

Post-kwantumbeveiliging begint met migratie, niet met kwantumcomputers

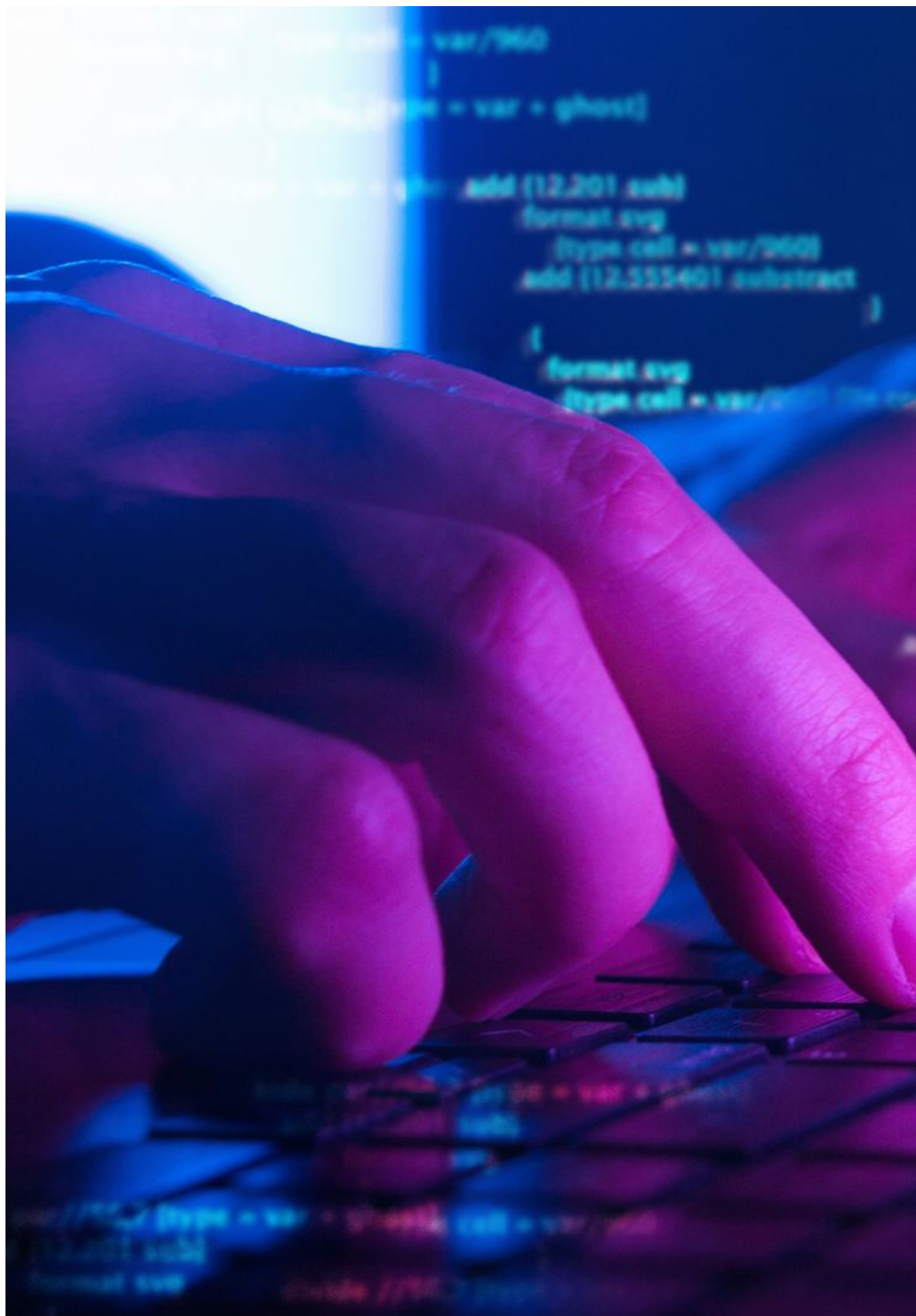
02 juli 2026, 10:00

Farhad Aghili

Ludwig De Locht

Waarom organisaties zich ruim voor 'Q-day' moeten voorbereiden

Veel organisaties beschouwen post-kwantumbeveiliging nog steeds als een zorg voor de toekomst. Cryptografisch relevante kwantumcomputers (Cryptographically Relevant Quantum Computers – CRQC's) die de huidige publieke-sleutelcryptografie kunnen kraken, bestaan nog niet op industriële schaal, en niemand weet met zekerheid wanneer 'Q-day' zal aanbreken. De vraag is echter niet wanneer kwantumcomputers hun intrede zullen doen, maar hoe organisaties zich kunnen voorbereiden op een transitie die jaren in beslag kan nemen. Aangezien geconnecteerde producten, industriële systemen en digitale platformen tientallen jaren in gebruik blijven en regelgeving zoals de Cyber Resilience Act (CRA) en NIS2 de verantwoordelijkheden op het gebied van beveiliging gedurende de gehele levenscyclus afdwingen, wordt post-kwantumbeveiliging een enorme uitdaging op het gebied van bedrijfsvoering, architectuur en migratie, en die begint vandaag al.



Waarom post-kwantumbeveiliging nu al belangrijk is

Vrijwel elke organisatie gebruikt vandaag publieke-sleutelcryptografie, zoals RSA en ECC. Die technologie beveiligt onder meer softwareapplicaties, geconnecteerde producten, industriële systemen, cloudomgevingen, communicatieprotocollen en identiteits- en certificaatinfrastructuren. Kwantumcomputers vormen een bedreiging voor een deel van die basis. Verwacht wordt dat deze veelgebruikte cryptografische mechanismen op basis van publieke sleutels zullen worden gekraakt zodra voldoende krachtige, cryptografisch relevante kwantumcomputers beschikbaar worden. Het exacte tijdstip blijft weliswaar onzeker, maar die onzekerheid is geen reden om de voorbereiding uit te stellen. De transitie is niet langer een louter theoretisch gegeven, want de eerste normen voor post-kwantumcryptografie zijn al gepubliceerd.

