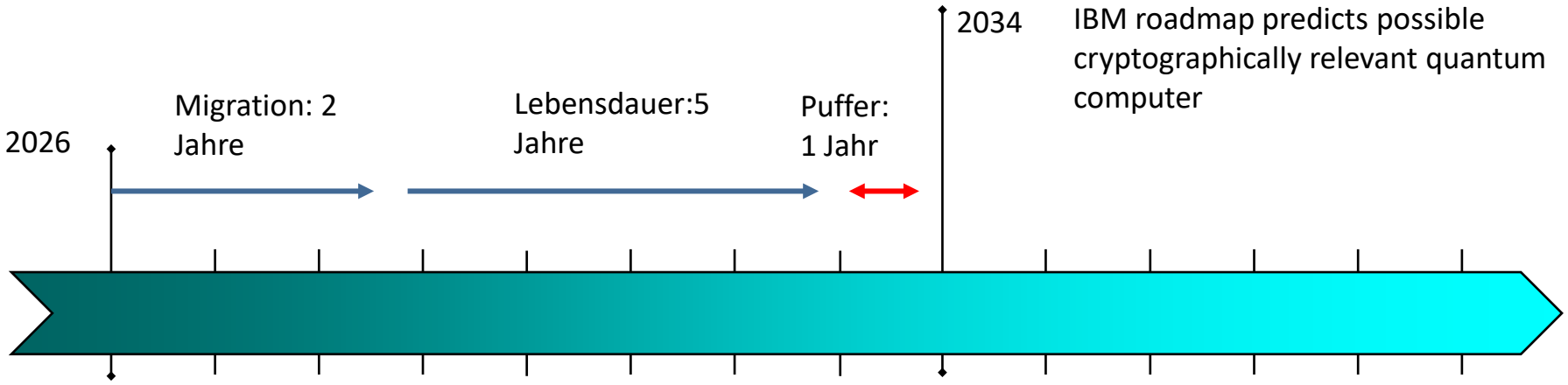
Die verbleibende Zeit könnte wesentlich kürzer sein …

- Technologische Durchbrüche
- Begrenzte öffentliche Informationen (under-the-radar-research)

Copyright © 2026 Accenture. All rights reserved.

“Harvest now – decrypt later”

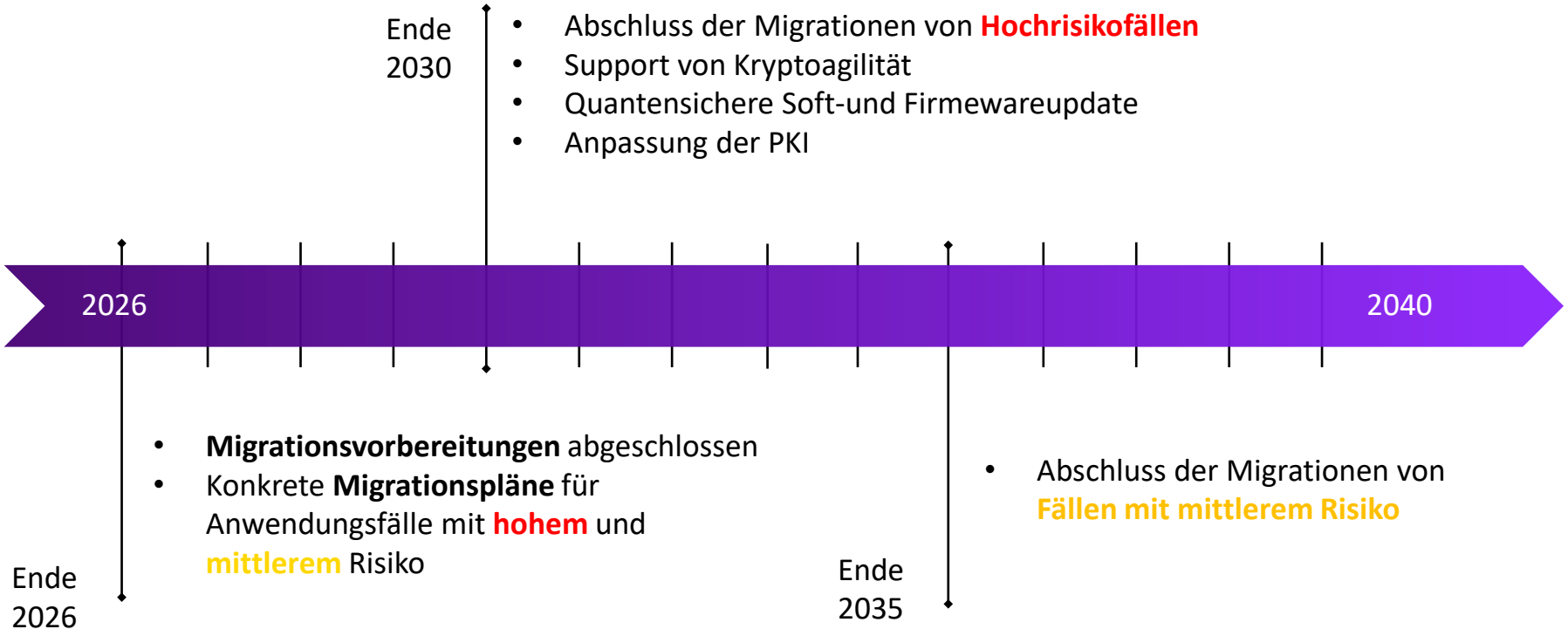
Der individuelle Migrationsplan sollte risikobasiert und abhängig von der Lebensdauer der Daten gewählt werden.



