ZfPC

Zeitschrift für Product Compliance
2/2026 | Seiten 57–116

Post-Quanten-Kryptografie als gesetzliche Produktanforderung

Editorial

Resilienzanforderungen gewinnen im Produktrecht zunehmend an Bedeutung. Digitale Produkte müssen nicht nur heute sicher sein, sondern auch gegenüber absehbaren zukünftigen Risiken widerstandsfähig bleiben. Eine dieser Risiken ist der Einsatz leistungsfähiger Quantencomputer, die etablierte kryptographische Verfahren fundamental angreifen können.

Quantencomputer unterscheiden sich grundlegend von klassischen Rechnern. Sie arbeiten mit Quantenbits, sogenannten Qubits. Diese sind im Gegensatz zu klassischen Bits nicht entweder 0 oder 1, sondern befinden sich in Superposition beider Zustände. Durch diese Parallelisierung lassen sich bestimmte – ausdrücklich nicht alle – Rechenprobleme erheblich schneller lösen als mit klassischen Computern. Viele heute eingesetzte kryptographische Verfahren basieren darauf, dass bestimmte mathematische Aufgaben – etwa die Faktorisierung großer Zahlen – für klassische Computer in kurzer Zeit praktisch unlösbar sind. Genau diese Annahme wird durch Quantencomputer infrage gestellt.

Der zentrale Angriffspunkt ist der sogenannte Shor-Algorithmus. Er ermöglicht es, große Zahlen effizient in zwei Primzahlfaktoren zu zerlegen. Damit lassen sich die mathematischen Grundlagen vieler asymmetrischer Verschlüsselungsverfahren (nahezu) exponentiell schneller brechen. Diese asymmetrischen Verschlüsselungsverfahren sichern heute zentrale Funktionen moderner Produkte: Authentifizierung, sichere Kommunikation, Software-Updates und Integritätsnachweise. Ein späteres kryptographisches Versagen kann daher unmittelbare Sicherheits- und Haftungsfolgen haben.

Entscheidend für die Compliance-Bewertung ist: Die Verwundbarkeit dieser Verfahren ist seit Jahrzehnten bekannt. Das genaue zeitliche Erscheinen leistungsfähiger Quantencomputer ist zeitlich ungewiss, Fortschritte sind jedoch gegenwärtig. Für langlebige Produkte reicht es daher nicht aus, sich auf die heutigen möglichen Angriffe zu berufen.

Ein wesentlicher Wendepunkt wurde 2024 erreicht: Das US-amerikanische National Institute of Standards and Technology (NIST) hat nach jahrelanger Arbeit die drei ersten Post-Quanten-Kryptografie-Standards veröffentlicht. Diese Verfahren gelten als resistent gegenüber Quantencomputern, auch gegenüber zukünftig noch deutlich leistungsfähigeren Quantencomputern. Damit ist Post-Quanten-Kryptografie kein Forschungsprojekt mehr, sondern Realität. Für Hersteller ist dies nicht nur ein technisches, sondern vor allem ein haftungs- und compliance-relevantes Thema. Maßgeblich ist u.a. der im Produkthaftungsrecht verankerte Maßstab des Stands von Wissenschaft und Technik. Er bestimmt, welche Sicherheitsmaßnahmen bei Entwicklung und Inverkehrbringen eines Produkts als zumutbar gelten. Spätestens seit der Standardisierung der Post-Quanten-Kryptografie im Jahr 2024 ist der Einsatz von Quantencomputern zum effizienten Knacken von traditionellen Verschlüsselungsverfahren kein theoretisches Zukunftsszenario mehr, sondern ein konkret adressierbares Risiko.

Die Migration von Betriebssystemen, Kryptobibliotheken und Kommunikationsprotokollen ist komplex. Sie betrifft nicht nur einzelne Algorithmen, sondern gesamte Sicherheitsarchitekturen: Schlüsselmanagement, Zertifikatsinfrastrukturen, Update-Mechanismen und teilweise auch Hardware-Ressourcen. Ein kurzfristiger Wechsel ist in vielen Produktklassen unrealistisch.

Für die Produkthaftung ist zudem entscheidend, dass Sicherheitsmaßnahmen ex ante bewertet werden. Wer heute Produkte entwickelt, die über Jahre oder Jahrzehnte im Einsatz sind, muss absehbare technologische Entwicklungen berücksichtigen. Neben der Produkthaftung erhöhen auch neue europäische Regulierungen den Handlungsdruck. Die NIS2-Richtlinie ist verabschiedet und verpflichtet betroffene Unternehmen zur Umsetzung technischer und organisatorischer Maßnahmen nach dem Stand von Wissenschaft und Technik, was sich auch auf kryptographische Verfahren erstreckt. Auch der neue Cyber Resilience Act zielt auf sichere Produkte über den gesamten Lebenszyklus hinweg. Kryptographische Resilienz wird damit zu einem Kernelement moderner Product Compliance.

Prof. Dr. Patrick Glauner, TH Deggendorf