STAATSCOURANT
Officiële uitgave van het Koninkrijk der Nederlanden sinds 1814.
Nr. 16768
21 maart
2018

Regeling van de Staatssecretaris van Economische Zaken en Klimaat van 17 maart 2018, nr. WJZ / 17196814, houdende wijziging van de Regeling nationale EZ-subsidies en de Regeling openstelling EZK- en LNV-subsidies 2018 in verband met de invoering en openstelling van een subsidiemodule betreffende samenwerking op het gebied van cyberweerbaarheid

De Staatssecretaris van Economische Zaken en Klimaat,

Gelet op de artikelen 2, eerste lid, 4, 5, 14, 15, 16, 17, eerste en derde lid, 18, eerste en vijfde lid, 19, tweede en derde lid, 23, onderdeel b, 25 en 50 van het Kaderbesluit nationale EZ-subsidies;

Besluit:

ARTIKEL I

De Regeling nationale EZ-subsidie wordt als volgt gewijzigd:

A

Aan artikel 3.17.10, tweede lid, wordt toegevoegd 'Deze ontheffing kan ook na het tijdstip van vaststelling van de subsidie worden verleend'.

B

Aan hoofdstuk 4a wordt een titel toegevoegd, luidende:

TITEL 4A.2. BELEIDSEXPERIMENT CYBERWEERBAARHEID

Artikel 4a.2.1. Begripsomschrijvingen

In deze titel wordt verstaan onder niet-vitale onderneming: onderneming die geen product of dienst aanbiedt waarvan de beschikbaarheid en de betrouwbaarheid van vitaal belang zijn voor de Nederlandse samenleving.

Artikel 4a.2.2. Subsidieaanvraag

1. De minister verleent op aanvraag subsidie voor de uitvoering van een cyberweerbaarheidsplan aan:
   a. een rechtspersoon die de cyberweerbaarheid van niet-vitale ondernemingen, behartigt, of
   b. een deelnemer aan een samenwerkingsverband dat de cyberweerbaarheid van niet-vitale ondernemingen behartigt.

2. Het cyberweerbaarheidsplan:
   a. strekt tot versterking van de cyberweerbaarheid van niet-vitale ondernemingen in Nederland;
   b. wordt uitgevoerd door, of in samenwerking met, ten minste twee niet in een groep verbonden niet-vitale ondernemingen;
   c. is gebaseerd op een integrale visie ten aanzien van de ambitie om de cyberweerbaarheid van niet-vitale ondernemingen duurzaam te versterken; en
   d. heeft een looptijd van ten minste één en ten hoogste drie jaar.

3. Het cyberweerbaarheidsplan bestaat uit een samenhangend geheel van twee van de volgende activiteiten:
   a. het vormen en in stand houden van een netwerk voor de versterking van niet-vitale ondernemingen met behulp waarvan contacten worden onderhouden met relevante derden, alsmede het door derden laten uitvoeren van netwerkactiviteiten ten behoeve van niet-vitale ondernemingen;
   b. het stimuleren van bewustwording van cyberweerbaarheid bij niet-vitale ondernemingen;
   c. het geven van inzicht in digitale kwetsbaarheden van niet-vitale ondernemingen;

d. het verrichten van diensten voor niet-vitale ondernemingen om de cyberweerbaarheid van de desbetreffende ondernemingen te versterken;
e. het anderszins versterken van de cyberweerbaarheid van niet-vitale ondernemingen.

4. Een samenwerkingsverband bevat maximaal acht deelnemers en de penvoerder is een ondernemer.

Artikel 4a.2.3. Hoogte subsidie

De subsidie bedraagt 50% van de subsidiabele kosten, doch ten hoogste € 200.000 per cyberweerbaarheidsplan.

Artikel 4a.2.4. Subsidiabele kosten

1. In afwijking van artikel 11 van het besluit worden de kosten voor activiteiten als bedoeld in artikel 4a.2.2, derde lid, berekend overeenkomstig artikel 14 van het besluit.

2. Voor de toepassing van deze titel bedraagt het vaste uurtarief, bedoeld in artikel 14 van het besluit, € 80.

Artikel 4a.2.5. Verdeling van het subsidieplafond

De minister verdeelt het subsidieplafond op volgorde van rangschikking van de aanvragen.

Artikel 4a.2.6. Realisatietermijn

De termijn, bedoeld in artikel 23, onderdeel b, van het besluit, is drie jaar, en wordt gerekend vanaf de aanvang van de activiteiten, bedoeld in artikel 4a.2.2.

Artikel 4a.2.7. Afwijzingsgronden

De minister beslist afwijzend op een aanvraag, indien:
a. door de subsidieaanvrager niet aannemelijk wordt gemaakt dat uitvoering van het cyberweerbaarheidsplan leidt tot een duurzaam netwerk voor de versterking van de cyberweerbaarheid van niet-vitale ondernemingen;
b. onvoldoende vertrouwen bestaat dat uitvoering van het cyberweerbaarheidsplan een bijdrage levert aan de versterking van de cyberweerbaarheid van niet-vitale ondernemingen;
c. het netwerk voor de versterking van de cyberweerbaarheid van niet-vitale ondernemingen niet openstaat voor nieuwe toetreders;
d. in het cyberweerbaarheidsplan activiteiten zijn opgenomen die bestaan uit:
   1°. het ontwikkelen van hardware of software om de cyberweerbaarheid van ondernemingen te versterken, of het aanschaffen daarvan anders dan voor het verwerken of delen van informatie voor de versterking van cyberweerbaarheid;
   2°. het continu op afstand monitoren van de cybersecurity van ondernemingen om aanvallen op de IT-infrastructuur te voorkomen, af te weren, op te sporen of op te lossen; of
   3°. het adviseren van ondernemingen die door een cybersecurityincident zijn getroffen, over het oplossen van het incident;
e. meer dan 25 procent van de kosten voor de uitvoering van het cyberweerbaarheidsplan bestaat uit het aanschaffen van hardware en software voor het verwerken of delen van informatie voor de versterking van cyberweerbaarheid.

Artikel 4a.2.8. Adviescommissie

1. Er is een Adviescommissie cyberweerbaarheid die tot taak heeft de minister op diens verzoek te adviseren omtrent de rangschikkingscriteria, bedoeld in artikel 4a.2.9, eerste lid.

