

16:50 – 17:10 Uhr

Quantencomputer und die Auswirkungen auf die digitale Sicherheit

Filip Vukadin

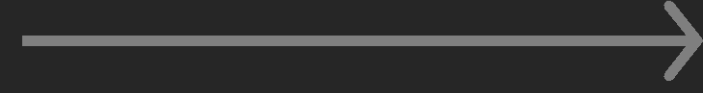
Quantencomputer und die Auswirkungen auf die digitale Sicherheit

Bechtle Xperience 30.10.2025



Was ist ein Quantencomputer?

Der Schritt in die Quantenwelt



Klassische Bits können nur zwei Zustände annehmen - 0 oder 1 - ähnlich wie ein Lichtschalter, der entweder ein- oder ausgeschaltet ist.

Ein Qubit hingegen funktioniert wie ein Dimmer: Es kann nicht nur 0 oder 1 darstellen, sondern auch alle Zwischenzustände gleichzeitig.

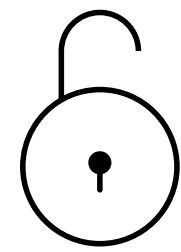


Warum Quantencomputer unsere digitale Sicherheit gefährden

Aktuell genutzte kryptografische Verfahren basieren auf mathematischen Problemen, die Quantencomputer künftig effizient lösen könnten.

Klassische Computer

Quantencomputer



Millionen Jahre

Stunden

**Betroffen sind
hauptsächlich:**

Digitale Signaturen

Schlüsselaustausch

Die EU-Kommission rät zu ersten Schritten, die bis **Ende 2026** umgesetzt werden sollen, wobei für Anwendungsfälle mit hohem Risiko bereits **2031** eine Umsetzung erforderlich ist.

Regierungsorganisationen gehen davon aus, dass ab **2030-2035** mit der Existenz von “kryptografisch relevanten” Quantencomputern zu rechnen ist. (NIST, BSI, ANSSI u.a.)

1. [EU: Publication of Post Quantum Encryption Roadmap – June 2025](#)

Was wird ein “Cyber-Krimineller” tun können?

Harvest now, decrypt later

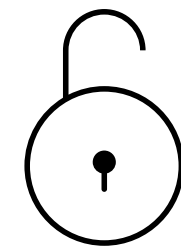
Davor



Aufzeichnung von verschlüsselten vertraulichen Daten, um sie später zu entschlüsseln

Verfügbarer leistungsfähiger Quantencomputer

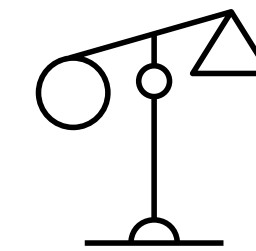
Danach



Stehlen von kryptografischen Schlüsseln und Entschlüsseln von Daten



Störung von digitalen Aktivitäten durch betrügerische Authentifizierung



Manipulation von digitalen Verträgen und der Historie durch Fälschung von digitalen Signaturen

Wozu brauchen wir asymmetrische (“Public Key”) Kryptografie

Vertraulichkeit | Authentifizierung | Integrität | Nichtabstreitbarkeit

Quantenresilienz im gesamten Unternehmensökosystem

IBM Quantum Safe
EXECUTION FRAMEWORK

Unternehmen & Strategie

Etablierung einer Vision und klarer Governance-Strukturen zur Förderung einer unternehmensweiten Vereinheitlichung von Massnahmen zur Modernisierung der Kryptografie



C-Level



**Compliance, Risiko
und Cybersicherheit**

Wichtige Erkenntnisse

Beginnen Sie mit Abhängigkeiten, nicht mit Krypto-Artefakten

- Kryptografie wirkt nicht isoliert.
- Abhängig von Anwendungen, Infrastrukturen, Anbietern.
- Verständnis dieser Abhängigkeiten ist entscheidend für Planung und Auswirkung.

Geschäftsfelder, Apps & Plattformen

Transformation von Systemen, Anwendungen und DevOps-Pipelines hin zu agilen und zukunftsicheren kryptografischen Verfahren



**Business Asset /
Project Owners**



**Entwickler / Plattform
Teams**

Klarheit des Zielzustands ermöglicht eine sinnvolle Planung

- Ohne gemeinsame Architektur-Vision wird Migration reaktiv.
- Fragmentierte Ansätze durch Legacy-Systeme und Anbieter-Roadmaps.

