Breed Gedragen Programma (BGP) Cybersecurity

De Kennis en Innovatie Agenda Sleuteltechnologieën (KIA-ST) initieerde in het najaar van 2021 het Breed Gedragen Programma (BGP) Cybersecurity, waarvan Topsector ICT en dcypher trekker zijn. Voor het eerst werken alle 10 Topsectoren samen en dragen langs 7 thema's bij aan cybersecuritykennis en -innovatie ten behoeve van de maatschappelijke transities waar Nederland voor staat.

Cybersecurity is randvoorwaardelijk voor het veilig en toekomstbestendig functioneren van de Nederlandse samenleving die in rap tempo digitaliseert. Digitale veiligheid draagt ook bij aan economische groei. Het belang en impact van digitalisering en de complexiteit van de bijbehorende cybersecurity oplossingen, maken het noodzakelijk dat multidisciplinair, sector overstijgend en in de hele innovatieketen wordt samengewerkt. De massa die ontstaat door deze samenwerking zorgt voor tempo in de ontwikkeling. Hiervoor is het BGP Cybersecurity opgestart vanuit de KIA Sleuteltechnologieën. De Topsector ICT en dcypher zijn de trekkers. Digitale weerbaarheid, strategische autonomie en het verhogen van het economisch verdienvermogen van Nederland zijn de achterliggende belangen van het BGP Cybersecurity.

Het BGP Cybersecurity betrekt de hele innovatieketen: wetenschappelijk en toegepast wetenschappelijk onderzoek, het cybersecurity bedrijfsleven, de industrie die cybersecuritytoepassingen in producten verwerkt én de private en publieke eindgebruikers. Naast multisectorale projecten die concreet naar oplossingen toewerken, worden er ook NWO-calls geïnitieerd ter bevordering van het wetenschappelijk onderzoek van cybersecurity.

10 Topsectoren en 7 vraaggestuurde inhoudelijke thema's

Alle tien Topsectoren zijn aangesloten op het BGP Cybersecurity, net als ACCSS, Cyberveilig Nederland, NWO en TNO, kortom: de hele keten. Op zeven thema's worden concrete programma's van publiek-private samenwerking gevormd op basis van gedeelde innovatiebehoeftes uit de Topsectoren. De thema's zijn: Security by design, veilig datagedreven werken, veilige en robuuste connectiviteit, OT/IT security, cyberrisicomanagement, systeem- en ketenveiligheid en human capital.

Beoogde looptijd van het programma is 2023-2027. Dit programma draagt bij aan de verhoging van de digitale veiligheid in alle Topsectoren en daarmee het duurzame economisch verdienvermogen van die tien sectoren. Het zijn juist deze sectoren die internationaal gezien een uitstekende reputatie en uitgangspositie hebben om innovaties te ontwikkelen voor de maatschappelijke transities.

Meer informatie en contact via Topsector ICT en op de website van dcypher.

Q: Voor wie is het BGP Cybersecurity bedoeld?
A: Alle topsectoren onderschrijven het belang van samenwerking aan cybersecurity. Die samenwerking zal sectoroverstijgend zijn en zowel wetenschap, overheid als het bedrijfsleven in projecten samenbrengen. De hele innovatieketen wordt daarbij betrokken: van wetenschappelijk en toegepast wetenschappelijk onderzoek, het cybersecurity bedrijfsleven, de industrie die cybersecuritytoepassingen in producten verwerkt én de private en publieke eindgebruikers.

Q: Wat maakt het BGP Cybersecurity uniek?
A: Om de maatschappelijke transities te kunnen realiseren waar we als Nederland voor staan, moeten grote cybersecurity vraagstukken worden opgelost. Van die vraagstukken is een aantal relevant voor twee of meer Topsectoren. De belangrijkste cybersecurity thema's zijn voor het BGP in kaart gebracht; thema's die de basis zijn voor een kennis- en innovatieprogramma. Een stevig fundament van projecten en research calls op die thema's en de brede, vraag gestuurde benadering maken het BGP Cybersecurity uniek. De beoogde resultaten zijn innovaties die breed toepasbaar zullen zijn.

Q: Wat staat straks in het programmavoorstel BGP Cybersecurity?
A: Het beoogde programmavoorstel (en programma) zal uit de volgende onderdelen bestaan: 1. een inhoudelijke visie en kennis- en innovatie-agenda (de 7 thema's), 2. NWO-calls o.b.v. Kennis en Innovatie Convenant middelen voor wetenschappelijk onderzoek vanuit de Kennis en Innovatie Agenda's Sleuteltechnologieën en Veiligheid (onder voorbehoud van besluitvorming) en 3. op use cases gebaseerde projectvoorstellen binnen de 7 thema's.

Q: Wie beslist welke projecten in januari 2023 van start gaan?
A: Voor de op use cases gebaseerde projectvoorstellen beslissen de deelnemende partijen zelf. Dat zijn partijen met een use case (vraag, uitdaging of probleem) die binnen de genoemde thema's valt en op meerdere topsectoren en hun achterban betrekking heeft. Andere partijen die daar een antwoord op willen en/of kunnen vinden, kunnen daar op inspringen, samen met partijen die er financieel aan willen bijdragen. Zo ontstaan ketens van samenwerking, waarbij op elk van de thema's meerdere projecten kunnen ontstaan.

Q: Hoe kan ik een use case aanmelden?
A: De use cases worden via de topsectoren, gebruikersorganisaties, industrie of wetenschap aangedragen. Herkenning van de probleemstelling en bereidheid om mee te investeren van minimaal twee topsectoren is nodig. Het programmateam is het eerste loket voor voorstellen.

Q: Waar moet een use case aan voldoen?
A: Een use case is een cybersecurityprobleem, dat voortkomt uit een maatschappelijke transitie (bijvoorbeeld de energietransitie) en de bijbehorende digitalisering. De use case is relevant voor twee of meer topsectoren (die dat expliciet bevestigen) en er bestaat behoefte aan nieuwe kennis, technologie of innovatie rondom de use case. Projectvoorstellen o.b.v. use cases moeten worden gedekt door bestaande financiële regelingen van de topsectoren en andere bestaande publieke en private financieringsinstrumenten.

Q: wat gebeurt er in het BGP met een use case?
A: Use cases worden door een werkgroep bestaande uit vertegenwoordigers van topsectoren, wetenschap, TNO, NWO, industrie en anderen uitgewerkt tot zogenaamde projectkaarten. Dit zijn projectvoorstellen, inclusief beschrijving van doelen en onderzoeksvragen, beoogde deelnemers en financiële dekking (dat mag een mix van publieke en private middelen zijn). Uitwerking gebeurt in de periode april – juni 2022. Projectvoorstellen worden opgenomen in het voorstel BGP Cybersecurity, dat op 3 oktober 2022 ter besluitvorming wordt aangeboden aan het Thematteam Sleuteltechnologieën.