2. De commissie bestaat uit ten minste vier en ten hoogste zeven leden.

3. De voorzitter en de andere leden van de commissie worden door de minister voor een termijn van ten hoogste één jaar benoemd.

Artikel 4a.2.9. Rangschikkingscriteria

1. De minister kent aan een cyberweerbaarheidsplan een hoger aantal punten toe, naarmate:
   a. het cyberweerbaarheidsplan een grotere bijdrage levert aan het versterken van de

cyberweerbaarheid van niet-vitale ondernemingen, waardoor maatschappelijke en economische schade kan worden beperkt;
b. het netwerk waarbinnen het cyberweerbaarheidsplan wordt uitgevoerd:
   1. in hogere mate aantoonbaar tot doel heeft en door de samenstelling van het netwerk geschikt is om de cyberweerbaarheid van niet-vitale ondernemingen duurzaam te versterken;
   2. een groter netwerk kan vormen waarbinnen ervaring en kennis over cyberweerbaarheid aanwezig is en wordt uitgewisseld;
c. het cyberweerbaarheidsplan innovatiever is.

2. Het aantal punten bedraagt bij de onderdelen a en b van het eerste lid ten minste één en ten hoogste veertig punten, en bij onderdeel c van het eerste lid ten minste één en ten hoogste twintig punten.

3. De minister rangschikt de aanvragen, waarop niet afwijzend is beslist, hoger, naarmate in totaal meer punten aan het cyberweerbaarheidsplan zijn toegekend.

4. Geen subsidie wordt verleend voor een cyberweerbaarheidsplan dat lager is gerangschikt dan een soortgelijk cyberweerbaarheidsplan.

Artikel 4a.2.10. Evaluatie

1. De subsidieontvanger verleent medewerking aan een evaluatie van de effecten van de door hem uitgevoerde activiteiten, bedoeld in artikel 4a.2.2, voor zover deze medewerking redelijkerwijs van hem verlangd kan worden.

2. De subsidieontvanger verleent medewerking aan de verdere verspreiding van ervaringen en resultaten van het cyberweerbaarheidsplan door de minister of door een door de minister aangewezen derde.

3. De verplichtingen, bedoeld in het eerste en tweede lid, gelden tot drie jaar na de datum van de beschikking tot subsidievaststelling.

Artikel 4a.2.11. Informatieverplichtingen

1. Indien de aanvrager een mkb-ondernemer betreft bevat een aanvraag voor subsidie op grond van artikel 4a.2.2. ten minste de gegevens, bedoeld in artikel 6, tweede lid, van de algemene groepsvrijstellingsverordening.

2. Onverminderd het eerste lid bevat een aanvraag voor subsidie op grond van artikel 4a.2.2 ten minste:
   a. een verklaring de-minimissteun;
   b. gegevens over de aanvrager, waaronder de naam van de organisatie, het KvK-nummer, het post- en bezoekadres en het rekeningnummer;
   c. gegevens over de contactpersoon bij de aanvrager, waaronder de naam, het telefoonnummer en het e-mailadres;
   d. een begroting waarin de totale kosten van de uitvoering van het cyberweerbaarheidsplan en de omvang van de gevraagde subsidie zijn opgenomen;
   e. een cyberweerbaarheidsplan;
   f. een planning van de uitvoering van de activiteiten in het cyberweerbaarheidsplan;
   g. een samenvatting van het cyberweerbaarheidsplan die door de minister kan worden gebruikt in voor een ieder toegankelijke publicaties.

3. De aanvraag voor de vaststelling van de subsidie bevat ten minste:
   a. gegevens over de aanvrager, waaronder de naam van de aanvrager en het door de minister verstrekte referentienummer;
   b. de omvang van de vast te stellen subsidie en de kerngegevens voor de onderbouwing van de subsidievaststelling;
   c. een samenvatting van de resultaten van het cyberweerbaarheidsplan die door de minister kan worden gebruikt in voor ieder toegankelijke publicaties.

Artikel 4a.2.12. Staatssteun

De subsidie, bedoeld in artikel 4a.2.2, bevat staatssteun en wordt gerechtvaardigd door de algemene de-minimisverordening, of, indien de subsidie wordt verleend aan een mkb-ondernemer, door artikel 18 van de algemene groepsvrijstellingsverordening voor zover het

consultancysteun betreft en de algemene de-minimisverordening voor zover het steun voor overige activiteiten betreft.

Artikel 4a.2.13. Vervaltermijn

Deze titel vervalt met ingang van 1 april 2019, met dien verstande dat deze van toepassing blijft op subsidies die voor deze datum zijn verleend.

ARTIKEL II

Aan de tabel van artikel 1, tweede lid, van de Regeling openstelling EZK- en LNV-subsidies 2018 wordt een rij toegevoegd, luidende:

Titel 4a.2 Beleidsexperiment cyberweerbaarheid	4a.2.2			16-04-2018 t/m 31-05-2018	€ 1.000.000

ARTIKEL III

Deze regeling treedt in werking met ingang van 1 april 2018, en werkt ten aanzien van artikel I, onderdeel A, terug tot en met 1 januari 2018.

Deze regeling zal met de toelichting in de Staatscourant worden geplaatst.

's-Gravenhage, 17 maart 2018

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

TOELICHTING

I Algemeen

1. Aanleiding en doel

Cybercrime vormt een flinke schadepost voor de Nederlandse economie. Zowel op het gebied van kennis als op het vlak van preventieve maatregelen valt nog veel te winnen. Uit het rapport 'Preventie door het MKB tegen digitale fraude' van de Kamer van Koophandel (3 oktober 2017) blijkt dat bijna twee op de vijf mkb-ondernemers in het afgelopen jaar te maken hebben gehad met digitale fraude.[1] Een derde van de mkb'ers geeft aan weinig of helemaal geen kennis te hebben over het voorkomen van identiteitsfraude, faillissementsfraude, ransomware of malware. Malware is kwaadaardige software en ransomware is een vorm van malware die een computer en/of gegevens die erop staan blokkeert en vervolgens van de gebruiker geld vraagt om de computer weer te 'bevrijden'. In de digitale economie is het belangrijk dat ondernemers veilig zaken kunnen doen en consumenten veilig gebruik kunnen maken van digitale diensten en producten. Daarvoor moeten ondernemers zich bewust zijn van de risico's van cybercrime en investeren in beveiliging.

