

Ist die aktuelle Verschlüsselung noch eine wirksame Schutzmaßnahme?

Bei den technischen Maßnahmen zum Schutz von sensiblen Daten und Systemen zählt die Verschlüsselung zu den wichtigsten Sicherheitsmechanismen. Doch wie wirksam ist diese Schutzmaßnahme langfristig, wenn leistungsfähige Quantencomputer künftig in der Lage sein könnten, heute eingesetzte Verschlüsselungsverfahren zu brechen? Der nachfolgende Beitrag beleuchtet die damit verbundenen Risiken und zeigt auf, weshalb Organisationen sich bereits heute mit dem Thema Post-Quanten-Kryptographie auseinandersetzen sollten.



Vermeintlich sichere Verschlüsselungen könnten in der Zukunft aufbrechen.

Das Thema Daten- und Systemsicherheit ist heute auf allen Hierarchieebenen präsent. Einerseits nimmt die Bedrohungslage im Cyberraum stetig zu, andererseits steigen die gesetzlichen und regulatorischen Anforderungen an den Schutz von Daten kontinuierlich. Einen wesentlichen Impuls setzte unter anderem die Datenschutz-Grundverordnung (DSGVO), die seit Mai 2018 in der Europäischen Union gilt. Sie verlangt zum Schutz personenbezogener Daten angemessene technische und organisatorische Maßnahmen. Auch das revidierte Schweizer Datenschutzgesetz, das im September 2023 in Kraft trat, verfolgt diesen risikobasierten Ansatz.

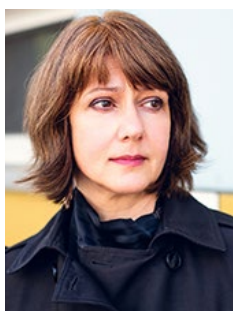
Zu den klassischen technischen Schutzmaßnahmen gehört die Verschlüsselung. Dabei werden Daten so umgewandelt, dass sie nur mit einem passenden kryptographischen Schlüssel gelesen werden können. Die Verschlüsselung trägt wesentlich zur Sicherstellung der Vertraulichkeit und Integrität von Informationen bei und schützt Personendaten vor unbefugtem Zugriff. Verschlüsselungsverfahren spielen auch eine wesentliche Rolle beim Nachweis der Integrität des Autors oder Eigentümers von Daten und Systemen.

Genau diese Schutzwirkung wird jedoch durch ein Phänomen infrage gestellt, das unter dem Be-

griff „Harvest Now, Decrypt Later“ (HNDL) oder „Jetzt ernten, später entschlüsseln“ bekannt ist. Ein weiteres Bedrohungsszenario ist „Trust Now, Forge Later“ (TNFL), was „Jetzt vertrauen, später manipulieren“ bedeutet. Dabei werden verschlüs-



Anja Schmitz ist Juristin und Partner/Senior Consultant bei der Projektas GmbH, mit Sitz in Zug/Schweiz. Sie berät im Bereich Corporate Governance, Compliance, Datenschutz & Projektmanagement, ein Schwerpunkt ihrer Arbeit liegt in der Umsetzung von Compliance-Projekten, dem juristischen Projektmanagement und der Management-Beratung.



Xenia Bogomolec ist Cyber-sicherheitsexpertin und Gründerin der Quant-X Security & Coding GmbH. Sie berät kritische Infrastruktur-Provider mit hohen regulatorischen Anforderungen in Cybersicherheit und leitet Technologietransfer-Projekte in Post-Quanten-Sicherheit, Quantenkryptographie und KI im Cybersicherheitskontext.

selte und digital signierte Daten bereits heute abgefangen oder entwendet und für eine spätere Entschlüsselung oder Manipulation gespeichert. Die Angreifer spekulieren darauf, dass zukünftige Quantencomputer die heute eingesetzten kryptographischen Verfahren brechen können. Besonders problematisch ist dies für Daten mit langen Aufbewahrungs- oder Vertraulichkeitsfristen, wie beispielsweise Gesundheits-, Kunden- oder Personaldaten. Dies betrifft auch Daten, die bereits vor vielen Jahren gesammelt wurden und noch einige Jahre sensibel bleiben werden.

Damit entsteht eine neue Form der Cyberbedrohung: Selbst, wenn verschlüsselte Daten heute nicht lesbar sind, könnte ihre Vertraulichkeit und Integrität in einigen Jahren gefährdet sein. Organisationen stehen deshalb vor der Herausforderung, ihre kryptographischen Verfahren rechtzeitig auf quantenresistente Alternativen umzustellen, bevor leistungsfähige Quantencomputer verfügbar werden.

Post-quanten-sichere Kryptografie (PQC) wird schon seit den frühen 2000er Jahren erforscht. Das global führende National Institute of Standards and Technology (NIST) des U.S. Department of Commerce hat seit 2017 die ersten Kandidaten für Schlüsselaustausch und Digitale Signaturen evaluiert und im August 2024 drei ausgewählte Standards veröffentlicht. Die Standardisierung von zwei weiteren PQC-Verfahren läuft. Die ISO-Organisation in Genf und das European Telecommunications Standards Institute (ETSI) haben danach zusätzliche PQC-Standards veröffentlicht. Parallel haben verschiedene nationale und internationale Behörden Migrationsstrategien veröffentlicht. Die EU strebt an, kritische Systeme bis Ende 2030 auf PQC zu migrieren. Systeme mit mittlerem und geringem Risiko sollen bis Ende 2035 migriert werden. Das NIST verfolgt einen technischen Ansatz, nach dem bis 2030 alle Verfahren mit einer Sicherheit von 112 oder weniger Bit als veraltet gelten werden. Dabei steht die Bit-Sicherheit nicht für die Schlüssellänge, sondern für die Komplexität des effizientesten Angriffs auf das Verfahren. Das weit verbreitete Verfahren RSA-2048 fällt zum Beispiel unter diese Kategorie. Ab 2035 sind dann alle Verfahren nicht mehr compliant mit den NIST-Anforderungen, die nicht als post-quanten-sicher gelten. Angesichts der Komplexität unserer digitalen Infrastrukturen sind das sportliche, aber trotzdem notwendige Zeitpläne.

18 EU-Mitgliedsstaaten haben schon im November 2024 in Securing Tomorrow, Today: Transitioning to Post-Quantum Cryptography zur dringenden Priorisierung der PQC-Migrationen aufgerufen. Aufgrund neuer Entwicklungen im Quantum Computing hat z. B. Google es sich zum Ziel gesetzt, bis 2029 post-quanten-sichere Dienste anzubieten. Es wird empfohlen, mit sogenannten hybriden Verfahren zu beginnen. Das sind Verfahren, die PQC und klassische Kryptografie kombinieren.

Anja Schmitz und Xenia Bogomolec