Geüpdate samenvatting van de call tot het indienen van aanvragen voor PPS-Innovatie middelen bij Topsector ICT en Topsector LS&H, betreffende de 3e Cybersecurity TKI-call: "Veilige sensoren in de thuis- en ziekenhuisomgeving" voor publiek-private samenwerking in 2025[1]

Introductie

Topsectoren werken regelmatig samen met andere Topsectoren aan thematische TKI cross over calls. Topsector ICT en Topsector LSH trekken dit jaar gezamenlijk op in een TKI-cross-over call op het gebied van Cybersecurity Technologies[2], met als thema: "Veilige sensoren in de thuis- en ziekenhuisomgeving". Dit thema past binnen het thema Cybersecurity onder de vlag van de KIA Digitalisering, de Nationale Technologie Strategie en is gelieerd aan het domotica en het Internet of Things thema. Deze call is relevant voor vakgroepen en bedrijven die werken op het gebied van sensoren/sensoriek, cybersecurity, medische technologie, (intramurale/thuis) zorg en domotica. Topsectoren ICT en LSH stellen in 2025 hiervoor gezamenlijk 2€ miljoen PPSi-middelen beschikbaar.

Kernvereisten

- Het onderzoek past binnen de missie van Topsector ICT zoals beschreven in de Kennis- en Innovatie Agenda (KIA) Digitalisering en de centrale missie van Topsector LS&H zoals beschreven in de KIA Gezondheid & Zorg 2024-2027.
- Het onderzoek past binnen tenminste één van de prioritaire **digitale** sleuteltechnologieën uit de Nationale Technologie Strategie (NTS): 'Cybersecurity Technologies' of AI/Data. Onderzoek en innovatie op het snijvlak van andere technologieën en toepassingsdomeinen wordt aangemoedigd.
- Het project is van maatschappelijke en economische toegevoegde waarde.
- De hoofdaanvrager is een in Nederland gevestigde onderzoeksorganisatie of een in Nederland gevestigde onderneming met winstoogmerk.
- Het consortium bestaat uit tenminste één onderneming met winstoogmerk en één onderzoeksorganisatie.
- Het project wordt uitgevoerd voor gezamenlijke rekening en risico.
- Het project omvat industrieel onderzoek of experimentele ontwikkeling, of een combinatie daarvan.
- Het project duurt maximaal 3 jaar.
- Per project mag het consortium in totaal aanspraak maken op maximaal €500.000,00 PPSi-middelen
- Voor onderzoeksorganisaties geldt een maximum van 70% financiering via PPSi-middelen (zowel voor industrieel onderzoek, als experimentele ontwikkeling).
- Voor mkb geldt een maximum van 60% financiering via PPSi-middelen bij industrieel onderzoek en een maximum van 40% financiering via PPSi-middelen bij experimentele ontwikkeling.

---

[1] Dit is een samenvatting van de call. Hieraan kunnen geen rechten worden ontleend. De definitieve integrale call-tekst wordt begin juli gepubliceerd door Topsector ICT.

[2] https://www.rijksoverheid.nl/documenten/beleidsnotas/2024/01/19/de-nationale-technologiestrategie

De deadline is **13 oktober 2025 CET 17:00**
De beoordeling vindt plaats op basis van de volgende criteria en onderdelen van het aanvraagformulier:

- Passendheid binnen de PPS-Innovatieregeling;
- Passendheid binnen tenminste één van de prioritaire **digitale** sleuteltechnologieën uit de Nationale Technologie Strategie (NTS): 'Cybersecurity Technologies' of 'AI/Data'.
- Passendheid binnen de KIA Digitalisering en de KIA Gezondheid & Zorg
- Wetenschappelijke kwaliteit;
- Impact en relevantie;
- Haalbaarheid;

In aanloop naar de deadline bestaat de mogelijkheid om consortium specifieke vragen te stellen aan het Topsector ICT team. Deze vragen kunnen tot een week voor de deadline van de volledig uitgewerkte aanvraag worden ingediend door te mailen naar Topsector ICT via calls@topsector-ict.nl met als onderwerp: *Advies TKI call Veilige Sensoren - <naam hoofdaanvrager>.*

Context

Steeds meer apparaten zijn/worden slim en steeds meer van die slimme apparaten zijn op de een of andere manier gekoppeld aan elkaar in de thuiszorg- en ziekenhuisomgeving. Inzicht en kennis over hoe om te gaan met indringers buitenaf (*intrusion detection*) en binnenuit (*insider threat*) is nodig. Nieuwe (*Internet of Things*) systemen zijn bij patiënten (zoals apps en sensoren) in veel gevallen indirect of direct ook gekoppeld aan een groter geheel, zoals de ICT-infrastructuur van een zorginstelling.

