

Hoe bereid je je organisatie voor op post-kwantumbeveiliging? Een praktisch stappenplan

02 juli 2026, 09:00

Farhad Aghili

Ludwig De Locht

Van inventarisatie tot migratieroadmap: 5 stappen naar een kwantumbestendige organisatie

In een [vorig artikel](#) legden we uit waarom organisaties vandaag al moeten nadenken over post-kwantumbeveiliging. De komst van cryptografisch relevante kwantumcomputers mag dan nog onzeker zijn, de voorbereiding op die transitie kan jaren duren. Een volledige migratie is vandaag nog niet nodig, maar organisaties kunnen nu al belangrijke stappen zetten om toekomstige risico's te beperken. Door inzicht te krijgen in waar cryptografie wordt gebruikt en hoe systemen kunnen worden aangepast, wordt de overgang naar post-kwantumbeveiliging een stuk beheersbaarder.

Stap 1: Breng je cryptografie in kaart

Een succesvolle migratie begint met inzicht. Veel organisaties weten niet precies waar cryptografie wordt toegepast of welke systemen afhankelijk zijn van kwetsbare algoritmen. Breng daarom in kaart waar cryptografie wordt gebruikt, bijvoorbeeld in:

- Producten
- Systemen
- Communicatieprotocollen
- Softwareafhankelijkheden
- Certificaten en PKI-infrastructuren
- Ingebedde componenten

Deze inventaris vormt de basis voor alle volgende stappen.

image of encrypted data

Stap 2: Identificeer kritieke systemen met een lange levensduur

Niet elk systeem hoeft dezelfde prioriteit te krijgen. Focus eerst op systemen die nog jarenlang operationeel zullen blijven of moeilijk aangepast kunnen worden. Denk bijvoorbeeld aan systemen

die:

- Nog vele jaren in gebruik zullen blijven
- Moeilijk op afstand kunnen worden bijgewerkt
- Hoge vervangkosten hebben
- Essentieel zijn voor de bedrijfsvoering

Hoe langer een systeem in gebruik blijft, hoe belangrijker het is om vandaag al rekening te houden met toekomstige cryptografische migraties.

Stap 3: Evalueer de crypto-agility van uw systemen

Een belangrijke eigenschap van toekomstbestendige systemen is crypto-agility: de mogelijkheid om cryptografische algoritmen te vervangen zonder het volledige systeem opnieuw te moeten ontwerpen. Ga daarom na:

- Welke cryptografische mechanismen eenvoudig kunnen worden vervangen;
- Welke onderdelen sterk afhankelijk zijn van specifieke algoritmen;
- In welke mate de huidige architectuur modulair is opgebouwd.

Hoe flexibeler de architectuur, hoe eenvoudiger toekomstige migraties zullen verlopen.

Stap 4: Breng afhankelijkheden in kaart

Cryptografie zit vaak niet alleen in eigen software, maar ook verborgen in externe componenten en diensten. Daarom is het belangrijk om inzicht te krijgen in alle afhankelijkheden. Bekijk onder meer:

- Leveranciers
- Software van derden
- Cloudplatformen
- Industriële ecosystemen

Deze afhankelijkheden bepalen mee hoe complex een toekomstige migratie zal worden.

Stap 5: Werk een migratieroadmap uit

De transitie naar het post-kwantumtijdperk is geen eenmalig project. Het is een langdurig proces dat prioritering, aansturing en een gefaseerde besluitvorming vereist. Een roadmap helpt om prioriteiten te bepalen, risico's te beheren en investeringen te spreiden. Zo kan de migratie stap voor stap worden voorbereid zonder de bedrijfsvoering te verstoren.

A picture of employees making a roadmap

Bouw samen praktische vaardigheden op

Post-kwantumcryptografie blijft een actief onderzoeksgebied. Tegelijkertijd zijn veel organisaties op zoek naar praktische richtlijnen die aansluiten bij reële industriële omgevingen. De vragen gaan vaak over:

- Migratiestrategieën
- Gevolgen voor de integratie
- Cryptoflexibiliteit
- Beperkingen op het gebied van ingebedde systemen en OT
- Levenscyclusbeheer
- Operationele haalbaarheid

Ook hebben organisaties nood aan praktische manieren om cryptografische afhankelijkheden in kaart te brengen, migratieopties te beoordelen en de gevolgen daarvan in reële operationele omgevingen te toetsen. Om die transitie te ondersteunen, onderzoekt Sirris hoe praktische methodologieën, validatieactiviteiten en toegepaste expertise Belgische bedrijven kunnen helpen om zich voor te bereiden op de migratie naar post-kwantumtechnologie in realistische industriële contexten.

Het doel is niet om bepaalde technologieën of leveranciers op te leggen, dan wel om organisaties te helpen de gevolgen te begrijpen, in te schatten in hoeverre ze er klaar voor zijn en praktische stappen te identificeren om zich voor te bereiden. Naarmate kwantumbestendige systemen werkelijkheid worden, zullen collectief leren en praktisch experimenteren een belangrijke rol spelen om de industrie te ondersteunen bij deze transitie.

Begin vandaag met de voorbereiding

Wilt u beter begrijpen welke gevolgen de post-kwantumtransitie kan hebben voor uw producten, systemen of digitale infrastructuur en welke praktische stappen u vandaag al kunt ondernemen? Sirris helpt ondernemingen om risico's in te schatten, migratietrajecten te verkennen en praktische expertise op te bouwen voor cyberweerbaarheid op de lange termijn.

[Contacteer ons](#)

Dit artikel maakt deel uit van een tweeluik over post-kwantumbeveiliging.

Deel 1: [Post-kwantumbeveiliging begint met migratie, niet met kwantumcomputers](#)

Deel 2: Hoe bereid je je organisatie voor op post-kwantumbeveiliging? Een praktisch stappenplan ?

Auteurs



Farhad Aghili



Ludwig De Locht