Migration zur Post-Quanten-Kryptografie: Wann lohnt sich der Quantensprung?

Asymmetrische Kryptografie ist weit verbreitet. Doch Algorithmen, die heute als sicher gelten, können von Quantencomputern von morgen gebrochen werden.

Auch wenn der Durchbruch in der Quanteninformatik noch einige Jahre auf sich warten lässt, müssen sich Organisationen rechtzeitig auf den reibungslosen Übergang zu quantensicheren Systemen vorbereiten. Die Auswahl geeigneter Algorithmen sowie das Umstellen auf quantensichere Systeme können eine besondere Herausforderung sein.

Schätzungen zufolge könnten kryptografisch relevante Quantencomputer bereits ab 2030 verfügbar sein. Nicht nur asymmetrische Verschlüsselungs- und Signaturverfahren sind dadurch gefährdet, sondern auch symmetrische Verschlüsselungsverfahren und Hashfunktionen. Mit dem in den 90er Jahren entwickelten Such-Algorithmus „Grover" kann die Komplexität von Suchproblemen auf ungeordnete Daten stark reduziert werden. Über eine Anpassung der Schlüssellänge kann die Reduktion kompensiert werden. Schon heute wird bei Neuentwicklungen davon abgeraten, AES-128 zu verwenden. Stattdessen sollte AES-256 genutzt werden, da eine Schlüssellänge von 256 Bit als notwendig erachtet wird, um auch langfristig einen hinreichenden Schutz gegen Quantencomputer-Angriffe zu bieten.

HEUTE FÜR DIE QUANTENKRYPTOGRAFIE VON MORGEN RÜSTEN

Auch wenn die Quantentechnologie aktuell noch weiterentwickelt werden muss, wurden in den letzten Jahren bereits enorme Fortschritte erzielt. Daher sollten sich Organisationen rechtzeitig auf einen reibungslosen Übergang hin zu quantensicheren Systemen vorbereiten. Vor allem jene, die gefährdete Verfahren zum Schutz von Daten mit langer Lebensdauer verwenden – z. B. Gesundheitsdaten, die zehn Jahre sicher aufbewahrt werden müssen, sollten bereits heute nach einer geeigneten Alternative suchen. Doch die Auswahl geeigneter Algorithmen und das Umstellen auf quantensichere Systeme können eine besondere Herausforderung für Organisationen darstellen. Wenn 2030 der erste kryptografisch relevante Quantencomputer zur Verfügung stehen sollte, könnten Angreifer verschlüsselte Daten schon jetzt abfangen und erst später entschlüsseln – nach dem Prinzip „hack now – decrypt later."

VERFAHREN DER ZUKUNFT

Auch das BSI hat bereits erste Empfehlungen ausgesprochen. Dazu zählen z. B. die Entwicklung von kryptoagilen Lösungen und die Verwendung von Post-Quanten-Kryptografie-Algorithmen in Kompositionsform. Komposition bedeutet die Kombination mit klassischen kryptografischen Algorithmen, da viele Verfahren noch sehr jung und wenig erforscht sind. Womit die Gefahr noch groß ist, dass Kryptoanalysen gefunden werden, die diese brechen. Weitere Herausforderungen sind: Kryptografische Protokolle müssen weiterentwickelt werden und die Public-Key-Infrastruktur muss in der Lage sein, Zertifikate zu verarbeiten, die sowohl die klassischen Schlüssel in längerer Variante, als auch die quantensicheren Schlüssel enthalten.

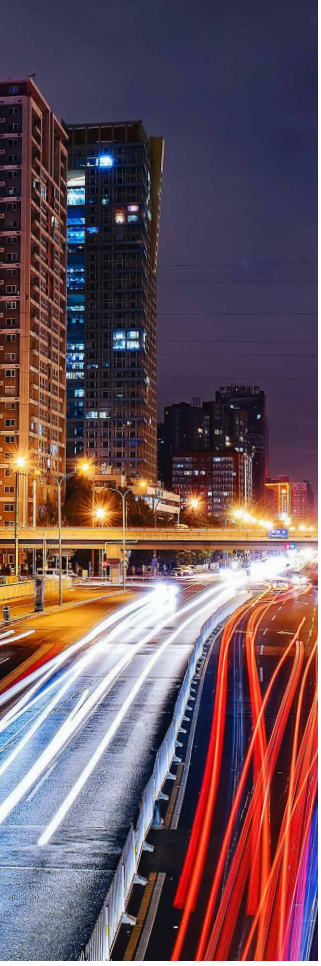
Auch wenn es bisher nur sehr wenige offizielle Lösungen gibt, die ebenfalls in Bibliotheken

HISOLUTIONS

HiSolutions AG
Schloßstraße 1
12163 Berlin

info@hisolutions.com
www.hisolutions.com

Fon +49 30 533 289-0
Fax +49 30 533 289-900



HISOLUTIONS

Einzug halten, die die asymmetrischen kryptografischen Verfahren ersetzen, kann man heute schon einiges tun:

