Die Bedeutung der Post-Quanten-Kryptografie für Finanzinstitute

Christoph Capellaro

Januar 2026

Building a better working world

Agenda

1. Die Quantenbedrohung für Finanzinstitute
2. Besondere Herausforderungen für Finanzinstitute
3. Lösungsbausteine
4. Integration in den Betrieb

01

Die Quantenbedrohung

Für Finanzdienstleister ist das Risiko einer massiven Sicherheitsverletzung nicht zu vernachlässigen

Das Risiko, dass Kriminelle Quantencomputer einsetzen, um Public-Key-Verschlüsselungsalgorithmen zu knacken, die das Rückgrat der sicheren Übertragung bilden, ist erheblich und kann zu Informationsverlusten, Vermögensschäden und Reputationsschäden führen. Auch wenn der Zeitrahmen für eine solche potenzielle Bedrohung ungewiss ist, ist es jetzt an der Zeit, sich darauf vorzubereiten.

Geschätzte Verluste

2 Billionen Dollar

Wenn ein Angriff mit einem Quantencomputer den Zugang einer der fünf größten Banken zum Fedwire Funds Service stören würde [1]

[1] Arthur Herman und Alexander Butler, „Prosperity at risk: The quantum computer threat to the financial system" (Wohlstand in Gefahr: Die Bedrohung des Finanzsystems durch Quantencomputer), Hudson Institute, 3. April 2023

Geschätzte Ausgaben der Banken für Quantencomputer im Jahr 2027 [2]

630 Millionen

Banken haben begonnen, Anwendungsfälle für Quantencomputer in verschiedenen Geschäftsbereichen zu testen

[2] https://www.inSeitequantumtechnology.com/

Datensicherheit

25 Jahre

Zeitraum, in dem sensible Bankdaten geschützt werden müssen [3]

[3] Skip Sanzeri, "Banks need to act now to ensure post-quantum cybersecurity," Security Today, March 7, 2022

Prozentualer Anteil der weltweit verschlüsselten Daten, die gefährdet sind

90 %

Prozentualer Anteil der globalen Finanzdaten, die durch Public-Key-Verschlüsselung gesichert sind, die von Quantencomputern mit dem Shor-Algorithmus geknackt werden kann [4]

[4] Skip Sanzeri, "Banks need to act now to ensure post-quantum cybersecurity," Security Today, March 7, 2022

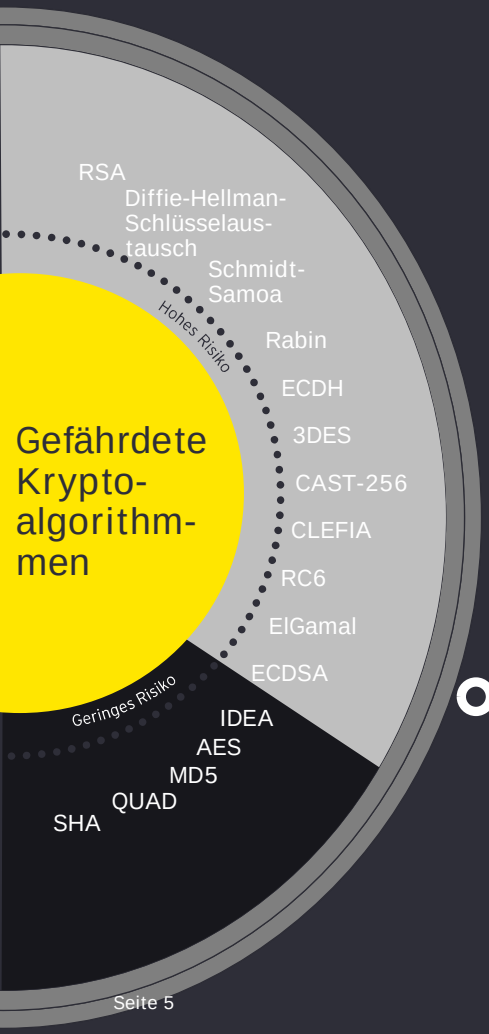
Prozentualer Anteil des gefährdeten digitalen Bargeldes

25 %

Prozentualer Anteil der Bitcoins, die derzeit anfällig für Angriffe durch Quantencomputer-Hardware sind [5]

[5] https://www.inSeitequantumtechnology.com/

Die derzeitige Kryptografie wird unsicher sein, die Frage ist nur, wann



Quantenalgorithmen

Verlassen sich ausschließlich auf Quantencomputer

1. Shors Algorithmus

1994 entwickelte Peter Shor einen Quantenalgorithmus, der gegenüber klassischen Computern eine exponentielle Beschleunigung bei der

- Faktorisierung großer Ganzzahlen
- Lösung diskreter Logarithmen

2. Grovers Algorithmus

1996 entwickelte Grover einen Algorithmus, der eine polynomiale Beschleunigung bei der unstrukturierten Suche ermöglicht.

Anwendungen

- Internet-Banking
- Geldautomaten-Transaktionen
- Kryptowährungen und digitale Vermögenswerte
- Internet der Dinge
- Remote-Arbeit
- ...

Schwachstellen in Kryptoalgorithmen, die Quantencomputer angreifen könnten

- Die Sicherheit der asymmetrischen Kryptografie beruht auf der praktischen Unlösbarkeit bestimmter mathematischer Probleme für moderne Computer.
- Symmetrische Algorithmen sind anfällig für Brute-Force-Angriffe.

Hybride Algorithmen

Kombinieren die Stärke gewöhnlicher Computer mit die Leistungsfähigkeit bestehender Quanten- und Annealing-Computer.

1. Annealing-„Quanten"-Computer

Chinesische Wissenschaftler berichteten, dass sie in der Lage waren, eine 20-Bit-Primzahl mit einem hybriden Algorithmus auf einem herkömmlichen Computer zu faktorisieren, wobei sie 94 Qubits in einem speziellen D-WEB-Quantencomputer nutzten[1] .

