Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2018–2019

# 26 643 Informatie- en communicatietechnologie (ICT)

**Nr. 560**

Ter griffie van de Tweede Kamer der Staten-Generaal ontvangen op 19 september 2018.

De wens om over de voorgenomen voordracht voor de vast te stellen ministeriële regeling nadere inlichtingen te ontvangen kan door of namens de Kamer of door ten minste dertig leden van de Kamer te kennen worden gegeven uiterlijk op 19 oktober 2018.

De voordracht voor de vast te stellen ministeriële regeling kan niet eerder worden gedaan dan op 20 oktober 2018 dan wel binnen veertien dagen na het verstrekken van de in de vorige volzin bedoelde inlichtingen

Bij de termijnen is rekening gehouden met de recesperiode van de Tweede Kamer.

## BRIEF VAN DE STAATSSECRETARIS VAN ECONOMISCHE ZAKEN EN KLIMAAT

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 19 september 2018

Graag informeer ik u over de voorstellen die in het kader van de eerste tranche van het «beleidsexperiment cyberweerbaarheid» subsidie hebben ontvangen. Daarnaast stel ik voor dit beleidsexperiment met twee jaar te verlengen. Hieronder wordt dit gemotiveerd.

In mijn brief van 26 juni 2018[1] is vermeld dat in mei van dit jaar een subsidiemodule met een budget van één miljoen euro is opengesteld voor bedrijven die op het terrein van cybersecurity willen samenwerken. Bij sluiting van de openstellingsperiode van de subsidiemodule op 31 mei jl. bleken 15 aanvragen te zijn ingediend. De voorstellen zijn inmiddels beoordeeld door een onafhankelijke adviescommissie op basis van drie criteria: 1) maatschappelijke impact van het voorstel, 2) de slaagkans van het samenwerkingsverband, 3) het innovatieve karakter van het voorstel. Met als resultaat dat er aan zes voorstellen een subsidie is toegekend. De maximale ondersteuning per initiatief is € 200.000.

Het gaat om de volgende zes samenwerkingsverbanden:

1. Cyberweerbaarheid Nederlandse Industrie Defensie- & Veiligheid

De Nederlandse Defensie- en Veiligheidsgerelateerde industrie (DVI) heeft een belangrijke rol in de ondersteuning van de Nederlandse Defensie, haar internationale partners (w.o. NAVO) en de Openbare Orde en Veiligheidssector (OOV-sector). Het voorstel richt zich op de verbetering van de cyberweerbaarheid van de DVI als geheel, te beginnen met die bedrijven en organisaties die betrokken zijn bij producten en diensten waarbij met Departementaal Vertrouwelijk (DepV) of Staatsgeheim (STG) gerubriceerde informatie gewerkt wordt. Het voorstel bestaat onder andere uit een register met partners die aan de Algemene Beveiligingseisen Defensie Opdrachten (kunnen) voldoen.

[1] Kamerstuk 26 643, nr. 545

kst-26643-560
ISSN 0921 - 7371
's-Gravenhage 2018

2. Cyberweerbaarheidscentrum Maakindustrie

Novel-T, een publiek-private samenwerking binnen Oost-Nederland werkt samen aan het weerbaar maken van de maakindustrie in provincie Overijssel en Gelderland. Daarvoor creëert Novel-T een netwerk waar bedrijven in de maakindustrie terecht kunnen voor het verkrijgen en delen van dreigingsinformatie, het bieden van een handelingsperspectief en beveiligingsdiensten.

3. Cyber Security Awareness Havengemeenschap Port of Amsterdam

Port of Amsterdam start een netwerk van (initieel) vijf publieke en private partijen om de digitale weerbaarheid van het Noordzeekanaalgebied (NZKG) te versterken. Het doel van het project is om, door middel van het creëren van bewustwording de cyberweerbaarheid van de bedrijven in het NZKG te verbeteren. Hierbij is de onderlinge ketenafhankelijkheid van bedrijven en organisaties een belangrijk aandachtspunt. De samenwerking gaat aan de slag met het versterken van de digitale veiligheid op het opbouwen van de benodigde kennis en expertise op het terrein van cyberweerbaarheid.

