Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

Minister van Justitie en Veiligheid

Programma Nederland Digitaal Veilig

Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl

Datum
26 juni 2023

Ons kenmerk
4179114

Dossiernummer
tbd

nota

Beslisnota bij Kamerbrief uitkomsten verkenning verdergaande samenwerking NCSC, DTC en CSIRT-DSP

Algemene leiding	
Minister	SG
Datum/eindparaaf	Datum/paraaf

1. Aanleiding

Bijgevoegde brief informeert de Kamer over de voortgang van de integratie van het Nationaal Cybersecurity Centrum (NCSC) van het Ministerie van Justitie en Veiligheid (J&V), het Digital Trust Center (DTC) van het Ministerie van Economische Zaken en Klimaat (EZK) en het Cyber Security Incident Response Team voor digitale dienstverleners (CSIRT-DSP), eveneens van EZK. Dit is conform de toezegging tijdens het commissiedebat Digitale Zaken van 15 december 2022 dat het kabinet de Kamer hierover zou informeren voor de zomer. Daarnaast biedt u met deze brief het rapport 'Beleidskader herinrichting Computer Security Incident and Respons Team (CSIRT) stelsel' aan. De brief wordt mede ondertekend door de Minister van Economische Zaken en Klimaat.

2. Geadviseerd besluit

Het advies is kennis te nemen van de voortgang van de integratie en in te stemmen met het toesturen van de brief aan de Tweede Kamer en het aanbieden van het rapport 'Beleidskader herinrichting CSIRT stelsel'.

3. Kernpunten

- Eerder zijn de uitkomsten van verkenning naar verdergaan samenwerking tussen NCSC, DTC en CSIRT-DSP gedeeld met de Tweede Kamer. Uit deze verkenning kwam naar voren dat een integratie van deze drie organisaties tot één gezamenlijke organisatie de cyberweerbaarheid van Nederland verhoogt.
- In de Nederlandse Cybersecurity Strategie (NLCS) is de ambitie uitgesproken om deze vernieuwde organisatie daadwerkelijk op te richten en toe te werken naar een volledige integratie van de drie organisaties.
- Door deze integratie zal de vernieuwde organisatie efficiënter en effectiever te werk kunnen gaan, met behoud van de doelgroep-kennis. Door één organisatie te vormen zal het voor doelgroep organisaties duidelijker zijn waar zij terecht kunnen voor expertise en steun.

- De organisatie wordt zo vormgegeven dat ze meer onafhankelijk en met meerdere opdrachtgevers kan werken aan de digitale weerbaarheid van de Nederlandse maatschappij en het bedrijfsleven.
- De minister van Justitie en Veiligheid wordt eigenaar van de nieuwe organisatie en beleidsafdelingen binnen JenV en EZK worden de opdrachtgevers. Op termijn zal ook het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) naar alle waarschijnlijkheid als opdrachtgever bij de algemene aansturing van de nieuwe organisatie worden betrokken.
- Bij het uitwerken van de kaders voor de vernieuwde organisatie wordt daarnaast rekening gehouden met het feit dat er na de implementatie van de Europese Network and Information Security (NIS2) richtlijn, andere departementen ook de rol van opdrachtgever zullen gaan vervullen wanneer zij er voor kiezen om de sectorale CSIRT taken uit de NIS2 richtlijn door het NCSC te laten uitvoeren.

- In de transitie worden twee fases onderscheiden: de initiële fase tot eind 2024 en de optimalisatiefase die loopt tot begin 2026. Na afronding van de initiële fase dient bereikt te zijn dat de vernieuwde organisatie de hoofdtaken in samenhang en in voldoende mate kan uitvoeren. De hoofdtaken zijn:
    - **Nationaal Computer Security Incident Response Team (Nationaal CSIRT)** - Als Nationaal CSIRT verzamelt en analyseert, verrijkt en distribueert de nieuwe organisatie, in samenwerking met publieke en private partners en in zowel nationaal als internationaal verband, informatie en data over cyberdreigingen, -kwetsbaarheden, -incidenten en trends en ontwikkelt handelingsperspectieven voor alle organisaties in Nederland.
    - **Kennis- en adviescentrum-** Als kennis- en adviescentrum voor digitale weerbaarheid verbindt de nieuwe organisatie eigen kennis met die van andere deskundige organisaties (zoals inspecties en de veiligheidsdiensten) en zet deze om in praktisch toepasbare algemene preventieadviezen, handreikingen en instrumenten
    - **Uitvoeringscoördinator in het cybersecuritystelsel -** Als uitvoeringscoördinator voert de nieuwe organisatie het operationeel beheer van een landelijk cybersecuritystelsel van sectorale CSIRTs, publieke en private partners, departementen en andere relevante partijen dat in samenwerking de digitale weerbaarheid van organisaties in Nederland helpt te bevorderen.
    - **Sectoraal Computer Security Incident Response Team (Sectoraal CSIRT)-** Als sectoraal CSIRT voert de nieuwe organisatie regie en coördinatie op sectoraal niveau op verzoek van het verantwoordelijke vakdepartement.
- In de periode tot 2026 worden de taken en processen vervolgens volledig geïntegreerd en geoptimaliseerd. De digitale infrastructuur, nodig voor een optimale uitvoering van alle taken, is dan ook ontwikkeld en in gebruik genomen.
- Er wordt momenteel een transitie manager aangesteld die het overkoepelende proces tot begin 2026 zal leiden. Hier zal een stuurgroep waar de PSG JenV, PSG EZK, pNCTV en de directeur Digitale Economie op sturen.

