

AH 3027

2026Z16508

Antwoord van minister Van Veldhoven-van der Meer (Klimaat en Groene Groei) (ontvangen 11 september 2026)

Zie ook Aanhangsel Handelingen, vergaderjaar 2025-2026, nr. 2615

1

Bent u bekend met het artikel "*Stroomnet kwetsbaar voor cyberaanval: 'Geen kwestie van óf, maar wanneer'?*"?

Antwoord

Ja.

2

Hoe beoordeelt u de waarschuwing van cybersecurity- en energiespecialisten dat de toenemende digitalisering van het elektriciteitssysteem, waaronder slimme netten, thuisbatterijen, zonnepanelen, laadpalen en andere verbonden apparaten, ook leidt tot een groter aanvalsoppervlak voor kwaadwillenden?

Antwoord

De ontwikkeling naar een meer decentrale energievoorziening maakt lokale opwek en opslag mogelijk en is onderdeel van een succesvolle energietransitie. Deze decentralisatie gaat gepaard met een digitaliseringsslag. Zo kunnen decentrale assets bijvoorbeeld op afstand een (beveiligings)update ontvangen of op afstand worden aangestuurd. Dit is onder meer noodzakelijk om de beveiliging van de assets up-to-date te houden en biedt kansen voor bijvoorbeeld een slimmer gebruik van het elektriciteitsnet. Naast deze voordelen brengt de digitalisering van het energiesysteem ook risico's met zich mee.

Digitale verbindingen maken de toegang tot deze assets op afstand makkelijker waardoor deze verbindingen een aanvalsoppervlak kunnen vormen voor kwaadwillenden om decentrale assets te manipuleren. Daarom gelden voor (consumenten)apparatuur cybersecurity eisen op basis van wet- en regelgeving zoals de Radio Equipment Directive 3.3 en de Cyber Resilience Act. Om de digitale weerbaarheid van het energiesysteem verder te verhogen en risico's te mitigeren, treft het kabinet daarnaast nog andere maatregelen. Deze maatregelen zijn toegelicht in de beantwoording van vraag 3.

3

In hoeverre wordt digitale weerbaarheid momenteel als randvoorwaarde meegenomen bij de uitvoering van de energietransitie en de uitbreiding van het elektriciteitsnet?

Antwoord

In het ontwerp van het energiesysteem houdt het kabinet rekening met digitale risico's. Zo worden cybersecurityeisen gesteld aan digitale systemen van energiepartijen en wordt kritieke (digitale) energie-infrastructuur geïdentificeerd en weerbaarder gemaakt. Een concreet voorbeeld is het meenemen van (digitale) weerbaarheid als voorwaarde bij de vergunningsverleningsinstrumenten van nieuwe windparken op zee. Hierbij zijn weerbaarheid en nationale veiligheidszorgen onderzocht en zijn vervolgens veiligheidsmaatregelen genomen, zoals het stellen van voorwaarden voor de herkomst van windmolenonderdelen op basis van de Europese Net Zero Industry Act (NZIA).¹

Ook voor bestaande energie-infrastructuur gelden strenge eisen en is er toezicht om de digitale weerbaarheid te verhogen. Met de inwerkingtreding van de Cyberbeveiligingswet (Cbw) op 15 augustus jl. is het bestaande wettelijke cybersecuritykader voor energie-infrastructuur versterkt en worden energiebedrijven verplicht om zorg te dragen voor de beveiliging van hun (digitale) systemen om hun bedrijfscontinuïteit te waarborgen. Aanvullend op de Cbw geldt de Netcode voor Cybersecurity Gedelegeerde Verordening (EU) 2024/1366 (NCCS) ter versterking van de digitale weerbaarheid van het Europese elektriciteitsnet om de veiligheid, continuïteit en betrouwbaarheid ervan te waarborgen. Onderdelen van de NCCS zijn al geïmplementeerd; de NCCS wordt volledig van kracht per 2028.