2. Quanten-klassisch, speziell für ein bestimmtes Kryptographieschema

(1) https://link.springer.com/article/10.1007%2Fs11433-018-9307-1

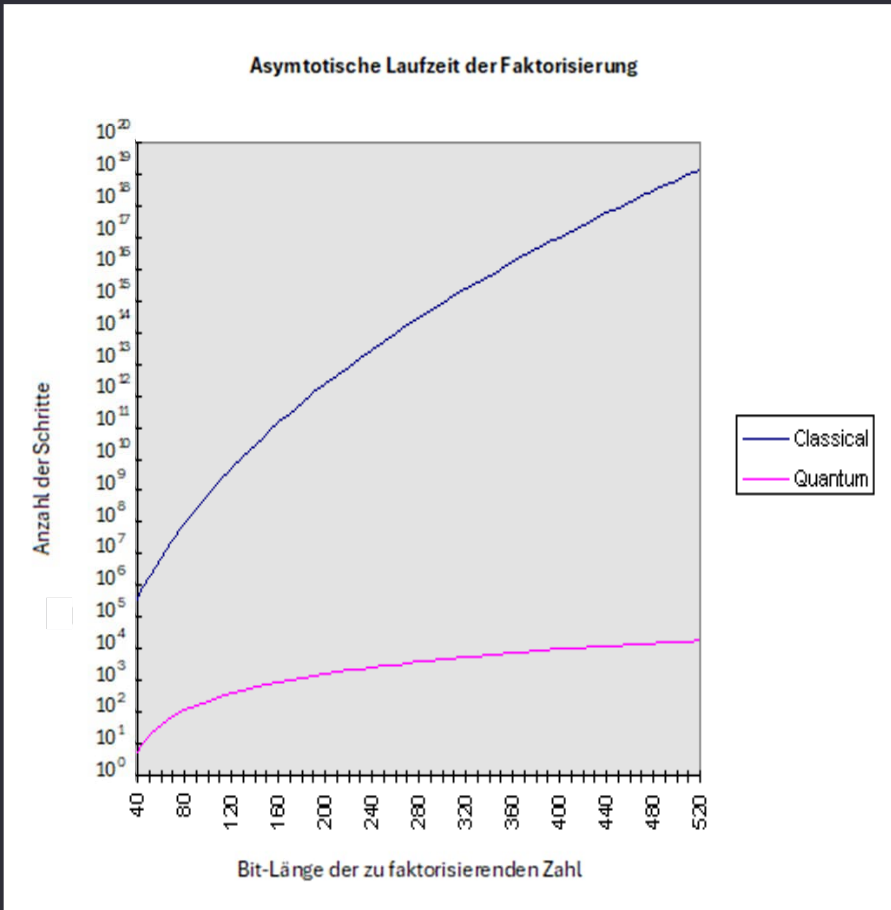
Effizienzgewinn des Quantencomputers bei der Faktorisierung von Zahlen

- Bislang sind für klassische Computerarchitekturen nur Algorithmen mit exponentieller Laufzeit zur Lösung des Faktorisierungsproblems bekannt.
- Der Quantencomputer benötigt

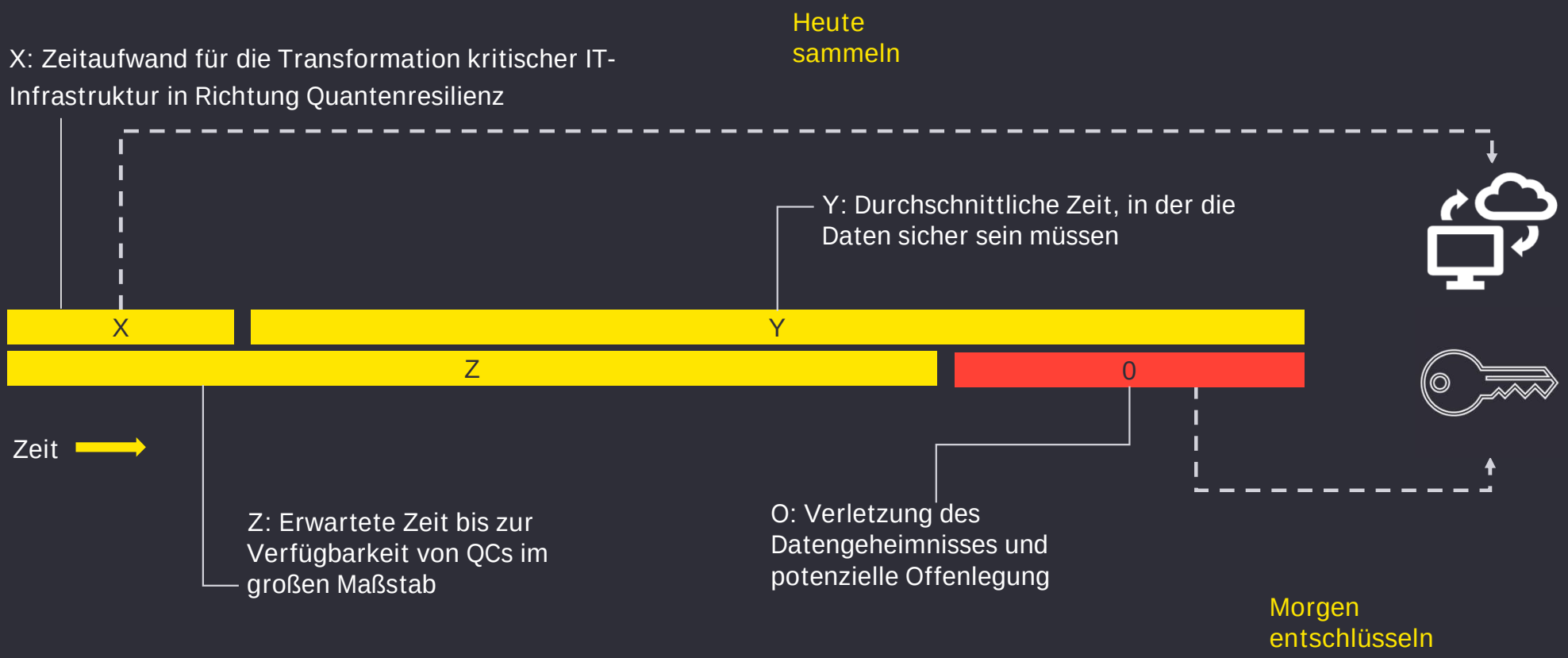
$$O\left((\log n)^2 \log\ \log n\right)$$

Schritte zur Faktorisierung einer Zahl mit einer Länge von *n* Bits.

- Für die vollständige Schlüsselsuche bei einem symmetrischen Kryptoverfahren, wie z.B. AES, gibt es einen Algorithmus für Quantencomputer der mit *O* (log *n*) Schritten auskommt.

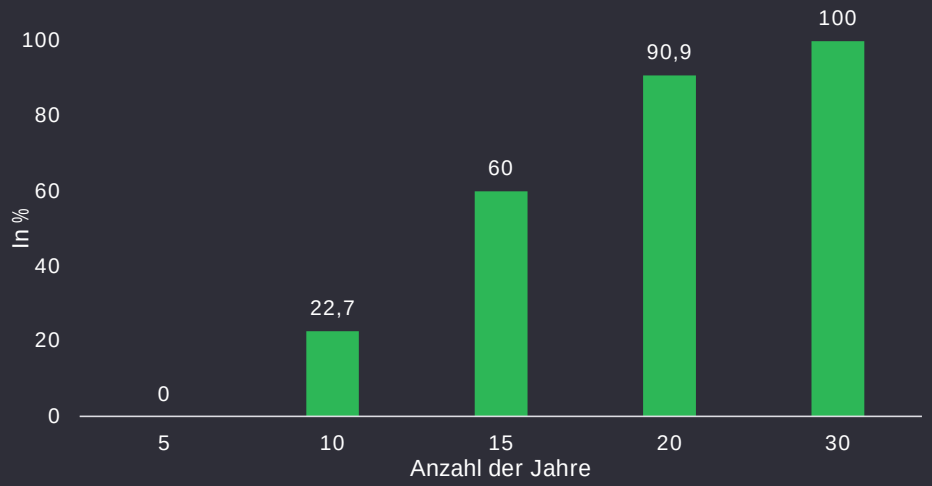


Daten können heute gesammelt werden, um sie evtl. in der Zukunft zu entschlüsseln



