EUROPESE
COMMISSIE

Brussel, 28.10.2019
COM(2019) 546 final

VERSLAG VAN DE COMMISSIE AAN HET EUROPEES PARLEMENT EN DE RAAD

over de beoordeling van de coherentie van de aanpak van de lidstaten met betrekking tot de identificatie van aanbieders van essentiële diensten overeenkomstig artikel 23, lid 1, van Richtlijn 2016/1148/EU houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie

1. Inleiding

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[1] (richtlijn inzake netwerk- en informatiebeveiliging) is het eerste instrument van de interne markt gericht op het verbeteren van de veerkracht van de EU tegen cyberbeveiligingsrisico's. De richtlijn is gebaseerd op artikel 114 van het Verdrag betreffende de werking van de Europese Unie en heeft ten doel de continuïteit van de dienstverlening te waarborgen zodat de economie en samenleving in de Unie naar behoren kunnen functioneren. Met het oog hierop bevat de richtlijn concrete maatregelen om de capaciteit inzake cyberbeveiliging binnen de EU op te bouwen en de toenemende bedreigingen voor netwerk- en informatiesystemen die worden gebruikt voor de levering van essentiële diensten in belangrijke sectoren tegen te gaan.

Na de inwerkingtreding van de richtlijn in augustus 2016 moesten de lidstaten uiterlijk op 9 mei 2018[2] nationale maatregelen vaststellen om te voldoen aan de bepalingen van de richtlijn inzake netwerk- en informatiebeveiliging (NIS-richtlijn). De richtlijn bevordert een cultuur van risicobeheer bij bedrijven of andere entiteiten die essentiële diensten verlenen en overeenkomstig artikel 5 worden gedefinieerd als "aanbieders van essentiële diensten". Aanbieders waarop de richtlijn van toepassing is, moeten passende en evenredige technische en organisatorische maatregelen nemen om de risico's voor de beveiliging van netwerk- en informatiesystemen te beheersen en ernstige incidenten aan bevoegde autoriteiten te melden.

De medewetgevers hebben de uitvoering van de richtlijn inzake netwerk- en informatiebeveiliging gedelegeerd aan de lidstaten, die essentiële diensten moeten vaststellen en aanbieders van essentiële diensten moeten identificeren op hun grondgebied. Artikel 5, lid 7, van de richtlijn verplicht de lidstaten er daarom toe om de resultaten van deze identificatie aan de Commissie te verstrekken. Om ervoor te zorgen dat de rapportage

[1] PB L 194 van 19.7.2016, blz. 1.
[2] In september 2019 hadden alle 28 lidstaten kennisgegeven van volledige omzetting.

gecoördineerd verloopt, hebben de Commissie[3] en de samenwerkingsgroep die bij de richtlijn is ingesteld[4] de lidstaten bijgestaan in het identificatieproces.

Overeenkomstig artikel 23, lid 1, wordt in het onderhavige verslag de coherentie van de aanpak van de lidstaten met betrekking tot de identificatie van aanbieders van essentiële diensten beoordeeld. Daar de coherentie van de identificatie van aanbieders van essentiële diensten en het risico van fragmentatie in de interne markt op dit gebied nauw met elkaar verbonden zijn, zal dit verslag ook worden meegenomen in de bredere beoordeling van de richtlijn inzake netwerk- en informatiebeveiliging, zoals vastgesteld in artikel 23, lid 2, waarin wordt bepaald dat de Commissie de algemene werking van de richtlijn op gezette tijden evalueert en de lijst van sectoren en deelsectoren waarvoor aanbieders van essentiële diensten moeten worden geïdentificeerd en de soorten digitale diensten die onder de richtlijn vallen moet beoordelen. Het eerste verslag moet uiterlijk op 9 mei 2021 worden ingediend.

1.1 Doel van het verslag

Vanwege hun belangrijke rol voor de economie en de samenleving als geheel moeten aanbieders van essentiële diensten een bijzonder hoge mate van veerkracht tegen cyberincidenten bezitten. Met het oog hierop is een consistente benadering bij de identificatie van aanbieders van essentiële diensten door de lidstaten belangrijk, en wel om verschillende redenen:

1. **Om de risico's wat betreft grensoverschrijdende afhankelijkheid te beperken:**

   Wanneer belangrijke aanbieders die grensoverschrijdende diensten verlenen niet consistent worden geïdentificeerd, kan de veerkracht van cyberspace tussen verschillende lidstaten verschillen, waardoor het risico dat een grensoverschrijdend incident schade zou veroorzaken aan kritieke infrastructuren of burgers het leven zou

[3] *Mededeling van de Commissie aan het Europees Parlement en de Raad: De NIS-richtlijn ten volle benutten – naar de doeltreffende uitvoering van Richtlijn (EU) 2016/1148 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie,* COM(2017) 476.

[4] De NIS-samenwerkingsgroep, die bestaat uit vertegenwoordigers van de lidstaten, de Commissie en het Enisa (het Agentschap van de Europese Unie voor cyberbeveiliging), heeft een afzonderlijke werkstroom opgezet voor de uitwisseling van informatie en beste praktijken inzake de identificatie van aanbieders van essentiële diensten tussen de lidstaten.

kosten toeneemt[5]. Zo zijn bijvoorbeeld aanbieders op het gebied van energietransmissie of registers voor topleveldomeinnamen, beide op de lijst met soorten entiteiten in bijlage II, entiteiten die optimaal van de interne markt profiteren door grensoverschrijdende diensten aan consumenten en bedrijven te verlenen. Een consistente identificatie van dergelijke aanbieders binnen de Unie zou daarom kunnen helpen voorkomen dat cyberdreigingen zich in de interne markt verspreiden[6].

2. **Om te zorgen voor een gelijk speelveld voor aanbieders op de interne markt:**

   De richtlijn inzake netwerk- en informatiebeveiliging legt de lidstaten de verplichting op beveiligingseisen en procedures voor de melding van incidenten voor aanbieders van essentiële diensten op te stellen. Daar de richtlijn een minimumharmonisatiebenadering volgt ten aanzien van aanbieders van essentiële diensten, staat het de lidstaten vrij eisen aan aanbieders op te leggen die strenger zijn dan de eisen die de richtlijn stelt. Dergelijke maatregelen verhogen weliswaar de veerkracht van de lidstaten, maar ze kunnen extra uit de regelgeving voortvloeiende kosten met zich meebrengen voor de betrokken aanbieders. Het is daarom van belang dat aanbieders die vergelijkbare diensten van vergelijkbare relevantie verlenen onderworpen zijn aan vergelijkbare regelgeving.

3. **Om het risico van uiteenlopende interpretaties van de richtlijn te beperken:**

   De richtlijn moet de lidstaten de ruimte geven relevante entiteiten te selecteren om rekening te houden met specifieke nationale kenmerken. Tegelijkertijd verhoogt deze benadering het risico dat de bepalingen van de richtlijn op uiteenlopende manieren ten uitvoer worden gelegd en kan deze ertoe leiden dat de lidstaten inconsistente maatregelen vaststellen. Dit is met name van belang voor bedrijven die in verschillende landen actief zijn en daarom moeten voldoen aan de regelgevingsvereisten van meerdere lidstaten.

---

[5] Zo had bijvoorbeeld de ransomware cryptoworm WannaCry in mei 2017 slechts één dag nodig om zich in meer dan 150 landen te verspreiden en naar schatting 200 000 computers te infecteren.

[6] Volgens de NIS-samenwerkingsgroep kan de openheid van de interne markt voor diensten tot "grensoverschrijdende risico's en afhankelijkheid leiden die de beschikbaarheid, integriteit en vertrouwelijkheid van deze diensten fundamenteel kan aantasten".

4. **Om een uitgebreid overzicht van de mate van veerkracht van cyberspace binnen de EU te verkrijgen:**

   Aanbieders van essentiële diensten worden onderworpen aan toezichtactiviteiten om na te gaan of het beveiligingsbeleid daadwerkelijk wordt uitgevoerd en significante incidenten worden gemeld. Toezicht bevordert de samenwerking tussen publieke en private partijen, waarbij kennis over de paraatheid op het gebied van cyberbeveiliging in een lidstaat wordt uitgewisseld. Dankzij de samenwerkingsgroep kan de uitwisseling van ervaringen op nationaal niveau, waaronder informatie over gemelde incidenten[7], op EU-niveau worden geaggregeerd en bijdragen aan een nauwkeurigere beoordeling van de belangrijkste bedreigingen en behoeften. Om deze informatie-uitwisseling echter doeltreffend te laten zijn, zouden alle partijen het erover eens moeten zijn welke entiteiten als aanbieders van essentiële diensten worden geïdentificeerd.

1.2 Identificatieprocedure op grond van de richtlijn inzake netwerk- en informatiebeveiliging

Bijlage II bij de richtlijn inzake netwerk- en informatiebeveiliging bevat een lijst met zeven sectoren en de bijbehorende deelsectoren en soorten entiteiten die relevant zijn voor het identificatieproces (Tabel 1). Krachtens artikel 5, lid 3, moeten de lidstaten een lijst met essentiële diensten opstellen op basis van deze sectoren, deelsectoren en soorten entiteiten. De minimumharmonisatiebenadering van de richtlijn geeft de lidstaten de ruimte meer sectoren en deelsectoren te identificeren dan worden genoemd in bijlage II.

[7] Overeenkomstig artikel 10, lid 3, van de richtlijn inzake netwerk- en informatiebeveiliging dienen de lidstaten eenmaal per jaar bij de samenwerkingsgroep een samenvattend verslag in over de ontvangen meldingen.

