Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2020–2021

27 625 Waterbeleid

Nr. 522

BRIEF VAN DE MINISTER VAN INFRASTRUCTUUR EN WATERSTAAT

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 4 november 2020

Naar aanleiding van mondelinge vragen van het Lid Van Brenk op 22 september jl.[1] over een artikel op Follow the Money (FTM) over de digitale beveiliging van Waternet[2] informeer ik u hierbij over mijn inzet voor het versterken van de cyberweerbaarheid in de watersector en ga ik in op specifieke vragen van het lid Van Brenk.

Het Lid Stoffer heeft tijdens het mondelinge vragenuur gevraagd of de Waternet casus kan worden meegenomen in de door de Minister van Justitie en Veiligheid (JenV) toegezegde brief over de samenhang van de kabinetsinzet rond het thema digitalisering en digitale veiligheid. Met de Minister van JenV heb ik afgesproken dat ik in deze brief inga op mijn verantwoordelijkheden en bevoegdheden, omdat dit de basis vormt voor de beantwoording van de vragen van het Lid Van Brenk. Daarmee ga ik ook in op het verzoek[3] van het Lid Stoffer.

Tot slot ga ik in deze brief in op het aanbod dat ik bij het algemeen overleg water[4] op 22 juni 2020 heb gedaan aan het Lid Geurts om meer tekst en inkleuring te geven bij de begroting voor cybersecurity in het waterbeheer, in het bijzonder het versterkingsprogramma digitale beveiliging waterstaatswerken van Rijkswaterstaat (RWS).

---

[1] Handelingen II 2020/21, nr. 4.
[2] https://www.ftm.nl/artikelen/beveiliging-waternet-lekt.
[3] Verzoek Lid Stoffer: Kan de Minister de Waternet casus en wellicht ook de uitkomsten van het onderzoek dat volgt, meenemen in de brief n.a.v. de Algemene Politieke Beschouwingen, waarin de versnippering en coördinatie rond digitale veiligheid aan de orde zullen komen?
[4] Kamerstuk 27 625, nr. 507.

kst-27625-522
ISSN 0921 - 7371
's-Gravenhage 2020

Verantwoordelijkheden en Bevoegdheden Cybersecurity Watersector

Als Minister van Infrastructuur en Waterstaat ben ik op basis van de Waterwet en de Drinkwaterwet systeemverantwoordelijk voor de continuïteit van het waterbeheer en de openbare drinkwatervoorziening. Deze systeemverantwoordelijkheid geldt ook voor de cybersecurity van waterstaatswerken en de openbare drinkwatervoorziening. De primaire verantwoordelijkheid ligt uiteraard bij de waterbeheerders: waterschappen, gemeenten, de drinkwaterbedrijven en Rijkswaterstaat. Voor RWS ben ik rechtstreeks verantwoordelijk.

In het kader van de Wet beveiliging netwerk- en informatiesystemen (Wbni) zijn de drinkwaterbedrijven aangewezen als Aanbieder van Essentiele Diensten (AED[5]). De zorgplicht uit de Wbni is aanvullend op de eisen die de Drinkwaterwet[6] al stelde voor de komst van de Wbni. Voor drinkwaterbedrijven ben ik op grond van artikel 4 van de Wbni de bevoegde autoriteit. Ik wijs AED's binnen het IenW domein aan, stel nadere eisen aan de zorgplicht, behandel meldingen van cyberincidenten en draag zorg voor de handhaving van de Wbni. Als niet wordt voldaan aan de Wbni kan de ILT een beveiligingsaudit opleggen, een bindende aanwijzing voor te nemen maatregelen geven en een last onder bestuursdwang of bestuurlijke boete opleggen. Overigens heb ik besloten om – in overleg met de Minister van JenV – voor alle AED's binnen het beleidsterrein van IenW een ministeriële regeling in het kader van de Wbni op te stellen met nadere eisen voor cybersecurity, waarin de zorgplicht[7] van AED's verder wordt geoperationaliseerd. Deze regeling zal naar verwachting begin 2021 in werking treden.

