

Risk Based Cyber Security Chain

Publieke samenvatting / Public summary

Aanleiding

In de huidige samenleving zijn eindproducten het resultaat van complexe, non-lineaire ketens van bedrijven. Tegelijkertijd vindt er een digitaliseringslag plaatst, waarbij IT partijen een belangrijke rol in de keten spelen. Daarnaast zijn ketens heterogeen, met organisaties verschillend qua grootte, sector, geopolitieke locatie en mate van cyber-volwassenheid. Ketens brengen een complex scala aan veiligheidsrisico's met zich mee, welke mede door het cascade effect tot grote financiële en maatschappelijke consequenties kunnen leiden. Nieuwe wetgeving (NIS2) legt de verantwoordelijkheid voor de cyberveiligheid bij afnemers in de keten, waarbij - indien men in gebreke blijft - boetes te verwachten zijn. Om de ketenproducten en de daarbij behorende datastromen op een verantwoorde, efficiënte manier te beveiligen is een integrale ketenaanpak benodigd.

Doelstelling

In dit voorstel, onderzoekt en ontwikkelt het consortium een robuuste security-ketenarchitectuur, die enerzijds een aanpak biedt voor overleg binnen de keten om gezamenlijk tot een veilige aanpak te komen, alsmede een raamwerk van risico-gebaseerde beveiligingsmaatregelen. De aanpak is risico-gebaseerd met weerbaarheid als doel, voor een balans tussen veiligheid en kosten. Het werkveld geeft aan dat er bij een gezamenlijke ketenaanpak veel logistieke en organisatorische uitdagingen zijn. Daarom wordt specifiek aandacht besteed aan de besturing en kennisoverdracht binnen de keten: hoe spreek je elkaar aan en help je

Projectinformatie / Project information

Projectnummer / Project number

TKITOETKI23-RBCSC_(CS4NL)

Subsidiebedrag / Grant amount

€ 351.509,00

Algemene informatie / General information

Penvoerder / Secretariat

Hogeschool Utrecht

Volg Topsector Energie op X / Follow Topsector Energie on X

@TSEnergie

elkaar met de veiligheid bij de ander, welke indirect of direct invloed heeft op je eigen bedrijfsvoering.

Korte omschrijving

Het consortium ontwikkelt: (a) een overlegmodel voor het uitwisselen van kennis en ervaring tussen de ketenpartijen, rekening houdend met verschil in kennis en omvang van de partijen; (b) een beschrijving van een algemeen toepasbaar proces en op te leveren resultaten voor de ontwikkeling van cyber security ketenarchitectuur; en (c) een ketenarchitectuur voor de Energiesector, op basis van de deze aanpak. Het overlegmodel is gebaseerd op bestaande methoden voor kennisuitwisseling maar specifiek toegepast op ketenpartijen met uiteenlopende expertisen en volwassenheid. De ketenarchitectuur combineert kaders en praktijken van huidige ramenwerken en standaards om een integraal aanpak te ontwikkelen met bijzondere focus op keten-brede maatregelen. De toepassing daarvan op CO₂-vrije energieopwekking is nieuw in deze vorm. De coalitie richt zich op de Topsectoren ICT en Energie. Voor ICT wordt een overlegmodel en de aanpak voor de ontwikkeling van ketenarchitecturen ontwikkeld; een concrete invulling daarvan wordt toegepast op kritische ketens bij de CO₂-vrije opwekking van energie. Dit is in lijn met de respectievelijk KIA's.

Resultaat

Het resultaat is een transparante analyse en innovatieve aanpak van de cyber weerbaarheid van de gehele keten (CS4NL-thema: "Identify and Address"). Onze insteek is te komen tot een model voor security-ketenarchitecturen die schaalbaar en bruikbaar zijn voor alle sectoren. Energieketens bestaan uit een breed pallet van bedrijven/dimensies/uitdagingen, zodat dit voorstel representatief is voor ketens en derhalve breed bruikbaar is. We kiezen voor een multidisciplinaire aanpak, waarin zowel academische en praktijk kennis gecombineerd wordt, alsmede de kennis van verschillende disciplines (cyber security, recht, bedrijfskunde, psychologie, architectuur). De coalitie bestaat naast kennisinstellingen uit een verscheidenheid aan private bedrijven, van

energieproducenten tot afnemers, van architecten tot ontwikkelaars, van grote multinationals tot MKB. Deze verscheidenheid aan kennis en ervaring, zichtbaar in de brede coalitie van deze aanvraag, zal leiden tot de vergroting van de cyberweerbaarheid binnen de Topsectoren.

De data in deze applicatie is afkomstig van de Rijksdienst voor Ondernemend Nederland (RVO) en wordt in samenwerking met de Topsector Energie ontsloten.

Voor meer informatie over de Topsector Energie, ga naar www.topsectorenergie.nl.

Voor meer informatie over de TSE / Energie-Innovatie regelingen die RVO aanbiedt, ga naar www.rvo.nl/tse.