Topsectoren bundelen innovatiekracht cybersecurity in CS4NL

Den Haag, 19 oktober 2022 – CS4NL (*spreek uit: Sie Es for En El), voorheen het Breed Gedragen Programma Cybersecurity,* bundelt de cybersecurity innovatiekracht van alle Topsectoren in Nederland. Het programma pakt cyberveiligheidsvraagstukken op die voortkomen uit grote maatschappelijke transities en organiseert hiertoe efficiënte ketens van samenwerking. CS4NL richt zich op het bevorderen van cybersecuritykennis en -innovatie door het bundelen van vraag én aanbod op specifieke vraagstukken, het organiseren van een ecosysteem langs de hele valorisatieketen en het vrijmaken van nieuwe financiële middelen uit bestaande innovatie-instrumenten. “Het overkoepelende doel van CS4NL is niet alleen het versterken van de cyberweerbaarheid van Nederlandse organisaties. Het effect gaat namelijk zijn dat we er de Nederlandse economie en concurrentiepositie in de wereld mee versterken,” aldus Frits Grotenhuis, directeur Topsector ICT. CS4NL gaat werken met een geschat budget van 27 tot 36 miljoen euro over vijf jaar.

Samenwerking op zeven vraaggestuurde thema’s
CS4NL pakt zeven vraaggestuurde cyberthema’s op, die horen bij de grote maatschappelijke transities waar Nederland voor staat. Zoals de energietransitie, vernieuwingen in mobiliteit en het veilig verplaatsen van medische zorg naar huis. De CS4NL thema’s zijn relevant voor de cybersecurity-opgaven van twee of meer Topsectoren en betreffen security by design, veilig datagedreven werken, veilige connectiviteit, OT/IT security, cyberrisicomanagement, systeem- en ketenveiligheid en cyber awareness, kennis en vaardigheden. Eddy Boot, directeur dcypher: “Voor de thema’s hebben we op voorhand onderzocht of bestaande kennis en technologie kunnen worden ingezet, maar dat bleek niet het geval. Er is nog veel ontbrekende kennis en technologie en bestaande concepten zijn nog niet toepasbaar op specifieke transities. Daar gaan we nu keihard aan werken.”

Van thema’s naar investeringen in kennis en innovatie
Op de zeven thema’s worden calls voor wetenschappelijk onderzoek uitgezet. Kennisinstellingen kunnen hierop inschrijven in samenwerking met het bedrijfsleven, overheden en maatschappelijke organisaties. Dit versterkt de cybersecuritykennisbasis in Nederland. Ook zijn voor elk van de thema’s verdiepende praktische probleemstellingen gedefinieerd (‘use cases’). Deze vormen het vertrekpunt voor extra calls voor gerichte innovatietrajecten vanuit de Topsectoren. Ook hiervoor kunnen breed samengestelde consortia zich inschrijven.

Tot dusverre zijn twaalf use cases uitgewerkt. Waaronder veilige digitalisering van patiëntenzorg op afstand; zekerheid over de juistheid van sensordata van windmolenparken voor veilig onderhoud en leveringszekerheid van energie; het beter begrijpen van de steeds complexere IT en OT systemen en netwerken die nodig zijn voor maatschappelijke sectoren als energie, waterbeheer en tuinbouw, en cyberweerbaarheid van kleinere ondernemingen in o.a. de logistieke sector. De calls rondom de thema’s voor onderzoek en use cases voor innovatie gaan naar verwachting vanaf 2023 van start.

Het belang van cybersecurity
De maatschappelijke transities waar Nederland voor staat, leunen sterk op betrouwbare en veilige digitalisering. Cybersecurity is dus randvoorwaardelijk voor het verantwoord en toekomstbestendig functioneren van de Nederlandse samenleving en de economische groei. Het belang én de urgentie van digitale weerbaarheid worden breed onderkend, o.a. door de talrijke ransomware-aanvallen en de oorlog in Oekraïne. Het onderwerp heeft dan ook een plek in het Missiegedreven Topsectoren- en Innovatiebeleid (MTIB).

Stevig fundament
Aan de basis van het CS4NL staat een breed ecosysteem dat bestaat uit alle tien Topsectoren en organisaties uit hun achterban. Zo hebben de Academic Cyber Security Society (ACCSS), het HBO, NWO, TNO, Cyberveilig Nederland (cyberbedrijfsleven), Regionale Ontwikkelmaatschappijen (via Innovation Quarter) en het ministerie van Defensie als eindgebruiker van cybersecurity meegewerkt aan de totstandkoming ervan. Via de KIA Veiligheid zijn ook de departementen van Economische Zaken en Klimaat (EZK) en Justitie en Veiligheid (JenV) betrokken. Het programma is geïnitieerd door Topsector ICT en dcypher binnen de Kennis en Innovatie Agenda Sleuteltechnologieën.

Noot voor de redactie

Over Topsector ICT
Topsector ICT identificeert, prioriteert en organiseert ICT-onderzoek en innovatie door publieke en private partijen bijeen te brengen met focus op ICT-sleuteltechnologieën en maatschappelijke uitdagingen. Hierbij bestrijkt Topsector ICT het traject van fundamenteel onderzoek tot en met valorisatie. Opleiden van nieuw talent, om- en bijscholing, kennis-disseminatie, breed betrekken van MKB en internationale samenwerking vormen een belangrijk onderdeel van de missie. www.dutchdigitaldelta.nl

Over dcypher
dcypher is het samenwerkingsplatform voor onderzoek en ontwikkeling op het gebied van cybersecurity in Nederland. dcypher faciliteert bedrijven, kennisinstellingen en overheden die samen willen werken om Nederland digitaal veiliger, sterker en autonomer te maken. Bij dcypher vindt u de partners, financiering en expertise om onderzoek om te zetten in effectieve toepassingen, cyberbeveiligingsprofessionals op het hoogste niveau op te leiden en de Nederlandse kennispositie op het gebied van cybersecurity te versterken.
www.dcypher.nl

Meer informatie
Tessa Weber
PR- en communicatieadviseur Topsector ICT
E: tessa.weber@dutchdigitaldelta.nl
T: +316 1415 5898

Marcel Ruijken
Communicatieadviseur dcypher
E: marcel.ruijken@dcypher.nl
T: +316 5436 2331