Ministerie van Infrastructuur en Waterstaat

> Retouradres Postbus 20901 2500 EX Den Haag

De voorzitter van de Tweede Kamer
der Staten-Generaal
Binnenhof 4
2513 AA DEN HAAG

Ministerie van Infrastructuur en Waterstaat

Rijnstraat 8
2515 XP Den Haag
Postbus 20901
2500 EX Den Haag

T 070-456 0000
F 070-456 1111

Kenmerk
IENW/BSK-2021/130024

Datum 2 juni 2021
Betreft Update Versterken Cyberweerbaarheid in de Watersector

Geachte voorzitter,

Naar aanleiding van mijn Kamerbrief[1] van 2 april jl. over het onderzoek van de Inspectie van de Leefomgeving en Transport (ILT) over de digitale beveiliging bij Stichting Waternet informeer ik u hierbij over de laatste stand van zaken met betrekking tot mijn inzet[2] in het kader van het versterken van de cybersecurity in de watersector. In deze update ga ik achtereenvolgens in op:

- de Ministeriele Regeling Beveiliging Netwerk- en Informatiesystemen;
- het toezicht op het naleven van de Wet beveiliging netwerk- en informatiesystemen (Wbni);
- de intensivering van de aanvullende cybersecurity afspraken in het kader van het bestuursakkoord water (BAW+);
- het Rijkswaterstaat Versterkingsprogramma Cybersecurity.

Ministeriele Regeling Beveiliging Netwerk- en Informatiesystemen
Op 26 mei 2021 is de Regeling beveiliging netwerk- en informatiesystemen IenW (verder regeling) in de Staatscourant gepubliceerd[3]. Deze regeling zal 1 juli as. voor alle aanbieders van essentiële diensten (AED's) binnen het IenW-domein in werking treden. Dat betreft AED's binnen de sectoren drinkwater, luchtvaart en maritiem. Het gewijzigde Besluit beveiliging netwerk- en informatiesystemen (Bbni[4]) biedt de juridische grondslag voor deze regeling.

Doel van de regeling is om de zorgplicht verder in handhaafbare- en uitvoerbare bepalingen uit te werken, zodat een logische opbouw van Wbni, Bbni, regeling en richtinggevende sectorspecifieke normen ontstaat. Kern van deze regeling is het toepassen van een risicogestuurd cybersecurity management systeem. Met deze regeling geef ik invulling aan het advies[5] van de ILT voor een bindend en samenhangend totaalkader aan risicobeheersingsmaatregelen.

---

[1] Tweede Kamer, vergaderjaar 2020-2021, 27 625, nr. 529
[2] Tweede Kamer, vergaderjaar 2019-2020, 27 625, nr. 507 en 522
[3] Stcrt-2021-25471: https://www.officielebekendmakingen.nl/stcrt-2021-25471.html
[4] Publicatie gewijzigde Bbni: Staatsblad (2021, 160)
[5] Paragraaf 3.2 van het gewijzigde Bbni over de handhaafbaarheids-, uitvoerbaarheids- en fraudebestendigheidstoets (HUF-toets) van de ILT

Toezicht op de Wbni door de ILT
De bindende voorschriften in het gewijzigde Bbni en de nieuwe regeling zijn randvoorwaardelijk voor effectief toezicht door de ILT op de naleving van de zorgplicht. Voor dit toezicht heeft de ILT recentelijk haar capaciteit versterkt. Over het diepgaand onderzoek dat door de ILT bij Waternet is verricht heb ik u al via mijn Kamerbrief[6] van 2 april jl. en in mijn beantwoording van Kamervragen van de Leden Van Ginneken en De Groot[7] op 12 mei jl. uitgebreid geïnformeerd.

De ILT heeft op mijn verzoek onlangs een thematische verkenning naar de inrichting van het kwetsbaarheden- en patchmanagement van de procesautomatisering bij de sectoren drinkwater, luchtvaart en maritiem afgerond. De uitkomsten van deze verkenning geven volgens de ILT een bemoedigend beeld. De AED's zijn zich bewust van het belang van kwetsbaarheden- en patchmanagement. Naar aanleiding van deze uitkomsten plan ik met de betreffende sectoren, de ILT, de NCTV en het NCSC een evaluatiesessie waarbij de lessen die kunnen worden getrokken uit dit onderzoek besproken worden. Hierbij zullen voorbeelden ter beschikking worden gesteld om het kwetsbaarheden- en patchmanagement bij alle AED's verder te verbeteren. Aangezien deze verkenning een eerste meting is, zullen de resultaten input vormen voor het aangekondigde vervolgonderzoek dat de ILT in 2021 instelt naar de naleving van de zorg- en meldplicht uit de Wbni.

Intensivering cybersecurity afspraken Bestuursakkoord Water (BAW+)
Zoals aangekondigd in mijn brief van 4 november 2020[8], heb ik in de Stuurgroep Water van 20 januari 2021 samen met de bestuurders van de waterpartners afspraken gemaakt om de inzet op drie bestaande BAW+ afspraken te intensiveren. Ik ga hieronder kort in op de trajecten, die onder de regie van het programma versterken cyberweerbaarheid in de watersector[9] worden uitgevoerd.