Copyright © 2026 Accenture. All rights reserved.

Roadmap der europäischen Kommission

Die Erwartungen des Regulators nehmen Form an.



Copyright © 2026 Accenture. All rights reserved.

Die Quantenbedrohung im Detail

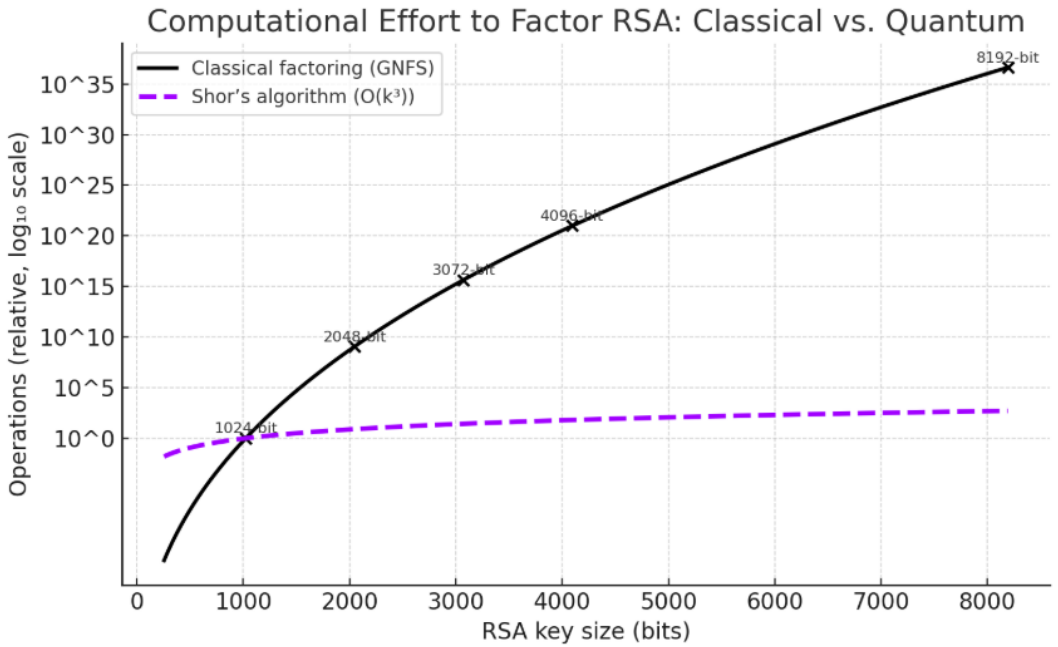
Nicht jede Verschlüsselung ist gefährdet.

