01/2026

sopra steria

POST-QUANTEN-SICHERHEIT IN DER PRAXIS

WEGE ZUR POST-QUANTEN-KRYPTOGRAPHIE

INHALT

DAS NEUE ZEITALTER **DER KRYPTOGRAPHIE**

Wir stehen am Beginn einer technologischen Zäsur. Quantencomputer, die bislang vor allem in Forschungslaboren existierten, rücken Schritt für Schritt in die Praxis vor und damit auch in die Reichweite von Bedrohungsakteuren. Die besondere Rechenleistung der Quantencomputer zeigt sich speziell beim Faktorisieren großer Zahlen und der Lösung diskreter Logarithmen.

Diese Rechenpower stellt eine existenzielle Bedrohung für die heute weltweit genutzte Kryptographie dar. Verfahren wie Rivest-Shamir-Adleman (RSA), Digital Signature Algorithm (DSA), Elliptic Curve Diffie Hellman (ECDH) und Elliptic Curve Digital Signature Algorithm (ECDSA) bilden seit Jahrzehnten die Grundlage digitaler Sicherheit. In absehbarer Zeit könnten diese kryptographischen Algorithmen gebrochen werden.

Die Entwicklung betrifft nicht nur kryptographische Systeme im engeren Sinne, sondern die gesamte digitale Infrastruktur: Kommunikationsnetze, industrielle Steuerungen, Cloud-Plattformen, Gesundheitsdaten, Verwaltungsprozesse. Überall dort, wo Vertraulichkeit, Integrität und Authentizität auf kryptographischen Verfahren beruhen, steigt das Sicherheitsrisiko.

Darauf gilt es sich vorzubereiten. Der Begriff Post-Quantum Cryptography (PQC) beschreibt neue kryptographische Verfahren, die selbst gegenüber leistungsfähigen und derzeit bereits vereinzelt existierenden Quantencomputern resistent sind. Der Übergang, also von klassischen zu quantensicheren Verfahren, ist jedoch kein einfacher Technologiewechsel. Das ganze Ökosystem aus Anwendungen, Geräten, Standards und Lieferketten benötigt eine Migration ins neue Kryptographie-Zeitalter.

WARUM HANDELN JETZT BEREITS ENTSCHEIDEND IST

Noch existiert zwar kein universeller Quantencomputer, das Risiko ist jedoch heute bereits real. Angriffe nach dem Prinzip „Store now, decrypt later" zielen darauf ab, heute verschlüsselte Daten abzugreifen, um sie in Zukunft, sobald leistungsfähige Quantencomputer auch für Angreifer zur Verfügung stehen, zu entschlüsseln. Besonders für vertrauliche oder langfristig schützenswerte Informationen, etwa in Verwaltung, Medizin oder Industrie, besteht ein erhebliches Risiko. Sie sind hochattraktive Ziele für Bedrohungsakteure.

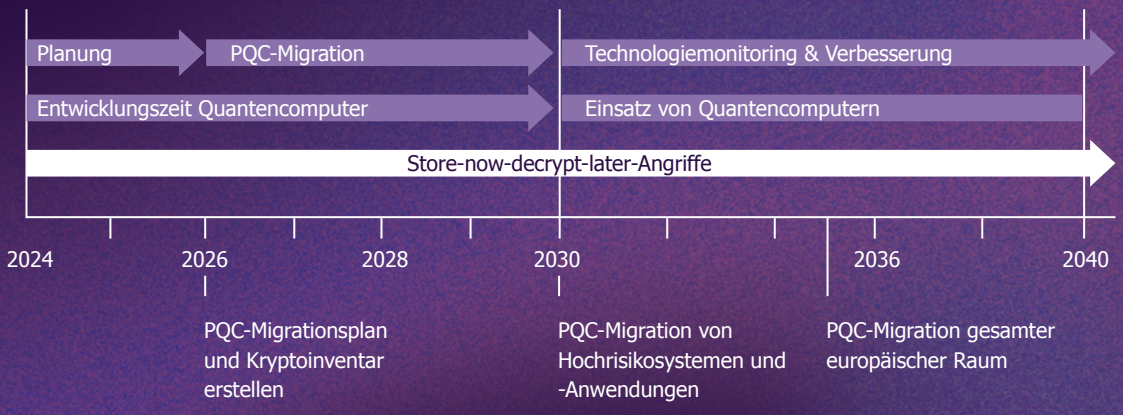
Hinzu kommt der regulatorische Druck:

- Die EU-NIS-2-Richtlinie fordert explizit den Schutz kritischer Informationssysteme auf Grundlage des Standes der Technik.
- Das BSI arbeitet an verschiedenen Stellen an Handlungshilfen zur Vorbereitung einer frühzeitigen Migration in die Post-Quanten-Kryptographie.
- Programme wie die Hightech Agenda Deutschland fördern Forschung und Transfer quantensicherer Technologien.
- Das EU Quantum Technologies Flagship forscht darüber hinaus im Bereich der Quantenkryptographie, z. B. in der sicheren Schlüsselverteilung (Quantum Key Distribution = QKD) mittels quantenmechanischer Effekte.

Die zentrale Herausforderung: Die meisten Organisationen wissen heute nicht, wo Kryptographie überall eingesetzt wird, und schon gar nicht, in welcher Form. Ohne diese Transparenz lässt sich keine fundierte Migrationsstrategie entwickeln.

STARTPUNKT KRYPTOINVENTUR: WISSEN, WO MAN STEHT

Vor der Auswahl quantensicherer Verfahren steht deshalb die Bestandsaufnahme. Ähnlich wie in der klassischen IT-Sicherheitsarchitektur gilt es, zunächst sichtbar zu machen, was vorhanden ist. Die wichtigste Frage:



Übersicht: Entwicklung und Verfügbarkeit leistungsfähiger Quantencomputer

Welche Systeme und Anwendungen nutzen welche kryptographischen Bibliotheken, Protokolle oder Algorithmen?

Die reine Erfassung kryptographischer Verfahren ist das eine. Für eine fundierte Migrationsstrategie ist es allerdings entscheidend, die jeweiligen Anwendungen genauer zu analysieren:

Anwendungen unterscheiden sich hinsichtlich ihrer Schutzziele (z. B. Vertraulichkeit, Integrität, Authentizität), des angestrebten Sicherheitslevels sowie verschiedener Einschränkungen, etwa:

- verfügbarer Hardware-Ressourcen,
- Laufzeit- oder Latenzanforderungen,
- regulatorischer Vorgaben oder Interoperabilitätszwänge.

Es wäre daher nicht zielführend, klassische kryptographische Verfahren pauschal durch ein Post-Quanten-Äquivalent zu ersetzen. Auswahl und Priorisierung sollten je nach Bedarf erfolgen: Welche Anwendungen sind wirklich kritisch, welche können warten und welche Anforderungen erlauben oder begrenzen eine Migration?

Zusätzlich ist zu bewerten, wie kryptoagil bestehende Systeme bereits heute sind – also inwieweit sich kryptographische Algorithmen und -parameter austauschen lassen, ohne dass ganze Anwendungen oder Protokoll-Stacks angepasst werden müssen. Diese Kryptoagilität beeinflusst den Migrationsaufwand.