Ten opzichte van de decentrale overheden in het waterbeheer heb ik – behoudens bevoegdheden voor calamiteiten in de Waterwet[8] – geen specifieke bevoegdheden op het vlak van cybersecurity. Zij zijn dus zelfregulerend op het gebied van cybersecurity. Juist daarom zet ik hier in op het door middel van samenwerking binnen het Bestuursakkoord Water (BAW) stimuleren van de cyberweerbaarheid. Gemeenten, waterschappen, provincies en het Rijk hebben gezamenlijk besloten de Baseline Informatiebeveiliging Overheid (BIO) vanaf 2019 in te voeren. Het Kabinet heeft in december 2018 bepaald[9] dat de BIO wordt gehanteerd in de informatie-uitwisseling met alle bestuurslagen.

---

[5] Een AED is een vitale aanbieder die afhankelijk is van netwerk- en informatiesystemen en waarvan het proces is vermeld in bijlage II van de NIB-richtlijn. Een AED heeft vanuit de Wet beveiliging netwerk- en informatiesystemen (Wbni) rechten en plichten op het gebied van cybersecurity, zoals een zorgplicht en meldplicht. Voor IenW betreffen dit op dit moment vitale aanbieders binnen de vitale processen drinkwater, luchtvaart en maritiem.

[6] In de Drinkwaterwet zijn eisen gesteld aan leveringsplannen van de drinkwaterbedrijven, die op basis van scenario's maatregelen moeten bevatten die verstoring van de drinkwatervoorziening voorkomen en daartoe behoort ook cybersecurity. De ILT beoordeelt de leveringsplannen, keurt deze goed en ziet toe op de naleving van de wettelijke eisen. De Drinkwaterwet bevat als extra waarborg noodbevoegdheden voor de Minister van IenW om de drinkwatervoorziening veilig te stellen in geval van buitengewone omstandigheden.

[7] De zorgplicht uit artikel 7 en 8 van de Wbni is de wettelijke plicht die AED's hebben om passende en evenredige maatregelen te nemen om de beveiligingsrisico's van netwerk- en informatiesystemen te beheersen, zodat cyberincidenten worden voorkomen en de gevolgen daarvan worden beperkt.

[8] Rijk en provincies beschikken bij calamiteiten over aanwijzings- en in de plaatstredings bevoegdheden. Deze bevoegdheden kunnen worden uitgeoefend, als bij gevaar voor waterstaatswerken het bestuur van een waterschap niet of niet voldoende optreedt.

[9] https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/informatieveiligheid/kaders-voor-informatieveiligheid/baseline-informatiebeveiliging-overheid/.

Digitale beveiliging Waternet en andere drinkwaterbedrijven

Het Lid Van Brenk heeft op 22 september 2020 diverse mondelinge vragen gesteld die betrekking hebben op de cyberrisico's bij Waternet en andere drinkwaterbedrijven. Stichting Waternet is een waterketenbedrijf dat integraal watertaken uitvoert voor het Hoogheemraadschap Amstel, Gooi en Vecht (verder waterschap AGV) en de gemeente Amsterdam. Vanwege de governance structuur van Waternet is er voor cybersecurity juridisch gezien, sprake van een situatie waarin de publiekrechtelijke (eind)verantwoordelijkheid voor de taken die Waternet uitvoert voor waterschap AGV en de gemeente Amsterdam berust bij deze partijen. Elk voor zover het de eigen taken betreft. Zij houden ook toezicht op de (wijze van) uitvoering van die taken (drinkwater, riolering, afvalwaterzuivering, water keren) door Waternet. Voor het antwoord op de vraag van het Lid van Brenk of het management van Waternet capabel is voor hun taak verwijs ik dan ook door naar het waterschap en de gemeente. De eigenaren van het drinkwaterbedrijf Waternet zijn verantwoordelijk voor de naleving van verplichtingen op grond van de drinkwaterregelgeving. ILT is voor dat deel belast met toezicht en handhaving.

Naar aanleiding van de eerdere publicatie over Waternet door FTM heeft de ILT als toezichthouder op het drinkwaterbedrijf in het kader van de Wbni op 27 oktober jl. een gesprek met de directie van Waternet gevoerd. Op 2 november jl. heeft FTM een nieuw artikel gepubliceerd[10] waarin wordt gesteld dat Waternet bewust een kritisch extern onderzoek (een zogeheten pen-test[11]) zou hebben achtergehouden. De ILT was voorafgaand aan de publicatie van FTM niet op de hoogte van de inhoud van de rapportage over deze test. De conclusies van de pen-test en het feit dat Waternet de ILT niet eerder heeft geïnformeerd baren de ILT zorgen. Daarom zal de ILT de resultaten van het door Waternet ingestelde onderzoek – dat 2 tot 3 weken is vertraagd – niet afwachten en zelf een onderzoek instellen. Dit onderzoek zal zich richten op het voor drinkwater relevante deel van Waternet en de naleving van de Wbni, de governance van de organisatie en de leveringszekerheid van drinkwater.

