CS4NL

Breed Gedragen Programma Cybersecurity

Kennis en innovatie voor de Topsectoren

dcypher

Datum: 19 oktober, 2022

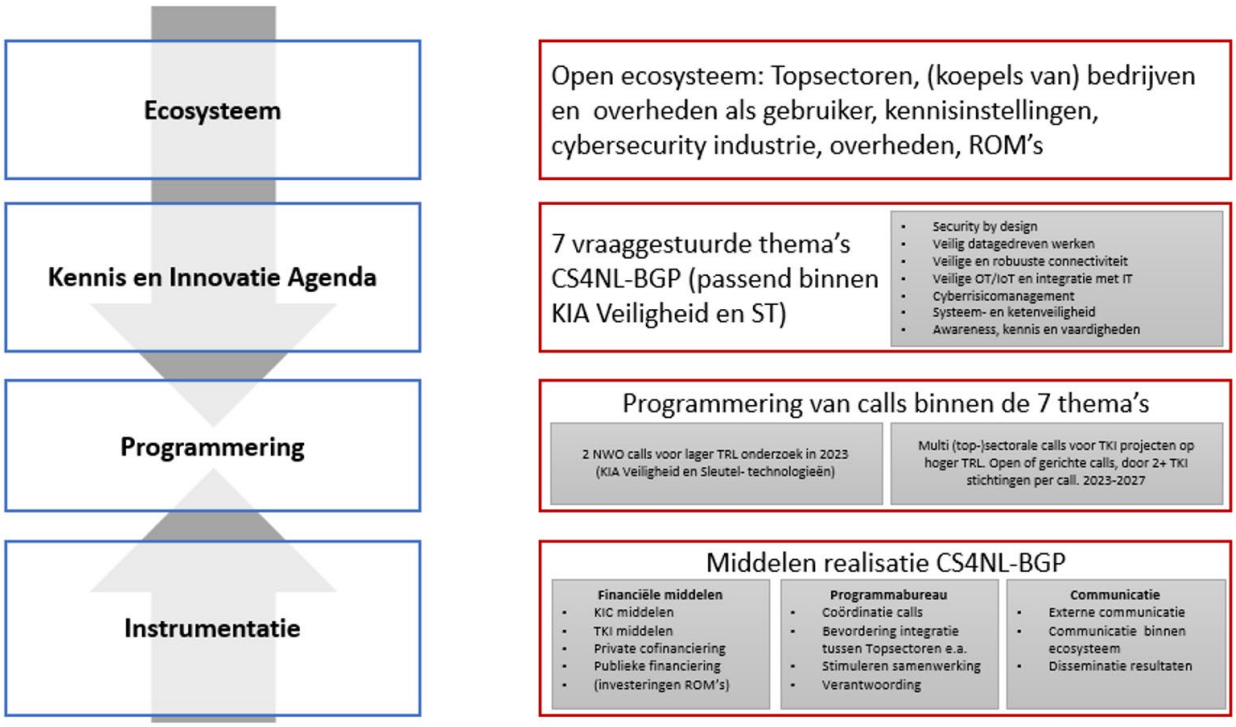
Topsector ICT & dcypher

dutch digital delta
connect and create

Na goedkeuring door het Kern- en Thematean van de Kennis- en Innovatie Agenda Sleuteltechnologieën op 3 oktober 2022, gaat per 1 januari 2023 het Breed Gedragen Programma (BGP) Cybersecurity kennis en innovatie voor de Topsectoren van start, onder de naam CyberSecurity voor Nederland (CS4NL). CS4NL-BGP zal o.a. NWO-calls en calls op basis van Topsectoren-middelen coördineren, om tot impactvolle kennis- en innovatieprojecten te komen. Daarnaast wordt vanuit het CS4NL met partners gewerkt aan doorontwikkeling, waaronder een mogelijk Nationaal Groeifondsvoorstel voor cybersecurity. Samengevat "10-7-2": CS4NL biedt een ecosysteem rond de 10 Topsectoren, een kennis- en innovatieagenda met 7 vraaggestuurde thema's en 2 programmeringsstromen.