- Sensibilisierung für das Thema/ Vorbereitung auf die Migration:
  - Ermittlung von Verantwortlichkeiten
  - Identifizierung der Baustellen (wo werden in der Organisation kryptografische Produkte eingesetzt und welche?)
  - Erstellung eines Migrationskonzeptes
- Umsetzung der Maßnahmen, die bereits veröffentlicht sind:
  - Migration auf größere Schlüssellängen (mind. 256 Bit bei symmetrischen Verfahren)
  - Flexible Gestaltung der kryptografischen Mechanismen, um kommende Standards einfacher/schneller umsetzen zu können (Kryptoagilität)

IHR QUANTENSPRUNG MIT HISOLUTIONS

Unsere Fachleute analysieren für Sie Ihre spezifischen Systeme, die kryptografische Verfahren verwenden. Danach werden die notwendigen Änderungen für die Migration zu Post-Quanten-Kryptografie-Lösungen unter Berücksichtigung spezifischer Anforderungen identifiziert. Dabei entwickeln wir für Sie geeignete Migrations- und Übergangslösungen. Ebenfalls möchten wir das Bewusstsein für die Problematik schärfen, die sich aus der Entwicklung der Quanteninformatik für Unternehmen ergibt.

Mehr Informationen zum Quantencomputer und den Gefährdungen wie Lösungsmöglichkeiten finden Sie in einem Dokument des BSI oder in unserem Beitrag im HiSolutions Research-Blog.

VORGEHENSWEISE: MIGRATION ZUR POST-QUANTEN-KRYPTOGRAFIE

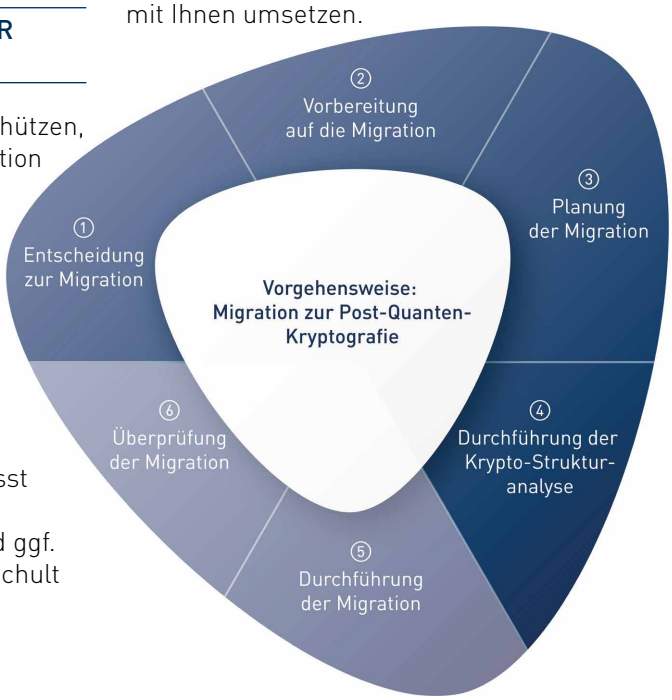
Um Informationen angemessen zu schützen, muss deren Bedeutung für die Institution klar und in einem Klassifikationsschema festgehalten sein. Zunächst muss für die Migration zur Nutzung der neuen Algorithmen ein Konzept entstehen. Dafür sollten organisatorische Regelungen sowie die Aufgabenverteilung festgelegt und bestehende Betriebsprozesse hinsichtlich der Anwendung der kryptografischen Algorithmen identifiziert und angepasst werden. Die IT sollte ausreichend im Migrationsprozess berücksichtigt und ggf. müssen Mitarbeitende zusätzlich geschult werden.

Für die alternativen Post-Quanten-Kryptografie-Verfahren wird sichergestellt, dass etablierte und von der Fachwelt anerkannte Algorithmen und Schlüssellängen Verwendung finden. Die Verfahren werden im Migrationskonzept dokumentiert.

Folgende Schritte sind erforderlich:

1. Entscheidung zur Migration
   a. Aufklärung
   b. Informierte Entscheidung
2. Vorbereitung auf die Migration
   a. Festlegung der Verantwortlichkeit
   b. Identifizierung der Ressourcen
   c. Festlegung der Post-Quanten-Kryptografie-Verfahren
   d. Analyse der vorhandenen Public-Key-Infrastruktur
3. Planung der Migration
   a. Erstellung eines Umsetzungplans
   b. Risikomanagement
   c. Planung von Ausfallzeiten
4. Durchführung der Krypto-Strukturanalyse
   a. Klassifikation von Informationen
   b. Durchführung der Krypto-Strukturanalyse
   c. Outsourcing (Identifizierung der relevanten Dienstleister)
   d. Identifizierung der eingesetzten kryptografischen Verfahren
5. Durchführung der Migration
   a. Herstellung von Kryptoagilität, wo sie noch nicht vorhanden ist
   b. Migration der Verfahren
   c. Überwachung
   d. Dokumentation
6. Überprüfung der Migration
   a. Durchführung eines technischen Audits

Die Schritte 1 bis 5a können wir schon heute mit Ihnen umsetzen.



Ihre Ansprechpartner

Barbara Grutzig
Holger von Rhein

info@hisolutions.com
Fon +49 30 533 289-0