Sector	Deelsector
1. Energie	a) Elektriciteit
	b) Aardolie
	c) Gas
2. Vervoer	a) Luchtvervoer
	b) Spoorvervoer
	c) Vervoer over water
	d) Vervoer over de weg
3. Bankwezen	
4. Infrastructuur voor de financiële markt	
5. Gezondheidszorg	
6. Levering en distributie van drinkwater	
7. Digitale infrastructuur	

Tabel 1: Lijst van sectoren en deelsectoren uit bijlage II bij de richtlijn inzake netwerk- en informatiebeveiliging

Artikel 5, lid 2, geeft drie **criteria** aan de hand waarvan de lidstaten aanbieders van essentiële diensten moeten identificeren:

1. De betreffende entiteit moet een **dienst verlenen die van essentieel belang is** voor de instandhouding van kritieke maatschappelijke en/of economische activiteiten. Hiertoe moeten nationale bevoegde autoriteiten hun eerder opgestelde lijsten van essentiële diensten raadplegen.
2. De verleende dienst is **afhankelijk van netwerk- en informatiesystemen**.
3. Een incident zou aanzienlijke **verstorende effecten** hebben voor de verlening van die dienst. In artikel 6 staat dat bij het bepalen van de omvang van een incident rekening moet worden gehouden met **sectoroverschrijdende factoren** en, waar passend, **sectorspecifieke factoren**[8].

Verder stipuleert artikel 5, lid 4, van de richtlijn dat de lidstaten overleg moeten plegen als zij vaststellen dat een potentiële aanbieder van essentiële diensten diensten in meer dan één

[8] Voorbeelden van sectoroverschrijdende factoren zijn het aantal gebruikers dat afhankelijk is van een dienst of het marktaandeel van een entiteit. Voorbeelden van sectorspecifieke factoren zijn het aantal autonome systemen die verbonden zijn met een internetknooppunt of het aantal transacties per jaar van een financiële instelling.

lidstaat verleent. Deze verplichte procedure moet de lidstaten helpen de mogelijke gevolgen van een cyberincident dat grensoverschrijdend opererende entiteiten treft te beoordelen en bedrijven waarvoor de procedures van verschillende lidstaten gelden te beschermen.

1.3 Methode van het verslag

De resultaten van het verslag zijn gebaseerd op een beoordeling die is uitgevoerd tussen november 2018 en september 2019. Veel lidstaten hadden de voor het verslag benodigde informatie niet op tijd aan de Commissie verstrekt. De goedkeuring van het verslag moest daarom worden uitgesteld tot na 9 mei 2019, de goedkeuringsdatum die was opgenomen in artikel 23, lid 1, van de richtlijn inzake netwerk- en informatiebeveiliging. De gegevens werden via diverse kanalen verzameld: door de lidstaten verstrekte informatie op basis van een gestandaardiseerde template van het Enisa, gestandaardiseerde gesprekken met vertegenwoordigers van geselecteerde nationale autoriteiten en bijeenkomsten van de samenwerkingsgroep, waaronder een workshop over het onderwerp die werd gehouden op 19 maart 2019.

Op basis van de verzamelde informatie wordt in het verslag de samenhang van de aanpak van de lidstaten voor de identificatie beoordeeld door

1. de verschillende door de nationale autoriteiten gekozen identificatiemethoden met elkaar te vergelijken,
2. de lijsten van essentiële diensten en door de lidstaten gekozen drempels te onderzoeken,
3. het aantal aanbieders van essentiële diensten in elke lidstaat te analyseren.

In het verslag wordt ook geëvalueerd hoe uitvoering is gegeven aan de bepalingen van de richtlijn betreffende grensoverschrijdend overleg (artikel 5, lid 4) en het *lex specialis*-beginsel (artikel 1, lid 7). Het verslag bevat een feitelijke analyse van het door de lidstaten uitgevoerde identificatieproces, voorlopige conclusies en open vragen voor nadere reflectie.

1.4 Beschikbaarheid van gegevens

Krachtens de bepalingen van de richtlijn inzake netwerk- en informatiebeveiliging hoeven de lidstaten slechts een beperkte hoeveelheid gegevens aan de Commissie te verstrekken. Nationale autoriteiten hoeven bijvoorbeeld niet de namen van geïdentificeerde aanbieders op

te geven, waardoor het voor de diensten van de Commissie lastig is om de resultaten van het identificatieproces op het punt van volledigheid van de lijst en de gevolgen voor bedrijven van dezelfde grootte uit dezelfde sector met elkaar te vergelijken.

Krachtens artikel 5, lid 7, moesten alle lidstaten de voor dit verslag benodigde informatie uiterlijk op 9 november 2018 verstrekken. Op die datum hadden echter slechts 15 landen voldoende gegevens verstrekt (zie de tabel in de bijlage in punt 4.1). Ook na herhaalde herinneringen van de Commissie ontbraken nog steeds veel gegevens. De Commissie stuurde daarom op 26 juli 2019 aanmaningsbrieven naar zes lidstaten[9] waarin zij werden opgeroepen de ontbrekende gegevens binnen twee maanden aan te vullen.

Op de datum van publicatie van dit verslag hadden 23 lidstaten alle gegevens die zij uit hoofde van artikel 5, lid 7, moesten indienen verstrekt: Bulgarije, Kroatië, Cyprus, Tsjechië, Duitsland, Denemarken, Estland, Griekenland, Spanje, Finland, Frankrijk, Ierland, Italië, Litouwen, Luxemburg, Letland, Malta, Nederland, Polen, Portugal, Zweden, Slowakije en het Verenigd Koninkrijk. De overige vijf lidstaten (Oostenrijk, België, Hongarije, Roemenië en Slovenië) hebben slechts gedeeltelijk gegevens over de nationale identificatie van aanbieders van essentiële diensten verstrekt, aangezien zij er niet in zijn geslaagd hun identificatieproces op tijd voor de publicatie van dit verslag af te ronden.

[9] België, Griekenland, Hongarije, Oostenrijk, Roemenië en Slovenië.

2. Identificatie van nationale aanbieders van essentiële diensten in de lidstaten

De richtlijn inzake netwerk- en informatiebeveiliging bevat een kader voor de identificatie van aanbieders van essentiële diensten dat de lidstaten de ruimte biedt rekening te houden met specifieke nationale kenmerken. De lidstaten hebben daarom zeer uiteenlopende identificatiepraktijken ontwikkeld.

2.1 Door de lidstaten gebruikte methoden

De lidstaten hebben volop gebruikgemaakt van de flexibiliteit die de richtlijn inzake netwerk- en informatiebeveiliging biedt en verschillende methoden voor het identificeren van aanbieders ontwikkeld. Een van de elementen die van invloed was op nationale methoden was het feit dat er al een kader bestond, onder meer Richtlijn 2008/114/EG van de Raad inzake de identificatie van Europese kritieke infrastructuren[10] of andere nationale bepalingen inzake "essentiële aanbieders". In dergelijke gevallen hebben de lidstaten hun opgedane ervaringen gebruikt als referentiepunt en specifieke kenmerken met betrekking tot de richtlijn inzake netwerk- en informatiebeveiliging opgenomen in bestaande methoden.

De verschillen in nationale methoden kunnen in de volgende twee hoofdcategorieën worden ingedeeld: essentiële diensten, gebruik van drempels, mate van centralisatie, autoriteiten belast met de identificatie en beoordeling van de afhankelijkheid van netwerk- en informatiesystemen. Vanwege hun belang voor het beoordelen van de consistentie bij de identificatie van aanbieders van essentiële diensten zijn afzonderlijke punten gewijd aan de analyse van essentiële diensten en drempels. In dit punt zullen de overige criteria aan bod komen.

Mate van centralisatie

De meeste lidstaten hebben ervoor gekozen de besluitvorming met betrekking tot verschillende elementen van het identificatieproces voor een deel te delegeren aan sectorale autoriteiten (ministeries, agentschappen enz.). De mate van decentralisatie varieert van geval

[10] Richtlijn 2008/114/EG van de Raad van 8 december 2008 inzake de identificatie van Europese kritieke infrastructuren, de aanmerking van infrastructuren als Europese kritieke infrastructuren en de beoordeling van de noodzaak de bescherming van dergelijke infrastructuren te verbeteren. De richtlijn moet de bescherming van kritieke infrastructuren in de sectoren energie en vervoer verbeteren.

tot geval; de meeste lidstaten wijzen één autoriteit aan die sectorale autoriteiten moet bijstaan en informatie moet bundelen. Een aantal landen heeft er echter voor gekozen de verantwoordelijkheid voor het identificatieproces bij één autoriteit neer te leggen. Er zijn ook gevallen met een extreem hoge mate van decentralisatie waarbij sectorale autoriteiten hun eigen methoden moeten ontwikkelen.

Veel lidstaten hebben de verschillende aspecten van de institutionele structuur van de identificatie van aanbieders van essentiële diensten zorgvuldig tegen elkaar afgewogen. Autoriteiten noemen het vermijden van belangenconflicten een van de voordelen van een gecentraliseerde identificatie: aanbieders blijken er huiverig voor te zijn om relevante informatie aan sectorale toezichthouders te verstrekken, omdat zij vrezen dat deze informatie ook gebruikt zou kunnen worden voor andere toezichtdoeleinden.

Een gedecentraliseerde aanpak daarentegen lijkt de dialoog tussen voor netwerk- en informatiebeveiliging bevoegde autoriteiten (zowel met betrekking tot cyberbeveiliging als op sectoraal gebied) te bevorderen, waardoor zij de implicaties van sectoroverschrijdende afhankelijkheden beter kunnen identificeren. Bovendien hebben sectorale autoriteiten vaak meer inzicht in de sectoren dan de hoofdautoriteiten.

Identificatieprocedure (top-down vs. bottom-up)

Een ander belangrijk onderscheid kan worden gemaakt tussen lidstaten waarin overheidsinstanties het identificatieproces uitvoeren (top-downidentificatie) en lidstaten waarin marktaanbieders worden verzocht zelf na te gaan of zij als aanbieders van essentiële diensten voldoen aan de eisen (zogenaamde bottom-upidentificatie of zelfidentificatie). Om deze laatste aanpak doeltreffend te laten zijn, zouden de lidstaten boetes moeten opleggen die hoog genoeg zijn om aanbieders af te schrikken om geen melding te doen, zoals bedoeld in artikel 21 van de richtlijn inzake netwerk- en informatiebeveiliging. In de meeste gevallen is het identificatieproces top-down. In de praktijk passen autoriteiten echter vaak een aantal zelfbeoordelingselementen toe, en moeten potentiële aanbieders van essentiële diensten bijvoorbeeld vragenlijsten invullen.

