Post-Quantum Security

Die Bedrohung besteht heute, die Folgen liegen in der Zukunft.

Quantencomputer stellen eine ernsthafte **Bedrohung** für die **klassische Kryptographie** dar. Da sie mathematische Probleme schnell und effizient lösen, können sie **gängige Algorithmen und Protokolle** wie **RSA** oder Diffie-Hellman Key Exchange binnen kürzester Zeit **kompromittieren.** Dies **gefährdet** erheblich die **Sicherheit** sensibler Daten und digitaler Kommunikation.

FortIT unterstützt Sie aktiv bei der **Umstellung** auf **Post-Quanten-Kryptographie (PQC)**, um Ihre kritischen Daten und Systeme gegen Quantenbedrohungen zu **schützen**.

Herausforderungen der Post-Quanten-Kryptographie (PQC)

Betroffenheit: Verständnis der spezifischen Risiken und Identifizierung der Datenflüsse und Systeme, die von Quantencomputern betroffen sind.

Geschäftskontinuität: Aufrechterhaltung der Geschäftstätigkeit während der Umstellung auf PQC und der Neuverschlüsselung bestehender Daten.

Aufwändige Migration: Umfassende Anpassungen auf technischer und organisatorischer Ebene sind für den Wechsel zu PQC nötig.

Legacy Systeme: Analyse und spezifische Anpassung von Legacy-Systemen für PQC-Kompatibilität.

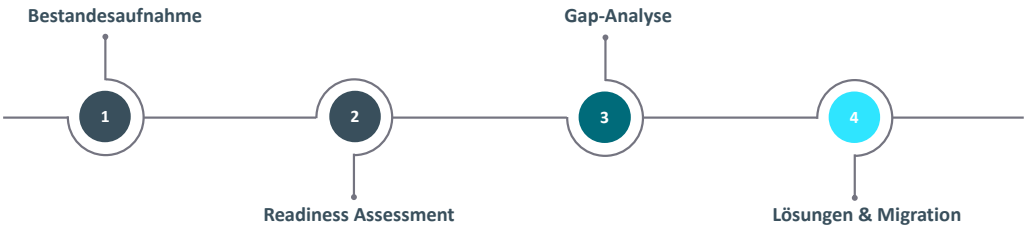
Unklarer ROI: Die Investition in PQC steht oft in Frage, da der unmittelbare Nutzen oftmals nicht erkennbar ist.

Management Buy-in: Aufbau vom Verständnis für die Risiken und Notwendigkeit der Umstellung auf PQC im Unternehmen.

Post-Quantum Security

Schritt-für-Schritt zu einer post-quantenresistenten IT-Landschaft

Wir begleiten Sie auf effizientem und praktikablem Weg zu Ihrer Sicherheit gegen Quanten unterstützte Angriffe.



1. **Sind wir betroffen?** In einem high-level PQC-Impact-Analysis Workshop mit dem Management-Team werden die kritischen Geschäftsprozesse und die darunter liegenden Systeme/Daten identifiziert. Das Ergebnis ist ein PQC-Risiko-Inventar, inkl. konkreten Empfehlungen zur PQC-Umstellung.
2. **Was müssen wir schützen?** Durch eine detaillierte Strukturanalyse und Aufschlüsslung der relevanten Daten, abhängigen IT-Ressourcen und Prozesse werden die genauen Bedürfnisse an der Soll-Zustand der identifizierten Schutzobjekte anhand der konkreten Bedrohung durch Quantenrisken eruiert.
3. **Wie gehen wir vor?** Ein priorisierter Umsetzungsplan (Roadmap) wird erstellt, unter Berücksichtigung von Quick-Wins und Abhängigkeiten der vorgeschlagenen Massnahmen sowie laufenden Projekten.
4. **Migration zu einer post-quanten-resistenten IT-Landschaft**. Durch technische Projektleitung, fachliche Unterstützung und Reviews, unterstützen wir Ihre erfolgreiche Migration zu PQC.

Ihre Vorteile durch die Implementierung eines post-quanten Konzepts

Vertrauen im Markt	Wettbewerbsvorteil	Zukunftsfähigkeit	Kostensenkung
Erhöhte Datenintegrität stärkt das Kundenvertrauen	Optimiertes Prozess- und Sicherheits-management	Langfristige Datensicherheit gegen Quantenbedrohungen	Reduzierte Sicherheits-kosten durch Anpassung an neue Standards

Setzen Sie auf unsere Expertise und Erfahrung für Ihren Erfolg

- ✓ Fundiertes Wissen über Kryptografie, Prozessgestaltung und Architektur.
- ✓ Umfassende Expertise in post-quanten sicheren Algorithmen und NIST PQC Challenge.
- ✓ Ganzheitlicher Risikomanagementansatz für optimale Sicherheit.

Kontaktieren Sie uns heute!

Saner Çelebi
Head Consulting Services
saner.celebi@fort-it.ch

Dominik König
Lead Secure Cryptography
dominik.koenig@fort-it.ch