Ministerie van Infrastructuur
en Waterstaat

> Retouradres Postbus 20901 2500 EX Den Haag

De voorzitter van de Tweede Kamer
der Staten-Generaal
Postbus 20018
2500 EA 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

Ons kenmerk
IENW/BSK-2021/288555

Datum 11 november 2021
Betreft Beantwoording Kamervragen over de kwetsbaarheid van bruggen en riolen voor hackers

Geachte voorzitter,

Via deze brief beantwoord ik de vragen die Lid Madlener (PVV) mij heeft gesteld (Kamerstuk 2021Z18070) over de kwetsbaarheid van bruggen en riolen voor hackers.

Vraag 1
Bent u op de hoogte van het gepubliceerde artikel in Het Financieel Dagblad en het onderzoek dat op 14 oktober 2021 is gepubliceerd door de vakbladen Binnenlands Bestuur en AG Connect?

Antwoord 1
Ja

Vraag 2
Zijn er bruggen en rioleringssystemen die op dit moment kwetsbaar zijn en geen update kunnen krijgen met de laatste beveiligingsmaatregelen? Zo ja, welke zijn dit?

Antwoord 2
Bruggen en rioleringssystemen zijn veelal in beheer bij decentrale overheden. Decentrale overheden zijn zelf verantwoordelijk om op basis van risicoanalyse en risicoafweging beveiligingsmaatregelen te nemen. Ik heb geen signalen van de sector of koepelorganisaties VNG, UvW of IPO ontvangen dat Industriële Controle Systemen (ICS) van bruggen en rioleringen bij decentrale overheden op grote schaal kwetsbaar zouden zijn en dat het ontbreken van updates benodigde beveiligingsmaatregelen zou belemmeren, zie ook de beantwoording van vraag 3.

Vraag 3
Welke risico's lopen de controlesystemen bij onder andere rioleringen, sluizen en verkeerslichten op dit moment op?

Antwoord 3
Risico's van controlesystemen zijn in het algemeen systeem-, organisatie-, locatie- en tijdsspecifiek en hangen samen met beveiligingsmaatregelen die door een organisatie zijn getroffen. Iedere organisatie opereert binnen haar eigen organisatie-specifieke context en maakt op basis van een risicoanalyse een risicoafweging. Risico's die bij ICS systemen kunnen ontstaan, worden vooral veroorzaakt door koppelingen aan het internet waardoor systemen op afstand kunnen worden gemanipuleerd, overgenomen of onklaar worden gemaakt. Om uitval te voorkomen zijn er veelal terugval opties aanwezig, zoals bijvoorbeeld de handbediening van bruggen en sluizen.

Vraag 4
Welke acties heeft u getroffen naar aanleiding van het kritische rapport van de Algemene Rekenkamer vanaf 2019?

Antwoord 4
Sinds publicatie van het rapport van de Algemene Rekenkamer 'Digitale Dijkverzwaring: cybersecurity en vitale waterwerken' uit 2019[1] heeft er bij Rijkswaterstaat (RWS) een flinke verbeterslag plaatsgevonden. Ik heb uw Kamer in 2020[2] geïnformeerd over mijn inzet in deze. Op 2 juni 2021[3] heb ik uw Kamer geïnformeerd over de laatste stand van zaken via mijn brief 'Update Versterken Cyberweerbaarheid in de Watersector'.
RWS investeert in verbetering van de digitale beveiliging, via het RWS-versterkingsprogramma. Één van de prioritaire maatregelen betreft de aansluiting van extra objecten op het Security Operations Centre (SOC[4]).. In 2019 zijn alle vitale objectenl aangesloten. Van de overige niet-vitale objecten zijn momenteel 12 van de 60 aangesloten. Het betreft daarbij objecten zoals bijvoorbeeld bruggen en sluizen, van het Hoofdwatersysteem (HWS), het Hoofdwegennet (HWN) en het Hoofdvaarwegennet (HVWN). De verwachting is dat in 2023 alle 60 objecten zijn aangesloten.

Vraag 5
Kunt u de kamer informeren over de huidige stand van zaken en wat het plan van aanpak is om onze infrastructuur te beschermen tegen hackers?

