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

3846

Vragen van de leden **Rajkowski** en **Erkens** (beiden VVD) aan de Ministers van Justitie en Veiligheid en voor Klimaat en Energie over *het artikel «Hacker ontdekt dat Chinese zonnepanelen een bedreiging zijn voor ons stroomnet»* (ingezonden 26 juli 2022).

Antwoord van Minister **Jetten** (Klimaat en Energie), mede namens de Minister van Justitie en Veiligheid (ontvangen 2 september 2022).

Vraag 1
Bent u bekend met dit artikel?[1]

Antwoord 1
Ja.

Vraag 2
Bent u bekend met het feit dat 43% van de Nederlanders zich zorgen maakt om de uitval van vitale processen, zoals onderzocht door de Nationaal Coordinator Terrorismebestrijding en Veiligheid (NCTV)? Hoe beoordeelt u dit? Welke mogelijkheden ziet u met deze zorgen aan de slag te gaan?[2]

Antwoord 2
Ja. Uit de Risico-en crisisbarometer voorjaar 2022[3], uitgevoerd in opdracht van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) blijkt dat Nederlanders zich zorgen maken om cyberdreigingen (47%), geopolitieke dreigingen (45%) en uitval van vitale processen(43%). Het kabinet onderkent deze zorgen. Zoals ook blijkt uit het Dreigingsbeeld Statelijke Actoren 2021[4] (DBSA) en het Cybersecurity Beeld Nederland 2022[5] (CSBN) zijn vitale processen doelwit van statelijke actoren en digitale aanvallen. Om die reden heeft het Kabinet in 2021 de versterkte aanpak ter bescherming van de vitale infrastructuur aangekondigd en werkt het kabinet

[1] https://www.ftm.nl/artikelen/hack-chinese-zonnepanelen-bedreiging-stroomnet
[2] https://www.nctv.nl/actueel/nieuws/2022/07/19/grootste-zorgen-over-cyber-geopolitieke-dreigingen-en-uitval-vitale-processen
[3] Risico- en crisis barometer voorjaar 2022, I&O research
[4] Kamerstuk 30 821, nr. 125
[5] Cybersecuritybeeld Nederland CSBN 2022

ah-tk-20212022-3846
ISSN 0921 - 7398
's-Gravenhage 2022

aan het tegengaan van statelijke dreigingen. In de Kamerbrief Voortgang Aanpak Statelijke Dreigingen[6] uit 2021 bent u hierover geïnformeerd.
Met de versterkte aanpak wordt ingezet op het verbeteren van de bescherming van de Nederlandse vitale infrastructuur door het vitaal beleid, het vitaalstelsel en de wetgeving tegen het licht te houden en waar nodig te herzien. Daarnaast wordt ook vanuit de Europese Unie sinds 2020 gewerkt aan de Critical Entities Resilience Directive (CER) en de Network- and Information Security 2 Directive (NIS2). Beide richtlijnen gaan Nederland helpen te komen tot een verbeterde bescherming van de vitale infrastructuur om via wetgeving te borgen dat vitale aanbieders passende maatregelen nemen tegen risico's die de continuïteit, integriteit of vertrouwelijkheid van hun vitale proces kunnen schaden. Om die reden wordt de toekomstige implementatie van beide richtlijnen binnen de versterkte aanpak voorbereid en betrokken bij het verbeteren van de bescherming van de Nederlandse vitale infrastructuur.

Vraag 3 en 4
Hoe beoordeelt u het gevaar voor ons stroomnet zoals in het artikel omschreven?
Hoe beoordeelt u het feit dat China, of andere kwaadwillenden die het systeem kunnen (binnendringen en) beheersen, op deze manier digitale ontwrichting in gang zou kunnen zetten?