Asymmetrische Verfahren **in Gefahr**

Symmetrische Verfahren **(weitgehend) sicher**

Attack vector

- Asymmetrische Verschlüsselung beruht auf **rechenintensiven Problemen:**
  - RSA: Primzahlenzerlegung
  - Diffie-Hellmann: diskreter Logarithmus
- Rechenaufwand wächst dramatisch mit der Größe des Problems
- Quantenalgorithmen skalieren besser (Shor's Algorithmus)
- Vergrößerung der Schlüssellänge keine Option



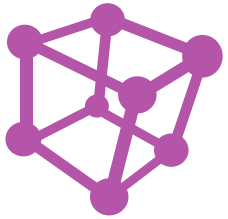
Copyright © 2026 Accenture. All rights reserved.

Neue Strategien für den Schlüsselaustausch



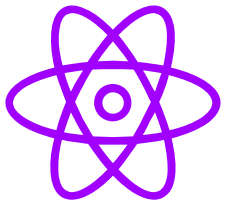
1. Pre-shared keys

- Geeignet für **spezifische Anwendungsfälle**
- **Kaum skalierbar**



2. Post Quantum Cryptography

- **Quantensichere & standardisierte “klassische” Algorithmen**
- Integration in **vorhandene Protokolle & Infrastruktur**



3. Quantum Key Distribution

- Schlüsselaustausch **abgesichert durch Quantenphysik**
- **Frühes Entwicklungsstadium** der neuen Quantenhardware

Copyright © 2026 Accenture. All rights reserved.

Die G7 CEG PQC-Roadmap

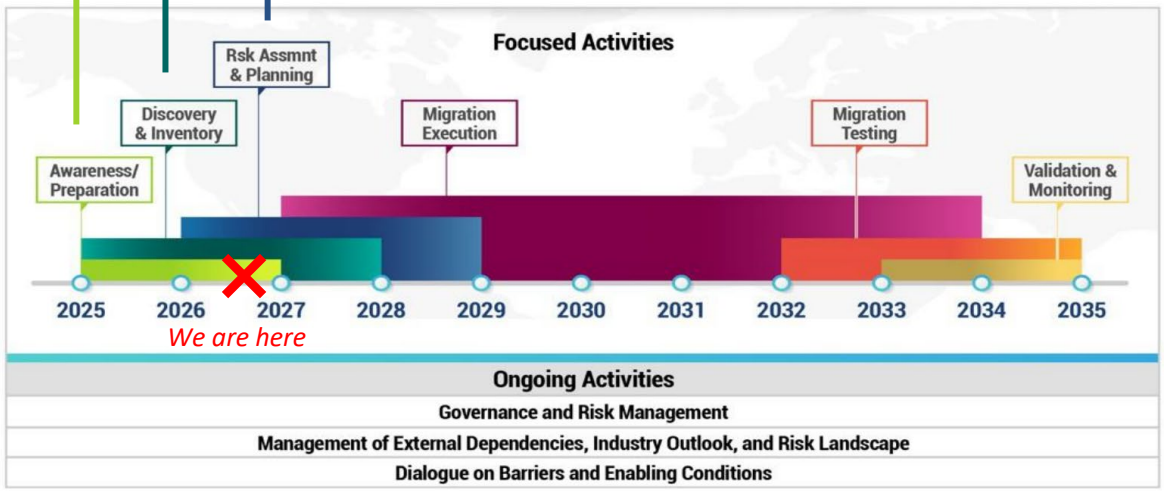
Die Cyber Expert Group hat eine exemplarische Roadmap zur Post-Quanten-Migration erarbeitet.

1 Awareness & Preparation — Risikobewusstsein, initiale Strategien, Schlüsselrollen, Assetmanagement

2 Discovery & Inventory — Inventarisierung & Gapanalyse

3 Risk Assessment & Planning — Migrationspläne & Kompetenzaufbau, angepasste Governance und Risikomanagementprozesse

Schwerpunkte in 2026



Copyright © 2026 Accenture. All rights reserved.

Was ist ein Kryptoinventar?