Dit beleidsexperiment kan bijdragen aan het versterken van de cyberweerbaarheid van het niet als vitaal aangemerkte bedrijfsleven. Onder weerbaarheid wordt het vermogen verstaan van personen, organisaties of samenlevingen om weerstand te bieden aan negatieve invloeden op de beschikbaarheid, vertrouwelijkheid en/of integriteit van (informatie)systemen en digitale informatie (conform Cybersecuritybeeld Nederland 2017). Door subsidieverstrekking worden activiteiten gestimuleerd die inzicht geven in de kwetsbaarheden van de IT-infrastructuur en het verrichten van diensten om de cyberweerbaarheid van bedrijven te versterken. Denk hierbij aan zelf-assessment, security testen, benchmarken, audits, reviews. Het is voor een ondernemer erg belangrijk om geïnformeerd te zijn over de risico's en maatregelen die ze kunnen nemen. Het is van belang dat ondernemers hier actief mee aan de slag gaan.

In het kader van deze subsidieregeling werken ondernemers samen aan het versterken van de digitale veiligheid en het opbouwen van de benodigde kennis en expertise op het terrein van cyberweerbaarheid. De resultaten en instrumenten die binnen de samenwerkingsverbanden worden ontwikkeld, kunnen gebruikt worden bij andere netwerken die de cyberweerbaarheid van niet-vitale ondernemingen behartigen (hierna: cyberweerbaarheidsnetwerken), waardoor er navolging kan plaatsvinden. Een goede informatie-uitwisseling tussen publieke en private organisaties met betrekking tot actuele dreigingsinformatie, kwetsbaarheden en handelingsperspectieven kan ervoor zorgen dat bedrijfsgevoelige gegevens niet weglekken en cascade-effecten worden voorkomen (WannaCry). Het doel van deze subsidieregeling is de digitale weerbaarheid van ondernemers te vergroten door middel van het stimuleren van samenwerkingsverbanden op het terrein van cybersecurity. Aan de slag gaan, samenwerking en kennisoverdracht staan hierbij centraal.

2. Digital Trust Centre (DTC)

Het Digital Trust Centre (DTC) is in 2018 opgericht om het bedrijfsleven weerbaarder te maken tegen cyberdreigingen. In een brief aan de Tweede Kamer van 23 september 2017 is uiteengezet hoe het ministerie van Economische Zaken en Klimaat invulling zal geven aan het DTC.[2] Aanleiding voor de oprichting van het DTC is een aantal onderzoeken waaruit blijkt dat het bedrijfsleven kwetsbaar is voor cyberaanvallen en onvoldoende kennis heeft om zich hiertegen te weren.[3] Goede samenwerking tussen overheid en bedrijfsleven, gerichte informatiedeling en objectieve advisering aan alle bedrijven is nodig om de weerbaarheid tegen cyberaanvallen te vergroten.[4]

Het Nationaal Cyber Security Centrum (NCSC) richt zich primair tot de rijksoverheid en organisaties in de vitale infrastructuur voor het uitwisselen van informatie. Het NCSC informeert daarnaast waar nodig het bredere publiek om de digitale weerbaarheid in algemene zin te verhogen. Het DTC zal de hoogwaardige technische kennis van het NCSC ontsluiten voor het bredere publiek en samenwerkingsverbanden aanjagen die mogelijk met het NCSC verbonden zullen worden.
Aangezien cybercriminaliteit de hele Nederlandse economie raakt, is het aanjagen en faciliteren van kennisdeling en publiek-private samenwerking via het DTC van belang om de digitale veiligheid van

---

1 Kamer van Koophandel: Preventie door het MKB tegen digitale fraude, september 2017 https://www.kvk.nl/advies-en-informatie/fraude/mkb-heeft-weinig-kennis-over-het-voorkomen-van-digitale-fraude/.
2 *Kamerstukken II* 2017/18, 26 643, nr. 488.
3 Advies Verhagen: Nederland op droge voeten, oktober 2016; Rathenau Instituut: Een nooit gelopen race, maart 2017; TNO rapport: Informatiedeling Topsectoren, maart 2017.
4 Cyber Security Raad Advies: Naar een dekkend stelsel van informatieknooppunten, juli 2017.

het hele bedrijfsleven te versterken. Men spreekt van vitale infrastructuur, opgedeeld in vitale sectoren, als het gaat om producten, diensten en onderliggende processen, die – als zij uitvallen – tot maatschappelijke ontwrichting kunnen leiden. Dat kan zijn, omdat er sprake is van veel slachtoffers en grote economische schade, of als het herstel heel lang gaat duren en er geen reële alternatieven zijn, terwijl deze producten en diensten niet gemist kunnen worden.

Met dit beleidsexperiment wordt beoogd de komende jaren het ontstaan van een landelijk dekkend stelsel van cyberweerbaarheidsnetwerken voor de versterking van cyberweerbaarheid van niet-vitale ondernemingen tot stand te helpen brengen. De regeling is tot stand gekomen in nauwe samenwerking met het Nationaal Cyber Security Centrum en het Ministerie van Justitie en Veiligheid.

3. Cyberweerbaarheidsnetwerken

Deze regeling biedt cyberweerbaarheidsnetwerken de mogelijkheid om aan de slag te gaan met cyberweerbaarheid en het weerbaar maken van ondernemingen. In een cyberweerbaarheidsnetwerk kunnen ondernemers samenwerken met andere organisaties binnen en tussen niet-vitale branches, sectoren en regio's aan het vergroten van de cyberweerbaarheid. Ook ondernemingen die actief zijn in vitale sectoren, mogen onderdeel zijn van het netwerk. Deze ondernemingen vormen weliswaar niet de doelgroep van deze subsidieregeling, maar kunnen wel bijdragen aan het succes van het cyberweerbaarheidsnetwerk. Zij beschikken over veel kennis en expertise en kunnen de slagingskans van het netwerk vergroten.

