Ministerie van Economische Zaken
en Klimaat

[redacted]

TER ADVISERING

Aan de Minister van Economische Zaken en Klimaat

Directoraat-generaal
Economie en Digitalisering
Directie Digitale Economie

Auteur
[redacted]

Datum
11 mei 2023

Kenmerk
DGED-DE / 27242521

Kopie aan
[redacted]

nota

Parafenroute
[redacted]

Bijlage(n)
1. BNC-fiche herziening CSA
2. BNC-fiche Cyber Skills Academy
3. BNC-fiche Cyber Solidarity Act

Aanleiding

De Europese Commissie heeft op 18 april een voorstel gepubliceerd voor een nieuw beleidspakket voor cybersecurity. Dit pakket bevat drie onderdelen: de Cyber Solidarity Act, een herziening van de Cybersecurity Act (CSA) en een mededeling over de Cyber Skills Academy (hierna: 'de Academie'). EZK is verantwoordelijk voor de coördinatie op en BNC-fiches over de herziening van de CSA en de mededeling voor de Cyber Skills Academy. Het ministerie van Justitie en Veiligheid is verantwoordelijk voor de Nederlandse inzet op de Cyber Solidarity Act.

In deze nota wordt u geïnformeerd over de inhoud en eerste appreciatie van de voorstellen, en over bijbehorend BNC-proces. Daarnaast wordt u gevraagd om in te stemmen met de door EZK opgestelde BNC-fiches. Het fiche dat is opgesteld door J&V over de Cyber Solidarity Act is ter informatie toegevoegd.

Advies

U wordt geadviseerd om in te stemmen met de BNC-fiches voor herziening van de CSA en voor de Cyber Skills Academy.

Kernpunten

- EZK is eerstverantwoordelijk ministerie voor de herziening van de CSA en voor de Cyber Skills Academy. Op 16 mei bespreekt het interdepartementaal BNC-overleg de bijbehorende fiches. Op 23 mei bespreekt de CoCo de fiches. De fiches zullen vervolgens geagendeerd staan tijdens de ministerraad van 26 mei, waarna ze worden verzonden naar de Eerste Kamer, Tweede Kamer en de Nederlandse Europarlementariërs.
- De herziening van de CSA en de mededeling voor de Cyber Skills Academy maken onderdeel uit van een breder pakket aan cybersecuritybeleid dat de Europese Commissie op 18 april naar buiten heeft gebracht. Naast de twee eerder genoemde voorstellen bevat dat pakket ook de Cyber Solidarity Act. Hiervoor is JenV het eerstverantwoordelijke ministerie.

Ontvangen BBR

- Ten aanzien van de herziening van de CSA staat het kabinet in beginsel positief tegenover het voorstel, maar is meer verduidelijking nodig over de noodzaak en afbakening van de geïntroduceerde nieuwe categorie voor cybersecuritycertificering.
- Het kabinet is in beginsel positief over de mededeling voor de Cyber Skills Academy. Wel heeft het kabinet kritische vragen over de samenwerking met andere EU-organisaties, de voorgestelde juridische basis en de aansluiting op generiek onderwijs- en arbeidsmarkt beleid van de Commissie.
- Het kabinet kijkt kritisch naar de grote hoeveelheid wet- en regelgeving die door de Commissie wordt opgesteld voor cybersecurity. Hoewel soms nodig, brengt dit aanzienlijke belasting met zich mee voor nationale partijen die de nieuwe initiatieven moeten beoordelen en implementeren. Voor goede implementatie van al aangenomen wetgeving moet voldoende capaciteit overblijven.

Toelichting

Herziening CSA

- Het voorstel betreft een wijziging op de Cyberbeveiligingsverordening (Cybersecurity Act, hierna: CSA) die in 2019 is gepubliceerd. Met het voorstel wordt het bestaande toepassingsgebied van het Europese cybersecuritycertificeringskader (ICT-producten, ICT-diensten en ICT-processen) verbreed met een categorie "beheerde beveiligingsdiensten".[1] Het doel hiervan is om de kwaliteit van aanbieders van beheerde beveiligingsdiensten te verbeteren en hun vergelijkbaarheid te vergroten door Europese certificeringschema's voor cybersecurity op te stellen.
- De Commissie stelt dat Europese certificering een doeltreffend middel is om vertrouwen op te bouwen in de kwaliteit van die diensten, en zo de opkomst van een betrouwbare Europese cyberbeveiligingsdienstensector te vergemakkelijken en bijdraagt aan het voorkomen van versnippering van de interne markt. Er zijn namelijk diverse lidstaten die zijn begonnen met de adaptatie van nationale certificeringsregelingen. De wijziging beoogt de werking van de interne markt te verbeteren en voorkomt fragmentatie.