Het Lid Van Brenk vraagt eveneens of er door Waternet onacceptabele beveiligingsrisico's worden genomen, waardoor de drinkwaterlevering in gevaar zou kunnen komen. De ILT geeft aan op dit moment geen reden te zien om aan te nemen dat de leveringszekerheid van het drinkwater bij Waternet als gevolg van cyberrisico's in het geding is. De verwachting van de ILT is dat begin 2021 een completer beeld beschikbaar is. Hierbij zal de ILT ook het externe auditrapport over Waternet betrekken. Ik zal uw Kamer hierover te zijner tijd nader informeren.

Voor wat betreft de vraag van het Lid Van Brenk naar de situatie bij de andere drinkwaterbedrijven, geeft de ILT aan dat er op dit moment geen concrete signalen zijn dat deze niet zouden voldoen aan hun wettelijke verplichtingen. Als dit wel het geval zou zijn, heeft de ILT de bevoegdheid om in te grijpen. Uit de auditrapporten van de diverse drinkwaterbedrijven komen verbeterpunten naar voren. De ILT zal de wijze waarop deze door de drinkwaterbedrijven worden opgepakt meenemen in haar toezicht op grond van de Wbni. Vanwege het belang van het tijdig opvolgen van beveiligingsadviezen, heb ik de ILT verzocht om dit jaar een onderzoek te verrichten naar het inzicht in bekende kwetsbaarheden en de borging en

[10] https://www.ftm.nl/artikelen/waternet-verzwijgt-vernietigende-veiligheidstest.

[11] Penetratietest: Handmatige controle waarbij men zo diep mogelijk wil binnendringen in een systeem om zwakke plekken te vinden en de gevolgen hiervan te kennen. Men gebruikt de zwakke plekken om nog wat dieper in het systeem te komen.

werking van het patchmanagement bij alle AED's van IenW, inclusief Waternet.

Het Lid Van Brenk vroeg of een aangenomen motie van 50PLUS, over het verbeteren van de cybersecurity van de vitale waterwerken, ook voor Waternet geldt. De motie over de inhaalslag in het programma Beveiligd Werken Rijkswaterstaat (Kamerstuk 30 821, nr. 80) heeft alleen betrekking op de vitale waterwerken van Rijkswaterstaat en is – zoals onderbouwd in mijn brief van 15 juni 2020[12] – uitgevoerd. Deze motie is dus niet van toepassing op Waternet.

Intensivering afspraken Bestuursakkoord Water (BAW)

In een aanvullend akkoord op het Bestuursakkoord Water (BAW)[13] hebben in 2018 de waterschappen, drinkwaterbedrijven gemeenten, provincies, Rijkswaterstaat en het kerndepartement afspraken gemaakt om de cyberweerbaarheid in de watersector te verhogen. Daarnaast heb ik in overleg met de waterpartners een Kennis & Innovatie programma ontwikkeld en aanvullende afspraken gemaakt met de drinkwatersector. De projecten worden in het programma « Versterking Cyberweerbaarheid in de watersector» uitgevoerd. Het programmamanagement en de benodigde budgetten worden door het Ministerie van I&W geleverd. Van de waterpartners wordt een actieve inbreng van expertise verwacht in vijftien gezamenlijk vastgestelde projecten.[14] Er zijn al goede stappen gezet, maar gezien de urgentie kan er wat mij betreft een tandje bij. Daarom bespreek ik met de waterpartners welke intensivering in 2021 haalbaar is.

