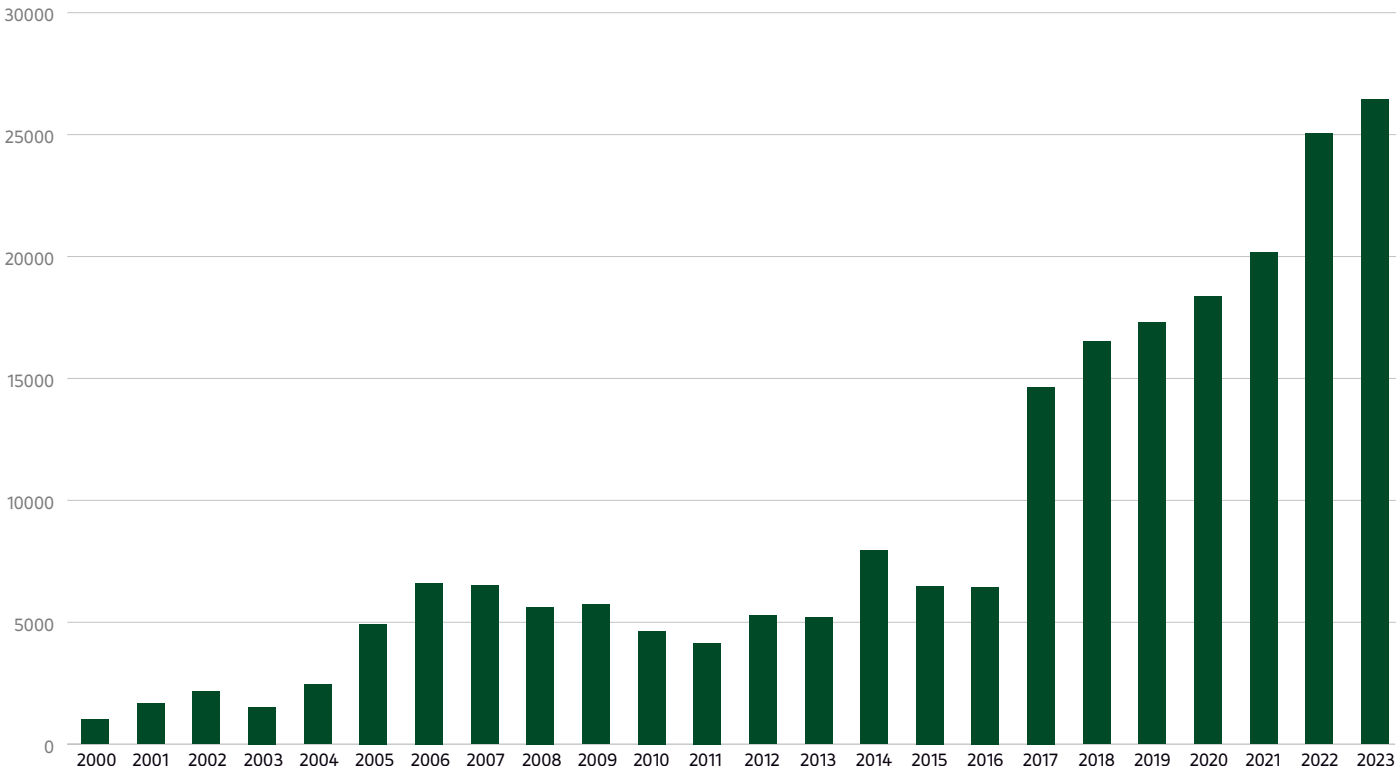
bechtle

Ein Quantensprung
in puncto Sicherheit.

Zukunftsstarke und quantensichere IT.

bechtle.com

Die Landschaft der IT-Sicherheit ist konstant in Bewegung *und Bedrohungen im Bereich der Cyber-Sicherheit treten von Jahr zu Jahr häufiger auf.*



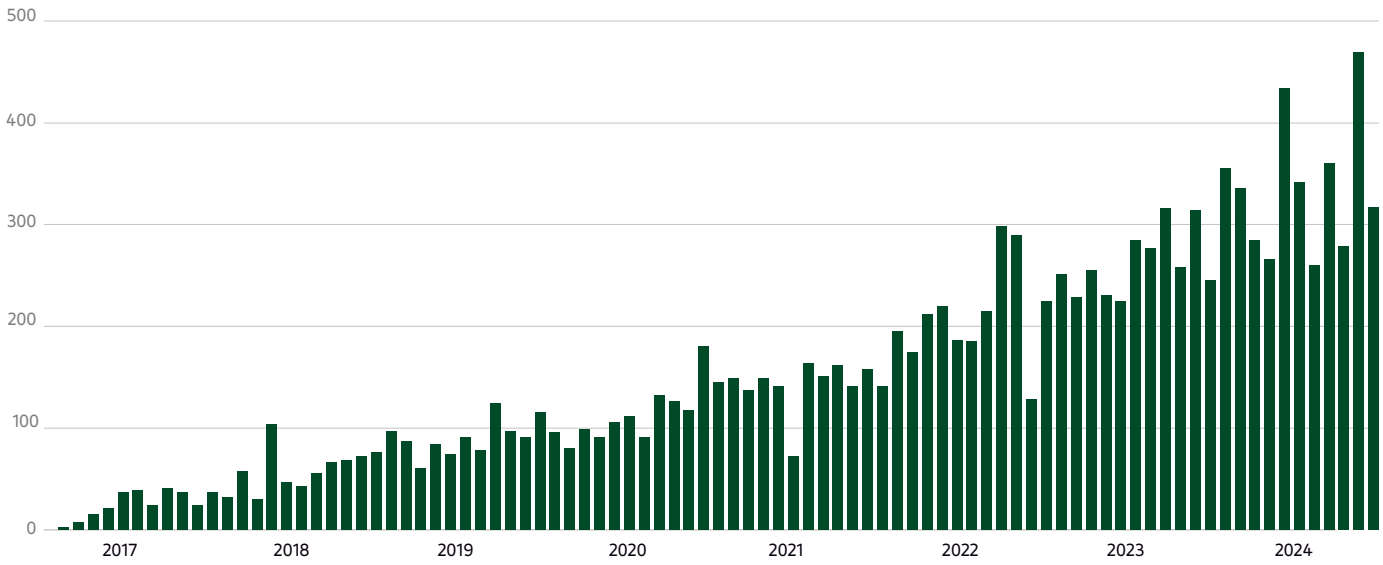
Gesamtzahl der Schwachstellen nach Jahr (2000-2023)

