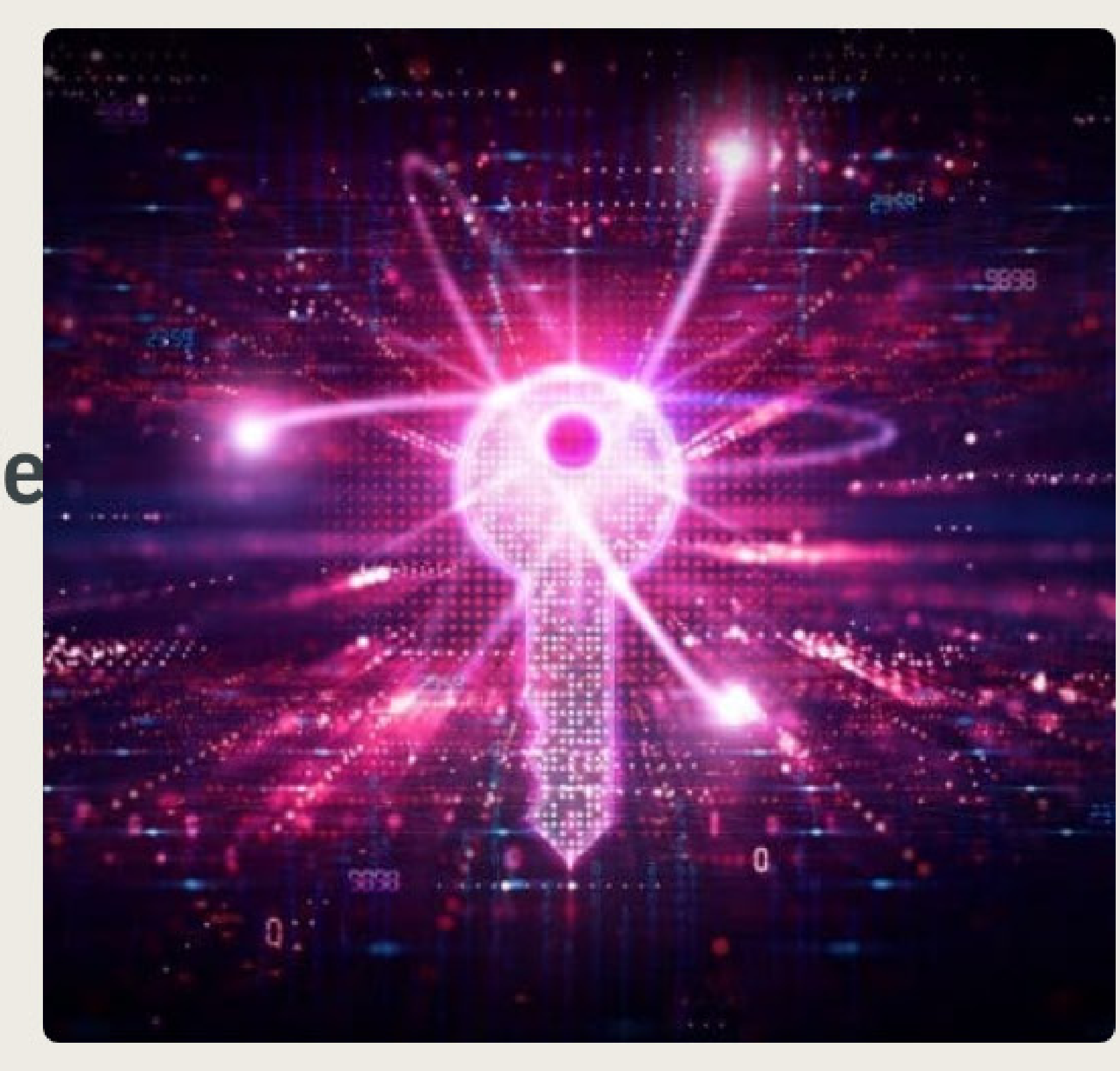
4MIN ● SECURITY

Toekomstige beveiligingsrisico's: waarom quantumcryptografie hoger op de agenda moet staan


YAROSLAV ROSOMAKHO
Guest expert
VP Field CTO bij Zscaler
Jun 10, 2025, 10:30 AM UTC



Hoewel veel IT-teams nog bezig zijn hun beveiligingsinfrastructuur aan te passen om AI-gebaseerde aanvallen te weerstaan, is er alweer een andere opkomende technologie die de komende jaren voor aanzienlijke disruptie zal zorgen: post-quantumcryptografie.

De naderende commercialisering van quantumcomputing – en de cryptografische implicaties die dit met zich meebrengt – kan ernstige gevolgen hebben voor organisaties die zich hier niet op voorbereiden. Maar hoe moeten ze hun netwerken en data hierop aanpassen? En hoe snel kunnen cybercriminelen ook gebruikmaken van deze technologie?