Im Umkehrschluss sollte bereits die Migration der kryptographischen Verfahren in eine Post-Quanten-Sicherheit kryptoagile Strukturen fördern. So lassen sich zukünftige Umstellungen auf neue oder verbesserte Verfahren mit vertretbarem Aufwand durchführen.

Hierbei hilft ein moderner Ansatz: die teilautomatisierte Bestandsaufnahme kryptographischer Assets, strukturiert nach dem offenen CycloneDX-Standard in Form einer Cryptography Bill of Materials (CBOM).

Eine CBOM erlaubt es, Kryptographie erstmals über Systemgrenzen hinweg zu inventarisieren: **nachvollziehbar, maschinenlesbar und anschlussfähig** an bestehende Sicherheitsprozesse.

Damit entsteht die Grundlage, Risiken zu priorisieren, Migrationspfade zu planen und Investitionen zielgerichtet zu steuern.

MIT GEBÜNDELTEM WISSEN BESSER HANDELN

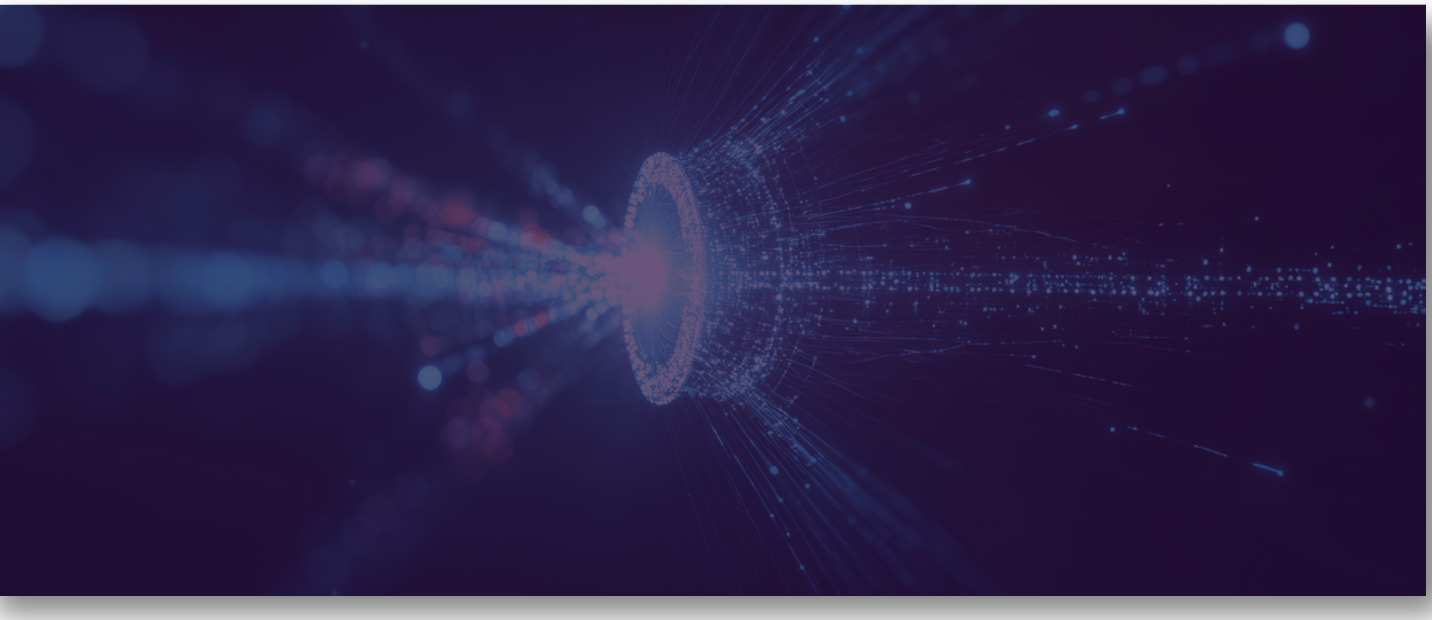
Das gemeinsame Whitepaper von Sopra Steria, enclaive, BITMARCK und der Hochschule Darmstadt (h_DA) beleuchtet das Thema Post-Quanten-Sicherheit bewusst aus vier Perspektiven:

- der Sicht des Umsetzungspartners und Beratungsdienstleisters, der seine Kunden bei der Migration strategisch und praktisch begleitet,
- der Sicht des IT-Herstellers, der Hardware und sichere Trust-Anker bereitstellt,
- der Sicht der potenziell Betroffenen, die die Herausforderungen und den Nutzen aus dem kryptographischen Tagesbetrieb heraus kennen,
- der Sicht der Wissenschaft, die Standards, Forschung und Zukunftsfähigkeit bewertet.

Gemeinsam zeichnen wir ein Bild davon, wie Organisationen den Schritt ins Post-Quanten-Zeitalter gestalten können: strukturiert, faktenbasiert und mit dem Ziel, heute die Grundlage für die Sicherheit von morgen zu schaffen.

Wir wünschen eine spannende Lektüre.

HEUTE BEREITS **INS HANDELN KOMMEN**



Der technologische Fortschritt schreitet schneller voran als die Fähigkeit vieler Organisationen, ihn sicher zu beherrschen. In kaum einem Bereich wird das so deutlich wie in der Kryptographie. Während Forschung und Standardisierung bereits auf die Post-Quanten-Ära zusteuern, fehlt in der Praxis häufig noch der Überblick. Unklar ist oft, welche Systeme, Anwendungen und Kommunikationskanäle betroffen sind und wo man überhaupt mit der Migration beginnen soll.

Aus der Beratungsperspektive zeigt sich: Der Weg zur Post-Quanten-Sicherheit ist vor allem ein Transformationsprozess auf technischer, organisatorischer und kultureller Ebene. Denn Post-Quanten-Kryptographie betrifft nicht nur Algorithmen, sondern auch Geschäftsprozesse, Lieferketten und das Vertrauen in die gesamte digitale Wertschöpfung.

KRYPTOGRAPHISCHES KNOW-HOW IST EIN KRITISCHER FAKTOR

Neben Prozessen, Werkzeugen und Strukturen entscheidet ein weiterer Aspekt über den erfolgreichen Übergang in das Post-Quanten-Zeitalter: kryptographische Expertise. Die Anforderungen an moderne IT-Sicherheit verschieben sich zunehmend in Richtung spezialisierter Kenntnisse über Algorithmen, Standards, Protokollarchitekturen und Migrationspfade.

Diese Qualifikationen sind im Markt allerdings äußerst knapp. Der Fachkräftemangel trifft die Kryptographie noch stärker als andere Bereiche der IT-Sicherheit. Viele Organisationen verfügen zwar über interne Kompetenzen auf den Fachgebieten Infrastruktur, Entwicklung oder Compliance. Spezialisierte Fachleute, die kryptographische Verfahren bewerten, Migrationsstrategien entwickeln oder die Auswirkungen neuer PQC-Standards auf bestehende Systeme fundiert einschätzen können, sind allerdings rar gesät.

Unternehmen und Verwaltungen werden nicht umhinkommen, diese Lücke mithilfe von externem Know-how zu schließen: Umsetzungs- und Beratungspartner bündeln kryptographische Expertise

und können sie skalierbar bereitstellen, etwa für die Analyse komplexer Systemlandschaften, die Erstellung von Kryptoinventaren (CBOM), die Bewertung von Risiken oder die Ausgestaltung einer migrationsfähigen Architektur. Externe Expertenteams sind zudem eng mit Forschung, Herstellern und Standardisierungsgremien verzahnt. Damit können sie aktuelle Entwicklungen frühzeitig einordnen und in konkrete Handlungsempfehlungen überführen.

