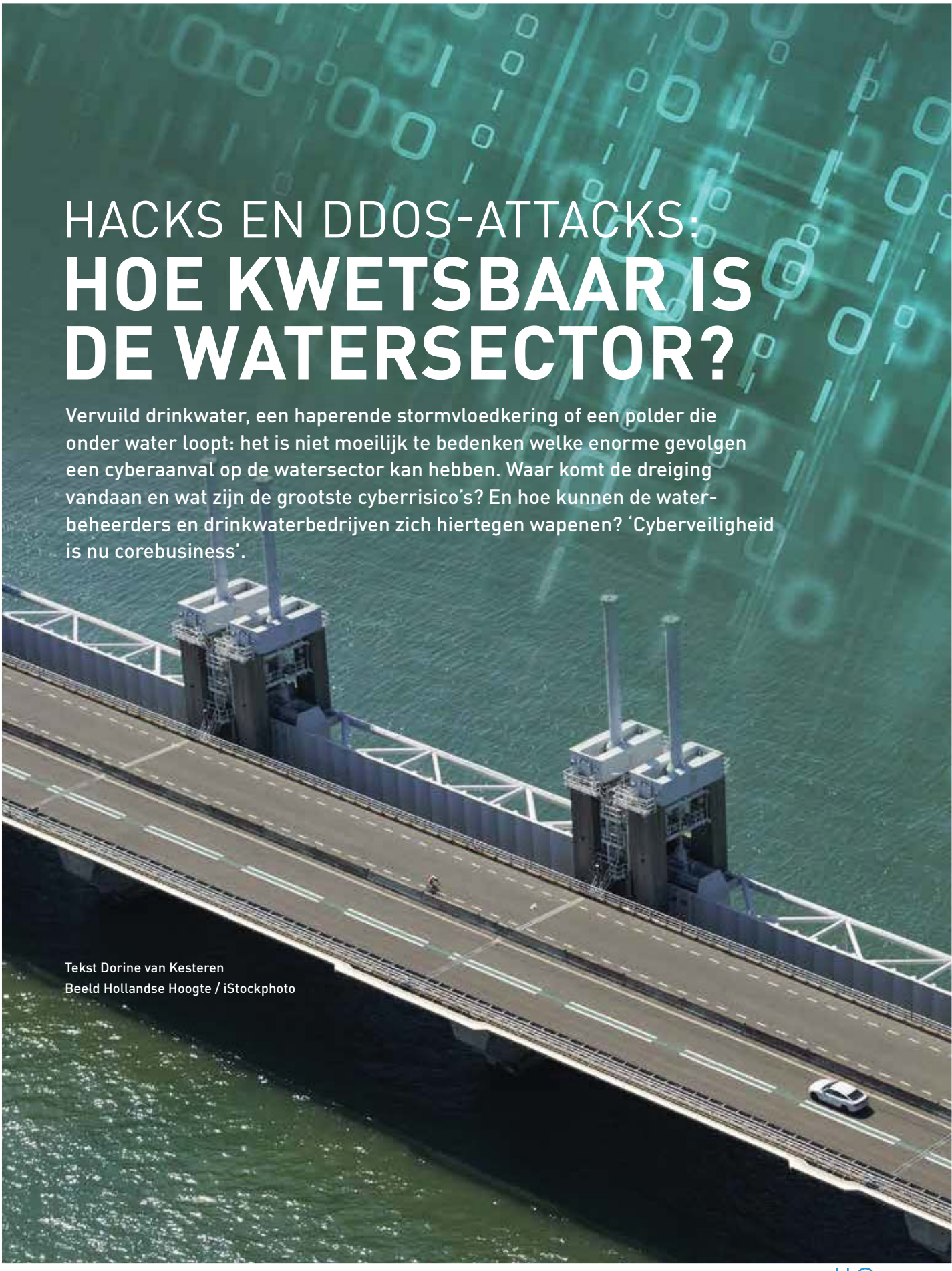

# HACKS EN DDOS-ATTACKS: HOE KWETSBAAR IS DE WATERSECTOR?

**Vervuild drinkwater, een haperende stormvloedkering of een polder die onder water loopt: het is niet moeilijk te bedenken welke enorme gevolgen een cyberaanval op de watersector kan hebben. Waar komt de dreiging vandaan en wat zijn de grootste cyberrisico's? En hoe kunnen de waterbeheerders en drinkwaterbedrijven zich hiertegen wapenen? 'Cyberveiligheid is nu corebusiness'.**

Tekst Dorine van Kesteren
Beeld Hollandse Hoogte / iStockphoto

‘Er wordt steeds meer gedigitaliseerd en hoe meer digitalisering, hoe meer kwetsbaarheden’

De NOS meldde het een tijdje geleden vrij populair en kort door de bocht: verschillende sluizen en gemalen van de waterschappen zijn onvoldoende beveiligd tegen hacks. De bedieningssystemen van sluizen en pompen gaan vaak tientallen jaren mee, maar krijgen niet op alle locaties tijdig een beveiligingsupdate, zo meldde een anonieme bron. Het was niet de eerste keer dat dit soort berichten de media haalden. In 2012 onthulde het televisieprogramma *Een Vandaag* dat het gemaal in Veere ‘kinderlijk eenvoudig’ te hacken was.

