

Interview

Souveränität heißt Kontrolle

[21.10.2026] Digitale Souveränität, sichere Verschlüsselung und die Bedrohung durch Quantencomputer: Die öffentliche Verwaltung muss sich auf neue Herausforderungen einstellen. Warum die Kontrolle über kryptografische Schlüssel entscheidend ist, erläutert Rasmus Lemke von Thales im Interview mit move – moderne verwaltung auf der Smart Country Convention 2026.

Herr Lemke, welche Bedeutung hat die Smart Country Convention für [Thales](#)? Was erwarten Sie von der Messe?

Die Smart Country Convention gibt dem Markt wichtige Impulse. Man merkt, wie viel Energie in der Digitalisierung der öffentlichen Verwaltung steckt. Die Messe ist sehr gut besucht, das Publikum ist interessiert und die Gespräche sind ausgesprochen zielgerichtet. Das unterscheidet sie von vielen allgemeinen IT-Messen. Gleichzeitig ist das Themenspektrum enorm breit – von der Parkplatzverwaltung über digitale Identitäten bis hin zur IT-Sicherheit. Für uns ist die Veranstaltung vor allem ein Gradmesser: Welche Themen beschäftigen die öffentliche Hand? Welche Fragen stellen sich die Verantwortlichen und an welchen Projekten arbeiten sie? Es geht uns weniger darum, möglichst viele neue Kontakte zu generieren, sondern darum, die Entwicklungen im Markt zu verstehen. Gerade weil Projekte in der öffentlichen Verwaltung häufig längere Vorlaufzeiten haben, ist dieser Austausch wichtig.

Mit welchen Lösungen präsentiert sich Thales auf der Smart Country Convention?

Wir sind gemeinsam mit unserem Partner [SIGN8](#) vertreten, der sich unter anderem mit der europäischen digitalen Identitätswallet und qualifizierten elektronischen Signaturen beschäftigt. Thales liefert dafür mit Hardware Security Modules, kurz HSM, eine wesentliche Sicherheitskomponente. Diese Module dienen als besonders geschützte Speicher für kryptografische Schlüssel. Man kann sie sich als digitalen Tresor vorstellen, der die Grundlage für sichere Authentifizierungs- und Signaturprozesse bildet.

Welche besonderen Anforderungen stellen Bundes-, Landes- und Kommunalbehörden an solche Sicherheitslösungen?

Zunächst sind die entsprechenden Zertifizierungen entscheidend. Ohne bestimmte Sicherheitsnachweise braucht man in diesem Markt gar nicht erst anzutreten. Gerade wenn es um Verschlusssachen oder andere hochkritische Informationen geht, müssen sowohl die Verschlüsselung als auch die Aufbewahrung der Schlüssel höchsten Anforderungen genügen. Wir haben für unsere Luna-7-HSMs inzwischen auch eine entsprechende BSI-Zulassung erreicht. Das hat eine deutlich steigende Nachfrage ausgelöst. Wir hatten mit einem wachsenden Bedarf gerechnet, aber jetzt sehen wir sehr konkret, wie wichtig solche zertifizierten Lösungen für öffentliche Auftraggeber sind.

Was genau leistet ein Hardware Security Module und warum ist es für die Datensicherheit so wichtig?

Ein HSM ist vereinfacht gesagt eine Hardwarebox, die kryptografische Schlüssel erzeugt und sicher speichert. Das Entscheidende ist, dass die Schlüssel die geschützte Hardware nicht verlassen. Sie lassen sich also nicht einfach kopieren. Man kann sich das wie einen Hauptschlüssel für eine große Schließanlage vorstellen. Wenn dieser Hauptschlüssel in falsche Hände gerät, ist das gesamte System

gefährdet. Genau das soll ein HSM verhindern. Die Geräte sind hochspezialisiert. Sie können vergleichsweise wenige Dinge, aber das, was sie tun – Schlüssel erzeugen und schützen –, beherrschen sie extrem sicher. Hinzu kommt das Schlüsselmanagement. Dabei geht es darum, aus einem Hauptschlüssel weitere Schlüssel abzuleiten, diese zu verwalten und kontrolliert bereitzustellen. Solche Lösungen werden längst nicht mehr nur in eigenen Rechenzentren eingesetzt, sondern zunehmend auch in Cloud-Umgebungen.