Meerdere ondernemingen kunnen gezamenlijk een cyberweerbaarheidsplan opstellen en een penvoerder vraagt vervolgens namens de individuele bedrijven een subsidie aan. De penvoerder is een van de deelnemers aan het samenwerkingsverband. Ook is het mogelijk dat een verband met rechtspersoonlijkheid (bijvoorbeeld een stichting) dat tot doel heeft de behartiging van cyberweerbaarheid van niet-vitale ondernemingen, een subsidie aanvraagt. De subsidie wordt dan verstrekt aan deze stichting.

Per cyberweerbaarheidsplan bedraagt de subsidie maximaal 50% van de subsidiabele kosten met een maximum van € 200.000. Bij de activiteiten van een cyberweerbaarheidsnetwerk kunnen drie aandachtsgebieden worden onderscheiden:

1. Informatieknooppunt: een centrum waar informatie over digitale dreigingen en kwetsbaarheden beschikbaar is voor en gedeeld wordt met ondernemers;
2. Expertisecentrum: een centrum waar de capaciteit en expertise aanwezig is om informatie over digitale dreigingen en kwetsbaarheden te verrijken en (specifiek) handelingsperspectief te bieden voor haar ondernemers;
3. Collectief computercrisisteam: een team/organisatie die verantwoordelijk is voor het bieden van de noodzakelijke diensten voor het oplossen van cybersecurityincidenten voor haar deelnemers. Dit kunnen zowel preventie-, detectie-, monitoring- en in ieder geval respons diensten zijn.

Door middel van deze subsidieregeling wordt beoogd om de cyberweerbaarheidsnetwerken in te richten als een informatieknooppunt en/of expertisecentrum. Tijdens deze eerste twee stappen is de impact van de regeling het grootst: ondernemers bij elkaar brengen, kenniscirculatie bevorderen, kwetsbaarheden in kaart brengen en ermee aan de slag gaan. Nederland heeft bijna 1,6 miljoen bedrijven; variërend van horecabedrijven tot high-tech bedrijven en van bouwbedrijven tot autoindustrie. Via cyberweerbaarheidsnetwerken kunnen informatie en gespecialiseerde diensten worden aangeboden en kan een grote doelgroep worden bereikt. De expertise die binnen de cyberweerbaarheidsnetwerken wordt opgebouwd (in de vorm van best practices of blauwdrukken), kan vervolgens ook gebruikt worden bij andere organisaties, zodat er navolging kan plaatsvinden en de reikwijdte van het DTC verder kan worden vergroot.

Afhankelijk van de behoefte en het volwassenheidsniveau van het samenwerkingsverband kunnen cyberweerbaarheidsnetwerken ook doorgroeien naar een computercrisisteam. De activiteiten die kenmerkend zijn voor een computercrisisteam komen op grond van deze subsidiemodule echter niet voor subsidie in aanmerking. Een computercrisisteam is met name interessant voor bedrijven die beschikken over specifieke of hoogwaardige kennis die door digitale dreigingen onder druk kunnen komen staan.

4. Beoordeling aanvragen

De aanvragen die worden ingediend en voldoen aan de gestelde eisen, zullen worden vergeleken aan de hand van een aantal rangschikkingscriteria. Voor het beoordelen van de aanvragen wordt de Adviescommissie cyberweerbaarheid om advies gevraagd. Subsidie wordt toegekend aan subsidieaanvragers waarvan het cyberweerbaarheidsplan het beste uit de vergelijking komt. De kwaliteit van de aanvraag is hierbij doorslaggevend. Indien er soortgelijke plannen worden ingediend, komt alleen

het plan met het hoogste aantal punten voor subsidie in aanmerking. Een soortgelijk plan is een plan dat in doel en activiteiten veel overlap vertoont en waarvan de toegevoegde waarde erg gering is. Om effectief met de beschikbare publieke middelen om te gaan, wordt bij soortgelijke projecten daarom alleen het hoogst gerangschikte project gehonoreerd.

De aanvragen zullen worden vergeleken aan de hand van de volgende rangschikkingscriteria:

1. Maatschappelijke impact
   De maatschappelijke impact is het grootst als:
   - het cyberweerbaarheidsplan wordt uitgevoerd door of in samenwerking met ondernemingen die over specifieke of hoogwaardige kennis beschikken en daardoor door digitale dreigingen onder druk kunnen komen te staan. Als deze bedrijven beter beschermd worden tegen digitale dreigingen zal dit vanuit veiligheid, economisch en maatschappelijk perspectief de grootste impact hebben.
   - er sprake is van een grote ketenafhankelijkheid en vitale processen geraakt kunnen worden. De keten is zo zwak als de zwakste schakel.
2. Slaagkans samenwerkingsverband: de kwaliteit van het samenwerkingsverband wordt bepaald door de samenstelling van het netwerk en de mate waarin relevante partijen zijn betrokken in het cyberweerbaarheidsnetwerk en zich daadwerkelijk hebben gecommitteerd aan het versterken van de weerbaarheid. Daarnaast is van belang in hoeverre activiteiten binnen het cyberweerbaarheidsplan leiden tot een blijvende verbetering of continuering van het cyberweerbaarheidsnetwerk door de deelnemers kan worden gefinancierd.
3. Innovatief karakter:

De mate waarin initiatieven best practices of blauwdrukken opleveren die door andere bedrijven en sectoren kunnen worden gebruikt.

Het subsidieplafond van € 1 miljoen biedt de mogelijkheid om voor de uitvoering van ten minste vijf cyberweerbaarheidsplannen een maximaal subsidiebedrag van € 200.000 toe te kennen.

5. Evaluatie beleidsexperiment

Om te kunnen beoordelen of dit beleidsexperiment succesvol is verlopen, zal het beleidsexperiment aan de hand van vooraf opgestelde criteria worden geëvalueerd. Daarvoor wordt medewerking van de subsidieontvangers gevraagd.

Met dit beleidsexperiment wordt beoogd vast te stellen onder welke randvoorwaarden een cyberweerbaarheidsnetwerk effectief is. Met andere woorden, in hoeverre kunnen natuurlijke netwerken in de regio of binnen de branche of een sector bijdragen aan het versterken van de cyberweerbaarheid van het niet-vitale bedrijfsleven in Nederland? En kunnen kleine en grote ondernemers voldoende worden bereikt? Naast de netwerkfunctie zal in het beleidsexperiment ook gekeken worden in hoeverre het beleidsexperiment bijdraagt aan betere kennisbenutting door ondernemers en extra product- en/of dienst-toepassingen op het terrein van cyberweerbaarheid.