Het quantumrisico

Een quantumcomputer kan wiskundige problemen oplossen die te uitdagend zijn voor traditionele computers, zoals het ontbinden van grote getallen. Dit betekent echter ook dat quantumcomputing veel moderne cryptografische algoritmen kan kraken die veel worden gebruikt op verschillende IT-platforms om communicatie te versleutelen, gegevens te beveiligen of digitale handtekening te creëren.

Quantumcomputers zijn nog niet commercieel beschikbaar, maar ik denk dat organisaties post-quantumcryptografie om twee redenen nu al als strategische zorg moeten beschouwen. Ten eerste is er de zeer reële kans op retrospectieve aanvallen. Cryptografische technologieën zijn zo ver geïntegreerd in bedrijfsprocessen dat de meeste gegevens zowel 'in rust' als 'in beweging' digitaal worden versleuteld. Bij retrospectieve aanvallen verzamelen cybercriminelen versleutelde gegevens en slaan deze op tot het moment dat ze deze kunnen kraken met behulp van quantumcomputers. Hoewel de gegevens tegen die tijd mogelijk al een paar jaar oud zijn, kunnen ze nog steeds gevoelig zijn en schade toebrengen aan bedrijven, werknemers en klanten.

De tweede reden voor bezorgdheid is de omvang van de investering en operationele overhead die nodig zijn om verouderde IT-systemen te upgraden of te vervangen. Momenteel vormt quantumcomputing nog geen direct gevaar, maar grote particuliere bedrijven en overheden investeren hier aanzienlijk in. De verwachting is dan ook dat we slechts een paar jaar verwijderd zijn van een doorbraak. Om de financiële last te verlichten, zouden bedrijven hun systemen nu al stapsgewijs moeten upgraden, in plaats van te wachten op deze doorbraak in quantumcomputing en gedwongen worden om in één keer fors te investeren (en het risico te lopen achterop te raken op de concurrentie).

De quantum-tijdlijn

Hoewel er nog geen consensus is over wanneer commerciële quantumcomputers beschikbaar zullen zijn, zijn de meeste wetenschappers het erover eens dat dit over minstens drie tot vijf jaar zal zijn. Overheden doen echter nu al aanbevelingen aan bedrijven om zich voor te bereiden op de overgang naar quantumversleuteling. Zo heeft het Britse National Cyber Security Centre (NCSC) onlangs richtlijnen gepubliceerd die bedrijven aanmoedigen zich nu al voor te bereiden op deze overgang naar quantumcomputing. Deze richtlijnen moeten een soepele, gecontroleerde migratie mogelijk maken en het risico op

overhaaste implementaties en bijbehorende beveiligingslekken verkleinen. Als onderdeel hiervan riep het NCSC organisaties op om te investeren in zichtbaarheid, om te begrijpen welke systemen ze hebben en welke systemen vóór de migratie moeten worden geüpgraded.

Ook in Nederland wordt er aandacht besteed aan quantumcomputing. Zo hebben de Algemene Inlichtingen- en Veiligheidsdienst (AIVD), het Centrum Wiskunde & Informatica (CWI) en TNO samen een handboek uitgebracht voor quantumveilige cryptografie. Dit handboek bevat de nieuwste inzichten en praktische richtlijnen om de risico's van quantumcomputers aan te pakken en is bedoeld om CIO's, CTO's en CISO's te helpen tijdig over te stappen naar quantumveilige cryptografie.

De Europese Unie werkt ook aan richtlijnen voor quantumversleuteing en ik verwacht dat er snel regelgeving volgt die post-quantumcryptografie bevat als onderdeel van fundamentele nalevingsmaatregelen, vergelijkbaar met NIS2 en DORA. Hoewel alle overheidsdocumentatie rond quantum momenteel slechts een richtlijn is, raad ik CISO's en IT-leiders aan om dit zo snel mogelijk op de agenda van hun bestuur te zetten. Dit voorkomt dat ze zich gehaast moeten aanpassen aan regelgeving en in één keer veel tijd en geld moeten besteden wanneer deze richtlijnen van kracht worden.

Voorkom een achterstand, start nu met plannen

Hoewel de tastbare dreiging van quantumcomputing nog een paar jaar op zich laat wachten, zijn de risico's die het met zich meebrengt aanzienlijk genoeg om nu al proactieve maatregelen te rechtvaardigen. Bedrijven kunnen zich voorbereiden door het inzicht in hun huidige systemen te vergroten en stapsgewijs upgrades te plannen om een soepele overgang naar post-quantumcryptografie te garanderen. Zo kunnen ze het risico van retrospectieve aanvallen beperken en de financiële en operationele druk van overhaaste implementaties vermijden.