Het eerste traject betreft het stapsgewijs uitwerken van een brede cyberstandaard/handreiking voor de procesautomatisering als aanvulling op de Baseline Informatiebeveiliging Overheid (BIO). Dit wordt in twee deelprojecten uitgevoerd. Onder regie van Rijkswaterstaat en het Waterschapshuis wordt gewerkt aan het aanpassen van de bestaande Cybersecurity Implementatierichtlijn Objecten RWS (CSIR) naar een implementeerbare versie voor de waterschappen. Parallel daaraan wordt - rekening houdend met de CSIR - een Baseline Industriële Automatisering Cyber Security (BIACS) ontwikkeld, een breed toepasbaar algemeen kader voor procesautomatisering dat bruikbaar is voor meerdere sectoren. Dit in navolging van het advies van de Cyber Security Raad[10] hierover en in samenwerking de ministeries van Binnenlandse Zaken en Koninkrijksrelaties, Economische Zaken en Klimaat en Justitie en Veiligheid.

De tweede intensivering betreft het doorontwikkelen van het Computer Emergency Response Team (CERT) Water Management naar een Security Operations Center

---

[6] Tweede Kamer, vergaderjaar 2020-2021, 27 625, nr. 529

[7] https://www.rijksoverheid.nl/documenten/kamerstukken/2021/05/12/vragen-van-de-leden-van-ginneken-en-de-groot-d66-aan-de-minister-van-ienw-over-het-ilt-rapport-over-de-stichting-waternet

[8] Tweede Kamer, vergaderjaar 2019-2020, 27 625, nr. 522

[9] Programma Versterken Cyberweerbaarheid in de Watersector - Helpdesk water

[10] CSR Advies 'Industrial Automation & Control Systems (IACS)' - CSR-advies 2020, nr. 2 | Advies | Cyber Security Raad

(SOC) Water Management. Om de samenwerking binnen de watersector op het gebied van cybersecurity te versterken is een verkenning uitgevoerd t.b.v. een '*proof of concept'* (PoC) en een plan van aanpak opgesteld. In een gemeenschappelijk project van Rijkswaterstaat en het Waterschapshuis worden objecten van twee waterschappen aangesloten op het SOC van RWS. Dit als onderdeel van een haalbaarheidsonderzoek voor het leveren van de monitoringsdienst vanuit het SOC van Rijkswaterstaat aan de waterschappen. In een separaat project wordt binnen de drinkwatersector een onderzoek uitgevoerd naar de beste samenwerkingsmodaliteiten op het inzetten van een SOC.

Het derde intensiveringstraject betreft het toetsen van een ontwikkelde methodiek voor ketenrisico's door het toepassen op concrete waterketens. Om beter inzicht te krijgen in de zogenaamde cascade-effecten is in 2020 gestart met het ontwikkelen van een methodiek om ketenafhankelijkheden in kaart te brengen en een sectorbrede afhankelijkheids- en kwetsbaarheidsanalyse uit te voeren. De voorlopig vastgestelde methodiek is toegepast in een pilot over de afvoer van overtollig regenwater in het Noordzeekanaal. Vervolgens is gestart met toepassing in de keten (drink)waterkwaliteit. Daarna volgt de waterveiligheidsketen. Met de VNG heb ik afgesproken dat ook een keten waar het zwaartepunt bij de gemeenten ligt wordt opgepakt.

Digitale beveiliging waterwerken Rijkswaterstaat
In mijn Kamerbrieven[11] uit 2020 en tijdens het Wetgevingsoverleg van 1 december 2020 ben ik uitvoerig ingegaan op de maatregelen die Rijkswaterstaat (RWS) heeft genomen en gaat nemen om de aanbevelingen uit het rapport van de Algemene Rekenkamer (ARK) "Digitale Dijkverzwaring, Cybersecurity en Vitale Waterwerken" op te volgen. In 2021 en 2022 wordt extra geïnvesteerd in de cyberweerbaarheid van RWS. De komende twee jaar staat sturing door middel van risicobeheersing centraal, zowel via het RWS-versterkingsprogramma als een jaarlijks op te stellen informatiebeveiligingsbeeld (dit IB-beeld is bedoeld om meer op risicobeheersing en preventie te sturen). Als onderdeel van het versterkingsprogramma investeert RWS in 'security by design' bij vernieuwing & renovatie, voert het cybertesten uit als onderdeel van de functionele inspectie testen (FIT) uit, sluit het de komende jaren extra objecten voor monitoring door het SOC aan, neemt het risico gestuurd (acute) problemen weg en oefent het met de crisisorganisatie. Met deze aanpak is RWS beter in control en wordt de cybersecurity van de drie hoofdnetwerken verbeterd.

Hoogachtend,

DE MINISTER VAN INFRASTRUCTUUR EN WATERSTAAT,

drs. C. van Nieuwenhuizen Wijbenga

---

[11] Tweede Kamer, vergaderjaar 2019-2020, 27 625, nr. 507 en 522