Antwoord 3 en 4
Zoals ook blijkt uit het CSBN nemen de risico's op digitale incidenten toe door de toegenomen digitalisering en de opkomst van het Internet of Things (IoT).[7] Dit wordt versterkt doordat statelijke actoren zeer actief zijn in het digitale domein. Deze statelijke actoren gebruiken het digitale domein in toenemende mate bij het behartigen van hun geopolitieke belangen.
De beschreven casus maakt daarnaast duidelijk dat dit soort IoT apparatuur aan hogere veiligheidsnormen moet voldoen met het oog op de nationale veiligheid.
Het kabinet zet zich in om te voorkomen dat deze risico's een bedreiging vormen voor de continuïteit, integriteit en vertrouwelijkheid van de Nederlandse vitale processen, waaronder het landelijke transport, distributie en productie van energie. Om die reden zijn vitale aanbieders op basis van wetgeving, waaronder de Wet bescherming netwerk- en informatiesystemen (Wbni), verplicht tot het treffen van passende maatregelen ter beveiliging van hun netwerk- en informatiesystemen (zorgplicht) en worden zij geacht om inzicht te hebben in de risico's die hun dienstverlening kunnen raken.
In dat kader heeft de Minister van Economische Zaken en Klimaat ondernemingen in deze sector aangewezen als zogenaamde Aanbieders van Essentiele Diensten (AEDs), onder de Wet beveiliging netwerk- en informatiesystemen (Wbni). Het Agentschap Telecom (AT) houdt toezicht op deze aanbieders. Incidenten met aanzienlijke gevolgen voor de dienstverlening, moeten gemeld worden bij AT en het Nationaal Cyber Security Centrum (NCSC). Ook kunnen deze AEDs andere vrijwillige meldingen doen bij het AT en het NCSC. Het NCSC heeft als primaire taak om vitale aanbieders en Rijksoverheidsorganisaties in geval van dreigingen en incidenten met betrekking tot hun netwerk- en informatiesystemen te informeren, adviseren en indien nodig bijstand te verlenen.
Daarnaast wordt er in Europees verband nu gewerkt aan een Europese, gedelegeerde verordening over cybersecurity in de elektriciteitssector (Netcode on Cybersecurity). Dit is specifieke Europese regelgeving waarin bindende voorschriften voor cybersecurity worden opgelegd aan entiteiten die, wanneer zij mikpunt zouden worden van een cyberaanval, een risico vormen voor de stabiliteit van het Europese elektriciteitsnet. Op de naleving van deze verplichtingen zal toezicht worden gehouden, door onder andere het AT en de Autoriteit Consument en Markt. Onder deze Netcode kunnen ook entiteiten vallen die omvormers op grote schaal op afstand aansturen, ook wanneer zij zich niet op Europees grondgebied bevinden.

---

[6] Kamerstuk 30 821, nr. 125
[7] Kamerstuk 26 643, nr. 891

Vraag 5
Bent u het ermee eens dat dit een gevaar is voor onze nationale veiligheid?

Antwoord 5
De beschreven casus maakt duidelijk dat IoT apparatuur aan hoge veiligheidsnormen moet voldoen met het oog op onze nationale veiligheid. De antwoorden op vraag 3,4, 6 en 7 gaan in op de wijze waarop veiligheidsrisico's worden gemitigeerd.

Vraag 6 en 7
Wat wordt gedaan de risico's op korte termijn te beperken? In hoeverre zijn software- of hardwarematige aanpassingen een oplossing?
Wat wordt gedaan deze veiligheidsrisico's in de toekomst te voorkomen?