Als de voorschriften en drempels voor de identificatie van aanbieders van essentiële diensten expliciet en transparant zijn, zouden top-down- en bottom-upidentificatie vergelijkbare resultaten moeten opleveren. Het zou voor de consistentie in principe dan ook niet mogen uitmaken welke aanpak wordt gekozen.

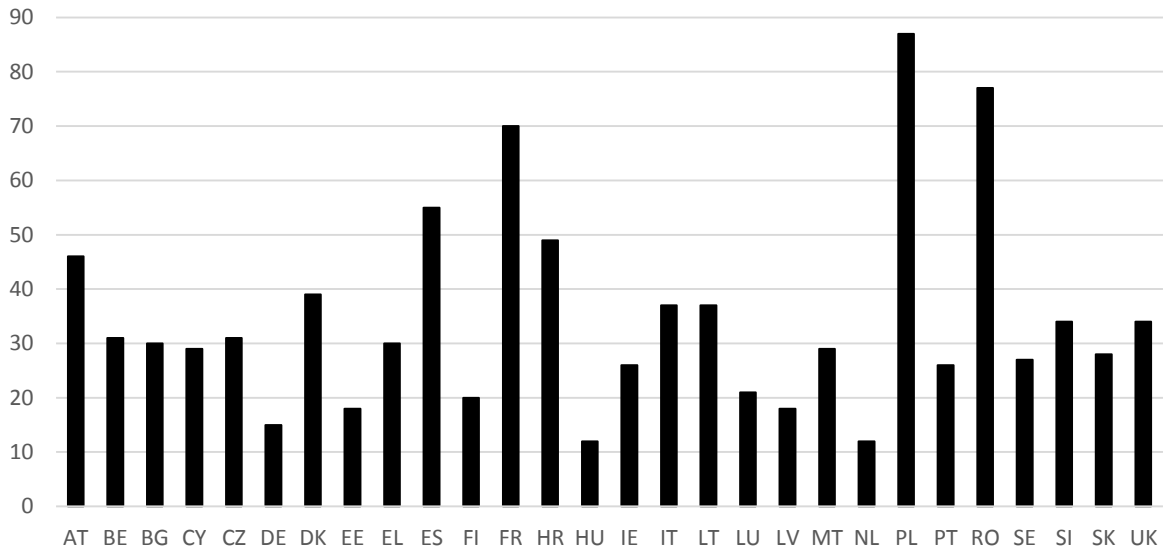
Beoordeling van netwerkafhankelijkheid

Zoals in punt 1.2 is uitgelegd, moeten de lidstaten uit hoofde van artikel 5, lid 2, onder b), de afhankelijkheid van een aanbieder van netwerk- en informatiesystemen beoordelen in het kader van de identificatieprocedure van aanbieders van essentiële diensten. Veel lidstaten beschouwen de afhankelijkheid van netwerk- en informatiesystemen bij de toepassing van deze criteria als een gegeven in de hedendaagse digitale economie. Sommige autoriteiten kiezen echter voor een uitgebreidere aanpak en voeren uitvoerige beoordelingen uit of vragen aanbieders om hun mate van afhankelijkheid zelf in te schatten.

2.2 Identificatie van diensten

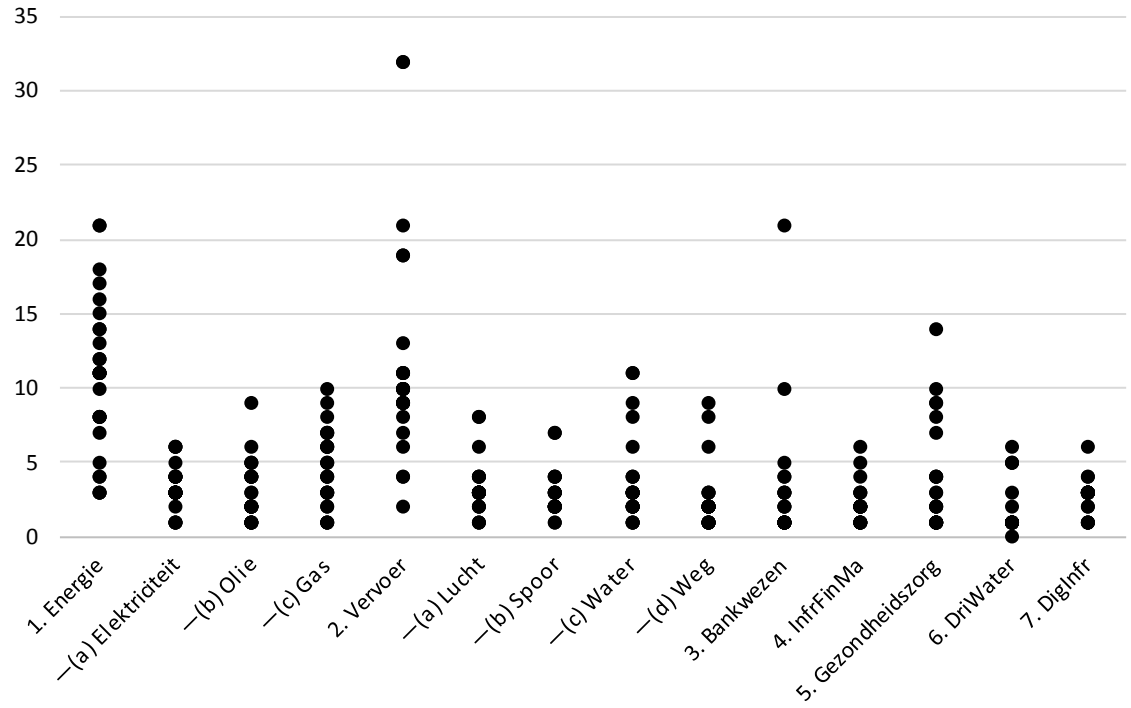
Overweging 23 van de richtlijn inzake netwerk- en informatiebeveiliging noemt de lijsten van essentiële diensten expliciet als inbreng bij de "beoordeling van de regelgevingspraktijken van de lidstaten met het oog op het waarborgen van de algehele samenhang van het identificatieproces tussen de lidstaten". Daar de lijsten van essentiële diensten die door de lidstaten zijn opgesteld als basis dienen voor de identificatie van aanbieders, kunnen verschillen in de geïdentificeerde diensten tot een inconsistente identificatie van aanbieders in de verschillende lidstaten leiden, met name als specifieke diensten die in alle landen worden verleend slechts door een aantal lidstaten worden geïdentificeerd.

Het aantal door de lidstaten geïdentificeerde diensten die onder bijlage II van de richtlijn inzake netwerk- en informatiebeveiliging vallen en aan de Commissie zijn gemeld, verschilt aanzienlijk tussen de lidstaten (punt 4.2 in de bijlage geeft de aantallen voor alle lidstaten). Het aantal geïdentificeerde diensten ligt tussen 12 en 87, met gemiddeld 35 diensten per lidstaat, zoals te zien is in Figuur 1. Grotere lidstaten identificeren doorgaans iets meer diensten dan kleinere lidstaten, maar er lijkt geen sterke correlatie te zijn tussen de grootte van een lidstaat en het aantal geïdentificeerde diensten. Dit werd ook verwacht, omdat consumenten en bedrijven in de praktijk meestal in alle lidstaten toegang hebben tot dezelfde soorten diensten, ongeacht de grootte van een land.



Figuur 1: Totale aantal door de lidstaten geïdentificeerde essentiële diensten

Het aantal geïdentificeerde diensten varieert niet alleen als we kijken naar de lidstaten als geheel, maar ook op het niveau van sectoren en deelsectoren. In het bankwezen bijvoorbeeld ligt het aantal geïdentificeerde diensten tussen 1 en 21. Zoals weergegeven in Figuur 2 verschilt het aantal geïdentificeerde diensten tussen landen in de meeste sectoren en deelsectoren aanmerkelijk.



Figuur 2: Aantal door de lidstaten geïdentificeerde diensten per sector en deelsector. Elk gegevenspunt staat voor het aantal door een lidstaat geïdentificeerde diensten in de betreffende (deel)sector[11].

Tot op zekere hoogte weerspiegelen de cijfers uit Figuur 2 de verschillen in methodologische aanpak tussen de landen. Sommige lidstaten hebben voor de identificatie van diensten bijvoorbeeld voor een meer granulaire aanpak gekozen dan andere lidstaten, waardoor de aantallen in deze lidstaten hoger uitvallen. Uit de gegevens die de Commissie van de lidstaten heeft ontvangen, komt echter duidelijk naar voren dat de verschillen in aantallen ook voortkomen uit inconsistenties in de aanpak die lidstaten hebben gekozen, zoals te zien is in het volgende voorbeeld van de deelsectoren elektriciteit en spoorvervoer:

[11] Identieke gegevenspunten worden bovenop elkaar uitgezet. Om deze reden zijn niet alle 28 gegevenspunten in het diagram zichtbaar. Zo hebben 17 lidstaten bijvoorbeeld exact drie essentiële diensten geïdentificeerd onder Digitale infrastructuren.

