EUROPESE
COMMISSIE

Brussel, 4.10.2017
COM(2017) 476 final

ANNEX 1

NOTE
This language version reflects the corrections done to the original EN version transmitted under COM(2017) 476 final of 13.9.2017 and retransmitted (with corrections) under COM(2017) 476 final/2 of 4.10.2017

BIJLAGE

bij

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

INHOUDSOPGAVE

BIJLAGE 4
1. Inleiding 4
2. Nationale strategie voor de beveiliging van netwerk- en informatiesystemen 5
2.1. Reikwijdte van de nationale strategie 5
2.2. Inhoud en procedure voor de vaststelling van de nationale strategieën 6
2.3. Procedure en aan te pakken problemen 6
2.4. Concrete stappen die de lidstaten moeten nemen vóór de omzettingstermijn 9
3. NIS-richtlijn: nationale bevoegde autoriteiten, centrale contactpunten en Computer Security Incident Response Teams (CSIRT's) 10
3.1. Soort autoriteiten 11
3.2. Openbaarmaking en andere relevante aspecten 12
3.3. Artikel 9 van de NIS-richtlijn: Computer Security Incident Response Teams (CSIRT's) 17
3.4. Taken en voorschriften 17
3.5. Bijstand voor de ontwikkeling van CSIRT's 18
3.6. Rol van het centrale contactpunt 19
3.7. Sancties 20
4.1. Aanbieders van essentiële diensten 20
4.1.1. Soort entiteiten als vermeld in bijlage II bij de NIS-richtlijn 21
4.1.2. Identificatie van aanbieders van essentiële diensten 23
4.1.3. Opneming van andere sectoren 23
4.1.4. Jurisdictie 24
4.1.5. Aan de Commissie te verstrekken informatie 25
4.1.6. Hoe moet het identificatieproces worden uitgevoerd? 25
4.1.7. Grensoverschrijdend overlegproces 31
4.2. Beveiligingseisen 31
4.3 Meldingseisen 32
4.4. NIS-richtlijn, bijlage III: digitaledienstverleners 32
4.4.1. Categorieën digitaledienstverleners 33
4.4.2. Beveiligingseisen 36
4.4.3. Meldingseisen 36
4.4.4. Risicogebaseerde regelgevende aanpak 36
4.4.5. Jurisdictie 37

4.4.6. Vrijstelling van beveiligings- en meldingsverplichtingen voor digitaledienstverleners van beperkte omvang 37
5. Verhouding tussen NIS-richtlijn en andere wetgeving 37
5.1. NIS-richtlijn, artikel 1, lid 7: *lex specialis*-bepaling 38
5.2. NIS-richtlijn, artikel 1, lid 3: telecomaanbieders en verleners van vertrouwensdiensten 42
6. Bekendgemaakte documenten in verband met nationale cyberbeveiligingsstrategieën 43
7. Lijst van goede praktijken en aanbevelingen van het Enisa 47

BIJLAGE

1. Inleiding

Deze bijlage heeft tot doel bij te dragen tot een doeltreffende toepassing, uitvoering en handhaving van Richtlijn (EU) 2016/1148 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie[1] (hierna "de NIS-richtlijn" of "de richtlijn" genoemd) en de lidstaten te helpen met het oog op een doeltreffende toepassing van het EU-recht. Deze bijlage heeft met name drie specifieke doelstellingen: a) de nationale autoriteiten meer duidelijkheid bieden over de voor hen geldende verplichtingen die zijn vastgesteld in de richtlijn, b) ervoor zorgen dat de voor bepaalde entiteiten geldende verplichtingen inzake beveiliging en melding van incidenten uit hoofde van de richtlijn doeltreffend worden gehandhaafd, en c) in het algemeen bijdragen aan de rechtszekerheid voor alle betrokken actoren.

Hiertoe verschaft deze bijlage richtsnoeren over de volgende aspecten, die van cruciaal belang zijn om de doelstelling van de NIS-richtlijn te verwezenlijken, namelijk het waarborgen van een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de EU die de werking van onze samenleving en economie ondersteunen:

- de verplichting voor de lidstaten om een nationale strategie voor de beveiliging van netwerk- en informatiesystemen vast te stellen (deel 2);
- de oprichting van nationale bevoegde autoriteiten, centrale contactpunten en Computer Security Incident Response Teams (deel 3);
- de eisen inzake beveiliging en melding van incidenten die van toepassing zijn op aanbieders van essentiële diensten en digitaledienstverleners (deel 4); en
- de verhouding tussen de NIS-richtlijn en andere wetgeving (deel 5).

