PRESSEMITTEILUNG

Der Post Quantum Datenschutz-Gau passiert schon heute

Viele warten mit Datenschutzmaßnahmen für die Quanten-Computer-Ära, bis es so weit ist. Doch was ist, wenn die verheerendsten Datenschutzverletzungen bereits heute und damit Pre-Quantum passieren?

Die Widersprüchlichkeit in den Prognosen zur Einsatzfähigkeit von Quantencomputern ist ein historisches Merkmal von disruptiven Technologien. Die einen sprechen von baldigen ersten Ergebnissen, die anderen von einem Zeithorizont von 15 Jahren oder mehr. Dabei wäre eine möglichst genaue Eingrenzung der Verfügbarkeit von Quantencomputern für den operativen Einsatz entscheidend. Denn ab dem Zeitpunkt, zu dem Quantencomputer der reinen Entwicklung und Forschung entwachsen sind, ist die Mehrzahl der bisherigen technischen Bemühungen für den Datenschutz obsolet. Und das ist nur die halbe Wahrheit, denn der Datenschutz-Supergau passiert vermutlich bereits heute.

Verschlüsselte Daten gestohlen? Egal! Oder doch nicht?

Seit einiger Zeit gilt das Credo, dass Unternehmen und Organisationen ihre Daten sowohl at-rest als auch in-transit ordentlich verschlüsseln müssen, damit ein potenzieller Diebstahl oder ein Abfangen durch Cyberkriminelle oder staatlich gesteuerte Spionage ins Leere läuft. Aus der heutigen Perspektive betrachtet ist das zutreffend. Denn aktuell können die Cyberkriminellen verschlüsselte Daten nicht lesen, was diese gegenwärtig nutzlos macht.

Die bösartigen Akteure wissen allerdings sehr genau, welche Art von Daten interessant sind und auch, welche Brisanz in diesen steckt. Und da viele Daten auch in einigen Jahren noch relevant für kriminelle Handlungen sind, liegt es nahe, dass die Daten erst einmal geparkt werden und auf den richtigen Zeitpunkt gewartet wird – das Harvest-now-decrypt-later-Szenario.

Insbesondere asymmetrisch verschlüsselte Daten sind wie Rohdiamanten. Man bekommt sie einfach und günstig. Wer zu einem späteren Zeitpunkt die passenden Entschlüsselungswerkzeuge hat, kann sie Jahre nach dem eigentlichen Diebstahl, quasi im geschliffenen Zustand, für ein Zigfaches der ursprünglichen Investition nutzen. Ergo wird es kaum Cyberkriminelle geben, die erbeutete verschlüsselte Daten wegwerfen. Vielmehr ist anzunehmen, dass diese ihre Beute massenhaft archivieren, um die asymmetrische Verschlüsselung bei verfügbarer Quantum-Computing-Leistung zu entschlüsseln und zu Geld zu machen – ähnlich einer Wertanlage oder Altersvorsorge.

Klare Zielvorgabe

Laut Gartner könnten die bisher als sicher geltenden asymmetrischen Verschlüsselungsmethoden wie RSA oder ECC durch Quantum Computing ab dem Jahr 2029 entschlüsselt werden. Das sind gerade einmal vier Jahre, ein Wimpernschlag in der IT-Technologie und gleichzeitig eine Zeitspanne, in der gerade in der IT sehr viel Potenzial für Neuerungen steckt. Organisationen, wie das BSI, die EU-Kommission und das NIST (National Institute of Standards and Technology, USA) fordern daher dazu auf, den künftigen kriminellen Entschlüsselungsmöglichkeiten vorzubeugen und bereits heute quantensichere Verschlüsselungsverfahren einzusetzen.

Die Grundlage dafür liefert die im Juni 2025 veröffentlichte Roadmap der NIS-Kooperationsgruppe, die auf eine koordinierte Post Quantum Kryptographie (PQC)-Transition in allen Mitgliedstaaten mit klar definierten Meilensteinen abzielt:

- Bis 31.12.2026:
  - Entwicklung von nationalen PQC-Roadmaps
  - Einbindung von Stakeholdern und Durchführen von Risikoanalysen
  - Start der Pilotprojekte für High- & Medium-Risk-Anwendungen
- Bis 31.12.2030:
  - Abschließen der PQC-Umstellung für High-Risk-Anwendungsfälle
  - Finalisierung der Umsetzungspläne für Medium-Risk-Szenarien
- Bis 31.12.2035:
  - Abschluss der PQC-Transition für möglichst viele Medium- und Low-Risk-Systeme

Was hält heute schon morgen Stand?