Eén belangrijke bezorgdheid is het scenario 'harvest now, decrypt later'. Gevoelige, versleutelde informatie kan nu al worden verzameld en in de toekomst worden ontsleuteld, wanneer de kwantumtechnologie verder is ontwikkeld. Voor organisaties die vertrouwelijke gegevens voor de lange termijn verwerken, bestaat mogelijk vandaag al een risico op toekomstige openbaarmaking.

Een andere uitdaging is de lange levensduur van veel digitale systemen. Heel wat producten en infrastructuren die vandaag worden ontwikkeld of ingezet, zullen nog operationeel zijn wanneer kwantumbedreigingen een realiteit worden. Dat geldt onder meer voor industriële machines, geconnecteerde producten, IoT-apparaten, OT-omgevingen, embedded systemen en softwareplatformen met een lange levensduur. Hoe langer een systeem in gebruik blijft, hoe minder tijd er overblijft voor een soepele migratie in de toekomst.



De migratie is de echte uitdaging

Bij discussies over post-kwantumbeveiliging gaat de aandacht vaak uit naar nieuwe algoritmen en cryptografische normen. In werkelijkheid vertegenwoordigt de technologie slechts een deel van de uitdaging. De echte uitdaging bestaat erin inzicht te verwerven in waar cryptografie wordt toegepast, hoe diep deze in de systemen is ingebed en hoe organisaties deze systemen kunnen verder ontwikkelen zonder de bedrijfsvoering te verstoren. Organisaties botsen vandaag al op praktische vragen

- Waar wordt cryptografie in onze systemen toegepast?
- Welke onderdelen zijn afhankelijk van kwetsbare mechanismen?
- Welke onderdelen zijn afhankelijk van cryptografische mechanismen die in de toekomst mogelijk moeten worden vervangen?
- Welke leveranciers brengen cryptografische afhankelijkheden met zich mee?
- Kunnen systemen op afstand worden bijgewerkt?
- Wat zijn de operationele risico's van migratie?
- Welke gevolgen heeft dit voor de prestaties of de interoperabiliteit?