Antwoord 6 en 7
IoT Apparaten
Internet of Things-apparaten, zoals de omvormers van zonnepanelen die beschreven zijn in het artikel, kunnen een risico vormen voor het elektriciteitsnet als deze slecht beveiligd en grootschalig aan te sturen zijn. Deze omvormers zijn nodig om het elektriciteitssysteem effectief te laten werken. Alle netbeheerders hebben op grond van Elektriciteitswet 1998 de verplichting de veiligheid en betrouwbaarheid van de netten en het transport van elektriciteit over de netten op de meest doelmatige wijze te waarborgen, echter kunnen netbeheerders apparaten achter de elektriciteitsmeter niet zonder meer weren van het elektriciteitsnet. Netbeheerders sluiten huizen, bedrijfspanden en andere onroerende zaken aan op hun elektriciteitsnet, maar kunnen niet zien of toezicht houden op het type apparaten dat binnen een huis of bedrijfspand op een stopcontact zit. Netbeheerders treffen om die reden voorbereidingen voor een eventuele, grootschalige inzet van IoT-apparaten in een cyberaanval, maar kunnen niet voorkomen dat apparaten met dergelijke veiligheidsrisico's worden aangeschaft en in gebruikt worden genomen binnen een woning of bedrijfspand. Dit betekent dat er eveneens een belangrijke verantwoordelijkheid ligt bij leveranciers en fabrikanten van apparatuur om risico's voor het elektriciteitsnet te verkleinen (hieronder worden de wettelijke trajecten die gaan gelden voor fabrikanten en leveranciers verder toegelicht).
Om risico's van deze apparaten te mitigeren, wordt er ingezet op preventie, awareness en aanvullend wetgeving die producten softwarematig maar ook hardwarematig weerbaarder maakt tegen digitale aanvallen en mogelijk misbruik.
In dat kader wordt er op dit moment gewerkt aan verschillende trajecten van Europese wet- en regelgevingen om veiligheidsrisico's te mitigeren. Onder de *Radio Equipement Directive (RED)* zijn cybersecurityeisen als markttoegangseisen voor draadloos verbonden apparaten aangenomen. Omvormers vallen ook onder de scope van de RED. 1 augustus 2024 moeten draadloos verbonden apparaten die de Europese markt op komen voldoen aan deze cybersecurityeisen. Apparaten die niet aan de eisen voldoen kunnen vanaf dat moment door AT van de markt worden geweerd en gehaald. In voorbereiding op het van kracht worden van de cybersecurityeisen onder de RED heeft AT naar aanleiding van deze casus een onderzoek ingesteld naar omvormers. Het AT zal het gesprek aan gaan met de desbetreffende fabrikanten hoe verbeteringen van de cybersecurity gerealiseerd kunnen worden.
Daarnaast wordt in het najaar een Europees wetsvoorstel van de Europese Commissie verwacht voor horizontale regulering voor de cybersecurity van ICT-producten en diensten, de *Cyber Resilience Act*. Nederland zet bij de *Cyber Resilience Act* in op een zorgplicht voor fabrikanten en leveranciers van alle ICT-producten en diensten in de hele productlevenscyclus. Hiervoor is een non-paper opgesteld en aangeboden aan uw Kamer op 14 december 2021.[8] De Markttoezichtverordening (EU) 2019/1020 is van toepassing op de RED (EU) 2014/53. Deze verordening bevat regels en procedures voor marktdeelnemers betreffende producten die onder bepaalde harmonisatiewetgeving van de Unie vallen. Relevant is dat producten die binnen het toepassingsgebied van de RED vallen alleen in de handel mogen worden