„Wir müssen stärker auf Resilienz setzen.“

Digitale Souveränität ist eines der zentralen Themen der Messe. Was bedeutet dieser Begriff aus Ihrer Sicht, insbesondere beim Einsatz von Cloud-Diensten?

Für mich ist eine Unterscheidung ganz entscheidend: Souveränität bedeutet nicht Autarkie, sondern Kontrolle. Das wird häufig verwechselt. Digitale Souveränität heißt nicht, dass ich alles selbst entwickeln und betreiben muss. Ich muss aber jederzeit die Kontrolle über meine Daten und die dafür notwendigen Sicherheitsschlüssel behalten. Eine Behörde kann beispielsweise durchaus einen amerikanischen Cloud-Anbieter nutzen. Entscheidend ist, dass dieser Anbieter nicht gleichzeitig über den Hauptschlüssel verfügt, mit dem sich die gespeicherten Daten entschlüsseln lassen. Ich muss selbst bestimmen können, wer wann und unter welchen Bedingungen auf meine Informationen zugreifen darf. Natürlich ist es wünschenswert, europäische oder deutsche Anbieter einzusetzen. Aber letztlich kommt es darauf an, die Kontrolle technisch und organisatorisch sicherzustellen.

Welche Rolle spielt dabei die europäische Datenschutzgesetzgebung?

Wir haben in Europa und insbesondere in Deutschland ein hohes Datenschutzniveau. Das hilft uns allerdings wenig, wenn wir unsere Daten freiwillig in Umgebungen übertragen, in denen andere rechtliche Rahmenbedingungen gelten. Deshalb brauchen wir eine zusätzliche Sicherheitsebene. Im Zweifelsfall ist das eine konsequente Verschlüsselung. Daten können trotz aller Schutzmaßnahmen abfließen. Wenn sie aber wirksam verschlüsselt sind und der Schlüssel unter unserer Kontrolle bleibt, kann ein Angreifer mit ihnen nichts anfangen. Das ist aus meiner Sicht ein wesentlicher Baustein digitaler Souveränität.

Mit dem Quantencomputing zeichnet sich eine neue Bedrohung für bestehende Verschlüsselungsverfahren ab. Wie akut ist diese Gefahr?

Die heute eingesetzten Verschlüsselungsverfahren sind grundsätzlich sicher, weil es mit klassischen Computern extrem lange dauern würde, sie zu brechen – bei richtigem Einsatz unter Umständen viele Tausend Jahre. Leistungsfähige Quantencomputer könnten das grundlegend verändern. Es gibt Prognosen, nach denen entsprechende Systeme gegen Ende dieses Jahrzehnts oder Anfang der 2030er-Jahre eine ernsthafte Bedrohung darstellen könnten. Das bedeutet allerdings nicht, dass Quantencomputer sämtliche Verschlüsselungen auf einen Schlag knacken können. Betroffen sind bestimmte kryptografische Verfahren. Wir wissen bereits, wie wir darauf reagieren können. Es gibt sogenannte postquantensichere Algorithmen, die auf anderen mathematischen Grundlagen beruhen und international standardisiert werden. Auch Thales arbeitet an deren Entwicklung und Umsetzung mit.

Warum sollten sich Behörden bereits heute mit dieser Entwicklung beschäftigen, wenn leistungsfähige Quantencomputer noch gar nicht verfügbar sind?

