

## MSP's: Verhoog De Winstmarge Met 25%

Eén abonnement voor beheer, beveiliging en back-up van alle Endpoints

Boek een demo

5MIN • SECURITY

## Criminelen verzamelen nu al data voor de quantumcomputer van morgen

Migratie naar quantum-resistente encryptie duurt jaren en moet nu beginnen



KIM LOOHUIS

Jun 24, 2025, 9:16 AM UTC



Experts schatten in dat binnen 5 tot 15 jaar een cryptografisch relevante quantumcomputer standaard encryptie in minder dan 24 uur kan kraken. Die waarschuwing komt uit het [Quantum Threat Timeline Report van het Global Risk Institute](#).

Tijdens de recente SANS Emerging Threats Summit in de Verenigde Staten werd duidelijk: de quantumdreiging is geen toekomstmuziek meer, maar een realiteit waar organisaties nu al mee te maken hebben.

De reden is simpel maar verontrustend. Criminelen en vijandige staten verzamelen nu al massaal versleutelde data, niet om die direct te kraken, maar om die over enkele jaren te ontsleutelen met quantumcomputers. Deze 'harvest now, decrypt later'-aanvallen vormen een groeiend risico dat veel Nederlandse organisaties onderschatten.

Nederlandse cryptografie-experts waarschuwen al jaren voor deze ontwikkeling. Wat internationale experts nu op de SANS Summit signaleren, voorspelden Nederlandse onderzoekers van het Centrum Wiskunde & Informatica (CWI) al langer. "We hebben gezien dat de migratie van SHA-1 naar SHA-256 gemakkelijk vijf tot tien jaar duurde," zegt [Marc Stevens](#), senior onderzoeker in de cryptologie-onderzoeksgroep van het CWI. "We moeten er dus vanuit gaan dat de migratie naar quantum-veilige cryptografie minstens dat tijdsbestek zal kosten."

## Zeven internationale lessen, Nederlandse context

De Amerikaanse SANS-experts formuleerden zeven cruciale inzichten voor organisaties wereldwijd. Deze takeaways krijgen in Nederland extra gewicht door de expertise die Nederlandse onderzoekers al jaren hebben opgebouwd:

- 1. Quantumcomputers zijn nabij en zullen huidige encryptie breken** Deze internationale consensus wordt door Stevens al jaren ondersteund: "Hoewel quantumcomputers momenteel nog niet sterk genoeg zijn om onze huidige cryptografiesystemen te breken, is de kans reëel dat er in de toekomst wel een moment komt dat ze dat kunnen. Het is daarom van essentieel belang dat bedrijven zich hier nu op voorbereiden."
- 2. Post-quantum cryptografie (PQC) is de defensieve prioriteit** Nederland loopt voorop in deze ontwikkeling. [Léo Ducas](#) van het CWI was betrokken bij twee van de vier nieuwe [NIST-standaarden](#) die vorig jaar werden gepubliceerd. "De selectie van onze algoritmes als standaard betekent dat ze wereldwijd zullen worden ingezet om de privacy van miljarden gebruikers te beschermen," zegt Ducas.
- 3. Data van vandaag zijn morgen kwetsbaar** Het 'harvest now, decrypt later'-concept dat op de SANS Summit werd benadrukt, herkent Stevens direct. "Als deze informatie over jaren kan worden ontsleuteld, kan die worden gebruikt om een land op het juiste moment op strategische wijze in verlegenheid te brengen," waarschuwde hij al eerder. Het gaat niet alleen om huidige staatsgeheimen, maar ook om bedrijfsgegevens die nu worden verzameld voor latere exploitatie.
- 4. De quantumshift raakt elke sector** De Nederlandse overheid heeft dit erkend. De AIVD ontwikkelde samen met TNO en CWI een [praktisch migratiehandboek](#) specifiek voor overheden, bedrijven, vitale sectoren en kennisinstellingen. "Er is geen één strategie voor alle organisaties," benadrukt Stevens. "Niet elke organisatie heeft dezelfde belangen en ICT-structuur."
- 5. Migreren naar quantum-veilige systemen is uitdagend maar essentieel** Stevens waarschuwde al voor de complexiteit van deze migratie, vooral bij langlevende systemen. "Denk aan auto's bijvoorbeeld, of bruggen en sluizen," legt hij uit. Deze systemen worden nu ontwikkeld en geïmplementeerd, maar zijn later nauwelijks te upgraden naar quantum-veilige cryptografie omdat de nieuwe standaarden krachtigere hardware vereisen.
- 6. Regelgevingsmomentum neemt toe** Waar Amerikaanse experts op de SANS Summit spraken over toenemende regelgevingsdruk, kiest Nederland voor een andere aanpak. "We zien meer een bottom-up benadering in Nederland," zegt Stevens. "Het handboek hebben we voorgelegd aan een klankbordgroep met technische mensen van verschillende ministeries. Die hebben intern al een migratie geïnitieerd."
- 7. Nu is het moment om te handelen** De internationale oproep tot actie sluit aan bij wat Stevens adviseert: "Begin in ieder geval met een inventarisatie. Laat je niet verrassen over wat je binnen je organisatie hebt en gebruikt op het moment dat het daadwerkelijk gaat spelen. Zorg dat je nu al weet wat je risico's zijn en wat je kunt doen."

## Cryptografische wendbaarheid als Nederlandse kracht

Voor Nederlandse IT-afdelingen betekent dit concreet handelen. "We zien vaak dat cryptografie en versleuteling nu op de diepere niveaus in systemen zijn ingebouwd. Dat is een van de redenen waarom migratie zo lang gaat duren, omdat je per systeem moet kijken wat er is en hoe je dat naar de nieuwe standaard kunt overzetten," zegt Stevens.

