Ministerie van Economische Zaken
en Klimaat

> Retouradres Postbus 20401 2500 EK Den Haag

De Voorzitter van de Tweede Kamer
der Staten-Generaal
Binnenhof 4
2513 AA DEN HAAG

Directoraat-generaal Energie, Telecom & Mededinging
Directie Energiemarkt en Innovatie

Bezoekadres
Bezuidenhoutseweg 73
2594 AC Den Haag

Postadres
Postbus 20401
2500 EK Den Haag

Overheidsidentificatienr
00000001003214369000

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

Datum 22 januari 2018
Betreft Toezegging digitalisering infrastructuur en cybersecurity elektriciteitssector

Ons kenmerk
DGETM-EI / 17207474

Uw kenmerk
2017Z11667

Geachte Voorzitter,

In de Regeling van Werkzaamheden van 7 september jl. is gevraagd om een brief naar aanleiding van het rapport 'Mobiliteit en elektriciteit in het digitale tijdperk' van het Planbureau voor de Leefomgeving (PBL).
In deze brief geef ik mede namens mijn collega van Justitie en Veiligheid een schriftelijke reactie op het rapport en informeer ik u over de invulling van de toezegging gedaan tijdens het 30-ledendebat over bovengenoemd rapport van 4 oktober jl. om de gevolgen van digitalisering voor de elektriciteitssector te onderzoeken en u over de resultaten te informeren.

Digitalisering biedt volop kansen voor het oplossen van maatschappelijke uitdagingen zoals de transitie naar duurzame energie. Om deze kansen te kunnen pakken is versterking van cybersecurity in onze vitale infrastructuur een essentiële randvoorwaarde. Daartoe zal ik in de komende periode de onderstaande acties inzetten en u informeren bij relevante ontwikkelingen.

Mobiliteit en elektriciteit in het digitale tijdperk
Het rapport 'Mobiliteit en Elektriciteit in het digitale tijdperk; publieke waarden onder spanning' beoogt een opkomend maatschappelijk vraagstuk te signaleren en agenderen. Het rapport constateert terecht dat digitalisering van infrastructuur en daarmee verbonden dienstverlening grote voordelen heeft. Als keerzijde stelt het dat publieke waarden als toegankelijkheid, leveringszekerheid, privacy en democratische controle onder druk komen te staan, omdat door toenemende complexiteit systemen minder begrijpelijk en daarmee minder controleerbaar worden.

Het rapport vormde voor uw Kamer aanleiding om te stellen dat onze vitale infrastructuur steeds kwetsbaarder wordt voor digitale aanvallen, en aandacht te vragen voor het belang van cybersecurity in de energiesector. Het PBL gaat in haar rapport echter niet direct in op cybersecurity, maar richt zich op het borgen van publieke waarden en biedt handvatten daartoe. Ik herken de door het PBL gesignaleerde ontwikkelingen, met name waar het gaat om toenemende complexiteiten en afhankelijkheden in de energievoorziening. Op basis van dit rapport valt daarmee niet te stellen dat de cybersecurity van de vitale

Directoraat-generaal Energie, Telecom & Mededinging
Directie Energiemarkt en Innovatie

infrastructuur niet op orde is. Wel deel ik met uw Kamer de constatering dat cybersecurity van toenemend belang is voor de leveringszekerheid

De gevolgen van digitalisering voor de elektriciteitssector
Om invulling te geven aan de toezegging heeft het Ministerie van Economische Zaken en Klimaat gesprekken gevoerd met stakeholders uit de elektriciteitssector, waaronder netbeheerders, energieleveranciers en producenten van elektriciteit. Alle betrokkenen erkennen dat de elektriciteitssector onder invloed van digitalisering en de transitie naar een duurzame energievoorziening snel verandert. Daarbij worden digitalisering en flexibilisering unaniem gezien als een van de bouwstenen van een betaalbare, betrouwbare en duurzame elektriciteitsvoorziening. Tegelijkertijd stellen deze ontwikkelingen de sector ook voor nieuwe uitdagingen, waaronder toenemende complexiteit van systemen en afhankelijkheden tussen voorheen autonome systemen en sectoren.

