Waterschappen duiken in Internet of Things

Het Internet of Things kan waterschappen ondersteunen bij hun zorg voor droge voeten en schoon water. Voordat de waterbeheerders de mogelijkheden daarvan in het veld gaan beproeven, willen ze de apparatuur in een veilige omgeving toetsen op de cyberveiligheid. Vijf partijen werken met drie waterschappen aan de inrichting van LoRaWAN-netwerken voor uitgebreide testen.

Tekst: David van Baarle Fotografie: Industrie

Door veranderingen in het klimaat staan de Nederlandse waterschappen voor grote uitdagingen. Er is steeds vaker sprake van extreem weer met intense regenbuien, afgewisseld door langere periodes van droogte. Deze ontwikkelingen hebben een grote impact op de veiligheid en de economische bedrijvigheid in Nederland. Elk waterschap bereidt zich voor om de weerbaarheid tegen deze klimaateffecten in haar regio te verhogen. Dit zal mogelijk leiden tot een situatie waarbij er veel vaker en op veel meer plekken metingen moeten worden uitgevoerd van watergerelateerde omgevingsvariabelen. Ict kan de waterschappen ondersteunen bij het uitvoeren van deze taken en dan met name de nieuwe mogelijkheden die met het Internet of Things (IoT) beschikbaar komen. Zo kan het complexe systeem van sluizen, stuwen en waterkeringen mogelijk beter worden ingezet, naarmate er meer detailinformatie beschikbaar wordt gemaakt over bijvoorbeeld lokale omstandigheden.

Daarnaast kan ook de waterkwaliteit in het geding komen na lange perioden van droogte of in het geval van illegale lozingen. Ook dit kan worden gemonitord met slimme sensoren, die waarschuwen als kritische waarden worden overschreden.

Cybersecurity

Met het ontsluiten van de informatie in deze voor Nederland kritieke infrastructuur, ontstaat wel een nieuw probleem: hoe weet je zeker dat de sensorinformatie waar je je beslissingen op baseert, klopt met de realiteit en niet onderweg is gemanipuleerd? En hoe voorkom je dat derden toegang krijgen tot die informatie en daarmee mogelijk tot kritische assets? Om die vragen te beantwoorden, hebben TNO, TMX, Croonwolter&dros, Applied Risk en KPN, met de waterschappen Hunze en Aa's, Aa en Maas en Brabantse Delta het initiatief genomen tot een onderzoeksproject. Het project wordt uitgevoerd samen met het TKI Hightech Systemen en Materialen (HTSM), dat in de

Er is steeds vaker sprake van extreem weer met hevige en intense regenbuien.

Roadmap HTSM Security expliciet heeft aangegeven dat de bescherming van deze vitale infrastructuur een topprioriteit is. Het project is in januari gestart en gedurende achttien maanden werken de partners gezamenlijk aan het vinden van antwoorden op de onderzoeksvragen op basis van vier proefopstellingen: twee in het lab en twee in het veld.

Hiddo Hut is cybersecurity-expert bij TNO en samen met onder andere IoT-specialist Edwin Matthijssen verantwoordelijk voor de proeven die de partners gezamenlijk uitvoeren bij de veiligheidscluster The Haque Security Delta (HSD). Dit gebeurt met de uiteenlopende apparatuur die door de partners beschikbaar is gesteld. Hut: 'HSD biedt een centrale omgeving waar we onder gecontroleerde condities de testopstellingen kunnen realiseren en de apparatuur veilig kunnen testen. KPN, TMX, Applied Risk en Croonwolter&dros leveren de benodigde apparatuur en infrastructuur, maar stellen ook hun kennis op het gebied van zowel ict en systeembeveiliging, als ook procesautomatisering en informatisering beschikbaar. Daarnaast wordt nauw samengewerkt met de toekomstige gebruikers van deze nieuwe IoT-technologie: de waterschappen Hunze en Aa's, Aa en Maas en Brabantse Delta.'