Cybersecurity is randvoorwaardelijk voor het veilig en toekomstbestendig functioneren van de Nederlandse samenleving, die in rap tempo digitaliseert. Cybersecurity draagt ook bij aan economische groei. Het belang én de urgentie worden inmiddels onderkend. Het onderwerp heeft dan ook een belangrijke plek in het Missiegedreven en Topsectoren en Innovatiebeleid (MTIB). De maatschappelijke transities waar Nederland voor staat, zijn immers vaak afhankelijk van digitalisering en dat kan alleen verantwoord met de cybersecurity ook op orde. Soms kan dat met bestaande technologie, soms zijn nieuwe oplossingen nodig. Het belang en impact van digitalisering en de complexiteit van de bijbehorende nieuwe cybersecurity-oplossingen, maken het noodzakelijk dat multidisciplinair, (top-)sectoroverstijgend en in het hele ecosysteem wordt samengewerkt. Om de samenwerking voor nieuwe oplossingen te bespoedigen, is op initiatief van de Kennis- en Innovatie Agenda (KIA) Sleuteltechnologieën (ST) en in samenwerking met de KIA Veiligheid het voorstel voor BGP Cybersecurity (nu: CS4NL-BGP) geschreven. De Topsector ICT en dcypher zijn de penvoerders van dit programma.

CS4NL-BGP beoogt door het bespoedigen van samenwerking via programmering van open en gerichte subsidieoproepen (calls) een substantiële impuls te geven aan cybersecurity-kennis en -innovatie in Nederland. Deze kennis en innovaties dienen bij te dragen aan oplossingen die maatschappelijke transities en de bijbehorende veilige digitale transformaties bespoedigen. Dit heeft direct en indirect ook economische impact. De essentie van CS4NL-BGP is weergegeven in onderstaande figuur.

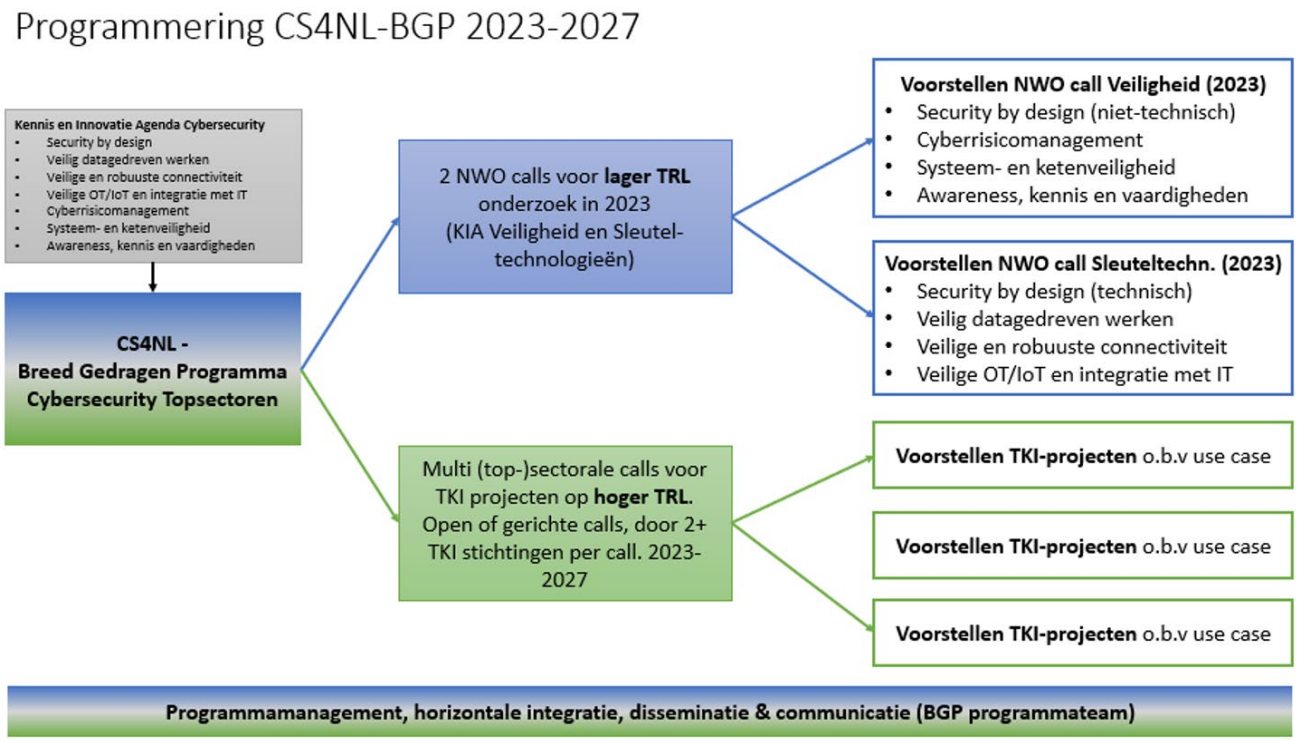


Figuur: overzicht van CS4NL (BGP Cybersecurity deel)