Het kabinet werkt doorlopend aan het verder versterken van de weerbaarheid van het energiesysteem. Zo is er in de actualisatie van het Nationaal Plan Energiesysteem (NPE) aandacht voor een (digitaal) weerbaar energiesysteem om de betrouwbaarheid en betaalbaarheid van energie te kunnen waarborgen. Het geactualiseerde NPE wordt met Prinsjesdag aan de Kamer verstuurd. Een verdere toelichting op de kansen en risico's van de digitalisering van het energiesysteem, inclusief een uitwerking van benodigde acties, is opgenomen in de Actieagenda Digitalisering Energiesysteem (ADE)².

4

Kunt u aangeven welke risicoanalyses zijn uitgevoerd naar de cybersecurity van decentrale energiebronnen, zoals thuisbatterijen, zonnepanelen, laadpalen en energiebeheersystemen, en welke conclusies daaruit zijn getrokken?

Antwoord

Het ministerie van EZK werkt samen met andere overheidsorganisaties, netbeheerders, energiebedrijven en onderzoeksinstituten om zoveel mogelijk kennis en inzichten te verzamelen over de risico's in het decentrale energiesysteem. Uit deze analyses komen kwetsbaarheden naar voren die worden vertaald naar beleid en wet- en regelgeving. Een voorbeeld is het rapport van Energy Innovation NL (in opdracht van de Rijksdienst voor Ondernemend Nederland)

¹ Kamerstuk 33561, nr. 103.

² Bijlage bij kamerstuknummer 29023, nr. 602.

over de cyberveiligheid van zonnepanelen.³ Een conclusie uit dit rapport is dat het verhogen van de digitale weerbaarheid van decentrale energie assets een gedeelde verantwoordelijkheid is van alle spelers in de keten waarbij samenwerking essentieel is. Om uitvoering te geven aan de wet- en regelgeving op digitale weerbaarheid, zoals toegelicht in de beantwoording op vraag 2 en 3, werkt het kabinet samen met verschillende energiebedrijven en brancheverenigingen. Daarnaast stimuleert het kabinet de ontwikkeling van sectorale Information Sharing and Analyses Centers (ISACs), zoals de ISAC voor de zonne-energiesector. Het doel van een ISAC is om de digitale weerbaarheid te vergroten binnen een sector via vertrouwelijke informatie-uitwisseling over dreigingen en incidenten en het delen van handelingsperspectief en gedeelde lessen. Daarnaast bevordert het kabinet samenwerkingsinitiatieven zoals het sectorpact 'Weerbaar Energiesysteem' van Energie Nederland en Netbeheer Nederland.

Het kabinet zet verschillende stappen om cybersecurity via wet- en regelgeving te versterken, zoals toegelicht in de beantwoording op vraag 3. Daarnaast voeren sectorpartijen zelf risicoanalyses uit en nemen zij indien nodig passende maatregelen om risico's te mitigeren. Zo worden bijvoorbeeld bij grote aanbestedingen door de netbeheerders risicoanalyses gemaakt en passende maatregelen genomen.⁴ De Cbw en NCCS verplichten bedrijven om een risicoanalyse uit te voeren en rekening te houden met risico's in hun toeleveringsketen en bij het verwerven, ontwikkelen of onderhouden van (digitale) producten en diensten in hun netwerk- en informatiesystemen.

5

Hoe beoordeelt u de stelling dat de Europese energie-infrastructuur steeds vaker doelwit is van cyberaanvallen? In hoeverre spelen achterstallige modernisering van systemen, verouderde technologie en tekortschietende basisbeveiliging daarbij een rol? Kunt u uw antwoord toelichten?