Quantencomputer stellen eine erhebliche Bedrohung für die Cybersicherheit dar

Expertenmeinungen zur Wahrscheinlichkeit einer erheblichen Quantenbedrohung für die Cybersicherheit als Funktion der Zeit



Quelle: Zeitachse der Quantenbedrohung, Global Risk Institute, evolution Q. Hinweis: Die Expertenmeinungen gehen weit auseinander; weitere Expertenantworten finden Sie im Bericht zur Zeitachse der Quantenbedrohung 2023

[1] RSA (Rivest-Shamir-Adleman) ist ein Public-Key-Kryptosystem, das häufig für die sichere Datenübertragung verwendet wird.

[2] Im November 2023 behauptete der Forschungswissenschaftler Ed Gerck, den RSA-2048-Schlüssel mit einem Quantencomputer geknackt zu haben. Diese Arbeit wurde nicht unabhängig bestätigt.

[3] Global Future Council on Quantum Computing – Häufig gestellte Fragen, Weltwirtschaftsforum, Juni 2020

- Derzeit als sicher geltende Daten könnten durch Quantenkryptografie entschlüsselt werden: Es ist bekannt, dass Quantenalgorithmen bestehende Sicherheitsalgorithmen knacken können. Der Shor-Algorithmus ist gut verstanden, aber die erforderliche Quantenhardware ist noch nicht verfügbar. Jüngste Veröffentlichungen, beispielsweise von Ed Gerck, schlagen alternative Quantenalgorithmen vor, um RSA mit noch geringeren Anforderungen an Quantencomputer zu knacken. Auch wenn dies noch nicht unabhängig überprüft wurde, zeigt es doch, dass das Risiko allgegenwärtig ist.[2]
- Quantencomputer bedrohen unsere gesamte digitale Infrastruktur. Alle kritischen Infrastrukturen, Transaktionen und Prozesse, die auf Kryptografie basieren und nicht quantenresistent sind, sollten als potenziell verloren gegenüber einem Quantenangreifer betrachtet werden, was zu weitreichenden Störungen führen würde.
- Viele Geräte sind gefährdet Das Weltwirtschaftsforum schätzt, dass in den nächsten 10 bis 20 Jahren weltweit über 20 Milliarden digitale Geräte aufgerüstet oder ersetzt werden müssen, um quantenresistente Kryptografie nutzen zu können.[3]
- Quantencomputer erhöhen Risiken durch Technologien der künstlichen Intelligenz (KI). Quantencomputer werden die Fähigkeiten des maschinellen Lernens (ML) verbessern, was zu einer breiteren Einführung von ML- und KI-Lösungen und -Produkten in allen Branchen führen wird.

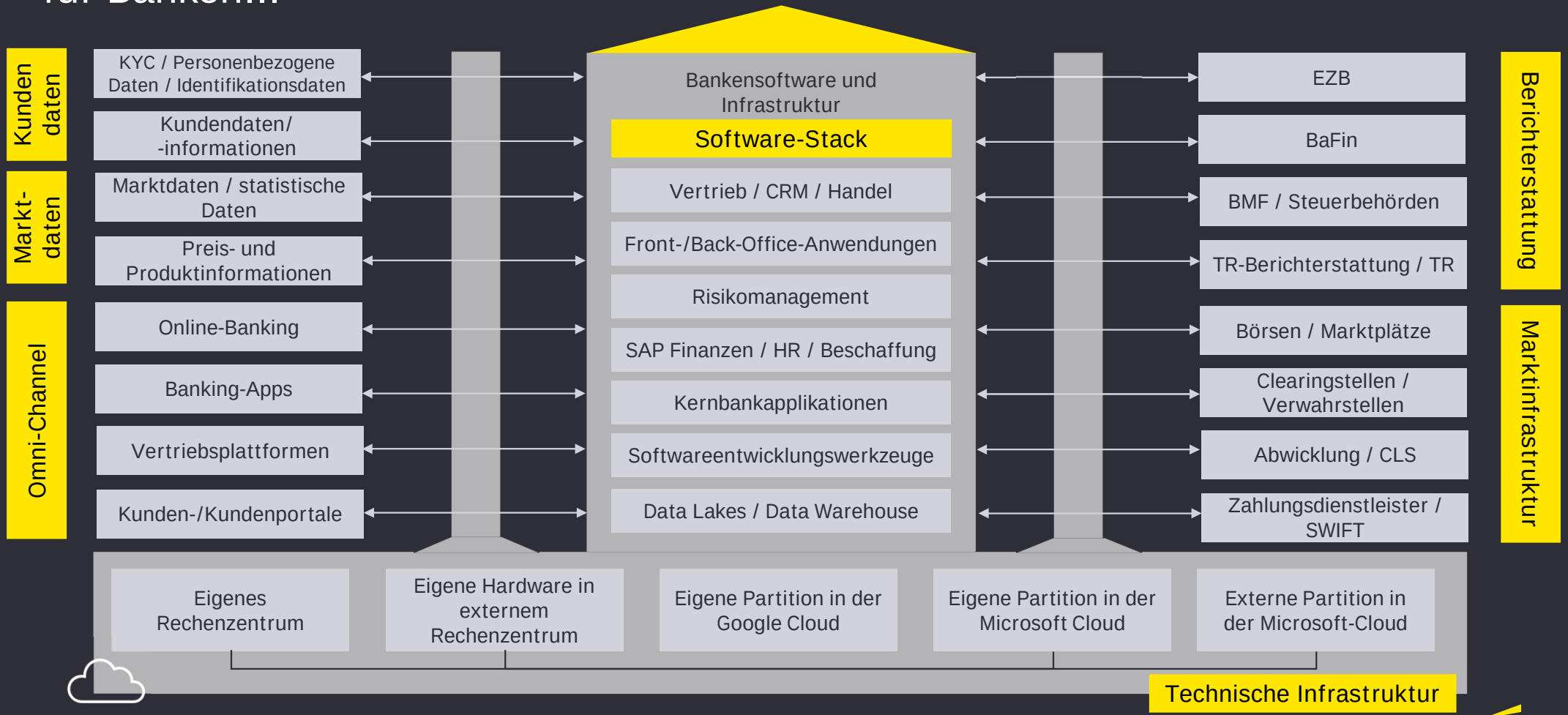
Demo

- Ein Q-Bit
- Superposition und Zufallszahlen
- CNOT und Verschränkung
- Quantensuperiorität am Beispiel des Deutsch-Algorithmus

02

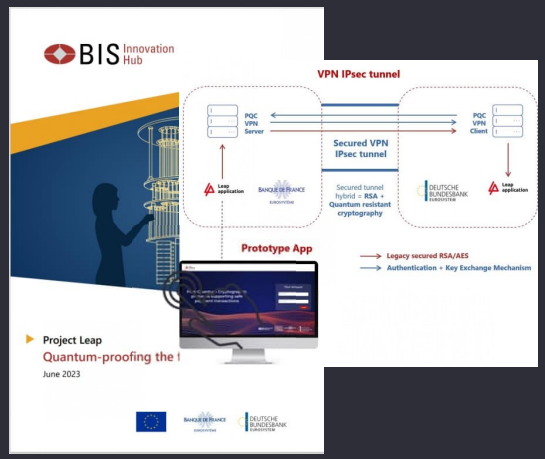
Besondere Herausforderungen

Die Umstellung auf quantenresistente Kommunikation und Datenaustausch führt aufgrund der hohen Vernetzung zu einem komplexen Migrationsprojekt für Banken...