Het aantal subsidieontvangers zal mede bepalend zijn voor het type analyse en evaluatie, waarvoor gekozen zal worden. Op basis van de ervaringen in het pilotjaar wordt bekeken of en hoe de aanjaagfunctie van cyberweerbaarheidsnetwerken het meest effectief en efficiënt kan worden voortgezet.

6. Openstelling

Voorstellen kunnen gedurende 6 weken worden ingediend, van 16 april 2018 tot en met 31 mei 2018. Het subsidieplafond bedraagt € 1 miljoen.

7. Staatssteun

Bij dit beleidsexperiment is rekening gehouden met de Europese regels betreffende staatssteun. De begunstigden van de te verstrekken subsidie zijn een rechtspersoon die of deelnemers aan een samenwerkingsverband dat de cyberweerbarheid van niet-vitale ondernemingen behartigt. De subsidiemodule bevat staatssteun. Voor mkb-ondernemingen wordt de consultancysteun gerechtvaardigd door artikel 18 van de algemene groepsvrijstellingsverordening en voor overige activiteiten moet de subsidieaanvrager voldoen aan de voorwaarden van de algemene de-minimisverordening. Uit het cyberweerbaarheidsplan en de begroting blijkt of de kosten worden gerechtvaardigd door artikel 18 van de algemene groepsvrijstellingsverordening of dat de algemene de-minimisverordening van toepassing is. Voor grote ondernemingen bevat de subsidie staatssteun die kan worden gerechtvaardigd door de algemene de-minimisverordening. Subsidieaanvragers moeten daarom bij de aanvraag een de-minimisverklaring indienen.

8. Regeldruk

Deze regeling heeft regeldrukeffecten. Deze bestaan uit aanvraag, verantwoording en evaluatie. Er zullen naar verwachting 10 aanvragen worden ingediend, waarvan er ten minste 5 kunnen worden gehonoreerd. De administratieve lasten voor ondernemingen komen uit op 4,67% van het totale subsidiebedrag. De totale administratieve lasten van deze openstelling bedragen € 46.683.

9. Uitvoering

De uitvoering van deze subsidieregeling is belegd bij RVO.nl, onderdeel van het Ministerie van Economische Zaken en Klimaat. Op de website van RVO.nl zijn de benodigde formulieren voor het aanvragen van de subsidie verkrijgbaar.

10. Inwerkingtreding

Artikel I, onderdeel A treedt in werking met ingang van 1 april 2018 en werkt terug tot en met 1 januari 2018. Omdat het besluit, zoals in artikel I, onderdeel A van het artikelsgewijs deel wordt toegelicht, per 1 januari 2018 is gewijzigd (Stb. 2017, 502), wordt aan deze wijziging van artikel 3.17.10 terugwerkende kracht verleend tot en met dezelfde datum. Tegen terugwerkende kracht bestaat in dit geval geen bezwaar, omdat deze begunstigend is voor de doelgroep. Artikel I, onderdeel B, treedt in werking met ingang van 1 april 2018, een vast verandermoment. Met publicatie minder dan twee maanden voordien wordt afgeweken van het beleid inzake vaste verandermomenten, zoals opgenomen in aanwijzing 4.17 van de Aanwijzingen voor de regelgeving. Deze afwijking is gerechtvaardigd, daar de doelgroepen gebaat zijn bij een spoedige inwerkingtreding.

II Artikelen

Artikel I, onderdeel A

Van de gelegenheid is gebruik gemaakt om een wijziging van de subsidiemodule Toekomstfondskrediet onderzoeksfaciliteiten mee te nemen. Bij het Besluit van 4 december 2017 tot wijziging van enkele algemene maatregelen van bestuur op de terreinen van het Ministerie van Economische Zaken en Klimaat en het Ministerie van Landbouw, Natuur en Voedselkwaliteit in verband met het herstel van technische gebreken en leemten alsmede het aanbrengen van andere wijzigingen van ondergeschikte aard (Stb. 2017, 502) is in artikel 42, derde lid, van het Kaderbesluit nationale EZ-subsidies (hierna: besluit) verduidelijkt dat een ontheffing van een terugbetalingsverplichting van een verleende subsidie alleen voorafgaand aan de vaststelling van de subsidie kan worden verleend. Daarbij is wel de mogelijkheid gecreëerd om bij ministeriële regeling te bepalen dat ontheffing ook nadien kan worden verleend. Deze toevoeging houdt verband met het feit dat in uitzonderlijke omstandigheden toch behoefte kan bestaan om ook ná vaststelling van de subsidie ontheffing te kunnen verlenen. Als voorbeeld hiervan werd in de nota van toelichting bij het genoemde wijzigingsbesluit gewezen op de subsidiemodule Toekomstfondskrediet onderzoeksfaciliteiten, in titel 3.17 van de Regeling nationale EZ-subsidies. Met die module wordt beoogd in hoogwaardige onderzoeksinfrastructuren te investeren. De commercialisatie van zo'n onderzoeksinfrastructuur is lastiger. Er zijn op dat moment geen (eigen) innovatieve producten die direct vercommercialiseerd kunnen worden, zoals bij andere subsidiemodules met terugbetalingsverplichtingen het geval is. Commercialisatie zal dus moeten bestaan uit andere activiteiten, zoals de verhuur van de infrastructuur aan ondernemingen, de uitvoering van onderzoeksdiensten voor ondernemingen of het verrichten van contractresearch. In het exploitatieplan maakt de aanvrager hier al een inschatting van op het moment van de subsidieaanvraag voor de bouw of verbetering van de onderzoeksinfrastructuur. Deze inschatting kan in de praktijk tegenvallen. Daar komt nog bij dat de module is gericht op onderzoeksorganisatie als subsidieontvanger, in plaats van ondernemers zoals bij andere modules waarvoor een terugbetalingsverplichting geldt. Om deze reden is nu voor deze subsidiemodule gebruikgemaakt van de in artikel 42, derde lid, van het besluit opgenomen mogelijkheid dat ontheffing ook na vaststelling van de subsidie kan worden verleend. Dit is toegevoegd aan artikel 3.17.10, derde lid, van de Regeling nationale EZ-subsidies. Afhankelijk van de omstandigheden kan een gehele of gedeeltelijke ontheffing worden verleend. Een gedeeltelijke ontheffing kan bijvoorbeeld aan de orde zijn indien het project wel leidt tot enige commerciële toepassing, maar niet zodanig als op het moment van de subsidieaanvraag werd ingeschat.