Für betroffene Organisationen sind Partner damit eine wichtige Unterstützung: Interne Teams müssen nicht zu Kryptographie-Spezialisten werden, sondern können ihre aktuellen Aufgaben weiterführen, während Fachleute sicherstellen, dass kryptographische Entscheidungen fachlich fundiert, regulatorisch belastbar und technisch tragfähig getroffen werden. Das erleichtert den Übergang von punktuellen Maßnahmen zu einer kontinuierlichen Kryptostrategie und erhöht langfristig die Sicherheit und Stabilität der gesamten IT-Landschaft.

TRANSPARENZ ALS GRUNDLAGE JEDER STRATEGIE

Der erste Schritt auf diesem Weg ist die Sichtbarkeit kryptographischer Abhängigkeiten. In der Praxis wissen viele Unternehmen nicht, wo und in welchem Umfang Kryptographie tatsächlich eingesetzt wird – ob auf Webservern, in Backend-Systemen, Datenbanken, Cloud-Workloads oder auf eingebetteten Geräten.

Hier schafft eine Cryptography Bill of Materials (CBOM) Abhilfe:
Auf Basis des offenen CycloneDX-Standards lässt sich die kryptographische Landschaft einer Organisation automatisiert erfassen und dokumentieren. Das Ergebnis: ein maschinenlesbares Inventar aller kryptographischen Artefakte – vom Algorithmus bis zum Zertifikat – und damit ein klarer Ausgangspunkt für jede PQC-Migrationsstrategie.

Beratungs- und Technologiepartner integrieren diesen Schritt in ihre IT-Governance-Analyse:

- teilautomatisierte Erkennung von Kryptoverfahren und -bibliotheken,
- Zuordnung zu Systemen und Prozessen,
- Priorisierung nach Kritikalität und regulatorischer Relevanz.

So entsteht Transparenz – nicht als Selbstzweck, sondern als Entscheidungsgrundlage.

VON DER BESTANDSAUFNAHME ZUR ROADMAP

Nach der Inventarisierung folgt die Bewertung: Welche Verfahren gelten als kritisch? Wo müssen kurzfristig Maßnahmen umgesetzt werden? Und wo genügt ein Monitoring? Hier unterstützen externe Partner mit Risikomodellen und Migrationsszenarien, die auf BSI-, NIST- und ETSI-Leitlinien basieren.

Das Ziel ist eine strukturierte Roadmap, die technische Machbarkeit, Ressourcen und Geschäftsprioritäten in Einklang bringt. Dabei fließen sowohl klassische Migrationsmethoden wie Re-Keying und Dual-Stack-Verfahren als auch neue Ansätze ein, etwa die Koexistenz von klassischen und quantensicheren Verfahren in Hybridarchitekturen.

DIE PQC-MIGRATION ALS KONTINUIERLICHER PROZESS

Quantensicherheit ist kein einmaliges Projekt, sondern ein dauerhafter Prozess. Mit der Einführung quantensicherer Verfahren steigen die Anforderungen an Governance, Schlüsselmanagement und Überwachung.

Externe Beratungsunternehmen begleiten diesen Wandel durch:

- Integration der CBOM-Ergebnisse in bestehende Sicherheits- und Compliance-Prozesse,
- Aufbau quantensicherer Key-Management-Infrastrukturen,

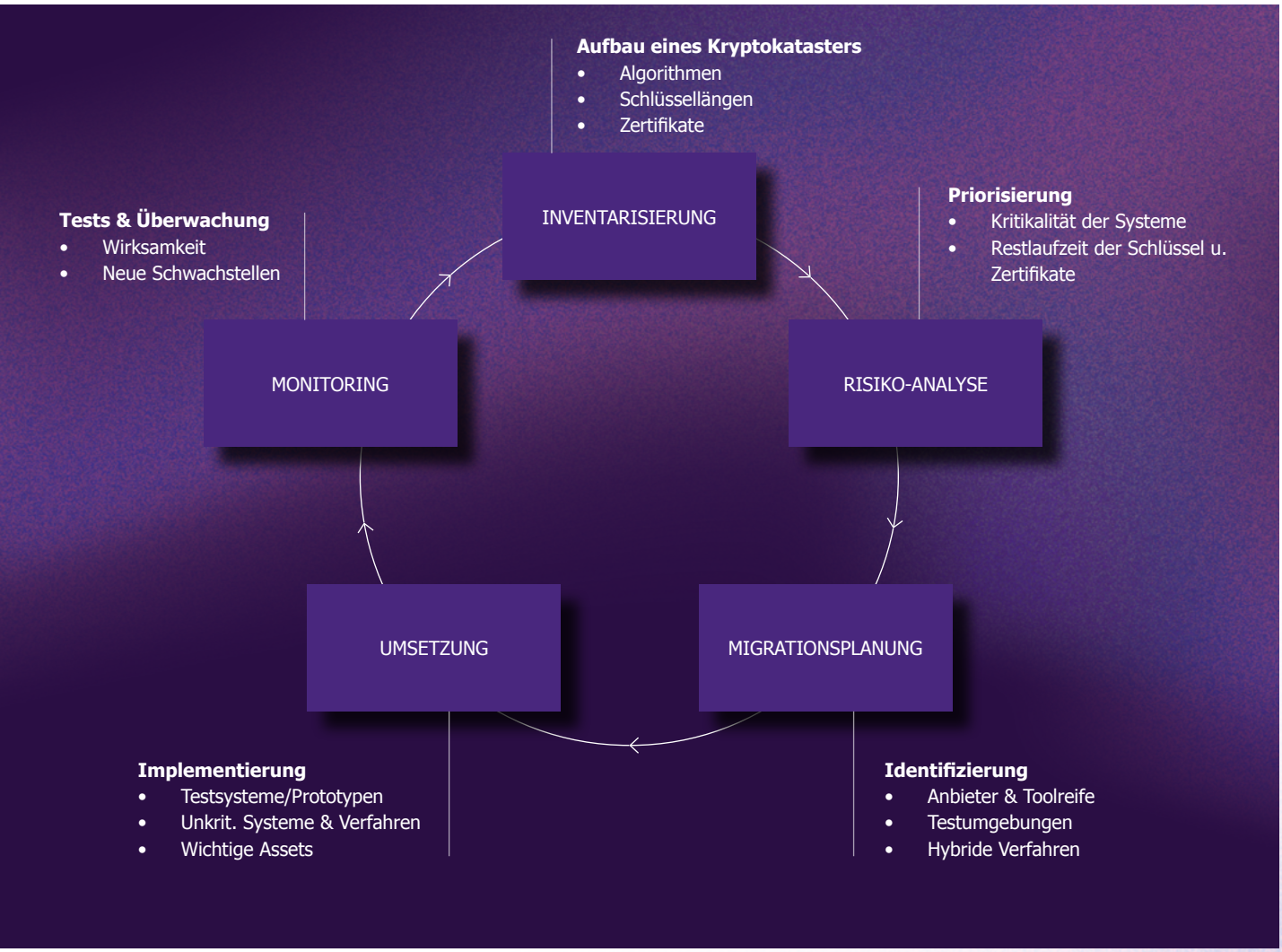
- Schulung und Awareness-Programme für IT- und Sicherheitsverantwortliche.

