Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2021–2022

27 625 Waterbeleid

Nr. 570

BRIEF VAN DE MINISTER VAN INFRASTRUCTUUR EN WATERSTAAT

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 7 juni 2022

Toenemende digitalisering maakt vitale sectoren, waaronder de watersector, kwetsbaar voor cyberincidenten. Daarnaast is door de veranderende geopolitieke verhoudingen zoals door de oorlog in Oekraïne, de digitale dreiging toegenomen. Cybersecurity is dan ook een essentiële randvoorwaarde voor een veilige en steeds meer digitaliserende watersector. In de Voortgangsbrief Water van 16 november 2021[1] is toegezegd dat de Kamer medio 2022 wordt geïnformeerd over het versterken van de cyberweerbaarheid in de watersector, specifiek de concrete resultaten die worden geboekt.
In deze brief informeer ik u over de laatste stand van zaken met betrekking tot:
– de continuering van het verscherpt toezicht op Waternet door de ILT;
– het Rijkswaterstaat Versterkingsprogramma Cybersecurity;
– de intensivering van de aanvullende cybersecurity afspraken op het Bestuursakkoord Water (BAW+). Tevens is als bijlage een overzicht van projecten toegevoegd;
– de Cybersecurity Strategie van het Ministerie van Infrastructuur en Waterstaat (IWCS).

Continuering verscherpt toezicht cybersecurity op Waternet door de ILT

In april 2021 is Stichting Waternet onder verscherpt toezicht geplaatst van de Inspectie Leefomgeving en Transport (ILT). De redenen hiervoor waren tekortkomingen in de cybersecurity en besturing bij Waternet, waardoor een verhoogd risico voor de leveringszekerheid en kwaliteit van drinkwater werd geconstateerd. Uw kamer is hierover geïnformeerd via diverse kamerbrieven[2].

[1] Kamerstuk 27 625, nr. 557
[2] Kamerstuk 27 625, nr. 539

kst-27625-570
ISSN 0921 - 7371
's-Gravenhage 2022

In de afgelopen periode heeft Waternet een verbeterplan opgestart en in uitvoering genomen. Uit de monitoring door de ILT blijkt dat progressie is geboekt, maar tegelijkertijd heeft de ILT geconstateerd dat er nog het nodige moet gebeuren, zowel voor het volledig in control komen op de cybersecurity als voor het verbeteren van doeltreffendheid van besturing. Volgens de ILT is daarmee het eerder geconstateerde verhoogde risico voor leveringszekerheid en kwaliteit van het drinkwater nog steeds aan de orde. In de tweede helft van 2022 zal de ILT opnieuw bekijken of het verscherpt toezicht kan worden afgeschaald.

Rijkswaterstaat Versterkingsprogramma Cybersecurity

Uw Kamer is eerder geïnformeerd over het versterkingsprogramma dat bij Rijkswaterstaat (RWS) wordt uitgevoerd naar aanleiding van het rapport van de Algemene Rekenkamer: «Digitale dijkverzwaring: Cybersecurity en vitale waterwerken» (Kamerstuk 30 821, nr. 69) en over de voortgang daarvan, middels de brieven voor de Commissie Debatten Water. RWS heeft de afgelopen jaren hard gewerkt om de aanbevelingen uit het rapport van de ARK op te volgen. Ook is uw kamer op 27 januari 2021 middels een, vanwege het vertrouwelijke karakter, besloten technische briefing geïnformeerd over de opvolging van de aanbevelingen en moties. Bij de instandhoudingsmaatregelen de komende jaren wordt rekening gehouden met cybersecurity en nationale- en economische veiligheid. Daarnaast wordt de cyberweerbaarheid verder verbeterd door middel van het RWS-versterkingsprogramma. Eén van de maatregelen betreft de uitbreiding van het Security Operations Centre (SOC), waarin objecten gemonitord worden van het Hoofdwatersysteem (HWS), Hoofdwegennet (HWN) en het Hoofdvaarwegennet (HVWN). Sinds de start van het versterkingsprogramma zijn de belangrijkste objecten geschouwd en zijn de eerste 30 van de circa 60 extra objecten (bovenop de al bestaande aangesloten objecten) aangesloten op het SOC. Het merendeel van de overige aansluitingen zal dit jaar plaatsvinden. Andere voorbeelden van maatregelen die tot uitvoering worden gebracht middels het versterkingsprogramma zijn het uitvoeren van een Baseline Informatiebeveiliging Overheid onderzoek, het uitvoeren van cybertesten als onderdeel van de functionele inspectietesten (FIT), het trainen en oefenen in voorbereiding op een cybercrisis.
Tijdens de begrotingsbehandeling van het Ministerie van IenW op 4 november 2021 is een Motie van de heer Madlener aangenomen met het verzoek de Kamer nader te informeren over de veiligheid van onze Hoofdnetwerken. In reactie daarop heb ik u toegezegd later dit jaar nader te informeren in een besloten technische briefing[3].

