

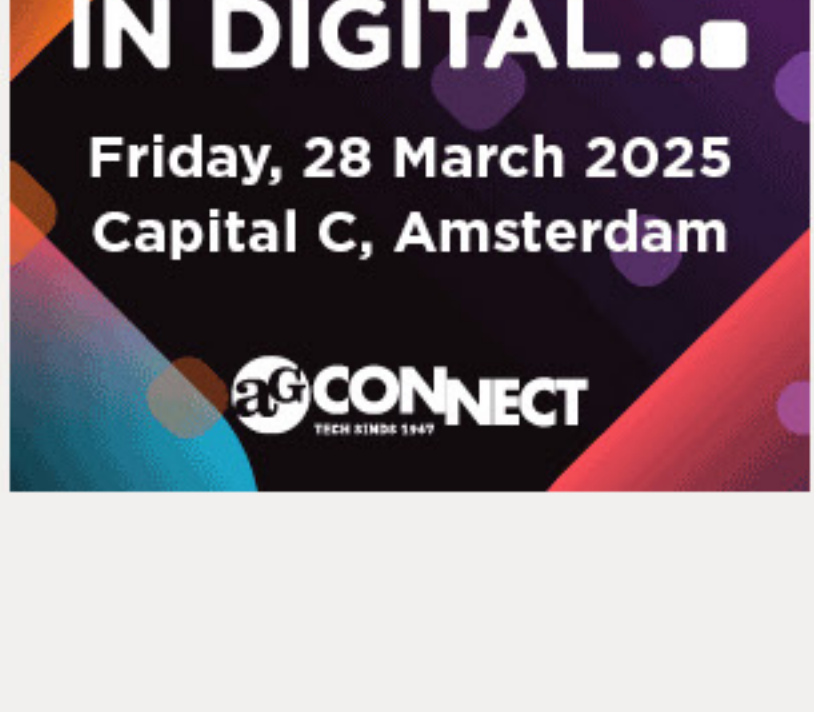


Achtergrond • Quantum + PRO

gisteren om 13:16🕒 leestijd 2 minuten💬 0 reacties

Vernieuwd handboek quantumveilige cryptografie bereidt voor op Q-Day

De Algemene Inlichtingen- en Veiligheidsdienst (AIVD), Centrum Wiskunde & Informatica (CWI) en TNO publiceerden deze week een vernieuwd handboek voor quantumveilige cryptografie. Het [PQC-migratiehandboek](#) moet organisaties helpen in de voorbereiding op Q-Day, de dag dat quantumcomputers in staat zijn veelgebruikte cryptografie te breken.



- Lees ook: [Nederland krijgt flink deel van Europese fabriek fotonische chips](#)

Chris Nap

is freelance journalist en tekstschrijver.
ketnocontent@gmail.com.

[Meer van deze auteur](#)



De tweede editie bevat de nieuwste ontwikkelingen en adviezen voor de overstap naar een quantumveilige omgeving, inclusief concreter advies voor het vinden van cryptografische componenten, het beoordelen van quantumrisico's en het opzetten van cryptografische wendbaarheid. Tijdens het Symposium 'Post-Quantum Cryptography' op 3 december 2024 in Den Haag is het overhandigd aan de staatssecretaris voor digitalisering Zsolt Szabó.

Q-Day komt eraan

Volgens experts kan Q-Day al binnen vijf tot vijftien jaar een feit zijn. Kwaadwillenden kunnen dan met inzet van quantumcomputers cryptografie omzeilen, zoals RSA-beveiliging en ECC (elliptic curve cryptografie), die worden gebruikt voor versleuteling en digitale handtekeningen. Volgens de auteurs beginnen de risico's voor de huidige cryptografie vandaag al. Beveiligde data kan al onderschept worden en dan vanaf Q-Day met een quantumcomputer worden ontcijferd. Daarom moeten organisaties die werken met belangrijke versleutelde informatie – zoals staats- of bedrijfsgeheimen - nu al beginnen met de overstap naar een quantumveilige omgeving. Het handboek helpt risico's te identificeren en geeft concrete stappen om te werken aan een migratiestrategie.

GERELATEERDE ARTIKELENG

Nieuws • Encryptie

Justitie-minister zet toegang tot versleutelde berichten voor politie nog niet uit het hoofd

Kabinet kijkt naar Brussel, om in Europees verband te zoeken naar oplossingen voor tóch toegang tot versleutelde berichten.

