Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal
Postbus 20018
2500 EA Den Haag

Ons kenmerk
9d7ec029-or1-1.1

Uw kenmerk

Bijlagen
1

Datum 20 januari 2025
Betreft Vernieuwd handboek voor quantumveilige cryptografie

Hierbij bied ik u, mede namens de staatssecretaris Digitalisering en Koninkrijksrelaties, het vernieuwde handboek voor de migratie naar quantumveilige cryptografie aan. Dit PQC-migratiehandboek is uitgebracht door de AIVD, Centrum Wiskunde & Informatica (CWI) en TNO op 3 december 2024.

Een belangrijke aanleiding voor het verschijnen van de nieuwe editie van het handboek is de publicatie van internationaal omarmde standaarden voor post-quantum cryptografie (PQC) in augustus 2024. Deze standaarden geven organisaties de mogelijkheid om quantumveilige cryptografie concreet in te zetten. De adviezen en migratiestrategieën in het PQC-migratiehandboek zijn geactualiseerd op basis van deze standaarden.

Het handboek bevat adviezen om in drie stappen de migratie naar quantumveilige cryptografie uit te voeren: Inventarisatie, Planning en Uitvoering. Deze uitgebreide tweede editie bevat de nieuwste ontwikkelingen en concrete adviezen voor de overstap naar een quantumveilige omgeving. Ook zijn “no-regret moves” beschreven die de informatiebeveiliging van een organisatie altijd ten goede komen.

Dit handboek helpt organisaties om risico’s te identificeren en geeft actiegerichte stappen om te werken aan een migratiestrategie, waarbij gebruik wordt gemaakt van de kennis die sinds de eerste druk is opgedaan. De inzichten uit het PQC-migratiehandboek zullen worden meegenomen in de migratie van de Rijksoverheid naar PQC, onder het programma Quantumveilige Cryptografie Rijk.

De minister van Binnenlandse Zaken en Koninkrijksrelaties,

J.J.M. Uitermark