Estland (minst granulaire aanpak)	Portugal	Denemarken	Bulgarije (meest granulaire aanpak)
Levering van elektriciteit	Distributiesysteembeheerders	Elektriciteitsdistributie	Distributie van elektriciteit
			Waarborgen van de werking en het onderhoud van een distributiesysteem voor elektrische energie
	Transmissiesysteembeheerder	Elektriciteitstransmissie	Transmissie van elektriciteit
			Werking, onderhoud en ontwikkeling van een elektriciteitstransmissiesysteem
	(zeer uiteenlopend)	Elektriciteitsopwekking	Elektriciteitsopwekking
	(zeer uiteenlopend)	*(zeer uiteenlopend)*	Elektriciteitsmarkt

Tabel 2: Voorbeelden van de aanpak die lidstaten hebben gekozen voor de identificatie van essentiële diensten in de deelsector elektriciteit

In Tabel 2 wordt een aantal manieren waarop lidstaten essentiële diensten in de deelsector elektriciteit hebben geïdentificeerd met elkaar vergeleken. Sommige landen (zoals Estland) hebben gekozen voor een zeer algemene noemer, waardoor praktisch elke aanbieder die volgens hen essentiële diensten in de deelsector elektriciteit verleent kan worden geïdentificeerd. Andere landen (zoals Portugal, Denemarken en Bulgarije) hebben gekozen voor een veel meer granulaire aanpak. Zo heeft Bulgarije bijvoorbeeld een extreem gedetailleerde dienstenlijst opgesteld waarin zelfs een dienst wordt vermeld die niet onder bijlage II valt (elektriciteitsmarkten). Portugal en Denemarken hebben daarentegen voor een granulaire aanpak gekozen en hebben bepaalde diensten die andere landen aan hun lijst hebben toegevoegd buiten beschouwing gelaten. Dit kan resulteren in een ongelijk speelveld tussen aanbieders van essentiële diensten binnen de interne markt.

Zeer uiteenlopende diensten zoals deze zijn geïdentificeerd in Tabel 2 zijn het gevolg van verschillende nationale uitvoeringen van de richtlijn inzake netwerk- en informatiebeveiliging, en bij sectoren die niet onder bijlage II vallen (zoals elektriciteitsmarkten), een gevolg van de minimumharmonisatiebenadering. Waar sprake is van zeer uiteenlopende diensten, wil dat dus niet per se zeggen dat lidstaten die een bepaalde

dienst niet hebben geïdentificeerd de bepalingen van de richtlijn niet correct hebben toegepast.

Tabel 3 laat zien welke aanpak vier landen hebben gekozen voor de deelsector spoorvervoer. Frankrijk heeft een zeer gedetailleerde en uitgebreide lijst van diensten opgesteld die essentieel zijn voor het functioneren van het spoorvervoer, terwijl de overige drie landen slechts een kleine subset van deze diensten hebben geselecteerd. In het geval van Polen is niet geheel duidelijk welke diensten onder de categorieën "goederenvervoer per spoor" en "personenvervoer per spoor" vallen. Hun aanmerkingen zijn zo algemeen gehouden dat er mogelijk ook diensten onder vallen die door Frankrijk zijn geïdentificeerd, zoals "verkeersleiding van het spoorvervoer". Hierbij dient te worden opgemerkt dat de Commissie niet over de middelen beschikt dit soort gevallen nader te onderzoeken: volgens de richtlijn inzake netwerk- en informatiebeveiliging hoeven nationale autoriteiten geen gedetailleerdere informatie te verstrekken.

Finland	Frankrijk	Ierland	Polen
Infrastructuurbeheer door de overheid	Onderhoud van infrastructuur	Infrastructuurbeheerders	*(zeer uiteenlopend)*
(zeer uiteenlopend)	Onderhoud van rollend materieel	*(zeer uiteenlopend)*	*(zeer uiteenlopend)*
Verkeersleidingdiensten	Verkeersleiding van het spoorvervoer	*(zeer uiteenlopend)*	Treindienstregelingen opstellen
(zeer uiteenlopend)	Vracht en gevaarlijke materialen	Spoorwegondernemingen	Goederenvervoer per spoor
(zeer uiteenlopend)	Personenvervoer		Personenvervoer per spoor
(zeer uiteenlopend)	Metro's en tramdiensten (met inbegrip van ondergrondse diensten)		*(zeer uiteenlopend)*
(zeer uiteenlopend)	Spoorwegdiensten	*(zeer uiteenlopend)*	*(zeer uiteenlopend)*

Tabel 3: Voorbeelden van de aanpak die lidstaten hebben gekozen voor de identificatie van essentiële diensten in de deelsector spoorvervoer

De lidstaten die zijn opgenomen in Tabel 2 en Tabel 3 zijn uitsluitend ter illustratie gekozen en omdat hun methodologische aanpak gemakkelijk te vergelijken is. De meeste andere

lidstaten hebben vergelijkbare diensten geselecteerd en vertonen daarom soortgelijke "zeer uiteenlopende" diensten. "Zeer uiteenlopende" diensten zoals in de deelsectoren elektriciteit en spoorvervoer komen in feite in alle lidstaten en sectoren uit bijlage II bij de richtlijn voor. Deze inconsistentie is grotendeels toe te schrijven aan diensten die alleen in een aantal, maar niet in alle lidstaten zijn geïdentificeerd. De volledige lijsten van diensten in de deelsectoren elektriciteit en spoorvervoer voor alle lidstaten zijn te vinden in de bijlage bij dit verslag.

2.3 Drempels

De meeste lidstaten hanteren drempels bij het identificeren van aanbieders van essentiële diensten, maar de rol die deze drempels spelen, varieert van land tot land. Sectoroverschrijdende drempels kunnen worden vastgelegd op basis van

- een enkele kwantitatieve factor (bv. het aantal gebruikers dat afhankelijk is van een dienst) om te bepalen of een entiteit die een bepaalde dienst verleent, kan worden beschouwd als een aanbieder van essentiële diensten;
- een groter aantal kwantitatieve factoren (bv. het aantal gebruikers dat afhankelijk is van een dienst plus het marktaandeel);
- een combinatie van kwantitatieve en kwalitatieve factoren.

De richtlijn staat de lidstaten ook toe naast sectoroverschrijdende ook sectorspecifieke drempels toe te passen. Dit geeft nationale autoriteiten meer vrijheid om in het identificatieproces rekening te houden met specifieke nationale en sectorale kenmerken. Hierdoor ontstaat er wel een zeer grote diversiteit aan drempels, wat negatieve gevolgen kan hebben voor de algehele consistentie bij de identificatie van aanbieders van essentiële diensten.

Tabel 4 geeft een voorbeeld van deze uiteenlopende benaderingen. Hieruit blijkt dat de door de lidstaten gekozen drempels in de sector digitale infrastructuur niet alleen kwantitatief van elkaar verschillen (zo worden DNS-dienstverleners in Duitsland geïdentificeerd als aanbieders van essentiële diensten als zij ten minste 250 000 domeinen beheren, terwijl in Polen de drempel bij slechts 100 000 domeinen ligt), maar ook kwalitatief (bv. "aantal verbonden autonome systemen" vs. "marktaandeel").

Consistent gekozen kwantitatieve drempels alleen vormen nog geen garantie dat de aanpak in verschillende lidstaten volledig consistent is. Gezien het feit dat drempels in sommige lidstaten slechts een van de criteria voor de identificatie van aanbieders van essentiële

diensten zijn, kan het identificatieproces alsnog zeer uiteenlopende resultaten opleveren, zelfs als vergelijkbare drempels worden toegepast. Sommige lidstaten maken bijvoorbeeld gebruik van complexe scoresystemen waarbij verschillende factoren worden ingevoerd in één enkele formule[12]. Het kan bij deze factoren bijvoorbeeld gaan om de afhankelijkheid van een entiteit van netwerk- en informatiesystemen of om een aantal van de factoren uit artikel 6, lid 1, van de richtlijn inzake netwerk- en informatiebeveiliging. Er zijn ook lidstaten die in het geheel geen drempels toepassen of alleen in de eerste fase van de beoordeling. Deze overwegingen gelden niet alleen voor de sector digitale infrastructuur, maar voor alle sectoren uit bijlage II.

Het kan een uitdaging zijn om de juiste drempel in te stellen, vooral bij sectoren die worden gekenmerkt door een groot aantal kleine aanbieders. Een voorbeeld van een dergelijke diversiteit zijn de vele kleinschalige gezondheidszorginstellingen (bv. klinieken of medische spoedhulp) die een essentiële dienst verlenen aan een relatief klein aantal gebruikers, maar die patiënten bij onbeschikbaarheid vanwege een cyberbeveiligingsincident het leven zou kunnen kosten. Een ander probleem treedt op als het functioneren van toeleveringsketens afhangt van diensten van aanbieders die een kleine maar essentiële schakel in deze ketens vormen (bijvoorbeeld in sectoren zoals de logistiek[13]). Eén lidstaat onderzoekt of dit probleem mogelijk op te lossen is door criteria toe te passen die verband houden met het belang of de kriticiteit van de verleende dienst.

[12] Eén lidstaat heeft bijvoorbeeld zeven factoren ontwikkeld (vier zogenaamde "aanbiederafhankelijke factoren" en drie "impactafhankelijke factoren" die worden ingevoerd in één enkele formule. Wanneer de eindwaarde van de berekening een bepaalde drempel overschrijdt, wordt de aanbieder in kwestie herkend als een aanbieder van essentiële diensten.

