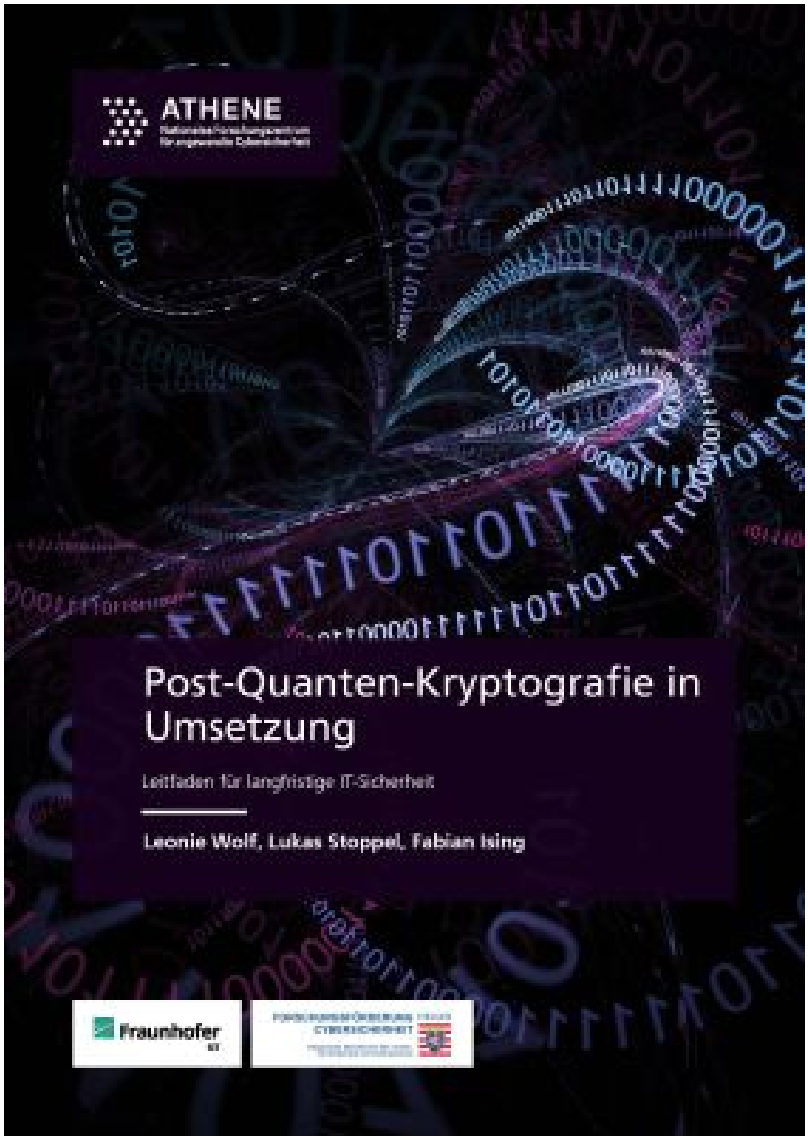
Quantensicher in die Zukunft

28.05.2026, 10:10 | IT, New Media & Software

Pressemitteilung von: *idw - Informationsdienst Wissenschaft*



Das Fraunhofer-Institut für Sichere Informationstechnologie SIT hat gemeinsam mit dem Hessischen Ministerium des Innern, für Sicherheit und Heimatschutz einen praxisorientierten Leitfaden zur Post-Quanten-Kryptografie (PQC) veröffentlicht. Der Leitfaden unterstützt Kommunen, Landesbehörden und andere Organisationen beim Übergang zu quantensicheren IT-Systemen und berücksichtigt behördentypische Beschaffungsregeln sowie Besonderheiten kommunaler Softwarelösungen. Der Leitfaden kann hier kostenfrei heruntergeladen werden: https://www.athene-center.de/angebote/downloads#c16100.

Weltweit arbeiten IT-Forschende an der Entwicklung von Quantencomputern. Mit deren Hilfe lassen sich in Zukunft aber nicht nur schneller neue Medikamente und Materialien entwickeln, sondern auch viele aktuelle Verschlüsselungsverfahren brechen. Damit wird unsere gesamte Online-Kommunikation unsicher, wie Banking-Verfahren oder E-Mail-Verkehr. Angreifer speichern deshalb bereits heute verschlüsselte Daten, um sie zu entschlüsseln,

sobald die Technologie dazu bereit ist. Wer also sensible Informationen langfristig schützen will, muss schon jetzt handeln.

