provincie groningen

v o o r d r a c h t

29 januari 2019
Documentnummer: 2019-005564, ECP
Dossiernummer : K12452

Nummer 3/2019

Voordracht van Gedeputeerde Staten aan Provinciale Staten van Groningen in het kader van de consultatie van Provinciale Staten over het principebesluit van Gedeputeerde Staten om het project "Cyber Security Noord-Nederland" te subsidiëren.

1. Samenvatting

Ter gedeeltelijke financiering van het project "Cybersecurity Noord-Nederland", verzoekt de Rijksuniversiteit Groningen als penvoerder van het consortium om een financiële bijdrage uit het Ruimtelijk Economisch Programma ZuiderZeeLijn (REP-ZZL) ter grootte van € 3.242.785,-. Het project heeft als doel om onze economische infrastructuur te versterken en zal leiden tot directe groei van onze werkgelegenheid rondom het thema cybersecurity. Alles overwegende zijn wij tot de conclusie gekomen dat de Rijksuniversiteit Groningen en haar consortiumpartners een deugdelijke subsidieaanvraag hebben ingediend die voldoet aan de voorwaarden en criteria zoals wij die in het REP-ZZL kader hebben vastgelegd. Daarnaast past het voorgestelde project binnen een aantal vastgestelde provinciale beleidskaders. Wij hebben dan ook het principebesluit genomen om de gevraagde subsidie ad € 3.242.785,- toe te kennen. Middels deze voordracht stellen wij u in de gelegenheid wensen en bedenkingen te uiten voordat wij overgaan tot een definitief besluit.

2. Doel en wettelijke grondslag

De Rijksuniversiteit Groningen verzoekt ter gedeeltelijke financiering van het project "Cybersecurity Noord-Nederland" om een financiële bijdrage uit het Ruimtelijk Economisch Programma ZuiderZeeLijn (REP-ZZL) ter grootte van € 3.242.785,-.

In diverse commissievergaderingen is door uw Staten benadrukt dat zij betrokken willen worden bij de besluitvorming over de REP-ZZL projecten en wij hebben u toegezegd dit te doen. In dit verband verwijzen wij u naar ons, aan de Statencommissie Economie en Mobiliteit gericht schrijven d.d. 26 januari 2011, kenmerk 2011-04313/4/A.25, EZP.

Middels deze voordracht brengen wij u op de hoogte van ons principebesluit om de gevraagde bijdrage te verlenen. Middels deze voordracht stellen wij u in de gelegenheid wensen en bedenkingen te uiten voordat wij overgaan tot een definitief besluit.

3. Procesbeschrijving en planning

Onze regio kent een sterk en dynamische ICT-sector. Een sector waarbinnen bedrijfsleven, kennisinstellingen en overheid samenwerken rondom diverse thema’s. Cybersecurity is één van deze thema's. Dit omdat de toenemende digitalisering niet alleen kansen biedt maar ook een bedreiging kan vormen. Een bedreiging die alleen in een kans kan worden omgezet wanneer alle betrokken samenwerken. In het voorjaar van 2018 is er een gezamenlijk plan gemaakt, gelet op de hier aanwezige kennis, om van onze regio dé Cybersecurity regio van Europa te maken.

Het bezoek van Staatssecretaris Keijzer (Ministerie EZK) in april 2018 aan onze provincie bij de aftrap van het project "Lessen internetveiligheid op basisscholen" is het startmoment geweest voor het opstellen van deze REP-subsidieaanvraag. Digitale veiligheid is ook één van de projecten binnen het provinciaal programma Groningen@Work.

Om nadere samenwerking tussen de belangrijkste stakeholders op het gebied van digitalisering in de Provincie Groningen te bevorderen is in 2018 besloten tot de oprichting van de Coalitionboard. Hierin nemen vertegenwoordigers zitting vanuit onderwijs- en kennisinstellingen, de gemeente Groningen en provincie, met een staande uitnodiging voor participatie van het Ministerie van Economische Zaken en Klimaat (EZK). Het bedrijfsleven vraagt aandacht voor, en benadrukt het belang van, een doorlopende leerlijn van basisschool tot wetenschappelijk onderwijs om de kennis van digitale veiligheid te verbeteren. Daarom heeft de Provincie Groningen het initiatief ingebracht

om een dergelijke doorlopende leerlijn te implementeren. De Coalitionboard heeft het belang van een dergelijk initiatief onderschreven. Op basis daarvan zijn de kennisinstellingen met de Provincie Groningen aan de slag gegaan om een programma te ontwikkelen dat gericht is op kennisontwikkeling en product- en procesinnovaties, de vertaling van deze kennis naar onderwijsprogramma's en product/diensten-ontwikkelingen en concrete ondersteuning aan bedrijven/MKB.

