Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2021–2022

Aanhangsel van de Handelingen

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

652

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).

Antwoord van Minister **Visser** (Infrastructuur en Waterstaat), mede namens de Minister van Justitie en Veiligheid (ontvangen 11 november 2021).

Vraag 1
Bent u bekend met bovenstaand bericht?[1]

Antwoord 1
Ja.

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?

Antwoord 2
Ja. De beveiliging van dergelijke systemen vereist een andere aanpak dan reguliere IT-systemen. Dit komt door de specifieke risico's die samenhangen met het toepassingsgebied. Deze systemen hebben een langere levensduur en zijn complexer. Juist daarom is er de laatste jaren extra aandacht voor de beveiliging van operationele technologie, bijvoorbeeld in het programma «Versterken Cyberweerbaarheid in de Watersector». Zie ook het antwoord bij vraag 6.

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?

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

ah-tk-20212022-652
ISSN 0921 - 7398
's-Gravenhage 2021

Antwoord 3
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 (NCSC). Er zijn de afgelopen twee jaar geen Wbni-meldingen gedaan door Rijkswaterstaat (RWS). RWS investeert actief in de verbetering van de digitale beveiliging. Zowel via het RWS versterkingsprogramma als ook via het jaarlijkse informatiebeveiligingsbeeld vanuit het CISO-domein worden diverse acties opgesteld en uitgevoerd ten behoeve van de (digitale) veiligheid, zoals uitvoeren van cybertesten als onderdeel van functionele inspectietesten en het oefenen van planvorming tijdens een cybercrisis ProRail heeft systemen voor de besturing van bruggen, tunnels en beveiliging op het spoor. Deze worden (deels) op afstand bestuurd vanuit de Verkeersleiding-posten. Er zijn geen succesvolle (cyber)aanvallen uitgevoerd. Op de essentiële systemen is een zwaar cybersecurity regime van toepassing. Dit regime wordt met regelmaat door externe onderzoeksbureaus getoetst op betrouwbaarheid en werking.

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?

Antwoord 4
De door u genoemde kwetsbaarheden die bij Industriële Controle Systemen (ICS) kunnen ontstaan, kunnen vooral benut worden door hackers indien er koppelingen zijn met het internet waardoor systemen op afstand kunnen worden gemanipuleerd, overgenomen of onklaar worden gemaakt. Risico's van controle-systemen zijn in het algemeen systeem-, organisatie-, locatie- en tijd specifiek en hangen samen met beveiligingsmaatregelen die door de organisatie zijn getroffen.
Ons beleid is erop gericht organisaties bewust te maken van deze kwetsbaarheden, kennis te delen en te waarborgen dat er maatregelen worden genomen om deze nationale risico's zoveel mogelijk te verkleinen. Het programma «Versterken Cyberweerbaarheid in de Watersector» levert hier een belangrijke bijdrage aan. De uitvoering van het programma wordt bekostigd uit het IenW-budget van de Nationale Cyber Security Agenda (NCSA). Zie voor de inzet van regelgeving ook vraag 6.

Vraag 5
Klopt het dat een goedwillende hacker op afstand het rioleringssysteem van een grote gemeente kon overnemen, dit vervolgens meldde bij de betreffende gemeente, maar het vervolgens maanden duurde voor de benodigde 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?

Antwoord 5
Uit navraag blijkt geen nadere informatie beschikbaar over een casus van een goedwillende hacker die het rioleringssysteem van een grote gemeente kon overnemen.
Voor de aanpak van de veiligheidsrisico's die volgen uit kwetsbaarheden in een systeem, zie de beantwoording van vraag 4, 6, 7 en 9.

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?

Antwoord 6
Op 1 juli j.l. is voor alle Aanbieders van Essentiele Diensten (AED's) binnen het IenW-domein de Regeling beveiliging netwerk- en informatiesystemen IenW (MR)[2] in werking getreden om de AED's meer handvatten te bieden bij de uitvoering van hun zorgplicht, waaronder maatregelen op het gebied van detectie en respons en patchmanagement. Met deze MR wordt ook de ILT in staat gesteld hier goed toezicht op te houden. Het Nationaal Cybersecurity Centrum (NCSC) heeft voor het adequaat patchen van industriële besturingssystemen diverse handreikingen opgesteld [3]. Daarnaast wordt er regelmatig door het NCSC en de diverse ministeries, samen met leveranciers gesproken over (de noodzaak van) goed patchmanagement. Hierbij wordt samen gewerkt in diverse initiatieven[4], bijvoorbeeld in de Cybersecurity Alliantie. Al deze maatregelen tezamen borgen dat de betreffende organisaties weerbaarder zijn bij cyberrisico's: ze hebben inzicht in de mate waarop de maatregelen doeltreffend zijn, de risico's kunnen beter beheerst worden en ze zijn in staat voortdurend bij te sturen.