In de Verenigde Staten hebben kwaadwillenden al daadwerkelijk hun slag geslagen in de watersector. Zo slaagde in 2000 een medewerker van een drinkwaterbedrijf in de staat Michigan erin om rioolwater door te sluizen naar de kraan. En in 2005 wist een medewerker van de Taum Sauk Water Storage Dam in Missouri de kering een stukje open te zetten. De gevolgen laten zich raden.

Niet voor niets rekent de Nederlandse rijksoverheid zowel de waterbeheerders als de drinkwaterbedrijven tot de vitale infrastructuur, die tegen elke prijs moet worden beschermd. Tot nu toe zijn hier – gelukkig – nog geen serieuze incidenten geweest, maar dat betekent niet dat de Nederlandse watersector achterover kan leunen, aldus Pieter van Gelder, hoogleraar Veiligheidskunde aan de TU Delft. “De sector bedient zich van complexe systemen. Er wordt steeds meer gedigitaliseerd en hoe meer digitalisering, hoe meer kwetsbaarheden.”

## BINNEN EN BUITEN

De dreiging komt zowel van binnen als van buiten. Van Gelder: “Het is denkbaar dat ontevreden medewerkers van een waterschap of drinkwaterbedrijf met behulp van sensordata inzicht krijgen in het operationele proces en vervolgens schade aanrichten. Ze openen of sluiten bijvoorbeeld een waterkering of manipuleren de data van een zuiveringsinstallatie zo dat het lijkt of het drinkwater bij een zuiverheidsgraad van slechts 75 procent wél helemaal schoon is.”

Cybercriminelen en vijandige staten vormen het externe gevaar. “Deze staten sorteren voor op een digitale oorlog en proberen de kritieke infrastructuur plat te leggen. Criminelen op hun beurt gebruiken bijvoorbeeld ransomware om de computers van drinkwaterbedrijven en waterbeheerders te gijzelen, in ruil voor losgeld in bitcoins. En met een DDoS-aanval kunnen zij een server of groep van servers lamleggen, door er heel veel internetverkeer tegelijk op af te sturen.”

De watersector neemt allereerst technische maatregelen om zich hier tegen te wapenen. Antivirussoftware en intrusion detection-systemen moet digitale inbrekers tegenhouden. “Met een goede veiligheidsschil rond het gehele waterschap voorkomen we dat er mensen van buiten naar binnen komen. Maar ook daarna is er nog een beveiligingslaag van interne firewalls. Binnenkort hebben alle waterschappen een audit gehad op dit terrein, in het kader van ISO 27001, de internationale norm voor informatiebeveiliging”, vertelt Piet Sennema, voorzitter van het uitvoerend overleg cybersecurity van de waterschappen. >

**DDOS-AANVAL OP RIJKSWATERSTAAT**

Eind januari kregen banken, Belastingdienst en DigiD enkele dagen forse DDoS-aanvallen te verduren. Ook Rijkswaterstaat lag onder vuur. "We detecteerden een DDoS-aanval en hebben die succesvol afgewend", zegt woordvoerder Cherryl Naarden. "Er is bij ons geen enkele verstoring van de dienstverlening geweest."

De aanval is gedetecteerd door het Security Operations Center (SOC), vertelt Naarden. "Dit is een samenwerkingsverband van Rijkswaterstaat en waterschappen op het terrein van operationeel waterbeheer en cyberveiligheid. Het SOC heeft de DDoS-aanval gezien en vervolgens afgewend." Rijkswaterstaat heeft samen met de waterschappen ook het Computer Emergency Response Team Watermanagement, kortweg CERT WM. Naarden: "Dit team hoefde niet in actie te komen, omdat de aanval met de reguliere security-organisatie kon worden afgehandeld."