De Commissie heeft deze richtsnoeren opgesteld aan de hand van input en analyses die zijn verzameld tijdens de voorbereiding van de richtlijn, en input van het Agentschap van de Europese Unie voor netwerk- en informatiebeveiliging (Enisa) en de samenwerkingsgroep. De ervaringen van bepaalde lidstaten zijn eveneens in aanmerking genomen. Waar nodig heeft de Commissie rekening gehouden met de leidende beginselen voor de uitlegging van het EU-recht: de formulering, de context en de doelstellingen van de NIS-richtlijn. Aangezien de richtlijn nog niet is omgezet, bestaat hierover nog geen rechtspraak van het Hof van Justitie van de Europese Unie (HvJ-EU) of van de nationale rechtbanken. Het is derhalve niet mogelijk om jurisprudentie als leidraad te gebruiken.

Door deze informatie in één document te bundelen, krijgen de lidstaten een goed beeld van de richtlijn en kunnen ze rekening houden met deze informatie bij het uitwerken van hun

[1] 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. De richtlijn is op 8 augustus 2016 in werking getreden.

nationale wetgeving. Tegelijkertijd beklemtoont de Commissie dat deze bijlage niet bindend is en niet bedoeld is om nieuwe regels te creëren. De uiteindelijke bevoegdheid om het EU-recht uit te leggen ligt bij het Hof.

2. Nationale strategie voor de beveiliging van netwerk- en informatiesystemen

Overeenkomstig artikel 7 van de NIS-richtlijn moeten de lidstaten een nationale strategie voor de beveiliging van netwerk- en informatiesystemen vaststellen die gelijkwaardig kan worden geacht aan de term "nationale cyberbeveiligingsstrategie" (NCSS). De functie van een nationale strategie bestaat erin de strategische doelstellingen en de passende beleids- en regelgevingsmaatregelen op het gebied van cyberveiligheid vast te stellen. Het concept van een NCSS wordt internationaal en in Europa veelvuldig gebruikt, met name in het kader van de werkzaamheden op het gebied van nationale strategieën van het Enisa en de lidstaten, die onlangs een geactualiseerde gids voor goede praktijken voor NCSS hebben opgesteld[2].

In dit deel licht de Commissie toe op welke manier de paraatheid van de lidstaten wordt versterkt door de in de NIS-richtlijn vastgestelde verplichting om krachtige nationale strategieën voor de beveiliging van netwerk- en informatiesystemen vast te stellen (artikel 7). In dit deel worden de volgende aspecten behandeld: a) de reikwijdte van de strategie, en b) de inhoud en de vaststellingsprocedure.

Zoals hieronder verder wordt uiteengezet, is de correcte omzetting van artikel 7 van de NIS-richtlijn van fundamenteel belang om de doelstellingen van de richtlijn te verwezenlijken, en hiervoor moeten voldoende financiële en personele middelen worden uitgetrokken.

2.1. Reikwijdte van de nationale strategie

Overeenkomstig artikel 7 geldt de verplichting om een NCSS vast te stellen alleen voor de in bijlage II genoemde sectoren (namelijk energie, vervoer, bankwezen, infrastructuur voor de financiële markt, gezondheidszorg, levering en distributie van drinkwater en digitale infrastructuur) en de in bijlage III bedoelde diensten (onlinemarktplaats, onlinezoekmachine en cloudcomputerdiensten).

Het beginsel van minimumharmonisatie is uitdrukkelijk opgenomen in artikel 3 van de richtlijn, op grond waarvan de lidstaten bepalingen kunnen vaststellen of handhaven met het oog op het tot stand brengen van een hoger niveau van beveiliging van netwerk- en informatiesystemen. Aangezien dit beginsel van toepassing is op de verplichting om een NCSS vast te stellen, kunnen de lidstaten meer sectoren en diensten opnemen dan die welke zijn bedoeld in de bijlagen II en III bij de richtlijn.