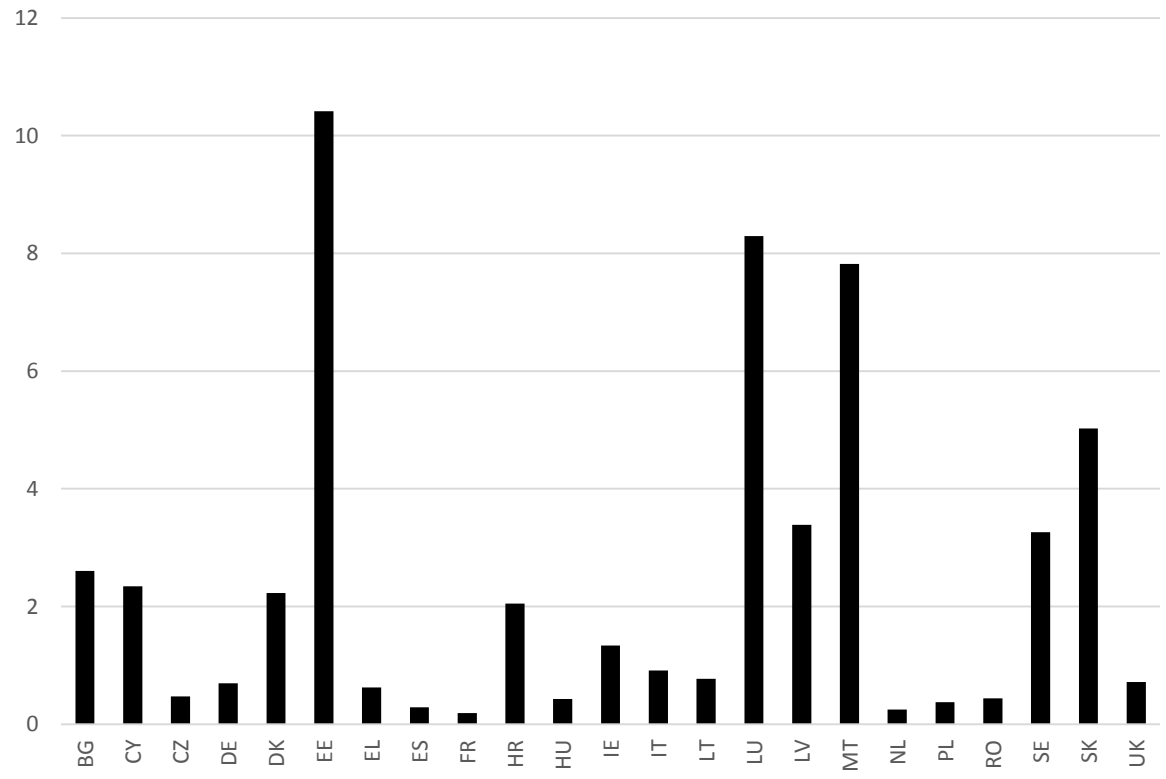
[13] De logistieke sector valt niet onder bijlage II bij de richtlijn inzake netwerk- en informatiebeveiliging.

Land	Internetknooppunten (IXP's)	DNS-dienstverleners	Registers voor topleveldomeinnamen
Gebruik van met name sectorspecifieke drempels			
AT	verbonden autonome systemen > 100	DNS-resolvers: 88 000 gebruikers; Toegelaten DNS: 50 000 domeinen	50 000 domeinen
DE	verbonden autonome systemen > 300	DNS-resolvers: 100 000 gebruikers; Toegelaten DNS: 250 000 domeinen	*(dienst niet geïdentificeerd)*
DK	gem. dagelijks gegevensvolume > 200 Gbit/s	DNS-resolvers: 100 000 gebruikers; Toegelaten DNS: 100 000 domeinen	500 000 domeinen
EE	*(dienst niet geïdentificeerd)*	*(dienst niet geïdentificeerd)*	Register van nationale TLD's
FI	*(dienst niet geïdentificeerd)*	*(dienst niet geïdentificeerd)*	Registers van nationale en regionale TLD's
FR	*(geen officiële drempel)*	*(geen officiële drempel)*	*(geen officiële drempel)*
HR	verbonden leden > 15	DNS-dienst voor nationale TLD's	Register van nationale TLD's
IE	*(drempel onbekend)*	DNS-resolvers: 100 mln. query's per etmaal; Toegelaten DNS: 50 000 domeinen	Register van nationale TLD's
MT	25 % van het marktaandeel	DNS-resolvers: 78 000 aanvragen/dag; Toegelaten DNS: 7 800 domeinen	750 000 aanvragen/dag
PL	verbonden autonome systemen ≥ 100	Toegelaten DNS: 100 000 domeinen	TLD-registers voor ten minste 100 000 abonnees
SE	*(dienst niet geïdentificeerd)*	DNS-resolvers: 100 000 gebruikers; Toegelaten DNS: 25 000 domeinen	250 000 domeinen
SK	*Autonoom systeem (AS) dat ten minste twee andere AS verbindt met 2 Gbps*	DNS-resolvers: 3 mln. query's per etmaal; Toegelaten DNS: > 1 000 domeinen	Register van TLD's
UK	marktaandeel > 50 % of interconnectiviteit met wereldwijde internetroutes ≥ 50 %	DNS-resolvers: 2 000 000 clients/dag; Toegelaten DNS: 250 000 domeinen	TLD-registers ≥ 2 miljard query's/dag
Gebruik van sectoroverschrijdende drempels			
CY	50 000 gebruikers of 5 % van abonnees op de markt	50 000 gebruikers of 5 % van abonnees op de markt	50 000 gebruikers of 5 % van abonnees op de markt
LT	inwoners > 145 000	inwoners > 145 000	inwoners > 145 000
LU	Marktaandeel 100 %	13 500 contracten	Marktaandeel 100 %

Tabel 4: Door 16 lidstaten gekozen drempels in de sector digitale infrastructuur

2.4 Aantal geïdentificeerde aanbieders

De lijsten van essentiële diensten en de drempels zijn de belangrijkste bepalende factoren voor een consistente identificatie van aanbieders van essentiële diensten. Uit de voorgaande punten blijkt dat de lidstaten de bepalingen van de richtlijn inzake netwerk- en informatiebeveiliging in beide gevallen op verschillende manieren hebben toegepast, wat zou kunnen leiden tot een consistentieprobleem als vervolgens aanbieders van essentiële diensten worden geïdentificeerd. In dit punt worden de aantallen geïdentificeerde aanbieders in de sectoren en deelsectoren van bijlage II in de lidstaten met elkaar vergeleken.

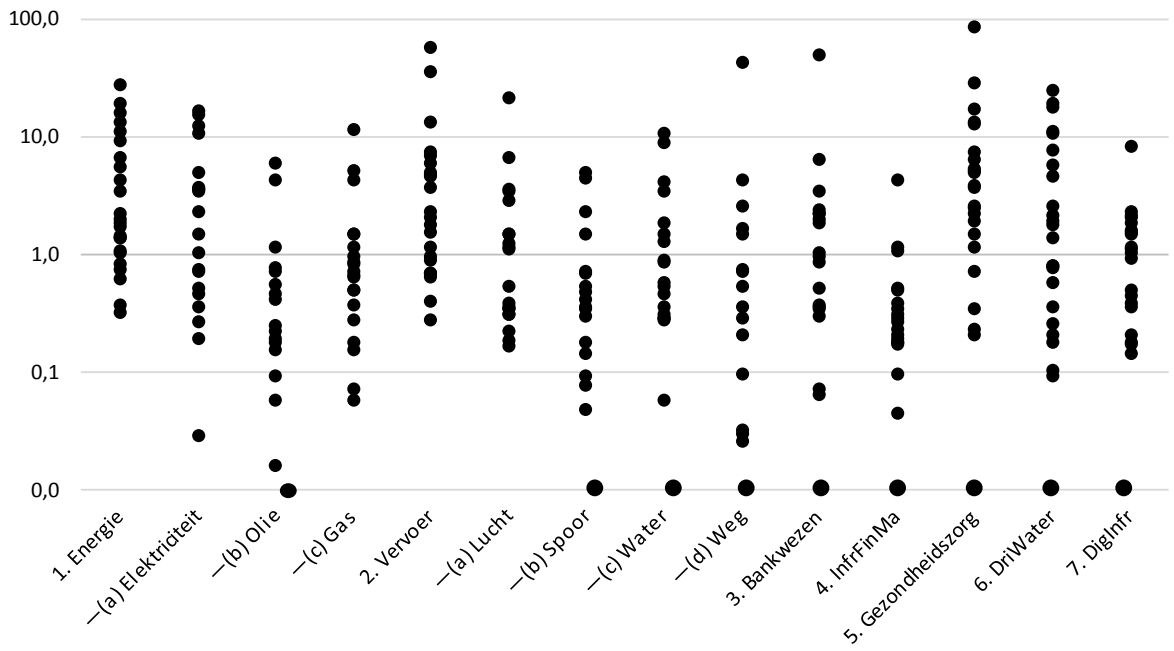


Figuur 3: Door de lidstaten geïdentificeerde aanbieders van essentiële diensten in alle sectoren van bijlage II (per 100 000 inwoners, uitschieters en ontbrekende gegevens zijn omwille van de duidelijkheid weggelaten)

De totale aantallen aanbieders van essentiële diensten die door de lidstaten aan de Commissie zijn gemeld, lopen uiteen van 20 tot 10 897, met een gemiddelde van 633 aanbieders van essentiële diensten per lidstaat (aantallen voor alle lidstaten staan in punt 4.2 van de bijlage bij dit verslag). Over het geheel genomen is er een duidelijk positief verband tussen de grootte van een land en het aantal geïdentificeerde aanbieders. Dit verklaart echter

onvoldoende waar de grote verschillen in de aantallen die de lidstaten hebben gemeld vandaan komen. Om rekening te houden met het verband tussen grootte en bevolking, worden in Figuur 3 de aantallen geïdentificeerde aanbieders van essentiële diensten in de lidstaten per 100 000 inwoners vergeleken. Hieruit komt naar voren dat de benaderingen die de lidstaten hebben gekozen voor het identificeren van aanbieders sterk uiteenlopende resultaten hebben opgeleverd.

Uit een grondiger onderzoek van de sectoren en deelsectoren blijkt dat er tussen de lidstaten aanzienlijke verschillen bestaan in de geïdentificeerde aantallen voor alle sectoren uit bijlage II (Figuur 4). In de energiesector bijvoorbeeld ligt het aantal tussen 0,3 en 29 aanbieders per 1 000 000 inwoners. De aantallen in het bankwezen liggen tussen 0,07 en 51 aanbieders per 1 000 000 inwoners (lidstaten die in deze sector geen enkele aanbieder van essentiële diensten hebben geïdentificeerd, zijn buiten beschouwing gelaten).



Figuur 4: Door 25 lidstaten geïdentificeerde aantal aanbieders van essentiële diensten in elke sector en deelsector (per 1 000 000 inwoners, op een logaritmische schaal; uitschieters omwille van de duidelijkheid weggelaten). Elk gegevenspunt staat voor het aantal door een lidstaat geïdentificeerde aanbieders van essentiële diensten in de betreffende (deel)sector[14].

[14] Identieke gegevenspunten worden bovenop elkaar uitgezet. Om deze reden zijn niet alle 25 gegevenspunten in het diagram zichtbaar. Zo hebben Denemarken en Nederland bijvoorbeeld 0,35 aanbieders van essentiële diensten per 1 000 000 inwoners in de deelsector luchtvervoer geïdentificeerd.