Bundesbank & BSI: Klare Empfehlung, mit den Vorbereitungen für eine quantenresistente Zukunft zu beginnen

BIS / Bundesbank – Projekt „Leap“



- Test zwischen dem BIS Innovation Hub, der Banque de France und der Bundesbank zur Implementierung einer quantenresistenten Kommunikation zwischen den Teilnehmern und zur Verwendung von Post-Quanten-Kryptografie für Zentralbankprozesse wie Zahlungen.

BSI – Quanten-Kryptografie

- BSI: „Quantencomputer stellen eine ernsthafte Bedrohung für die heute verwendete Public-Key-Kryptografie dar. Um im Hinblick auf ein angemessenes Risikomanagement vorbereitet zu sein, müssen die Vorbereitungen für die Post-Quanten-Ära bereits heute beginnen.“

Aktuelle regulatorische Anforderungen an Verschlüsselung beziehen Krypto-Agilität mit ein

	Digital Operational Resilience Act RTS 1774 **DORA**	Cyber Resilience Act **CRA**	Network and Information Security Directive 2 **NIS2**
Umsetzung	Anzuwenden in der EU seit Januar 2025	Anzuwenden in der EU ab Dezember 2027	Deutschland: NIS2-Umsetzungsgesetz (NIS2UmsuCG) Seit Dezember 2025 in Kraft
Anwendungs-bereich	Finanzinstitute	Hersteller und Händler	Kritische Infrastruktur
Verschlüsselung	Pflicht – ruhende Daten Pflicht – übertragene Daten Option – genutzte Daten	Pflicht – ruhende Daten Pflicht – übertragene Daten	Ende-zu-Ende Verschlüsselung empfohlen ruhende Daten übertragene Daten genutzte Daten
Krypto-Agilität	Finanzunternehmen sollten einen flexiblen Ansatz verfolgen, der auf Risikominderung und –überwachung basiert, um mit der dynamischen Landschaft kryptografischer Bedrohungen, einschließlich Bedrohungen durch Quanten-fortschritte, umzugehen.	Implementierung modernster Technologien: ▪ Einführung von Krypto-Agilität ▪ Betrachtung kryptographischer Halbwertszeiten	▪ Kryptografiekonzept ist zu implementieren ▪ Governance-Prozesse sind notwendig ▪ Unabhängige Überprüfung der Netzwerk- und Informationssicherheit ▪ Regelmäßige Aktualisierung

Das NIST hat bereits Algorithmen für die Public-Key-Verschlüsselung und digitale Signaturen für die Standardisierung festgelegt.

NIST analysiert neue quanten- und klassisch resistente Verschlüsselungsstandards

Zu standardisierende Algorithmen

Public-Key-Verschlüsselung

- CRYSTALS-KYBER

Digitale Signatur

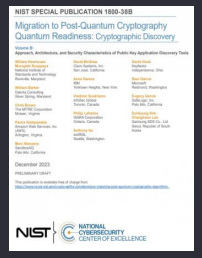
- CRYSTALS–Dilithium
- FALCON
- SPHINCS+

- Um eine weitere Risikostreuung zu erreichen, werden derzeit in der vierten Runde weitere Verschlüsselungsmethoden analysiert
- Die ISO 18033 Serie wird um die von der NIST vorgeschlagenen Algorithmen aktualisiert. Insbesondere werden Key Encapsulation Mechanisms (ML-KEM, ehemals Kyber) integriert.

NIST-Projekt: Migration zur Post-Quanten-Kryptografie

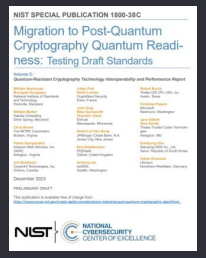
NIST-Veröffentlichunen FIPS 203, 204, 205:

Quantenresistente Kryptoalgorithmen für Schlüsselaustausch und Digitale Signaturen



NIST-Veröffentlichung 1800-38B:

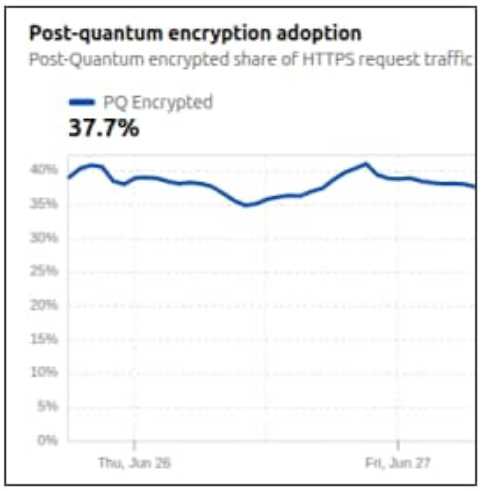
Migration to Post-Quantum Cryptography Quantum Readiness: Approach, Architecture, and Security Characteristics



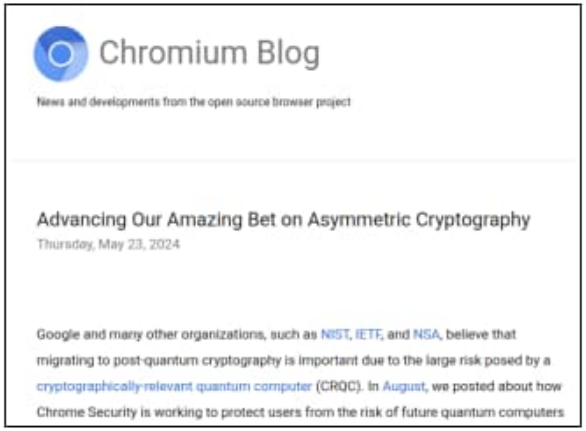
NIST-Veröffentlichung 1800-38C:

Migration to Post-Quantum Cryptography Quantum Readiness: Interoperability and Performance Report

