

COMPUTABLE *Techwire*
PLAATS ZELF UW PERSBERICHTEN ONLINE



KLIK HIER



Van links naar rechts: Bas Dunnebier (AIVD), Zsolt Szabó (staatssecretaris voor Digitale Zaken en Koninkrijksrelaties), Ton de Kok (CWI) en Maarten Tossings (TNO). Foto: TNO.

Handboek voor quantumveilige cryptografie vernieuwd

17 DECEMBER 2024 - 12:03 | ACTUEEL | INNOVATIE & TRANSFORMATIE | AIVD | CWI | MINISTERIE VAN BZK | TNO



Alfred Monerie

AIVD, CWI en TNO hebben het vernieuwde handboek voor quantumveilige cryptografie uitgebracht. De uitgave helpt organisaties om zich voor te bereiden op Q-Day, de dag waarop quantumcomputers bepaalde veelgebruikte cryptografie kunnen kraken. Die ontwikkeling staat nu al te gebeuren.

De [tweede editie](#) bevat de laatste ontwikkelingen en adviezen voor de overstap naar een quantumveilige omgeving. Het geeft advies over het vinden van cryptografische componenten en het beoordelen van quantumrisico's. Ook bevat het stappen om te werken aan een migratiestrategie.

Het handboek is tijdens het Symposium Post-Quantum Cryptography in Den Haag overhandigd aan staatssecretaris Zsolt Szabó (Digitale Zaken en Koninkrijksrelaties). Een van de hoofdonderwerpen van die dag was de ontwikkeling van een Europese roadmap om de Europese digitale infrastructuur quantumveilig te maken. Dat moet leiden tot een gecoördineerde transitie, met aandacht voor interoperabiliteit, standaarden en kennisdeling binnen Europa. Nederland speelt hierin een leidende rol, samen met Duitsland en Frankrijk.

Cryptografie wordt gebruikt om gegevens te beschermen die niet leesbaar mogen zijn door anderen. Toch is niet elke vorm van cryptografie veilig tegen aanvallen met quantumcomputers. Mogelijk vindt Q-Day al plaats in de komende vijf tot vijftien jaar, aldus [sommige experts](#).

Kwaadwillenden, zoals vijandige statelijke actoren, kunnen dan bepaalde hedendaagse cryptografie grotendeels omzeilen. Dan gaat het bijvoorbeeld om een asymmetrisch encryptiealgoritme-beveiliging en *elliptic curve*-cryptografie, die worden gebruikt voor versleuteling en digitale handtekeningen. Beveiligde data zijn evenwel te onderscheppen en dan vanaf Q-Day met een quantumcomputer te ontcijferen.

Daarnaast duurt het overstappen op nieuwe cryptografie soms wel tien jaar of langer. Vandaar dat organisaties die werken met versleutelde informatie zoals staatsgeheimen nu al bezig moeten zijn met de overstap naar een quantumveilige omgeving

More about

CRYPTOGRAFIE | QUANTUM

Share



Read more



ACTUEEL | INNOVATIE & TRANSFORMATIE

Meer digitale samenwerking om nieuwbouw te versnellen



ACTUEEL | DATA & AI

Design-ai-leerd: Hoe ver is Nederland met adoptie van ai?



ACTUEEL | INNOVATIE & TRANSFORMATIE

Navo kiest Nederlandse startups voor innovatieprogramma



OPINIE | CARRIÈRE

Gerust groeien: cruciale it-denkstappen (3) voor startups



ACTUEEL | CARRIÈRE

OU benoemt Bromuri tot hoogleraar Software Engineering en AI



ACHTERGROND CARRIÈRE

Directeur Qutech enthousiast over nieuwe quantumchip Google

Geef een reactie

Je moet [inloggen](#) om een reactie te kunnen plaatsen.

Populaire berichten

- Reorganisatie bij Centric leidt tot verlies van 350 arbeidsplaatsen →
- Rijk huurt onverminderd externe it'ers in →
- Sanderink bijna failliet (hoewel fortuin op hem wacht) →
- Twitter versus het UWV – wie te vertrouwen? →
- Hoe Rodeo-oprichter Pieter Vos uit het zadel viel →

[More articles](#) >

Uitgelicht



PARTNERARTIKEL

ADVERTORIAL | INNOVATIE & TRANSFORMATIE

Digitale Bibliotheek voor de Nederland...

IT maakt cultureel erfgoed toegankelijker dan ooit. De Digitale Bibliotheek voor de Nederlandse Letteren (DBNL) heeft op dit vlak een bijzondere mijlpaal bereikt. Ze heeft namelijk van de Stichting De...

Direct naar	Producten	Contact	Social
Kennisbank	Adverteren en meer...	Colofon	Facebook
Planning	Jouw Producten en Bedrijfsprofiel	Computable en de AVG	X
Computable Awards	Whitepapers & Leads	Service & contact	LinkedIn
Magazine	Vacatures & Employer Branding	Inschrijven nieuwsbrief	YouTube
Abonneren Magazine	Persberichten	Inlog	Instagram
Cybersec e-Magazine			