Ministerie van Economische Zaken
en Klimaat

> Retouradres Postbus 20401 2500 EK Den Haag

De Voorzitter van de Tweede Kamer
der Staten-Generaal
Prinses Irenestraat 6
2595 BD DEN HAAG

Directoraat-generaal Klimaat en Energie
Directie Energiemarkt

Bezoekadres
Bezuidenhoutseweg 73
2594 AC Den Haag

Postadres
Postbus 20401
2500 EK Den Haag

Overheidsidentificatienr
00000001003214369000

T 070 379 8911 (algemeen)
F 070 378 6100 (algemeen)
www.rijksoverheid.nl/ezk

Datum 10 februari 2023
Betreft Beantwoording Kamervragen over het bericht 'Russische hackers hebben het gemunt op Nederlandse gasinstallaties'

Ons kenmerk
DGKE-DE / 26164892

Uw kenmerk
2022Z23572

Geachte Voorzitter,

Hierbij zend ik u, mede namens de minister van Justitie en Veiligheid, de antwoorden op de vragen van het lid Bontenbal (CDA) over het bericht ‘Russische hackers hebben het gemunt op Nederlandse gasinstallaties’
(kenmerk: 2022Z23572; ingezonden 30 november 2022).

R.A.A. Jetten
Minister voor Klimaat en Energie

Directoraat-generaal Klimaat en Energie
Directie Energiemarkt

Ons kenmerk
DGKE-DE / 26164892

2022Z23572

1
Bent u bekend met het bericht 'Russische hackers hebben het gemunt op Nederlandse gasinstallaties'?[1]

Antwoord
Ja.

2
Bent u ook bekend met het bericht uit april 2022 waarin al werd gewaarschuwd voor nieuw ontdekte malware, specifiek gericht op het aanvallen van de energie-industrie?[2]

Antwoord
Ja.

3
Onderschrijft u dat de Nederlandse en Europese gasinfrastructuur momenteel uitermate kwetsbaar zijn en tegelijk van groot belang zijn voor onze nationale veiligheid en onze energievoorziening?

4
Kunt u toelichten welke maatregelen, fysiek en digitaal, worden genomen om de gasinfrastructuur te beschermen tegen sabotage en cyberaanvallen? Kunt u bevestigen dat niet alleen infrastructuur op zee, maar ook infrastructuur op land zoals de LNG-terminals in de Rotterdamse haven en de Eemshaven wordt meegenomen in de maatregelen?

Antwoord 3 en 4
Ik onderschrijf dat onze en de Europese gasinfrastructuur van groot belang zijn voor onze energievoorziening en daarmee van groot belang voor de nationale veiligheid. De overheid werkt samen met direct betrokken partijen om zo veel mogelijk dreigingen te voorkomen en risico's te beheersen. Waar risico's of dreigingen zich toch voordoen wordt samengewerkt om snel en adequaat te reageren.

Entiteiten die gasinfrastructuur beheren zijn in eerste instantie zelf verantwoordelijk voor de continuïteit van hun dienstverlening en hun rol in het vitale proces en ook voor het op orde hebben van hun digitale weerbaarheid. De overheid is zich echter bewust dat vitale aanbieders zich niet in alle gevallen voldoende kunnen weren tegen door statelijke actoren gesteunde sabotage, spionage en manipulatie. De overheid ondersteunt hen daarom hierbij, onder

[1] RTL Nieuws, 25 november 2022, 'Russische hackers hebben het gemunt op Nederlandse gasinstallaties', https://www.rtlnieuws.nl/economie/artikel/5348201/hackers-rusland-lng-gasterminal-nederland-europese-unie-cyberoorlog
[2] Washington Post, 13 april 2022, 'U.S. warns newly discovered malware could sabotage energy plants', https://www.washingtonpost.com/technology/2022/04/13/pipedream-malware-russia-lng/

andere door kennis en informatie te delen. Dit geldt zowel voor de infrastructuur op zee als op land.