2.5 Toepassing van de richtlijn op andere sectoren dan die uit bijlage II

Uit een onderzoek van de verstrekte gegevens blijkt dat 11 van de 28 lidstaten essentiële diensten hebben geïdentificeerd in sectoren die niet binnen de werkingssfeer van bijlage II bij de richtlijn vallen. Van deze 11 lidstaten hebben er 7 in totaal 157 aanbieders van essentiële diensten geïdentificeerd die diensten verlenen die niet onder de soorten entiteiten van bijlage II vallen.

Aanvullende sector	Voorbeelden van entiteiten	Aantal lidstaten
Informatie-infrastructuren	Datacenters, serverfarms	5
Financiële diensten (entiteiten die niet zijn opgenomen in bijlage II)	Verzekerings- en herverzekeringsondernemingen	4
Overheidsdiensten	Elektronische diensten voor burgers	4
Warmte	Warmteproducenten en -leveranciers	3
Afvalwater	Installaties voor de verzameling en behandeling van afvalwater	3
Logistiek	Postdiensten	2
Levensmiddelen	Producenten, handelsplatformen	2
Milieu	Verwijdering van gevaarlijke afvalstoffen	2
Nationale veiligheids-/noodhulpdiensten	112, crisisbeheersing	2
Chemische industrie	Leveranciers en producenten van stoffen	2
Sociale diensten	Uitkeringsinstanties	1
Onderwijs	Autoriteiten belast met nationale examens	1
Collectieve cateringdiensten	Distributiebeheer	1
Water	Hydraulische structuren	1

Tabel 5: Door lidstaten gekozen sectoren als aanvulling op de sectoren genoemd in bijlage II

Informatie-infrastructuren (door vijf lidstaten geïdentificeerd), financiële diensten verleend door entiteiten die niet worden genoemd in bijlage II (door vier lidstaten geïdentificeerd) en

overheidsdiensten (door vier lidstaten geïdentificeerd) zijn de populairste categorieën (Tabel 5).

Gezien het fundamentele belang van de veerkracht van cyberspace voor het functioneren van de economie en de samenleving als geheel heeft een aantal lidstaten besloten van de gelegenheid gebruik te maken en sectoren op te nemen die niet worden genoemd in bijlage II. Het feit dat verschillende lidstaten ervoor hebben gekozen de richtlijn inzake netwerk- en informatiebeveiliging ook op andere sectoren toe te passen, roept de vraag op of de huidige werkingssfeer van bijlage II toereikend is om te voldoen aan de doelstelling om alle aanbieders in de Unie die kritiek zijn voor de samenleving en de economie te beschermen.

2.6 De grensoverschrijdende raadplegingsprocedure

Uit hoofde van artikel 5, lid 4, van de richtlijn inzake netwerk- en informatiebeveiliging moeten de lidstaten met elkaar overleg plegen alvorens zij een definitief besluit nemen inzake aanwijzing van aanbieders die in meer dan één lidstaat diensten verlenen. De samenwerkingsgroep heeft in juli 2018 een referentiedocument gepubliceerd om de lidstaten te helpen effectief grensoverschrijdend overleg te plegen[15].

Op basis van de ontvangen informatie heeft slechts een enkele nationale autoriteit contact opgenomen met zijn tegenhanger in een andere lidstaat, en hebben slechts twee lidstaten uitvoerig contact opgenomen met andere lidstaten. Bovendien hebben slechts een paar lidstaten aangegeven op minder systematische wijze in contact te zijn getreden met andere autoriteiten. Ondanks het grote belang van grensoverschrijdende diensten in de interne markt hebben de meeste lidstaten die contact hebben opgenomen met andere lidstaten dit slechts gedaan voor een zeer beperkt aantal aanbieders. Hoewel de lidstaten weinig gebruik hebben gemaakt van de procedure, hebben veel nationale autoriteiten aangegeven belangstelling te hebben voor de grensoverschrijdende raadplegingsprocedure en beschouwen zij deze als een belangrijk element van het NIS-identificatiekader. Verschillende lidstaten hebben hun bezorgdheid geuit dat aanbieders zonder doeltreffend grensoverschrijdend overleg mogelijk te maken krijgen met een groot aantal verschillende regelgevingseisen of worden benadeeld

[15] *Identification of Operators of Essential Services – Reference document on modalities of the consultation process in cases with cross-border impact*, publicatie samenwerkingsgroep 07/2018.

ten opzichte van andere aanbieders van essentiële diensten die op de markt actief zijn in minder sterk gereguleerde sectoren.

Samen met de nationale autoriteiten heeft de Commissie een aantal redenen geïdentificeerd waarom de raadplegingsprocedure niet zo vaak wordt toegepast als de bedoeling was:

- Veel lidstaten hadden meer tijd nodig dan verwacht om aanbieders van essentiële diensten te identificeren. "Vroege toepassers" meenden daarom niet bij deze landen te kunnen aankloppen.
- Het gebrek aan veilige kanalen voor informatieoverdracht: Sommige lidstaten gaven aan terughoudend te zijn in de communicatie met hun tegenhangers omdat zij de namen van aanbieders als gerubriceerde informatie beschouwen.
- Het grote aantal bestaande grensoverschrijdende afhankelijkheden, waardoor er contact moest worden opgenomen met een flink aantal betrokken lidstaten, met name in het geval van pan-Europese aanbieders.
- Het gebrek aan overeenstemming over de doelen en werkingssfeer van grensoverschrijdende raadpleging: sommige lidstaten zien hierin slechts een middel om elkaar in kennis te stellen van geïdentificeerde aanbieders van essentiële diensten met grensoverschrijdende gevolgen, terwijl andere lidstaten van mening zijn dat deze kan dienen om drempels en regelgevingseisen op één lijn te brengen. Overweging 24 van de richtlijn lijkt erop te wijzen dat het vooral een procedure is om gezamenlijk het kritieke karakter van een aanbieder ten behoeve van het identificatieproces te beoordelen.
- Een ander probleem ontstaat als een lidstaat door twee andere lidstaten over dezelfde aanbieder wordt gecontacteerd. In dat geval kan de lidstaat in kwestie zijn regelgeving mogelijk niet tegelijkertijd aan die van beide lidstaten aanpassen. Voor dit soort gevallen voorziet overweging 24 in multilaterale besprekingen. Het is belangrijk dat de lidstaten van deze mogelijkheid gebruikmaken om consistentie te waarborgen.

2.7 Het *lex specialis*-beginsel in het identificatieproces in overweging nemen

De Commissie heeft enige inconsistentie tussen de lidstaten geïdentificeerd op het gebied van de toepassing van het *lex specialis*-beginsel. Hierdoor is de richtlijn niet overal op dezelfde wijze toegepast, wat er enerzijds toe heeft geleid dat aanbieders van essentiële diensten zijn geïdentificeerd voor sectoren waarvoor sectorspecifieke regels gelden, maar anderzijds voor

een aantal sectoren uit bijlage II onvoldoende aanbieders van essentiële diensten zijn geïdentificeerd.

In artikel 1, lid 3, wordt bepaald dat de richtlijn inzake netwerk- en informatiebeveiliging niet van toepassing is op ondernemingen die zijn onderworpen aan de eisen van de kaderrichtlijn telecommunicatie[16]. Het lijkt er echter op dat sommige lidstaten aanbieders van essentiële diensten hebben geïdentificeerd die diensten verlenen die eigenlijk onder de kaderrichtlijn telecommunicatie vallen, zoals internettoegang en telefoniediensten.

Bovendien zijn de bepalingen van de richtlijn inzake netwerk- en informatiebeveiliging over beveiligingseisen en de melding van incidenten blijkens artikel 1, lid 7, niet van toepassing op aanbieders waaraan krachtens sectorspecifieke rechtshandelingen van de Unie verplichtingen met een ten minste gelijkwaardig effect zijn opgelegd.

De meeste lidstaten hebben aanbieders van essentiële diensten in het bankwezen en de sector financiële markten geïdentificeerd, maar een klein aantal lidstaten heeft geen aanbieders van essentiële diensten geïdentificeerd omdat aanbieders volgens hen diensten verlenen die onder *leges speciales* vallen.

De Commissie is nog bezig gedetailleerde informatie te verzamelen over de toepassing van het *lex specialis*-beginsel op grond van de richtlijn inzake netwerk- en informatiebeveiliging. Zij voert momenteel diepgaand onderzoek uit naar de nationale wetgevingen en brengt bezoeken aan de lidstaten om te beoordelen hoever deze zijn met de omzetting en uitvoering, ook wat betreft de *lex specialis*-bepalingen. Op basis hiervan wil de Commissie het *lex specialis*-beginsel verder bespreken met de samenwerkingsgroep om een betere afstemming tussen de lidstaten te bereiken.

[16] Richtlijn 2002/21/EG van het Europees Parlement en de Raad van 7 maart 2002 inzake een gemeenschappelijk regelgevingskader voor elektronische-communicatienetwerken en -diensten (Kaderrichtlijn).

3. Conclusies

In dit verslag wordt de aanpak van de lidstaten voor het identificeren van aanbieders van essentiële diensten op grond van de richtlijn inzake netwerk- en informatiebeveiliging geëvalueerd. Dit moet een beeld geven van de mate van consistentie tussen de praktijken van lidstaten met het oog op de mogelijke impact van het huidige kader op de werking van de interne markt en het beheer van de risico's in verband met cyberafhankelijkheid.

Uit de uitgevoerde analyse komt naar voren dat de richtlijn inzake netwerk- en informatiebeveiliging in veel lidstaten als katalysator heeft gefungeerd en de weg heeft vrijgemaakt voor echte verandering in het institutionele en regelgevingslandschap met betrekking tot cyberbeveiliging. Daarnaast heeft de verplichting om aanbieders van essentiële diensten te identificeren geleid tot een uitgebreide beoordeling van de risico's voor aanbieders die zich bezighouden met kritieke activiteiten en voor moderne netwerk- en informatiesystemen in bijna alle lidstaten. Dit kan als een prestatie voor de Unie als geheel worden beschouwd conform de doelstellingen van de richtlijn.