Antwoord 5
Binnen de overheid lopen er meerdere initiatieven om de vitale infrastructuur te beschermen en de digitale weerbaarheid te verhogen. Voor de stand van zaken van de Nationale Cybersecurity Agenda verwijs ik naar de beleidsreactie Cyber Security Beeld Nederland 2021 en voortgangsrapportage NCSA die op 28 juni 2021 door de Minister van Justitie en Veiligheid met uw Kamer is gedeeld[5].
Samen met de drinkwaterbedrijven, waterschappen, gemeenten, provincies en Rijkswaterstaat heeft het ministerie van Infrastructuur en Waterstaat het

[1] Algemene Rekenkamer, 28 maart 2019, 'Digitale dijkverzwaring: cybersecurity en vitale waterwerken'
[2] Kamerstuk 27625-522
[3] Kamerstuk 27625-539
[4] Een Security Operations Center (SOC) bewaakt de netwerken van een organisatie om cyberincidenten te voorkomen en te adresseren onder andere door monitoring, detectie, analyse en mitigatie.
[5] Kamerstuk 26643-767

Programma Versterken Cyberweerbaarheid in de Watersector 2019-2022 (PVCW[6]) opgezet. Binnen het programma zijn vijftien projecten geformuleerd die moeten bijdragen aan de versterking van de cyberweerbaarheid in de watersector. De projecten richten zich met name op de cybersecurity van de operationele technologie. Meer informatie kunt u vinden in de eerder genoemde brief[7].

Vraag 6
Bent u al in gesprek getreden met gemeenten, provincies en de waterschappen inzake de beveiligingsrisico's?

Antwoord 6
Ja, bijvoorbeeld in het programma "Versterken Cyberweerbaarheid in de Watersector" vindt regelmatig overleg plaats met en tussen de decentrale overheden en betrokken organisaties, zie ook antwoord op vraag 5.

Vraag 7
Zijn er al casussen aangetroffen waarbij er daadwerkelijk problemen zijn ontstaan in het verkeer of de waterkwaliteit doordat er een controlesysteem gehackt is geweest? Zo ja, welke casussen zijn dit?

Antwoord 7
Nee, dergelijk casussen in Nederland zijn nog mij niet bekend. De Wet beveiliging netwerk- en informatiesystemen (Wbni) verplicht vitale aanbieders en aanbieders van essentiële diensten incidenten of inbreuken met aanzienlijke gevolgen voor de continuïteit van de verleende dienst te melden bij het Nationaal Cyber Security Centrum.

Vraag 8
Bent u bereid om bijvoorbeeld bij aanbestedingen en inkooptrajecten strengere eisen te stellen inzake beveiligingsupdates en de controle daarop?

Antwoord 8
Het is sinds de aanscherping van de nationale veiligheidsrisico's voor inkoop en aanbesteding in 2018 staand beleid vanuit de Rijksoverheid dat nationale veiligheidsoverwegingen worden meegewogen. Een overheidsorganisatie die ICT-producten en –diensten inkoopt moet de eisen uit de Baseline Informatiebeveiliging Overheid (BIO) vertalen naar inkoopcontracten en afspraken maken over de naleving van die contracteisen. Bij de aanschaf en implementatie van gevoelige apparatuur wordt rekening gehouden met eventuele risico's in relatie tot de leverancier en met het concrete gebruik van de systemen.

Vraag 9
Waarom is er in het Deltaprogramma 2022 geen aandacht geschonken aan deze bevolkingsproblematiek?

Antwoord 9
Samenwerkingsafspraken over cybersecurity, met thema's zoals de door u genoemde beveiligingsproblematiek, verlopen via het Bestuursakkoord Water en een apart ingericht programma voor de implementatie daarvan (zie ook antwoord

[6] https://www.helpdeskwater.nl/onderwerpen/wetgeving-beleid/bestuursakkoord/cyberweerbaarheid/
[7] Kamerstuk 27625-539

op vraag 6). Op pagina 22 van het Deltafonds 2022[8] wordt de aanpak van cyberweerbaarheid beschreven.

Hoogachtend,

DE MINISTER VAN INFRASTRUCTUUR EN WATERSTAAT,

drs. B. Visser

Ministerie van Infrastructuur en Waterstaat

Ons kenmerk
IENW/BSK-2021/288555

[8] Kamerstuk 35 925 J, nr. 2