Ministerie van Economische Zaken
en Klimaat

[redacted]

17/11/22

[redacted]
Directie Energiemarkt

Auteur
[redacted]

Aan de Minister voor Klimaat en Energie
[redacted]
CC de Staatssecretaris voor de Mijnbouw

TER BESLISSING
Datum
17 november 2022

Kenmerk
DGKE-DE / 22483938
Bhm: 22543582

WJZ bhm 22483872

Kopie aan

Bijlage(n)
1. Wijzigingsregeling
2. Nota Voornemen aanwijzen Aanbieders van Essentiële Diensten in de oliewaardeketen en gasmarkt
3. Kamerbrief wijziging Regeling en wijziging naam vitale processen energiesector

nota

Wijziging Regeling aanwijzing aanbieders essentiële diensten EZK in verband met de aanwijzing van dienstverleners in de energiesector en wijziging vitale processen in het energiedomein

Parafenroute

[redacted]

Aanleiding

Afgelopen april bent u geïnformeerd (zie bijlage 2) over de beoogde wijziging van de Regeling aanwijzing aanbieders van essentiële diensten EZK om Aanbieders van Essentiële Diensten (AED) in de energiesector (olie en gas) aan te wijzen. Inmiddels is de regeling uitgebreid geconsulteerd en ter advies voorgelegd aan het Adviescollege Toetsing Regeldruk (ATR) en voor een handhavingstoets aan Agentschap Telecom (AT).
U informeert de Tweede Kamer over de wijziging middels bijgevoegde Kamerbrief.

Geadviseerd besluit

1. MKE: U kunt akkoord gaan met de bijgevoegde regeling en de bijbehorende toelichting en beide stukken ondertekenen.
2. MKE: U kunt akkoord gaan met de Kamerbrief en ondertekenen.
3. MEZK, SMB: U kunt kennisnemen van de inhoud van de bijgevoegde regeling, bijbehorende toelichting en Kamerbrief.

Kernpunten

- De Kamerbrief wordt verstuurd nadat de regeling gepubliceerd is.
- Op grond van het Besluit beveiliging netwerk- en informatiesystemen (Bbni) bent u bevoegd om voor bepaalde diensten AED's in de energiesector aan te wijzen. Dit gebeurt via de Regeling aanwijzing aanbieders van essentiële diensten EZK (hierna: regeling).
- Door de aanwijzing valt de aangewezen groep aanbieders onder een cybersecurity meld- en zorgplicht op basis van de Wet beveiliging netwerk- en informatiesystemen (Wbni). Agentschap Telecom (AT) houdt namens u toezicht op deze bedrijven.

- Daarnaast hebben deze AED's recht op ondersteuning van het Nationaal Cyber Security Centrum (NCSC). Dit houdt bijvoorbeeld in dat zij dreigingsinformatie betreffende cybersecurity ontvangen van het NCSC .
- De bestaande regeling[1] wijst aanbieders van digitale infrastructuur aan als AED. In de toelichting bij die regeling is aangekondigd dat bepaalde mogelijke toekomstige processen in de energiesector tevens aangewezen kunnen worden in de genoemde regeling.
- U wijzigt deze regeling door een toevoeging van AED's in het energiedomein voor de diensten gasopslag, het vloeibaar maken van aardgas of de invoer, de verlading en de hervergassing van LNG, beheer van oliepijpleidingen, productie, opslag, transport, raffinage, en behandeling van olie.
- Met deze wijzigingsregeling worden ongeveer 20 entiteiten aangewezen als AED die onder deze categorieën vallen.
- U wijzigt deze regeling (i.p.v. MEZK), omdat u verantwoordelijk bent voor de vitale processen binnen de energiesector.
- Er zijn binnen de energiesector op grond van de Wbni eerder aanbieders aangewezen, bijvoorbeeld de netbeheerders en de NAM vallen al onder de cybersecurity meld- en zorglicht. Gezien het vitale belang van olie- en gaslevering en de grote effecten op de leveringszekerheid die gepaard gaan met een succesvolle cyberaanval, is het proportioneel om ook binnen de hierboven genoemde sectoren AED's aan te wijzen.
- De entiteiten binnen deze sectoren zijn via de brancheorganisaties geïnformeerd over de conceptregeling en hebben positief gereageerd. Vele partijen zien het nut en het belang van een aanwijzing.
- ATR heeft positief geadviseerd over het concept met wat kleine aandachtspunten betreffende verdere invulling van de zorgplicht met name wat betreft het gebruik van open normen. Dit punt is al vaker aangedragen door ATR, omdat dit mogelijk onduidelijkheden zou kunnen opleveren voor vitale aanbieders. Zo ziet het ATR het risico dat partijen onnodig veel beveiligingsmaatregelen gaan nemen. Omdat EZK en vooral AT open normen prefereren, is hier geen gehoor aan gegeven, maar verder onderbouwd waarom een open norm de voorkeur heeft. Dit is al eerder zo toegelicht en deze lijn is in de regeling aangehouden.
- Agentschap Telecom heeft de regeling als handhaafbaar beoordeeld.
- U heeft in Kamerbrief aandacht voor het vitaalbeleid van EZK. Het vitaal beleid staat los van cybersecurity beleid, maar wordt wel door elkaar gevoed. Cybersecurity spreekt over essentiële diensten. Het vitaal beleid spreekt over vitale processen. Partijen worden als vitaal vastgesteld voordat ze formeel als aanbieder van een essentiële dienst worden aangewezen.
- U wijzigt een aantal vitale processen om de nieuwe vitale partijen te includeren. Tevens wijzigt u de namen van de vitale processen om te bevestigen dat de infrastructuur (net op zee en kabels onder de windparken), op de Noordzee vitaal is.
- Deze regeling treedt in werking met ingang van 1 januari 2023, hetgeen in overeenstemming is met het beleid inzake vaste verandermomenten.