Artikel I, onderdeel B

Artikel 4a.2.1

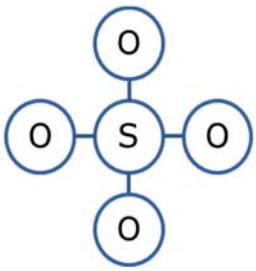
In artikel 4a.2.1 wordt de betekenis van het begrip niet-vitale onderneming, dat meermaals in de

artikelen wordt gebruikt, uiteengezet. Zoals in het algemeen deel van deze toelichting is toegelicht richt deze regeling zich op het versterken van de cyberweerbaarheid van niet-vitale ondernemingen in Nederland. In artikel 1 van de Wet gegevensverwerking en meldplicht cybersecurity is aangegeven dat onder een vitale aanbieder wordt verstaan een aanbieder van een product of dienst waarvan de beschikbaarheid en betrouwbaarheid van vitaal belang zijn voor de Nederlandse samenleving. In de begripsomschrijving van een niet-vitale onderneming is de tegenhanger van deze begripsomschrijving geformuleerd, om te verduidelijken dat deze subsidiemodule zich niet richt op de vitale aanbieder.

Artikel 4a.2.2

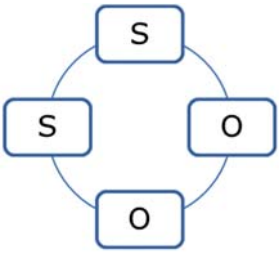
In artikel 4a.2.2 wordt geregeld welke aanvrager voor subsidie in aanmerking kan komen en voor welke activiteit subsidie kan worden verleend. Een subsidie kan worden verleend voor de uitvoering van een cyberweerbaarheidsplan. Het cyberweerbaarheidsplan moet worden uitgevoerd door, of in samenwerking met, ten minste twee niet in een groep verbonden niet-vitale ondernemingen.
Ingevolge artikel 1 van het besluit wordt onder een onderneming verstaan iedere eenheid, ongeacht haar rechtsvorm of wijze van financiering, die een economische activiteit uitoefent. Door te eisen dat het plan wordt uitgevoerd door of in samenwerking met niet-vitale ondernemingen, wordt gewaarborgd dat er daadwerkelijk een netwerk wordt gevormd waaraan de doelgroep deelneemt en wordt samengewerkt om de cyberweerbaarheid van niet-vitale ondernemingen te versterken. De ondergrens is dat het cyberweerbaarheidsplan wordt uitgevoerd door, of in samenwerking met twee ondernemingen, maar het wordt voor het vormen van een netwerk aangemoedigd dat er meer partijen betrokken zijn. Deze ondernemingen kunnen subsidieaanvrager zijn, maar het mogen ook ondernemingen zijn die een rol spelen bij de uitvoering van het cyberweerbaarheidsplan zonder dat zij subsidie aanvragen.
In een cyberweerbaarheidsplan wordt beschreven welke activiteiten uit het derde lid de subsidieaanvrager wil ondernemen om de cyberweerbaarheid van niet-vitale ondernemingen te versterken. In elk onderdeel van het derde lid is een andere activiteit opgenomen, waarvoor subsidie kan worden verstrekt. Er worden ten minste twee activiteiten uit de verschillende onderdelen gekozen, maar er mag ook een combinatie van meer dan twee activiteiten worden gemaakt.

Dit cyberweerbaarheidsplan kan worden uitgevoerd door twee typen aanvragers.
Het plan kan worden uitgevoerd door één aanvrager, namelijk een rechtspersoon die de cyberweerbaarheid van niet-vitale ondernemingen behartigt. Hieronder is een eenvoudig schematisch voorbeeld opgenomen van een dergelijke subsidieaanvrager en het netwerk waarmee het plan wordt uitgevoerd.



S = subsidieaanvanger
O = niet-vitale onderneming die geen subsidieaanvrager is

Hierbij kan worden gedacht aan een stichting die de cyberweerbaarheid van niet-vitale ondernemingen behartigt. Alleen deze stichting ontvangt dan subsidie, maar een cyberweerbaarheidsplan moet wel worden uitgevoerd door, of in samenwerking met, ten minste twee niet in een groep verbonden niet-vitale ondernemingen.
Het is ook mogelijk dat een subsidieaanvraag wordt ingediend door een samenwerkingsverband dat de cyberweerbaarheid van niet-vitale ondernemingen behartigt. Hieronder is een eenvoudig schematisch voorbeeld opgenomen van een samenwerkingsverband (de subsidieaanvragers) dat in samenwerking met een tweetal niet-vitale ondernemingen (die geen subsidie aanvragen) een cyberweerbaarheidsplan uitvoeren.



S = subsidieaanvrager
O = niet-vitale onderneming die geen subsidieaanvrager is

Een samenwerkingsverband bezit ingevolge artikel 1 van het besluit geen rechtspersoonlijkheid en bestaat uit ten minste twee niet in een groep verbonden deelnemers. Dit betekent dat een samenwerkingsverband bijvoorbeeld niet kan bestaan uit twee ondernemingen met een moeder-dochter relatie. Het samenwerkingsverband is opgericht ten behoeve van de uitvoering van activiteiten en is niet vormgegeven als een vennootschap. Het samenwerkingsverband bestaat uit maximaal acht deelnemers, maar bij de uitvoering van het cyberweerbaarheidsplan kan worden samengewerkt met andere partijen die geen subsidie ontvangen. Een penvoerder vraagt namens de deelnemers aan het samenwerkingsverband subsidie aan voor de uitvoering van een cyberweerbaarheidsplan. De penvoerder is een ondernemer die deelneemt aan het samenwerkingsverband. Een ondernemer kan ingevolge artikel 1 van het besluit een natuurlijke persoon, rechtspersoon of een vennootschap zijn, die een onderneming in stand houdt, niet zijnde een rechtspersoon die krachtens publiekrecht is ingesteld. De individuele deelnemers aan het samenwerkingsverband ontvangen subsidie voor de uitvoering van het cyberweerbaarheidsplan.