Quelle: 2023 Threat Landscape Year in Review: If Everything Is Critical, Nothing Is | Qualys Security Blog

Die Ursache dafür liegt zum einen in der ständig steigenden Komplexität von Software, wodurch Angriffe auf Lieferketten begünstigt werden. Zum anderen stehen den Akteur:innen hinter den Angriffen immer mehr Werkzeuge zur Verfügung, um Schwachstellen in IT-Infrastrukturen ausfindig zu machen.

Die Vorgehensweise von schadhafter Software wird kontinuierlich verbessert, was das Beheben der betroffenen Schwachstellen zunehmend schwieriger gestaltet.

Rate of vulnerability remediation over time.



Durchschnittliche Behebungszeit (in Tagen) nach Monat.

Quelle: www.sonatype.com/state-of-the-software-supply-chain/

Klassische Angriffe stellen bereits große Herausforderungen für die IT-Sicherheit dar. Neue Werkzeuge verschärfen die Lage nun weiter: künstliche Intelligenz und Quantencomputer. Diese Technologien haben das Potenzial, die IT-Sicherheit in neuen Formen auf die Probe zu stellen. Um dem entgegenzuwirken sowie schnell und angemessen reagieren zu können, bedarf es neuer Methoden. Kryptoagilität und quantensichere Kryptografie sind sinnvolle Maßnahmen, die Schutz bieten und IT-Systeme besser absichern können.

Auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) ruft zum Handeln auf: In einer Erklärung von Ende 2024 mit Partnern aus 17 weiteren Mitgliedsstaaten der EU werden die Wirtschaft, die Betreiber Kritischer Infrastrukturen sowie die öffentliche Verwaltung adressiert – mit der Forderung, den Übergang hin zur Post-Quanten-Kryptografie einzuleiten, einem Schutz gegen Angriffe durch Quantencomputer.

Um welche Bedrohungen geht es im Speziellen und welche konkreten Maßnahmen können Unternehmen heute ergreifen? Wir bringen Sie auf den aktuellen Stand und verschaffen Ihnen Überblick und Navigation im Bereich von Quantum-Safe IT und Kryptoagilität. Steigen Sie jetzt mit uns in diese Thematik ein.

Grundlagen des Quantencomputings.

Quantencomputer nutzen einzelne quantenmechanische Zustände für die Informationsspeicherung und -verarbeitung und setzen damit eine neue Art des Rechnens um. Als elementare Einheit werden Qubits genutzt, die auf verschiedene Weisen und mit unterschiedlichen Technologieplattformen realisiert werden können. Qubits lassen sich miteinander verschränken und in Überlagerungszustände bringen, wodurch eine große Menge an Informationen in größere Qubit-Register kodiert werden kann. Diese Fähigkeiten können wie neuartige Operationen verstanden werden, die auf ganzen Datenräumen gleichzeitig agieren statt auf einzelnen Bits. Die entsprechende Leistungsfähigkeit des Quantencomputers steigt dadurch mit der Anzahl der Qubits im Idealfall exponentiell an – vor allem hierin liegt die Mächtigkeit gegenüber dem klassischen Computing.

Qubit, Superposition, Verschränkung.

Qubit:

Qubits sind die elementaren Einheiten eines Quantencomputers. Im Gegensatz zu Bits speichern Qubits nicht eine binäre Information in Form von 1 und 0 ab, sondern einen quantenmechanischen Zustand. Aus diesem Grund bestehen Qubits aus winzigen quantenmechanischen Systemen wie etwa einem Photon, Elektron, Atom oder Ion, aber zum Beispiel auch einem winzigen supraleitenden Stromkreis. Qubits können direkt miteinander interagieren und unterliegen somit nicht der klassischen von-Neumann-Architektur, da sich Speicher und Rechenwerk am selben Ort befinden.

Superposition:

Da Qubits einen quantenmechanischen Zustand speichern, ist es ebenso möglich, eine Überlagerung von Zuständen zu realisieren. Quantenmechanische Systeme können sich zu Anteilen in mehr als einem Zustand gleichzeitig befinden. Ähnlich einer Münze, die in die Luft geworfen wird, ist das Resultat eine Zeit lang noch nicht festgelegt und beide Möglichkeiten existieren zur selben Zeit. Der Vorteil dieser Eigenschaft liegt darin, dass mit diesem noch „unentschiedenen" System Berechnungen durchgeführt werden können. Man muss also nicht warten, bis die Münze auf Kopf oder Zahl gelandet ist, sondern kann beide Wege zugleich verfolgen und erst am Ende ein Resultat auslesen. Das ermöglicht es, viele Wege eines Algorithmus parallel zu erforschen, ohne jeden Zweig individuell oder auf parallelen Ressourcen rechnen zu müssen.