Dritte & Lieferanten

Abstimmung mit externen Partnern und Plattformanbietern hinsichtlich ihrer Krypto-Standards, um ein sicheres und richtlinienkonformes Ökosystem zu etablieren



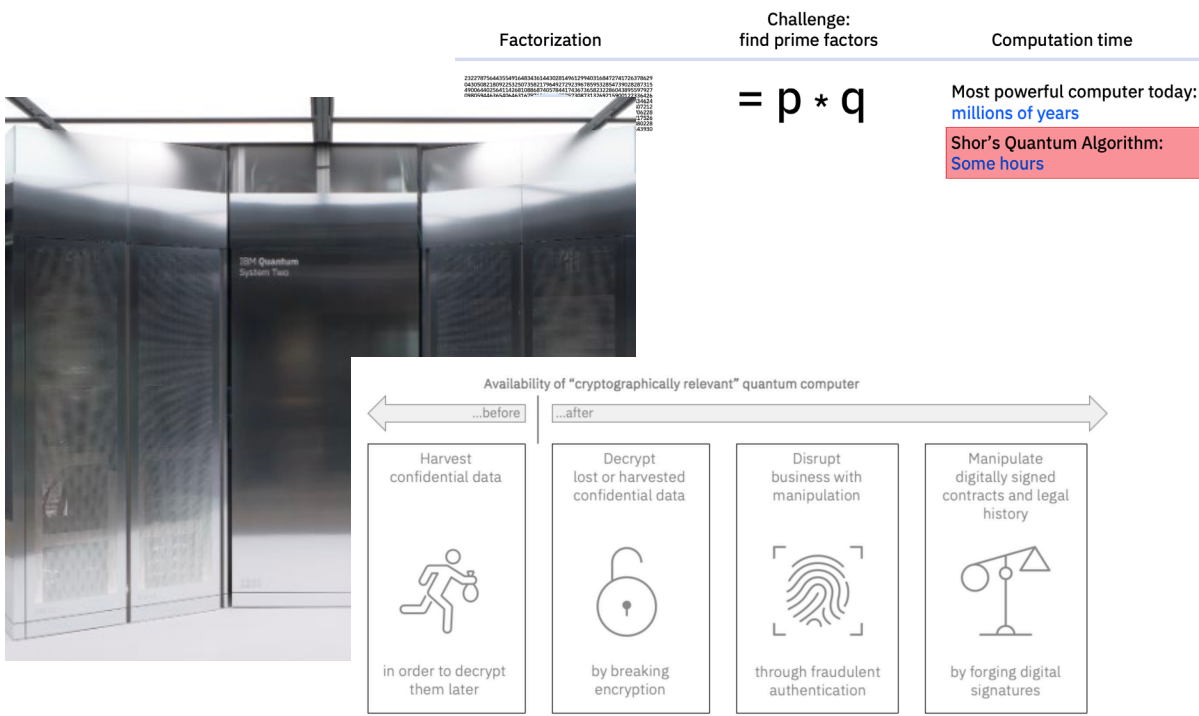
**3rd Party
Entwickler /
Technologieanbieter**

Migration ist ein Lebenszyklusproblem, nicht nur ein technisches Upgrade

- Erfolg braucht abgestimmte Asset-Zeitpläne.
- Reale Migrationsrisiken aktiv managen.
- Transformationsmomente nutzen.
- Kryptografie als integrierten Teil der Gesamtstrategie behandeln.

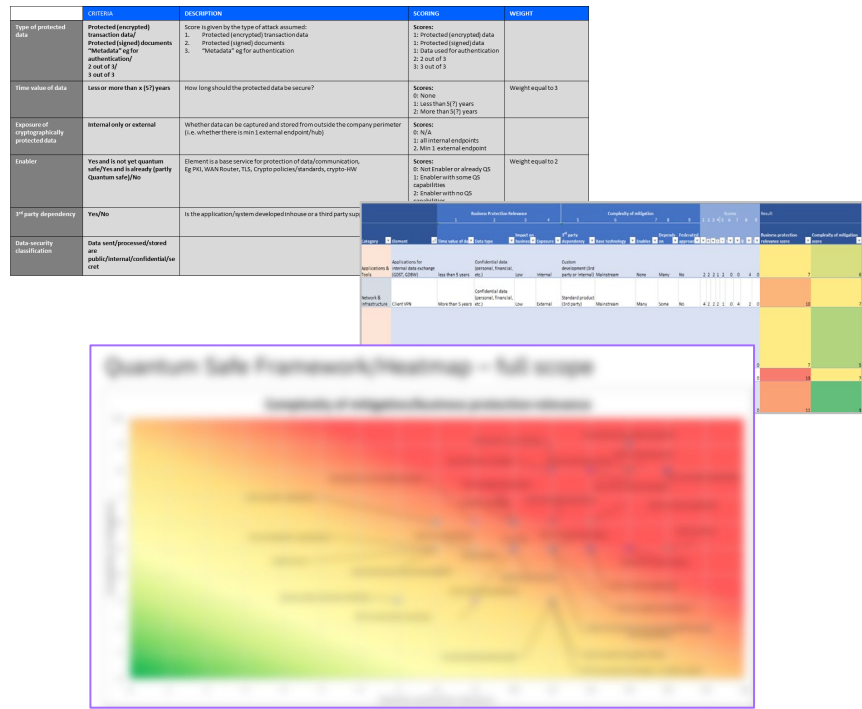
Unser Fahrplan zur Quantenresilienz – Mögliche erste Schritte