Hessens Innenminister Roman Poseck erklärt: „Die Bedrohung durch Quantencomputer ist real und sie erfordert jetzt unser Handeln. Mit dem neuen Leitfaden ‚Post-Quanten-Kryptografie in Umsetzung' geben wir Kommunen und Behörden in Hessen ein praktisches Werkzeug an die Hand, um ihre IT-Systeme zukunftssicher zu machen. Gemeinsam mit dem Fraunhofer SIT haben wir eine Schritt-für-Schritt-Anleitung erarbeitet, die nicht nur technisch fundiert, sondern auch behördenspezifisch umsetzbar ist. So schützen wir sensible Daten langfristig und stärken die digitale Resilienz unseres Landes."

Hier setzt der neue Leitfaden „Post-Quanten-Kryptografie in Umsetzung" an. Er richtet sich an Kommunen, Landesbehörden und weitere Organisationen, die ihre IT-Infrastruktur auf Post-Quanten-Kryptografie (PQC) umstellen möchten – also auf Verschlüsselungsverfahren, die auch Entschlüsselungsversuchen leistungsfähiger Quantencomputer standhalten. Der Leitfaden ist auch für Entscheidungsträgerinnen und Entscheidungsträger ohne technischen Hintergrund verständlich aufbereitet. Denn die Umstellung ist kein reines IT-Projekt. Viele unterschiedliche Bereiche müssen ineinandergreifen. Sie betrifft bestehende Systeme ebenso wie künftige Beschaffungen und muss deshalb frühzeitig geplant werden, da IT-Systeme oft viele Jahre laufen.

Quantensicher in vier Schritten

Die Europäische Union hat im Juni 2025 einen Umsetzungsfahrplan für den Übergang zur Post-Quanten-Kryptografie in den Mitgliedstaaten veröffentlicht. Der neue Leitfaden schließt an diesen EU-Fahrplan an und zeigt konkret und praxisnah, wie die Umstellung auf kommunaler Ebene gelingt. Der Leitfaden empfiehlt vier zentrale Aktivitäten für die Umsetzung:

Zunächst sollten alle eingesetzten IT-Systeme und kryptografischen Verfahren vollständig erfasst werden. Anhand dieser Bestandsaufnahme lassen sich die Risiken für IT-Systeme bewerten und priorisieren. Als nächster Schritt können auf vielen Standardsystemen bereits heute mit überschaubarem Aufwand erste Migrationsschritte umgesetzt werden. Und schließlich sollten neue IT-Beschaffungen von Anfang an auf Quantensicherheit ausgelegt sein.

Behörden und Kommunen können die Kryptografie allerdings nicht einfach so umstellen. Zum einen nutzen sie oft Spezialsoftware, für die mitunter noch keine zukunftssicheren Alternativen existieren. Zum anderen stellen auch behördliche Vergabeverfahren in manchen Fällen eine Herausforderung dar. Für Letzteres definiert der Leitfaden Vergabekriterien in einem Stufenmodell, die Kommunen bei der Beschaffung anwenden können. Für das Problem der Spezialsoftware beschreibt der Leitfaden als pragmatische Übergangslösung die Übertragung über einen quantensicheren Tunnel.

Erstellt wurde der Leitfaden vom Fraunhofer SIT in Darmstadt in enger Zusammenarbeit mit dem Hessischen Ministerium des Innern, für Sicherheit und Heimatschutz sowie mit Vertreterinnen und Vertretern hessischer Kommunen.

Den vollständigen Leitfaden „Post-Quanten-Kryptografie in Umsetzung" gibt es kostenlos zum Download unter https://www.athene-center.de/angebote/downloads#c16100.

wissenschaftliche Ansprechpartner:
Leonie Wolf, Fabian Ising

Originalpublikation:
https://www.athene-center.de/angebote/downloads#c16100.

Fraunhofer-Institut für Sichere Informationstechnologie SIT

AnnaSpiegel (Mitarbeiter in der Presse- und Öffentlichkeitsarbeit)

presse@sit.fraunhofer.de

News-ID: 1313064 • Views: 138 (Stand: 04.08.2026)

Link zur Pressemitteilung:
https://www.openpr.de/news/1313064/Quantensicher-in-die-Zukunft-idw.html