AIVD, CWI en TNO publiceren vernieuwd handboek voor quantumveilige cryptografie

Nieuwsbericht | 03-12-2024 | 12:20

Om organisaties voor te bereiden op Q-Day, de dag dat quantumcomputers in staat zijn om bepaalde veelgebruikte cryptografie te breken, publiceren de Algemene Inlichtingen- en Veiligheidsdienst (AIVD), Centrum Wiskunde & Informatica (CWI) en TNO een vernieuwd handboek voor quantumveilige cryptografie. Deze uitgebreide tweede editie bevat, onder andere, 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 inrichten van cryptografische wendbaarheid. Tijdens het Symposium 'Post-Quantum Cryptography' in Den Haag is het overhandigd aan de Staatssecretaris voor Digitale Zaken en Koninkrijksrelaties Zsolt Szabó.

Beeld: ©AIVD

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. De AIVD waarschuwt al sinds 2014 dat Q-Day kan plaatsvinden in 2030. Kwaadwillenden, zoals vijandige statelijke actoren, kunnen dan bepaalde hedendaagse cryptografie grotendeels omzeilen. Dan gaat het bijvoorbeeld om RSA-beveiliging en ECC (elliptic curve cryptografie), die worden gebruikt voor versleuteling en digitale handtekeningen. Maar de risico's voor de huidige cryptografie beginnen vandaag al. Beveiligde data kunnen nu onderschept worden en dan vanaf Q-Day met een quantumcomputer worden ontcijferd.

Daarnaast duurt het overstappen op nieuwe cryptografie soms wel tien jaar of langer. Vandaar dat organisaties die werken met belangrijke versleutelde informatie – zoals staats- of bedrijfsgeheimen - nu al bezig moeten zijn met de overstap naar een quantumveilige omgeving. Dit handboek helpt organisaties om risico's te identificeren en geeft concrete stappen om te werken aan een migratiestrategie, waarbij gebruik wordt gemaakt van de kennis die sinds de eerste druk is opgedaan.

Verder worden er praktische ervaringen rondom de migratie gedeeld én bevat het de nieuwe adviestool PQChoiceAssistant die bedrijven helpt bij hun keuze van PQC methode.

De AIVD kijkt altijd vooruit naar technologieën die belangrijk voor Nederland kunnen worden. De AIVD onderzoekt onder meer (het veilige gebruik) van post quantum crypografie.

Documenten

- Het PQC-migratie handboek

  Dit handboek ondersteunt organisaties met concrete stappen en advies om de dreiging van quantumcomputers voor cryptografie te ...

  Publicatie | 03-12-2024

Zie ook

- Informatiebeveiliging
  Onderwerp
- Cyberdreiging
  Onderwerp