Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2022–2023

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 1058

BRIEF VAN DE MINISTERS VAN JUSTITIE EN VEILIGHEID EN VAN ECONOMISCHE ZAKEN EN KLIMAAT

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 26 juni 2023

Het belang van een digitaal weerbare samenleving is door dit kabinet al meermaals onderstreept. In de Nederlandse Cybersecurity Strategie (NLCS) is aangegeven dat dit belang zo groot is dat het realiseren van deze weerbaarheid niet alleen een verantwoordelijkheid is van individuele organisaties, maar dat zij hierbij passende ondersteuning moeten krijgen vanuit de overheid. Om dit te bereiken heeft het kabinet onder andere besloten om de bestaande cybersecurity rijksoverheidsorganisaties, het Nationaal Cyber Security Centrum (NCSC) van het Ministerie van Justitie en Veiligheid (JenV) en het Digital Trust Center (DTC) en het Computer Security Incident Response Team voor digitale dienstverleners (CSIRT-DSP), beide van het Ministerie van EZK, te integreren in één nieuwe organisatie. Dit betekent dat er één centrale, zichtbare en effectieve organisatie komt die de nationale cybersecurityorganisatie wordt.

Doel van de integratie is om de versnippering in het cybersecuritystelsel tegen te gaan en de schaarse expertise zo efficiënt mogelijk in te zetten. Na de integratie kunnen alle organisaties in Nederland terecht bij één herkenbaar loket voor cybersecurityadvies, bijstand bij digitale incidenten en kan de nieuwe nationale cybersecurityorganisatie snel en adequaat reageren op dreigingen en incidenten op nationaal en sectoraal niveau. De eerste belangrijke stappen in de integratie zijn reeds gezet. De organisaties werken al zoveel mogelijk samen. Bijvoorbeeld door het gezamenlijk organiseren van het waarschuwen van slachtoffers en doelwitten van een cyberaanval en te komen tot één set van meest effectieve maatregelen voor alle organisaties in Nederland waardoor zij zich beter kunnen weren tegen aanvallers.

In deze brief informeren wij u conform toezegging in het Commissiedebat Digitale Zaken van 15 december jl. (Kamerstuk 26 643, nr. 961) over de voortgang van de integratie van het NCSC, DTC en CSIRT-DSP.

kst-26643-1058
ISSN 0921 - 7371
's-Gravenhage 2023

Stand van zaken

De afgelopen periode is in gezamenlijkheid van de betrokken organisaties gewerkt aan de opdracht en randvoorwaarden om de transitie naar één nationale cybersecurityorganisatie zorgvuldig te doorlopen, met aandacht voor de bestaande dienstverlening, medewerkers en stakeholders. Dit proces heeft bijgedragen aan wederzijds begrip van elkaars werkwijze en mogelijkheden tot synergie. Daarmee is een mooie stap gezet richting de toekomst. De Minister van JenV wordt de eigenaar van de vernieuwde organisatie. JenV en EZK vervullen samen de rol van opdrachtgever. De vernieuwde organisatie is dadelijk gefundeerd op de sterke eigenschappen van de huidige organisaties. Dit zal de vernieuwde organisatie in staat stellen om alle organisaties in Nederland, groot of klein, publiek of privaat, vitaal of niet-vitaal van passende informatie en kennis te voorzien en hulp te bieden bij incidenten.

De vernieuwde organisatie kent daarbij vier hoofdtaken:

1. Nationaal Computer Security Incident Response Team (CSIRT): als nationaal CSIRT verzamelt en analyseert, verrijkt en distribueert de vernieuwde 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.
2. Uitvoerend coördinator cybersecuritystelsel: als uitvoeringscoördinator voert de vernieuwde 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 alle organisaties helpt bevorderen.
3. Kennis- en adviescentrum: als kennis- en adviescentrum voor digitale weerbaarheid verbindt de vernieuwde organisatie eigen (verrijkte) kennis met die van andere deskundige organisaties (zoals inspecties en de veiligheidsdiensten) en zet deze om in praktisch toepasbare algemene preventieadviezen, handreikingen en instrumenten.
4. Sectoraal Computer Security Incident Response Team (CSIRT): als sectoraal CSIRT voert de vernieuwde organisatie regie en coördinatie op sectoraal niveau. Dit betreft vooral maar niet uitsluitend Network and Information Security (NIS2) richtlijn -sectoren waarvoor met de verantwoordelijke departementen is overeengekomen, dat de sectorale CSIRT-functie door de vernieuwde organisatie wordt ingevuld.[1]