Als gevolg van het stijgende aandeel hernieuwbare energie, het streven naar het dalende gebruik van aardgas en het toenemende gebruik van elektrisch vervoer zal het elektriciteitsverbruik naar verwachting sterk stijgen. De energietransitie vraagt daarom om meer flexibiliteit in het systeem om de betrouwbaarheid en betaalbaarheid van de Nederlandse elektriciteitsvoorziening op peil te houden. Op dit moment vinden al pilots plaats met vraag- en aanbodsturing, waardoor bijvoorbeeld elektrische auto's laden op het moment dat veel duurzame energie beschikbaar is. De elektriciteitsvoorziening ontwikkelt zich daarmee van een vraag-gestuurd naar een aanbod-gestuurd systeem. Wanneer dergelijke oplossingen grootschalig worden uitgerold zal de leveringszekerheid van elektriciteit mede afhankelijk worden van de robuustheid en cyberveiligheid van de daarvoor noodzakelijke digitale diensten, externe partijen en de onderliggende energie- en ICT-infrastructuur. Daarmee is aandacht voor cybersecurity binnen de elektriciteitsvoorziening van nu en die van de toekomst van groot belang.

Borgen van leveringszekerheid
Op dit moment is de leveringszekerheid geborgd door de Elektriciteitswet 1998, waarbij de verantwoordelijkheid voor de leveringszekerheid primair is belegd bij de netbeheerder. Gezien bovenstaande ontwikkelingen zal ik in de komende periode nader verkennen welke waarborgen noodzakelijk zijn om de leveringszekerheid van elektriciteit ook in de toekomst op peil te houden. Daartoe zal ik onderzoeken welke lessen wij kunnen leren van onze buurlanden in Noordwest Europa waar het gaat om het borgen van de veiligheid van vitale infrastructuur in het kader van digitalisering.

De netbeheerders zijn naast de verplichtingen in de Elektriciteitswet 1998 aangemerkt als vitale partijen in het kader van het programma Vitaal van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). Uw Kamer wordt door de minister van Justitie en Veiligheid periodiek over de voortgang geïnformeerd (zie bijvoorbeeld Kamerstuk 29 517, nr. 136). De vitale aanbieders behoren op grond van de Wet Gegevensverwerking en Meldplicht Cybersecurity (WGMC) tot de partijen waar het Nationaal Cyber Security Centrum (NCSC) zich

Directoraat-generaal Energie, Telecom & Mededinging
Directie Energiemarkt en Innovatie

Ons kenmerk
DGETM-EI / 17207474

op richt vanuit zijn taak als Computer Emergency Response Team (CERT) voor de Rijksoverheid en de vitale infrastructuur.

In het debat van 4 oktober is herhaaldelijk verwezen naar de implementatie van de Richtlijn Netwerk- en Informatiebeveiliging (EU 2016/1148 Het wetsvoorstel Cybersecuritywet ter implementatie van deze richtlijn is d.d. 4 januari jl. door de Raad van State van advies voorzien en zal zo spoedig mogelijk aan uw Kamer worden aangeboden. Doel van de Richtlijn is om de Europese samenwerking en paraatheid bij ICT-incidenten te verbeteren en om de veerkracht van netwerk- en informatiesystemen van vitale diensten te versterken. De aanbieders van zogeheten "essentiële diensten" krijgen een meldplicht van ICT-incidenten en een zorgplicht die verplicht tot het treffen van maatregelen met betrekking tot de beveiliging van hun netwerk- en informatiesystemen.
Gezien de ontwikkelingen op het gebied van digitalisering zal parallel met de implementatie van de cybersecuritywet voor de energiesector worden heroverwogen welke partijen tot de vitale infrastructuur behoren.
Hierbij zal ik opnieuw beoordelen of naast de huidige vitale aanbieders ook partijen zoals producenten, leveranciers of aanbieders van bepaalde diensten kunnen worden geïdentificeerd die gezien hun belang voor de sector als vitale aanbieder kunnen worden aangemerkt.

Tot slot
Het belang van cybersecurity blijkt ook uit het regeerakkoord. De inzet op onderzoek, bewustwording en cyberweerbaarheid van de maatschappij zullen ook de vitale infrastructuur, waaronder de elektriciteitssector, mede ten goede komen. De hier ingezette acties dragen dan ook bij aan de cybersecurity agenda, en breder de digitaliseringsagenda, van het kabinet.

Eric Wiebes
Minister van Economische Zaken en Klimaat