Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2020–2021 **Aanhangsel van de Handelingen**

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

2759

Vragen van de leden **Van Ginneken** en **Tjeerd de Groot** (beiden D66) aan de Minister van Infrastructuur en Waterstaat over *het ILT Onderzoeksrapport Stichting Waternet* (ingezonden 20 april 2021).

Antwoord van Minister **Van Nieuwenhuizen Wijbenga** (Infrastructuur en Waterstaat) (ontvangen 12 mei 2021).

Vraag 1
Hoe beoordeelt de Minister de conclusie van de Inspectie Leefomgeving en Transport (ILT) dat er een verhoogd – maar moeilijk te kwantificeren – risico aanwezig is op een cyberincident met mogelijke gevolgen voor de kwaliteit en/of de continuïteit van drinkwater?

Antwoord 1
Ik ga uit van het oordeel dat de ILT in het inspectierapport over de cyberweerbaarheid bij Waternet heeft gegeven. Er wordt op het gebied van cybersecurity niet voldaan aan de Wet beveiliging netwerk- en informatiesystemen (Wbni) en de Drinkwaterwet. Waternet staat daarom onder verscherpt toezicht. Het is de eerste keer in Nederland dat een drinkwaterbedrijf door de ILT onder verscherpt toezicht wordt geplaatst omdat de grip op de cyberweerbaarheid niet op orde is. Voor Waternet is het nu de opgave om er met prioriteit voor te zorgen dat de cyberverdediging weer op orde is. Hiertoe heeft Waternet op 29 april jl. een verbeterplan bij de ILT ingediend. Het is nu aan de ILT om in het kader van het verscherpt toezicht de uitvoering van het verbeterplan actief te bewaken.

Vraag 2
Taxeert de Minister dat dit risico aanvaardbaar is, hangende het verscherpte toezicht? En zo nee, wat gaat de Minister doen om de risico's beter in beeld te krijgen en te beheersen?

Antwoord 2
Op dit moment doen zich voor zover mij bekend geen acute risico's voor bij Waternet ten aanzien van de veiligstelling van de openbare drinkwatervoorziening die aanleiding zouden kunnen zijn tot verdere interventies. De ILT heeft tot op heden geen incidentmeldingen ingevolge de Wbni of Drinkwaterwet met betrekking tot de levering en kwaliteit van drinkwater ontvangen die kunnen worden gerelateerd aan het geconstateerde verhoogde risico voor

ah-tk-20202021-2759
ISSN 0921 - 7398
's-Gravenhage 2021

cyberincidenten. In mijn Kamerbrief van 4 november 2020[1] heb ik toegelicht dat de eindverantwoordelijkheid voor cybersecurity bij Waternet (drinkwaterrelevante deel) primair bij het bestuur van de gemeente Amsterdam ligt. De ILT constateert dat het risicomanagement bij Waternet onvoldoende op orde is. Het is daarom in de eerste plaats aan het Stichtingsbestuur van Waternet en de gemeente Amsterdam om invulling te geven aan de bestuurlijke taxatie van de risicoacceptatie van de digitale beveiliging in relatie tot de bedrijfscontinuïteit. Dit overeenkomstig de bepalingen omtrent de risicogebaseerde aanpak in de bijlage bij artikel 3a, eerste lid, van het Besluit beveiliging netwerk- en informatiesystemen (Bbni).[2]
Waternet heeft op basis van de gesignaleerde tekortkomingen in het ILT-rapport een verbeterplan ingediend. De ILT zal beoordelen of de onderbouwing van de risicoacceptatie en daarbij gehanteerde systematiek (en prioriteit van te nemen risicobeheersingsmaatregelen) van Waternet voldoende is. Vervolgens moet Waternet de noodzakelijke risicobeheersingsmaatregelen treffen om de cybersecurity in voldoende mate op orde te krijgen. Daar kan ik nu niet op vooruit lopen.

Vraag 3
Wat is de Minister voornemens te doen om het tempo te verhogen van het implementeren van de door de ILT voorgestelde oplossingen?

Antwoord 3
In het verbeterplan dat door Waternet aan de ILT is aangeboden is voor alle in het ILT-rapport vermelde tekortkomingen aangegeven hoe en wanneer deze zijn opgelost, inclusief de stappen op weg daarnaartoe. Het is aan de ILT om te beoordelen of de planning en uitvoering van de voorgestelde maatregelen voldoet en de voortgang daarvan gedurende het verscherpte toezicht te bewaken.

Vraag 4
Wordt er in het verscherpte toezicht ook nader gekeken naar de organisatiestructuur en de besturing van de organisatie, en de bijdrage die dat volgens het ILT-onderzoek levert aan de tekortkomingen in de cybersecurity? Zo ja, op welke manier? Zo nee, waarom niet?

Antwoord 4
Ja. Het oplossen van de tekortkomingen in de besturing, zoals in het onderzoek aangegeven, maakt onderdeel uit van het verbeterplan van Waternet. Waternet pakt zaken op die op korte termijn verbeterd kunnen worden en evalueert de zaken waarvoor een meer structurele verandering noodzakelijk is die meer voorbereiding vraagt. Gedurende het onderzoek heeft Waternet al stappen gezet die bijdragen aan de verbetering van de cybersecurity, bijvoorbeeld door de aanstelling van een CIO (Chief Information Officer). Bij het verscherpt toezicht onderhoudt de ILT intensief contact met Waternet over de voortgang van de verbeteringen.

Vraag 5
Zijn er naast het verscherpte toezicht nog andere stappen die door u of de ILT worden gezet om te zorgen dat de cybersecurity bij Waternet structureel verbetert? Welke stappen worden er door de organisatie van Waternet zelf precies gezet en dragen die naar uw mening voldoende bij aan het voorkomen van cyberincidenten?

Antwoord 5
De ILT beoordeelt eerst het verbeterplan dat door Waternet is opgesteld. Waternet is nu aan zet om de gesignaleerde tekortkomingen te verbeteren. De ILT monitort de voortgang daarvan.
Voor wat betreft de andere stappen heb ik u in mijn brief van 2 april 2021[3] toegezegd om u ten behoeve van de commissievergadering Water en Wadden van 10 juni as. schriftelijk te informeren over de vervolgacties in het

[1] Kamerstuk 27 625, nr. 522
[2] Staatsblad 2021, 160 | Overheid.nl > Officiële bekendmakingen (officielebekendmakingen.nl)
[3] Kamerstuk 27 625, nr. 529

kader van het versterken van cybersecurity in watersector. De instrumenten die in het kader van dit programma worden ontwikkeld, zijn ook bedoeld voor de structurele verbetering van de cyberweerbaarheid van Waternet. Hierbij gaat het onder andere om de Ministeriële Regeling beveiliging netwerk- en informatiesystemen die voor alle AED's van IenW per 1 juli as. in werking treedt en om de ontwikkeling van een brede cyberstandaard/handreiking voor de procesautomatisering als aanvulling op deze regeling en de Baseline Informatiebeveiliging Overheid (BIO). Daarnaast wordt specifiek voor de drinkwatersector een haalbaarheidsstudie gestart naar de samenwerkingsopties voor een security operations centre (SOC) en is een serious game op het gebied van cybersecurity, crisismanagement en operationele technologie ontwikkeld. Verder wordt een Red Team Blue Team training voor professionals in de watersector aangeboden, waaraan ook Waternet deelneemt.

Vraag 6
Kunt u deze vragen elk afzonderlijk beantwoorden?

Antwoord 6
Ja.