Weil die Bedrohung in gewisser Weise bereits existiert. Wir sprechen vom Prinzip „Harvest now, decrypt later“. Angreifer können heute verschlüsselte Daten abgreifen und speichern, um sie später mit

leistungsfähigeren Quantencomputern zu entschlüsseln. Das ist vor allem bei hochsensiblen Informationen relevant, die über viele Jahre vertraulich bleiben müssen. Deshalb reicht es nicht, erst dann zu reagieren, wenn entsprechende Quantencomputer verfügbar sind. Behörden müssen sich schon jetzt darauf vorbereiten.

Was sollten Kommunen und andere öffentliche Einrichtungen konkret tun, um ihre Daten langfristig zu schützen?

Die größte Herausforderung ist zunächst gar nicht die Technologie, sondern die Organisation. Eine Behörde muss sich zuerst einen Überblick verschaffen: Welche Datenbestände gibt es? Welche Verschlüsselungsverfahren werden eingesetzt? Welche Informationen müssen auch in zehn oder zwanzig Jahren noch geschützt sein? Und welche Systeme müssen dafür umgestellt werden? Gerade in der öffentlichen Verwaltung ist das nicht einfach, weil dort häufig historisch gewachsene IT-Landschaften existieren. Teilweise sind noch Systeme im Einsatz, die in der Privatwirtschaft längst abgelöst wurden. Deshalb braucht es zunächst eine Bestandsaufnahme und anschließend eine konkrete Migrationsstrategie. Das lässt sich nicht innerhalb weniger Monate erledigen. Hinzu kommt, dass das notwendige Spezialwissen weder in Unternehmen noch in Behörden flächendeckend vorhanden ist. Ich rechne damit, dass die entsprechenden Fachleute künftig sehr gefragt sein werden. Erst wenn diese organisatorischen Fragen geklärt sind, folgt die eigentliche technische Umsetzung.

Welche Unterstützung erhalten Behörden bei der Vorbereitung auf die Postquanten-Kryptografie?

Das Bundesamt für Sicherheit in der Informationstechnik beschäftigt sich intensiv mit diesem Thema und veröffentlicht entsprechende Empfehlungen. Darin wird beschrieben, welche Schritte sinnvoll sind und in welchen Zeiträumen bestimmte Maßnahmen umgesetzt werden sollten. Es gibt also durchaus Orientierung und eine Roadmap. Die Verantwortung, die eigenen Systeme zu analysieren und die notwendigen Veränderungen einzuleiten, bleibt aber bei den jeweiligen Organisationen.

„Es reicht nicht, erst dann zu reagieren, wenn Quantencomputer verfügbar sind.“

Was unterscheidet postquantensichere Verschlüsselungsverfahren von den heute gebräuchlichen Algorithmen?

Vereinfacht gesagt beruhen sie auf einer anderen Mathematik. Klassische Computer arbeiten mit Bits, die entweder den Zustand null oder eins annehmen. Quantencomputer nutzen dagegen Qubits, die sich quantenmechanische Eigenschaften zunutze machen. Dadurch können bestimmte mathematische Probleme, auf denen heutige kryptografische Verfahren beruhen, erheblich schneller gelöst werden. Postquanten-Algorithmen setzen deshalb auf andere mathematische Verfahren, für die solche effizienten Quantenangriffe bislang nicht bekannt sind. Diese Algorithmen werden intensiv untersucht und standardisiert. Es geht also nicht um eine proprietäre Technologie einzelner Hersteller, sondern um international abgestimmte Sicherheitsstandards.

Thales beteiligt sich unter anderem an der Entwicklung des Postquanten-Algorithmus Falcon. Welche Bedeutung hat diese Arbeit für Ihre Sicherheitslösungen?