Volgens het standpunt van de Commissie en in het licht van de doelstelling van de NIS-richtlijn, namelijk een hoog gemeenschappelijk niveau van beveiliging van netwerk- en

[2] Enisa, *National Cyber-Security Strategy Good Practice*, 2016. Beschikbaar op https://www.enisa.europa.eu/publications/ncss-good-practice-guide.

informatiesystemen in de Unie tot stand brengen[3], is het raadzaam een nationale strategie te ontwikkelen die betrekking heeft op alle relevante aspecten van de samenleving en de economie, en niet alleen op de sectoren en de digitale diensten die zijn opgenomen in respectievelijk bijlage II en III bij de NIS-richtlijn. Dit stemt overeen met internationale beste praktijken (zie de verderop vermelde richtsnoeren van de ITU en de analyse van de OESO) en de NIS-richtlijn.

Zoals hieronder nader wordt toegelicht, is dit met name het geval voor overheidsinstanties die bevoegd zijn voor sectoren en diensten die niet zijn opgenomen in de bijlagen II en III bij de richtlijn. Overheidsinstanties kunnen te maken krijgen met gevoelige informatie, waardoor ze onder een NCSS en beheersplannen moeten vallen om lekken te vermijden en ervoor te zorgen dat deze informatie naar behoren wordt beschermd.

2.2. Inhoud en procedure voor de vaststelling van de nationale strategieën

Op grond van artikel 7 van de NIS-richtlijn moet een NCSS ten minste het volgende omvatten:

i) de doelstellingen en de prioriteiten van de nationale strategie voor de beveiliging van netwerk- en informatiesystemen;
ii) een governancekader ter verwezenlijking van de doelstellingen en de prioriteiten van de nationale strategie;
iii) de bepaling van maatregelen inzake paraatheid, reactie en herstel, met inbegrip van samenwerking tussen de publieke en de particuliere sector;
iv) een vermelding van de relevante onderwijs-, bewustmakings- en opleidingsprogramma's;
v) een vermelding van de plannen voor onderzoek en ontwikkeling;
vi) een risicobeoordelingsplan om risico's te identificeren; en
vii) een lijst van de actoren die betrokken zijn bij de uitvoering van de strategie.

Noch in artikel 7, noch in de overeenkomstige overweging 29 worden de vereisten voor de vaststelling van een NCSS uiteengezet of wordt er dieper ingegaan op de inhoud van de NCSS. Wat de procedure en de aanvullende elementen in verband met de inhoud van de NCSS betreft, beschouwt de Commissie de hieronder beschreven aanpak als een geschikte manier om een NCSS vast te stellen. Dit is gebaseerd op de analyse van de lidstaten en de ervaringen van derde landen met de manier waarop de lidstaten hun eigen strategieën hebben ontwikkeld. Een andere bron van informatie is het opleidingsinstrument voor NCSS van het Enisa, dat beschikbaar is op de website in de vorm van videoclips en downloadbare media[4].

2.3. Procedure en aan te pakken problemen

De procedure voor de opstelling en daaropvolgende vaststelling van een nationale strategie is complex en veelzijdig, en kan alleen doeltreffend en succesvol zijn indien deskundigen op het gebied van cyberbeveiliging, het maatschappelijk middenveld en het nationale politieke

[3] Zie artikel 1, lid 1.
[4] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-training-tool

proces er voortdurend bij worden betrokken. Administratieve ondersteuning op hoog niveau, ten minste op het niveau van de staatssecretaris of een gelijkwaardig niveau in het eerstverantwoordelijke ministerie, en politieke steun zijn een noodzakelijke voorwaarde. Om een NCSS met succes vast te stellen, kan het volgende vijfstappenplan (zie figuur 1) worden gevolgd:

Stap 1 - **Vaststelling van leidende beginselen en strategische doelstellingen die voortvloeien uit de strategie**