Digitale beveiliging waterwerken Rijkswaterstaat

Bij RWS heeft een inhaalslag plaatsgevonden om de aanbevelingen uit het rapport van de Algemene Rekenkamer (ARK) «Digitale Dijkverzwaring, Cybersecurity en Vitale Waterwerken» op te volgen. In 2020 en 2021 zal extra worden geïnvesteerd in de cyberweerbaarheid van Rijkswaterstaat (RWS) en ga ik meer op risicobeheersing sturen, zowel via het RWS-versterkingsprogramma als een jaarlijks op te stellen informatiebeveiligingsbeeld (dit IB-beeld is bedoeld om meer op de risicobeheersing en preventie te sturen). De uitkomsten van het cyberdreigingsbeeld voor de vitale objecten hebben geleid tot verdiepende risico-assessments en een impuls om het areaal van Rijkswaterstaat beter te beveiligen. Met het RWS-versterkingsprogramma worden eenmalig maatregelen uitgevoerd die gericht zijn op het verminderen van risico's waaronder het uitvoeren van de BWR Restpunten (Programma Beveiligd Werken Rijkswaterstaat). Tevens wordt gezorgd dat al vanaf de ontwerpfase van de drie hoofdnetten de integrale veiligheidskaders afdoende zijn geborgd. Hiermee staat de borging van de continuïteit en betrouwbaarheid van missiekritieke processen als hoofddoelstelling centraal.

Het RWS-versterkingsprogramma bestaat uit veertien hoofdmaatregelen, welke sinds afgelopen juli, na de toekenning van de extra middelen voor cybersecurity, gestart zijn. De uitvoering loopt de komende twee a drie jaar. Een belangrijke hoofdmaatregel uit het RWS-versterkingsprogramma betreft de opschaling van de detectie- en responsecapaciteit door detectie en monitoring uit te breiden naar de niet-vitale objecten. Vanaf 2021 worden er in twee jaar tijd risicogestuurd twintig extra objecten van het

[12] Kamerstuk 27 625, nr. 503.
[13] Bijlage bij Kamerstuk 35 000 J, nr. 7.
[14] Zie bijgevoegde factsheet versterken cyberweerbaarheid in de watersector 2019–2022, Raadpleegbaar via www.tweedekamer.nl.

HoofdWaterSysteem gefaseerd aangesloten op het SOC. Dit bovenop de al eerder aangesloten vitale objecten. Naast deze extra twintig objecten van het HWS-netwerk worden er ook nog veertig andere objecten aangesloten (20 voor het HoofdWegenNet en 20 voor het HoofdVaarwegenNet) als onderdeel van het RWS-versterkingsprogramma.

In 2021 wordt een onderzoek (incl. ketenanalyse) uitgevoerd aan de hand van de Baseline Informatiebeveiliging Overheid (BIO2019) en andere relevante kaders, zoals de Rijkswaterstaat Cybersecurity Implementatierichtlijn Objecten (CSIR). Dit onderzoek moet leiden tot aanbevelingen voor verbeteringen in bestaande processen en zorgt er voor dat RWS naar de toekomst toe, risicogestuurd beslissingen kan nemen. Eerder heb ik aan uw Kamer gemeld dat Rijkswaterstaat eind 2019 met cyberscenario's heeft geoefend en vervolgens het bijbehorende calamiteitenplan heeft vastgesteld. Hiermee is een gerichte scenariovoorbereiding op cybercrisis opgenomen in het crisismodel van RWS. Met het vaststellen van het calamiteitenplan is tevens een aanpak vastgesteld om in 2020 het onderwerp cybercrisis de komende drie jaar verder vorm te geven binnen Rijkswaterstaat.
Het Landelijk Meetnet Water (LMW) is een systeem dat zorgdraagt voor het beschikbaar stellen van waterkwantiteit-, waterkwaliteit-, meteo- en objectgegevens aan afnemers binnen en buiten Rijkswaterstaat. Een goed functionerend LMW is onmisbaar voor de bediening van onze stormvloedkeringen, de berichtgeving aan het scheepvaartverkeer en om slim watermanagement te kunnen voeren. LMW is voor Rijkswaterstaat te kwalificeren als missiekritiek. Het LMW wordt nu op meerdere onderdelen de komende drie a vier jaar vernieuwd. Met het project LMW2 wordt het onderliggende platform zo gebouwd dat de continuïteit en kwaliteit van de levering van meetgegevens geborgd blijft naar de toekomst. Dit o.a. door de toepassing van marktconforme en herbruikbare oplossingen.

De Minister van Infrastructuur en Waterstaat,
C. van Nieuwenhuizen Wijbenga