So wird aus einem einmaligen Inventurprojekt ein lebendiger Prozess der Kryptographie-Governance, der sich in die gesamte IT-Sicherheitsstrategie integriert.

FAZIT: HANDLUNGSFÄHIGKEIT HERSTELLEN

Es reicht somit nicht, Quantensicherheit nur auf dem strategischen Zettel zu haben. Post-Quanten-Kryptographie ist keine Zukunftsmusik mehr. Organisationen können heute bereits viele Vorbereitungen treffen. Diejenigen, die früh handeln, sichern nicht nur ihre Daten, sondern bleiben handlungsfähig in einer sich wandelnden Tech-Landschaft.

— Sebastian Kavalir, Sopra Steria



Prozessablaufdiagramm Post-Quanten-Migration

HARDWARE ALS FUNDAMENT FÜR **SICHERHEIT**

Mit dem Aufkommen leistungsfähiger Quantencomputer steht die IT-Sicherheitsarchitektur vor einer grundlegenden Veränderung. Klassische kryptographische Verfahren, die auf Faktorisierung oder diskreten Logarithmen basieren (z. B. RSA, DSA), werden perspektivisch angreifbar. Um Vertraulichkeit und Integrität von Daten und Systemen nachhaltig zu schützen, muss Post-Quanten-Sicherheit ganzheitlich und in mehreren Dimensionen betrachtet werden.

DREIDIMENSIONALE PQC-VERSCHLÜSSELUNG ZUR WAHRUNG DER VERTRAULICHKEIT

Post-Quanten-Sicherheit betrifft alle Phasen der Datenverarbeitung und darf nicht auf einzelne Aspekte wie Transportverschlüsselung reduziert werden. Ein quantensicheres Gesamtkonzept muss daher Daten in den Dimensionen „at rest", „in transit" und „in use" berücksichtigen. Nur durch die gleichzeitige Absicherung aller drei Dimensionen kann das Sicherheitsziel der dauerhaften Vertraulichkeit in einer Post-Quanten-Welt erreicht werden.

POST-QUANTEN-SICHERHEIT IN DER INTEGRITÄTSKONTROLLE UND VERTRAUENSKETTE

Post-Quanten-Sicherheit betrifft nicht nur die Vertraulichkeit, sondern auch die Integrität von IT-Systemen. Grundlage dafür ist eine hardwarebasierte Komponente, der das gesamte System vertraut. Diese Root of Trust stellt über so genannte Secure Elements oder Security-Prozessoren kryptographische Vertrauensketten bereit.

Diese Strukturen bilden die Basis für:

- Authentizität von Software und Systemen über PKI-Zertifikate und Signaturen,
- Integritätsprüfungen vom Systemstart bis zur Remote Attestation einer Trusted Execution Environment (TEE),
- verifizierbare Vertrauensbeziehungen in Cloud- und Edge-Umgebungen.

Daher muss auch die Public Key Infrastructure (PKI) selbst PQ-sicher gestaltet werden. Das umfasst:

- die Nutzung postquantensicherer Signaturalgorithmen,
- angepasste Zertifikats- und Schlüsselverwaltungsprozesse,
- hybride PKI-Modelle zur Wahrung der Kompatibilität.

Eine PKI setzt darüber hinaus auf Hardware Security Modules (HSMs) auf, um das Zertifikat der Root Certificate Authority sicher zu schützen. HSMs dienen als physisch und logisch abgeschirmte Vertrauenselemente zur Generierung, Speicherung und Nutzung kryptographischer Schlüssel. Nur wenn Root of Trust, PKI und HSM-Infrastruktur gemeinsam auf PQ-resistente Verfahren umgestellt werden, bleibt die gesamte Vertrauenskette von der Hardware über Firmware bis zu Anwendungen und Cloud-Diensten auch in einer Post-Quanten-Ära vertrauenswürdig.

QUANTUM-ENKLAVEN ALS BAUSTEIN DER POST-QUANTUM READINESS

Moderne Sicherheitsarchitekturen müssen nicht nur klassischen Angriffsvektoren standhalten, sondern auch die absehbaren Auswirkungen leistungsfähiger Quantencomputer berücksichtigen. Die Verwendung quantenresistenter Algorithmen und die Absicherung der Laufzeitumgebung spielen dabei zentrale Rollen. Vertrauliche Ausführungsumgebungen (Confidential Execution Environments (CEEs)) schaffen hierfür einen technischen Rahmen, indem sie Anwendungen in isolierten, hardwaregestützten Umgebungen (Trusted Execution Environments (TEEs)) ausführen. Diese Umgebungen schützen Code, Daten oder KI-Modelle gegenüber Betriebssystem, Hypervisor und Cloud-Infrastruktur. Sie bilden damit einen vertrauenswürdigen Raum für sicherheitskritische oder sensible Anwendungen, Dienste, Daten und Prozesse (Workloads).

Ein wesentlicher Vorteil solcher CEE-basierter Virtualisierungsarchitekturen besteht darin, dass bestehende Anwendungen häufig ohne Anpassung in eine geschützte Umgebung überführt werden können. Das erleichtert insbesondere Organisationen mit gewachsenen IT-Landschaften den Übergang zu PQ-sicheren Betriebsmodellen. Durch die Abkopplung von der umgebenden Infrastruktur können Anwendungen migrationsfähig in isolierten Bereichen ausgeführt werden, während kryptographische Verfahren schrittweise auf PQC-Standards umgestellt werden. Insbesondere proprietäre Legacy-Anwendungen, deren Wartung immer kostspieliger wird, können durch Quantum-Enklaven in einem PQ-sicheren Tresor geschützt werden.

Ein weiterer Baustein ist die umfassende Absicherung der Datenverarbeitung, unabhängig davon, ob Daten gespeichert (at rest), übertragen (in transit) oder verarbeitet (in use) werden. Viele CEE-Implementierungen nutzen hardwarebasierte Speicherverschlüsselung. Dadurch bleibt die Vertraulichkeit auch während der Ausführung geschützt. Perspektivisch müssen diese Mechanismen jedoch durch PQC-resistente Verfahren ergänzt werden, insbesondere in Bezug auf Attestation-Protokolle, Schlüsselmanagement und die sichere Initialisierung von Vertrauensbeziehungen.

Darüber hinaus ist es von großer Bedeutung, den kryptographischen Zustand der IT-Landschaft transparent und damit nachvollziehbar zu machen. Hierzu tragen Verfahren wie Remote Attestation bei. Sie weisen kryptographisch nach, dass eine Anwendung tatsächlich in einer unveränderten und vertrauenswürdigen Umgebung läuft. Kombiniert mit einer strukturierten Erfassung aller verwendeten kryptographischen Komponenten – etwa

in Form einer Cryptography Bill of Materials – entsteht ein durchgängiges Modell zur Bewertung der PQ-Readiness einer Umgebung. Während Remote Attestation die Authentizität des Systems sicherstellt, dokumentiert eine CBOM die eingesetzten Algorithmen, Bibliotheken, Schlüsselarten und deren Post-Quanten-Status. In Kombination erhalten Organisationen eine belastbare Grundlage für Compliance-Anforderungen, Audits und regulatorische Nachweise.

