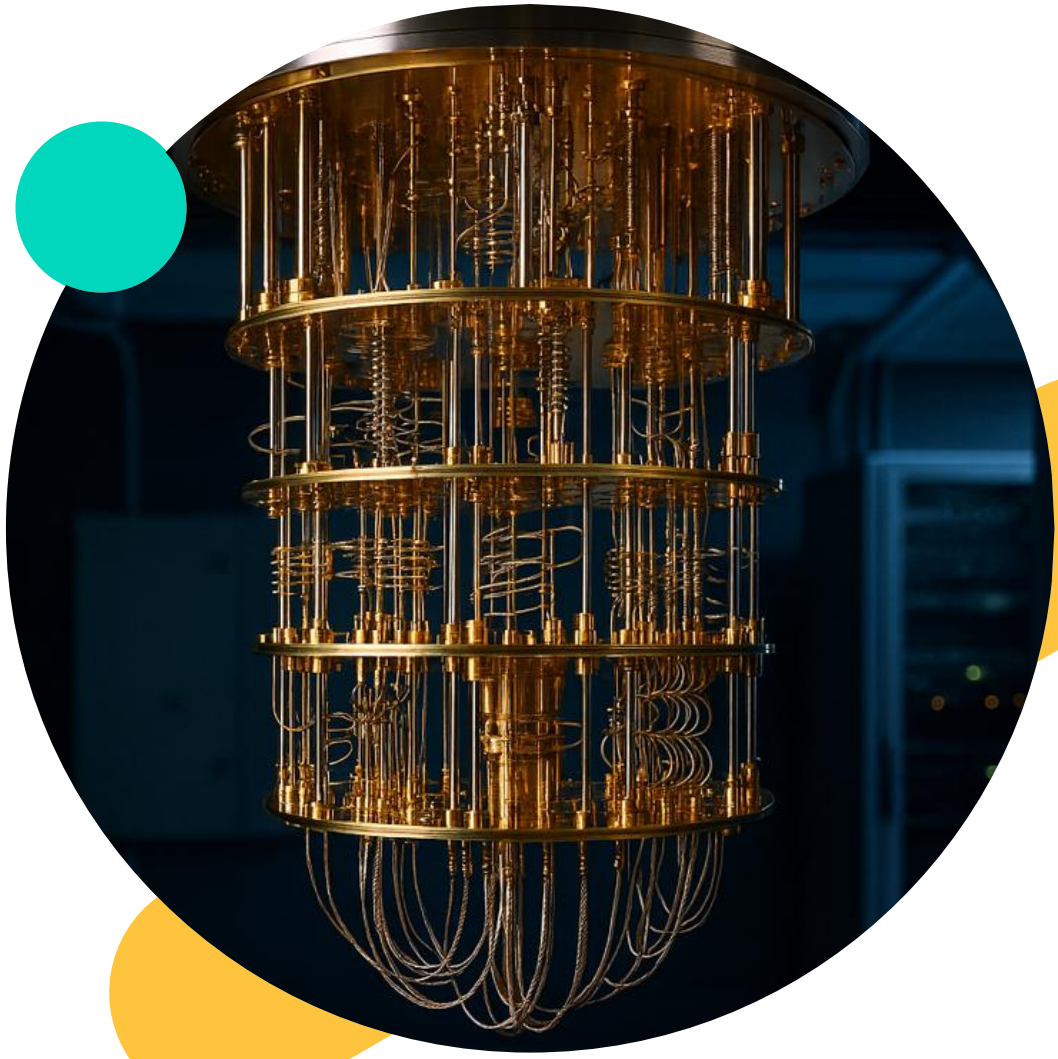
Verschlüsselung im Quantum Zeitalter



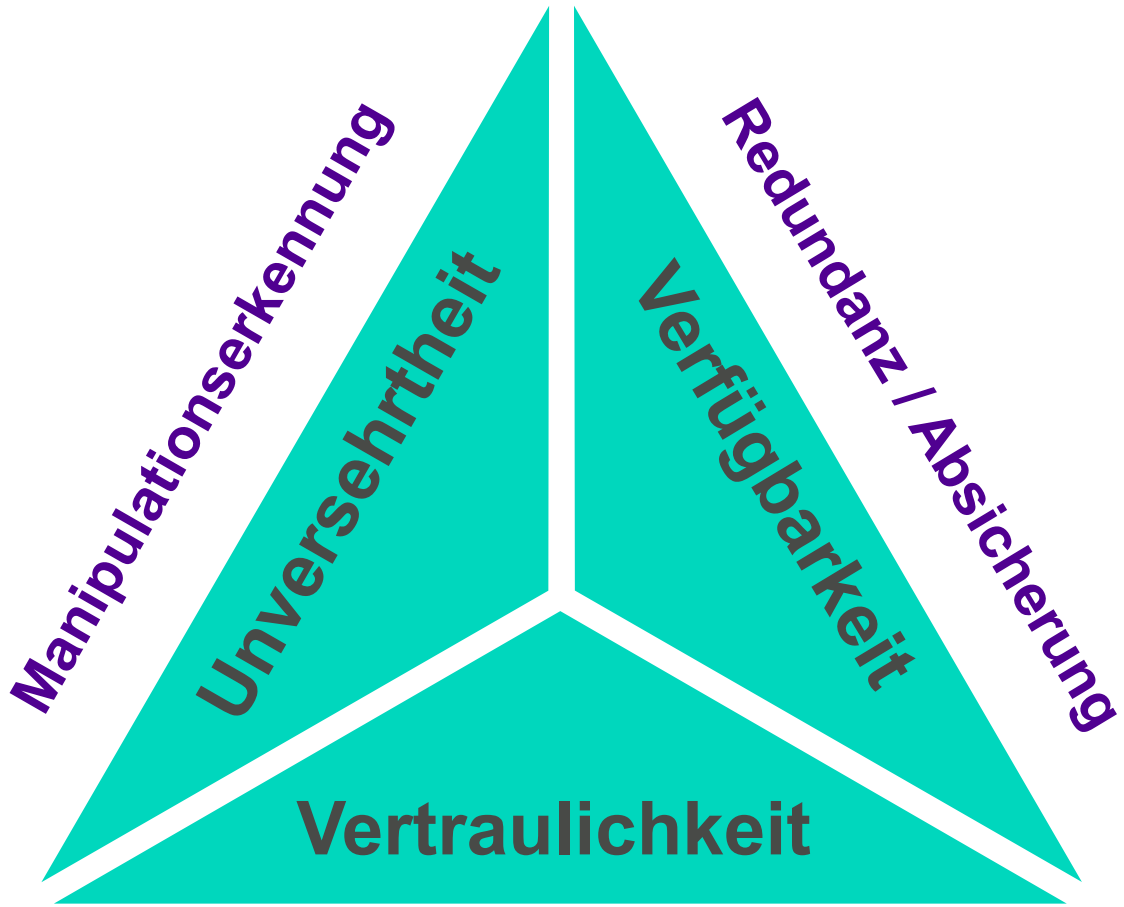
Klemens Birner
Produktmanager Optische Dienste
Colt Technology Services

November 2025

Agenda

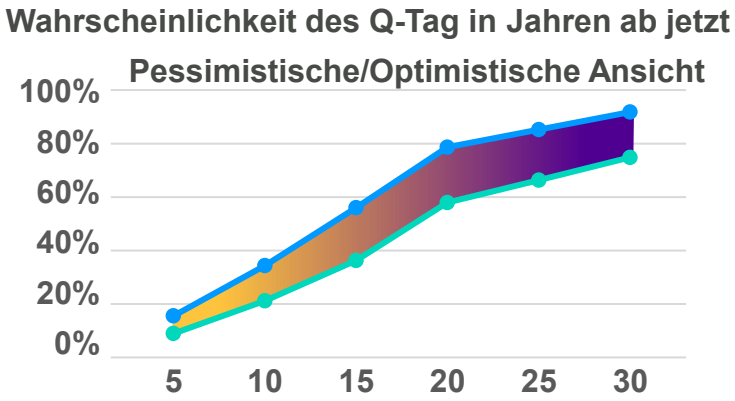
1. Einführung
2. Risiken klassischer Verschlüsselung
3. Möglichkeiten dem Risiko zu begegnen
4. Verschlüsselungsoptionen zur Quantum Sicherheit heute
5. Warum ist das wichtig für Colt Kunden?
6. Empfohlene Schritte
7. Colt Quantum Sicherheit Projekte zur Technologie Erprobung
8. Colt Angebot – Optionen