Verschränkung:

Verschränkung ist eine Eigenschaft, die durch die Interaktion von Qubits miteinander zustande kommt. Während klassische Bits lediglich über Boole´sche Operatoren miteinander interagieren können, haben Qubits Zugriff auf Operationen, die die Informationen in den gespeicherten Quantenzuständen miteinander mischen und korrelieren. Auf diese Weise können zwei oder mehr Qubits in einen gemeinsamen Zustand gebracht werden, der nicht mehr eindeutig einem Qubit zugewiesen werden kann. Dadurch ist es möglich, Korrelationen und Zusammenhänge innerhalb der gespeicherten Information auszudrücken, die mit weiteren quantenmechanischen Operationen bearbeitet werden können. Diese Information ist überall und gleichzeitig auf allen miteinander verschränkten Qubits vorhanden und trägt somit zur Gleichzeitigkeit der Berechnungen bei.

Quantencomputer erlauben damit in speziellen Fällen optimierte sowie völlig neuartige Anwendungen, wobei bislang ungenutzte quantenphysikalische Phänomene zum Einsatz kommen und technisch nutzbar gemacht werden.

Quantencomputing *und IT-Sicherheit.*

Neue Möglichkeiten durch Quantencomputer:

- Erzeugung echter Zufallszahlen
- Teleportation von Zuständen
- Abhörsichere Kommunikation
- Effizientere Lösung spezieller Probleme
  - Schnellere Primfaktorzerlegung großer Zahlen
  - Suche in großen Datenmengen
  - Lösung komplexer kombinatorischer Optimierungsprobleme
  - Fortschrittlichere Simulationen

Signifikante Vorteile sind bislang nur bei bestimmten mathematischen Problemen nachgewiesen und die Überlegenheit gegenüber klassischem Computing ist meist theoretischer Natur.

Auswirkungen auf die IT-Sicherheit:

- Quantencomputer stellen bisherige Annahmen zur Sicherheit kryptografischer Verfahren infrage.
- Aktuelle Verfahren basieren auf der Annahme, dass klassische Computer sie nicht in sinnvoller Zeit berechnen können.
- Neue Algorithmen und Methoden erfordern ein Umdenken in der Kryptografie und gegebenenfalls die Entwicklung neuer Verfahren.

Bei den technischen Umsetzungen gilt es noch einige Hürden zu nehmen. Heutige Quantensysteme sind etwa in der Leistungsfähigkeit sehr begrenzt und weisen noch eine ganze Reihe an Limitationen auf. Für komplexe Kryptografie- bzw. industrierelevante Problemberechnungen müssen sie noch stark weiterentwickelt werden, etwa in puncto Menge und Qualität der nutzbaren Qubits oder bei Fehlerkorrekturverfahren. Denn die Quantenzustände, die zum Rechnen genutzt werden, sind sehr fehleranfällig und fragil, sodass sie vor Interaktionen mit der Umgebung abgeschirmt werden müssen, was nach wie vor eine große technische Herausforderung ist.

Anwendung in der **Kryptografie.**

Die Entwicklungen der letzten Jahre weisen jedoch deutlich darauf hin, dass die neuen Quantentechnologien gerade im Kryptografiebereich hochrelevant sein werden. Hier ergeben sich neue Angriffsstrategien, beispielsweise mit „store now, decrypt later"-Ansätzen, sodass schon heute gehandelt werden sollte, um IT-Systeme zukunftssicher zu machen.

Wie viel Zeit bleibt für die Migration hin zur Quantum-Safe IT?

Um abzuschätzen, wann die Migration zu quantensicherer Kryptografie notwendig ist, ist die folgende Überlegung des Physikers M. Mosca aus [Mos15] sehr anschaulich.

Sei

- **X** die Anzahl der Jahre, die die zu schützenden Daten abgesichert bleiben müssen,
- **Y** die Anzahl der Jahre, die man benötigt, um das entsprechende System auf quantensichere Kryptografie umzustellen, sowie
- **Z** die Anzahl der Jahre, die es noch dauert, bis Quantencomputer existieren, die die aktuell verwendete Kryptografie gefährden.

Dann gilt: Wenn **X** + **Y** >**Z**, **dann haben Sie ein Problem!**

Abbildung: Veranschaulichung zu Theorem von Mosca.

Aufgrund von technischen Limitationen lassen sich heutige Verschlüsselungsalgorithmen mit derzeitig realisierbaren Quantencomputern nicht dekodieren. Die reale Gefährdung resultiert daraus, dass Informationen und Daten mit Verschlüsselungsalgorithmen nach dem derzeitigen State of the Art (langzeit) archiviert werden. Durch fortschreitende technische Entwicklungen im Bereich des Quantencomputings entsprechen diese Algorithmen für den Zeitraum der Archivierung aber nicht mehr dem Stand der Technik und sind somit heute schon als unsicher einzustufen.

Dies sind reale Herausforderungen, denen man bereits jetzt begegnen muss.

Grover- und Shor-*Algorithmus.*

Schon vor über 30 Jahren wurden erste Quantencomputer-Algorithmen postuliert, die die Sicherheit kryptografischer Verfahren bedrohen können. Die beiden häufigsten Vertreter dieser Klasse sind die Algorithmen nach Shor oder Grover.