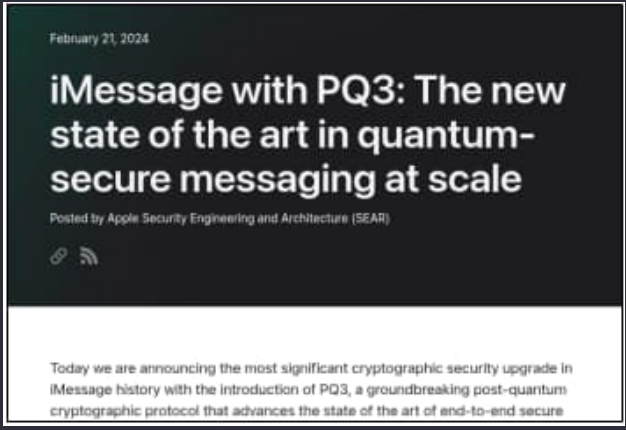
PQK wird bereits in verschiedenen Anwendungen eingesetzt

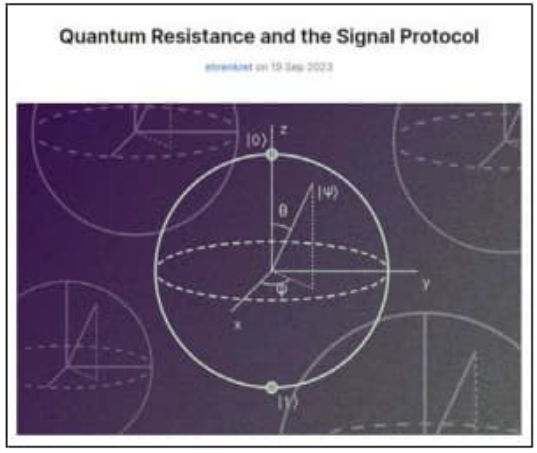


Eine Analyse von Cloudflare zeigt, dass bereits 37,7 % der HTTPS-Anfragen mit PQK verschlüsselt sind



Chrome verwendet standardmäßig TLS 1.3 mit ML-KEM768+X25519 für den Schlüsselaustausch





Quelle: Dr. Andrea Thevis, BSI, Post-Quanten-Kryptographie: Empfehlungen und Aktivitäten des BSI, 2025, Bonn.

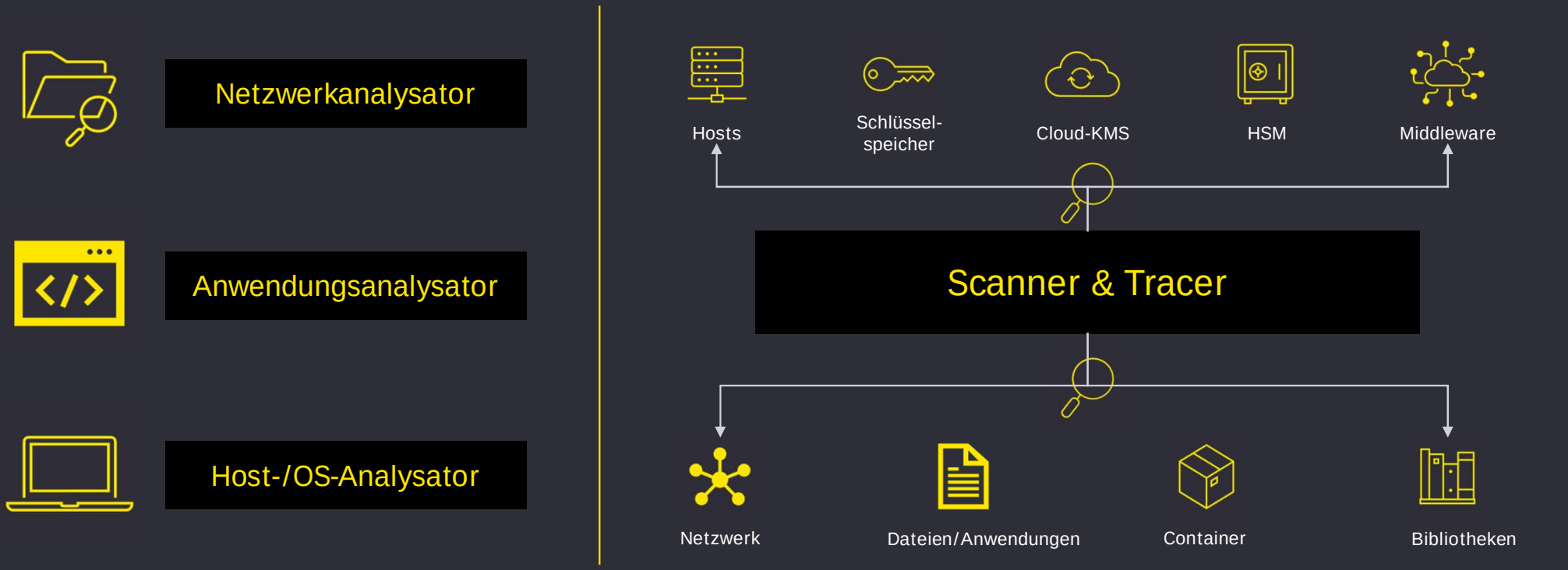
03

Lösungsbausteine

Krypto-Agilität und die Migration zu quantensicheren Kryptoalgorithmen lassen sich in drei Hauptblöcke unterteilen

Krypto-Agilität und Migration zu quantenresistenten kryptografischen Methoden erfordern die Erkennung und Bestandsaufnahme kryptografischer „Assets“.