Vanuit veiligheidsoogpunt wil Naarden geen informatie geven over hoe Rijkswaterstaat zich tegen DDoS-aanvallen beveiligt. "Cybersecurity heeft onze continue aandacht. Het onderwerp heeft voor ons en onze ketenpartners een hoge prioriteit. We hebben veel kennis in huis en werken nauw samen met onder meer het Nationaal Cyber Security Centrum. Cyberveiligheid is corebusiness."

Het euvel bij de 'gemakkelijk te hacken' sluizen en gemalen die onlangs in het nieuws waren, zit hem in de opzet en beveiliging van de automatiseringssystemen, ofwel de operationele technologie (OT). Onderdeel hiervan zijn de programmable logic controllers (plc's): de soft- en hardware voor het besturingssysteem van deze sluizen en gemalen. Deze plc's kunnen tot wel 25 of 30 jaar meegaan, maar worden, afhankelijk van het type hardware, slechts zeven jaar ondersteund met beveiligingsupdates.
"Dit is vergelijkbaar met Microsoft dat na drie tot vijf jaar geen updates meer geeft voor bijvoorbeeld Windows XP", zegt Johan de Wit, solution manager security bij Siemens, dat plc's levert aan onder andere Rijkswaterstaat. "In de informatietechnologie en kantoorautomatisering is iedereen aan deze levensduur en ondersteuningstermijn gewend, maar in de OT verwacht men ineens een levensduur van enkele decennia, en dat vaak zonder updates en aanpassingen."
De Wit vervolgt: "Vaak kunnen we nog beveiligingsmaatregelen treffen om het OT-systeem als geheel – waaronder de beveiliging van de plc's – up-to-date te houden, maar soms moet toch ook nieuwe hardware worden aangeschaft. Wij zijn momenteel bezig voor Rijkswaterstaat om de besturingssystemen in waterbouwkundige kunstwerken te upgraden door verouderde hardware te vervangen door nieuwe. Daarmee brengen we tegelijk de beveiliging op orde." Sennema: "Als waterschappen stellen wij tegenwoordig nadrukkelijk de eis in aanbestedingen dat de leverancier van de plc's ook zorgt voor regelmatige en tijdige updates."

'Als bv Nederland hebben wij de plicht om te zorgen voor cyberveiligheid. En als iets er niet is, moet je meehelpen bouwen."

VERSLEUTELEN

Op het vlak van de technische maatregelen staan de ontwikkelingen niet stil. Zo werkt Hoogheemraadschap Delfland aan een nieuwe methode om de gegevens van de sensoren van gemalen en waterzuiveringen veilig te transporteren. Dit doen ze samen met een startup van de TU Delft. "Deze pakketjes met data worden soms getransporteerd over een beveiligd kanaal, maar soms ook over een openbaar kanaal. Daarom worden de gegevens versleuteld. De wiskundige formule hiervoor is hetzelfde, maar het vernieuwende is dat alleen wijzelf – en niet een derde, zoals de partij die de versleuteling heeft bedacht – beschikken over de sleutel. Het grote voordeel daarvan is dat wij het onmiddellijk in de gaten hebben als iemand de sleutel steelt en wij ook meteen een nieuwe sleutel kunnen creëren. De gestolen sleutel is dan waardeloos geworden. Als je hiervoor een derde nodig hebt, duurt het veel langer", legt chief information officer René Kint uit.
Het einddoel van het hoogheemraadschap is om ook de besturingssoftware van de gemalen op deze manier te beveiligen. "Die software is een stuk ingewikkelder dan een enkele sensor. Het eerste half jaar van 2018 gebruiken we om samen met de startup onderzoek te doen. De tweede helft van het jaar willen we één gemaal op deze manier beveiligen, en vervolgens laten we er een professionele hacker of studenten van de TU op los om te kijken hoe goed dit is gelukt."
De andere waterschappen zijn zeker geïnteresseerd in deze nieuwe methode, aldus Kint. "Maar ze vinden het eng om als overheidsorgaan zo'n instrument echt zelf te gaan bouwen en ontwikkelen. Dit brengt immers risico's met zich mee. Ze wachten dus liever af tot een commerciële partij het oppakt en ze het gewoon kunnen kopen. Ik denk daar anders over: als bv Nederland hebben wij de plicht om te zorgen voor de cyberveiligheid. En als iets er niet is, moet je meehelpen bouwen."


