protiviti®
Global Business Consulting

POST-QUANTUM CRYPTOGRAPHY

KRYPTOGRAFISCHE RESILIENZ FÜR DAS QUANTENZEITALTER

Foto: Getty Images

Quantencomputer werden derzeit eingesetzte Public-Key-Verfahren wie RSA, Diffie-Hellman und Elliptic Curve Cryptography perspektivisch angreifbar machen. Gleichzeitig können Angreifer bereits heute verschlüsselte Daten sammeln, um sie später mit Quantenrechnern zu entschlüsseln („store now, decrypt later"). Informationen, die über viele Jahre vertraulich bleiben müssen, sind dadurch bereits heute gefährdet – und sollten schon jetzt geschützt werden.

Post-Quantum Cryptography

Post-Quantum Cryptography (PQC) umfasst mathematisch fundierte Verschlüsselungs- und Signaturverfahren, die gezielt so entworfen wurden, dass sie auch künftigen Angriffen durch leistungsfähige Quantencomputer standhalten. Diese Verfahren lassen sich bereits auf heutiger Hardware und in bestehenden IT-Landschaften implementieren und bieten zugleich eine hohe Resistenz gegenüber bekannten klassischen wie quantenbasierten Angriffen. Dadurch kann PQC schrittweise, kosteneffizient und ohne den Austausch der gesamten Infrastruktur in vorhandene Systeme und Prozesse integriert werden.

Kernfragen einer PQC-Readiness

- Welche Daten und Prozesse sind langfristig kritisch?
- Wo wird Kryptografie heute eingesetzt – intern und/oder bei Dritten?
- Welche Verfahren sind quantenanfällig?
- Wie schnell können Algorithmen ausgetauscht werden?

Wie Protiviti Ihnen helfen kann

Protiviti unterstützt Sie über den gesamten Migrationsweg beim Aufbau einer belastbaren und krypto-agilen PQC-Roadmap: von der ersten Awareness und dem Aufbau eines zentralen Kryptographie-Inventars über eine fundierte Risiko- und Gap-Analyse bis zur Auswahl, Erprobung und produktiven Implementierung quantensicherer Algorithmen.

Warum jetzt handeln?

BSI: Übergang zu PQC jetzt einleiten

Das BSI stellt klar: Nicht mehr „ob" sondern „wann" steht im Vordergrund; die Migration zu PQC soll aktiv vorangetrieben werden.

„Store now, decrypt later" ist bereits relevant

Vor allem das Aushandeln der kryptographischen Schlüssel (Key Agreement) ist durch künftige Quantencomputer bedroht; langfristig schützenswerte Daten müssen heute betrachtet werden.

BSI fordert Krypto-Agilität

Neue und weiterentwickelte Kryptoprodukte sollten flexibel anpassbar sein, damit Verfahren gezielt ausgetauscht werden können.

Migration dauert Jahre, nicht Monate

Inventarisierung, Priorisierung, Tests und Umsetzung großer Kryptolandschaften erfordern einen strukturierten Transformationsansatz.

Wir machen Ihre Kryptografie zukunftsfähig.
Ein 100%iger Schutz vor technologischem Wandel ist nicht realistisch – aber eine strukturierte, krypto-agile Vorbereitung reduziert Migrationsrisiken und stärkt Ihre digitale Resilienz.

Die PQC-Methodik von Protiviti

Vom Kryptografie-Inventar zur krypto-agilen Umsetzung

1	**Sensibilisierung**	Stakeholder sensibilisieren, gemeinsame Sprache schaffen, Auswirkungen auf IT, Security, Compliance, Einkauf und Fachbereiche verstehen.
2	**Assessment**	Kryptografie- und Schlüssel-Inventar; Daten, Protokolle, Anwendungen, Drittparteien und technische Constraints erfassen.
3	**Planung & Priorisierung**	Risiko-basierte Roadmap für Quick Wins, Zielarchitektur, Budget, Standards, Lieferanten und technische Abhängigkeiten.
4	**Testing & Auswahl**	PQC-Algorithmen, Parameter, HSMs/Vendor-Produkte und Performance in relevanten Umgebungen testen.
5	**Implementierung & Agilität**	Migration priorisierter Use Cases und Aufbau einer Architektur, die zukünftige Algorithmuswechsel erleichtert.

Jetzt handeln! Erste PQC-Standards sind veröffentlicht; die Migration braucht Inventar, Priorisierung, Tests und technische Umsetzung.

IHRE VORTEILE AUF EINEN BLICK

TRANSPARENZ SCHAFFEN
Vollständiger Blick auf kryptografische Abhängigkeiten, Schlüssel, Protokolle und Drittparteien.

RISIKO PRIORISIEREN
Fokus auf Daten und Systeme mit hoher Kritikalität, langer Schutzdauer oder hoher Exposition.

KRYPTO-AGILITÄT ERHÖHEN
Architekturen vorbereiten, damit Algorithmen künftig schneller ersetzt werden können.

REGULATORIK UNTERSTÜTZEN
Nachvollziehbare Inventare, Roadmaps und Management Summary für Entscheidungsträger.

MIGRATION BESCHLEUNIGEN
Testbare Zielbilder, technische Empfehlungen und priorisierte Maßnahmen statt abstrakter Risikoanalyse.

DRITTPARTEIEN EINBINDEN
Vendoren, HSMs, Cloud-Services und Softwareabhängigkeiten in die PQC-Planung integrieren.

Ansprechpartner



DR. MICHAEL RIECKER
Director
+49 173 575 40 26
michael.riecker@protiviti.com



FLORIAN STRUCK
Senior Consultant
+49 175 659 69 76
florian.struck@protiviti.com

KONTAKTIEREN SIE UNS!

+49 69 963 768 100
contact@protiviti.de
www.protiviti.de

© 2026 PROTIVITI GMBH

protiviti®
Global Business Consulting



90	25	11.000
Standorte	Länder	Mitarbeitende

Protiviti berät Unternehmen praxisorientiert und auf Augenhöhe in den Bereichen Strategie, Organisationstransformation und -optimierung, ESG, Digitale Transformation, Risikomanagement, Interne Revision und Kontrollsysteme, Compliance sowie IT. Gemeinsam finden wir individuelle Lösungsansätze, um Ihr Unternehmen zukunftssicher aufzustellen.

We Care. We Collaborate. We Deliver.