Antwoord

Zoals in het Cybersecurity Beeld Nederland 2025 is aangegeven, blijven alle vitale sectoren een aantrekkelijk doelwit voor kwaadwillende actoren. De digitalisering van het energiesysteem zorgt voor een nauwere verwevenheid tussen het digitale en fysieke energiesysteem. Zo wordt verouderde operationele technologie (OT) vaker gekoppeld aan slimme informatietechnologie (IT)-systemen. Het nemen van passende beheersmaatregelen om risico's van mogelijk verouderde OT te mitigeren, zoals netwerksegmentatie, wordt met de Cbw en NCCS wettelijk verankerd. Energiepartijen dienen op grond van de Cbw en NCCS in hun IT- en OT-architectuur rekening te houden met deze risico's en passende en evenredige maatregelen te nemen, ook voor de beveiliging van OT. De Rijksinspectie Digitale Infrastructuur (RDI) houdt toezicht op de energiesector vanuit deze verplichtingen in de Cbw en NCCS. Het National Cyber Security Center (NCSC) deelt daarnaast diverse kennis- en informatieproducten met de energiesector, onder meer vanuit samenwerking met Europese partners, over basisbeveiliging voor digitale weerbaarheid en over risicomanagement van verouderde OT-systemen.

³ Zie het rapport van Secura - Scenario's en maatregelen voor cyberweerbare zonnestroominstallaties.

⁴ Aanhangsel Handelingen II 2025/26, nr. 873.

6

Op welke wijze werken de ministeries van Klimaat en Groene Groei en Economische Zaken en Klimaat samen om ervoor te zorgen dat investeringen in de energietransitie gepaard gaan met investeringen in digitale veiligheid?

Antwoord

Investerings in de energietransitie gaan onlosmakelijk gepaard met investeringen in digitale veiligheid omdat slimme energienetten en hernieuwbare bronnen sterk afhankelijk zijn van digitale aansturing. Binnen het ministerie van EZK wordt het onderwerp van digitale weerbaarheid en energie (security) daarom integraal opgepakt.

7

Worden er regelmatig gezamenlijke crisisoefeningen gehouden waarbij zowel een fysieke verstoring van het elektriciteitsnet als een cyberaanval wordt gesimuleerd? Zo ja, welke lessen zijn daaruit getrokken? Zo nee, waarom niet?

Antwoord

Ja, op lokaal, regionaal, nationaal en Europees niveau vinden regelmatig crisisoefeningen over stroomuitval plaats. Het betreft wisselende scenario's, variërend van fysieke verstoringen, cyberaanvallen en een combinatie daarvan. Daarnaast wordt er deelgenomen aan PENTA⁵ oefeningen, waarbij de Europese verordening voor risicoparaatheid in de elektriciteitssector centraal staat. In het Nationaal Crisisplan Elektriciteit (NCP-E) zijn daarnaast afspraken gemaakt om regelmatig gezamenlijk of per organisatie te oefenen. De Algemene Rekenkamer heeft mede op basis van bovengenoemde crisisoefeningen recent geconstateerd dat het ministerie van EZK en TenneT goede maatregelen hebben getroffen om crises op het hoogspanningsnet te voorkomen en dat zij goed zijn voorbereid op mogelijke storingen.⁶

Een vast onderdeel van een crisisoefening is een evaluatie door de betrokken organisaties. Uit de evaluaties van de crisisoefeningen van de afgelopen jaren zijn verschillende lessen getrokken met betrekking tot de crisisstructuur en werkprocessen. Zo kwam bijvoorbeeld naar voren dat de rijksoverheid in crisissituaties beter kan afspreken welke informatie wanneer wordt gedeeld en dat sommige plannen te abstract zijn. Deze lessen worden meegenomen in de actualisatie van het Nationaal Crisisplan Elektriciteit (NCP-E) naar een Landelijk Crisisplan Elektriciteit, dat naar verwachting begin 2027 met de Kamer zal worden gedeeld.

8

Deelt u de opvatting dat een succesvolle energietransitie alleen mogelijk is wanneer burgers en bedrijven erop kunnen vertrouwen dat het energiesysteem digitaal veilig en weerbaar is? Zo ja, welke aanvullende stappen bent u bereid te zetten om dit vertrouwen te versterken?