Transparenz über kryptografische Objekte und deren Einsatzkontext

Steuerung und Überwachung, insb. Im Hinblick auf die PQC-Migration

Zuordnung der Kryptobjekte zu Businessassets und -prozessen

Bewertung gegen regulatorische und interne Anforderungen

Identifikation von Schwachstellen und Auditnachweise

Ein Kryptoinventar erfordert zwei technische Kernfähigkeiten

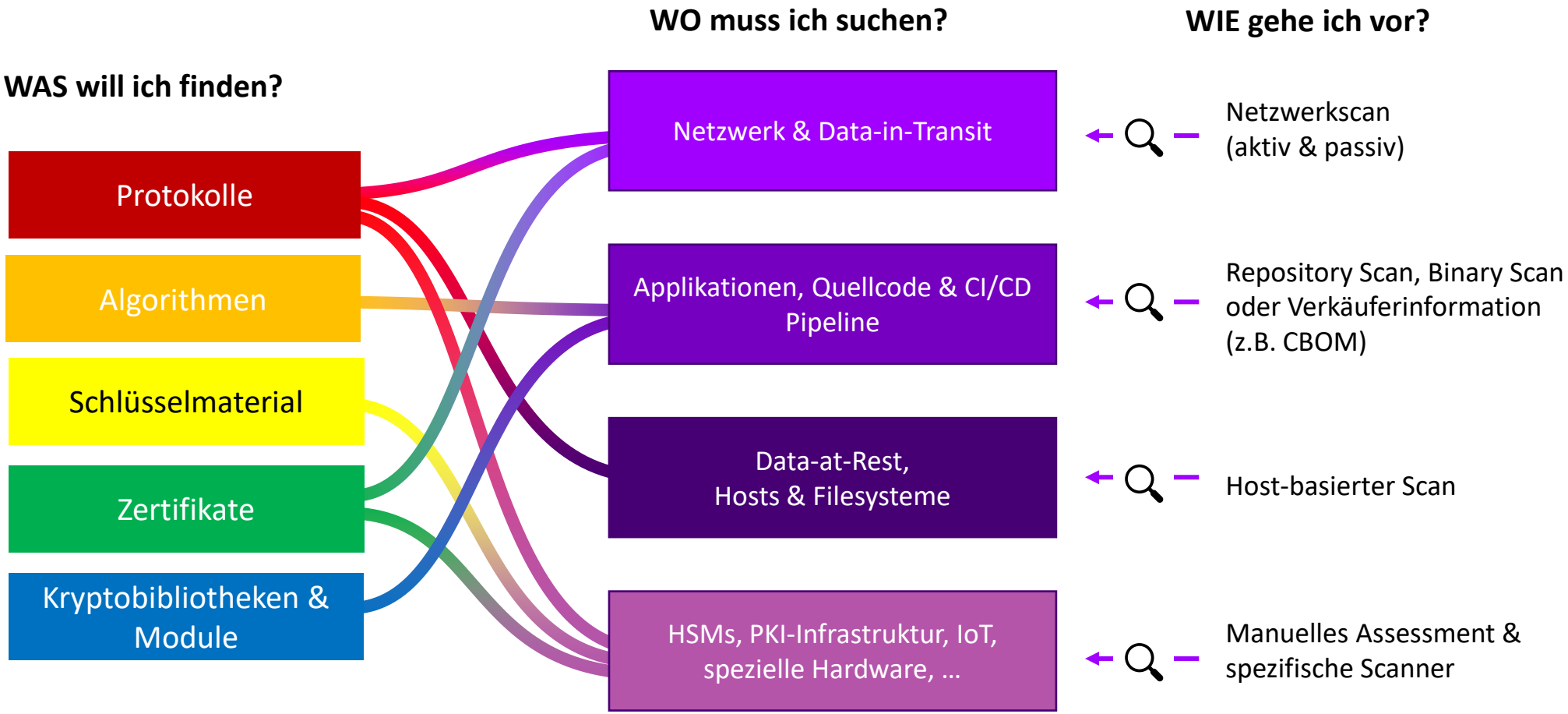
Erhebung der Kryptoobjekte

Darstellung der Kryptoobjekte

Copyright © 2026 Accenture. All rights reserved.