4. Begroting
De kosten die met dit besluit aan de orde zijn bedragen € 3.242.785,-. Deze kosten worden gedekt uit het Ruimtelijk Economisch Programma ZuiderZeeLijn (REP-ZZL).

Kostenbegroting

Begroting (**exclusief BTW**)	**Totaal**
Gebouwen en onroerend goed	0
Grond	0
Machines en apparatuur	500.000,-
Te verbruiken materialen en hulpmiddelen	0
Loonkosten (interne uren)	5.374.680,-
Projectmanagementkosten	455.000,-
Kosten derden (o.a. advieskosten extern)	75.000,-
Reis- en verblijfkosten	0
Promotie en publiciteit	190.000,-
Overige kosten	442.227,-
Niet verrekenbare btw	Pm*
Totaal subsidiabel	**7.036.907,-**
Niet-subsidiabele kosten	n.v.t.
Totaal kosten project	**7.036.907,-**

Financiering

Financiering	**[euro's]**		**[%]**
Totaal private bijdragen	930.000,-		13%
Qbit		650.000,-	
TNO		280.000,-	
Totaal publieke bijdragen	1.104.122,-		16%
RUG		601.622,-	
Hanzehogeschool		502.500,-	
Matching Derden	1.760.000,-		25%
Gevraagde REP-bijdrage	3.242.785,-		46%
Totaal financiering project	**7.036.907,-**		**100**

NB: Van diverse andere partijen is een steunbetuiging ontvangen voor een 'In kind' bijdrage. Deze steunbetuigingen zijn niet opgenomen in bovenstaand overzicht. De supportletters zijn bijgevoegd bij deze aanvraag.

5. Inspraak/participatie
Niet van toepassing.

6. Nadere toelichting

Inleiding
Bijgevoegd projectvoorstel ("Cybersecurity Noord-Nederland") is in nauwe samenwerking met de Rijkuniversiteit Groningen, Hanzehogeschool Groningen, Noorderpoort, Alfa-college, Q-bit, TNO en Gemeente Groningen opgesteld, en behelst het opzetten van een Cyber Security Hub in Groningen. Het voorgestelde programma heeft een looptijd van vier jaar met als doel om het bedrijfsleven beter te helpen beschermen tegen cyber-aanvallen, de samenleving veiliger te maken, innovatie te bevorderen en werkgelegenheid te creëren.

Aanleiding
Digitalisering is noodzakelijk, maar er zijn ook **uitdagingen** op het gebied van veiligheid aan verbonden. Criminele activiteiten spelen zich meer en meer af in het 'cyber-domein' en vormen een toenemende dreiging voor burgers, bedrijven en organisaties. De digitale transformatie stelt de maatschappij voor veel (cybersecurity) vragen waar vaak nog geen antwoord op gevonden is. De benodigde kennis is er nog niet of is niet toegankelijk voor de partijen die deze kennis nodig hebben. Veel bedrijven, met name in het MKB, hebben behoefte aan deze kennis en ondersteuning van cybersecurity professionals. Maar op dit moment is het aantal experts onvoldoende en ook het aantal studenten met kennis van cybersecurity is beperkt. Daarnaast ontstaat er een grote vraag naar cybersecuritycursussen en -trainingen door de toenemende aandacht voor cybersecurity in bestaande functies en liggen er kansen voor het bundelen van de in de kennisinstellingen en bedrijven aanwezige kennis.

Om een **antwoord** te vinden op deze uitdagingen is het noodzakelijk om samen te werken op het gebied van cybersecurity. Door gezamenlijk meer onderzoek te doen ontstaat er nieuwe kennis. Door de samenwerking tussen bedrijven, onderwijs- en kennisinstellingen en overheden te faciliteren, vindt er meer kennisdeling en -overdracht plaats, kunnen (cybersecurity) opleidingen worden ontwikkeld en worden meer studenten opgeleid tot cybersecurity professionals.

Het programma heeft een **sterk economische component.** Het onderzoek leidt tot nieuwe kennis en daarmee nieuwe producten en diensten die door (Noord-Nederlandse MKB) bedrijven kunnen worden gebruikt. Nieuwe kennis wordt, via bestaande organisaties en instellingen zoals Venturelab en het Marian van Os Centrum voor Ondernemerschap gekoppeld aan ondernemers die nieuwe bedrijven kunnen beginnen. Het project heeft als doelstelling om 500 nieuwe banen te realiseren, 15 nieuwe startups te creëren en via het MKB-support faciliteit duizend ondernemers per jaar te ondersteunen. Dit alles heeft tot gevolg dat bedrijven hun innovatiekracht en hun concurrentiepositie kunnen vergroten en dat de Noord-Nederlandse (digitale) economie veilig en duurzaam kan blijven groeien.