Intensivering van de aanvullende cybersecurity afspraken Bestuursakkoord Water (BAW+)

Door het programma «Versterken cyberweerbaarheid in de watersector» wordt gewerkt aan het uitvoeren van de aanvullende afspraken uit het Bestuursakkoord Water (BAW+) zoals vastgelegd in 2018. In eerdere Kamerbrieven bent u geïnformeerd over reeds geboekte resultaten[4]. In de bijlage vindt u een overzicht van de projecten die onder regie van het Ministerie van I&W door het programma worden uitgevoerd.
Hieronder een toelichting op een aantal projecten uit dit programma:
– Het proces keren & beheren waterkwantiteit is in 2016 aangemerkt als vitaal proces en Rijkswaterstaat als vitale aanbieder. Dit jaar vindt een herijking plaats van deze vitaalbeoordeling op basis van de voorgeschreven systematiek van de NCTV.

[3] Kamerstuk 35 925 XII, nr. 20
[4] Kamerstuk 27 625, nr. 539

– Zoals beschreven in het Cybersecurity Beeld Nederland 2021 (Kamerstuk 26 643, nr. 767) vormen ransomware aanvallen[5] een risico voor de nationale veiligheid als het gaat om de continuïteit van vitale processen. Dit geldt ook voor de watersector en daarom wordt in de komende periode extra ingezet op de weerbaarheid tegen ransomware aanvallen.
– Daarnaast word ingezet op het verbeteren van het proces van kwetsbaarheden- en patchmanagement en het ontwikkelen van een gezamenlijke red teaming testmethode[6]. Voor de ontwikkeling daarvan wordt aangesloten bij de Rijksbrede versterking van red teaming, waarover u eerder door de Staatssecretaris van BZK bent geïnformeerd[7].
– In navolging van eerdere ketenanalyses voor waterkwantiteit en -kwaliteit is recent een ketenanalyse afgerond van afvalwater waarbij ook een gemeente betrokken is geweest. De inzichten in ketenafhankelijkheden en -risico's zijn waardevol gebleken; hiermee zijn organisaties zich bewust van wederzijdse afhankelijkheden en kunnen adequate maatregelen worden genomen om deze risico's te verkleinen. Deze ketenanalyses worden de komende jaren dan ook verder uitgerold voor het gehele Hoofdwatersysteem.

In het coalitieakkoord (Bijlage bij Kamerstuk 35 788, nr. 77) staat dat we onze vitale sectoren beter moeten beschermen door centraal gecoördineerde structurele samenwerking tussen onder andere het Nationaal Cyber Security Centrum (NCSC), het Digital Trust Center (DTC), overheden, bedrijven en wetenschappers. Om de positieve ervaringen en kennis uit het programma van IenW breder te benutten wordt er samen met het NCSC, het DTC en Rijkswaterstaat gewerkt aan een intensievere samenwerking om kennis van cybersecurity in Operationele Techniek (OT) beter te borgen. Dit is ook overeenkomstig de eerdere adviezen van de Cyber Security Raad (CSR) met betrekking tot de integrale aanpak van cyberweerbaarheid[8], specifiek gericht op het versterken van de cyberweerbaarheid van vitale aanbieders en OT.

IenW Cybersecurity Strategie

De Minister van IenW is systeemverantwoordelijk voor de cybersecurity van een aanzienlijk deel van de vitale sectoren in Nederland. Momenteel wordt gewerkt aan een IenW Cybersecurity Strategie (2022–2026). Deze loopt synchroon met de herziening van de Nederlandse Cybersecurity Strategie onder coördinatie van de NCTV. De IenW Cybersecurity Strategie beschrijft de cybersecurity aanpak en heeft als doel om IenW en de vitale sectoren waar IenW een verantwoordelijkheid heeft digitaal veiliger te maken. Daarmee zijn we in staat op een betere wijze de kansen van digitalisering te verzilveren en tegelijkertijd onze veiligheid te beschermen.

Ik informeer de Kamer dit najaar over de IenW Cybersecurity Strategie.

De Minister van Infrastructuur en Waterstaat,
M.G.J. Harbers

---

[5] Ransomware is malware die de databestanden van gebruikers versleutelt, met als doel om deze later te ontsleutelen in ruil voor losgeld

[6] Red teaming is het gecontroleerd uitvoeren van geavanceerde cyberaanvallen door middel van echte aanvalstechnieken op basis van de meest actuele dreigingsinformatie. Hierbij is er sprake van een verdedigend (blue) en aanvallend (red) team om de beveiliging te testen

[7] Kamerstukken 26 643 en 31 490, nr. 836

[8] CSR Adviesrapport «Integrale aanpak cyberweerbaarheid» | Rapport | Cyber Security Raad