Post-Quantensicherheit und die Bedeutung der Kryptoagilität

Vorbereitung auf den „Q-Day“

Hannover, 18.11.2025

ICT BUSINESS & TECHNOLOGY CONSULTING

DOK SYSTEME


Foto von coldsmokender, CC BY-SA 4.0, via Wikimedia Commons

QUANTEN-COMPUTER

Qubits (Quanten-Bits)

Post-Quanten-Kryptografie (PQC)

Kryptografisch relevante Quantencomputer (CRQC)

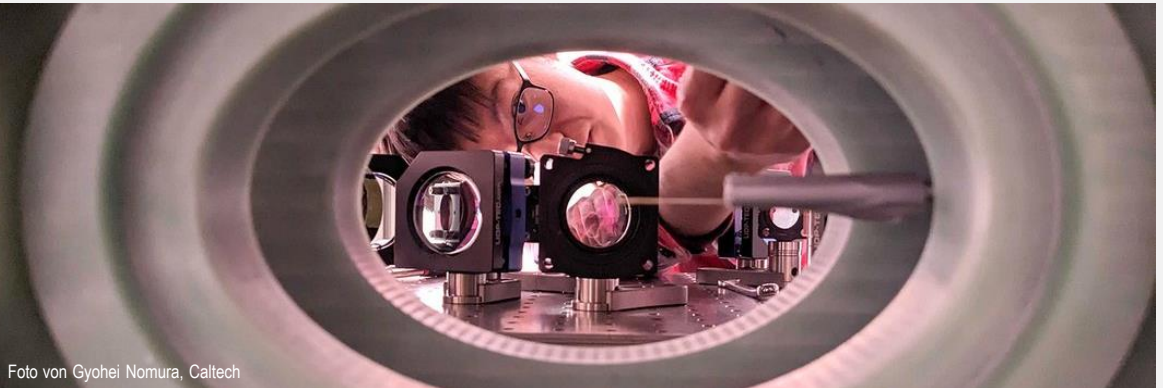


Foto von Gyohei Nomura, Caltech


Foto von Onri Jay Benally, CC BY-SA 4.0, via Wikimedia Commons

Public-Key-Kryptografie

Klassische asymmetrische kryptografische Algorithmen basieren auf **schweren mathematischen Problemen**.

Auch der schnellste (klassische) Super-Computer bräuchte Abermilliarden von Jahren, um einen 2048bit RSA-Schlüssel zu brechen.

Mit dem **Shor-Algorithmus** kann ein Quantencomputer diese Berechnungen innerhalb von Stunden durchführen.

>> Klassische Public-Key-Kryptografie wird unbrauchbar.

Symmetrische Verfahren

Klassische symmetrische Algorithmen werden durch Quantencomputer nicht gebrochen, aber **geschwächt**.

>> Der **Grover-Algorithmus halbiert die „effektive Sicherheitsstufe“** von symmetrischen Algorithmen

Für Daten mit langer Lebensdauer oder hoher Sensitivität müssen Schlüssel- bzw. Hashgröße erhöht werden.

AES-128 und SHA-256 sind nicht mehr ausreichend.

Primäre Bedrohungsszenarien

Store Now, Decrypt Later

>> Angreifer sammeln und speichern verschlüsselte Daten, um sie später mit einem Quantencomputer zu entschlüsseln.

Langfristige Wahrung von **Integrität**, **Authentizität** und **Nichtabstreitbarkeit**

>> Fälschung von digitalen Signaturen

>> Nachträgliches Abstreiten der signaturleistenden Partei

Umstellungszeiten von **komplexen Systemen** und **Geräten mit langer Lebensdauer**

>> Trotz vorhandener Lösungen kann die Umstellung auf PQC ggf. zu lange dauern

Unsichere Anwendungsfälle im Unternehmen

Anwendungsfälle, bei denen klassische, **asymmetrische Algorithmen** und Verfahren zum Einsatz kommen, können vollständig gebrochen werden:

Public-Key-Infrastrukturen und **alle Anwendungsfälle von digitalen Zertifikaten**

Digitale Signaturen und **Zeitstempel**

E-Mail-Signaturen und **-Verschlüsselung**

Unsichere Anwendungsfälle im Unternehmen

Anwendungsfälle, bei denen klassische, **asymmetrische Algorithmen** und Verfahren zum Einsatz kommen, können vollständig gebrochen werden:

Authentifizierung und Logins

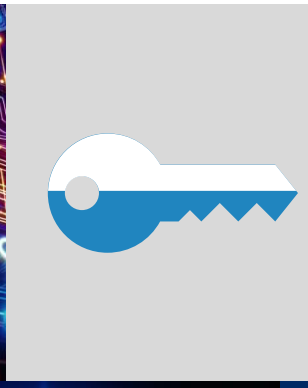
TLS-basierte Verbindungen

Fernzugriff und VPN

Symmetrische Anwendungsfälle im Unternehmen

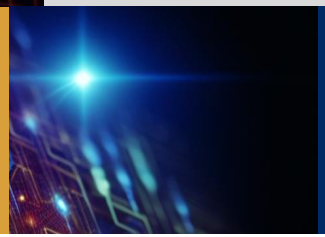
Anwendungsfälle, bei denen klassische, **symmetrische Algorithmen**
und Verfahren zum Einsatz kommen, verlieren ungefähr die Hälfte ihrer Sicherheitsstärke:

Verschlüsselung der Kommunikation



Integritäts- und Authentizitätsprüfung

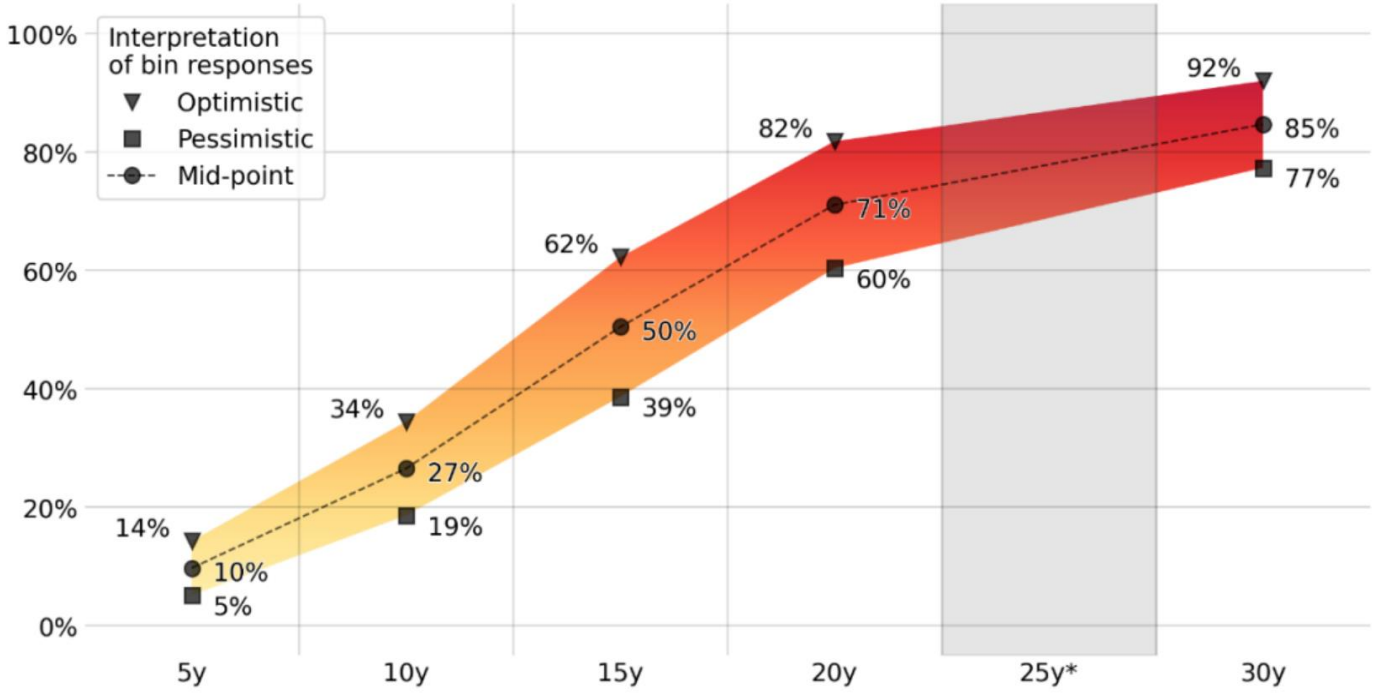
Verschlüsselung von Daten im Ruhezustand