[8] Kamerstuk 21 501-33, nr. 900

gebracht als er in de Unie een marktdeelnemer is die onder andere (technische) informatie kan verstrekken aan markttoezichtautoriteiten over het product en medewerking kan verlenen aan corrigerende maatregelen.
Als gevolg van de herziening van de NIS2 zullen meer bedrijven dan op nu in o.a. de energiesector in de toekomst moeten voldoen aan wettelijke verplichtingen voor cybersecurity. Deze verplichtingen bestaan uit een meldplicht voor incidenten en een zorgplicht om risico's voor de continuïteit van de dienstverlening te beperken. Hierbij dient ook rekening gehouden te worden met risico's die afkomstig zijn van leveranciers. Daarnaast zal de eerder genoemde Netcode on Cybersecurity tevens zorgen voor hogere cybersecurity eisen aan o.a. grootschalig aan te sturen omvormers.
Melden van kwetsbaarheden
Ten slotte wordt, om de veiligheid van informatiesystemen verder te verbeteren, aan de hand van de leidraad Coordinated Vulnerabilty Disclore (CVD) van het NCSC[9] het melden van kwetsbaarheden in software gestimuleerd. Eigenaren van ICT-systemen kunnen op deze manier kwetsbaarheden verhelpen vóórdat deze actief misbruikt kunnen worden. Indien het gaat om een complexe kwetsbaarheid die meerdere partijen raakt of als de eigenaar of leverancier niet of onvoldoende reageert, kan het NCSC optreden als bemiddelaar.

Vraag 8
Wanneer ontvangt de Tweede Kamer het toegezegde onderzoek/scan naar afhankelijkheden van vitale Nederlandse processen van landen met een cyberoffensief?[10]

Antwoord 8
Op 5 april 2022 is de motie[11] van de leden Rajkowski en Van Weerdenburg aangenomen die het kabinet verzoekt een scan uit te voeren op de aanwezigheid van apparatuur of programmatuur van organisaties uit landen met een tegen Nederland gerichte offensieve cyberagenda in de vitale infrastructuur. Op dit moment wordt door het Ministerie van Justitie en Veiligheid, in samenwerking met de betrokken departementen, verkend op welke manier opvolging kan worden gegeven aan de motie. Uw Kamer wordt hierover zo spoedig mogelijk geïnformeerd.

Vraag 9
Bent u het ermee eens dat het zeer onwenselijk is dat Nederland voor haar vitale processen, zoals het stroomnet, deze mate van afhankelijkheid kent zoals in het artikel is omschreven? Zo nee, waarom niet? Zo ja, welke concrete stappen gaat u hiertoe nemen? Welk tijdspad heeft u hiervoor ogen?

Antwoord 9
Het kabinet is zich bewust van de risico's met betrekking tot strategische afhankelijkheden en verstoringen in vitale processen en deelt de zorgen ten aanzien van elke ongewenste inmenging van statelijke actoren. Zoals ook in het DBSA, kunnen vitale processen doelwit zijn van voorbereidingshandelingen voor of daadwerkelijke (digitale) verstoring of sabotage. Zoals ook gesteld in het DBSA beschreven, is een toenemende afhankelijkheid van buitenlandse technologie een gegeven, aangezien geen land beschikt over alle kennis en productiemiddelen om technologisch onafhankelijk te opereren. De inzet van het kabinet is daarom om risico's op ongewenste strategische afhankelijkheden te mitigeren en tegelijkertijd het open investeringsklimaat van Nederland te beschermen. Daarnaast wordt, zoals ook gesteld in het antwoord op vraag 2, gewerkt aan een versterkte aanpak voor de bescherming van de vitale infrastructuur. Met een geactualiseerd instrumentarium worden onder andere technologische ontwikkelingen en geopolitieke veranderingen integraal meegewogen in het beoordelen van risico's en vervolgens bij het nemen van gepaste en proportionele weerbaarheidsverhogende maatregelen. Hierbij worden ook de (intersectorale) afhankelijkheden

[9] https://www.ncsc.nl/binaries/ncsc/documenten/publicaties/2019/mei/01/cvd-leidraad/CoordinatedVulnerabilityDisclosure.pdf
[10] (Kamerstuk 26 643, nr. 830)
[11] Kamerstuk 26 643, nr. 830

van vitale processen, specifieke grondstoffen of andere randvoorwaarden meegenomen.

Vraag 10
Werkt u ook aan het voorkomen van afhankelijkheden in onze energievoorziening die ontstaan door de optelsom van veel kleine en vaak decentrale afhankelijkheden, naast het al plaatsvinden van een versterking van het toezicht op de aanbestedingen van Tennet op en aan het hoogspanningsnet.