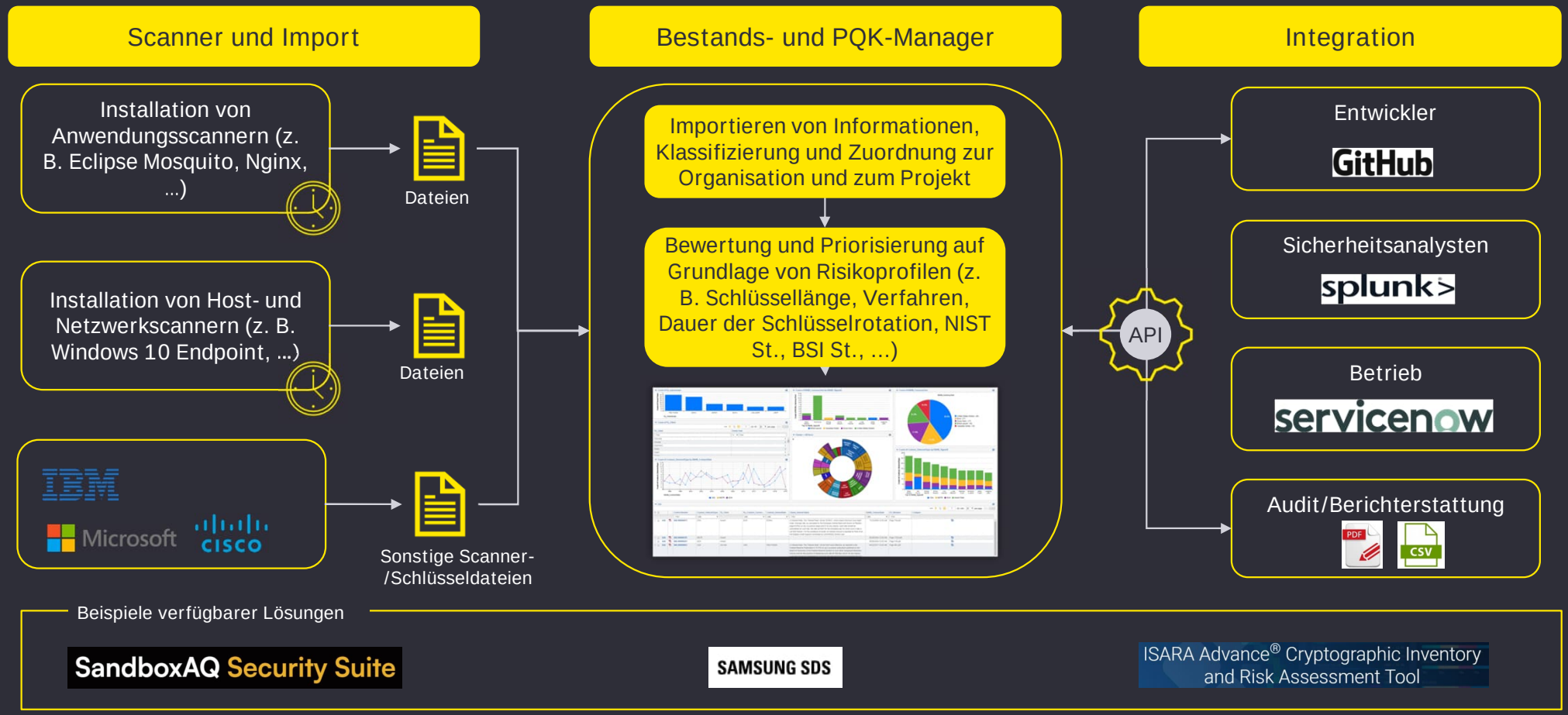
Die Erkennung der verwendeten kryptografischen Methoden erfolgt durch Scanner, die die Kommunikation aktiv überwachen oder Dateien durchsuchen.



Kryptografische „Assets“

Symmetrische Verfahren | Asymmetrische Verfahren (Hohes Risiko) | Hashes | Zertifikate

Die Erfassung und Verarbeitung der Scan-Ergebnisse erfolgt durch die Integration in verschiedene Entwickler- und Sicherheitstools



Bewertung der Risiken und Priorisierung der Risikomitigation

Die Transparenz der Quantenrisiken ermöglicht eine nachhaltige Priorisierung der Maßnahmen zur Risikomitigation.

Bottom-up – Kryptografische Sensibilität

- Erfassen der Anwendungen/Systeme mit entsprechenden Datenkritikalitäts-, Aufbewahrungs- und Kryptografieinformationen aus CMDB, CLM, Schwachstellenberichten und anderen verfügbaren Tools.
- Priorisieren der Anwendungen/Systeme mithilfe einer risikobasierten Methodik für die Behebungsstrategie.
- Aufteilen der Anwendungen/Systeme in Risikogruppen mit definierten Gegenmaßnahmen und Zeitplänen.

Top-down – Kryptografische Priorisierung

- Scannen der Umgebung, um kryptografische Objekte zu erkennen (z. B. Zertifikate, Schlüssel, Kryptosysteme) und ein Inventar mit Schwachstellen und Quantensicherheitslücken zu erstellen.
- Melden von kryptografischen Ergebnissen, um Risiken zu identifizieren, wie unsichere Schlüsselgrößen, kompromittierte Zertifikate oder die Verwendung quantenanfälliger Algorithmen.

Beispielhafte Ergebnisse

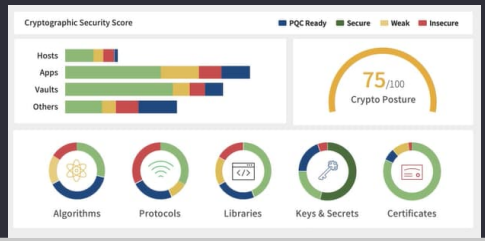
Priorisierte PQK-Asset-Bestandsaufnahme

Info Type						
						Asset Info
Attribute	Asset ID	Asset Name	Asset Owner (IT Owner)	Asset Type	Location/Environment	In
Example Source System	SNOW	SNOW	SNOW	SNOW	SNOW	S
Example(s)	Test System	Asset Business Name	John Smith	Platform, Database, Application	Core Data Center, Vendor Hosted	D

PQK-Risikobewertungsrahmen

Attribute	Grouping	Initial Scoring	Rank	Weight
Data Sensitivity/Criticality	Data	0 - Public, Internal 1 - Confidential 2 - Highly Confidential	1	100
Internet Facing	External Exposure	0 - No 2 - Yes	2	50
IRR Score	Data	0 - <50 1 - 50-60 2 - >60	3	50
Number of Records	Data	0 - <1,000,000 1 - 1,000,000-10,000,000 2 - >10,000,000	4	20
Criticality Level	Data	0 - CL 5,4 1 - CL 3,2,1 2 - CL 0	4	20
Downstream Systems	Data	0 - <10 1 - 10-20	5	10