1. Quantum-Safe Deep Dive



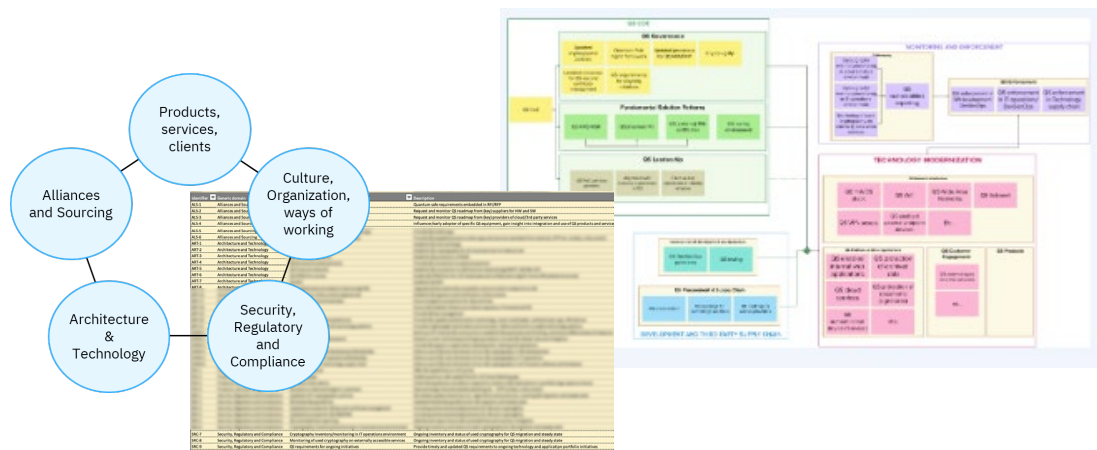
- Quantum-Safe Projektinitiierung (d.h. Kick-off, Identifikation der Stakeholder, Interviewplan, Dokumentenprüfung)
- Definition der Problemstellung im Bereich Quantum-Safe
- Beschreibung der Treiber und Rahmenbedingungen
- Überblick über die wichtigsten Lösungsansätze zur Risikominderung und deren Gültigkeitsbereich

2. Quantum-Safe Heatmap



- Bietet einen Überblick über relevante Kunden-Kontexte und deren Quantenexposition:
 - Relevante Geschäftsbereiche
 - Systeme/Technologien
 - Kritische geschützte Assets
 - Anwendungen und Tools
 - Unterzeichnete Dokumente
 - Richtlinien und Standards

3. Quantum-Safe Implementierungsmodell

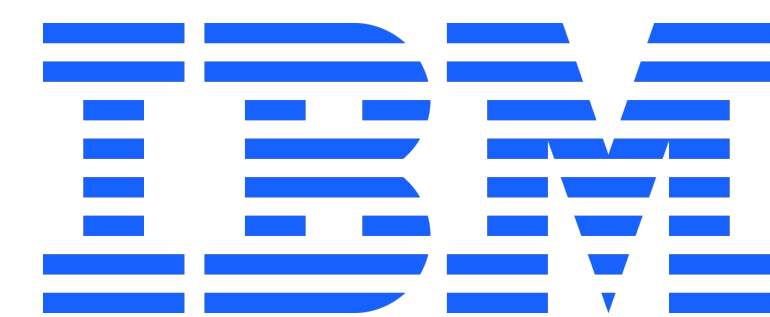


- Definition von organisatorischen und technischen Fähigkeiten für die Quantum Safe Transformation
- Entwicklung eines High-Level Implementierungsmodells für die Quantum-Safe Transformation