Einführung



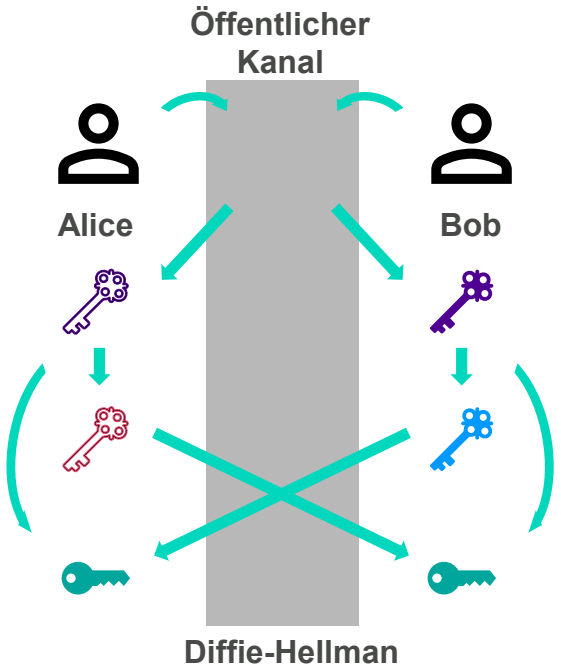
Quantum-sichere Verschlüsselung

Risiken klassischer Verschlüsselung



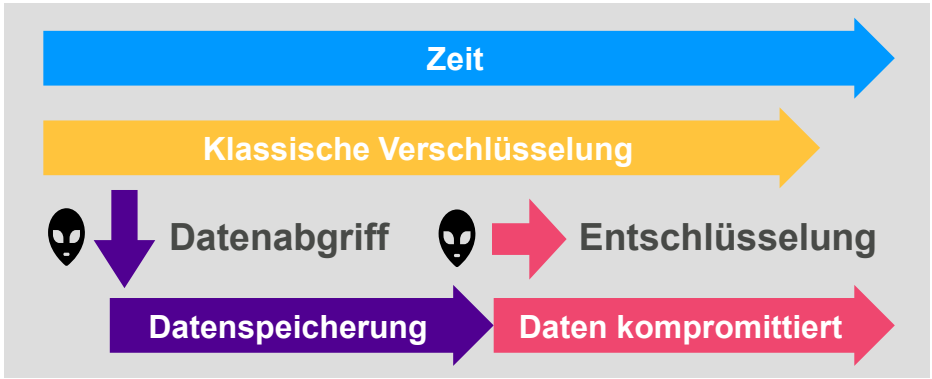
Aktuelle Verfahren zur Verschlüsselung nutzen häufig:

- AES256 zur Daten-Verschlüsselung
- Diffie-Hellman für den Schlüsselaustausch
- Layer 1 (Hardware), MacSEC (L2), IPsec (L3)



Es gibt 2 fundamentale Risiken dazu:

- Zeit bis zum "Q-Tag" ist unklar, hoher Aufwand und Dauer bis Lösungen implementiert sind
- Sensible Daten können heute abgegriffen und später entschlüsselt werden

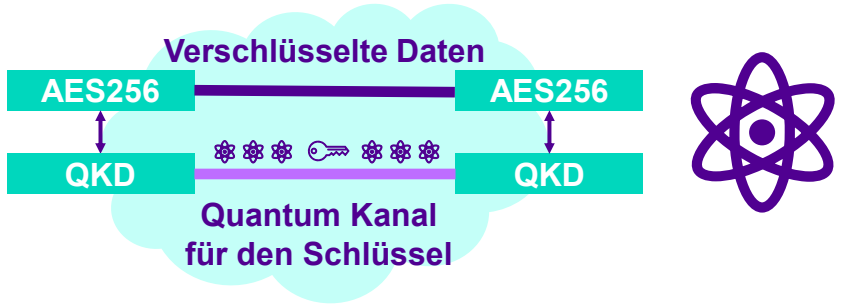


Möglichkeiten dem Risiko zu begegnen

Sicherheitstechnologien aus der Netzwerk- und Übertragungstechnik-Sicht:

A. QKD – Ein Schlüsselaustausch über Quantum-Kanal gilt aus heutiger Sicht als hochgradig sicher

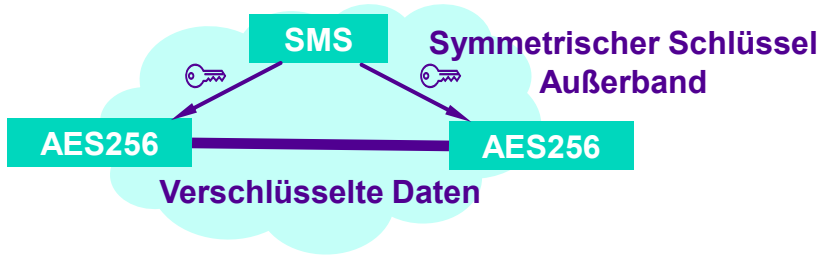
- Aktuelle Lösungen typischerweise im Metro-Bereich
- Gesicherte Knoten National und International
- Satelliten-basierte Lösungen bei der Langstrecke



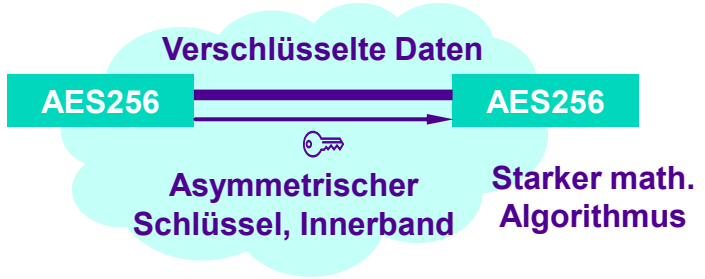
Mehr Details dazu auf der folgenden Seite...

B. Verschlüsselungstechnologien, die aus heutiger Sicht Quantum Computer Attacken widerstehen

- PSK – Pre-shared Key

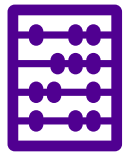


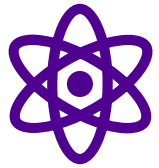
- PQC – Post Quantum Cryptography



Verschlüsselungsoptionen zur Quantum Sicherheit heute

	Klassische Hardware basierende Verschlüsselung	Post-Quantum Cryptography **PQC**	Pre-Shared Key **PSK**	Quantum Key Distribution **QKD**
Anwendungsfall	Bisherige/heutige Fälle	Quantum-Sicherheit	Quantum-Sicherheit	Hochsicherheit
Ansatz/Technologie	Mathematisch	Komplexe Mathematik	Schlüssel separiert	Quantum Physik
Anfälligkeit für Quantum Attacken	**Hoch**	Sehr niedrig	Sehr niedrig	**Quasi NULL**
Schlüsselaustausch	In-band, Asymmetrisch	In-band, Asymmetrisch	Out-Band, Symmetrisch	Out-Band, Quantum
Abhörerkennung	Nein	Nein	Nein	Ja
Einsatzfälle	Großflächig ausgerollt	Einzelne Anwendungen	Einzelne Anwendungen	Frühstadium, Pilot





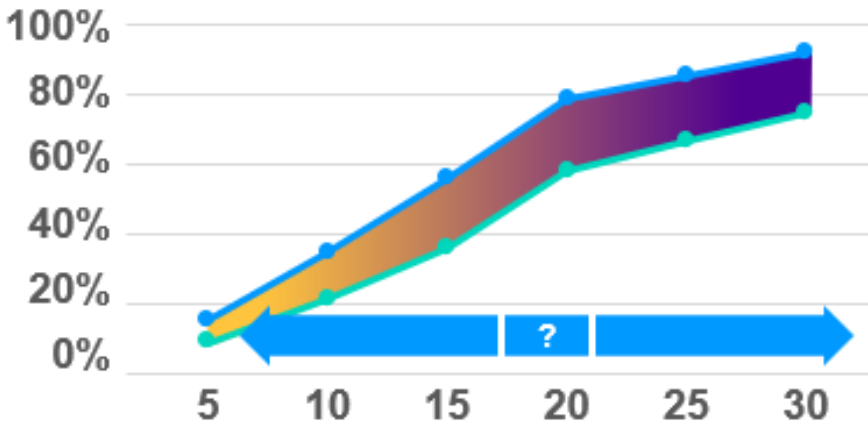
Warum ist das wichtig für Colt Kunden?