Overheden en cyberbeveiligingsinstanties bieden al richtlijnen om organisaties te helpen bij deze transitie. Het is cruciaal dat CISO's en IT-leiders dit probleem prioriteit geven en onder de aandacht brengen van hun directies. Vroegtijdige voorbereiding beschermt niet alleen gevoelige gegevens, maar zorgt ook voor een concurrentievoorsprong wanneer quantumcomputing werkelijkheid wordt.

Uiteindelijk ligt de sleutel tot toekomstig succes in een vooruitziende blik en strategische planning. Door het quantumrisico nu aan te pakken, zorgen organisaties ervoor dat hun beveiligingsinfrastructuur robuust en veerkrachtig blijft.

Dit is een ingezonden bijdrage van Zscaler. Via deze link vind je meer informatie over de mogelijkheden van het bedrijf.

Tags: post-quantum cryptografie / quantum cryptografie / zscaler

KEUZE VAN DE REDACTIE

Opera Neon zet agentic AI-browser in de schijnwerpers
Opera, het op vier na populairste browserbedrijf , heeft Opera Neon a...

Microsoft ontkent diensten ICC te hebben gestopt
Het Outlook-account van ICC-hoofdaanklager Karim Khan werd eerder dit...

CEO SAP noemt Europese plan voor eigen cloud-datacenters onzinnig
De topman van SAP, Europa's meest waardevolle bedrijf, vindt het zi...

Microsoft start gratis European Security Program: wat houdt het in?
Microsoft-president Brad Smith doet zijn politiek klinkende titel eer...

INSIGHT: ANALYTICS

SAS geeft data scientists de stuurknuppel voor het tijdperk AI(-agents)
SAS is met zijn rijke historie voor data scientists een rots in de br...

SAS lanceert op maat gemaakte AI-modellen voor bedrijfsprocessen
Een nieuwe reeks modellen van SAS is specifiek ontworpen voor het ver...


Twee jaar generatieve AI: waar staan we nu?
Van luchtkastelen naar praktische toepasbaarheid


Volwassen benadering geeft SAS een voordeel in AI-markt
Leeftijd is maar een getal, of is hoger juist beter?

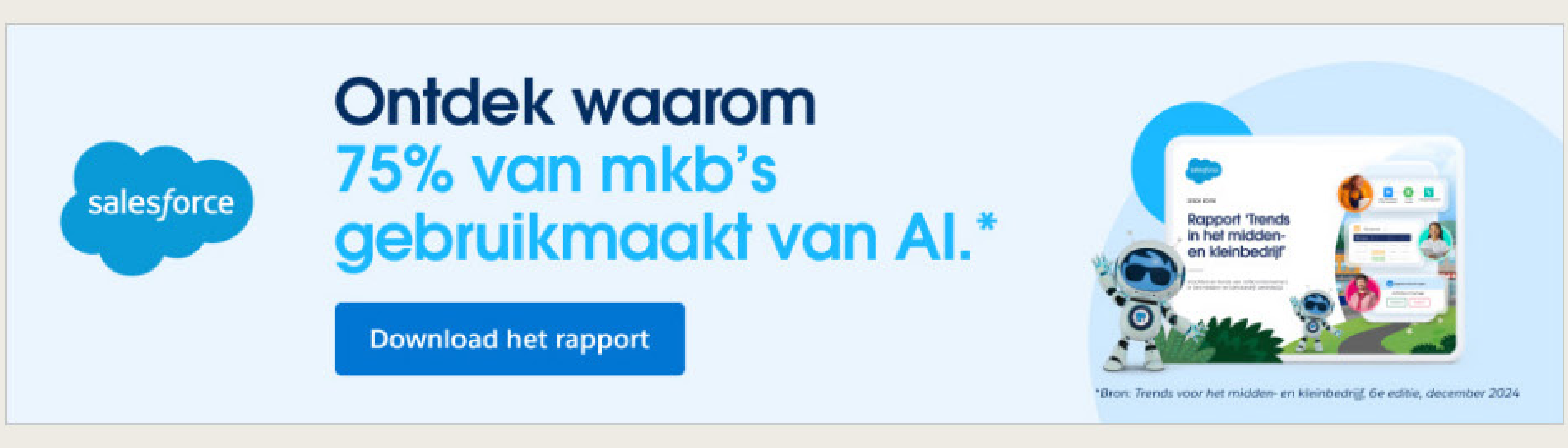
GERELATEERD

Europese IT-professionals vrezen impact van quantum computing op cybersecurity

HP voegt meer AI en PQC toe aan printers

Oracle lanceert Java 24 met verbeterde AI-ondersteuning en post-quantum cryptografie

