

WITOLD KEPINSKI - 04 JANUARI 2025

Deel dit artikel



AIVD, CWI en TNO publiceren vernieuwd handboek voor quantumveilige cryptografie

Om organisaties voor te bereiden op Q-Day, de dag waarop quantumcomputers bepaalde veelgebruikte cryptografieën kunnen kraken, publiceren de Algemene Inlichtingen- en Veiligheidsdienst (AIVD), Centrum Wiskunde & Informatica (CWI) en TNO een vernieuwd handboek voor quantumveilige cryptografie.

Quantum computing

Quantum technologie

Security

Cybersecurity

Overheid



Deze uitgebreide tweede editie bevat de laatste ontwikkelingen en adviezen voor de overgang naar een quantumveilige omgeving, waaronder concretere adviezen over het vinden van cryptografische activa, het beoordelen van quantumrisico's en het opzetten van cryptografische wendbaarheid. Het werd aangeboden aan de staatssecretaris voor Digitale Zaken en Koninkrijksrelaties, Zsolt Szabó, tijdens het 'Post-Quantum Cryptography'-symposium in Den Haag.

Cryptografie wordt gebruikt om data te beschermen die voor anderen niet toegankelijk zou moeten zijn. Echter, niet elke vorm van cryptografie is veilig tegen aanvallen van quantumcomputers. De AIVD waarschuwt al sinds 2014 dat Q-Day in 2030 zou kunnen plaatsvinden. Kwaadwillende actoren, zoals vijandige statelijke actoren, zouden dan bepaalde hedendaagse cryptografie grotendeels kunnen omzeilen. Denk hierbij aan RSA-beveiliging en ECC (elliptic curve cryptography), die worden gebruikt voor encryptie en digitale handtekeningen. Beveiligde data kan vandaag de dag worden onderschept en vervolgens vanaf Q-Day worden ontcijferd met een quantumcomputer.

PQC methode

Bovendien kan de overgang naar nieuwe cryptografie tien jaar of langer duren. Daarom moeten organisaties die met belangrijke gecodeerde informatie werken, zoals staats- of bedrijfsgeheimen, al bezig zijn met de overgang naar een quantumveilige omgeving. Dit handboek helpt organisaties risico's te identificeren en biedt concrete stappen om te werken aan een migratiestrategie, die gebruikmaakt van de knowhow die is opgedaan sinds de eerste editie.

Ook worden praktijkervaringen rondom de migratie gedeeld en is er aandacht voor de nieuwe adviestool [PQChoiceAssistant](#), die bedrijven helpt bij het kiezen van een PQC methode.

De AIVD kijkt altijd vooruit naar technologieën die voor Nederland van belang kunnen worden. De AIVD kijkt onder andere naar (het veilig gebruik van) post-quantumcryptografie.

[Lees het handboek hier.](#)

Tip de redactie

MEER OVER QUANTUM COMPUTING



► Video - Redactie - 18-12-2024

De trends volgens Pinewood: AI, quantum en aanvallen op wachtwoorden

SECURITY, DATA PROTECTION, INNOVATION, ARTIFICIAL INTELLIGENCE, QUANTUM COMPUTING



► Nieuws - Witold Kepinski - 17-12-2024

Eurofiber werkt met Quantum Bridge en Juniper Networks rond Quantum-veilige infrastructuur