4. Vergroting cyberweerbaarheid groentezaadveredelingsbedrijven

Drie groentezaadveredelingsbedrijven spannen zich gezamenlijk in om de cyberweerbaarheid van de bedrijfsketen te verhogen. Dit is belangrijk omdat zaadveredelingsbedrijven in Nederland beschikken over gewilde en hoogwaardige kennis. De organisaties zetten zich gezamenlijk in om het risicoprofiel van de sector in kaart te brengen, incidenten te analyseren en tot een collectief actieplan te komen.

5. Cyberweerbaarheid in Limburg

Platform Veilig Ondernemen Limburg en Brightlands – een publiek-private samenwerking tussen de provincie, universiteiten en bedrijven – brengen een actieve gemeenschap tot stand waar ondernemers inzicht krijgen in hun individuele situatie. Dit doen zij door middel van weerbaarheidscans, zelfevaluaties, en e-learning modules om zichzelf en hun medewerkers te trainen. De gemeenschap wordt ondersteund door een online platform en een servicedesk waar ondernemers terecht kunnen voor informatie over de aanpak.

6. Samenwerkingsverband Noord-Nederland

Samenwerkingsverband Noord-Nederland vormt de opstap tot het Cyber Security Expertise Centrum Noord (CSECN). De inmiddels 60 aangesloten bedrijven in de regio worden met ontbijtsessies en roadshows op een laagdrempelige manier benaderd en betrokken. Daarnaast worden er security scans uitgevoerd door mbo- en hbo studenten, hacklabs georganiseerd en komt er een security community.

Op 5 september jl. zijn deze zes samenwerkingsverbanden en het Digital Trust Center (DTC) in Utrecht bijeengekomen om elkaars initiatieven te leren kennen en afspraken te maken over kennisdeling. Door best practices uit te wisselen en samen te werken rond informatieverzameling en het opzetten van een platform kan versneld de leercurve doorlopen worden en kunnen ook efficiency voordelen behaald worden. Het DTC zal de uitbouw van dit open netwerk faciliteren en hiermee een stevige impuls geven aan een landelijk dekkend stelsel van regionale en sectorale aanspreekpunten voor het bedrijfsleven op het gebied van cybersecurity.

Ik ben zeer te spreken over het resultaat van de eerste uitvraag naar samenwerkingsverbanden op het gebied van cybersecurity voor bedrijven. De hoeveelheid voorstellen was boven verwachting en de gewenste geografische en sectorale spreiding onder de voorstellen is hierbij gerealiseerd. De meeste plannen voldeden ruimschoots aan de eisen van de subsidieregeling, wat de adviescommissie voldoende (keuze)mogelijkheden bood. Een sterke aftrap, maar slechts een eerste stap wat betreft de potentie van samenwerkingsverbanden tussen bedrijven (en overheid). Regio's en branches die nu nog niet aan bod zijn gekomen, partijen die nog niet klaar waren om mee te doen in de eerste ronde en mogelijk ook initiatieven die voor een tweede kans gaan met een verbeterd voorstel wil ik uitnodigen volgend jaar met voorstellen te komen. Daartoe ben ik voornemens de subsidieregeling opnieuw open te stellen rond 1 april 2019 en de looptijd van het beleidsexperiment te verlengen met twee jaar tot 1 april 2021.

Voor de nieuwe uitvraag van volgend jaar stel ik wederom één miljoen euro ter beschikking. Met een nieuwe uitvraag faciliteren we een groeiend netwerk voor veilig digitaal ondernemen en benutten we de energie en ideeën die momenteel vrij komen. Het doel is om op termijn naar een landelijk dekkend stelsel toe te werken, waarbij ondernemers zich gestimuleerd en gefaciliteerd voelen om de eigen digitale weerbaarheid te verbeteren. Zo zorgen we ervoor dat veilig digitaal ondernemen de norm wordt en het potentieel van de digitale economie optimaal benut kan worden.

Op grond van artikel 4.10, zevende lid, van de Comptabiliteitswet 2016 leg ik de regeling die strekt tot wijziging van het tijdstip waarop de subsidiemodule «beleidsexperiment cyberweerbaarheid» vervalt aan u voor en zal ik deze regeling niet eerder vaststellen dan 30 dagen na verzending van deze brief.

De Staatssecretaris van Economische Zaken en Klimaat,
M.C.G. Keijzer