H2O nieuws

Europese drinkwatersector wapent zich tegen cyberfysieke bedreigingen

20 juni 2017

De Europese drinkwatersector tilt de bescherming van de kritieke waterinfrastructuur tegen fysieke bedreigingen en cyberaanvallen naar een hoger niveau. Een aantal toonaangevende bedrijven en kennisinstituten ontwerpt hiertoe een geïntegreerd cyberfysiek systeem.

Deelnemers startbijeenkomst STOP-IT in Oslo

Het samenwerkingsproject waarbinnen dit plaatsvindt, heet STOP-IT. Deze afkorting staat voor ‘strategic, tactical, operational protection of water infrastructure against cyber-physical threats’. Aan het project nemen 22 waterbedrijven en kennisinstituten uit zeven Europese landen deel. De Nederlandse drinkwatersector wordt vertegenwoordigd door KWR Watercycle Research Institute. Het project is een belangrijk onderdeel van het onderzoeks- en innovatieprogramma Horizon 2020; de Europese Unie draagt bijna 8,3 miljoen euro bij.

De waterbedrijven worden door de snelle ICT-ontwikkelingen geconfronteerd met nieuwe soorten bedreigingen, vertelt Christos Makropoulos, Chief Information Officer bij KWR. “Wat vroeger als science fiction werd gezien, is nu werkelijkheid. De kritieke infrastructuur is door ICT-oplossingen veel opener dan vroeger, onder meer door het gebruik van sensors en actuatoren om op afstand verschillende onderdelen van de waterinfrastructuur te monitoren en bedienen. Hierdoor is het systeem kwetsbaarder geworden voor cyberaanvallen.” Het probleem is volgens Makropoulos dat het watersysteem van oudsher is ingericht als fysieke infrastructuur. Dat voldoet niet meer. “Er is een nieuwe manier van denken nodig. De fysieke en cyberkant moeten in één systeem worden geïntegreerd. Het ontwerpen van een cyberfysiek systeem is de grote uitdaging van STOP-IT.”

De deelnemers ontwerpen een risicobeheerkader, waarin methoden en instrumenten voor alle relevante risico’s zijn opgenomen. Dit kader is gebaseerd op ISO 31000, de internationale norm voor risicomanagement. Makropoulos benadrukt dat STOP-IT zich richt op drie niveaus: strategisch, tactisch en operationeel. “Ons doel is om deze niveaus met elkaar te verbinden. Dat is relatief nieuw. Tot nu toe werd bij cyberveiligheid vooral gekeken naar het operationele niveau en bij fysieke bescherming naar het strategische en tactische niveau.”

In het project worden ook methoden en softwareoplossingen ontwikkeld voor de bescherming tegen cyberaanvallen. De oplossingen worden in een modulair softwareplatform samengebracht. Hieruit kunnen waterbedrijven de voor hen relevante onderdelen selecteren en integreren in hun eigen bestaande systemen. Ook worden nieuwe onderzoeksideeën ontwikkeld om toe te passen voor de cyberveiligheid. Makropoulos noemt een voorbeeld. “We willen blockchaintechnieken, bekend van de bitcoin, gebruiken bij sensors. Je kunt zo voorkomen dat er wordt geknoeid met sensordata.”

Bij een aantal waterbedrijven worden projecten voor het demonstreren van oplossingen uitgevoerd. “Dat gebeurt bij de zogeheten frontrunner utilities ofwel voorloperbedrijven’ ”, licht Makropoulos toe. “Zij houden zich bezig met de hele watercyclus. Ook De Watergroep uit België, een nieuwe aandeelhouder van KWR, doet mee aan de demonstraties. De partners gaan kennis over oplossingen uitwisselen en informatie over bedreigingen en cyberaanvallen delen.”

KWR geeft binnen STOP-IT leiding aan de werkzaamheden in verband met de beoordeling en behandeling van risico’s op strategisch en tactisch niveau. Daarbij worden stresstesten uitgevoerd. KWR is ook betrokken bij het opzetten van een

praktijkgemeenschap voor de bescherming van de waterinfrastructuur. Makropoulos: “Het gaat om een platform voor eindgebruikers en ontwikkelaars. We leggen hierbij de verbinding met het brede Europese watertechnologieplatform WssTP. Want de resultaten van STOP-IT zijn van belang voor de hele watersector.”

Het Europese project duurt vier jaar. Wat wil Makropoulos dat er medio 2021 bereikt is? “Een cyberfysieke herziening van het watersysteem, een set van methoden en instrumenten op de drie niveaus en een actieve praktijkgemeenschap. En misschien wel het belangrijkste, dat er binnen Europa én wereldwijd grote aandacht is voor het cyberfysieke systeem.” Makropoulos wijst nog op de ontwikkeling richting een circulaire economie. “Ook dat vraagt om een geïntegreerde bescherming tegen risico’s.”