Eine Verschlüsselung von Daten ist nur dann wirksam, wenn die Verschlüsselung für den Weg der Übertragung und in der Cloud funktioniert, ohne Funktionen in den angestammten Anwendungen einzuschränken. Die Lösung für dieses Problem liegt in einem Verschlüsselungs-Gateway wie eperi sEcure, das die relevanten Daten mit zukunftssicheren Algorithmen verschlüsselt und trotz einer ununterbrochenen Verschlüsselung die Ver- und Bearbeitung der Daten in ihren Anwendungen zulässt.

Durch das neue Erweiterungsmodul eperi QuantumEdge lassen sich die Vorbereitungen für die Post-Quantum-Ära maßgeblich abkürzen. Unternehmen profitieren von einer sicheren, schrittweisen Migration hin zu einer hybriden oder vollständig postquantenresistenter Transportverschlüsselung. Damit erhalten Unternehmen nicht nur ein Werkzeug für eine sicher Post-Quantum-Verschlüsselung, sondern gleichzeitig auch ein Migrations-Tool, mit dem bisherige verschlüsselte Datenbestände auf das quantensichere Schutzniveau mit einem hohen Grad an Automatisierung angehoben werden können. Mit Hilfe eines Dashboards haben Unternehmen zudem über ihren gesamten Datenverkehr hinweg Klarheit, welche Verschlüsselungsalgorithmen von eingesetzten Anwendungen, Diensten und Endpunkten genutzt werden – unabhängig davon, ob sie bekannt oder Teil der Schatten-IT sind. Durch die Analyse bestehender Verbindungen erkennt die Lösung PQC-kompatible Systeme und ermöglicht hybride TLS-Verbindungen (klassisch + postquantenresistent).

Auf diese Weise wird die PQC-Transition transparent, steuerbar und ohne Eingriff in bestehende Anwendungen umsetzbar – ideal zur Einhaltung aktueller und kommender Compliance-Vorgaben. Die zusätzliche Reporting-Funktion dient auch als Nachweis für Stakeholder wie Versicherungen, Banken oder Kunden und Partner.

PQC-Transition jetzt

Das Problem einer bösartigen Datenentschlüsselung durch Quantencomputer ist keine Sache der Zukunft. Vielmehr werden heute Daten erzeugt und noch klassisch verschlüsselt, die bereits in absehbarer Zukunft zum Problem werden können, wenn sie nicht auf quantensichere Verschlüsselungstechnologien migriert werden. Der Übergang zu quantensicherer Kryptografie ist keine Option, sondern eine Notwendigkeit, mit der am besten heute begonnen werden sollte.

Über die Eperi GmbH:

Wir bei eperi® sind der festen Überzeugung, dass Datenschutz ein grundlegendes Menschenrecht ist. Unser Ziel ist es, dass Menschen und Unternehmen zu jeder Zeit die Kontrolle über ihre Daten behalten. Ohne Kompromisse und mit der besten Technologie. Mit dem Fokus auf die Sicherheit unserer Kunden haben wir eine Lösung geschaffen, die für den Benutzer unsichtbar ist und gleichzeitig die höchsten Sicherheitsstandards erfüllt.
Mit der eperi® Lösung profitieren unsere Kunden von allen Vorteilen der Cloud-Nutzung, wie beispielsweise einer effizienten unternehmensweiten Kollaboration, und bleiben dabei rechtssicher gemäß weltweiten Datenschutzgesetzen. Wir besitzen mehrere internationale Patente für unsere innovative Multi-Cloud-Technologie, die einen konkurrenzlosen Datenschutz für SaaS Anwendungen, individuelle Applikationen und Dateien bietet. Unsere Kunden behalten die alleinige Kontrolle über alle sensiblen Daten, da keine unverschlüsselten Daten in die Cloud gesendet werden.
Wir ermöglichen die Cloud – einfach, sicher, individuell, DSGVO-konform.

Pressekontakt eperi

Eperi GmbH
Sabine Jost
Werner-von-Siemens-Str. 2
64319 Pfungstadt
Tel: +49 (0)6157 95639 16
E-Mail: sabine.jost@eperi.com
Web: www.eperi.com

Pressekontakt Agentur

TC Communications
Thilo Christ
Tel: +49 171 6220610
Alexandra Schmidt
Tel: +49 170 3871064
E-Mail: eperi@tc-communications.de