Shors Algorithmus befasst sich mit dem schnellen Finden von Perioden in mathematischen Funktionen, was die Möglichkeit eröffnet, Primzahl-basierte, diskrete Logarithmen und modulare Algebra-Systeme zu brechen.

Im Gegensatz zur linearen Laufzeit klassischer Algorithmen ermöglicht **der Grover-Algorithmus** eine quadratische Beschleunigung. Dadurch ist es möglich, Lösungsräume schneller zu durchsuchen.

Beide Verfahren benötigen nach aktuellen Einschätzungen etwa eine Million Qubits zur Entschlüsselung von heute üblichen Schlüssellängen. Zur Zeit der Entwicklung dieser beiden Algorithmen waren noch nicht einmal einzelne Qubits realisiert worden und sie waren daher vollständig theoretisch. Heute nähern wir uns Systemen mit mehreren Hundert Qubits an. Das bedeutet, dass nicht nur die technischen Voraussetzungen zur Erforschung und Verbesserung der Algorithmen geschaffen werden, sondern auch die Grundlage für ein besseres Verständnis von Quantencomputern und damit die Möglichkeit, noch mehr potenzielle Angriffsarten zu entdecken. Die Dringlichkeit der Situation entsteht nicht aus der Anzahl der notwendigen Qubits. Gemäß einer Studie des BSI aus dem Jahr 2023 ist die Einschätzung von Unternehmen, dass es noch mindestens zehn Jahre dauert, bis ein kryptografierelevantes Quantensystem existiert. Wollte man der Problematik zum Beispiel begegnen, indem man die Schlüssellängen kryptografischer Verfahren verdoppelt, ginge dies mit erheblichen Performance-Einbußen einher und es ist möglicherweise auf älteren oder eingebetteten Systemen sogar vollkommen unmöglich. Ein solcher Prozess ist stark limitiert und nur in kleinem Maße möglich. Der Quantencomputer hingegen würde zum Berechnen dieses längeren Schlüssels nur wenige zusätzliche Qubits benötigen. Es ist naheliegend anzunehmen, dass in Quantencomputer mit Hunderttausenden oder Millionen von Qubits nahezu problemlos um einige wenige erweitert werden kann und damit das Rennen gegen die Skalierung klassischer Hardware gewinnen wird. Darum ist es so entscheidend, dieser Entwicklung nicht nur reaktiv, sondern proaktiv zu begegnen, denn hat der Quantencomputer den klassischen Computer erst einmal eingeholt, gibt es keinen Weg zurück, diesen Rückstand wieder aufzuholen.

Projektion.

Regelmäßig informiert das BSI zum Thema Quantum-Safe IT, zu kryptografischen Verfahren entsprechend dem State of the Art, zu quantensicheren Schlüsseleinigungs- und Signaturverfahren und veröffentlicht Handlungsempfehlungen.

Obwohl derzeit noch keine großen, leistungsstarken, fehlertoleranten Quantensysteme existieren, können entsprechende Entwicklungen in den nächsten Jahren die derzeitigen Public-Key-Kryptografieverfahren wie RSA und ECC gefährden. Vor dem Hintergrund möglicher „Store now, decrypt later"-Szenarien wird empfohlen, möglichst zeitnah Post-Quantum-Kryptografie (PQC) in hybriden Lösungen einzusetzen, die sowohl aktuelle klassische als auch Post-Quanten-Algorithmen kombinieren. Öffentliche Verwaltungen, Betreiber Kritischer Infrastrukturen und die Industrie werden aufgefordert, den Übergang zur PQC priorisiert anzugehen.

Im Dezember 2021 wurde der Leitfaden „Kryptografie quantensicher gestalten" veröffentlicht, in dem Handlungsempfehlungen aus dem Jahr 2020 für die Migration zur Post-Quanten-Kryptografie ergänzt und ausführlich eingeordnet wurden.

Zum Thema Quantum Key Distribution (QKD) hat das BSI mit europäischen Partnerbehörden im Januar 2024 zudem ein Positionspapier veröffentlicht, das technologische Einschränkungen von QKD aufzeigt und eine Einschätzung des Technologiereifegrades gibt.

Die Bedrohung der Informationssicherheit durch Quantencomputer werde weithin unterschätzt, wie z. B. das Ergebnis einer Marktumfrage zu Kryptografie und Quantencomputing ergab, die das BSI und KPMG in Deutschland durchgeführt haben. Die Ergebnisse wurden als besorgniserregend eingestuft.

Quantencomputer sind eine ernst zu nehmende Bedrohung für die derzeit eingesetzte Public-Key-Kryptografie. Für ein angemessenes Risikomanagement sollte heute mit den Vorbereitungen für die Quantencomputing-Ära begonnen werden. Im Fokus stehen hier die Entwicklung und Standardisierung von Verfahren, die auch gegen Quantencomputer-Angriffe resistent sind.