4. Toelichting

4.1 Politieke context

In het Coalitieakkoord is aangegeven: "We beschermen onze bedrijven, vitale infrastructuur en economisch kapitaal beter door centraal gecoördineerde structurele samenwerking tussen onder andere het Nationaal Cyber Security Centrum (NCSC), het Digital Trust Center (DTC), overheden, bedrijven en wetenschappers. Zij kunnen sneller en makkelijker informatie delen over digitale kwetsbaarheden en 'hacks'". Met de integratie wordt invulling gegeven aan de wens voor centraal gecoördineerde dienstverlening. Tevens sluit het aan bij de wens van de Tweede Kamer om te komen tot meer efficiëntie en minder versnippering in het cybersecurity stelsel.

4.2 Financiële overwegingen

Beleidskeuze uitgelegd Onderbouwing doeltreffend, doelmatig en evaluatie (CW 3.1)	
1. Doel	Betere dienst- en hulpverlening t.a.v. digitale veiligheid te realiseren voor organisaties in Nederland en efficiëntieslag te slaan door de drie organisaties te laten integreren.
2. Beleidsinstrument(en)	Er is gestart met het samenvoegen van de organisaties. Er worden o.a. nieuwe digitale systemen ontwikkeld, mensen geworven.
3A. Financiële gevolgen voor het Rijk	Geen additionele claim. Integratie vindt plaats binnen de bestaande financiële kaders.
3B. Financiële gevolgen voor de maatschappelijke factoren	Naar verwachting zal integratie er voor zorgen dat doelgroeporganisaties beter worden bijgestaan en de Nederlandse maatschappij beter wordt beschermd tegen digitale risico's zoals cybercriminaliteit of uitval.
4. Nagestreefde doeltreffendheid	De drie organisaties staan momenteel nog te ver van elkaar af. Daarbij is het DTC nog onderdeel van een beleidsafdeling van EZK. Omdat het in principe een uitvoeringsorganisatie betreft, is het wenselijk dat deze organisatie op afstand van haar beleidsbepalers staat. Om deze reden is het NCSC ook al eerder afgesplitst van de NCTV. De integratie van deze drie organisaties zal leiden tot effectievere en efficiëntere dienstverlening vanuit de overheid op het gebied van digitalisering. Hierbij

	kan o.a. gedacht worden aan: informatie uitwisseling, bijstand, het doen van meldingen.
5. Nagestreefde doelmatigheid	Door het samenvoegen van de drie organisaties zal er minder tijdsverlies plaatsvinden wanneer informatie tussen de organisaties moet worden gedeeld. Daarnaast kan de schaarse capaciteit effectiever worden ingezet en kunnen er schaalvoordelen bereikt worden. Daarnaast wordt een efficiëntiewinst verwacht op het gebied van bedrijfsvoering, huisvesting en ICT.
6. Evaluatieparagraaf	De voortgang op het voorstel zal ieder jaar worden geëvalueerd door middel van de monitoringsrapportage van de nieuwe Nederlandse cybersecurity strategie (NLCS). Daarnaast zal deze beleidskeuze worden geëvalueerd bij de brede NLCS evaluatie.

4.3 Juridische overwegingen
Onderdeel van het transitieproces is beoordelen of de huidige wettelijke kaders passen bij de taken en verantwoordelijkheden van de vernieuwde organisatie. De momenteel lopende wetgevingstrajecten - te weten de implementatie van de NIS2 in de Wet beveiliging netwerk- en informatiesystemen en het Wetsvoorstel Bevordering digitale weerbaarheid bedrijven (Wbdwb) ten behoeve van het vastleggen van de taken van het DTC – zijn geen onderdeel van deze brief. De Kamer wordt hierover met aparte brieven geïnformeerd.

4.4 Strategie
De integratie van het DTC, NCSC en CSIRT-DSP is een belangrijke maatregel uit de Nederlandse cybersecuritystrategie (NLCS) om de versnippering in het Nederlandse cybersecuritylandschap tegen te gaan, een duidelijke organisatiestructuur voor burgers en bedrijfsleven te creëren en efficiënter inzet van de beschikbare capaciteit te bewerkstelligen.

4.5 Implementatie
Onder leiding van de transitiemanager vindt de implementatie plaats. De eerste fase van de implementatie is eind 2024 afgerond.

4.6 Communicatie
Externe stakeholders zullen rond het moment van het uitgaan van de Kamerbrief worden geïnformeerd op een NLCS stakeholderdag. Deze staat gepland op 28 juni 2023. Een ander belangrijk element is de interne communicatie richting de betrokken medewerkers. Dit is een belangrijke prioriteit voor de transitiemanager.

5. Informatie die niet openbaar gemaakt kan worden
Niet van toepassing.