OT, IoT und Haustechnik

Wie dringend ist die Umstellung?

Basierend auf einer Expertenumfrage liegt die Wahrscheinlichkeit, dass ein kryptografisch relevanter Quantencomputer entwickelt wird, bei bis zu **14%** für **2030** und bis zu **34%** für **2035**.



Kumulative Wahrscheinlichkeit, dass **RSA-2048 innerhalb von 24 Stunden gebrochen** werden kann. (Quelle: Quantum Threat Timeline Report 2024, Global Risk Institute)

Zeitvorgaben und -empfehlungen

BSI:

„*Wir fordern die öffentliche Verwaltung, Anbieter kritischer Infrastrukturen, IT-Anbieter sowie die gesamte Industrie dringend auf, den Übergang zur Post-Quanten-Kryptografie zur* ***obersten Priorität*** *zu machen*."
(Quelle: Gemeinsame Erklärung des BSI und 17 weiteren europäischen Cybersicherheitsbehörden:
„Securing Tomorrow, Today: Transitioning to Post-Quantum Cryptography", November 2024)

Europäische Kommission:

bis Ende **2026**: **Planung** und Durchführung von PQC-Pilotprojekten
bis Ende **2030**: **Anwendungsfälle mit hohem Risiko** auf PQC umstellen
bis Ende **2035**: **Anwendungsfälle mit mittlerem Risiko** auf PQC umstellen
(Quelle: "A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography", Juni 2025)

NIST:

bis Ende **2030**: Empfehlung zur Umstellung auf PQC
bis Ende **2035**: **Nutzungsverbot** für klassische, asymmetrische Kryptoalgorithmen
(Quelle: NIST IR 8547 "Transition to Post-Quantum Cryptography Standards")

Die neuen PQC-Standards

NIST-Standardisierungsprozess von neuen PQC-Algorithmen fast abgeschlossen

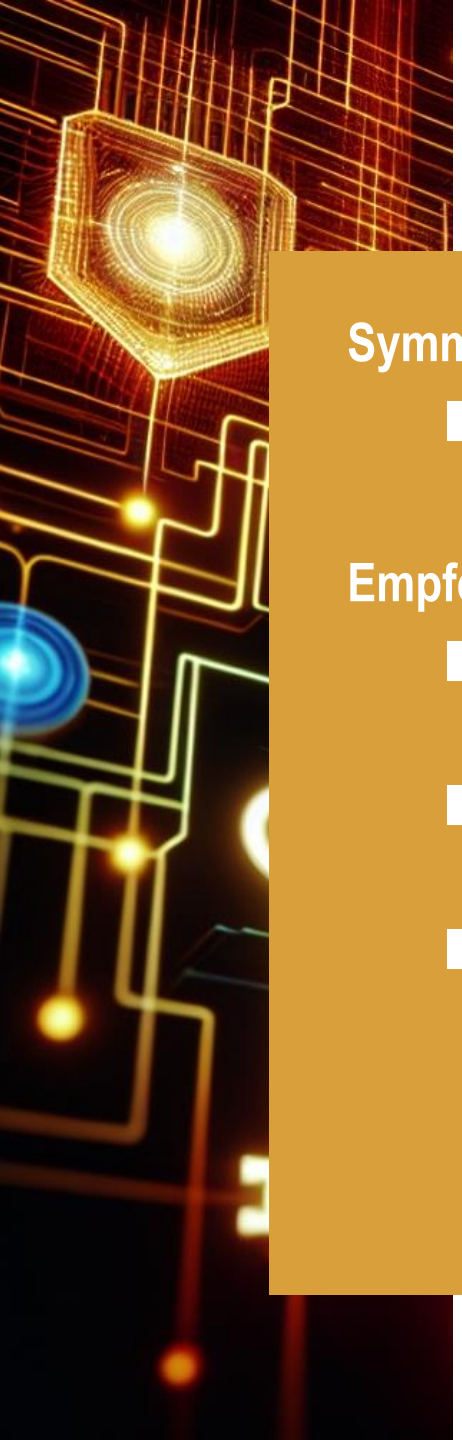
Neue PQC-Algorithmen für **Schlüsselaustausch**