4. Quantum-Safe Transformations-Roadmap



- Grober Fahrplan für den kurz-, mittel- und langfristigen Quantum-Safe Fokus.
- Definition der Fähigkeiten, Rollen und Verantwortlichkeiten, die für die Umsetzung von Horizont 1 (1 Jahr) erforderlich sind
- Erstellung eines Ausführungsplans zur Einleitung von Horizont 1
- Beschreibung der angemessenen Vorbereitungsmaßnahmen



Filip Vukadin

Quantencomputer und die Auswirkungen auf die digitale Sicherheit

Ihr Feedback zählt

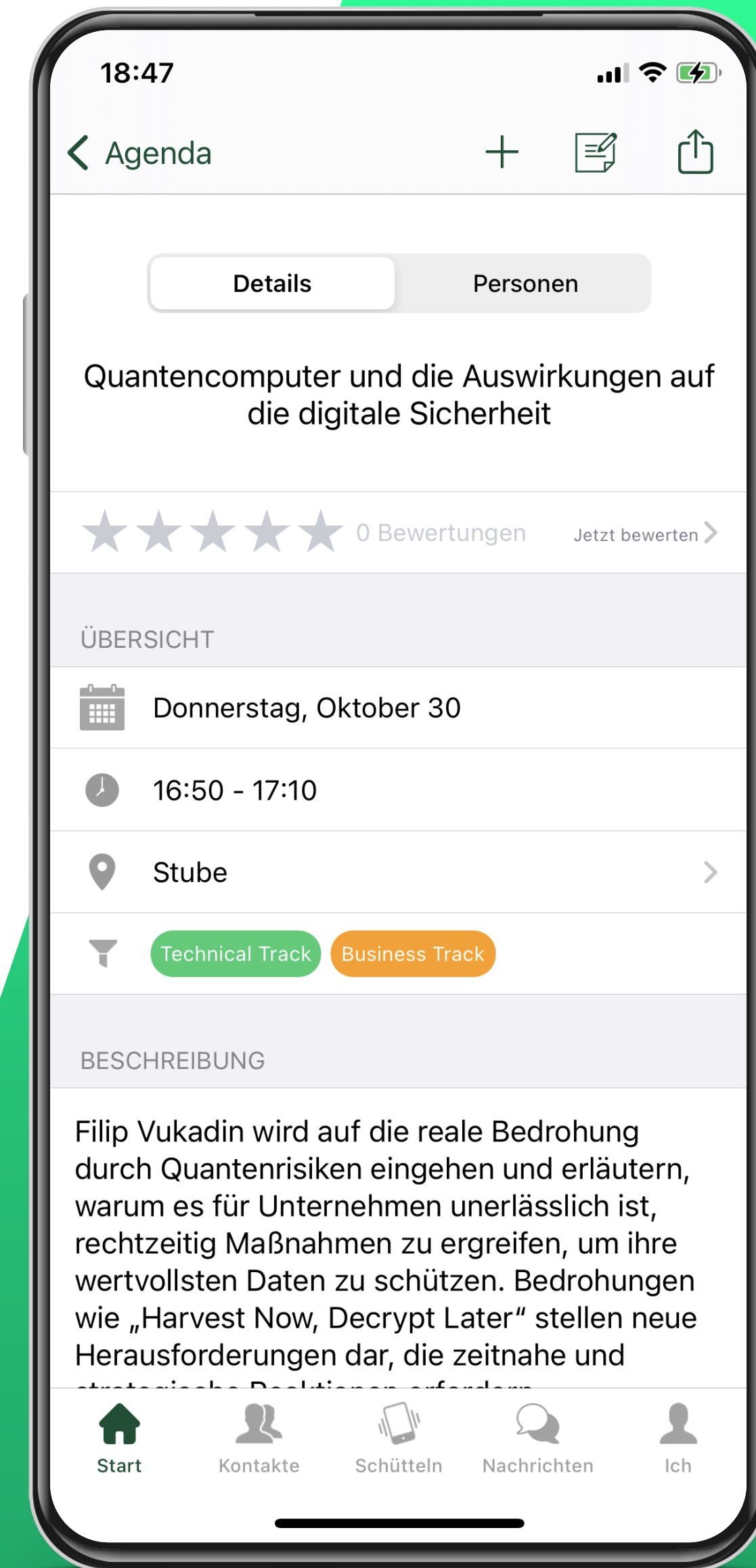
*Jetzt in der App
bewerten.*



App Store



Play Store



17:15 - 17:45 Uhr

Ofenhalle EG

Keynote: Ist KI ein Alleskönner?

Elisabeth Vinek

Claudio Mirti