⁵ Een regionaal energiesamenwerkingsverband tussen België, Nederland, Luxemburg, Frankrijk, Duitsland, Oostenrijk en Zwitserland.

⁶ Zie het rapport van de Algemene Rekenkamer - Resultaten verantwoordingsonderzoek 2025 Klimaat en Groene Groei en Klimaatfonds.

Antwoord

Ja, het kabinet deelt deze opvatting. Daarom werkt het kabinet aan het digitaal veilig en weerbaar houden van het energiesysteem, zoals beschreven in de beantwoording bij de vorige vragen. Aanvullend worden in opdracht van het ministerie van EZK Nederlandse Technische Afspraken (NTA's) ontwikkeld door het Nederlands Normalisatie Instituut (NEN) voor het slim en interoperabel maken van netintensieve apparaten. Dit voorziet dat laadpalen, zonne-omvormers, thuisbatterijen, warmtepompen en overkoepelend de Home Energy Management Systemen (HEMS) als aansturend systeem slim ingesteld kunnen worden en met elkaar kunnen communiceren. Deze afspraken worden opgesteld volgens Europese cybersecuritystandaarden, zodat eindgebruikers kunnen rekenen op een veilige aansturing.⁷

9

Welke gevolgen heeft de toenemende cyberveiligheidsopgave voor de huidige opgave rond de uitbreiding en verzwarend van het elektriciteitsnet? Worden aanvullende eisen aan digitale veiligheid meegenomen in de planning, uitvoering en kosten van deze uitbreidingen? Zo ja, op welke wijze? Zo nee, waarom niet?

Antwoord

Het is niet mogelijk om alle risico's volledig uit te sluiten. Tegen deze achtergrond zet het kabinet in op het zoveel mogelijk minimaliseren van risico's via een risico gebaseerde aanpak die de weerbaarheid effectief en efficiënt verhoogt. Dit betekent dat wordt gekeken naar de doelmatigheid, proportionaliteit en evenredigheid van maatregelen. Voor toekomstige energie-infrastructuur geldt dat maatregelen ten behoeve van (digitale) weerbaarheid het meest effectief en het meest kostenefficiënt zijn wanneer ze aan de voorkant van een traject worden geïmplementeerd. In het vormgeven van ruimtelijk beleid en het fysieke ontwerp van het energiesysteem wordt het aspect (digitale) weerbaarheid ook meegenomen. Binnen het fysieke ontwerp van het nationale energiesysteem gaat dit bijvoorbeeld om het wel of niet clusteren van energieproductielocaties en het wel of niet bundelen van energie-infrastructuur. De effecten van het fysieke ontwerp van het nationale energiesysteem op weerbaarheid zullen nader worden onderzocht, waarna keuzes zullen worden vastgelegd in het Programma Energiehoofdstructuur (PEH II). De hoofdlijnenbrief hierover zal begin 2027 naar de Tweede Kamer worden verzonden en het programma zal in 2028 worden vastgesteld.

10

Bent u bereid de Kamer vóór het einde van dit jaar te informeren over de samenhang tussen de voortgang van de energietransitie en de digitale weerbaarheid van de Nederlandse energie-infrastructuur?

Antwoord

Aankomende Prinsjesdag wordt de Tweede Kamer verder geïnformeerd over het toekomstige energiesysteem, onder andere middels het geactualiseerde NPE en de kabinetsreactie op het

⁷ Zie het rapport van Stichting Koninklijk Nederlands Normalisatie Instituut - De route naar interoperabiliteit en energieflexibiliteit: normontwikkeling voor slimme net-intensieve apparaten.

Energy Innovation NL rapport 'Autonoom en Veilig'. Hierin wordt de samenhang tussen de voortgang van de energietransitie en digitale weerbaarheid nader toegelicht.

11

Kunt u de vragen los van elkaar beantwoorden?

Antwoord

Ja.