De oplossing ligt in centralisatie. "Je wordt een stuk wendbaarder wanneer je een nieuwe cryptografische implementatie op een centrale plek zet waar je systemen met generieke calls toegang toe hebben. Een centraal systeem maakt het ook makkelijker om over te schakelen naar de nieuwe standaard. Het centraliseren van cryptografie binnen je organisatie is iets wat elk bedrijf nu al kan doen."

Het migratieproces begint met drie stappen die de AIVD samen met Nederlandse experts heeft uitgewerkt: diagnose, planning en implementatie. Organisaties moeten prioriteiten stellen bij data met langdurige gevoeligheid, zoals patiëntendossiers, onderzoeksgegevens of bedrijfsgeheimen die over jaren nog waardevol kunnen zijn voor aanvallers.

## Nederlandse voorsprong door samenwerking

Volgens [onderzoek van Deloitte](#) meet 52 procent van de organisaties wereldwijd al hun blootstelling aan quantum-gerelateerde risico's, terwijl nog eens 30 procent actief oplossingen implementeert. Nederlandse organisaties hebben een voorsprong door de expertise die het CWI en andere instituten al hebben opgebouwd.

"Door samen te werken kunnen organisaties effectiever migreren door kennis en informatie uit te wisselen en samen te leren," benadrukt Stevens. "Hoewel in ons land meer ad-hoc samenwerkingen lijken te zijn, is er zeker beweging, maar het is bottom-up."

De [quantumrevolutie is geen toekomstmuziek](#) meer, maar een realiteit die organisaties vandaag al raakt. De internationale waarschuwingen van de SANS Summit bevestigen wat Nederlandse experts al jaren signaleren. Nederlandse expertise biedt houvast, maar alleen als organisaties nu in actie komen. Want zoals de internationale experts waarschuwden: "Quantum komt eraan, of dat nu over zeven jaar is of over vijftien. Nu is het moment om te handelen. Als je wacht tot quantum er is, ben je al te laat."

Tags: [CWI](#) / [deloitte](#) / [quantumcryptografie](#) / [SANS Institute](#)



## MSP's: Verhoog De Winstmarge Met 25%

Eén abonnement voor beheer, beveiliging en back-up van alle Endpoints

Boek een demo

## Lees meer over Security



### WhatsApp verbannen van Apparaten Huis van Afgevaardigden VS wegens veiligheidsrisico's

De populaire berichtendienst WhatsApp is vanaf nu verboden op alle apparaten die eigendom zijn van het Amerik...

LAURENS VAN AGGELEN • 27 MINUTEN GELEDEN



### Zomerse zorg: cyberaanvallen pieken terwijl vaakzaamheid afneemt

Waar de zomermaanden voor velen in het teken staan van ontspanning, luiden experts juist alarm over een toene...

LAURENS VAN AGGELEN • 20 JUNI 2025

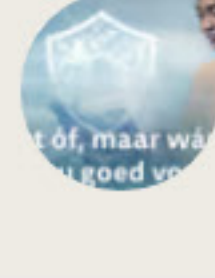


### Bedrijven beveiligen massaal inlogsystemen met tweestapsverificatie

Nederlandse bedrijven investeren steeds vaker in digitale beveiliging. Vooral tweestapsverificatie, ofwel twe...

LAURENS VAN AGGELEN • 20 JUNI 2025

#### WHITEPAPERS



#### Ontgrendel het volledige potentieel van je SAP-omgeving

In het document "Unlock the full potential of your SAP environment" w...



#### Hoffmann Tips Special – Cybersecurity Risk management

Niet óf, maar wanneer. Bent u goed voorbereid? Laat je in...

#### Een cloudstrategie is essentieel voor het succes van uw bedrijf

In veel fabrieken worden gegevens en informatie die relevant zijn voor...

#### Is Your Environment Adaptive Enough for Zero Trust?

In een poging om hun beveiliging te verhogen, passen meer organisaties...

#### TECH CALENDAR

#### Nürnberg Digital Festival 2025

30 JUNE 2025 NÜRNBERG

#### The AI reality tour

2 JULY 2025 HOEVEN

#### GITEX DIGI\_HEALTH 5.0 - Thailand

10 SEPTEMBER 2025 BITEC BANGKOK, THAILAND

#### IT Arena

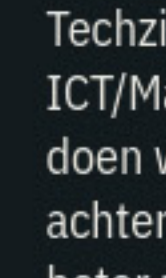
26 SEPTEMBER 2025 LVIV, UKRAINE

#### Innovation Week 2025

9 OCTOBER 2025 PRAGUE

#### Luxembourg Venture Days

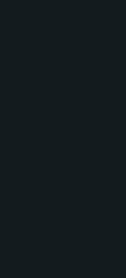
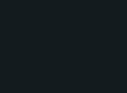
22 OCTOBER 2025 LUXEMBOURG



ICTMagazine.nl

ICT/Magazine richt zich op zakelijke beslissers en professionals die willen weten wat de impact van technologie is op een organisatie. Waar we met Techzine ingaan op de technologie, gaan we bij ICT/Magazine in op de business-kant van IT. Dat doen we door middel van nieuws en achtergrondverhalen. Door de business-kant van IT beter uit te leggen kunnen beslissers en influencers binnen een organisatie sturen richting de juiste oplossingen.

Follow us



ICT/Magazine Service

WORD EEN PARTNER  
ADVERTEREN  
OVER ONS  
CONTACT  
ALGEMENE VOORWAARDEN  
PRIVACYVERKLARING