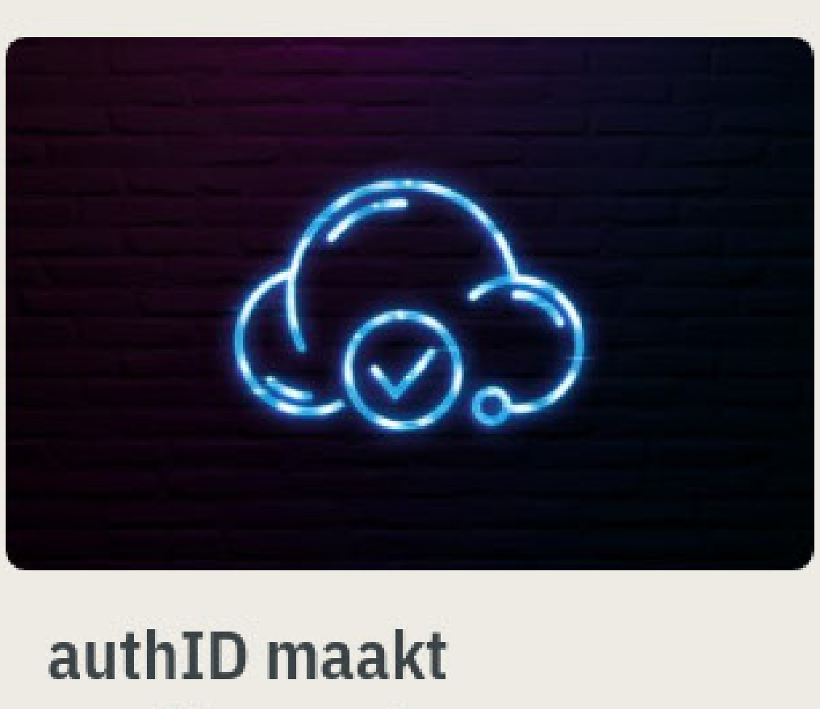
OT-security van datacenters moet veel hoger op de agenda staan



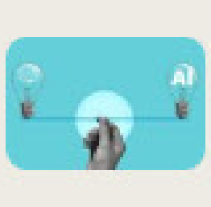
Lees meer over Security

Cyberincident verstoorde bedrijfsvoering levensmiddelengroothandels
United Natural Foods, een van de grootste levensmiddelengroothandels in de Verenigde Staten en leverancier va...
MELS DEES ● 3 UREN GELEDEN

Cisco waarschuwt voor kwetsbaarheid in cloud-wachtwoorden
Een ernstig beveiligingslek in Cisco Identity Services Engine (ISE) die draait op Amazon Web Services (AWS), ...
MELS DEES ● 6 JUNI 2025


authID maakt wachtwoorden overbodig met Ping Identity
authID heeft een nieuwe integratie aangekondigd met Ping Identity. Via PingOne DaVinci kunnen organisaties op...
ERIK VAN KLINKEN ● 5 JUNI 2025

WHITEPAPERS


Versnel je AI-succes met NVIDIA AI Computing van HPE
In het document "Sneller succes met AI dankzij NVIDIA AI Computing va...


Probeer gratis het nieuwste high-end Synology backup-systeem
Hoe zorg je ervoor dat jouw data veilig is en tegelijkertijd snel her...

Versterk je cybersecurity met DNS best practices
In het whitepaper "DNS Best Practices" van Infoblox worden essentiël...

Navigeren door technologische ontwrichting
Steeds meer bedrijven moeten zich aanpassen aan snelle innovaties om ...

TECH CALENDAR

Viva Technology
11 JUNE 2025 1 PLACE DE LA PORTE DE VERSAILLES,75015,PARIS,FRANCE

Kaseya DattoCon Europe
17 JUNE 2025 DUBLIN

Nutanix Cloud Day Nederland 2025
17 JUNE 2025 ZEIST

Akamai Customer Day Benelux
18 JUNE 2025 NIEUWEGEIN

Nürnberg Digital Festival 2025
30 JUNE 2025 NÜRNBERG

GITEX DIGI_HEALTH 5.0 - Thailand
10 SEPTEMBER 2025 BITEC BANGKOK, THAILAND

Techzine.nl
Techzine richt zich op IT-professionals en zakelijke decision makers door het publiceren van het laatste IT-nieuws en achtergrondverhalen. Het doel is om IT-professionals kennis te laten maken met nieuwe innovatieve producten en diensten, maar ook om diepgaande informatie te bieden om te helpen producten en diensten beter te begrijpen.