Bescherming van deze vitale infrastructuur is een topprioriteit

LoRaWAN

Als communicatieprotocol kozen de partners voor Low power long range Wide area network (LoRaWAN)-technologie. 'KPN is de eerste partij in Europa die een landelijk dekkend LoRaWAN-net heeft aangelegd', zegt Matthijssen. 'Daarnaast kan het een voordeel zijn dat het protocol in de publieke frequentieband opereert van 868 Megahertz in Nederland. Dat maakt het ook mogelijk om een eigen LoRaWAN-netwerk met eigen gateways op te zetten. TMX en Croonwolter&dros leveren de sensor-nodes die zowel op het publieke KPN-netwerk als op het op te bouwen private netwerk zullen worden aangesloten. Door het publieke KPN-netwerk en het eigen private netwerk beide uit te proberen, zowel in een gecontroleerde lab-omgeving als in het veld bij een waterschap, proberen de partners in het consortium te onderzoeken en vast te stellen of LoRaWAN voldoet aan de hooggespannen verwachtingen.' Hut: 'LoRaWAN is ontwikkeld in een tijd dat hacks aan de orde van de dag zijn. Er is, in elk geval in de specificatie, al veel rekening gehouden met ingebouwde security-technologie in plaats van dat het later is toegevoegd en optioneel is. Beveiliging van draadloze protocollen en netwerken, zoals bij 3G, 4G (LTE) en wifi, is vaak in het nieuws en wellicht daardoor is bij LoRaWAN gekozen voor gebruik van meerdere onafhankelijke encryptielagen, zowel op netwerk- als op applicatie-niveau.'

Volgens Hut wordt ook nog een extra beveiliging overwogen voor de opslag van cryptografische sleutels voor de proefopstelling, met het oog op de wat kritischere sensoren. 'Er zijn producten beschik-

baar, zoals de Sodaq Explorer, waarbij cryptografische sleutels kunnen worden opgeslagen in speciale 'secure hardware', een zogenaamd secure element zoals bij smartcards en simkaarten. Op die manier krijg je meer zekerheid over de veilige opslag van sleutelmateriaal in sensoren en backoffice-systemen.'

Implementatie

Onder andere door de dubbele 128 AES encrypted key en op basis van de specificaties ziet LoRaWAN er veelbelovend uit, zowel qua functionaliteit als qua veiligheid. Toch waarschuwt Hut voor een zorgvuldige inrichting van het draadloze netwerk. 'Je kunt nog zo'n goede netwerkspecificatie en -beveiliging hebben, de betrouwbaarheid en veiligheid staat of valt met de kwaliteit van de implementatie over de hele keten heen, waarbij de beveiliging van de sensor en de applicatie net zo belangrijk is. IoT-security is een samenspel van de juiste apparatuur en een doordachte netwerktopologie, in combinatie met een geschikte use-case waarbij de risico's beheersbaar zijn.'