QUANTUM COMPUTING, NETWERKEN, NETWORKING, INFRASTRUCTUUR, CONNECTIVITY



► Nieuws - Wouter Hoeffnagel - 13-12-2024

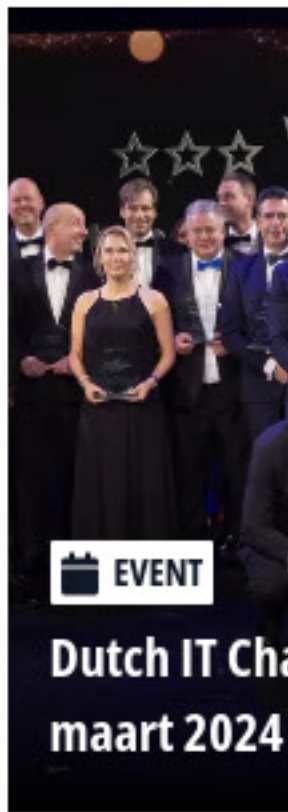
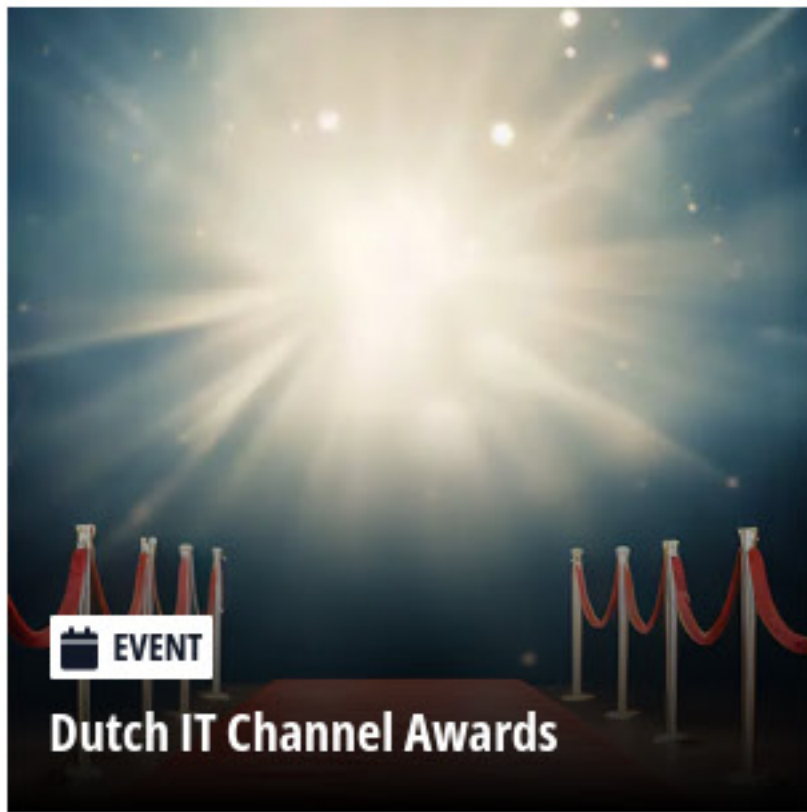
SoftwareOne: 2025 AI leidt in 2025 tot meer duurzaamheid en snelle ontwikkelingen

STORAGE, INNOVATION, SUSTAINABLE, ARTIFICIAL INTELLIGENCE, QUANTUM COMPUTING

Alles over Quantum Computing

DUTCH IT EVENTS

Alle events



OVER WITOLD KEPINSKI



Witold Kepinski (1969) is Bestuurder, Editor-in-Chief en Director Content van Dutch IT Channel en Dutch IT Leaders. Witold Kepinski is 25 jaar actief in de IT Media en Tech Business branche

Witold Kepinski geeft met een gespecialiseerd team van redacteuren, bloggers en videomakers inzicht in tech business trends en toepassingen waarmee IT-beslissers en Channel Partners impact maken.

Auteur pagina

Naam

Bedrijf

E-mailadres

Versturen

PROJECTEN

HR & Talent
Cultuur & Leiderschap
Future & Innovation
Sustainability & MVO

DUTCH IT LEADERS

Alle evenementen
Magazines
Partner en Content mogelijkheden
Ons team
Colofon
Tip De Redactie

ONZE SAMENWERKINGEN

Canalys
Cloudlunch
Gartner
NL Digital
Smart Profile

NIEUWSBRIEF ONTVANGEN?

Naam

Bedrijf

E-mailadres

Versturen

CONTACT

Dutch IT Media
Nieuwe Parklaan 17
2597 LA Den Haag
redactie@dutchitchannel.nl
[Per mail](#)

VOLG ONS OP