Antwoord 10
Ik ben mij bewust van de risico's die gepaard gaan met deze twee ontwikkelingen. De specifieke risico's voor de energievoorziening van veel kleine en decentrale eenheden manifesteren zich met name, wanneer deze gezamenlijk en gecoördineerd in worden gezet in het kader van een cyberaanval. Ik verwijs u terug naar de antwoorden op vraag 3,4, 6 en 7 voor een uiteenzetting van de instrumenten en maatregelen gericht op het voorkomen van dergelijke risico's.
Zoals eerder beschreven hebben netbeheerders een algemene taak om hun netten te beschermen, op grond van Europese regels en zoals vereist in de Elektriciteitsnet 1998 en de Gaswet. Er is al een uitgebreid Europees pakket aan wet- en regelgeving dat invult hoe netbeheerders in algemene zin veiligheidsrisico's moeten voorkomen en hoe zij de gevolgen van incidenten moeten mitigeren of wegnemen.

Vraag 11
Ziet u ook risico's voor individuele huishoudens en bedrijven door deze afhankelijkheid ontstaan? Hoe mitigeert u deze risico's?

Antwoord 11
Digitale apparaten van individuele huishoudens en bedrijven kunnen in theorie gehackt worden, zeker wanneer deze aan het internet gekoppeld zijn. Dat geldt dus ook voor apparaten waarmee elektriciteit wordt opgewekt (of opgeslagen). De beste manier om zulke risico's te mitigeren is via cyberveiligheidseisen die aan apparaten worden gesteld. Afronding en implementatie van de eerder genoemde *Radio Equipment Directive (RED) en Cyber Resilience Act (CRA)* zullen ervoor zorgen dat ook de digitale veiligheid van IOT apparaten van individuele huishoudens en bedrijven verhoogd wordt. De Netcode on Cybersecurity zal daarnaast voorzien in aanvullende cybersecurity eisen voor de elektriciteitssector.

Vraag 12 en 13
Zijn er andere energiebronnen waarvoor Nederland afhankelijk is van de Chinese techniek waar u soortgelijke risico's ziet? Hoe gaat u deze risico's mitigeren?
Lopen er op dit moment aanbestedingen, of worden er binnenkort aanbestedingen gestart, binnen de vitale sector die de afhankelijkheid van Nederland van landen met een offensieve cyberstrategie op onwenselijke wijze zal vergroten?

Antwoord 12 en 13
Het Rijk heeft niet inzichtelijk in hoeverre welke energiebronnen precies allemaal afhankelijk zijn van Chinese techniek en daarbij is er geen overzicht over alle lopende en aankomende aanbestedingen bij vitale aanbieders.
Wel biedt het Rijk ondersteuning en begeleiding op aanvraag aan vitale aanbieders wanneer zij te maken hebben met een (mogelijk) risicovolle aanbesteding. Hiervoor is instrumentarium ontwikkeld dat organisaties handvatten biedt bij het maken van een risicoanalyse en het nemen van mitigerende maatregelen. Het instrumentarium is ter beschikking gesteld binnen de rijksoverheid en medeoverheden, alsmede aan organisaties die onderdeel zijn van de vitale processen. Behoeftestellende partijen zijn zelf verantwoordelijk voor de toepassing van dit instrumentarium en het meewegen van nationale veiligheidsrisico's. Het Rijk kan daarbij ondersteuning bieden.
Met betrekking tot het digitaal veiliger maken van Internet of Things apparatuur, is eerder benoemd welke wetgeving in Europees verband van toepassing is.

