PODIUM

COÖRDINATIE: MIRJAM JOCHEMSEN | BEELD ISTOCKPHOTO

In het afgelopen najaar bracht *Follow the Money* berichten naar buiten over de gebrekkige beveiliging van computersystemen bij Waternet en ontoereikende organisatiestructuur. Waren de problemen te voorzien? En hoe staat de watersector ervoor wat cyberveiligheid betreft? Wat is er nodig om de situatie te verbeteren? Pieter van Gelder, hoogleraar Veilgheidskunde aan de TU Delft, roept als relatieve buitenstaander op tot meer actie.

CYBERVEILIGHEID: AD HOC TOETSEN KAN ECHT NIET MEER

Pieter van Gelder, hoogleraar Veilgheidskunde aan de TU Delft

ZIJN DE DIGITALE BEVEILIGINGSPROBLEMEN BIJ WATERNET UITZONDERLIJK?

"De details van de situatie bij Waternet ken ik niet. Maar zeker is dat dit soort dingen overal voorkomt. Bij ziekenhuizen, scholen universiteiten, energiecentrales. Zelfs in de bankenwereld, die we toch wel als een koploper in digitale beveiliging kunnen beschouwen. Veel mensen herinneren zich ook vast nog wel de grote hack bij de universiteit van Maastricht, nu ruim een jaar geleden. De watersector is in dit opzicht zeker niet uniek. Wat niet afdoet aan de urgentie om dit probleem aan te pakken, zeker in deze sector van vitaal belang, met de drinkwatervoorziening en het water(zuiverings)beheer."

ZIJN BEVEILIGING VAN DATA EN VAN PROCESBESTURING TWEE VERSCHILLENDE TAKKEN VAN SPORT?

"Nee, in essentie gaat het er bij beide om dat we ongewenste gebeurtenissen willen voorkomen en maatregelen

‘DIGITALE BEVEILIGING KOST MOEITE, TIJD EN GELD, EN VERMINDERT HET GEBRUIKSGEMAK’

willen treffen om ze te voorkomen. Wat dat betreft is er dus ook geen fundamenteel verschil met het managen van veiligheid in bijvoorbeeld het verkeer of in arbeidsomstandigheden. Wel krijgt tegenwoordig de beveiliging van kantoorautomatisering (IT) meer aandacht dan die van operationele processen zoals de bediening van sluizen, gemalen, rioolwaterzuiveringen en drinkwatervoorziening (OT). In die laatste zijn we achtergebleven. Digitale beveiliging kost moeite, tijd en geld, en vermindert het gebruiksgemak. Eerlijk is eerlijk: ook als burger zijn we in de verleiding om een goedkope webcam aan te schaffen, die misschien ‘lek’ is en buitenstaanders makkelijk mee laat kijken. Bovendien denkt een organisatie vaak ‘bij ons is voor hackers niks te halen’. Maar dan vergeet je dat ze wel grote schade kunnen veroorzaken. Met het gijzelen van gegevens of door te dreigen met het verstoren van bedrijfsprocessen hebben hackers bovendien een effectief chantagemiddel in handen om ‘losgeld’ te krijgen.”

WAAROM LIJKT ER NIET VEEL VERBETERING IN ONZE CYBERVEILIGHEID TE ZITTEN?

“Daar zijn verschillende oorzaken voor aan te wijzen. In de eerste plaats is de watersector groot, divers en complex. Dat betekent dat de sector een groot ‘aanvalsoppervlak’ heeft dat beschermd moet worden. Bovendien kun je je systemen alleen goed verdedigen door overal en altijd up-to-date te blijven. Je bent nooit klaar. Nieuwe bedreigingen moet je onmiddellijk signaleren en je moet direct maatregelen nemen. Daarvoor heb je deskundigen nodig, multidisciplinaire teams van wateringenieurs en cyberspecialisten. Dat brengt ons op de tweede oorzaak: de vraag naar cyberspecialisten is groot maar het aanbod is zeer beperkt, onder meer doordat er veel te weinig geïnvesteerd wordt in onderwijs en onderzoek. Slechts sporadisch komt er bij onze vakgroep een verzoek binnen van de Stowa of de Unie van Waterschappen. Er is behoefte aan veel meer geld, samenwerking, het gezamenlijk ontwikkelen en uitwisselen van kennis en tools. Niet erg sexy misschien, maar wel heel belangrijk.”

DIT IS ALLEMAAL GEEN ECHT NIEUWS, TOCH?

“Het komt allemaal langzaam wel van de grond. Er komen de laatste jaren meer juridische regelingen, toezichtstructuren en kennisnetwerken. Zo is er is de Wet beveiliging netwerk- en informatiesystemen (2018), in 2019 gevolgd door een Cyberstrategie van het ministerie van Infrastructuur en Waterstaat. Voor ‘aanbieders van essentiële diensten’ is de Inspectie Leefomgeving en Transport toezichthouder. Verder groeit er langzaam maar zeker meer samenwerking tussen het Nationaal Cyber Security Centrum (NCSC), RWS en de waterschappen. Ook de werken de waterschappen samen op dit terrein in Het Waterschapshuis. Maar het mag, nee moet, allemaal sneller en meer.”

WAT ZOU UW ADVIES ZIJN VOOR DE WATERSECTOR?

“Dat is niet verrassend: investeer in structurele samenwerking en kennisuitwisseling. Op nationaal niveau, en misschien zelfs op internationaal, Europees niveau. De fysieke processen zijn immers overal hetzelfde. De sluisdeuren moeten overal en altijd openen en sluiten tegen de zwaartekracht en de stroming in. Ik voorzie – en bepleit – een trend naar voortgaande uniformering en standaardisering. Daarnaast moet de vrijblijvendheid ervan af. Een collega van me keek naar de autowereld: daar heb je de APK-keuring, elk jaar, volgens vaste normen. Zonder keuring mag je de weg niet op. Zoiets missen we in de cyberwereld. Toetsingen gebeuren ad hoc en steekproefsgewijs. Dat kan echt niet meer.”•

‘HET MOET ALLEMAAL SNELLER EN MEER’

REAGEREN? IDEEËN?

- Ga naar **h2owaternetwerk.nl/h2o-podium/opinie**.
- **Meer informatie over waterschappen en cyberveiligheid:** https://www.hetwaterschapshuis.nl/informatieveiligheid-en-privacy https://www.h2owaternetwerk.nl/h2opremium/cyberveiligheid-is-nu-corebusiness (februari 2018)
- **Over digitale lekken Waternet:** https://www.h2owaternetwerk.nl/h2o-actueel/ilt-gaat-digitale-beveiliging-waternet-onderzoeken