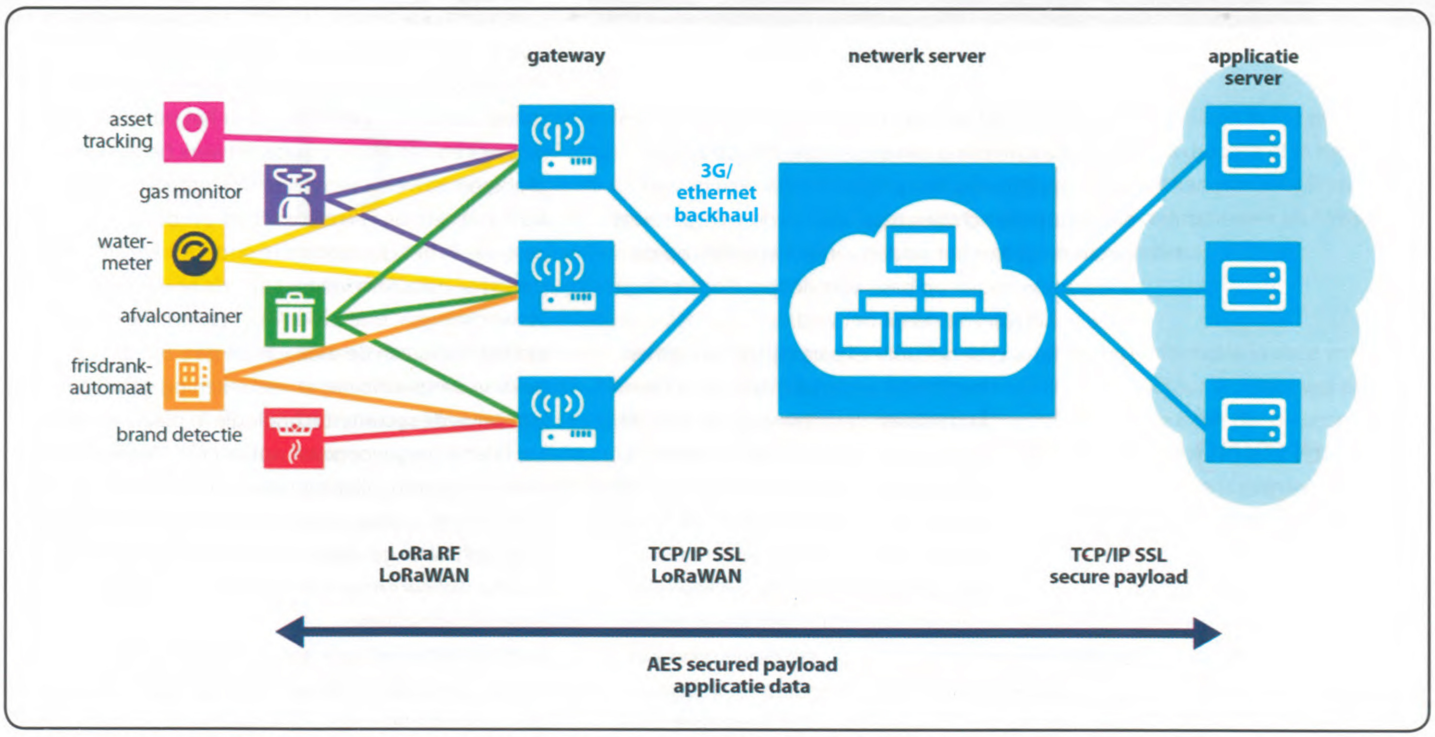
'De installateur die een dergelijk netwerk aanlegt of gebruikt, moet naar verwachting een lange adem hebben, omdat de ervaring leert dat in nieuwe technologie zwakheden kunnen zitten. Zulke veiligheidsproblemen kunnen meestal worden opgelost met een firmware-update. Het komt ook voor dat er nieuwe versies van de specificaties noodzakelijk zijn om structurele veiligheidsproblemen op te lossen, waarna leveranciers hun hard- en/of software moeten bijwerken om compatible te zijn met de laatste versie.

'Veel installateurs van industriële technologie zijn geen fan van patches'

Met meer detailinformatie over lokale omstandigheden kan het complexe systeem van sluizen, stuwen en waterkeringen beter worden ingezet.

Veel installateurs van industriële technologie zijn echter geen fan van patches, omdat de beschikbaarheid van een systeem of dienst het allerbelangrijkst is. Voor de continuïteit is het installeren van patches soms een groter risico dan het niet installeren van patches.'

Een andere manier om de betrouwbaarheid en de veiligheid te vergroten is om meerdere sensoren te gebruiken van verschillende leveranciers. Hut: 'Stel dat er twee sensorketens worden gebruikt voor een toepassing, waarbij er in de ene keten een meetafwijking of een securityprobleem is opgetreden en in de andere niet. Een vergelijk van de metingen van beide sensoren die naast elkaar in één gebied liggen, zou dan niet al te grote afwijkingen mogen vertonen. Dit soort scenario's willen we graag in de praktijk uitproberen. Daarnaast willen we zowel functionele testen als security-testen uitvoeren, om te onderzoeken of LoRaWAN geschikt is voor een nieuwe generatie van innovatieve watertoepassingen.' <



IoT kan waterschappen ondersteunen bij het uitvoeren van hun taken voor droge voeten en schoon water.