Vlaams Parlement

SCHRIFTELIJKE VRAAG

nr. 613
van **FREYA PERDAENS**
datum: 12 februari 2021

---

aan **ZUHAL DEMIR**
VLAAMS MINISTER VAN JUSTITIE EN HANDHAVING, OMGEVING, ENERGIE EN TOERISME

Waterzuiverings- en drinkwatersysteem - Digitale veiligheid

Hackers hebben over het internet, met de afstandstool TeamViewer, geprobeerd de watervoorraad van een kleine stad in Florida te vergiftigen. Met de aanval op het waterzuiveringssysteem van het stadje Oldsmar probeerden de hackers in kwestie om de hoeveelheid natriumhydroxide (bijtende soda) in het water te verhogen. De waterzuiveringsorganisatie zegt dat alleen erkende gebruikers vanop afstand zouden mogen inloggen. Een van die erkende gebruikers, die vanop afstand aan het werk was, verloor op vrijdag 5 februari de controle over zijn computermuis en zag op zijn scherm hoe een derde partij door de beheersoftware begon te manoeuvreren.

1. Op welke manier voorziet men bij onze waterzuiverings- en drinkwatersystemen in bescherming tegen mogelijke cyberaanvallen? Wordt voldoende aandacht besteed aan digitale veiligheid van nutsvoorzieningen en op welke manier wordt daarin ondersteuning geboden?
2. Staan er in de toekomst nog extra investeringen/programma's gepland rond cyberveiligheid?

ZUHAL DEMIR
VLAAMS MINISTER VAN JUSTITIE EN HANDHAVING, OMGEVING, ENERGIE EN TOERISME

ANTWOORD
op vraag nr. 613 van 12 februari 2021
van **FREYA PERDAENS**

---

1. De richtlijn 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie, de "NIS-richtlijn", werd omgezet voor België in de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, de "NIS-wet".

   De richtlijn en de wet die haar omzet, beogen een hoge graad van beveiliging van de netwerk- en informatiesystemen waarvan aanbieders van essentiële diensten van kritiek maatschappelijk of economisch belang (energie, vervoer, bankwezen, infrastructuur voor de financiële markt, gezondheidszorg, levering en distributie van drinkwater en digitale infrastructuur, zoals opgenomen in bijlage 1 bij de "NIS-wet") gebruik maken in het leveren van hun diensten.

   Naar aanleiding van die omzetting van de richtlijn 2016/1148 in de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, de "NIS-wet", werd in 2020 een Nationaal Comité voor de beveiliging van de levering en distributie van drinkwater opgericht. Het Comité zal voor de sector drinkwater de correcte uitvoering van de vereisten opgenomen in de NIS-wet moeten bewaken als sectorale autoriteit.

   Om te voldoen aan de bepalingen van de NIS-wet moeten de aanbieders van essentiële diensten "passende en evenredige technische en organisatorische maatregelen nemen om de risico's voor de beveiliging van netwerk- en informatiesystemen waarvan zijn essentiële diensten afhankelijk zijn, te beheersen.". Daarvoor moet door de aanbieders een beveiligingsbeleid voor hun netwerk- en informatiesystemen (I.B.B.) worden uitgewerkt met daarin concrete beveiligingsmaatregelen en -doelstellingen. Voor de drinkwatersector zijn de aanbieders onlangs aangewezen waardoor zij binnen 12 maanden hun I.B.B. moeten uitwerken en binnen 24 maanden de voorgestelde maatregelen moet implementeren.

   De voorgestelde beveiligingsmaatregelen en -doelstellingen moeten jaarlijks een interne audit ondergaan en minstens om de drie jaar een externe audit. Het auditschema moet worden opgestart binnen drie maanden na het uitwerken van het I.B.B.

   De NIS wet verplicht de aanbieders van essentiële diensten ook om melding te maken van incidenten aan zowel de sectorale autoriteit als aan het nationaal computer security incident response team (voor België is dit het Centrum voor Cybersecurity België of CCB). Het CSIRT biedt technische ondersteuning bij incidenten of potentiële incidenten.

   Voor de drinkwatersector is dit specifiek beleidskader dus in volle uitvoering. Voor het Vlaams Gewest zetelen vertegenwoordigers van VMM en van het Coördinatie- en Crisiscentrum van de Vlaamse overheid in het Nationaal Comité dat optreedt als sectorale autoriteit.

Ook los van het NIS-kader dat momenteel wordt geïmplementeerd, neemt de drinkwatersector digitale veiligheid van de nutsvoorziening en de beveiliging van de drinkwatersystemen zeer ernstig. Via vaste overlegmomenten bij AquaFlanders, Centrum voor Cybersecurity België, webinars, externe expertise... tracht de sector up to date te blijven van de laatste ontwikkelingen rond (cyber)security en mogelijke cyberaanvallen. Om cybersecurity op een gestructureerde manier aan te pakken zetten de waterbedrijven een ISMS (Information Security Management System) op volgens de internationale informatiebeveiligingsstandaard ISO27001. Binnen dit kader wordt een uitgebreide risicoanalyse uitgevoerd en worden de risico's op vlak van cybersecurity in de omgeving van de drinkwaterdistributie in kaart gebracht. Op basis van deze risicoanalyse zijn een aantal projecten gedefinieerd die het cybersecurityniveau moeten verhogen:

- Sensibilisering van medewerkers rond cybersecurity;
- Patchmanagement;
- Toegangsbeheer (beveiligen met controles en authenticaties);
- Netwerksegmentatie (d.m.v. firewalls, gescheiden netwerken);
- Cybersecurity monitoring (automatische updates, audits).

Voor wat betreft de publieke afvalwatersector geeft Aquafin aan dat zowel implementatie als awareness rond cybersecurity al duidelijke focuspunten zijn voor de organisatie. Alle gangbare/noodzakelijke securitymaatregelen en controlemechanismen zijn geïmplementeerd en worden nauwgezet opgevolgd. Hierdoor is Aquafin maximaal beschermd tegen een cybersecurity aanval. Een tweejaarlijkse exhaustieve security audit door externe gespecialiseerde firma's bevestigt dit. Evengoed naar remediering zijn alle processen en systemen zo optimaal mogelijk ingericht. Zo worden bijvoorbeeld elk jaar *disaster recovery testen* georganiseerd waarbij verschillende cyberincidenten gesimuleerd worden ter controle van de bestaande processen, zodat efficiënt geageerd wordt als er een echt incident plaatsvindt. Een intensieve awareness campagne naar eindgebruikers vindt al voor het tweede jaar op rij plaats.

Cybersecurity is met andere woorden al jaren een prioriteit binnen Aquafin.

In de toekomst plant Aquafin de huidige approach van cyberstrategie en snel schakelen blijvend toe te passen. Dit gaat van cybermanagement, componentbeveiliging tot awareness.

Cybersecurity en het digitale landschap zijn beiden constant in beweging, het is dus goed dat Aquafin hier ook in de toekomst flexibel en robuust op zal blijven inspelen.

2. Voor wat de acties en investeringen binnen de watersector betreft, verwijs ik naar het antwoord op deelvraag 1.

   U vraag gaat echter ruimer. U kunt zich voor de integrale problematiek richten tot de minister-president. Hij is bevoegd voor deze materie. Daarnaast is er nog het federale Centrum voor Cybersecurity België dat heel wat ondersteuning biedt (https://ccb.belgium.be/nl) en dat onder de federale bevoegdheid valt van de eerste minister.