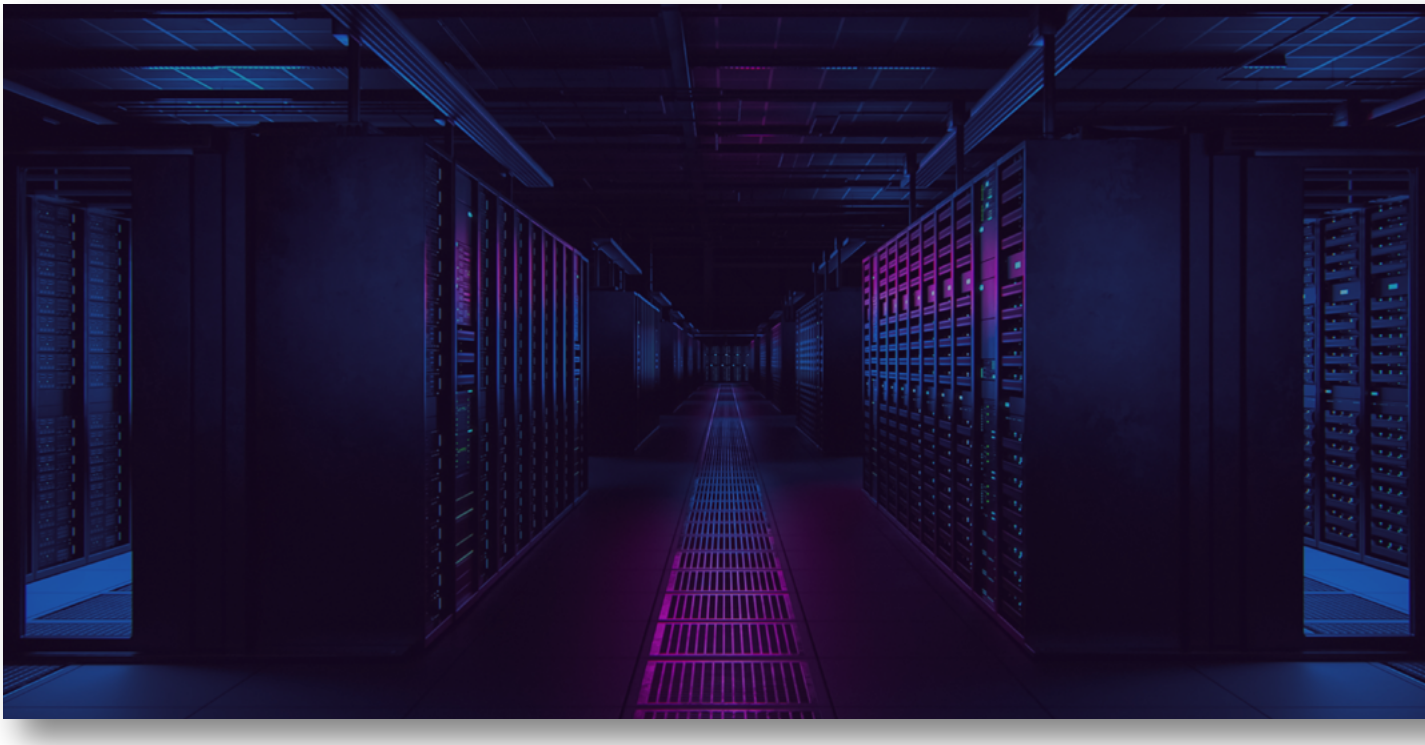
FAZIT

Hardwarebasierte Vertrauensanker und vertrauliche Ausführungsumgebungen können Organisationen beim Übergang zur Post-Quanten-Sicherheit wirksam unterstützen. Sie ermöglichen es, bestehende Anwendungen in isolierten, geschützten Bereichen auszuführen und deren Integrität kryptographisch zu überprüfen, ohne dass unmittelbare Anpassungen der Software notwendig sind.

Durch Mechanismen wie Remote Attestation und die strukturierte Erfassung des kryptographischen Zustands mithilfe einer Cryptography Bill of Materials (CBOM) entsteht eine überprüfbare Grundlage, um den Sicherheitszustand einer Umgebung transparent darzustellen.

Diese Kombination aus abgeschotteter Laufzeitumgebung, nachvollziehbarer Integritätsprüfung und dokumentierter Kryptographie bildet eine belastbare Basis, um die Migration in quantenresistente Verfahren schrittweise, kontrolliert und auditierbar zu gestalten.

— Dr. Sebastian Gajek, enclaive



VERTRAUEN DURCH KLARHEIT AUFBAUEN

Unternehmen und öffentliche Institutionen stehen am Beginn einer sicherheitskritischen Transformation: Der Übergang zur Post-Quanten-Kryptographie (PQK) verlangt sowohl technisch als auch organisatorisch eine Neubewertung bestehender Kryptostrukturen. Die PQK-Migration ist notwendig, um die Verlässlichkeit, Integrität und Authentizität der gesamten digitalen Infrastruktur sowie das Vertrauen der Nutzerinnen und Nutzer in sie langfristig zu gewährleisten. Diese Transformation ist komplex, wird mehrere Jahre in Anspruch nehmen und betrifft das gesamte digitale Ökosystem.
Die Motivation für die betroffenen Organisationen ist klar: Sie wollen wissen, wo sie besonders gefährdet sind und bei welchen Systemen die Umstellung beginnen muss.

AUSGANGSLAGE: KOMPLEXITÄT UND UNSICHERHEIT

Die Ausgangslage ist durch gewachsene, komplexe IT-Infrastrukturen in den Unternehmen und den Rechenzentren gekennzeichnet. Kryptographie wird in selbst entwickelter Software sowie in zugekaufter Software, Hardware, Geräten und SaaS-Systemen genutzt. Häufig mangelt es an Transparenz bezüglich der eingesetzten Verfahren, der Algorithmen, der Schlüsselverwaltung und der Protokolle. Für die Vorbereitung auf die PQK-Migration ist es essenziell, die eingesetzten kryptographischen Verfahren und deren Abhängigkeiten zu kennen, um die Risiken priorisieren und die Investitionen strategisch steuern zu können.

HERAUSFORDERUNGEN AUS KUNDENSICHT

Die Migration zur Post-Quanten-Kryptographie birgt aus Sicht potenziell bedrohter Organisationen mehrere praktische Herausforderungen:

- **Operative Prioritäten:** Der laufende Betrieb und kurzfristig anstehende Aufgaben stehen im Konflikt mit den langfristigen Migrationsprojekten.
- **Abhängigkeit von Lieferketten:** Aufgrund der zahlreichen Schnittstellen zu Lieferanten und Partnern besteht eine signifikante Abhängigkeit. Die Schnittstellen sowie die Produkte dieser Anbieter müssen genauso quantensicher gemacht werden wie selbstentwickelte Systeme.
- **Knappe Ressourcen:** Aufgrund des Fachkräftemangels, laufender Betriebsprioritäten und Abhängigkeiten in komplexen Lieferketten sind die verfügbaren Kapazitäten begrenzt. Viele Organisationen verfügen nicht über eigene Kryptographie-Experten und sind daher auf externe Unterstützung angewiesen.
- **Der Migrationsaufwand ist erheblich:** Die Umstellung ist ein komplexes, mehrjähriges Projekt, das das gesamte Geschäftsökosystem betrifft. Es ist eine Synchronisation zwischen Unternehmen, Lieferanten und Kunden erforderlich.