Falcon ist einer von mehreren Algorithmen, die im Rahmen der internationalen Standardisierung betrachtet werden. Thales beteiligt sich an dieser Entwicklung. Das hilft uns auch dabei, unsere Hardware frühzeitig auf die neuen Anforderungen auszurichten. Denn grundsätzlich können unsere heutigen Geräte bereits Postquanten-Algorithmen verarbeiten. Sie wurden allerdings ursprünglich nicht für diese Verfahren

optimiert. Deshalb wird die nächste Generation unserer Hardware Security Modules speziell auf die neuen Algorithmen ausgelegt sein und eine deutlich höhere Verarbeitungsgeschwindigkeit erreichen. Neben der organisatorischen Vorbereitung wird also irgendwann auch ein technologischer Wechsel erforderlich sein, um die notwendige Leistungsfähigkeit sicherzustellen. Die Entwicklung bleibt dabei dynamisch. Wie in der klassischen Kryptografie werden auch künftig neue Algorithmen hinzukommen oder bestehende Verfahren weiterentwickelt werden.

Wie zuversichtlich sind Sie, dass die Verschlüsselung auch im Zeitalter leistungsfähiger Quantencomputer zuverlässig funktionieren wird?

Ich bin sehr zuversichtlich, dass wir diese Herausforderung bewältigen können. Wir kennen die grundlegenden Probleme und verfügen bereits über geeignete Lösungsansätze. Außerdem darf man nicht vergessen, dass leistungsfähige Quantencomputer auf absehbare Zeit keine Geräte sein werden, die jeder zu Hause stehen hat. Solche Systeme werden zunächst vermutlich vor allem Staaten, sehr großen Unternehmen und spezialisierten Organisationen zur Verfügung stehen. Der Kreis potenzieller Angreifer ist damit zunächst begrenzt. Entscheidend ist, dass wir die vorhandene Zeit nutzen, um unsere Systeme rechtzeitig umzustellen. Ich bin überzeugt, dass uns das gelingen kann.

Neben dem Quantencomputing verändert auch Künstliche Intelligenz die IT-Sicherheit. Ist KI dabei eher Chance oder Risiko?

Beides. KI kann uns helfen, Angriffe schneller zu erkennen und Sicherheitsmaßnahmen zu verbessern. Gleichzeitig steht sie natürlich auch den Angreifern zur Verfügung. Wir sehen schon heute immer ausgefeiltere Cyber-Angriffe, die mithilfe von KI entwickelt oder unterstützt werden. Daraus ergibt sich eine grundlegende Erkenntnis: Eine hundertprozentige Sicherheit wird es nicht geben. Wir müssen davon ausgehen, dass Systeme irgendwann erfolgreich angegriffen werden. Deshalb reicht es nicht mehr aus, ausschließlich darauf zu setzen, einen Angriff zu verhindern.

„Das Entscheidende ist, dass die Schlüssel die geschützte Hardware nicht verlassen.“

Was bedeutet das für die Sicherheitsstrategie der öffentlichen Verwaltung?

Wir müssen stärker auf Resilienz setzen. Die entscheidenden Fragen lauten dann: Welche Auswirkungen hat ein erfolgreicher Angriff? Wie können wir den Schaden begrenzen? Wie schnell sind unsere Systeme wieder einsatzfähig? Und wie stellen wir sicher, dass wichtige Verwaltungsleistungen weiter erbracht werden können? Das betrifft insbesondere die Geschäftskontinuität und die Wiederherstellungsfähigkeit. Gleichzeitig müssen wir unsere Sicherheitskonzepte stärker an den Daten selbst ausrichten. Früher stand vor allem der Schutz des Netzwerks im Mittelpunkt, also die Absicherung des Perimeters. Heute brauchen wir zunehmend eine datenzentrische Sicherheit. Denn letztlich haben es die Angreifer auf die Daten abgesehen – sei es, um sie zu veröffentlichen, wirtschaftlich zu verwerten oder eine Organisation damit zu erpressen. Cyberkriminalität ist längst ein Geschäftsmodell. Verschlüsselung und sicheres Schlüsselmanagement sind deshalb zentrale Voraussetzungen für eine widerstandsfähige digitale Verwaltung.

()

Stichwörter: Digitale Souveränität, Thales, Cybersicherheit, IT-Sicherheit, Quantencomputing