Rijkswaterstaat
Ministerie van Infrastructuur en Waterstaat

Retouradres: Rijkswaterstaat | Postbus 2232 | 3500 GE Utrecht

RWS INFORMATIE
De president van de Algemene Rekenkamer
De heer drs. A.P. Visser
Lange Voorhout 8
2500 EA Den Haag

Rijkswaterstaat Centrale Informatievoorziening

Derde Werelddreef 1
2622 HA Delft
Postbus 2232
3500 GE Utrecht
T 088 797 2800
F 088 797 2909
civ-info@rws.nl
www.rijkswaterstaat.nl

Contactpersoon

Ons kenmerk
RWS-2019/7178

Datum 25 februari 2019
Onderwerp Onderzoek Algemene Rekenkamer 'Digitale dijkverzwaring: cybersecurity en vitale waterwerken 2018'

Geachte heer Visser,

Met belangstelling heb ik kennis genomen van de resultaten van uw onderzoek naar de wijze waarop de vitale waterwerken in beheer van Rijkswaterstaat, beschermd zijn tegen cyberaanvallen. Graag maak ik van de gelegenheid gebruik om op uw rapport 'Digitale dijkverzwaring, Cybersecurity en vitale waterwerken', d.d. 31 januari 2019 te reageren.

1. Algemeen

Digitalisering speelt een grote rol in de samenleving. Juist met het oog op de vitale infrastructuur bij mijn ministerie, zie ik het als mijn verantwoordelijkheid om de digitale veiligheid hiervan goed te organiseren. De digitale weerbaarheid van de watersector heeft in dat licht bezien mijn aandacht. Eind oktober heb ik met de ketenpartners in de watersector hieromtrent bestuurlijke afspraken gemaakt en heeft mijn ministerie recentelijk de IenW-brede Cybersecurity Strategie vastgesteld.

IenW werkt met een risico gestuurde aanpak. Zoveel als mogelijk worden de (cyber)risico's uitgesloten en gemitigeerd waarbij vanwege de begrenzing aan de beschikbare middelen geprioriteerd wordt op basis van het risico dat uitval/verstoring met zich mee kan brengen. De IenW-brede Cybersecurity Strategie geeft richting in het maken van deze prioritering.

2. Conclusies en aanbevelingen

Hoofdconclusie:
Ik onderschrijf uw hoofdconclusie dat Rijkswaterstaat de afgelopen jaren veel werk heeft verzet om alle objecten (meer dan 400, met ieder een unieke IT-infrastructuur) integraal te beveiligen waarbij u tegelijkertijd stelt dat Rijkswaterstaat nog stappen moet zetten om aan de eigen doelstellingen voor cybersecurity te voldoen. Uw conclusies en aanbevelingen zie ik als een ondersteuning van de reeds door mij in gang gezette strategie om de cybersecurity van IenW verder te verbeteren.

Aanbeveling 1: Cybersecurity-dreigingsniveau:
U beveelt aan, om onderzoek uit te voeren naar het actuele cybersecurity-dreigingsniveau voor de vitale waterwerken ten behoeve van nadere besluitvorming over allocatie van mensen en capaciteit.

Ik onderschrijf deze aanbeveling en zal (laten) inzetten op een praktische doorvertaling van de algemene dreigingsbeelden en de aanvullende informatie verkregen vanuit de samenwerking met de diensten naar mogelijke consequenties voor de individuele vitale objecten. Vanuit de IenW cybersecuritystrategie zal deze, object gerelateerde dreigingsinformatie, meegenomen worden in de besluitvorming over normering en hiervoor benodigde inzet van mensen en middelen.

Aanbevelingen 2 en 3: Afronding programma Beveiligd Werken Rijkswaterstaat:
Uw conclusies en bevindingen met betrekking tot het programma Beveiligd Werken Rijkswaterstaat (BWR) herken ik. Er is veel werk verzet maar op een aantal vlakken zijn de doelstellingen van BWR nog niet gehaald en zijn er nog een aantal stappen nodig om die alsnog te behalen.