In dit verslag heeft de Commissie de nationale identificatiemethoden, de diensten die nationale autoriteiten als essentieel beschouwen, de identificatiedrempels en de aantallen aanbieders van essentiële diensten die in de verschillende sectoren die onder de richtlijn vallen zijn geïdentificeerd tegen het licht gehouden:

- **De lidstaten hebben verschillende methoden ontwikkeld** voor de identificatie van aanbieders van essentiële diensten (punt 2.1), maar ook voor de definitie van essentiële diensten en het vaststellen van drempels. Dit kan negatieve gevolgen hebben voor de consistente toepassing van de NIS-bepalingen binnen de Unie met mogelijke gevolgen voor de correcte werking van de interne markt en de effectieve aanpak van cyberafhankelijkheden.

- Daarnaast lijkt het erop dat **lidstaten een essentiële dienst op grond van de richtlijn inzake netwerk- en informatiebeveiliging op uiteenlopende wijze interpreteren**, en passen zij verschillende niveaus van granulariteit toe (zie punt 2.2). Dat maakt het lastig om de lijsten van essentiële diensten te vergelijken. Bovendien **bestaat het risico dat de werkingssfeer van de richtlijn gefragmenteerd raakt**: sommige aanbieders krijgen te maken met aanvullende regelgeving (omdat zij in hun betreffende lidstaat zijn geïdentificeerd), terwijl andere aanbieders die vergelijkbare diensten verlenen hiervan

verschoond blijven (omdat zij niet zijn geïdentificeerd). Om deze inconsistenties aan te pakken, zouden verdere inspanningen op basis van de ervaringen van de lidstaten kunnen leiden tot een beter afgestemde lijst van essentiële diensten.

- In het verslag zijn ook aanzienlijke inconsistenties vastgesteld in de manier waarop de lidstaten drempels toepassen (punt 2.3). Dit probleem zou kunnen worden aangepakt door **drempels op EU-niveau verder op één lijn te brengen**. Dit zou bijvoorbeeld gedaan kunnen worden aan de hand van sectorale werkstromen onder de paraplu van de samenwerkingsgroep, waarbij rekening wordt gehouden met specifieke nationale kenmerken, zoals de bijzondere behoeften van kleine lidstaten.

- Het feit dat sommige landen gebruik hebben gemaakt van de mogelijkheid om essentiële diensten in aanvullende sectoren of deelsectoren te identificeren die niet worden genoemd in bijlage II **toont aan dat er naast de sectoren uit de richtlijn inzake netwerk- en informatiebeveiliging ook andere sectoren zijn die mogelijk kwetsbaar zijn voor cyberincidenten** (punt 2.5). De identificatie van aanbieders van essentiële diensten in sectoren zoals informatie-infrastructuren, financiële diensten die niet worden verleend door entiteiten genoemd in bijlage II of de overheid kan de veerkracht van cyberspace van organisaties in deze sectoren verbeteren. Als echter slechts een deel van de lidstaten aanbieders van essentiële diensten in deze sectoren identificeert, kan dit negatieve gevolgen hebben voor de interne markt en het gelijke speelveld waarvoor deze juist zou moeten zorgen.

De vele methoden en beste praktijken die nationale autoriteiten hebben ontwikkeld, zijn van bijzondere waarde en moeten in de toekomst in aanmerking worden genomen, bijvoorbeeld bij de werkzaamheden van de samenwerkingsgroep en de voortdurende identificatie van aanbieders van essentiële diensten door de lidstaten. De huidige mate van diversiteit kan echter een negatief effect hebben op de verwezenlijking van de doelstellingen van de richtlijn.

De Commissie komt tot de voorlopige conclusie dat de richtlijn inzake netwerk- en informatiebeveiliging weliswaar een cruciaal proces in gang heeft gezet om de risicobeheerpraktijken van aanbieders in kritieke sectoren uit te breiden en te verbeteren, maar dat de identificatie van aanbieders van essentiële diensten binnen de Unie nog zeer gefragmenteerd is. Dit is met name te wijten aan het ontwerp van de richtlijn, en deels aan de verschillende uitvoeringsmethoden die de lidstaten toepassen.

De lidstaten moeten proberen de bepalingen van de richtlijn inzake netwerk- en informatiebeveiliging zo consistent mogelijk toe te passen en zoveel mogelijk gebruikmaken van de richtsnoeren die de Commissie en de samenwerkingsgroep hebben opgesteld. De Commissie heeft daarom verschillende nationale maatregelen geïdentificeerd waarmee de in dit verslag beschreven problemen kunnen worden verlicht:

- Veel lidstaten hebben het proces van de identificatie van aanbieders van essentiële diensten niet afgerond binnen het tijdsbestek dat in de richtlijn is vastgesteld. Op de datum van publicatie van dit verslag hadden 23 lidstaten alle gegevens verstrekt die zij uit hoofde van artikel 5, lid 7, moesten indienen. Nog eens vijf lidstaten hadden gedeeltelijke informatie verstrekt. De Commissie **dringt er bij de nationale autoriteiten die zijn belast met de identificatie op aan het proces zo snel mogelijk af te ronden** en de benodigde informatie zo spoedig mogelijk aan de Commissie te verstrekken.

- De bevoegde autoriteiten moeten hun lijsten van essentiële diensten regelmatig evalueren en **ervoor zorgen dat alle bestaande essentiële diensten worden geïdentificeerd**, zodat het aantal "zeer uiteenlopende" essentiële diensten binnen de interne markt wordt teruggebracht.

- De lidstaten moeten vaker **overleg met elkaar plegen om hun drempels waar mogelijk op elkaar af te stemmen**, met name in sectoren met een sterk grensoverschrijdende dimensie zoals vervoer of energie. Dit kan worden bereikt middels de grensoverschrijdende raadplegingsprocedure uit artikel 5, lid 4, van de richtlijn inzake netwerk- en informatiebeveiliging, maar ook door beter gebruik te maken van de bestaande structuren van de samenwerkingsgroep.

- Nationale autoriteiten moeten overleg plegen om te waarborgen dat aan grensoverschrijdende aanbieders **vergelijkbare eisen worden gesteld op het gebied van beveiliging en de melding van incidenten** in de interne markt. Ook moeten lidstaten contact opnemen met deze aanbieders om meer informatie te verzamelen over verschillen in regelgeving. Een verbeterde veerkracht van cyberspace mag niet leiden tot gefragmenteerde regelgeving. Waar nodig moeten de lidstaten ook multilaterale besprekingen met elkaar voeren overeenkomstig overweging 24 van de richtlijn inzake netwerk- en informatiebeveiliging.

Naast de nationale maatregelen zijn er een aantal maatregelen die mogelijk op Unieniveau kunnen worden genomen en die tot meer samenhang zouden leiden. De Commissie zal besprekingen initiëren om het ongelijke en soms gefragmenteerde identificatielandschap te verbeteren. Mogelijke maatregelen die kunnen worden genomen zijn:

- **De rol van de NIS-samenwerkingsgroep moet worden versterkt** om tot overeenstemming te komen over hoe de richtlijn op een consistentere manier kan worden uitgevoerd. Hiertoe zal de Commissie voorstellen dat bij de bestaande speciale werkstroom voor de identificatie van aanbieders van essentiële diensten de **richtsnoeren snel worden geëvalueerd om bestaande inconsistenties beter aan te pakken**. De samenwerkingsgroep moet ook onderzoeken of er aanvullende sectorale werkstromen kunnen worden opgezet[17] om de samenhang tussen de lidstaten te vergroten en of er gebruik kan worden gemaakt van een communicatietool op maat om de samenwerking binnen de groep te versterken.

- Slechts een zeer klein aantal lidstaten maakt momenteel gebruik van de **grensoverschrijdende raadplegingsprocedure** voor het identificeren van aanbieders die essentiële diensten in meer dan één lidstaat verlenen. Om de informatie-uitwisseling te bevorderen, moet de samenwerkingsgroep haar "reference document on the modalities of the consultation process in cases with cross-border impact" herzien en overeenstemming bereiken over een consistente interpretatie van de werkingssfeer, doelstellingen en procedures van een dergelijke raadpleging. De Commissie zal ook manieren onderzoeken waarop **bevoegde autoriteiten veilig informatie kunnen uitwisselen**.

- Er lijkt een zekere mate van inconsistentie tussen de lidstaten te zijn in de toepassing van de bepalingen van de richtlijn inzake *lex specialis*. De Commissie zal derhalve gebruikmaken van de structuren van de samenwerkingsgroep om **gevallen te bespreken waarin het *lex specialis*-beginsel mogelijk niet correct is toegepast**.

Op Unieniveau genomen maatregelen moeten zorgen voor een samenhangend kader waarbij rekening wordt gehouden met zowel sectorale activiteiten die tot doel hebben specifieke of

[17] In juni 2018 en juli 2019 zijn werkstromen voor energie en digitale infrastructuren opgezet.

hogere eisen te stellen op het gebied van cyberbeveiliging als met andere Europese wetgeving.