[1] Dit zijn specifieke diensten die worden verleend door aanbieders van cyberbeveiligingsdiensten. Het gaat hierbij om respons op incidenten, penetratietests en beveiligingsaudits en -consultancy, om bedrijven en andere organisaties te helpen cyberincidenten te voorkomen, op te sporen, erop te reageren of te boven te komen.

- Het voorstel wijzigt verder niets aan werking van de CSA en blijft consistent met de Algemene verordening gegevensbescherming[2] (AVG). De wijziging verandert niets aan het vrijwillige karakter van de certificeringsregelingen. Het amendement volgt de vrijwilligheid van het verkrijgen van certificeringsschema's zoals nu vastgelegd is in de CSA. Het is echter niet ondenkbaar dit via andere regelgeving zoals bijvoorbeeld de NIB-2-richtlijn een verplicht karakter krijgt.
- In het BNC-fiche geven wij aan dat wij in beginsel positief staan tegenover het voorstel, omdat het zou kunnen bijdragen aan de kwaliteit van beheerde beveiligingsdiensten. Wel zijn er een aantal aandachtspunten:
    - Het is nog onvoldoende helder waarom er een nieuwe categorie te certificeren diensten geïntroduceerd wordt en hoe die precies zijn afgebakend. Diensten zoals pentesten en incidentenrespons die door de Commissie als beheerde beveiligingsdiensten worden aangemerkt, zouden mogelijk ook kunnen vallen onder de bestaande categorie ICT-diensten. Hierover moet de Commissie meer duidelijkheid geven.
    - Het risico bestaat dat het gebrek aan goede afbakening ertoe leidt dat onnodig veel diensten verplicht kunnen worden om een CSA-certificaat te verkrijgen, zonder zorgvuldige afweging met stijging van administratieve lasten voor bedrijven als gevolg hiervan.
- Het voorliggende voorstel is in behandeling genomen door het Europees Parlement en de Raad waarover nog in de vorm van raadswerkgroepen moet onderhandeld. De positie van het Europees Parlement op het voorstel is nog niet bekend. In het algemeen is het Europees Parlement voorstander van Europese geharmoniseerde certificeringsstelsel. Het voorstel wordt behandeld in het Committee on Industry Reseach and Energy (ITRE). De rapporteur is Josianne Cutajar (S&D).

Cyber Skills Academy

- Met het voorstel voor een Academie voor cybervaardigheden wil de Commissie het tekort aan gekwalificeerde cybersecurityprofessionals op de Europese arbeidsmarkt verkleinen. De EU moet kunnen beschikken over voldoende cybersecurityprofessionals om digitaal veilig te blijven. Het huidige tekort aan geschoolde professionals heeft een negatief effect op de Europese veiligheid en weerbaarheid, het concurrentievermogen en de economische groei.
- De Academie moet een centrale plek worden waar publieke initiatieven, private initiatieven en financiering voor cybersecurityonderwijs en trainingen bij elkaar komen. Succesvolle bestaande initiatieven kunnen via de Academie worden opgeschaald om hun impact te maximaliseren. De Academie kent vier pijlers: 1) kennisontwikkeling en training, 2) stakeholder betrokkenheid, 3) subsidies en 4) monitoring van de marktontwikkeling.

[2] Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (PbEU 2016, L 119).