In de eerste plaats moeten de nationale bevoegde autoriteiten enkele belangrijke elementen vaststellen die zullen worden opgenomen in de NCSS, ze moeten namelijk nagaan wat de gewenste resultaten zijn, *"doelstellingen en prioriteiten"* genoemd in de richtlijn (artikel 7, lid 1, onder a)), op welke manier deze resultaten het nationale beleid op sociaal en economisch vlak aanvullen, en of ze verenigbaar zijn met de rechten en plichten die voortvloeien uit het lidmaatschap van de Europese Unie. De doelstellingen moeten specifiek, meetbaar, haalbaar, realistisch en tijdgebonden (SMART) zijn. Een voorbeeld: "*We zullen ervoor zorgen dat deze [tijdgebonden] strategie gebaseerd is op een strikte en volledige reeks maatstaven aan de hand waarvan we de vooruitgang meten op het vlak van de resultaten die we moeten behalen*"[5].

Het bovenstaande omvat ook een politieke beoordeling van de vraag of een aanzienlijk budget kan worden vrijgemaakt om de strategie uit te voeren. Het omvat ook een beschrijving van de beoogde reikwijdte van de strategie en de verschillende categorieën belanghebbenden uit de publieke en particuliere sector die betrokken moeten worden bij de ontwikkeling van de verschillende doelstellingen en maatregelen.

Deze eerste stap kan worden gerealiseerd door middel van specifieke workshops met hoge ministeriële ambtenaren en politici, onder leiding van cyberdeskundigen met professionele communicatievaardigheden die kunnen toelichten wat de gevolgen voor een moderne digitale economie en samenleving zouden zijn als er geen of een zwakke cyberbeveiliging tot stand wordt gebracht.

Stap 2 - **Uitwerking van de inhoud van de strategie**

De strategie moet ondersteunende maatregelen, tijdgebonden acties en kernprestatie-indicatoren bevatten voor de daaruit voortvloeiende evaluatie, verfijning en verbetering na een vastgestelde uitvoeringsperiode. Deze maatregelen dienen ter ondersteuning van de doelstellingen, prioriteiten en resultaten die zijn vastgesteld als leidende beginselen. In artikel 7, lid 1, onder c), van de NIS-richtlijn is bepaald dat er ondersteunende maatregelen moeten worden vastgesteld.

Er wordt aanbevolen om een stuurgroep op te richten die wordt voorgezeten door het eerstverantwoordelijke ministerie om het ontwikkelingsproces te beheren en makkelijker input te leveren. Dit kan worden bereikt door middel van een aantal redactiegroepen van

[5] Passage uit de nationale cyberbeveiligingsstrategie van het VK, 2016-2021, blz. 67.

betrokken ambtenaren en deskundigen rond belangrijke algemene thema's, bijvoorbeeld risicobeoordeling, noodplanning, incidentenbeheer, vaardighedenontwikkeling, bewustmaking, onderzoek en industriële ontwikkeling, enzovoort. Elke sector (bijvoorbeeld energie, vervoer, enz.) moet ook afzonderlijk nagaan wat de gevolgen van de opneming in de richtlijn zijn, met inbegrip van middelentoewijzing, en moet de aangewezen aanbieders van essentiële diensten en belangrijke digitaledienstverleners betrekken bij het vaststellen van prioriteiten en het indienen van voorstellen in het kader van het ontwikkelingsproces. Het is van essentieel belang dat de sectorale belanghebbenden hierbij worden betrokken aangezien de richtlijn op een geharmoniseerde wijze moet worden uitgevoerd in de verschillende sectoren, waarbij tegelijkertijd ruimte wordt gelaten voor differentiatie per sector.

Stap 3 - **Ontwikkeling van een governancekader**

Met het oog op efficiëntie en doeltreffendheid moet het governancekader gebaseerd zijn op de voornaamste belanghebbenden, de vastgestelde prioriteiten in het ontwikkelingsproces en de beperkingen en de context van de nationale administratieve en politieke structuren. Het is wenselijk om rechtstreeks verslag uit te brengen aan het politieke niveau, waarbij het kader het vermogen heeft om besluiten te vormen en middelen toe te wijzen, en input te krijgen van deskundigen op het gebied van cyberbeveiliging en belanghebbenden uit de sector. In artikel 7, lid 1, onder b), van de NIS-richtlijn wordt verwezen naar het governancekader en worden *"de verantwoordelijkheden van de overheidsorganen en de andere betrokken actoren"* specifiek vermeld.