Hinzu kommt: Eine PQK-Migration hat kein Enddatum, und ein gewisser Aufwand im Tagesgeschäft bleibt. Die kryptographischen Verfahren werden häufiger ausgetauscht oder müssen an neue Standards angepasst werden, als dies bislang der Fall ist. Organisationen müssen zudem tendenziell schneller reagieren können.

WARUM TRANSPARENZ HILFT

Transparenz schaffen ist der zentrale Baustein einer PQK-Migration, denn die Bedrohung ist real und akut: Selbst wenn Quantencomputer derzeit noch nicht flächendeckend und für jedermann verfügbar sind, stellen Angriffe nach dem Prinzip „Store now, decrypt later" ein erhebliches Risiko für vertrauliche oder langfristig schützenswerte Daten dar. Das gilt speziell für langfristig schützenswerte Informationen in der öffentlichen Verwaltung, im Gesundheitssektor sowie bei Banken und Versicherungen.

ERSTELLUNG EINER CBOM

Der erste Schritt hin zur Post-Quanten-Sicherheit ist deshalb eine umfassende Bestandsaufnahme der kryptographischen Landschaft. Die Cryptography Bill of Materials (CBOM) schafft eine objektive Basis, um die betroffenen Assets zu identifizieren, Risiken zu priorisieren und für Budgets zu argumentieren.

- Die CBOM stellt eine Erweiterung der Software Bill of Materials (SBOM) dar.
- Das Dokument umfasst detaillierte Metadaten wie Algorithmen, Verwendungsmodi, Schlüssellängen, Schlüsselverwaltung (Key Storage/ Management), Zertifikate, Protokoll- und Bibliotheksversionen. Darüber hinaus finden sich darin nichttechnische Details wie die Datenklassifizierung, der Geschäftszweck und die verantwortliche Rolle (Owner).
- Die Inventur muss sowohl eigene Anwendungen als auch Drittanbietersoftware abdecken.
- Die Erfahrung mit CBOM-Pilotprojekten zeigt: Zur Bewältigung der Größenordnung – es geht um tausende Anwendungen und Endpunkte – und zur Gewährleistung von Vollständigkeit und Aktualität sind automatisierte Methoden zur Laufzeit erforderlich.
- Manuelle Methoden wie Code Reviews oder Befragungen sind zeitintensiv und oft unpräzise.
- Statische Scans von z. B. Quell- und Objektcode liefern häufig ungenaue Inventare. Der Grund: Sie erkennen kritische Fehler nicht, die von der Laufzeit oder Konfigurationsdateien abhängen.
- Drei Verfahren sollten aufeinander aufbauend genutzt werden:
  - einmalige Interviews,
  - dauerhafte Scans in der Softwareentwicklung sowie
  - Scans in der Infrastruktur zur Laufzeit.
- Ziel sollte es sein, eine tagesaktuelle Übersicht über die genutzten kryptographischen Verfahren zu haben.

ERGEBNIS UND NUTZEN EINER CBOM

Mit der Bestandsaufnahme lassen sich kritische Systeme identifizieren und deren Migration priorisieren. Kritisch sind Systeme beispielsweise dann, wenn sie Daten mit einer langen Lebensdauer (länger als zehn Jahre) schützen müssen oder wenn sie Daten mit einem hohen Schutzbedarf verarbeiten oder speichern.

Mithilfe des Kryptoinventars können Organisationen zudem Risikobewertungen durchführen, die beispielsweise die Kritikalität und regulatorische Vorschriften wie DORA und NIS 2 berücksichtigen.

AUSBLICK: VOM PROJEKT ZUR GOVERNANCE

Die Herstellung von Post-Quanten-Sicherheit ist kein einmaliges Projekt, sondern erfordert kontinuierliches Lernen und Verbessern. Unternehmen und Verwaltungen sollten deshalb Fähigkeiten, Methoden und Prozesse in ihrer Sicherheitsgovernance verankern, durch die sie kurzfristig auf neue kryptoanalytische Fortschritte reagieren können.

Kryptoagilität herstellen: Gemeint ist die Fähigkeit, kryptographische Algorithmen und Standards schnell und einfach auszutauschen oder zu aktualisieren, falls sich eine Schwachstelle zeigt oder neue Standards verfügbar werden.

Regelmäßige Kryptoinventuren: Inventuren sollten so selbstverständlich werden wie Schwachstellenscans. Der Prozess zur Pflege des Inventars sollte in die bestehenden Sicherheits- und Compliance-Prozesse (z. B. DevSecOps) integriert und automatisiert werden.

Zusammenarbeit: Die Zusammenarbeit und der Austausch mit Herstellern von Hardware und Softwareanbietern zum Thema CBOM und Kryptographie werden wichtiger und sollten institutionalisiert werden.

Teilnahme an Pilotprojekten: Organisationen sollten sich an Brancheninitiativen und Pilotprojekten beteiligen und gemeinsam Abläufe und Prozesse zur PQK-Migration und Kryptoagilität erarbeiten. Auf diese Weise können sie die Interoperabilität von PQK-Lösungen testen und bewährte Verfahren austauschen.

Die CBOM dient als verlässliche Landkarte und Kompass für die Transformation in Richtung Post-Quanten-Sicherheit. Regelmäßige Kryptoinventuren sind künftig ein integraler Bestandteil der IT-Sicherheitsmaßnahmen und stehen in engem Zusammenhang mit Schwachstellenscans oder Risikoaudits.

Die PQK-Migration ist als integraler Bestandteil einer langfristigen Digitalstrategie zu begreifen. Sie gewährleistet die Handlungsfähigkeit der Organisation in einer sich wandelnden technologischen Landschaft.

— Dr. Andreas Gallus, BITMARCK

AUS DEM LABOR **IN DIE PRAXIS**

Post-Quanten-Kryptographie ist längst Gegenstand internationaler Standardisierung. Der bei uns wohl bekannteste Standardisierungsprozess wird vom U.S. National Institute of Standards and Technology (NIST) koordiniert. Das Institut hat 2022 vier Verfahren ausgewählt, darunter ML-KEM (CRYSTALS-Kyber) und ML-DSA (CRYSTALS-Dilithium). Weitere Kandidaten befinden sich in der Evaluation.

Andere internationale Organisationen treiben die Definition und Harmonisierung quantensicherer Verfahren ebenfalls voran, darunter die ISO/IEC JTC 1/SC 27/WG 2 (ISO/IEC 18033)[1], die ITU-T (TR.ac-pqc)[2] sowie nationale Behörden wie das Bundesamt für Sicherheit in der Informationstechnik (BSI), das mit seiner Broschüre „Quantum-safe cryptography" eine technische Orientierung für die Praxis liefert.[3] Parallel entstehen Aktivitäten in zahlreichen weiteren Ländern, darunter China, Russland, Japan und Indien, sowie in europäischen Gremien wie ETSI (Europäisches Institut für Telekommunikationsnormen) und ENISA (Agentur der Europäischen Union für Cybersicherheit), die Leitlinien für den Übergang zu quantensicheren Verfahren entwickeln.

