Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

Nationaal Coördinator Terrorismebestrijding en Veiligheid
Afdelingen Cybersecurity en Weerbaarheid tegen Statelijke Dreigingen en Economische Veiligheid

Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.rijksoverheid.nl/jenv

Datum
28 november 2025

Onze referentie
XXXX

Bijlage(n)
1

nota

Kamerbrief: uitvoering moties Rajkowski c.s. en Chakor c.s. inzake digitale weerbaarheid

1. Aanleiding

Middels de bijgevoegde Kamerbrief informeert u de Kamer over de uitvoering van de moties van de leden Rajkowski (VVD) en c.s., Chakor (PvdA-GL) inzake digitale weerbaarheid. Aangezien de moties inhoudelijk verband met elkaar houden, wordt de Kamer in eenzelfde brief geïnformeerd over de uitvoering van deze moties.

2. Geadviseerd besluit

U wordt gevraagd in te stemmen met bijgevoegde Kamerbrief en deze aan de TK te verzenden.

3. Kernpunten

- Met bijgaande Kamerbrief wordt uitvoering gegeven aan een drietal moties:
    - De motie van het lid Rajkowski c.s. die het kabinet verzocht in kaart te brengen in hoeverre (analoge) terugvalopties nodig zijn voor het versterken van onze (digitale) weerbaarheid[1] en de motie van het lid Chakor c.s. die verzocht om plannen te ontwikkelen met overheden en vitale sectoren om essentiële dienstverlening in geval van grootschalige digitale storing zo veel mogelijk in stand te houden.[2] Met de inwerkingtreding van de Cyberbeveiligingswet (Cbw) en de Wet weerbaarheid kritieke entiteiten (Wwke) in Q2 2026 zullen kritieke entiteiten wettelijk verplicht zijn om een risicobeoordeling uit te voeren, op basis waarvan zij passende en evenredige technische, operationele en organisatorische maatregelen nemen voor de beveiliging van hun netwerk- en informatiesystemen die worden gebruikt voor de verlening van hun diensten. Ook moeten zij maatregelen nemen om incidenten te voorkomen of de gevolgen van incidenten te beperken, waaronder het in kaart brengen van (analoge) terugvalopties ten behoeve van de bedrijfscontinuïteit.
    - De motie van het lid Rajkowski c.s., waarin het kabinet werd opgeroepen tot het uitvoeren van een scan van apparatuur of programmatuur uit landen met een tegen Nederland gerichte offensieve cyberagenda die aanwezig is binnen (de kernsystemen van) de vitale sector. Naar aanleiding hiervan heeft TNO een verkenning uitgevoerd onder vitale aanbieders om te bezien in hoeverre zij afhankelijk zijn van leveranciers uit risicolanden. Op basis van deze verkenning is een zelfscantool ontwikkeld waarmee vitale aanbieders risico's kunnen afwegen die samenhangen met apparatuur en programmatuur uit landen met een offensief

[1] Kamerstukken II 2022/23, 26643, nr. 830.
[2] Kamerstukken II 2024/25, 26643, nr.1256.

Nationaal Coördinator Terrorismebestrijding en Veiligheid
Directie Cybersecurity en Weerbaarheid tegen Statelijke Dreigingen

Datum
28 november 2025

Onze referentie
XXX

cyberprogramma. Op 30 mei 2023 is tevens met uw Kamer gedeeld dat risico's bij inkoop- en aanbestedingen en strategische afhankelijkheden van producten en diensten - en de mogelijke invloed van buitenlandse partijen op een vitaal proces die daaruit kan voortvloeien – integraal onderdeel uitmaken van de weerbaarheidsanalyse. Alle vitale processen zullen deze weerbaarheidsanalyses doorlopen.[3]
    - Over het deel van de motie van Rajkowski (VVD) c.s. dat oproept om een scan te maken over hoe apparatuur en programmatuur van organisaties uit landen met een tegen Nederland gerichte offensieve cyberagenda geweerd kan worden uit aanbestedingen van de rijksoverheid is uw Kamer op 17 april 2023 geïnformeerd.[4]
- In het licht van het huidige dreigingsbeeld zal de uitwerking van de algemene zorgplicht van de Cbw en Wwke de mogelijkheid bevatten om een kritieke entiteit de verplichting op te leggen om producten of diensten van specifieke leveranciers te weren.

4. Politieke context

Tijdens de procedurevergadering van de VKC Digitale Zaken van 25 september 2024 heeft de commissie besloten dat zij zich tijdens een technische briefing nader wil laten informeren, nadat de Kamer per brief is geïnformeerd over beide moties van het lid Rajkowski c.s. Deze nog in te plannen technische briefing zal vertrouwelijk van aard zijn.

5. Informatie die niet openbaar gemaakt kan worden

In de openbaar gemaakte versie van deze nota zijn alle persoonsgegevens van ambtenaren geanonimiseerd.

[3] Kamerstukken II 2022/23, 30821, nr. 182.
[4] Kamerstukken II 2022/23, 26643, nr. 1007.