Erhebung der Kryptobjekte

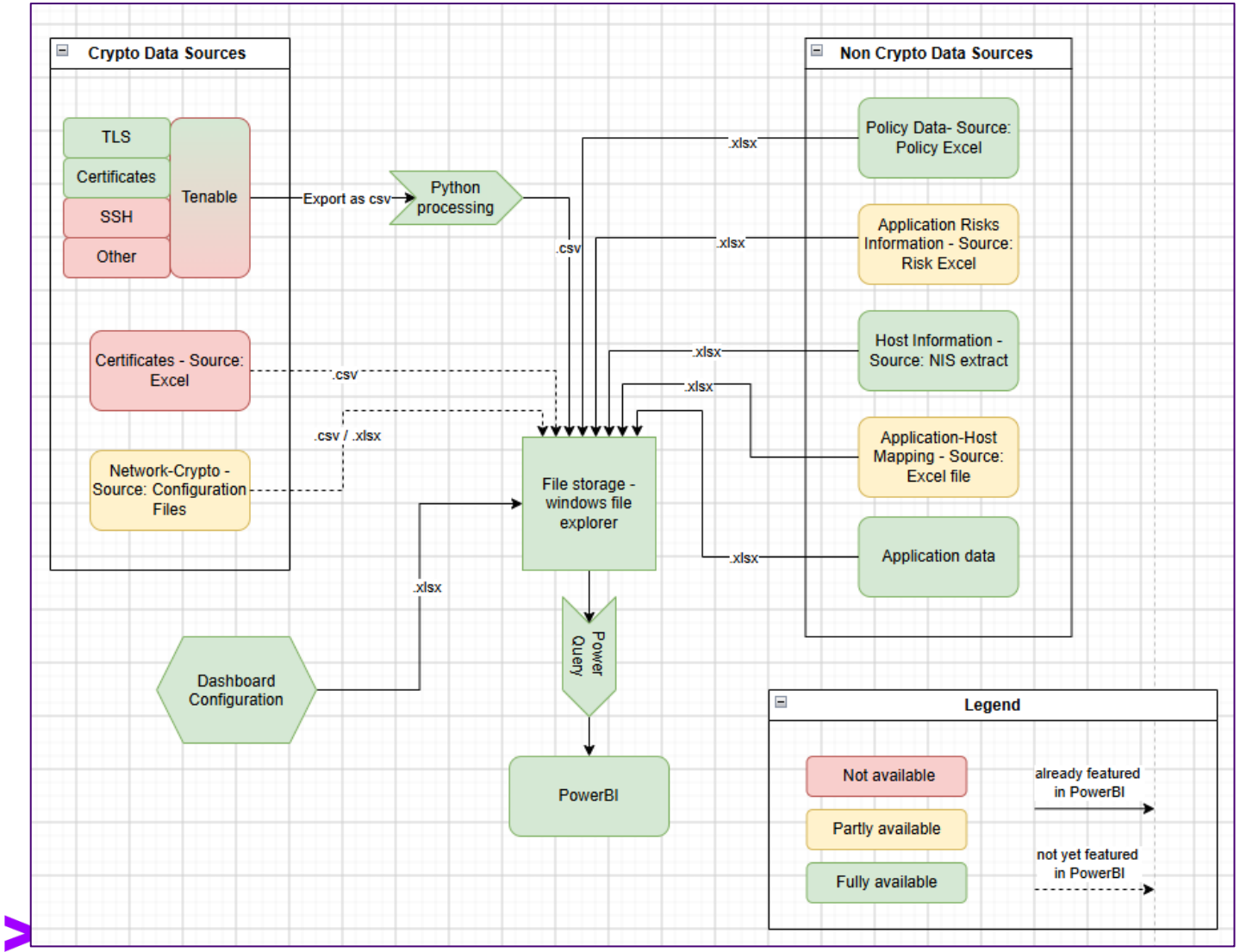
Kryptographie ist an jeder Ecke zu finden, man muss nur wissen, wo man suchen muss.



Copyright © 2026 Accenture. All rights reserved.

Es muss nicht kompliziert sein.

Eine Implementierung mit PowerBI und vorhandenen Scannern.