In den USA hingegen ist die Richtung bereits offiziell und klar vorgegeben. Bis 2033 müssen sämtliche öffentlichen Kommunikationswege quantensicher sein und die Migration hat bereits begonnen. Diese Roadmap wurde von der NSA veröffentlicht und stützt sich auf die Einschätzung der NIST und die aktuellen Entwicklungen von Quantencomputer-Hardware. Es ist daher anzunehmen, dass die US-Sicherheitsbehörden die Bedrohung jetzt schon als solche wahrnehmen und insbesondere die Sicherheit langlebiger Daten wie Infrastruktur und Zertifikate schützen wollen. Die NIST hat in ihrer aktuellen Veröffentlichung (NIST IR 8547 Transition to Post-Quantum Cryptography Standards) bereits klare Vorschläge zur Migration zu quantensicheren Algorithmen publiziert. Dort wird dargelegt, dass Finite Field Diffie-Hellman, Elliptic-Curve Diffie-Hellman und RSA ab 2030 als veraltet gelten und ab 2035 nicht länger zulässig sind. Das bedeutet, obwohl noch einige Jahre vergehen werden, bis Quantencomputer die notwendige Leistung besitzen, um diese Algorithmen effizient zu bedrohen, wird die Interoperabilität mit entsprechend aktueller Software und Services bereits in fünf Jahren eingeschränkt werden, sollte man sich dieser Migration nicht anschließen.

Quantum-Safe IT.

Quantensichere Kryptografie.

Im Bereich der PQC werden kryptografische Algorithmen entwickelt, von denen man annimmt, dass sie gegen kryptoanalytische Angriffe durch Quantencomputer sicher sind. Diese Annahme wird abgeleitet aus der theoretisch bekannten Funktionsweise von Quantenalgorithmen. Aus dem Wissen über die Stärken eines Quantencomputers können begründete Schlussfolgerungen dazu gezogen werden, welche Probleme auch für diese neuen Rechner als unlösbar gelten können.

PQC-Algorithmen lassen sich auf klassischer Hardware implementieren – im Gegensatz zu Verfahren aus dem Bereich der Quantenkryptografie, bei der Systeme mit speziellen quantenmechanischen Eigenschaften benötigt werden.

Quantenrobuste Methoden.

Klasse	Eigenschaften & Beispiele
Hash-basiert/symmetrisch	Für digitale Signaturen, keine Public-Key-Encryption; z. B. Merkle-Signaturen, SPHINCS+, Picnic
Code-basiert	Seit vielen Jahren gut studiert; z. B. McEliece, Niederreiter
Multivariante	Z. B. Oil-and-Vinegar-Methode
Gitter-basiert	Zeigen gute Eigenschaften für digitale Signaturen, Schlüsselaustausch und Key Encryption, relativ kurze Schlüssel und Cipher-Texte; z. B. NTRU, LWE, Ring LWE, Learning with Rounding, CRYSTALS-Kyber, CRYSTALS-Dilithium
Isogenies	Relativ langsame Verfahren; z. B. Supersingular Eliptic Curve Isogenies

Post-Quantum-Kryptografie-Algorithmen sind Stand heute meistens ineffizienter in der Implementierung, weswegen oft Kompromisse bei der Schlüssellänge, der Recheneffizienz, der Länge des Chiffretextes oder der Signatur eingegangen werden müssen.

Ein wichtiger Bereich ist die Standardisierung quantensicherer Kryptografie. Hierzu gibt es einige Aktivitäten, insbesondere das 2016 vom US-amerikanischen NIST (National Institute of Standards and Technology) gestartete „Post-Quantum Cryptography Project". Expert:innen waren dazu aufgerufen, entsprechende Kandidaten für quantensichere Algorithmen einzureichen. Über mehrere Runden wurden bereits zahlreiche eingereichte Verfahren eingehend geprüft. Ziel ist die Standardisierung einer Auswahl von Signaturverfahren, deren Sicherheit auf verschiedenen mathematischen Problemen basiert.

Im August 2024 hat das NIST erste PQC-Standards veröffentlicht. Dabei handelt es sich um drei Verfahren, die gegen zukünftige Bedrohungen durch Quantencomputer schützen sollen:

ML-KEM
(abgeleitet von CRYSTALS-Kyber): ein Schlüsselkapselungsverfahren, das für die allgemeine Verschlüsselung ausgewählt wurde, etwa für den Zugriff auf gesicherte Websites

ML-DSA
(abgeleitet von CRYSTALS-Dilithium): ein gitterbasierter Algorithmus, der für allgemeine digitale Signaturprotokolle ausgewählt wurde

SLH-DSA
(abgeleitet von SPHINCS+): ein hashbasiertes digitales Signaturverfahren

Unternehmen wird empfohlen, die Migration hin zu quantensicheren Algorithmen voranzutreiben, um die Sicherheit sensibler Daten auch in Zukunft zu gewährleisten. Deutsche und europäische Institutionen werden höchstwahrscheinlich zeitnah entsprechende Richtlinien und Handlungskonzepte im Quantum-Safe-Bereich erstellen und diese Standardisierung referenzieren. Erste Empfehlungen hat das BSI bereits unter TR-02102 „Kryptografie quantensicher gestalten" veröffentlicht.

Quantensicherer Datenspeicher.

Die meisten Anwendungsfälle im Bereich quantensicherer Kryptografie befassen sich mit dem Auswechseln nicht quantensicherer Verfahren gegen neue Algorithmen. Es gibt jedoch bereits erste Ansätze der Datenspeicherung, die agnostisch gegenüber kryptografischen Verfahren ist und dennoch Daten vollständig quantensicher (und somit auch sicher gegenüber klassischen Angriffen) speichert.