Digitale Souveränität ⇨ Schutz sensitiver Daten vor Abgriff und Missbrauch

Der Fokus liegt hier auf Risiken bei der Datenübertragung

Der "Q-Tag" wird kommen, wann ist unklar.

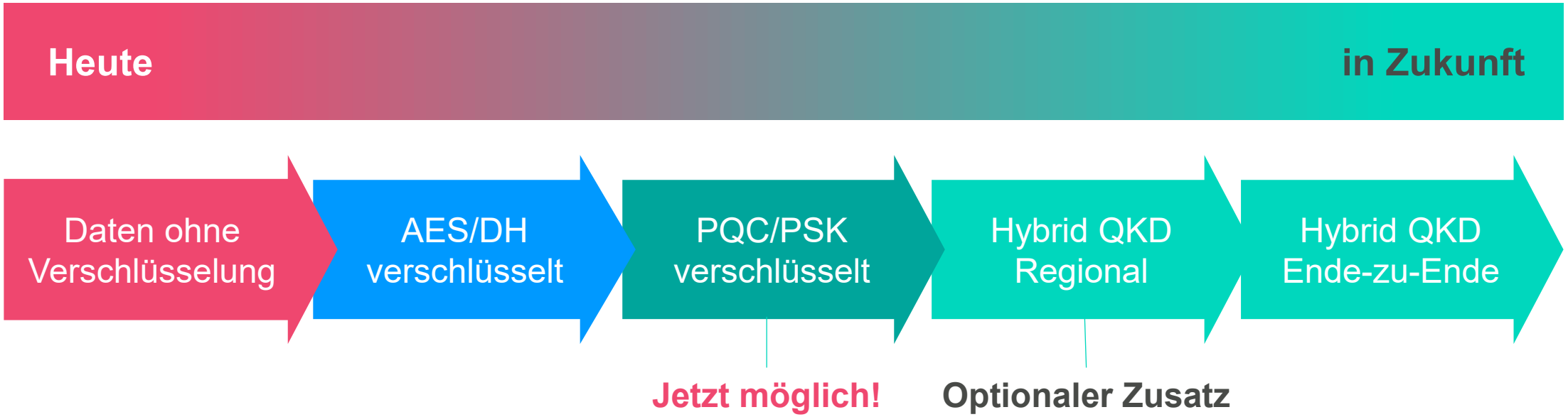
Daten könnten heute schon mitgeschnitten und später entschlüsselt werden.



Wir sind also gut beraten, uns schon heute dafür zu wappnen! Es wird Zeit brauchen, um die nötigen Schritte zu planen und umzusetzen, deshalb ist *jetzt* der beste Zeitpunkt damit zu beginnen.

Empfohlene Schritte

Colt kann helfen die Lücke zu schließen!



Colt Quantum Sicherheit – Projekte zur Technologie Erprobung

Ciena Nokia Adtran IDQ Toshiba

1 Metro

100 km, London City – Slough – Powergate

Quantum sichere (PSK, PQC) Technologie

1x/2x Faser(n), P2P/Trusted Node/Regen

2 International

1400 km, London – Frankfurt

Quantum sichere (PSK, PQC) Technologie

3 Interkontinental

6000 km, London – New York

Quantum sichere (PSK) Technologie *)

(in Zukunft) Satelliten-basierendes QKD

Live QKD Demonstration 2022 beim Berlinale Film Festival

*) Momentan in Arbeit

Colt Angebot – Mehrere Optionen, zugeschnitten auf Ihren Bedarf

Quantum-sichere Übertragung von Colt – die nächsten Quartale im Überblick:

Colt Encryption – Hardware-basiert — **bewährte Lösung, aber nicht Quantum-safe**

Colt Quantum-sichere Verschlüsselung – PQC- oder PSK-basierend — **Verfügbar** — **Neu!**

Interim Lösung — **Colt QKD Metro Lösung – Hybrid in Verbindung mit PQC oder PSK** — **Neu!**

Colt QKD Langstrecke

Danke für die Aufmerksamkeit