Ondertussen heeft Rijkswaterstaat een flinke inhaalslag gemaakt ten aanzien van de opvolging van de BWR restpunten. Het complete overzicht van de stappen die nog moeten worden gezet om de BWR doelstellingen de halen, is beschikbaar. De keuze ten aanzien van welke maatregelen met welke prioritering zullen worden opgevolgd, hangt met name af van de resultaten van de aanscherping van het actuele dreigingsniveau en de bijbehorende besluitvorming over de gewenste normering. Ditzelfde geldt voor de keuze in hoe verre instrumenten als FIT versterkt moeten worden

Aanbeveling 4: Detectie op cyberaanvallen bij vitale waterwerken voltooien:
U concludeert dat in het tijdvak 2017 en 2018 de doelstelling van de detectie van en response op mogelijke cyberaanvallen, op de door mij aangewezen vitale objecten niet is behaald. Hierbij beveelt u aan om de ingezette lijn te voltooien, op basis van het objectief vastgestelde dreigingsniveau (uw eerste aanbeveling).

Het SOC en de monitoring capaciteit van Rijkswaterstaat zijn inderdaad noodzakelijke voorwaarden om cyberaanvallen te kunnen detecteren en af te slaan. In welke mate versterking nodig is, zal afhankelijk zijn van de actualisatie van het dreigingsniveau zoals in aanbeveling 1 is geschetst. Deze geactualiseerde dreigingsinformatie zal meegenomen worden in de IenW cybersecuritystrategie waaruit de prioritering van cybersecuritymaatregelen, waaronder versterking van het SOC, plaats vindt.

Aanbeveling 5: Heroverweging screeningsniveau SOC-Personeel & informatie-rubricering Rijkswaterstaat:
U beveelt aan om het huidige screeningsniveau en informatie-rubriceringsniveau van Rijkswaterstaat te heroverwegen, afhankelijk van uw eerste aanbeveling.

Ik zal, in overleg met NCTV, de mogelijkheden laten onderzoeken om dit screeningsniveau beter aan te laten sluiten bij het vastgestelde dreigingsniveau.

Aanbeveling 6 en 7: Proces actuele crisis- en netwerkkaarten en crisisscenario's voor cybersecuritycrisis
U concludeert dat Rijkswaterstaat niet over een geborgd proces beschikt om de informatie met betrekking tot de crisiskaarten en netwerkkaarten actueel te (be)houden. Daarnaast heeft u geconstateerd dat Rijkswaterstaat nog niet beschikt over een specifiek crisisscenario voor cybersecurity

Ik neem uw aanbevelingen over. De noodzaak om cascade-effecten inzichtelijk te krijgen, heb ik opgenomen in het in oktober afgesloten Bestuursakkoord Water. Voor een breder beeld van deze cascade-effecten, sluit IenW aan bij de aanpak van intersectorale afhankelijkheden van het ministerie van Justitie en Veiligheid.

Aanbeveling 8: Expliciete risico's pentesten op Industriële Automatisering:
U beveelt tot slot aan om expliciet te maken welke risico's het doen van volwaardige penetratietesten op vitale waterwerken 'in de weg staan', om zodoende hierop maatregelen te treffen of aan te passen.

Uw aanbeveling heeft betrekking op bestaande objecten. In lijn met uw aanbeveling zal onderzocht worden wat de risico's en mogelijkheden zijn voor invoeren van pentesten bij bestaande systemen. Van belang is dat bij nieuwe aanleg en renovatieprojecten altijd pentesten worden uitgevoerd. Hiervoor wordt een voorziening ingericht.

3. Resultaat

U oordeelt dat Rijkswaterstaat als onderdeel van het ministerie van Infrastructuur en Waterstaat de goede weg is ingeslagen. Terecht constateert u dat hierbij het einddoel nog niet is bereikt. In de dagelijkse veranderlijke cyberwereld blijft investeren in de integrale beveiliging voor Nederland essentieel. Ik neem met genoegen kennis van uw uiteindelijke oordeel en reactie.

Hoogachtend,

DE MINISTER VAN INFRASTRUCTUUR EN WATERSTAAT,

drs. C. van Nieuwenhuizen Wijbenga