Ein Beispiel dazu ist das Lincos-Verfahren. Dabei werden die Daten auf mehrere Speicherorte aufgeteilt, und zwar nach den Regeln eines rein mathematischen Verfahrens. Es entsteht dadurch eine völlig neue Lage von Sicherheit, anstatt ein weiteres kryptografisches Verfahren auf dem bestehenden Stapel aufzusetzen. Dadurch kann eine kryptografische Architektur nicht nur gestärkt, sondern eventuell auch vereinfacht werden, da hier zum Beispiel die Notwendigkeit einer Schlüsselrotation entfällt. Das Verfahren ist so sicher, dass, selbst wenn ein Großteil der verteilten Daten von einem Angreifenden eingesammelt wird, es nicht möglich ist, die Daten im Klartext vollständig wiederherzustellen, selbst nicht für einen theoretisch perfekten Quantencomputer. Es bietet sich also sowohl für Einsatzmöglichkeiten an, bei denen große Datenmengen ohnehin verteilt gespeichert werden und viele Nutzende darauf zugreifen, als auch für Szenarien, bei denen einzelne Datensätze geschützt werden sollen. Dadurch wird ein Teil der Daten sicher gekapselt gespeichert und somit sind die restlichen Daten unbrauchbar oder man erhält eine zusätzliche Sicherheitslage ohne weiteren Overhead bei der Nutzerverwaltung.

Echte Zufallszahlen.

Quantencomputer bieten eine adäquate und gut skalierbare Lösung für das Problem von Pseudozufallszahlen-Generatoren (Pseudo Random Number Generators/Pseudo RNG bzw. True RNG) in Form von Quantenzufallszahlen-Generatoren (QRNG). Dabei handelt es sich um ein Schema, bei dem die inhärent zufällige und vollständig unvorhersehbare Natur von Quantensystemen genutzt wird, um Zufallszahlen zu erzeugen.

Ein Quantencomputer ist in der Lage, mit seinen Qubits Zufallszahlen unabhängig und effizient zu erzeugen. Dazu ist nicht einmal ein ganzer Quantencomputer nötig. Es existieren bereits erste Systeme, die kleine Quantensensoren verwenden, um dasselbe Prinzip zu nutzen. Diese Einheiten sind meist nicht größer als ein USB-Stick und sind in Quantenkommunikations-Hardware bereits vorhanden oder könnten als Add-on in klassischen Systemen genutzt werden. Dies ist ein schneller und kostengünstiger Weg, eine Verbesserung der kryptografischen Eigenschaften eines Systems zu erzeugen und die Infrastruktur gegenüber zukünftigen Angriffen durch KI oder Quantencomputer zu stärken.

Herkömmliche Verfahren, die Pseudo- oder True RNG nutzen, haben demgegenüber mehrere Nachteile – etwa deterministisch auftretende Muster, unzureichende Effizienz oder „Kaltstart-Probleme", Anfangs- bzw. Umgebungsbedingungen bei der Erzeugung, die Einfluss auf die erzeugten Werte haben und sich im schlimmsten Fall nachvollziehen und vorhersagen lassen.

	Pseudo RNG	True RNG	Quantum RNG
Mechanismus	Mathematisch	Physikalisch	Physikalisch
Gleich verteilt	Möglich	Möglich	Möglich
Unabhängig	Nein (deterministisch)	Ja	Ja
Effizient	Ja	Nein	Ja
„Kaltstart"-Problem	Nein	Möglich	Nein
Beispiel	Mathem. Funktion	Münzwurf	Spontane Emission von Photonen

Quantenkommunikation.

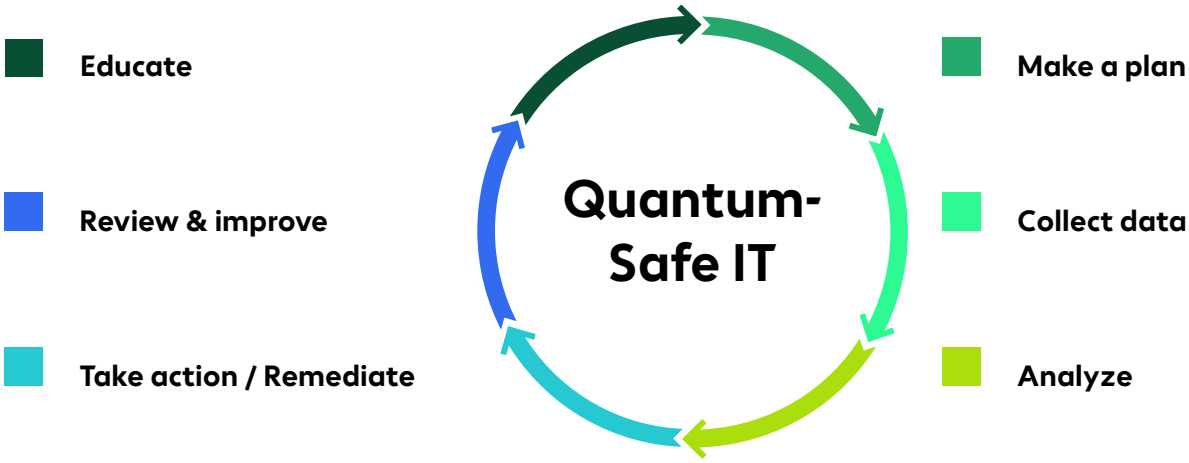
Bei der Quantum Key Distribution (QKD) handelt es sich um Verfahren der Quantenkryptografie, die Eigenschaften der Quantenmechanik nutzen, um zwei Parteien eine gemeinsame Zufallszahl zur Verfügung zu stellen. Diese kann als geheimer Schlüssel genutzt werden. Mit einem solchen Schlüsselaustausch und mit klassischer symmetrischer Verschlüsselung lassen sich Nachrichten nahezu abhörsicher übertragen. Unterschieden werden zwei Klassen: verschränkungsbasierte Verfahren (z. B. das E91-Protokoll) und nicht verschränkungsbasierte Verfahren (z. B. das BB84-Protokoll).