[1] Staatscourant 2021 nr. 22401

- Er wordt afgeweken van de minimale invoeringstermijn, omdat een spoedige inwerkingtreding van deze regeling aanmerkelijke ongewenste nadelen voor de doelgroep en de samenleving voorkomt. De vitaliteit van gas- en olie infrastructuur neemt toe. Sanctie maatregelen en incidenten laten zien dat de dreiging voor leveringszekerheid reëel is. De overheid dient in het fysieke veiligheid spectrum maar ook het digitale veiligheid spectrum de weerbaarheid te versterken.
- Deze afwijkingsmogelijkheid wordt geboden door aanwijzing 4.17, vijfde lid, onderdeel a, van de Aanwijzingen voor de regelgeving. Het is van belang dat de cyberweerbaarheid van genoemde bedrijven zo snel mogelijk wordt verbeterd.

Toelichting

- In 2021 is de Colonial pipeline in de VS buitenwerking gesteld door een cyber aanval(ransomware)[2]. [redacted] Energiebedrijven moeten adequate maatregelen nemen en daarop wordt toezicht gehouden wanneer zij zijn aangewezen als aanbieders van essentiële diensten.
- Reactie Agentschap Telecom in Bbni 2021[3] t.a.v. in deze nota genoemde aandachtspunt ATR:
  "Omdat deze zorgplicht van toepassing is op diverse sectoren met elk een eigen risicoprofiel van de beveiliging van netwerk- en informatiesystemen en daarbij passende veiligheidscultuur, normen en regulering, is gekozen voor een invulling die de benodigde ruimte laat aan de AED en de toezichthouder om tot een voor de sector passende invulling te komen, en die zo veel mogelijk ruimte laat om aan te sluiten bij bestaande en eventuele nieuwe normenkaders. De AED's zijn zelf primair verantwoordelijk voor het binnen genoemde wettelijke kaders voldoen aan de zorgplicht door het treffen van concrete maatregelen. De AED's zullen daarover steeds in contact staan met de toezichthouder. Deze invulling sluit aan bij zowel de gangbare normen op het gebied van informatiebeveiliging en continuïteit als bij de toezichtpraktijk van AT, zijnde systeemtoezicht op basis van open normen. Daarnaast biedt deze invulling haar als toezichthouder de ruimte om aan de voorkant proactief en preventief te interveniëren. Daar waar nodig wordt geacht, kan de minister die het aangaat besluiten om de zorgplicht voor een of meerdere sectoren in een ministeriële regeling nog verder in te vullen"

Strategie cybersecurity en energie:

- De sectoren aardolie en gas vallen onder de reikwijdte van de verplichtingen van de Europese richtlijn inzake beveiliging van netwerk-

[2] Grootste Amerikaanse brandstofpijplijn platgelegd door ransomware-aanval - Security.NL
[3] Staatsblad 2021, 160 | Overheid.nl > Officiële bekendmakingen (officielebekendmakingen.nl)

en informatiesystemen (NIB-richtlijn)[4] die zijn geïmplementeerd in de Wbni. Een aantal aanbieders van diensten (transport via buisleidingen, raffinage en het opslaan van aardolie) is zo belangrijk dat er grote negatieve economische, fysieke of sociaal-maatschappelijke gevolgen ontstaan, wanneer deze processen stil komen te liggen door bijvoorbeeld cyberaanvallen.

[redacted]

- Het Cybersecuritybeeld Nederland 2022 (CSBN 2022)[6] beschrijft in algemene zin dat de energietransitie verdere digitalisering stimuleert. Dit gaat gepaard met nieuwe risico's. Zowel statelijke actoren als criminelen maken misbruik van onze afhankelijkheid van digitale technologie. Op 10 oktober 2020 heeft de minister van Justitie en Veiligheid de nieuwe Nederlandse Cybersecurity Strategie (NLCS) gepresenteerd[7] met daarin een brede cybersecurityaanpak.

[redacted]

[4] Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie (PbEU 2016, L 194)
[5] EUR-Lex - 32022R1032 - EN - EUR-Lex (europa.eu)
[6] Kamerstuk 26643, nr. 891
[7] Nederlandse Cybersecuritystrategie 2022 - 2028