De zorgsector is bij uitstek een sector waar digitalisering een enorme vlucht heeft genomen. Denk hierbij aan het gebruik van elektronische patiënt dossiers, de inzet van sensors en apps om patiënten op afstand te monitoren, het toepassen van kunstmatige intelligentie/machine learning voor diagnosestelling en behandeling, en het beschikbaar stellen van informatie aan patiënten en cliënten via portalen en persoonlijke gezondheids-omgevingen.

De verplaatsing van zorg naar de thuissituatie is al in volle gang waarbij gebruik wordt gemaakt van medische apparatuur en applicaties. Zorginstellingen werken steeds meer samen in de (zorg)keten en gedragen zich steeds meer als netwerkorganisaties. Door de verplaatsing van zorg naar de thuissituatie wordt de thuis-/ leefomgeving ook onderdeel van de zorgketen. In de thuissituatie wordt vaak gebruik gemaakt van medische technologie; in combinaties van medische apparatuur, wearables (sensors en apps) en (cloud)applicaties. Specifiek is in de thuissituatie sprake van een combinatie van (gecontroleerde) apparatuur van zorginstellingen en niet-gecontroleerde sensors/apps en netwerkverbindingen van de consument.

In de zorg van morgen gaan persoonlijke zorg en technologie hand in hand samen. Hybride zorg is de norm, waarbij technologie mensen ondersteunt die hulp nodig hebben én naasten en professionals helpt om de juiste zorg op de juiste plaats te bieden. Door samen met de diverse sectoren in de ICT-technologie te ontwikkelen die eenvoudig in gebruik, schaalbaar en betaalbaar is, blijft de zorg overal en voor iedereen toegankelijk. Voor het ministerie van VWS wordt thuiszorg steeds belangrijker om

zo de ziekenhuizen te ontlasten[3]. Dat kan met goed ontwerp en gebruik van ICT (zoals veilige sensoren). Hoe betrouwbaar is echter het contact met doctoren en gezondheid instellingen zoals ziekenhuizen? Hoe kunnen we ervoor zorgen dat de cyberveiligheid twee kanten (van thuis naar ziekenhuis en andersom) op wordt gegarandeerd? Het kan gaan om levensbedreigende situaties als de veiligheid niet wordt gewaarborgd.

Verschillende soorten sensoren

Een sensor is een kunstmatige uitvoering van wat in de biologie een zintuig wordt genoemd. De meeste sensoren zijn elektronisch of mechanisch uitgevoerd, softwarematige en 'virtuele' sensoren zijn ook mogelijk. Met een sensor neemt een machine de omgeving waar of kan informatie verzameld worden waarmee processen gemonitord en bestuurd kunnen worden.
Voorbeelden van sensoren in de zorg zijn:

- Valsensoren
- Slimme lampen en thermometers
- Ritme sensoren
- Geluidssensoren

Sensor data is informatie die wordt verzameld door diverse typen sensoren. Sensoren detecteren en meten verschillende fysieke parameters, zoals temperatuur, druk, licht, beweging, vochtigheid en geluid, en zetten deze metingen om in gegevens die vervolgens kunnen worden geanalyseerd en verwerkt. Sensor data vormt daarmee een essentieel onderdeel van Internet of Things (IoT)-systemen.