Deze vragen reiken verder dan cryptografie. Ze raken aan systeemarchitectuur, software lifecycle management en systeemengineering. Een eerste uitdaging is dan ook zicht krijgen op waar cryptografie precies wordt gebruikt. Die zit vaak dieper ingebed dan organisaties denken, bijvoorbeeld in communicatiestacks, middleware, PKI-infrastructuren, hardwarebeveiligingsmodules, firmware, software van derden en clouddiensten. Daardoor is een migratie zelden een eenvoudige vervanging van een algoritme, maar een traject dat planning, prioritering en een gefaseerde uitvoering vraagt.

Elke sector staat voor andere uitdagingen

Geconnecteerde producten, machines en embedded systemen

Voor organisaties die geconnecteerde producten, industriële machines of IoT-oplossingen ontwikkelen, vormen de levenscyclusbeperkingen vaak de grootste uitdaging. Veel van deze systemen:

- Blijven nog vele jaren in gebruik
- Beschikken over beperkte computerbronnen
- Zijn moeilijk bij te werken
- Hangen af van de vaste hardwaremogelijkheden
- Omvatten meerdere leveranciers en protocollen

In deze omgevingen hangt de gereedheid voor het post-kwantumtijdperk nauw samen met updatebaarheid, cryptoflexibiliteit, moduleerbare architecturen, lifecyclebewust design. Het doel is niet alleen om de systemen vandaag te beveiligen. Men moet er ook voor zorgen dat ze zich in de loop van de tijd op een veilige manier kunnen blijven ontwikkelen. Dat wordt nog belangrijker in het kader van de Cyber Resilience Act, die de verantwoordelijkheden over de hele levenscyclus van digitale producten aanscherpt.

SaaS-aanbieders en digitale platformen

SaaS-aanbieders beschikken vaak over meer flexibiliteit om systemen bij te werken. Toch moeten ook zij diverse uitdagingen het hoofd bieden. Belangrijke overwegingen zijn:

- De vertrouwelijkheid van klantgegevens op de lange termijn
- De cryptografische afhankelijkheden in cloudomgevingen
- Het identiteits- en certificaatbeheer
- Integraties met externe diensten
- Vereisten op het gebied van naleving en vertrouwen

Voor organisaties die actief zijn in de gezondheidszorg, de financiële sector, de energiesector of op het gebied van kritieke infrastructuur, worden deze onderwerpen alsmaar belangrijker. De voorbereiding op het post-kwantumtijdperk wordt geleidelijk aan een onderdeel van bredere strategieën op het gebied van veerkracht en vertrouwen.

Productiebedrijven en industriële exploitanten

Industriële bedrijven ontwikkelen de onderliggende technologieën misschien niet zelf, maar zijn vaak sterk afhankelijk van digitale infrastructuren en geconnecteerde productieomgevingen. Daardoor worden ze geconfronteerd met uitdagingen zoals verouderde systemen, lange vervangingscycli, afhankelijkheden van leveranciers en een beperkt inzicht in de ingebedde technologieën waarop hun productieomgeving steunt.

Veel industriële omgevingen zijn bovendien nooit ontworpen met het oog op cryptoflexibiliteit of toekomstige cryptografische migraties. Naarmate de connectiviteit toeneemt, wordt het daarom steeds belangrijker om niet alleen inzicht te krijgen in waar cryptografie wordt toegepast, maar ook in de mate waarin de bedrijfsvoering ervan afhankelijk is.



Organisaties hoeven vandaag nog niet al hun cryptografie te vervangen. Wel is dit het moment om zicht te krijgen op waar cryptografie gebruikt wordt en hoe een toekomstige migratie eruit kan zien. Want wanneer post-kwantumbeveiliging noodzakelijk wordt, zal voorbereiding het verschil maken.

Hoe begin je daar concreet aan? In een volgend artikel bekijken we welke stappen organisaties vandaag al kunnen zetten om zich voor te bereiden op de migratie naar post-kwantumbeveiliging.

[Lees het volgende artikel](#)

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

Deel 1: Post-kwantumbeveiliging begint met migratie, niet met quantumcomputers ?

Deel 2: [Hoe bereid je je organisatie voor op post-kwantumbeveiliging? Een praktisch stappenplan](#)

Auteurs



Farhad Aghili



Ludwig De Locht