Impact
Door een ambitieus programma uit te voeren breiden we bestaande initiatieven uit en bouwen we aan onderzoeksprojecten waarin bedrijven, kennisinstellingen en de overheid nauw samenwerken aan het ontwikkelen en implementeren van cybersecurityoplossingen met als uiteindelijk doel dat onze (Noord-Nederlandse) samenleving beter beschermd wordt tegen cyberaanvallen.
Deze doelstellingen zijn vertaald in vijf ambities:

- *Versnellen en uitbreiden van onderzoek en kennisontwikkeling*

Er is nieuwe kennis nodig om een leidende rol in cybersecurity te kunnen spelen. Niet alleen technische kennis, er is een grote behoefte aan juridische- en gedragswetenschappelijk kennis. Bij de start van het programma "Cybersecurity Noord-Nederland" richt de RUG de leerstoel "Recht en Veilige Digitale Transformatie" in. De Hanzehogeschool breidt naar haar lectoraten "Juridische aspecten van de arbeidsmarkt" en New Business & ICT uit met het onderwerp cybersecurity. Noorderpoort en het Alfa-college stellen ten behoeve van het onderzoek gezamenlijk een practor aan en TNO stelt zijn onderzoekexpertise op het gebied van cybersecurity beschikbaar.

- *De weerbaarheid van (MKB) bedrijven te vergroten door middel van verbeterde kennis- en expertisedeling.*

Bedrijven en organisaties, en met name het MKB, hebben behoefte aan ondersteuning door professionals en praktische tools om haar weerbaarheid te vergroten. Het gaat hierbij niet alleen om technische tools maar juist ook om bewustwording, gedragsverandering en managementvaardigheden. Binnen dit programma worden deze tools ontwikkeld en geïmplementeerd.

- *Het ontwikkelen van test faciliteiten*

Internet of Things (IoT)" is één van de eerste toepassingsgebieden van het programma. Gevolg van de groei van het IoT is dat burgers en bedrijven meer last krijgen van criminele activiteiten (hacken, diefstal) en bedreigingen van hun veiligheid. Het is dus van groot belang dat (digitale) producten die op de markt komen veilig en beschermd zijn en dat deze uitvoerig getest zijn. Een van de eerste activiteiten van het programma is dat er, onder leiding van Qbit, een 'virtueel IoT security test lab' wordt opgezet in Groningen.

- *Via nieuwe kennis tot nieuwe producten en diensten en meer cybersecurity professionals*

De uit de onderzoeksprojecten verkregen kennis is belangrijk voor de toekomst. Het draagt bij aan een veiligere digitale omgeving, zorgt voor nieuwe producten en diensten en het biedt startups de gelegenheid deze verworven kennis om te zetten in nieuwe innovaties. Ook wordt nieuwe kennis gebruikt voor het reguliere en commerciële opleidingen. Opleidingen die er weer voor zorgen dat een groot aantal deskundigen en/of studenten met kennis van cybersecurity op de markt verschijnen. Deskundigen waar bedrijven met smart op zitten te wachten. Het programma heeft een speciaal werkpakket ingericht gericht op de valorisatie van resultaten.

- *Groei en continuïteit*

Het is belangrijk dat de continuïteit van het programma tijdens en na afloop van de "subsidieperiode" geborgd wordt. Daarom worden er al snel projectactiviteiten gestart ter bevordering van deze continuïteit. Voorbeelden daarvan zijn: beschikbaar stellen kennis en instrumenten aan het werkveld, stimuleren van ondernemerschap, zorgen voor aanvullende financiering voor het onderzoek, aansluiten bij andere initiatieven (regionaal, nationaal).

Resultaten

Voortbordurend op bestaande initiatieven streeft het programma er naar het bestaande in beeld te brengen en nieuwe ontwikkelingen in gang te zetten. Dit levert na vier jaar de volgende resultaten op:

- Een **netwerk** van bedrijven, kennisinstellingen, aanbieders van (cybersecurity) IT, overheidsinstellingen die gezamenlijk participeren in cybersecurity-projecten;
- Een **onderzoeksomgeving** op het gebied van cybersecurity met nationale- en internationale bekendheid met daarbinnen een nieuwe leerstoelgroep (Rijksuniversiteit Groningen, Faculteit Rechtsgeleerdheid) waarin onderzoek wordt gedaan naar het juridisch kader voor een veilige digitale transformatie. Binnen deze onderzoeksomgeving heeft de Hanzehogeschool haar lectoraten "Juridische aspecten van de arbeidsmarkt" en New Business & ICT uitgebreid met het onderwerp cybersecurity en doen de mbo-instellingen Noorderpoort en Alfa-college via haar practoraat onderzoek op het gebied van cybersecurity.
- Ruim **500 nieuwe banen** die gerelateerd zijn aan het domein cybersecurity bij: 1. bestaande bedrijven die bezig zijn met de digitale transitie, 2. aanbieders van (digitale) diensten en 3. startups;
- **15 start ups** die actief zijn in het werkveld van de cybersecurity;
- Een '**virtueel IoT security test lab'**, waarin in 2022 ca. ca 50 professionals werken;
- **4000/5000 studenten** MBO, HBO en WO die via reguliere opleidingsprogramma's kennis hebben verkregen van cybersecurity;
- 10 nieuw ontwikkelde commerciële **opleidingsprogramma's**;
- **10 miljoen uitgaven voor R&D** op gebied van cybersecurity;
- Een speciaal ingerichte **MKB-support faciliteit**, ingericht in de Werkplaats voor Digitaal Vakmanschap (Noorderpoort), waar ca. 1000 MKB-organisaties per jaar van informatie worden voorzien en waarin diverse (netwerk) bijeenkomsten en (mini)conferenties worden gehouden;
- Via **netwerkbijeenkomsten**, (miniconferenties) worden honderden bedrijven geïnformeerd over het belang van cybersecurity en het de resultaten van het onderzoek.

Rapportage en Rol Provincie

Jaarlijks zal het college van GS worden geïnformeerd over de voortgang van het project. Een beknopte voortgangsrapportage over de uitvoering van het programma zal informerend worden voorgelegd aan Provinciale Staten.

De Provincie Groningen is mede-initiatiefnemer van het project en stelt een subsidie beschikbaar voor de uitvoering ervan. De Provincie Groningen participeert tijdens de uitvoering van het project niet direct als projectpartner in het project, dit om de digitaliseringsdoelstellingen en -ambities van het project en de provincie te borgen. Wel leggen de projectpartners via de Stuurgroep verantwoording af aan de Provincie Groningen.

Motivatie REP-ZZL bijdrage

Het voorgestelde programma levert een directe bijdrage aan de hoofddoelstelling van het REP (het versterken van kansrijke sectoren en de ruimtelijke-economische structuur van Noord-Nederland)

door het ondersteunen van bedrijven op het gebied van digitale weerbaarheid, het verrichten van onderzoek op het gebied van Cybersecurity en door het valoriseren van nieuwe kennis in nieuwe producten en diensten. Het voorgestelde programma levert een directe bijdrage aan Opgave C (Versterken innovatief vermogen bedrijfsleven en arbeidsmarkt) programmalijnen 9 (MKB-algemeen) en 10 (arbeidsmarktpotentieel).

Conclusie
Alles overwegende zijn wij tot de conclusie gekomen dat de Rijksuniversiteit en haar consortiumpartners een deugdelijke subsidieaanvraag hebben ingediend die voldoet aan de voorwaarden en criteria zoals wij die in het REP-ZZL kader hebben vastgelegd. Daarnaast past het projectvoorstel binnen een aantal vastgestelde provinciale beleidskaders. Wij hebben dan ook het principebesluit genomen om de gevraagde subsidie van € 3.242.785,- toe te kennen.

7. Geheimhouding
Niet van toepassing.

8. Voorstel
Wij stellen u voor het in ontwerp bij deze voordracht gevoegde besluit vast te stellen.

Groningen, 29 januari 2019.

Gedeputeerde Staten van Groningen:

F.J. Paas , voorzitter.

H. Schrikkema , locosecretaris.

Behandeld door : J.G. Siegers
Telefoonnummer : 06-25762435
e-mail : j.g.siegers@provinciegroningen.nl

Bijlagen bij de voordracht

Nr.	Titel	Soort bijlage
1	Projectvoorstel	projectvoorstel
2	Begroting	begroting

Nr, 3/2019

Provinciale Staten van Groningen:

Gelezen de voordracht van Gedeputeerde Staten van 29 januari 2019, nr. 2019-004261, ECP;

Gelet op
Onze brief aan de Statencommissie Economie en Mobiliteit d.d. 26 januari 2011, kenmerk 2011-04313/4/A.25, EZP;
De doelstellingen van het Ruimtelijk Economisch Programma ZuiderZeeLijn (REP-ZFZL);

Besluiten:

1. Kennis te nemen van het principebesluit van Gedeputeerde Staten een subsidie van € 3.242.785,- toe te kennen aan de Rijksuniversiteit Groningen voor het project Cybersecurity Noord-Nederland;
2. Vast te stellen dat Provinciale Staten hiermee in staat zijn gesteld wensen en bedenkingen te uiten.

Groningen,

Provinciale Staten voornoemd:

, voorzitter.

, griffier.