4. Bijlagen

4.1 Overzicht van de beschikbare gegevens per lidstaat

Lidstaat	Indieningsdatum	Dienstenlijst	Aantal aanbieders van essentiële diensten	Drempels
AT	Te late indiening	Afgeleverd	ONTBREEKT	Afgeleverd
BE	Te late indiening	Afgeleverd	ONTBREEKT	ONTBREEKT
BG	Te late indiening	Afgeleverd	Afgeleverd	Afgeleverd
CY	Op tijd	Afgeleverd	Afgeleverd	Afgeleverd
CZ	Te late indiening	Afgeleverd	Afgeleverd	Afgeleverd
DE	Op tijd	Afgeleverd	Afgeleverd	Afgeleverd
DK	Op tijd	Afgeleverd	Afgeleverd	Afgeleverd
EE	Op tijd	Afgeleverd	Afgeleverd	Afgeleverd
EL	Te late indiening	Afgeleverd	Afgeleverd	Afgeleverd
ES	Op tijd	Afgeleverd	Afgeleverd	Afgeleverd
FI	Op tijd	Afgeleverd	Afgeleverd	Afgeleverd
FR	Op tijd	Afgeleverd	Afgeleverd	Geen officiële drempels
HR	Op tijd	Afgeleverd	Afgeleverd	Afgeleverd
HU	Op tijd	Gedeeltelijk afgeleverd	Gedeeltelijk afgeleverd	Gedeeltelijk afgeleverd
IE	Te late indiening	Afgeleverd	Afgeleverd	Afgeleverd
IT	Te late indiening	Afgeleverd	Afgeleverd	Afgeleverd
LT	Op tijd	Afgeleverd	Afgeleverd	Afgeleverd
LU	Te late indiening	Afgeleverd	Afgeleverd	Afgeleverd
LV	Te late indiening	Afgeleverd	Afgeleverd	Afgeleverd
MT	Te late indiening	Afgeleverd	Afgeleverd	Afgeleverd
NL	Te late indiening	Afgeleverd	Afgeleverd	Afgeleverd
PL	Op tijd	Afgeleverd	Afgeleverd	Afgeleverd
PT	Op tijd	Afgeleverd	Afgeleverd	Afgeleverd
RO	Te late indiening	Afgeleverd	Gedeeltelijk afgeleverd	ONTBREEKT
SE	Op tijd	Afgeleverd	Afgeleverd	Afgeleverd
SI	Te late indiening	Afgeleverd	ONTBREEKT	Afgeleverd
SK	Op tijd	Afgeleverd	Afgeleverd	Afgeleverd
UK	Op tijd	Afgeleverd	Afgeleverd	Afgeleverd

4.2 Geïdentificeerde aantal diensten en aanbieders van essentiële diensten per lidstaat

Lidstaat	Geïdentificeerde aanbieders van essentiële diensten	Diensten van bijlage II	Aanvullende diensten
AT	0	46	0
BE	0	31	0
BG	185	30	3
CY	20	29	17
CZ	50	31	12
DE	573	15	12
DK	128	39	0
EE	137	18	6
EL	67	30	0
ES	132	55	18
FI	10897[18]	20	0
FR	127	70	20
HR	85	49	2
HU	42	12	0
IE	64	26	0
IT	553	37	0
LT	22	37	0
LU	49	21	0
LV	66	18	0
MT	36	29	2
NL	42	12	0
PL	142	87	0
PT	1250	26	0
RO	86	77	0
SE	326	27	0
SI	0	34	2
SK	273	28	7
UK	470	34	0

[18] Door de in Finland gebruikte identificatiemethode is in de gezondheidszorg een groot aantal aanbieders van essentiële diensten geïdentificeerd.

4.3 Door de lidstaten geïdentificeerde diensten in de deelsector elektriciteit

Lidstaat	Geïdentificeerde diensten
AT	– Elektriciteitsopwekkingsinstallaties – Controlesystemen in opwekkingsinstallaties – Distributienetten – Transmissienetwerken
BE	– Productie-, vervoers- en distributiebedrijven – Elektriciteitsdistributie – Elektriciteitstransport
BG	– Productie van elektriciteit – Transmissie van elektriciteit – Werking, onderhoud en ontwikkeling van een elektriciteitstransmissiesysteem – Distributie van elektriciteit – Waarborgen van de werking en het onderhoud van een distributiesysteem voor elektrische energie – Elektriciteitsmarkt
CY	– Opwekking/levering – Distributie/transmissie – Diensten in de elektriciteitsmarkt
CZ	– Elektriciteitsopwekking – Verkoop van elektriciteit – Transmissienetexploitatie – Distributienetexploitatie
DE	– Stroomvoorziening
DK	– Elektriciteitstransmissie – Elektriciteitsdistributie – Elektriciteitsopwekking
EE	– Levering van elektriciteit
EL	– Levering van elektriciteit – Elektriciteitsdistributie – Elektriciteitstransmissie
ES	– Elektriciteitsopwekking – Elektriciteitstransmissie – Elektriciteitsdistributie – Centra voor het beheer en de regeling van elektrische systemen
FI	– Transmissiedienst – Distributie van elektriciteit in het distributienet – Levering van elektriciteit via hoogspanningsdistributienetten
FR	– Verkoop of wederverkoop van elektriciteit aan grootafnemers en eindklanten – Distributie van elektriciteit – Transmissie van elektriciteit
HR	– Productie van elektriciteit – Transmissie van elektriciteit – Distributie van elektriciteit
HU	– Elektriciteit
IE	– Distributiesysteembeheerders – Elektriciteitsbedrijven – Transmissiesysteembeheerders
IT	– Opwekking – Handel – Transmissie – Distributie
LT	– Elektriciteitsopwekkingsdienst – Elektriciteitstransmissiedienst – Elektriciteitsdistributiedienst – Elektriciteitsleveringsdienst

LU	– Levering van elektriciteit – Elektriciteitsdistributie – Elektriciteitstransmissie
LV	– Elektriciteitsopwekking – Elektriciteitsdistributie – Elektriciteitstransmissie
MT	– Elektriciteitsvoorziening aan consumenten – Transmissie en/of distributie van elektriciteit aan consumenten – Elektriciteitsopwekking voor consumenten
NL	– Transmissie en distributie van elektriciteit
PL	– Opwekking van elektrische stroom – Transmissie van elektrische stroom – Distributie van elektrische stroom – Handel in elektrische stroom – Opslag van elektrische stroom – Kwaliteitsborgingsdiensten en beheer van energie-infrastructuur
PT	– Distributiesysteembeheerders – Transmissiesysteembeheerders
RO	– Productie van elektriciteit – Levering van elektriciteit aan consumenten – Beheer van gecentraliseerde elektriciteitsmarkten – Transport van elektriciteit – Beheer van het stroomsysteem – Distributie van elektriciteit
SE	– Transmissiesysteembeheerders – Distributiesysteembeheerders – Productie – Groothandel
SI	– Productie van elektriciteit in waterkrachtcentrales – Productie van elektriciteit in thermische elektriciteitscentrales, kerncentrales – Transmissie van elektriciteit – Distributie van elektriciteit – Handel in elektriciteit
SK	– Elektriciteitsbedrijf – Transmissiesysteembeheerder – Distributiesysteembeheerder
UK	– Levering van elektriciteit – Elektriciteitstransmissie – Elektriciteitsdistributie

4.4 Door de lidstaten geïdentificeerde diensten in de deelsector spoorvervoer

Lidstaat	Geïdentificeerde diensten
AT	– Spoorweginfrastructuren – Goederenvervoer per spoor – Personenvervoer per spoor – Stations
BE	– Infrastructuurbeheerders – Spoorwegondernemingen
BG	– Levering, instandhouding en beheer van dienstvoorzieningen – Spoorvervoer door spoorwegmaatschappijen – Verstrekking van richtsnoeren voor spoorvervoer
CY	Geen identificatie in deze deelsector
CZ	– Spoorwegexploitatie – Exploitatie van spoorvervoer of dienstvoorziening
DE	– Spoor
DK	– Spoorweginfrastructuurbeheer – Spoorvervoer
EE	– Spoorweginfrastructuurbeheerder – Vervoersdienst per spoor
EL	– Spoorweginfrastructuurbeheer – Spoorwegdiensten
ES	– Spoorwegdienstbeheer – Spoorvervoerbeheer – Spoorwegnetwerkdiensten – Spoorinformatie- en telecommunicatiebeheer
FI	– Infrastructuurbeheer door de overheid – Verkeersleidingdiensten
FR	– Spoorwegdiensten – Verkeersleiding van het spoorvervoer – Onderhoud van infrastructuur – Vracht en gevaarlijke materialen – Personenvervoer – Onderhoud van rollend materieel – Metro’s en tramdiensten (met inbegrip van ondergrondse diensten)
HR	– Beheer en instandhouding van spoorweginfrastructuur, met inbegrip van verkeersleiding en subsysteem besturing en seingeving – Spoorvervoersdiensten van goederen en/of personen – Beheer van dienstvoorzieningen en dienstverlening in dienstvoorzieningen – Aanvullende dienstverlening voor spoorvervoer van goederen of personen
HU	Geen identificatie in deze deelsector
IE	– Infrastructuurbeheerders – Spoorwegondernemingen
IT	Geen identificatie in deze deelsector
LT	– Vervoer van personen en bagage per spoor – Goederenvervoer per spoor – Ontwikkeling, beheer en onderhoud van spoorweginfrastructuren
LU	– Spoorweginfrastructuurbeheer – Goederen- en personenvervoer per spoor
LV	N.v.t.
MT	N.v.t.
NL	Geen identificatie in deze deelsector

PL	– Treindienstregelingen opstellen – Personenvervoer per spoor – Goederenvervoer per spoor
PT	– Infrastructuurbeheerders zoals gedefinieerd in artikel 3, punt 2, van Richtlijn 2012/34/EU van het Europees Parlement en de Raad. – Spoorwegondernemingen zoals gedefinieerd in artikel 3, punt 1, van Richtlijn 2012/34/EU, inclusief exploitanten van dienstvoorzieningen zoals gedefinieerd in artikel 3, punt 12, van Richtlijn 2012/34/EU.
RO	– Verkeersleiding – Goederenvervoer – Vervoer van gevaarlijke stoffen – Personenvervoer – Metro- en tramdiensten – Onderhoud van spoorweginfrastructuur – Onderhoud van rollend materieel
SE	– Infrastructuurbeheer – Passagiersvervoer – Goederenvervoer
SI	– Interlokaal personenvervoer per spoor – Goederenvervoer per spoor – Dienstactiviteiten die voortvloeien uit vervoer over land (exploitatie van stations enz.)
SK	– Infrastructuurexploitanten – Spoorwegmaatschappijen
UK	– Spoorwegdiensten – Hogesnelheidsspoorwegdiensten – Metro’s en tramdiensten (met inbegrip van ondergrondse diensten) – Internationale spoorwegdiensten