Artikel 4a.2.3

De subsidie bedraagt 50% van de subsidiabele kosten. Dit betekent dat 50% van de subsidiabele kosten door middel van subsidie wordt bekostigd en dat 50% van de subsidiabele kosten door de subsidieaanvrager wordt betaald. Voor de uitvoering van een cyberweerbaarheidsplan kan maximaal € 200.000 worden verleend. Als een samenwerkingsverband gezamenlijk een cyberweerbaarheidsplan uitvoert, ontvangen de subsidieontvangers ieder een deel van dit bedrag.

Artikel 4a.2.4

Bij de berekening van de kosten voor de subsidiabele activiteiten wordt gebruik gemaakt van de vaste-uurtarief-systematiek die is opgenomen in artikel 14 van het besluit. Dit houdt in dat de subsidiabele kosten worden berekend door het aantal uren die zijn besteed aan de uitvoering van het cyberweerbaarheidsplan te vermenigvuldigen met een vast uurtarief van € 80. Hierin zijn zowel de directe loonkosten (dit zijn de bruto loonkosten, vermeerderd met de werkgeverslasten, de kosten van de secundaire arbeidsvoorwaarden, emolumenten en uitkeringen na ontslag) als daaraan toegerekende indirecte kosten begrepen. Dit bedrag wordt vermeerderd met de kosten van het gebruik van apparatuur en de kosten van verbruikte materialen en hulpmiddelen, indien deze in de administratie te onderscheiden zijn en de aan derden betaalde kosten. De afschrijvingskosten van apparatuur, zoals hard- en software, wordt lineair berekend als fractie van de aanschafprijs op basis van bedrijfseconomische grondslagen en normen, met een minimale afschrijvingstermijn van vijf jaar (artikel 10, vijfde lid, van het besluit).

Artikel 4a.2.5

Het subsidieplafond wordt verdeeld op volgorde van rangschikking van de aanvragen. Deze rangschikking vindt plaats op grond van de criteria die in artikel 4a.2.9 zijn opgenomen.

Artikel 4a.2.6

In artikel 23, onderdeel b, van het besluit is bepaald dat een subsidieaanvraag wordt afgewezen indien onaannemelijk wordt geacht dat de activiteiten binnen de realisatietermijn kunnen worden voltooid. In de begripsomschrijving van het cyberweerbaarheidsplan is aangegeven dat een cyberweerbaarheidsplan een looptijd heeft van ten hoogste drie jaar. Als niet aannemelijk is dat het cyberweerbaarheidsplan binnen een periode van drie jaar kan worden voltooid, dan wordt de aanvraag afgewezen.

Artikel 4a.2.7

In dit artikel wordt geregeld dat de minister een subsidieaanvraag afwijst, indien een of meer van de volgende afwijzingsgronden aan de orde is:

- Er wordt niet aannemelijk gemaakt dat de uitvoering van het cyberweerbaarheidsplan leidt tot een duurzaam netwerk voor de versterking van de cyberweerbaarheid van niet-vitale ondernemingen. Door middel van het stimuleren van samenwerking op het terrein van cybersecurity wordt immers beoogd het doel van deze subsidieregeling te bereiken: het vergroten van de cyberweerbaarheid van niet-vitale ondernemingen. Er moet dus daadwerkelijk een netwerk worden gevormd voor de versterking van de cyberweerbaarheid, en in dit vereiste komt ook tot uitdrukking dat aannemelijk moet zijn dat continuering van het netwerk door de deelnemers kan worden gefinancierd.
- Er bestaat onvoldoende vertrouwen dat uitvoering van het cyberweerbaarheidsplan een bijdrage levert aan de versterking van de cyberweerbaarheid. Zoals in het vorige punt is aangegeven wordt met deze subsidiemodule beoogd om de cyberweerbaarheid van niet-vitale ondernemingen te vergroten.
- Het netwerk voor de versterking van cyberweerbaarheid van niet-vitale ondernemingen staat niet open voor nieuwe toetreders. Zoals in het algemeen deel van de toelichting is aangegeven wordt de kwaliteit van het samenwerkingsverband bepaald door de samenstelling van het netwerk en de mate waarin relevante partijen zijn betrokken in het netwerk. Daarom wordt aangemoedigd dat partijen zich aansluiten bij het netwerk om de cyberweerbaarheid te vergroten (zonder dat deze partijen subsidie ontvangen voor de uitvoering van het cyberweerbaarheidsplan), en wordt een aanvraag afgewezen indien het netwerk hiertoe geen mogelijkheid biedt.
- Er wordt subsidie aangevraagd voor het ontwikkelen of aanschaffen van hardware en software om de cyberweerbaarheid van individuele ondernemingen te versterken. Het ontwikkelen van hard- en software vormt geen doel van deze subsidiemodule. Ook het aanschaffen van hardware en software om de cyberweerbaarheid van (individuele) ondernemingen te versterken komt op grond van deze module niet voor subsidie in aanmerking. Deze subsidiemodule ziet namelijk uitdrukkelijk op het stimuleren van samenwerking en netwerkvorming om de cyberweerbaarheid van niet-vitale ondernemingen te versterken. Dat is de reden dat kosten voor het aanschaffen van hardware en software voor het verwerken of delen van informatie voor de versterking van de cyberweerbaarheid wel mogen worden opgevoerd. Op deze manier wordt de subsidieaanvrager ondersteund bij de inrichting van en het functioneren als een informatieknooppunt of een expertisecentrum. De kosten voor het aanschaffen van apparatuur voor het netwerk mogen maximaal 25 procent van de kosten voor het uitvoeren van het cyberweerbaarheidsplan bedragen.
- Er wordt subsidie aangevraagd voor het continu op afstand monitoren van de cybersecurity van ondernemingen om aanvallen op de IT-infrastructuur te voorkomen, af te weren, op te sporen of op te lossen, of het adviseren van ondernemingen die door een cybersecurityincident zijn getroffen, over het oplossen van het incident. Dit vormen namelijk activiteiten die door een computercrisisteam worden uitgevoerd. Zoals in het algemeen deel van de toelichting is vermeld wordt met deze regeling beoogd om netwerken in te richten als informatieknooppunt of expertisecentrum en komen de activiteiten die kenmerkend zijn voor een computercrisisteam niet voor subsidie in aanmerking.