De transitie zal gefaseerd verlopen zodat er zoveel mogelijk rekening gehouden kan worden met aankomende wetgeving en lopende trajecten uit de Nederlandse Cybersecurity Strategie (NLCS). Daarom worden in ieder geval twee fases onderscheiden: de initiële fase tot 1 oktober 2024 en de optimalisatiefase die loopt tot 1 januari 2026. Na afronding van de initiële fase dient bereikt te zijn dat de vernieuwde organisatie de hierboven genoemde hoofdtaken in samenhang en in voldoende mate kan uitvoeren. Daarbij moet in ieder geval uitvoering kunnen worden gegeven aan de Wet beveiliging en informatiesystemen (Wbni), inclusief de Europese Network and Information Security (NIS2) richtlijn, aan sectorale wetgeving waarbinnen CSIRT-taken worden verricht en, nadat deze is aangenomen, aan de Wet bevordering digitale weerbaarheid bedrijven (Wbdwb) die momenteel in uw Kamer ligt. De huidige organisaties voeren na de initiële fase geen eigenstandige koers meer en bestaan alleen nog in formele zin in hun huidige vorm. In de periode tot

[1] Dit betreft bijvoorbeeld de CSIRT taken uit de Europese Netcode voor de cybersecurity van grensoverschrijdende elektriciteitsstromen.

1 januari 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. De vernieuwde organisatie ontwikkelt zich in de optimalisatiefase van een tijdelijke werkorganisatie naar een geformaliseerd vernieuwde organisatie.

Tijdens het hele transitieproces wordt er al zoveel mogelijk gewerkt vanuit het perspectief van de nieuwe organisatie. Zo werken er momenteel al medewerkers uit de operatie van zowel het Digital Trust Center als het CSIRT-DSP samen met medewerkers van de operatie van het Nationaal Cyber Security Center om beter bekend te raken met elkaars werkzaamheden en de daarvoor gebruikte systemen. Daarnaast wordt er gekeken naar de ontwikkeling van gezamenlijke informatieproducten die relevant zijn voor vitale en niet-vitale organisaties en hoe winst kan worden behaald in de communicatie richting hen. Ook hebben de drie organisaties nu al handen in één geslagen voor het ontsluiten van informatie op het gebied van doelwit- en slachtoffernotificatie.[2]

Om de gehele transitie te realiseren wordt op dit moment een transitiemanager aangesteld. De transitiemanager zal de transitie coördineren en de voortgang van de transitieopdracht en bijkomende afspraken bewaken. De transitiemanager onderhoudt ook de afstemming met andere relevante wetgevings- en NLCS-trajecten.

Uw Kamer wordt periodiek geïnformeerd over de voortgang van de transitie. Dit zal in de rapportage over de voortgang van de NLCS gebeuren.

Naast bovenstaande ontwikkelingen willen wij u ten slotte ook graag informeren over de uitvoering van een andere actie uit het de Nederlandse cybersecuritystrategie (NLCS), namelijk de verkenning die is uitgevoerd naar het organiseren van de in de NIS2 vastgelegde CSIRT-taken. Door deze nieuwe richtlijn krijgen meer sectoren verplichtingen op het gebied van cybersecurity, zoals het nemen van beveiligingsmaatregelen om cyberbeveiligingsrisico's voor hun netwerk- en informatiesystemen te beheersen. Tegelijkertijd krijgt de overheid voor meer sectoren de verplichting om te adviseren over digitale dreigingen en indien nodig bijstand te verlenen.

Rapport beleidskader herinrichting Computer Security Incident Respons Team (CSIRT) stelsel

Het uitbrengen van de NLCS, het implementeren van de NIS2 en de bovenstaande integratie naar één nationale cybersecurity organisatie was mede aanleiding een verkenning te laten uitvoeren naar de (her)inrichting van het CSIRT-stelsel in Nederland. Het Ministerie van Justitie en Veiligheid heeft namens de vakdepartementen een onafhankelijke verkenning laten uitvoeren naar de vormgeving van een beleidskader voor het herinrichten van het CSIRT-stelsel met een nationale en sectorale CSIRTs, rekening houdend met de impact van de NIS2-richtlijn en sectorale cybersecuritywet- en regelgeving. De Minister van Justitie en Veiligheid biedt u dit rapport aan.

In het rapport worden scenario's geschetst met daarbij onder andere aandacht voor politieke verantwoordelijkheden van vakministers, uitvoerbaarheid en toekomstbestendigheid van het stelsel. Het rapport doet daarbij aanbevelingen over te hanteren uitgangspunten voor een

[2] Zie pagina 10 van het actieplan NLCS, bijlage bij Kamerstuk 26 643, nr. 925.

nieuw stelsel en stelt vervolgstappen voor om te komen tot implementatie. De uitkomsten van het rapport worden meegenomen in het implementatietraject van de NIS2 richtlijn. Over de precieze inhoud van de implementatiewetgeving en bijbehorende implementatiekeuzes, ook ten aanzien van de inrichting van het CSIRT-stelsel, zal uw Kamer bij de parlementaire behandeling van de wetsvoorstellen separaat worden geïnformeerd.

De concept implementatiewet zal naar verwachting in het najaar van 2023 in consultatie worden gebracht.

De Minister van Justitie en Veiligheid,
D. Yesilgöz-Zegerius

De Minister van Economische Zaken en Klimaat,
M.A.M. Adriaansens