Piet Sennema


Pieter van Gelder


René Kint

**DRINKWATERBEDRIJVEN ZWIJGEN**

**Als onderdeel van de vitale infrastructuur is de drinkwatervoorziening verplicht om een leveringsplan op te stellen, met daarin een analyse van cyberdreigingen en –risico's. Hierbij werkt de sector nauw samen met het Nationaal Cyber Security Centrum. De drinkwatersector heeft ook zijn eigen Information Sharing and Analysis Centre (ISAC). Brancheorganisatie Vewin en een aantal drinkwaterbedrijven lieten weten 'hard te werken aan de cyberveiligheid' maar 'vanuit veiligheidsoverwegingen' in dit artikel niet nader te willen ingaan op de risico's en maatregelen.**

## ORGANISATORISCHE MAATREGELEN

Naast technische zijn er organistorische maatregelen om de cyberveiligheid te verbeteren. Deze komen deels van de overheid, deels uit de sector zelf. Zoals alle overheidsinstanties en private bedrijven heeft de watersector te maken met de ISO-norm 27001 voor informatiebeveiliging. Hoogleraar Van Gelder: "Deze norm geeft adviezen voor het opzetten, invoeren en beheren van een informatie security managementsysteem. Het is een richtlijn, geen wet of harde verplichting. Anders is dat voor de Wet gegevensverwerking en meldplicht cybersecurity, die vorig najaar in werking is getreden. Deze wet verplicht overheidsinstellingen en bedrijven van vitaal belang onder meer om cyberincidenten te melden bij het Nationaal Cyber Security Centrum (NCSC)."

De watersector werkt nauw samen met het NCSC, dat als belangrijke taak heeft om ervoor te zorgen dat organisaties informatie niet voor zichzelf houden, maar met elkaar delen. Daarnaast hebben zowel de waterbeheerders als de drinkwaterbedrijven een eigen Information Sharing and Analysis Centre (ISAC). Van Gelder: "De hierbij aangesloten partijen delen informatie over cyberdreiging, aanvallen en maatregelen in de branche. Het NCSC is het overkoepelende orgaan, zodat de relevante informatie uit de watersector ook de andere vitale sectoren in Nederland bereikt."

De derde categorie maatregelen is gericht op de mens. In de woorden van Sennema: de mens is altijd het grootste risico. "Alle waterschappen voeren bewustwordingstrajecten voor de medewerkers. Niet zomaar op links klikken in e-mails, niet slordig omgaan met passwords, bewust zijn van de gevaren. Een adequate cyberhygiëne in de organisatie, kortom."

## GEBREK AAN SPECIALISTEN

Als de watersector de maatregelen op deze drie niveaus – techniek, organisatie én mens – op orde heeft, dan zit het ook goed met de cyberveiligheid, aldus Van Gelder. Maar hij noemt wel een knelpunt: het gebrek aan cyberspecialisten in Nederland. "In Duitsland is onlangs een centrum voor cybersecurity opgericht met een budget van vijftig miljoen euro per jaar. In ons land daarentegen is nog geen één miljoen per jaar beschikbaar voor onderwijs en onderzoek op dit terrein. De Nederlandse overheid moet veel meer investeren. In wetenschappelijk onderzoek én in hbo-instellingen die operationele mensen opleiden die weten welke technische maatregelen ze moeten nemen om complexe systemen te beveiligen." Daarnaast is een goede opleiding voor de bestaande medewerkers in de watersector van groot belang, benadrukt hij. "De technici bij de waterschappen en drinkwaterbedrijven moeten natuurlijk ook weten wanneer een nieuwe patch moet worden geïnstalleerd."

Piet Sennema, in het dagelijks leven secretaris-directeur van waterschap Aa en Maas, ziet echter op dit moment geen problemen op dit vlak. "De arbeidsmarkt wordt krapper en goede technici en ict'ers bieden zich niet in grote getalen aan, maar we zijn op dit moment redelijk uitgerust. Schaarse kennis delen we met de twee andere waterschappen in Brabant. Bovendien kunnen we altijd een beroep doen op het Computer Emergency Response Team voor de rijksoverheid, dat beschikt over gespecialiseerde deskundigen."

## BLOCKCHAIN

Als er op termijn toch meer geld komt voor onderzoek, is de verdere uitwerking van de blockchaintechnologie volgens Van Gelder het eerste waarin knappe koppen hun tanden moeten zetten. "Blockchain kan worden ingezet om de cybersecurity te verbeteren. Hiermee is het bijvoorbeeld mogelijk om DdoS-aanvallen af te weren. In zo'n peer-to-peer-netwerk moet meer dan vijftig procent van de peers worden aangevallen om het systeem plat te leggen – en dat is bijna niet mogelijk. Een andere kansrijke ontwikkeling is de decentrale opslag van data. Als iedere decentrale opslag is beveiligd, moet een hacker steeds weer opnieuw zijn best doen om binnen te komen. De gevolgen van een cyberaanval zijn dan een stuk kleiner dan wanneer een enorme hoeveelheid data centraal is opgeslagen." |