CS4NL betrekt de hele innovatieketen: wetenschappelijk en toegepast wetenschappelijk onderzoek, cybersecurity bedrijven, de industrie die cybersecuritytoepassingen in producten verwerkt én de private en publieke eindgebruikers. Aan de basis van CS4NL staat dCSaarom een breed ecosysteem, dat bestaat uit alle topsectoren en organisaties uit hun achterban, de Academic Cyber Security Society (ACCSS), het HBO, NWO, TNO, Cyberveilig Nederland (cyberbedrijfsleven), Regionale Ontwikkelmaatschappijen (via Innovation Quarter) en het ministerie van Defensie. Via de KIA Veiligheid zijn ook de departementen van Economische Zaken en Klimaat (EZK) en Justitie en Veiligheid (JenV) betrokken. CS4NL is nadrukkelijk een open ecosysteem.

CS4NL werkt vraaggestuurd, vanuit de cybersecuritybehoeftes die voortvloeien uit de maatschappelijke transities en de bijbehorende digitale transformaties uit het MTIB. De gedeelde prioriteiten zijn benoemd in een agenda met zeven vraaggestuurde thema's: 1. Security by design, 2. veilig datagedreven werken, 3. veilige en robuuste connectiviteit, 4. OT/IT security, 5. cyberrisicomanagement, 6. systeem- en ketenveiligheid en 7. Cyber awareness, kennis & vaardigheden (human capital).

De beoogde looptijd van CS4NL is vooralsnog vijf jaar, vanaf 2023 t/m 2027. De programmering verloopt langs 2 sporen. Ten eerste een spoor voor lagere technologiegereedheidsniveaus (TRL) o.b.v. NWO Missie calls. De duur van projecten in dit spoor is tenminste 48 maanden en wordt primair ingevuld door PhD-studenten. Ten tweede een spoor voor hogere TRL met Topconsortia voor Kennis en Innovatie (TKI) (innovatie-)projecten, met variabele duur (vaak kort-cyclischer dan het eerste spoor). Voor dit tweede spoor zijn de thema's door vertaald naar concretere probleembeschrijvingen (use cases).



Figuur: overzicht programmering CS4NL 2023-2027

Voor het eerste spoor zullen Kennis & Innovatie Convenant (KIC) NWO-middelen worden ingezet (v.u. KIA ST en KIA Veiligheid). Voor het tweede spoor worden TKI-middelen ingezet (PPS Toeslag en andere middelen), private cofinanciering vanuit bedrijven die werken 'in cyber' of 'met cyber', publieke cofinanciering (o.a. vanuit Defensie) en eventuele middelen van regionale ontwikkelmaatschappijen. Voor dit tweede spoor zet CS4NL het mechanisme van de multisectorale of cross-over calls in, waarin tenminste twee TKI-stichtingen (en eventueel Defensie) samen projectvoorstellen op gedeelde use cases beoordelen en laten uitvoeren. Net als de thema's zijn de use cases i.s.m. de Topsectoren en hun achterban uitgewerkt (zie de bijlagen). In totaal zijn 12 use cases voorbereid in het voorstel en nieuwe kunnen gedurende het programma worden toegevoegd.

De in het voorstel CS4NL-BGP genoemde bedragen zijn indicatief. Totaal is de bandbreedte 27 – 36 miljoen Euro over vijf jaar, maar voor de meeste KIC-partners is het zeker voor het tweede spoor pas mogelijk om commitment af te geven op concrete calls en projectvoorstellen. Voor het eerste spoor (NWO-calls) hebben de Kernteams ST en Veiligheid ook een belangrijke stem in de besluitvorming. Dit heeft geleid tot toezeggingen van totaal 10,5 miljoen euro KIC middelen, excl. private cofinanciering.

Deze werkwijze hangt samen met de aard van BGP's en de visie binnen de KIA-ST op gezamenlijk programmeren binnen BGP's (zie "Notitie BGP commitment en governance", 15 maart 2022): "Het doel van een BGP is te komen tot afstemming tussen KIC-partners over ST-ontwikkeling. Inhoudelijke afstemming moet vervolgens leiden tot synergie in de aanwending van KIC-middelen, zodat de gezamenlijke inzet meer is dan de som der delen." Voor CS4NL gaan we verder dan enkel afstemming en synergie. Het onderwerp cybersecurity is namelijk té urgent gezien de stijgende trend in cybersecurity incidenten en té belangrijk vanwege de toenemende digitalisering van onze maatschappij, om géén substantiële impuls te geven aan kennis en innovatie. We stoppen dus ook niet bij het BGP-deel, maar zetten voor CS4NL in op groei!