CBOM-Bestandsaufnahme

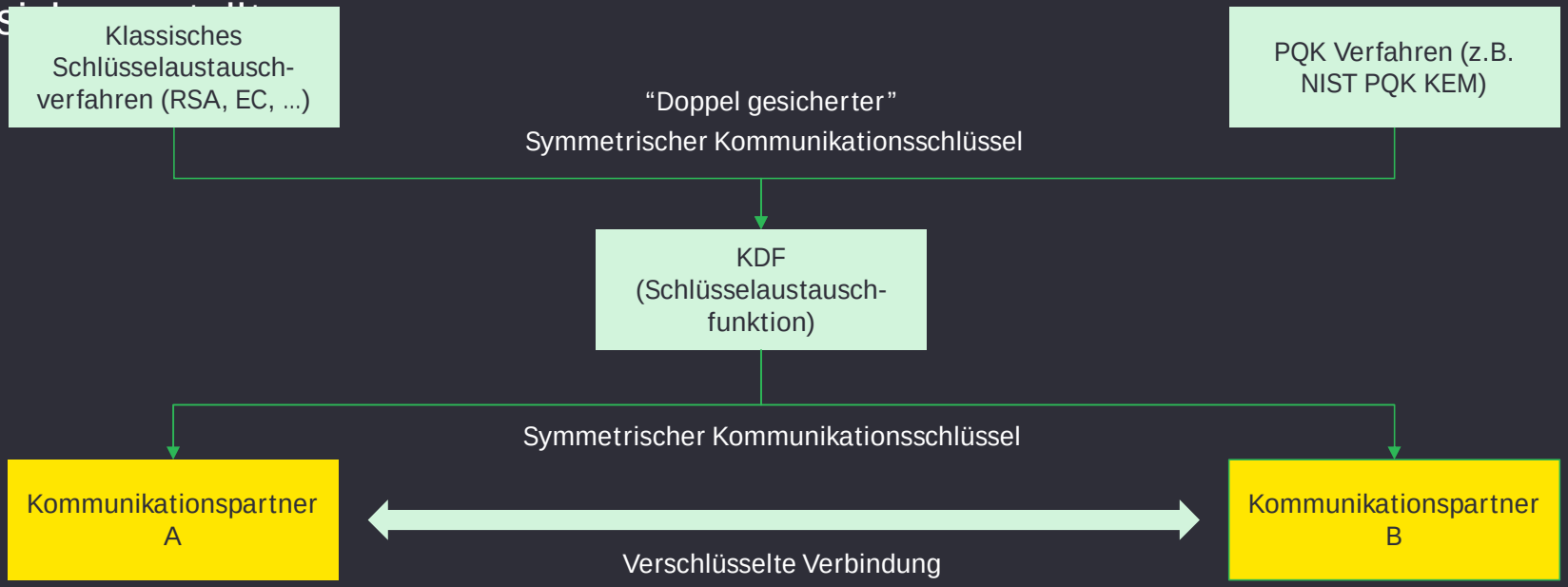


Quantenresistente Kommunikation kann durch verschiedene Ansätze gewährleistet werden, für die es bereits heute Lösungen gibt.

Quantumresistenter TLS-Tunnel	► Quantenresistente Verfahren müssen in bestehende Netzwerkprotokolle wie TLS eingebettet werden, wobei verschiedene Hersteller Lösungen anbieten. ► Die Lösungen generieren zusätzliche Schlüssel für das ausgewählte PQK-Verfahren, insbesondere wenn bereits klassische Schlüsselpaare ausgetauscht wurden. ► Eine weit verbreitete serverbasierte Softwarelösung ist QuSecure, die die Verwendung von PQK-Verfahren
Hybride Post-Quanten-Verschlüsselung VPN	► Im Juni 2023 veröffentlichte die IETF (Internet Engineering Task Force) die Standardisierung eines Post-Quantum-Protokolls für VPN ► Dieses Protokoll wurde nicht nur von der NATO verwendet, sondern auch im „Leap"-Projekt für die sichere Kommunikation zwischen der Bundesbank und der Banque de France eingesetzt ► EY nutzt ebenfalls die softwarebasierte Technologie von Post-Quantum, die jedoch in HSM integriert werden kann
Quantum Key Distribution (QKD)	► Bei QKD tauschen zwei Parteien nicht nur klassische Schlüssel, sondern auch Quantenzustände aus, die in einem optischen Zusatzkanal durch spezielle Hardware erzeugt werden. ► Das erste QKD-Netzwerk wurde 2021 in China geschaffen, aber auch BT verband 2023 verschiedene Rechenzentren in London miteinander. In Europa gibt es beispielsweise das Projekt „Nostradamus" mit der Telekom und Thales.

Hybride Verschlüsselung

Hybride Verschlüsselungsverfahren kombinieren klassische mit quantenresistenten Verfahren. Sie werden für den Austausch von Sitzungsschlüsseln verwendet. Sollte eines der beiden Verfahren gebrochen werden, so wird die Sicherheit des Schüsselaustauschs mit dem jeweils anderen s



Analoge Verfahren bestehen für Digitale Signaturen

Zertifizierung hybrider kryptographischer Verfahren

Im Juni 2025 wurde der Internet Standard IETF RFC 9794 veröffentlicht, der Zertifikatsformate für hybride Schemata mit klassischen und PQK Verfahren definiert.

Bestehende Zertifizierungsinstanzen sind dabei, Serviceangebote auf Basis von RFC 9794 bereitzustellen.

Verschiedene kommerzielle Zertifizierungsinstanzen bieten reine, auf PQK basierende Zertifikate an:

- KeyFactor, Digicert, AppViewX, Evertrust, AnkaTech

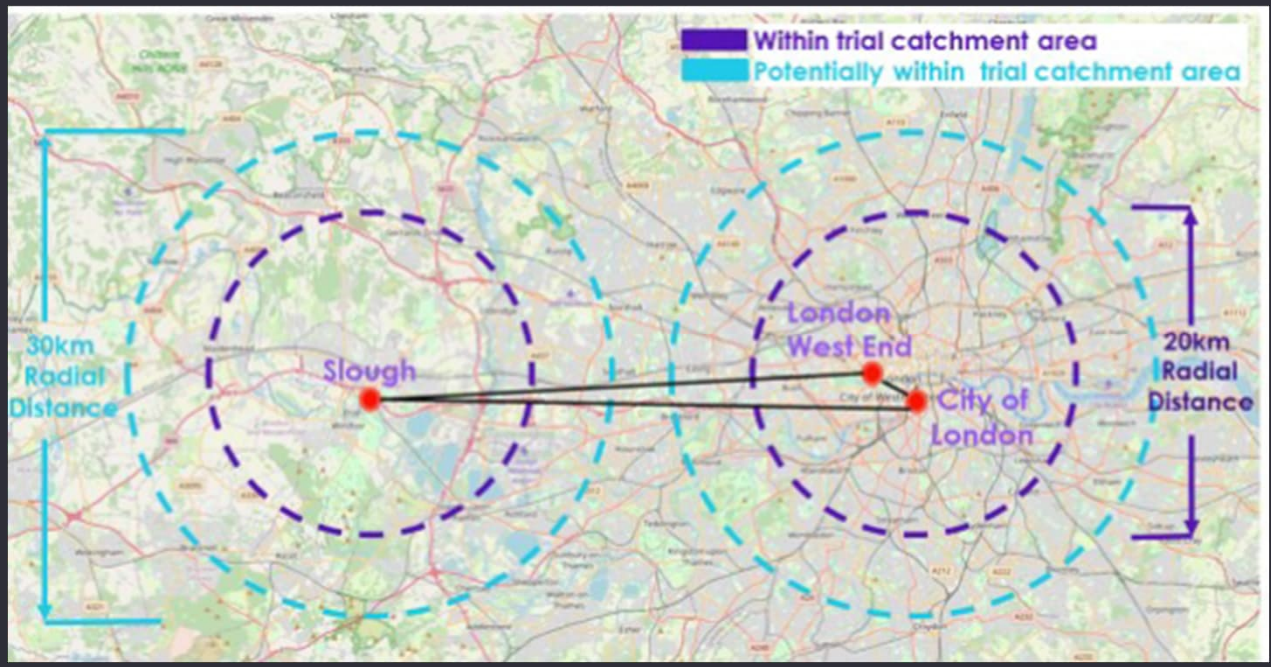
Software-Bibliotheken, die PQK Zertifizierung ermöglichen:

- BouncyCastle, Openssl, MTG, Eviden

London Quantum-Secured Metro Network
https://arxiv.org/pdf/2305.12866

QKD Metro Network in London

- BT und EY etablierten ein kommerziell genutztes QKD-Metronetz in London, komplett mit Kundenzugangskanälen und einem aggregierten zentralen Metroknoten, der mehrere Kunden unterstützen kann



04

Integration von PQK in den IT-Betrieb

Krypto-Agilität ist ein Kernelement der Lösung zur Abwehr von Quantenbedrohungen

Post-Quanten Kryptografie

Anwendung von kryptografischen Methoden

= Eckpfeiler der Cybersicherheit

- Sichere Kommunikation (Datenübertragung)
- Datenverschlüsselung (Daten im Ruhezustand)
- Authentifizierung
- Digitale Signaturen
- Integritätsprüfung (Hashes usw.)
- Schlüsselverteilung und -verwaltung
- Technologie (PKI, HSM, KMS usw.)