Vorteilhaft an der QKD ist, dass die Sicherheit auf physikalischen Gesetzen beruht und nicht auf Annahmen über die Leistungsfähigkeit von (zukünftigen) Computern oder den Möglichkeiten eines Angreifenden. QKD macht sich eines der Grundprinzipien der Quantenphysik zunutze: Beobachtungen verursachen Veränderungen im betrachteten System. Dadurch lassen sich Lauschangriffe mit hoher Wahrscheinlichkeit aufdecken.

Mit Partnerbehörden aus Frankreich, den Niederlanden und Schweden veröffentlichte das BSI im Januar 2024 ein Positionspapier zu QKD. Darin wird darauf hingewiesen, dass QKD wegen technologischer Einschränkungen bislang nur in speziellen Anwendungen eingesetzt werden kann und es aus Sicherheitssicht derzeit noch nicht vollständig ausgereift ist. Bei der Migration hin zu quantensicheren Verfahren sollte die Priorität daher auf der Post-Quanten-Kryptografie liegen.

In diesen bereits bekannten Möglichkeiten besteht jedoch nur der erste Schritt von Quantenkommunikation. Forschungsgruppen befassen sich bereits mit der Erkundung von vollständig abhörsicheren Quantenkanälen. Dabei kann ein Algorithmus auf einen Quantencomputer übertragen, dort ausgeführt werden und die Ergebnisse können zum Absender zurückgelangen, ohne dass sich Informationen an Zwischenstellen auslesen lassen. Damit ermöglicht Quantencomputing im Zusammenspiel mit Quantenkommunikation sogar eine noch engmaschigere Informationskette, als homomorphe Kryptografie es erlauben würde.

Erste *Schritte.*



Kryptoinventar.

Ein erster Schritt besteht nicht direkt im Austausch von kryptografischen Algorithmen, sondern in der Katalogisierung der genutzten Hard- und Software. Die Migration zu neuer Kryptografie bedeutet nicht nur eine große Aufgabe, es besteht auch jederzeit die Möglichkeit, dass neue Anpassungen oder Erkenntnisse weitere Updates notwendig machen. Darum raten Behörden und Expert:innen dazu, ein sogenanntes Kryptoinventar anzulegen und regelmäßig zu pflegen. Damit ist eine vollständige und erschöpfende Liste aller kryptografischen Verfahren, Geräte und Richtlinien innerhalb einer Infrastruktur gemeint. Dies dient nicht nur dem Erkennen veralteter Endpunkte, sondern erlaubt auch eine Priorisierung des Migrationsbedarfs, sodass kleinere und kritischere Substrukturen zuerst auf quantensichere Kryptografie umgestellt werden und die restliche Infrastruktur in sinnvollen Arbeitseinheiten aufgearbeitet wird.

Kryptoinventar

Erster Schritt: Erstellung eines Kryptoinventars (komplette Liste aller kryptografisch relevanten Verfahren, Geräte, Richtlinien).

Nutzen des Kryptoinventars:

- Identifikation veralteter Komponenten
- Priorisierung der Umstellung (z. B. zuerst kritische Systeme)
- Bessere Planung und Kontrolle
- Erhöhte Flexibilität für zukünftige Entwicklungen

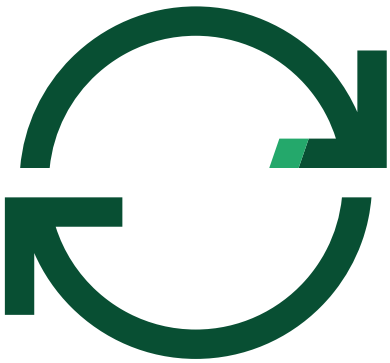
Bereits seit einigen Jahren werden Werkzeuge und Standards entwickelt, um eine solche Krypto-Inventarisierung durchzuführen. So wurde zum Beispiel, basierend auf dem existierenden SBOM-Standard, ein CBOM-Standard erschaffen. SBOM ist ein Verfahren, das umfassende Informationen über die Komponenten einer Software-Anwendung sammelt und transparent abbildet. Implementiert wird es durch Standards, wie zum Beispiel CyclonDX, und erhält so ein hohes Maß an Kompatibilität und Austauschbarkeit. Bislang waren Sicherheitsaspekte in SBOM lediglich durch die Identifikation von Herstellern und Lieferketten gegeben. CBOM zielt darauf ab, konkrete kryptografisch relevante Informationen in einer Erweiterung dieser Standards zu erfassen und somit die Sicherheit von verwendeten Anwendungen direkt zu gewährleisten statt wie bislang nur indirekt.

Es ist also möglich, bereits genutzte Datensätze basierend auf SBOM weiterzuverwenden und mit den notwendigen kryptografischen Informationen auf CBOM zu erweitern. Auch existiert bereits eine Auswahl an Werkzeugen, die aktiv, passiv oder manuell Netzwerke durchsuchen können und Sicherheitsrichtlinien sowie Kommunikationsprotokolle entdecken. Beispiele dafür sind das Quantum Safe Toolkit von IBM oder P-Cert von Data Warehouse.

