

2021Z18276

Vragen van de leden **Rajkowski**, **Rudmer Heerema** en **Peter de Groot** (allen VVD) aan de Ministers van Justitie en Veiligheid en van Infrastructuur en Waterstaat over *het bericht «Onderzoek: riolen en bruggen kwetsbaar voor hackers»* (ingezonden 20 oktober 2021).

Vraag 1

Bent u bekend met bovenstaand bericht?¹

Vraag 2

Bent u bekend met het onderzoek van Binnenlands Bestuur en AG Connect naar de kwetsbaarheden in industriële controlesystemen waarmee onder meer rioleringen, sluizen en verkeerslichtsystemen worden aangestuurd? Zo ja, hoe beoordeelt u de bevinding dat deze controlesystemen kwetsbaar zijn voor hackers?

Vraag 3

Hoe vaak is het in de afgelopen twee jaar binnen Rijkswaterstaat of ProRail voorgekomen dat een succesvolle aanval is gepleegd op de systemen van bediening, besturing en bewaking? Welke maatregelen zijn binnen het Chief Information Security Officer (CISO) domein genomen om inbreuk op vitale systemen in de toekomst te voorkomen?

Vraag 4

Klopt het dat de kwetsbaarheden in de controlesystemen onder meer worden veroorzaakt door de afwezigheid van beveiligingsupdates en het gebruik van verouderde besturingssystemen? Zo ja, hoe beoordeelt u dit beleid, zijn hierover afspraken gemaakt met de aanbieders van de besturingssystemen en wat zijn de kosten hiervan op jaarlijkse basis? Deelt u de mening dat een gebrek aan adequate beveiliging van dergelijke systemen kan leiden tot aanzienlijke (nationale) veiligheidsrisico's met mogelijk ontwrichtende gevolgen?

Vraag 5

Klopt het dat een goedwillende hacker op afstand het rioleringsstelsel van een grote gemeente kon overnemen, dit vervolgens meldde bij de betreffende gemeente, maar het vervolgens maanden duurde voor de benodigde

¹ Onderzoek: riolen en bruggen kwetsbaar voor hackers (fd.nl)

update werd uitgevoerd? Zo ja, hoe beoordeelt u deze gang van zaken? Bent u het eens dat, gezien de aanzienlijke veiligheidsrisico's van kwetsbaarheden in het systeem, snelheid hier geboden is?

Vraag 6

Kunt u toelichten welk beleid wordt gevoerd ten aanzien van beveiligingsproblemen en in het bijzonder van het updaten van software van industriële besturingssystemen? Zo ja, welke problemen worden hier ondervonden en wordt in samenwerking met experts gezocht naar oplossingen voor deze problemen? Zo nee, waarom niet?

Vraag 7

Welke veiligheidseisen worden gesteld bij de inkoop van software en hardware voor industriële besturingssystemen? Wordt een risicoanalyse uitgevoerd bij de aankoop van de betreffende software en wordt regelmatig getest of beiden voldoen aan de dan geldende veiligheidseisen? Zo ja, wat wordt gedaan met de uitkomsten van de risicoanalyses? Zo nee, waarom niet?

Vraag 8

Wat is de huidige stand van zaken van het uitvoeren van de aanbevelingen die de Algemene Rekenkamer in 2019 heeft gedaan ten aanzien van de cyberbeveiliging van waterwerken? Welke aanbevelingen zijn reeds overgenomen en uitgevoerd en welke nog niet?

Vraag 9

In hoeverre worden dreigingsbeelden ingezet en praktisch doorvertaald naar de bescherming van industriële besturingssystemen en in het bijzonder individuele vitale objecten zoals waterkeringen en sluizen?

Vraag 10

Bent u het eens dat bij het keren en beheren van water de fysieke veiligheid van miljoenen Nederlanders op het spel staat? Zo ja, bent u het dan ook eens dat het niveau van cybersecurity van systemen die rioleringen, bruggen en sluizen aansturen aanzienlijk hoger moet liggen dan nu het geval is? Zo ja, bent u bereid maatregelen te treffen om dit niveau te verhogen? Zo ja, welke? Zo nee, waarom niet?