Stap 4 - **Ontwikkeling en beoordeling van de ontwerpstrategie**

In deze fase moet de ontwerpstrategie worden ontwikkeld en beoordeeld aan de hand van de sterke punten, zwakke punten, kansen en bedreigingen (SWOT-analyse) om na te gaan of de inhoud ervan moet worden herzien. Na de interne beoordeling moeten de belanghebbenden geraadpleegd worden. Een openbare raadpleging is eveneens essentieel om het publiek te wijzen op het belang van de voorgestelde strategie, input te krijgen uit alle mogelijke bronnen en steun te zoeken voor de middelen die nodig zijn om de strategie vervolgens uit te voeren.

Stap 5 – **Formele vaststelling**

Deze laatste stap omvat de formele vaststelling op politiek niveau met een toereikend budget waaruit blijkt hoeveel belang de betrokken lidstaat hecht aan cyberbeveiliging. Om de doelstellingen van de NIS-richtlijn te verwezenlijken, moedigt de Commissie de lidstaten aan informatie over het budget op te nemen in het document over de nationale strategie dat aan de Commissie moet worden verstrekt overeenkomstig artikel 7, lid 3. Toezeggingen met betrekking tot het budget en de nodige personele middelen zijn van het uiterste belang om de strategie en de richtlijn doeltreffend uit te voeren. Aangezien cyberbeveiliging een nog relatief nieuw beleidsterrein is dat snel aan belang wint, zijn er in de meeste gevallen nieuwe investeringen nodig, ook al moet er in het algemeen bezuinigd en bespaard worden op overheidsfinanciën.

Verschillende openbare en academische bronnen, zoals het Enisa[6], het ITU[7], de OESO[8], het wereldwijde forum inzake cyberexpertise en de universiteit van Oxford[9], verstrekken advies over de procedure en de inhoud van nationale strategieën.

2.4. Concrete stappen die de lidstaten moeten nemen vóór de omzettingstermijn

Voorafgaand aan de vaststelling van de richtlijn hadden bijna alle lidstaten[10] reeds documenten gepubliceerd die werden aangemerkt als een NCSS. Deel 6 van deze bijlage bevat een lijst van de huidige strategieën van elke lidstaat[11]. Deze strategieën omvatten doorgaans strategische beginselen, richtsnoeren, doelstellingen en, in sommige gevallen, specifieke maatregelen om de risico's in verband met cyberbeveiliging te beperken.

Aangezien sommige van deze strategieën zijn aangenomen vóór de vaststelling van de NIS-richtlijn, is het mogelijk dat ze niet alle in artikel 7 vastgestelde elementen bevatten. Met het oog op een correcte omzetting moeten de lidstaten een kloofanalyse uitvoeren door de inhoud van hun NCSS te toetsen aan de zeven verschillende vereisten van artikel 7 ten aanzien van de lijst van de in bijlage II bij de richtlijn genoemde sectoren en de in bijlage III bedoelde diensten. De vastgestelde lacunes kunnen vervolgens worden aangepakt door hun bestaande NCSS te herzien of de beginselen van hun nationale NIS-strategie volledig opnieuw te herzien. De hierboven verstrekte richtsnoeren inzake de vaststellingsprocedure voor de NCSS zijn ook relevant voor de herziening en actualisering van de bestaande NCSS.

---

[6] Enisa, *National Cyber-Security Strategy Good Practice* (2016). Beschikbaar op https://www.enisa.europa.eu/publications/ncss-good-practice-guide.

[7] ITU, *National Cybersecurity Strategy Guide* (2011). Beschikbaar op http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf.
Het ITU zal ook een toolkit voor nationale cyberbeveiligingsstrategieën publiceren in 2017 (zie presentatie op http://www.itu.int/en/ITU-D/Cybersecurity/Documents/National%20Strategy%20Toolkit%20introduction.pdf).