- **ML-KEM** („CRYSTALS-Kyber“, FIPS 203)
- **HQC-KEM** („HQC“, FIPS 207)

Neue PQC-Algorithmen für **digitale Signaturen**

- **ML-DSA** („CRYSTALS-Dilithium“, FIPS 204)
- **SLH-DSA** („SPINCS+“, FIPS 205)
- **FN-DSA** („FALCON“, FIPS 206)

BSI Technische Richtlinie TR-02102
orientiert sich an den NIST-Standards



Die neuen PQC-Standards

Symmetrische Algorithmen

- Derzeit **keine** konkreten Pläne AES und SHA zu ersetzen

Empfehlungen:

- **Größere Schlüssel** bei Verschlüsselungsalgorithmen (AES-256 statt AES-128)
- **Höhere Sicherheitsstärke** bei Hash-Funktionen (mindestens 384 Bit)
- **Verwendung von SHA-3**-basierten Hash-Funktionen

Strategien zur Vorbereitung

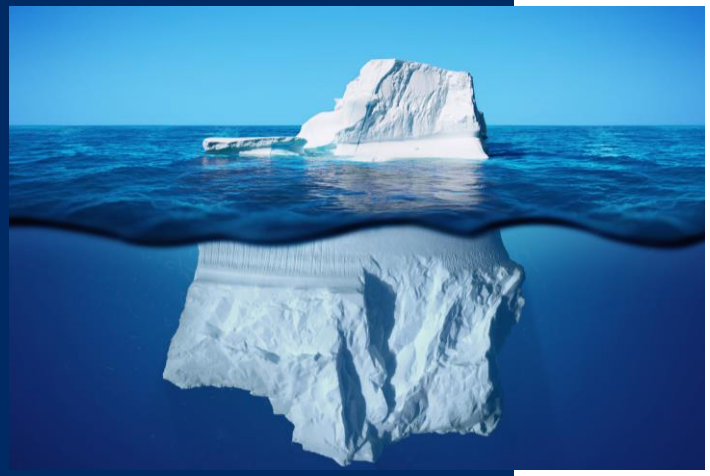
STAKEHOLDER &
ARBEITSGRUPPE

Strategisches Projekt bzw. **Arbeitsgruppe** starten

Verantwortlichkeiten definieren

Interne und externe **Stakeholder** identifizieren und einbinden

Strategien zur Vorbereitung



BESTANDS-
AUFNAHME

Erste Bestandsaufnahme erstellen

Inventar aller Assets erstellen, die kryptografische Algorithmen und Verfahren nutzen

Lebenszyklus kritischer Unternehmensdaten betrachten

Abhängigkeiten der Systeme, Dienste, Produkte, Applikationen und Funktionen dokumentieren