- Het Nederlandse beleid op het gebied van cybersecurityonderwijs en -arbeidsmarkt wordt uiteengezet in de Nederlandse Cybersecuritystrategie 2022-2028 (hierna: NLCS) en het onderliggende Actieplan. Om de toenemende vraag naar cybersecurityexpertise het hoofd te bieden wordt ingezet op voldoende specialisten op de arbeidsmarkt. Daartoe heeft het kabinet drie subdoelen geïdentificeerd: 1) zicht op de tekorten op de cybersecurity-arbeidsmarkt en hoe deze het hoofd te bieden, 2) meer mbo-, hbo- en wo-cybersecurityopleidingsplekken die aansluiten op de arbeidsmarkt, mede door een bijdrage van bedrijven en kennisinstellingen, 3), bij- en omscholingsprogramma's voor cybersecurity-expertise, aangeboden door organisaties. Daarnaast wordt benadrukt dat internationale samenwerking in EU- en NAVO-verband en daarbuiten essentieel is gezien het grensoverschrijdende karakter van cyberdreigingen.
- Het kabinet onderschrijft de doelstelling van het voorstel om het tekort aan gekwalificeerde cybersecurityprofessionals op de Europese arbeidsmarkt te verkleinen. Dit is in lijn met de NLCS. Daarom staat het kabinet in beginsel positief tegenover de voorgestelde Cybersecurity Skills Academy. Wel heeft het kabinet een aantal aandachtspunten bij de mededeling:
    - Het kabinet heeft vragen over wat de verhouding tussen het Europese Cybersecurity Competence Center (ECCC), het Europees Agentschap voor Netwerk- en Informatiebeveiliging (ENISA) en de Commissieonderdelen verantwoordelijk voor generiek onderwijs- en arbeidsmarktbeleid zal zijn tijdens bij de opzet van de Academie.
    - De Commissie stelt voor om een nieuw instrument in te zetten om het juridische raamwerk voor de Academie vorm te geven (EDIC). Bij dit instrument wordt een beroep gedaan op een op te richten samenwerkingsverband tussen lidstaten voor de opzet en uitvoer van de Academie. Het kabinet verkent graag op EU-niveau wat de mogelijkheden zijn om aan te sluiten op een consortium met andere (gelijkgestemde) lidstaten.
    - Tot slot acht het kabinet het belangrijk om een aanpak van het arbeidsmarkttekort aan cybersecurityvaardigheden op een logische wijze aan te laten sluiten op Europees beleid met betrekking tot het bredere tekort aan voldoende gekwalificeerde ICT-professionals.
- In algemene zin onderschrijven alle EU-lidstaten de doelstelling om het tekort aan gekwalificeerde cybersecurityprofessionals op de Europese arbeidsmarkt verkleinen. In het verlengde daarvan zullen veel lidstaten naar verwachting in beginsel het voorstel voor de Academie ondersteunen. De verwachting is wel dat een aantal lidstaten zich kritisch zal uitspreken over verschillende onderdelen van het initiatief.

- De grondhouding van het kabinet met betrekking tot de bevoegdheid, de subsidiariteit en de proportionaliteit van de mededeling is positief. De financiële gevolgen en regeldruk lijken beperkt doordat de budgetten voor de Academie reeds geoormerkt zijn in het Europese subsidieprogramma. Wel heeft het kabinet vragen over de daadwerkelijke impact die dit initiatief teweeg zal brengen.

Cyber Solidarity Act

- Het voorstel voor een Cybersolidariteitsverordening is het derde onderdeel van het recente cybersecuritybeleidspakket van de Commissie. Dit voorstel heeft de volgende doelen: 1) versterking van de EU-detectie van cyberdreigingen en -incidenten, 2) het versterken van de paraatheid van kritieke entiteiten door gemeenschappelijke responscapaciteiten te ontwikkelen en 3) respons op grote cyberincidenten gezamenlijk evalueren. Hiertoe worden inrichting van een Europees cyberschild, een Cybernoodmechanisme en een Evaluatiemechanisme voor cyberincidenten voorgesteld.
- Het Cyberschild bestaat uit een netwerk van nationale Security Operation Centres (SOCs) die informatie over incidenten uitwisselen. Het Cybernoodmechanisme bestaat uit het aanbieden van gecoördineerde veiligheidstests voor kritieke entiteiten en inrichting van een pool van incidentresponsdiensten van vertrouwde private aanbieders (de Europese Cybersecurity Reserve').
- Het ministerie van Justitie en Veiligheid coördineert de Nederlandse inzet op de Cyber Solidarity Act. Het kabinet staat in beginsel positief tegenover het voorstel, maar complementariteit op bestaande initiatieven en voldoende sturingsmogelijkheden vanuit de lidstaten zijn aandachtspunten. Voor EZK is meer helderheid over de rol van het ECCC belangrijk. Het definitieve BNC-fiche is ter informatie als bijlage toegevoegd.