Meer over het Cybersecurity thema

Data uit sensoren moet betrouwbaar zijn en afkomstig van de bron zijn, en onderweg niet gemanipuleerd kunnen worden. De CIA-triade[4] is een van de fundamentele modellen die worden gebruikt om beleid en strategieën voor het beschermen van informatie te sturen. De "CIA" in de triade staat voor Vertrouwelijkheid, Integriteit en Beschikbaarheid - drie primaire doelstellingen die organisaties moeten waarborgen om hun gegevens, communicatie en infrastructuur te beschermen tegen kwaadwillende aanvallen en onbedoelde inbreuken. Deze drie pijlers zijn essentieel voor het handhaven van een veilig en betrouwbaar netwerk, waardoor de CIA-triade een hoeksteen is van moderne cyberbeveiligingspraktijken.

Door ontwikkeling van kennis in de ontwikkelingen die er zijn op het gebied van datamanipulatie en innovatie, om die manipulatie te voorkomen en te detecteren wanneer het gebeurt, kunnen we als Nederland de operatie van onze ziekenhuis en thuiszorg infrastructuren veiligstellen. Deze call richt zich niet enkel op de sensoren zelf, maar ook op de dataverbinding met andere partijen in de keten, en de systemen die de data verwerken. Het kader is breed: het kan gaan om van sensor data naar de cloud en van de cloud naar de toepassing. De rode draad in deze call gaat over hoe je sensoren inherent veilig krijgt, zowel de hardware als de software als hun context/ecosysteem (netwerken, data en de rest van de stack), idealiter vanuit het *cybersecurity by design* paradigma. *Cybersecurity by design* is een belangrijk principe in de wereld van cybersecurity. Het houdt in dat beveiliging vanaf het begin van het ontwerpproces van een systeem of applicatie wordt geïntegreerd. Ook autonome

[3] https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2022/09/16/integraal-zorgakkoord-samen-werken-aan-gezonde-zorg/integraal-zorg-akkoord.pdf
[4] https://cwgreenport.nl/de-basis-van-informatiebeveiliging-de-cia-triade/

systemen en zelfbeschermingsvermogen kan worden meegenomen in het onderzoek en ontwikkeling binnen deze call.

Scope en onderzoeksvragen op hoofdlijnen, kennis/innovatie vragen:

- Hoe kan de authenticiteit van (cruciale) databronnen voor inspectie en detectie van problemen in de fysieke infrastructuur worden gewaarborgd; welke problemen zijn daarbij leidend?
- Hoe kan de authenticiteit, de integriteit, de confidentialiteit en beschikbaarheid van datastromen, zoals bescherming tegen spoofing worden gewaarborgd?
- Hoe beïnvloeden Internet of Things (IoT) systemen binnen de thuis- en ziekenhuisomgeving? Welke nieuwe IoT systemen zorgen voor welke mogelijke nieuwe dreigingen?
- Hoe kunnen we zorgen voor vernieuwing op het gebied van *intrusion detection* door voorspellen en monitoring van systeemprestaties, met gekoppelde nieuwe apparaten en versmelting van verschillende systemen die voorheen ontkoppeld waren? Welke vernieuwing is er nodig om *intrusion detection* geschikt te maken voor deze meer gekoppelde en complexe systemen?
- Hoe kunnen we securityproblemen (design) voorkomen, inbreuken detecteren, hoe daarop te reageren (response), welke aanvallen zijn er mogelijk, hoe moet de governance ingericht zijn, en hoe past de wet- en regelgeving hierin?
- Hoe kan het spanningsveld tussen gebruiksvriendelijkheid van securitymaatregelen het beste worden geregeld?
- Wat zijn de barrières (cyberrisico's), maar ook de drijfveren voor succes (maatregelen), om elk individu cyberveilige, gebruiksvriendelijke zorgoplossingen (medische apparatuur en applicaties) te bieden en te gebruiken in zijn of haar eigen leef- (of werk-) omgeving?
- Welke eisen stelt de *Medical Device Regulation* (MDR)[5] aan cybersecurity? In hoeverre zijn deze eisen concreet toepasbaar (blijft het apparaat of de app gebruiksvriendelijk per doelgroep?), hoe verhouden de eisen zich tot (inter)nationale standaarden en hoe certificeren we de security aspecten?
- Hoe worden de verschillende methodieken en de MDR-eisen in de praktijk toegepast door leveranciers, zorginstellingen en toezichthouders?

[5] https://english.igj.nl/medical-technology/new-european-regulations-mdr-and-ivdr