Artikel 4a.2.8

Met dit artikel is een Adviescommissie cyberweerbaarheid ingesteld die de Minister adviseert over de rangschikking van de subsidieaanvragen. Deze commissie bestaat uit ten minste vier en ten hoogste zeven leden. De leden van de adviescommissie worden voor ten hoogste één jaar benoemd, omdat deze subsidiemodule ook na één jaar vervalt.

Artikel 4a.2.9

In het eerste lid van dit artikel zijn de criteria opgenomen op basis waarvan de adviescommissie subsidieaanvragen kan rangschikken. Met deze criteria wordt beoogd via deze subsidieregeling de digitale weerbaarheid van ondernemers te vergroten door middel van het stimuleren van samenwerkingsverbanden op het terrein van cyberweerbaarheid. In onderdeel vier van het algemeen deel van de toelichting is uiteengezet wat onder deze rangschikkingscriteria wordt verstaan. In totaal kunnen op grond van het tweede lid aan een cyberweerbaarheidsplan honderd punten worden toegekend. Hierbij kunnen maximaal veertig punten worden toegekend voor de onderdelen a (maatschappelijke impact) en b (slaagkans samenwerkingsverband) en maximaal twintig punten voor onderdeel c (innovatief karakter). Een subsidieaanvraag wordt ingevolge het derde lid hoger gerangschikt naarmate er meer punten aan het cyberweerbaarheidsplan zijn toegekend. De aanvraag met het hoogste aantal punten komt als eerste voor subsidie in aanmerking. Bij een overschrijding van het subsidieplafond worden aanvragen met een gelijk aantal punten onderling gerangschikt door middel van loting. Zoals in het algemeen deel van de toelichting is uiteengezet, volgt uit het vierde lid dat in het geval soortgelijke cyberweerbaarheidsplannen worden ingediend, alleen het plan met het hoogste aantal punten voor

subsidie in aanmerking komt. Een soortgelijk plan is een plan dat in doel en activiteiten veel overlap vertoont en waarvan de toegevoegde waarde erg gering is. Om effectief met de beschikbare publieke middelen om te gaan, wordt bij soortgelijke plannen daarom alleen het hoogst gerangschikte plan gehonoreerd.

Artikel 4a.2.10

In artikel 4a.2.10, eerste lid, is geregeld dat de subsidieontvanger medewerking moet verlenen aan de evaluatie van de effecten van de door hem uitgevoerde activiteiten. Dit is slechts anders indien dat redelijkerwijs niet van de subsidieontvanger kan worden verwacht. Verder werkt een subsidieontvanger ingevolge het tweede lid ook mee aan de verdere verspreiding van ervaringen en resultaten van het cyberweerbaarheidsplan door de Minister of een aangewezen derde. Hierdoor kunnen de resultaten en instrumenten die binnen de samenwerkingsverbanden worden ontwikkeld, worden gebruikt bij andere cyberweerbaarheidsnetwerken, waardoor er navolging kan plaatsvinden. Daarom wordt op grond van artikel 4a.2.11 bij de subsidieaanvraag en subsidievaststelling om een samenvatting van (de resultaten van) het cyberweerbaarheidsplan gevraagd die verder verspreid kunnen worden. Een subsidieontvanger is tot drie jaar na de subsidievaststelling gehouden om medewerking te verlenen aan de evaluatie en de verdere verspreiding van ervaringen en resultaten.

Artikel 4a.2.11

In dit artikel is bepaald welke gegevens de aanvrager moet verstrekken bij het doen van een aanvraag voor subsidie. Een aanvraag tot vaststelling van een subsidie behoort uiterlijk dertien weken na afloop van de realisatietermijn te worden gedaan indien de subsidieomvang meer dan € 25.000 bedraagt. Naast de in dit artikel genoemde gegevens gaat de aanvraag tot vaststelling ingevolge artikel 50, tweede lid, van het besluit vergezeld van een eindverslag omtrent de uitvoering en de resultaten van de activiteiten, een mededeling van andere inkomsten waarmee de uitvoering van het cyberweerbaarheidsplan is gefinancierd en indien het subsidiebedrag € 125.000 of meer bedraagt, een controleverklaring van een accountant of accountant-administratieconsulent waaruit blijkt dat met de aanvraag wordt voldaan aan de voorschriften bedoeld in artikel 4:45 van de Algemene wet bestuursrecht. Indien de subsidieomvang minder dan € 25.000 bedraagt, wordt de subsidie ambtshalve vastgesteld op grond van artikel 50, negende lid, van het besluit.

Artikel 4a.2.12

In het algemeen deel van de toelichting is uiteengezet dat bij de onderhavige subsidieregeling sprake is van staatssteun, die wordt gerechtvaardigd door de de-minimisverordening en artikel 18 van de algemene groepsvrijstellingsverordening. Daarom moet een aanvraag vergezeld gaan van een verklaring de-minimissteun (artikel 4a.2.11, eerste lid).

Artikel 4a.2.13

Op grond van artikel 4.10, tweede lid, van de Comptabiliteitswet 2016 bevat een subsidieregeling een tijdstip waarop de regeling vervalt. Deze subsidiemodule vervalt een jaar na inwerkingtreding van de module met ingang van 1 april 2019. Hierin komt tot uitdrukking dat het een beleidsexperiment betreft. Zoals in het algemeen deel van de toelichting is uiteengezet wordt op basis van de ervaringen in het pilotjaar bekeken of en zo ja, hoe de aanjaagfunctie van cyberweerbaarheidsnetwerken het meest effectief en efficiënt kan worden voortgezet.

Artikel II

In de Regeling openstelling EZK- en LNV-subsidies 2018 wordt de openstelling van het beleidsexperiment cyberweerbaarheid geregeld. Het subsidieplafond bedraagt € 1 miljoen. Aanvragen kunnen worden ingediend vanaf 16 april tot en met 31 mei 2018 17.00 uur.

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