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?

Antwoord 7
Een overheidsorganisatie die ICT-producten en -diensten inkoopt moet de eisen uit de Baseline Informatiebeveiliging Overheid (BIO) vertalen naar inkoop-contracten en afspraken maken over de naleving van die contracteisen. Het uitvoeren van risicoanalyses en testen is hier onderdeel van. De aanscherping van de nationale veiligheidsrisico's voor inkoop en aanbesteding is eind 2018 geïmplementeerd door de rijksoverheid. Hiermee is het staand beleid vanuit de rijksoverheid dat nationale veiligheidsoverwegingen worden meegewogen bij de inkoop en aanbesteding van producten en diensten. 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 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?

Antwoord 8
Sinds het rapport van de Algemene Rekenkamer «Digitale Dijkverzwaring» uit 2019 heeft er bij Rijkswaterstaat (RWS) een flinke verbeterslag plaatsgevonden. RWS investeert in verbetering van de digitale beveiliging, via het RWS-versterkingsprogramma. Ik heb uw kamer hierover geïnformeerd in 2020[5] en onlangs over de laatste stand van zaken via mijn brief «Update Versterken Cyberweerbaarheid in de Watersector» op 2 juni 2021[6]. Sindsdien zijn de maatregelen voor procesautomatisering in de «Cybersecurity Implementatie Richtlijn Objecten» waarmee deze op bredere schaal kunnen worden toegepast. Een andere prioritaire maatregel betreft de aansluiting van extra objecten op het Security Operations Centre (SOC)[7] van RWS. Het betreft daarbij objecten, zoals bijvoorbeeld bruggen en sluizen,van het Hoofdwater-

[2] Staatscourant 2021, 25471 | Overheid.nl > Officiële bekendmakingen (officielebekendmakingen.nl)
[3] ICS weerbaar maken | ICS | Nationaal Cyber Security Centrum (ncsc.nl)
[4] Doe de Security Check Procesautomatisering | Digital Trust Center (Min. van EZK)
[5] Kamerstuk 27 625-522
[6] Kamerstuk 27 625-539
[7] 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.

systeem (HWS), het Hoofdwegennet (HWN) en het Hoofdvaarwegennet (HVWN). Hiermee kunnen kwetsbaarheden eerder gesignaleerd worden en kan er adequaat actie worden genomen om deze te verhelpen.

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?

Antwoord 9
Dreigingsbeelden worden gedeeld door de veiligheidsdiensten met de betreffende bedrijven en instellingen. Deze maken zelf een doorvertaling naar de systemen in eigen beheer en de organisatie specifieke impact. Vanuit onze beleidsverantwoordelijkheid bieden wij hierbij ondersteuning. Organisaties zijn zelf verantwoordelijk om de juiste maatregelen te implementeren. Waar het aanbieders van essentiële diensten (AED's) betreft, zien de toezichthouders hierop toe.

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?

Antwoord 10
Ja, ik deel uw mening dat het keren en beheren van water cruciaal is voor de bescherming van Nederland. Daarom is «keren en beheren van de waterkwantiteit» een vitaal proces in categorie A (infrastructuur die bij verstoring, aantasting of uitval ernstige gevolgen heeft op economisch, fysiek of sociaal-maatschappelijk vlak met mogelijke cascade gevolgen). Er wordt hard gewerkt aan het verhogen van het niveau van cyberweerbaarheid van vitale objecten binnen dit proces en deze vallen ook onder de Wbni, zie ook mijn antwoord onder vraag 8.
Verder heb ik vanuit mijn systeemverantwoordelijkheid aandacht voor de cybersecurity van systemen die riolering, bruggen en sluizen aansturen. Daarom werken we samen met decentrale overheden om ook hier de cyberweerbaarheid te verhogen en de Nederlandse infrastructuur blijvend te beschermen.