🕒 2 min💬 1

Achtergrond • Digitalisering PRO

Nederlandse zorgen over digitale leiderschapspositie

Terechte zorgen? Of een kwestie van vooruitzien en actie ondernemen?

🕒 6 min

Blik op tech • Computing in de toekomst PRO

Hoe zit het met al die varianten van kwantumcomputing?

AG Connect maakt je wegwijs in de verschillende stromingen.

🕒 2 min💬 1

PQC en QKD

De meest veelzijdige en volledige oplossing wordt post-quantumcryptografie (PQC) genoemd en kan worden ingezet om huidige systemen en computers te beveiligen tegen aanvallen met quantumcomputers. Een andere, gedeeltelijke oplossing heet quantum key distribution (QKD). De migratie van quantumkwetsbare cryptografie naar PQC is een kostbaar en tijdrovend proces. In augustus 2024 werden de eerste PQC-standaarden gepubliceerd door het Amerikaanse National Institute of Standards and Technology (NIST), waarmee de volgende fase in de PQC-migratie aanbrak.

Stappenplan

Het handboek volgt een driestappenplan om de quantumdreiging te mitigeren: (1) diagnose van quantumkwetsbaarheid, (2) planning en (3) uitvoering. De eerste stap bevat een aantal "no-regret"-maatregelen die de cyberweerbaarheid van een organisatie vergroten, zelfs los van de quantumdreiging. Met deze maatregelen kunnen organisaties hun cryptografie effectiever beheren en cryptografische veranderingen soepeler doorvoeren. Goed cryptografisch beheer vergemakkelijkt het identificeren en oplossen van risico's en verkort de reactietijd in het geval van een incident, ook als dit incident niet gerelateerd is aan quantumcomputers.

GERELATEERDE ARTIKELENG

Nieuws • Microsoft Ignite, Technologie Partner

Vier dagen Microsoft Ignite in vier minuten: Onze belangrijkste bevindingen

Ontdek de nieuwste AI, data security en Azure innovaties van Microsoft Ignite 2024!

🕒 2 min

Blog • Copilot Partner

Aan de slag met Microsoft 365 Copilot

Ontdek hoe Microsoft 365 Copilot je werk transformeert

🕒 1 min

Achtergrond • Applicatiebeheer Partner

Vijf redenen om je applicatiebeheer te moderniseren

Het moderniseren van applicatiebeheer is niet langer een luxe, maar noodzaak. Waarom? en hoe kom je daar?

🕒 4 min

MEER WHITEPAPERS

Whitepaper • Artificial Intelligence

Infographic: Is jouw organisatie AI-proof?

Hoe integreer je AI in je bedrijfsvoering? Deze infographic toont de belangrijkste stappen om een AI-proof organisatie te worden.

Whitepaper • Cloud

Praktische handleiding voor een succesvolle cloud migratie

Welke aandachtspunten zijn cruciaal voor een succesvolle cloudmigratie? Dit whitepaper biedt handvatten voor een soepele transitie.

Whitepaper • Datamanagement

Data-soevereiniteit: zorgen voor dataveiligheid over de grenzen heen

Ontdek hoe u data naar uw regio's brengt en de beveiliging waarborgt.

MEER WHITEPAPERS →

In concrete zin is het advies aan alle organisaties om te beginnen met een zogenaamde cryptografische inventarisatie, om tot een overzicht te komen van welke cryptografie er gebruikt wordt. Ten tweede dienen organisaties een risicobeoordeling voor de quantumdreiging uit te voeren en deze te integreren in hun bestaande risicobeheerprocedures.

PQC-migratie

Ten slotte moet elke organisatie haar beleid omtrent cryptografie herzien en bijwerken op basis van de veranderende wet- en regelgeving. Deze informatie zal duidelijk maken hoe een organisatie zich moet positioneren ten opzichte van de PQC-migratie. Daarnaast wordt met de beschikbaarheid van deze informatie ook het risico op een overhaaste, foutgevoelige migratie verkleind, wat onnodige kosten en risico's in de toekomst kan voorkomen.

Reacties

Bold_italic_

Typ uw reactie

Plaats reactie