Während sich die algorithmische Auswahl und Standardisierung zunehmend konsolidiert, verschiebt sich der Fokus der Forschung in Richtung praktische Migration. Es geht also um die Frage, wie quantensichere Verfahren in bestehende Systeme integriert werden können. Einen strukturierten Ansatz dafür stellt etwa der PQC Migration Management Process (PMMP) von N. von Nethen et al. (EICC 2024) vor, der Phasen, Rollen und Anforderungen für eine planbare Umstellung beschreibt.[4]

KRYPTOINVENTARISIERUNG ALS FORSCHUNGSFELD

Auch aus Sicht der Wissenschaft besteht die zentrale Herausforderung bei der PQC-Vorbereitung darin, überhaupt zu wissen, wo und wie Kryptographie eingesetzt wird. Hier setzt ein neues Forschungsfeld an: die Kryptoinventarisierung.

Bislang gibt es nur wenige standardisierte Methoden zur systematischen Erfassung kryptographischer Assets. Relevante Initiativen wie CycloneDX[5] oder die von IBM vorgeschlagene Cryptography-Bill-of-Materials-(CBOM-)Struktur[6] schaffen jedoch erste offene Rahmenwerke, mit denen Kryptographie maschinenlesbar dokumentiert werden kann. Die NIST SP 1800-38B Quantum Readiness: Cryptographic Discovery[7] adressiert genau diese Herausforderung und beschreibt Ansätze, wie Kryptographie über Werkzeuge und Schnittstellen automatisiert identifiziert werden kann.

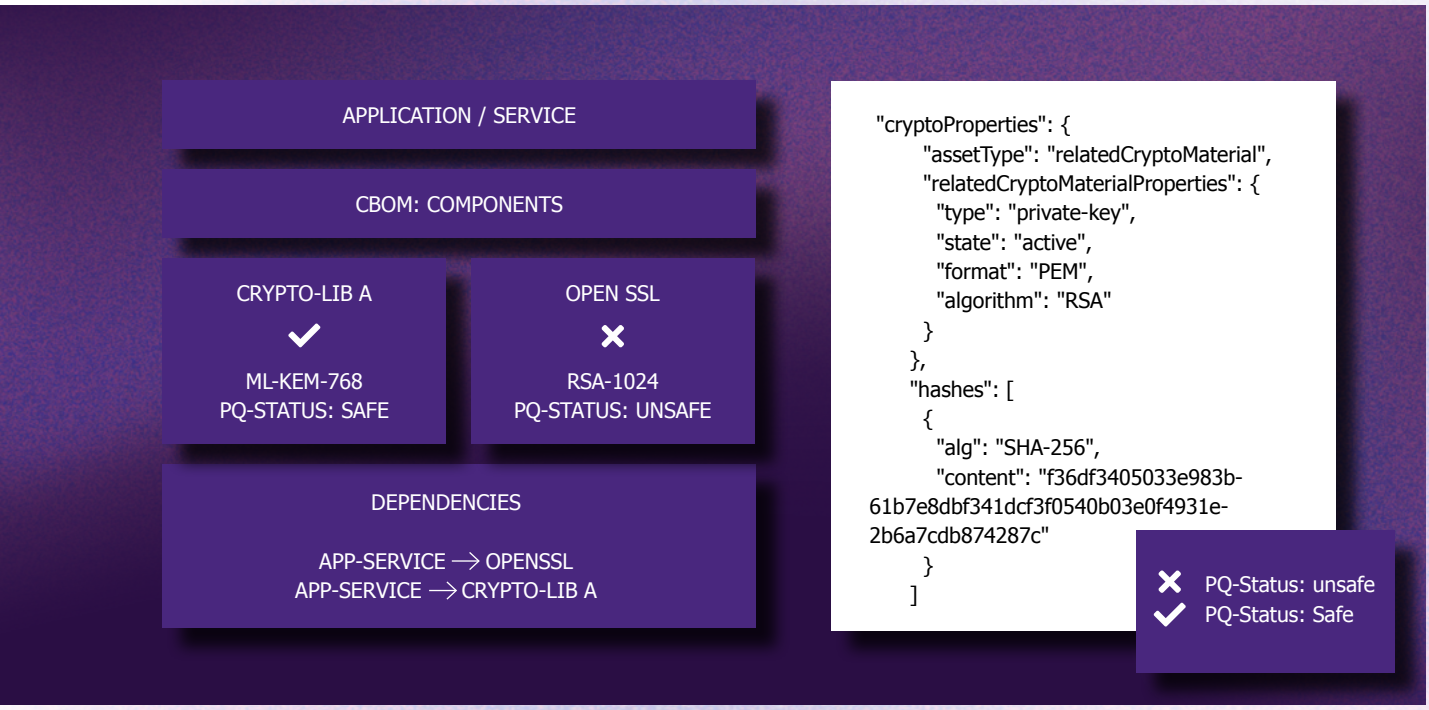
1 https://www.iso.org/standard/86890.html
2 https://www.itu.int/md/T25-SG17-250408-TD-WP1-0033
3 https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Brochure/quantum-safe-cryptography.html?nn=916626
4 PMMP-PQC Migration Management Process
5 https://cyclonedx.org/
6 https://github.com/IBM/CBOM
7 https://www.nccoe.nist.gov/sites/default/files/2023-12/pqc-migration-nist-sp-1800-38b-preliminary-draft.pdf

Forschungsarbeiten, etwa von Schmitt et al.[8], betonen dabei die Notwendigkeit, Kryptoinventarisierung nicht als einmalige Aufgabe, sondern als kontinuierlichen Prozess zu verstehen. Eng verwandt ist das Konzept der Kryptoagilität, also die Fähigkeit, kryptographische Verfahren flexibel austauschen zu können. Insbesondere unterliegt PQC, genauso wie die klassische Kryptographie, Alterungsprozessen, z. B. durch Fortschritte in der Kryptoanalyse oder der Technologie im Allgemeinen. Das heißt, kryptographische Verfahren oder Parameter, die heute als sicher gelten, müssen in Zukunft vermutlich angepasst werden.

Ein entsprechendes Reifegradmodell wurde u. a. von Hohm et al. (2023) vorgestellt (Towards a Maturity Model for Crypto-Agility Assessment).[9] Kryptoinventare können hier als Messinstrument dienen, um den Stand der Kryptoagilität zu bestimmen und gezielt zu erhöhen.

Die wissenschaftliche Herausforderung besteht vor allem in der Automatisierung solcher Prozesse, der Modellierung kryptographischer Abhängigkeiten und der Integration in bestehende Sicherheits- und Asset-Management-Systeme.

Forschungspapiere (u. a. Cryptoscope: Analyzing cryptographic usages in modern software) beleuchten, wie Kryptoinventarisierung mit Software Composition Analysis (SCA) oder Continuous Security Monitoring verknüpft werden kann.[10]



8 On Criteria and Tooling for Cryptographic Inventories, GI Sicherheit 2024

9 https://www.springerprofessional.de/foundations-and-practice-of-security/25196744#TOC

10 https://arxiv.org/abs/2503.19531

INTERDISZIPLINARITÄT ALS ERFOLGSFAKTOR

PQC ist kein isoliertes Thema der Kryptographie, sondern ein interdisziplinäres Feld. Mathematiker liefern die Grundlagen, Kryptographen übersetzen sie in implementierbare Verfahren und Cybersicherheitsexperten integrieren diese in reale Infrastrukturen, z. B. in Transport Layer Security (TLS), Virtual Private Networks (VPN) oder Public Key Infrastructures (PKIs).