Keine einmalige Aufgabe – regelmäßige Inventarisierung notwendig

Strategien zur Vorbereitung

KRYPTO-
GRAFISCHES
RISIKO-
MANAGEMENT

Schutzbedarf von kritischen Unternehmensdaten und Assets definieren

Einstufung und **Bewertung der Risiken**

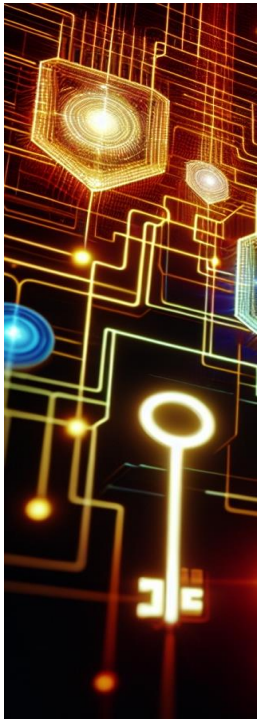
Lebenszyklus der Assets betrachten

Maßnahmen zur Risikobehandlung definieren

Prioritäten für die Umstellung setzen

Welche Maßnahme zur Risikobehandlung ist die Richtige?

Pro Anwendungsfall gibt es vier grundsätzliche Herangehensweisen:



Anpassung bzw. **Aktualisierung**
auf neue Produktversion, die PQC-Algorithmen unterstützt

Erhöhung der Schlüssel- bzw. **Hashgröße**
– nur bei Anwendungsfällen mit symmetrischer Kryptografie

Wechsel auf neues Produkt/System
mit PQC-Unterstützung

Außerbetriebnahme oder **Vermeidung des Anwendungsfalls**

» Wenn möglich, **hybride Lösungen nutzen**, die klassische Algorithmen und PQC-Algorithmen kombinieren.

Strategien zur Vorbereitung

KEINE BESCHAFFUNG OHNE PQC

Bei der **Beschaffung neuer Systeme**, Dienste, Produkte und Software muss das Thema „PQC“ berücksichtigt werden:

- Ist das Produkt „PQC-Ready“?
- Wie sieht die Umstellungsstrategie aus?
- Ist die Hardware leistungsfähig genug für PQC?
- Wird PQC bereits unterstützt?
- Kryptoagilität des Produktes
- Forderung von kryptografischer Stückliste (CBOM bzw. SBOM)

Kryptoagilität ist eine Investition in die Zukunft

Definition

Fähigkeit eines Systems, kryptografische Algorithmen, Verfahren, Protokolle, Materialien flexibel und schnell anzupassen

Kernprinzipen

- **Modularität**: Trennung von Kryptografie- und Applikationslogik
- **Konfigurierbarkeit**: Anpassungen ohne Codeänderung
- **Automatisierung**: Schlüsselrotation, Zertifikatsmanagement

Warum

Vorbereitung auf schnelle Migration/Umstellung
(PQC, Zero-Day-Schwachstellen, neue Compliance-Anforderungen etc.)

Strategien zur Vorbereitung

RICHTLINIEN

Erstellung bzw. Anpassung von
Kryptografie-Sicherheitsrichtlinien

Anpassung sonstiger
Informationssicherheitsrichtlinien
mit Bezug zur Kryptografie

Sensibilisierung der Mitarbeitenden

Fazit

Bedrohung durch Quantencomputer

- Klassische **asymmetrische** kryptografische Algorithmen werden **unbrauchbar**
- **Symmetrische** kryptografische Algorithmen werden **geschwächt**

Vorbereitung

- **Bestandsaufnahme** und **Risikobewertung** durchführen
- **Konkrete Pläne** für die die Umstellung definieren
- **Umstellung** auf Post-Quanten-Kryptografie bis **2030** bzw. **2035**

Kryptoagilität

- Maßgeblicher Hebel zur **Risikoreduktion**
- Wichtiges **Sicherheitsprinzip** für die Zukunft


Post-Quanten-Kryptografie:
Weil wir nicht wollen,
dass Schrödingers Katze
unsere Daten klaut.
ICT BUSINESS &
TECHNOLOGY CONSULTING
DOK
SYSTEME

ICT BUSINESS &
TECHNOLOGY CONSULTING

DOK SYSTEME

Nachhaltig ist, wenn Konzepte Generationen überstehen