Es ist möglich, Software entweder im Quellcode oder im ausführbaren Zustand analysieren zu lassen, um genutzte Krypto-Bibliotheken aufzulisten und somit dem Krypto-Inventar hinzuzufügen. Manche Werkzeuge unterstützen dabei sogar die vollständige Analyse von Hardware bis auf die Ebene der verwendeten Komponenten und Firmware-Versionen. Damit kann nicht nur ein exaktes Bild der kryptografischen Komposition einer Infrastruktur erstellt werden, sondern es kann auch ein Qualitätsmerkmal in der Sicherung kritischer Lieferketten sein. So reiht sich die Krypto-Inventarisierung direkt und sinnvoll in die Anforderungen von NIS 2 in Bezug auf die Offenheit von Lieferketten und die Sicherung gegenüber zukünftigen Angriffsszenarien ein.

Kompatible Services.

Der wahrscheinlich einfachste Schritt hin zu quantensicherer IT besteht darin, an existierende Lösungen anzuknüpfen.



Schon heute gibt es eine Auswahl an Services, die bereits kompatibel mit PQC-Algorithmen sind und auch aufseiten der Hardware-Hersteller werden seit ein paar Jahren erste Geräte mit entsprechenden Protokollen ausgeliefert. Daher stehen die Chancen gut, dass in jeder Infrastruktur mit einer gewissen Größe bereits Kontakte zu Hardware, Software oder Services vorliegen, die eine quantensichere Kommunikation bereits unterstützen. Diese Kontaktpunkte können als Ausgangsbasis und auch experimentelle Schnittstellen dienen, um einen Einstieg für die eigene Migration zu finden. Nennenswerte Beispiele sind ausgewählte Android- und Apple Services, Cloud Services von Cloudflare und E-Mail-Software von Tuta. Mozilla Firefox unterstützt bereits hybride quantensichere Verschlüsselungen, sodass es selbst ohne Wechsel des Browsers möglich ist, mit entsprechend gesicherten Online-Ressourcen zu kommunizieren. Auf Hardware-Seite sind bereits einige Produkte einschlägiger Hersteller, wie secunet, Adva und Rhode & Schwarz, bereits kompatibel mit den neuen Protokollen und ermöglichen unkomplizierte Updates der Hardware oder in manchen Fällen sogar rein Firmware-seitige Aktualisierungen.

Praktische Umsetzung: *Wir unterstützen Sie.*

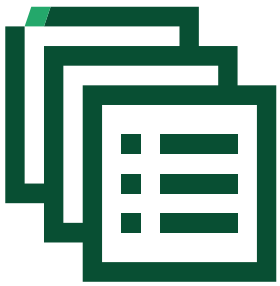
Durch unsere langjährige Erfahrung und unser umfassendes Netzwerk an Partnern kann Bechtle bestehende und neue Kunden auf jedem Schritt entlang dem Weg hin zu einer optimierten und zukunftssicheren IT unterstützen.

Wir führen Assessments Ihrer bestehenden IT-Sicherheitsinfrastruktur durch, um festzustellen, welcher Ansatz für Sie die besten Ergebnisse, mit der geringsten Störung des laufenden Betriebs und minimalem Aufwand erzielt. Dazu untersuchen und katalogisieren wir bestehende Krypto-Assets und erstellen eine priorisierte Liste von möglichen Schritten. Dieser Prozess kann weiter unterstützt werden durch die zeitgleiche Implementierung kryptoagiler Methoden. Dadurch werden nicht nur aktuell anstehende Migrationsprozesse vereinfacht, sondern auch zukünftige Updates können mit einem Bruchteil des Aufwands einer vollständigen Bewertung durchgeführt werden.

Sobald die notwendigen Arbeitsschritte erfasst sind, erstellen wir gemeinsam mit Ihnen eine Roadmap, die ideal zu Ihrer Unternehmensstrategie passt. Bechtle kann jeden Teil Ihrer Migration hin zu zukunftssicherer IT begleiten, beginnend mit Netzwerkkomponenten auf Hardwareebene bis hin zu Endanwender-Software. Da wir den gesamten Stack, von der ersten Netzwerkschnittstelle bis hin zu den täglichen Anwender:innen begleiten, ergibt sich für Sie eine nahtlose, unkomplizierte und ganzheitliche Lösung aus einer Hand.

Wir begleiten Ihr Sicherheitskonzept auch langfristig. Das beinhaltet die Verwaltung und Überwachung Ihrer Krypto-Assets, das Einpflegen neuer Komponenten und Systemeinheiten sowie Beratung und schnelle Unterstützung bei unerwartet auftretenden Herausforderungen.

Hintergrundinfos/Zum Weiterlesen:



Überblick zum Thema Post-Quanten-Kryptografie auf der BSI Webseite

Erklärung von BSI und Partnern aus 18 EU-Staaten vom 30.11.2024 mit Forderung zur Einführung und Nutzung von PQC

NIST Report von November 2024 zur Einführung von PQC-Standards

BWI Pressemeldung vom 25.01.2024 zum Thema quantensicheres Wide Area Network der Bundeswehr

Überblick zum Thema quantensichere Kryptografie des BWI

Pressemeldung des BMBF vom 27.11.2024 zum Thema quantenverschlüsselte Datenkommunikation

Marktumfrage Kryptografie und Quantencomputing

Kryptographische Verfahren: Empfehlungen und Schlüssellängen

Sie haben Fragen zum Thema quantensichere IT?
Nehmen Sie Kontakt mit uns auf:

quantum.bonn@bechtle.com