Ook bij andere energiebronnen dan elektriciteit maakt internationale handel ons in zekere mate afhankelijk van andere landen. In EU-verband zetten we in op het vergroten van onze veerkracht en op strategische autonomie, onder meer door het diversifiëren en versterken van wereldwijde toeleveringsketens van kritieke grondstoffen[12].
De handvatten voor bedrijven zijn onder anderen de Elektriciteitswet 1998 en Gaswet voor netbeheerders, waarin zij een wettelijke taak hebben hun netten te beschermen tegen invloeden van buitenaf. Er is in 2020 door het kabinet, in het licht van de invulling van de eigen vermogensbehoefte van TenneT Duitsland, een nationale veiligheidsanalyse uitgevoerd. Dit heeft geresulteerd in een aantal aanbevelingen tot wijziging van de Elektriciteitswet 1998. De Kamer is hierover geïnformeerd op 19 mei 2021[13].
Daarnaast is recent de Wet Veiligheidstoets Investeringen, Fusies en Overnames (Vifo) aangenomen. Deze wet voorziet in instrumenten om risico's voor de nationale veiligheid als gevolg van investeringen, fusies en overnames te mitigeren. Met deze wet kunnen zeggenschapswijzigingen in bepaalde bedrijven ex-ante worden getoetst, waarna eventueel mitigerende maatregelen kunnen worden opgelegd en in het uiterste geval transacties kunnen worden geblokkeerd. De Wet Vifo is van toepassing op vitale aanbieders die buiten bestaande sectorale investeringstoetsen vallen, zoals Elektriciteitswet, de Gaswet en de Telecommunicatiewet, alsmede op beheerders van bedrijfscampussen en ondernemingen actief op het gebied van sensitieve technologie. Gezien de ontwikkelingen in de energiesector zijn er een aantal energie-gerelateerde processen meegenomen in de deze wet. Dit zijn aanbieders van de volgende diensten: warmtetransport, gasopslag, kernenergie en winbare energie. De Wet Vifo treedt naar verwachting begin 2023 in werking zodra de benodigde lagere regelgeving bij de Wet Vifo gereed is.
Tot slot zijn er in de nieuwe Energiewet die deze zomer ter advisering aan de Raad van State is aangeboden, extra mogelijkheden gecreëerd zoals het kunnen toepassen van de Aanbestedingswet op Defensie- en Veiligheidsgebied (ADV).
De ADV heeft voorrang op de Aanbestedingswet (Aw) 2012 voor opdrachten die onder het toepassingsbereik van de ADV vallen. De ADV biedt meer mogelijkheden voor het nemen van risico mitigerende maatregelen dan de Aw 2012 in geval van risico's voor de nationale veiligheid en de bescherming van vitale processen in het bijzonder.

Vraag 14
Bent u het ermee eens dat bij aanbestedingen van vitale Nederlandse processen voorkomen moet worden dat landen met een offensief cyberstrategie deze mate van invloed krijgen vanwege de enorme veiligheidsrisico's en de kans op mogelijke digitale ontwrichting? Zo ja, welke mogelijkheden ziet u deze afhankelijkheid van deze landen te verminderen om ons land veiliger te maken? Zo nee, waarom niet?

Antwoord 14
Eind 2018 is een verscherpt inkoop- en aanbestedingsbeleid geïmplementeerd voor de rijksoverheid. Voor aanbestedingen geldt dat nationale veiligheidsoverwegingen worden meegewogen bij de inkoop en aanbesteding van producten en diensten. Bij de aanschaf van gevoelige apparatuur zal volgens dit beleid bij aanschaf en implementatie rekening gehouden worden met zowel eventuele risico's in relatie tot de leverancier, als met het concrete gebruik van de systemen, bijvoorbeeld waar het gaat om de toegang tot systemen door derden. Zoals wordt genoemd in antwoord op vraag 12 en 13 is ter ondersteuning van dit beleid een instrumentarium ontwikkeld dat organisaties handvatten biedt bij het maken van een risicoanalyse en het nemen van mitigerende maatregelen.

[12] Kamerstuk 22 112, nr. 2936
[13] Kamerstuk 28 165, nr. 325