Forschung leistet somit einen entscheidenden Beitrag, den Brückenschlag zwischen theoretischer Sicherheit, Standardisierung und industrieller Umsetzung zu ermöglichen.

AUSBLICK

Zukünftige Forschung auf diesem Gebiet wird sich unter anderem auf Automatisierung, Skalierbarkeit und Kryptoagilität konzentrieren.

Zentrale Fragestellungen sind:

- Wie lässt sich die Umstellung auf PQC automatisiert und sicher skalieren?
- Wie lässt sich dabei Kryptoagilität effizient integrieren?
- Welche hybriden Verfahren (klassisch + quantensicher) sind langfristig tragfähig?
- Wie kann Kryptoinventarisierung in DevSecOps-Prozesse eingebettet werden?

Eine langfristige Vision ist die Entwicklung automatisierter Kryptoinventarisierungsagenten, die fortlaufend prüfen, ob Systeme kryptographisch sicher sind. Sie sind vergleichbar mit heutigen Vulnerability-Scannern.

Damit verschmilzt Forschung mit Praxis: Aus punktuellen Projekten entsteht eine dauerhafte Kryptographie-Governance als integraler Bestandteil moderner IT-Sicherheitsstrategien.

— Prof. Dr. Alexander Wiesmaier,
Hochschule Darmstadt (h_da)

VOM WISSEN **INS HANDELN** KOMMEN

Der Weg in die Post-Quanten-Ära verlangt eine Teamanstrengung verschiedener Akteure: Externe Umsetzungspartner und Berater entwickeln die Instrumente zur automatisierten Kryptoinventarisierung, IT-Hersteller stellen hardwarebasierte Vertrauensanker und sichere Ausführungsumgebungen bereit, die potenziell betroffenen Unternehmen und Verwaltungen schaffen Transparenz in ihren komplexen IT-Landschaften und priorisieren Risiken, während die Forschung durch Standards, Methoden und wissenschaftliche Orientierung den Rahmen für belastbare Entscheidungen absteckt.
Mit diesen Perspektiven entsteht ein vollständiges Bild darüber, was Organisationen benötigen, um ihre digitale Infrastruktur langfristig quantensicher zu machen. Aus allen vier Sichten wird klar: Der entscheidende Schritt besteht darin, vom Wissen und vom Bewusstsein ins Handeln zu kommen.

Die Post-Quanten-Migration ist kein einmaliger Technologieaustausch, sondern ein strukturierter Transformationsprozess, der Transparenz, Priorisierung und eine langfristige Governance erfordert.
Empfohlene Schritte

1. **Kryptolandschaft erfassen (CBOM erstellen)**
   Eine belastbare Grundlage entsteht nur, wenn kryptographische Verfahren, Bibliotheken, Protokolle und Abhängigkeiten systematisch erfasst werden, idealerweise automatisiert und nach offenen Standards wie CycloneDX. Diese Transparenz ist Voraussetzung für jede fundierte Entscheidung.

2. **Risiken bewerten und priorisieren**
   Auf Basis des Inventars sollten Systeme nach Kritikalität, Schutzbedarf und regulatorischen Anforderungen bewertet werden. Besonders betroffen sind Anwendungen mit langen Vertraulichkeitszeiträumen sowie solche, die in komplexe und stark vernetzte Lieferketten eingebettet sind.

3. **PQC-ready-Strategie ableiten und umsetzen**
   Daraus gilt es eine Migrationsstrategie zu definieren, die technische Machbarkeit, Abhängigkeiten und Ressourcen berücksichtigt. Dazu gehören hybride Verfahren, kryptoagile Strukturen, die Integration quantensicherer Mechanismen in bestehende Infrastruktur sowie Governance-Prozesse, die eine laufende Anpassung ermöglichen.

Es lohnt sich, sich immer wieder vor Augen zu führen: Das Post-Quanten-Zeitalter ist kein Zukunftsthema. Organisationen, die heute mit der systematischen Vorbereitung beginnen, schaffen die Grundlage dafür, ihre digitale Integrität und Handlungsfähigkeit auch in den kommenden Jahrzehnten zu sichern.

Die Autoren dieses Whitepapers und das Projektkonsortium aus Sopra Steria, enclaive, BITMARCK und h_da verstehen sich dabei als Enabler von Transparenz, Orientierung und praktischer Umsetzung des Übergangs in ein Zeitalter der Post-Quanten-Sicherheit.

Sopra Steria ist ein führender europäischer Tech-Player mit 50.000 Mitarbeitenden in fast 30 Ländern und anerkannter Expertise in den Geschäftsfeldern Consulting, Digital Services und Solutions. Die Gruppe bietet umfassende End-to-End-Lösungen, die große Unternehmen und Behörden wettbewerbs- und leistungsfähiger machen – und zwar auf Grundlage tiefgehender Expertise in einer Vielzahl von Branchen, innovativer Technologien und eines kollaborativen Ansatzes. https://www.soprasteria.de/

---

enclaive ist ein deutsches Technologieunternehmen, das sich auf Confidential Computing spezialisiert hat, um sensible Daten und Anwendungen in der Cloud sicher zu schützen, indem es eine Isolationsschicht (sogenannte „Enklaven") schafft, die selbst den Cloud-Anbieter vom Zugriff ausschließt. enclaive bietet eine Multi-Cloud-Plattform, die es ermöglicht, Daten in Gebrauch zu verschlüsseln und so europäische Datensouveränität zu gewährleisten, auch bei großen Hyperscalern wie AWS, Azure und Google Cloud. https://www.enclaive.io/de

---

Als führender Digitalisierungspartner der gesetzlichen Krankenversicherung treibt **BITMARCK** die digitale Transformation in der Branche mit innovativen Produkten und Services voran. Grundlage hierfür ist der GKV-Softwarestandard BITMARCK_21c|ng, der bei den angeschlossenen Krankenkassen im Einsatz ist. Kunden der Unternehmensgruppe sind die Betriebs- und Innungskrankenkassen sowie die DAK-Gesundheit und weitere Ersatzkassen. https://www.bitmarck.de/

Die **Hochschule Darmstadt (h_da)** ist eine der größten deutschen Hochschulen für Angewandte Wissenschaften (HAWs). Sie bietet ihren aktuell 14.000 Studierenden ein praxisnahes und anwendungsorientiertes Studium in den Bereichen MINT, Wirtschaft und Gesellschaft sowie Architektur, Medien und Design. Viele Projekte und Inhalte in Studium, Forschung und gesellschaftlichem Transfer beschäftigen sich mit den Zukunftsthemen nachhaltige Entwicklung, Mobilität und Digitalisierung. https://h-da.de

---

ANSPRECHPARTNER

SEBASTIAN KAVALIR
Sopra Steria
sebastian.kavalir@soprasteria.com
+49 151 40626411

DR. SEBASTIAN GAJEK
enclaive
sebastian@enclaive.io
+49 151 40626411

DR. ANDREAS GALLUS
BITMARCK
andreas.gallus@bitmarck.de
+49 170 5591386

PROF. DR. ALEXANDER WIESMAIER
h_da
alexander.wiesmaier@h-da.de
+49 6151 533-60185

Sopra Steria SE
Hans-Henny-Jahnn-Weg 29
22085 Hamburg

T. 040 22703-0
E. info.de@soprasteria.com
W. www.soprasteria.com