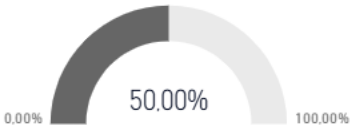
Hauptfunktionen

- **Compliance Monitoring**
- **Übersicht über Zertifikate**
- **PQC Readiness**
- **Risikobasierte Priorisierung**
- **Identifizierung der Verantwortlichen**

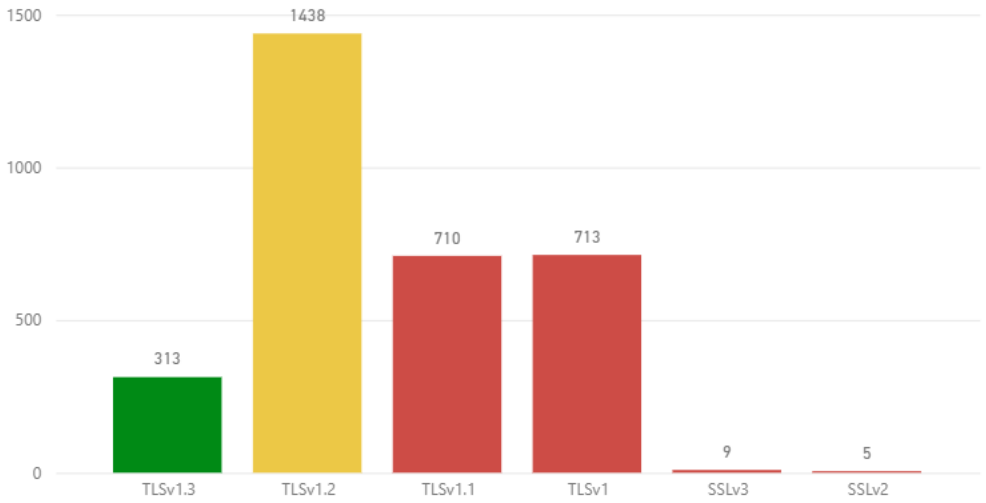
Copyright © 2026 Accenture. All rights reserved.

Es muss nicht kompliziert sein.

Compliance Status of TLS Versions

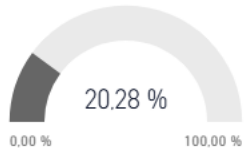


The gauge chart shows the percentage of servers offering only compliant policies (TLS1.3 or TLS1.2).

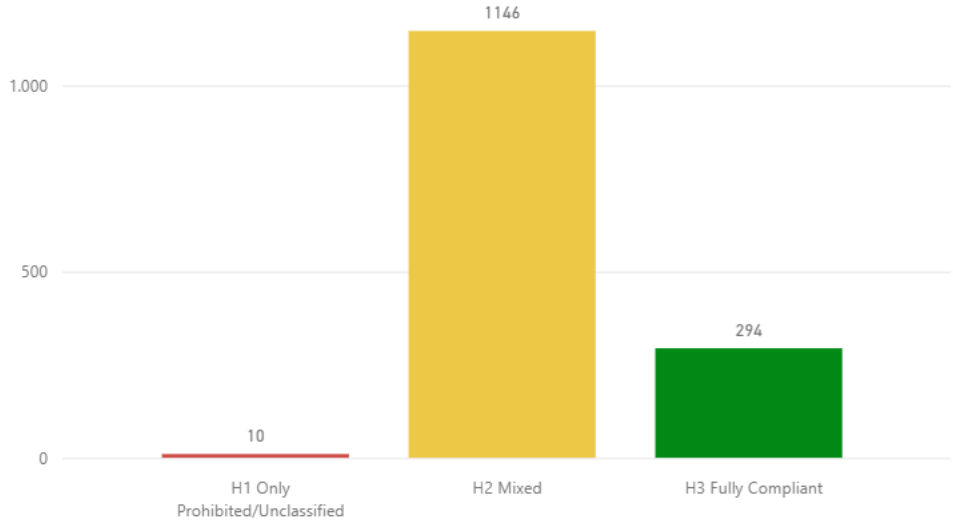


The barchart shows the numbers of servers supporting a given TLS version. The colours show the compliance status according to policy for a given TLS version. Permitted policies are shown in green, "use-with-caution"-policies in yellow, and prohibited policies in red. The categories are not exclusive, as one host may offer several TLS-versions.