Als minister voor Klimaat en Energie ben ik verantwoordelijk voor de vitale processen binnen de energiesector. Vanuit haar regierol op de vitale infrastructuur stel ik samen met de minister van Justitie en Veiligheid eisen op die worden vastgelegd in wet- en regelgeving en zie ik toe op de naleving ervan. Daarnaast faciliteer ik, met het oog op de leveringszekerheid vitale aanbieders bij het vergroten van hun weerbaarheid. Dit geldt ook voor vitale aanbieders in de gassector. Bijvoorbeeld door het vergroten van de mogelijkheden voor netbeheerders om hun inkoop processen te beperken via de Aanbestedingswet op defensie- en veiligheidsgebied onder de energiewet. Zie voor meer maatregelen ook de brief over leveringszekerheid die op 9 december naar uw Kamer is gestuurd (Kamerstuk 29023, nr. 384). Op lokaal niveau zijn Veiligheidsregio's verantwoordelijk voor risicobeheersing en crisisbeheersing. In dit kader vindt er samenwerking plaats met private partijen, waaronder vitale aanbieders.

Netbeheerders van gasinfrastructuur zijn door de overheid aangewezen als aanbieder van essentiële dienst (AED) op grond van de Wet beveiliging netwerk- en informatiesystemen (Wbni). Per 1 januari 2023 is het vitale proces uitgebreid naar 'Gasproductie (incl. gasbehandelingsinstallaties), gasopslag, landelijk en zee transport (incl. conversie) en regionale distributie van gas'[3] (Kamerstuk 2022Z24210). Entiteiten actief in dit proces zijn hierdoor ook aangewezen als AED. Op grond van de Wbni zijn AED's verplicht tot het treffen van passende en evenredige technische en organisatorische maatregelen om de risico's voor de beveiliging van hun netwerk- en informatiesystemen te beheersen en verstorende incidenten te melden. Sectorale toezichthouders houden toezicht op de manier waarop vitale aanbieders invulling geven aan deze zorgplicht, in dit geval is dat de Rijksinspectie Digitale Infrastructuur (RDI). Daarnaast hebben AED's recht op dienstverlening vanuit het Nationaal Cyber Security Centrum (NCSC). Het NCSC heeft primair de taak om vitale aanbieders en organisaties binnen de rijksoverheid bij te staan bij digitale dreigingen en incidenten én deze organisaties hierover te waarschuwen, informeren en te adviseren. Publieke en private partijen werken op dit gebied nauw samen.

5
Bent u het eens met de stelling dat naast fysieke maatregelen ter beveiliging van de gasinfrastructuur, ook het versterken van de cyberveiligheid van essentieel belang is, mede in het licht van het onder vraag 2 genoemde bericht?

Antwoord
Ja.

6
Is in het overleg met betrokken overheidsinstanties, zoals aangekondigd in uw brief 4 november 2022 (Kamerstuk 30821, nr. 168), zowel gesproken over de infrastructuur op zee als de infrastructuur op land?

[3] Aanwijzen van aanbieders essentiële diensten in de gas- en oliesector ter bevordering van de digitale veiligheid | Tweede Kamer der Staten-Generaal

Antwoord
Ja.

7
Wat is het resultaat van dit overleg en vindt dit overleg nog steeds plaats?

Antwoord
Dit overleg vindt doorlopend plaats. Op de korte termijn is gewerkt aan het beeld van de risico's op sabotage en spionage bij vitale infrastructuur op zee en welke maatregelen er direct kunnen worden genomen. TNO doet onderzoek naar de kwetsbaarheden en mogelijke weerbaarheidsmaatregelen van data- en energie-infrastructuur op zee. Voor de lange termijn werkt het kabinet, in het kader van de motie van het lid Boswijk c.s., aan een verkenning voor een gezamenlijke strategie ter bescherming van de cruciale infrastructuur op de Noordzee. Uw Kamer is hierover in november 2022 geïnformeerd in de Kamerbrief "Toezegging inzake toezending Kamerbrief over sabotage van Nord Stream 1 en 2" (Kamerstuk 30821, nr. 168). In deze verkenning worden dreigingen en mogelijke aanvullende maatregelen die noodzakelijk zijn om de weerbaarheid te vergroten meegenomen, onder meer tegen statelijke actoren.