Risiken durch veraltete Algorithmen und unzureichende Schlüssellängen

Regulatorische Anforderungen und Standards

DORA, NIS2, CRA, BSI 200-x, ISO270xx

Krypto-Agilität

Transparenz und Handlungsfähigkeit

Kernelemente der Krypto-Agilität

Krypto-Agilitätskonzept

- Proaktive Transformation (mit risikobasierter Priorisierung)
- Einrichtung flexibler, modularer Architekturen und Automatisierung
- Berücksichtigung relevanter Abhängigkeiten

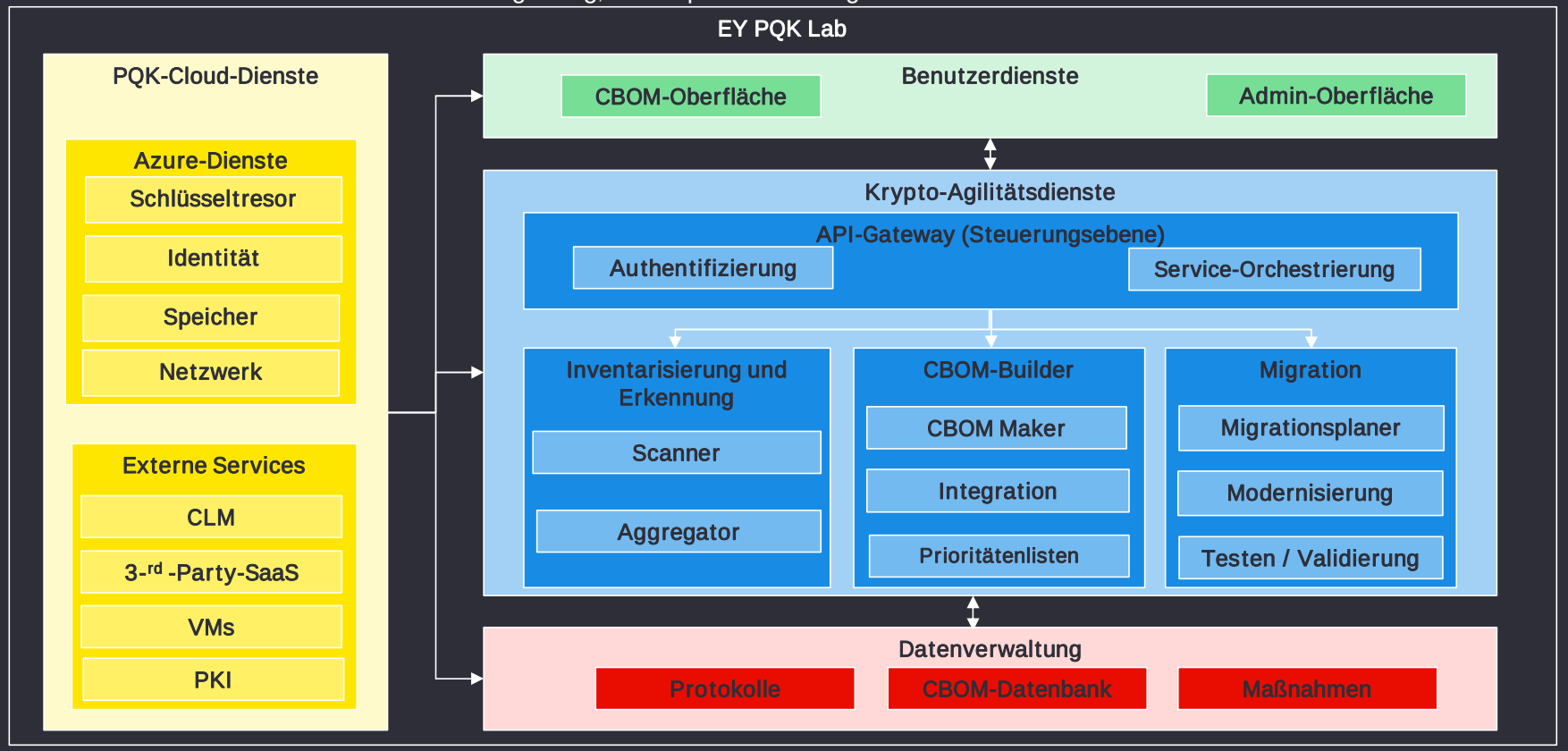
Krypto-Kataster / CBOM

- Systematischer Index (mit Aktualisierung)
- Verwendete kryptografische Verfahren (einschließlich Sicherheitsparameter, Zweck und Verantwortlichkeiten usw.)

Referenzarchitektur

PQK Lab wird auf Azure in einem eigenen abgesicherten Vnet-Bereich bereitgestellt. Der externe Datenverkehr wird über ein NAT-Gateway an das Subnetz jedes Dienstes weitergeleitet.

PQK Lab ist eine SaaS-basierte PKI-Sandbox, mit der quantenresistente Zertifikate generiert und getestet werden können. Sie ermöglicht das Testen quantenresistenter Maßnahmen in einer sicheren Umgebung, die bequem in Azure gehostet wird.



Referent

Dr. Christoph Capellaro

Director
christoph.capellaro@de.ey.com

Shape the future
with confidence

EY | Eine bessere Arbeitswelt schaffen

EY setzt sich für eine bessere Arbeitswelt ein, indem es dazu beiträgt, langfristige Werte für Kunden, Menschen und die Gesellschaft zu schaffen und Vertrauen in die Kapitalmärkte aufzubauen.

Unterstützt durch Daten und Technologie sorgen die vielfältigen EY-Teams in über 150 Ländern für Sicherheit und Vertrauen und helfen ihren Kunden, zu wachsen, sich zu verändern und erfolgreich zu agieren.

Die EY-Teams sind in den Bereichen Wirtschaftsprüfung, Beratung, Recht, Strategie, Steuern und Transaktionen tätig und stellen bessere Fragen, um neue Antworten auf die komplexen Probleme zu finden, mit denen unsere Welt heute konfrontiert ist.

BMC Agency
ED: Keine

ey.com