Compliance Status of supported Cipher Suites



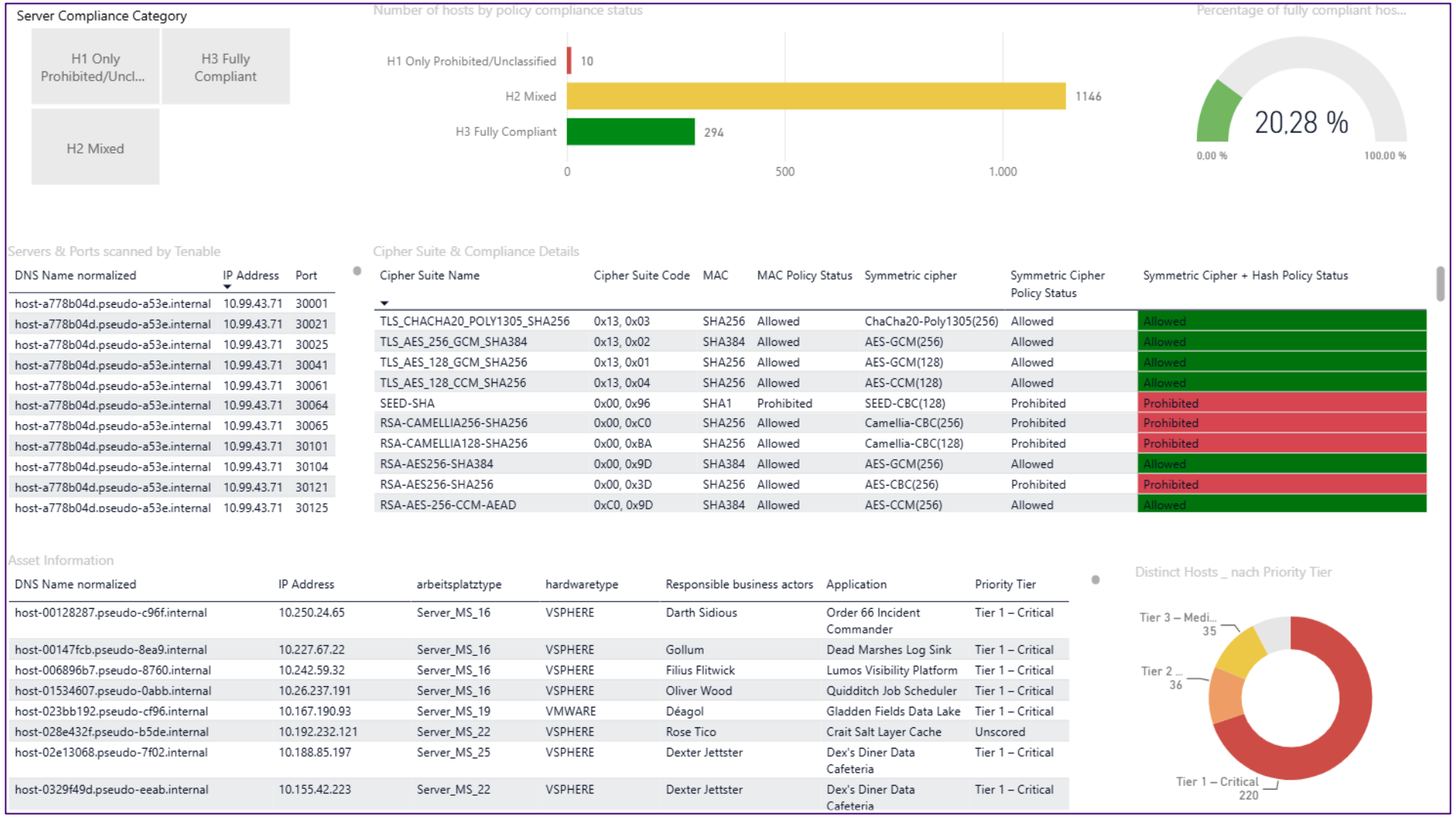
The gauge chart shows the percentage of servers offering only compliant cipher suites.



The barchart shows the numbers of servers based on the compliance status of supported TLS-Cipher suites. The red column shows servers offering prohibited cipher suites only, the green column those offering only permitted ciphers and the yellow column those offering both prohibited, permitted, and "use-with-caution"-cipher suites.

Copyright © 2026 Accenture. All rights reserved.

Es muss nicht kompliziert sein.



Copyright © 2026 Accenture. All rights reserved.

Fragen ihr habt?