8
Zijn bij dit overleg ook actief overheidsorganisaties betrokken die verantwoordelijk zijn voor de cyberweerbaarheid zoals het Nationaal Cyber Security Center (NCSC)?

Antwoord
Ja, het NCSC is bij dit overleg betrokken geweest.

9
Kunt u garanderen dat (acute) signalen over fysieke sabotage of een cyberaanval direct gedeeld kunnen worden met de juiste instanties om snel maatregelen te kunnen nemen?

Antwoord
Betrokken instanties hebben zowel regulier als incidenteel contact met vitale sectoren en delen hierbij relevante signalen en informatie uit over (acute) dreigingen, weerbaarheid en maatregelen. Er wordt continu gekeken of en welke beveiligingsmaatregelen nodig zijn en, afhankelijk van de ingeschatte dreiging, hoe deze maatregelen kunnen worden geïmplementeerd. Binnen de overheid vindt hierover nauwe samenwerking plaats tussen de verschillende departementen, de inlichtingen- en veiligheidsdiensten, NCSC en Nationale Politie.

Op het moment dat het NCSC concrete signalen van betrokken AED's of andere partijen ontvangt over een (dreigende) cyberaanval, informeert en adviseert het NCSC relevante partijen zo snel mogelijk en, in het geval van een daadwerkelijk cyberincident, staat het NCSC de organisatie bij en ondersteunt zij waar nodig de organisatie bij het treffen van maatregelen om de continuïteit van de dienst te waarborgen of te herstellen.

10
Hoe ziet u de rol van de overheid bij het beschermen van de gasinfrastructuur? Neemt de overheid ook zelf actief maatregelen om de veiligheid van infrastructuur te vergroten, naast het ondersteunen van vitale aanbieders?

Antwoord
Zie voor de beantwoording van vraag 10 de beantwoording onder vraag 3 en 4

11
Kunt u aangeven of er een noodplan klaarligt mocht bepaalde energie-infrastructuur worden gesaboteerd of worden aangetast en hierdoor de leveringszekerheid in het geding komt?

Antwoord
Voor gas is er het Bescherm -en Herstelplan Gas (BH-G). Dit plan kan worden ingeschakeld op het moment dat er een tekort aan gas ontstaat of dreigt te ontstaan. Op 9 december heb ik uw Kamer per brief geïnformeerd over de situatie met betrekking tot gasleveringszekerheid en de ontwikkelingen rond het BH-G (Kamerstuk 29023, nr. 384).

In geval van crisis bij energie-infrastructuur, bijvoorbeeld veroorzaakt door sabotage, is er een Nationaal Crisis Plan (NCP) Gas en NCP Elektriciteit. Deze NCP's beschrijven de crisisaanpak- en structuren en worden tweejaarlijks aangepast op basis van een actuele risicoanalyse. Daarnaast hebben netbeheerders van gasinfrastructuur ook hun eigen calamiteiten plannen.

De hierboven genoemde crisisplannen zijn specifieke uitwerkingen van de generieke crisisaanpak zoals beschreven in het Instellingsbesluit Ministeriële Commissie Crisisbeheersing 2022 en het Nationaal Handboek Crisisbeheersing. Beide zijn op 6 december 2022 met uw Kamer gedeeld (Kamerstuk 29517, nr. 225).

12
Kunt u bevestigen dat alle mogelijke maatregelen worden genomen voor de bescherming van kwetsbare (gas)installaties tegen acties door vijandige (statelijke)actoren?

Antwoord
Het kabinet draagt zorg voor het beschermen en bevorderen van de nationale veiligheid, dus ook voor kwetsbare (gas)installaties, welke bij een vijandige actie kunnen leiden tot een ontwrichting van de maatschappij. Er wordt risicogebaseerd maatregelen genomen. Dit betekent dat voor het grootste risico de zwaarste maatregelen worden genomen.