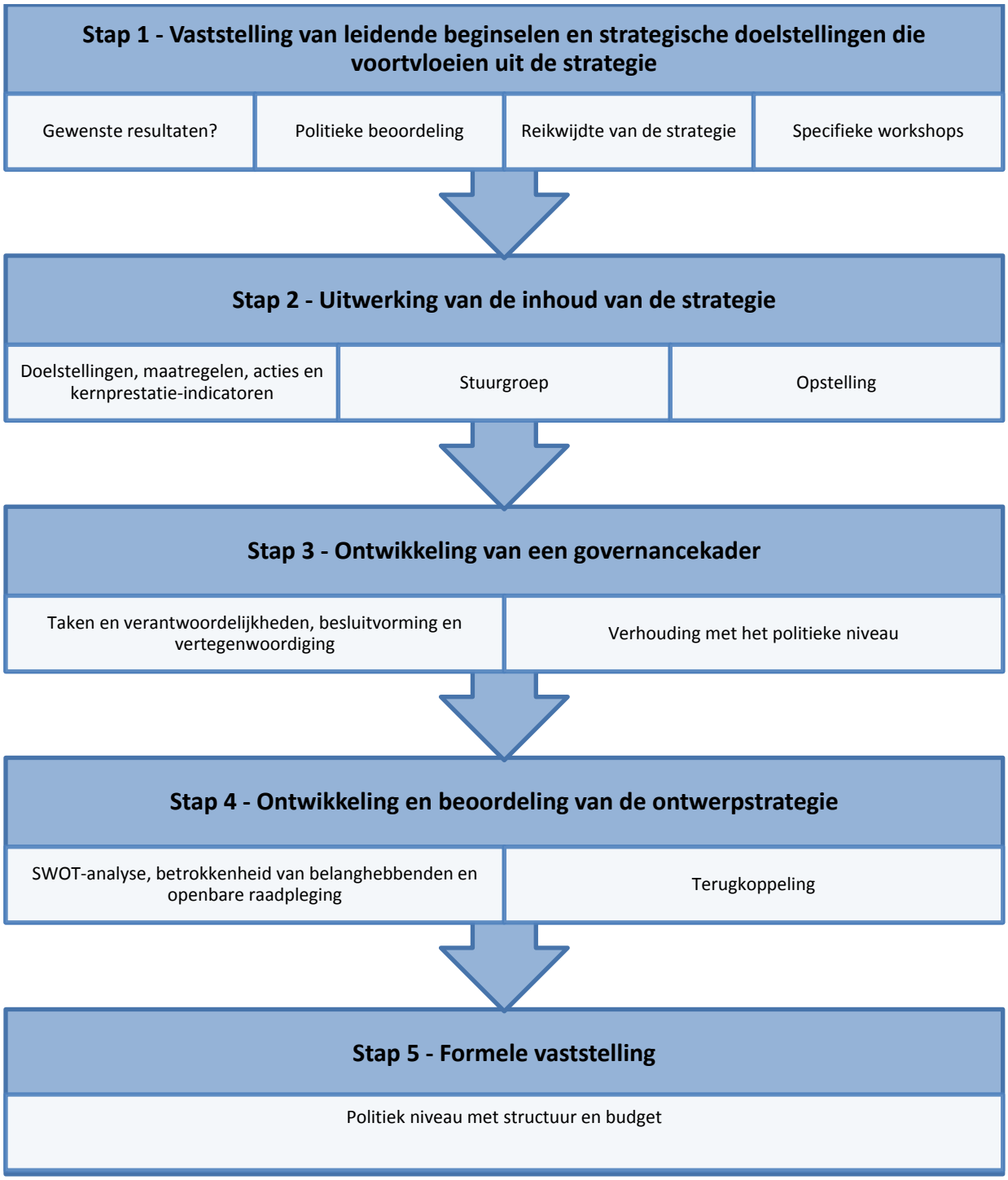
[8] OESO, *Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies* (2012). Beschikbaar op: http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf

[9] Centrum voor mondiaal cyberbeveiligingsvermogen en de universiteit van Oxford *Cybersecurity Capacity Maturity Model for Nations (CMM) - Revised Edition* (2016). Beschikbaar op: https://www.thegfce.com/binaries/gfce/documents/publications/2017/02/13/cybersecurity-cmm-for-nations/CMM+revised+edition.pdf

[10] Behalve Griekenland, waar een nationale cyberbeveiligingsstrategie wordt ontwikkeld sinds 2014 (te raadplegen op https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/national-cyber-security-strategy-greece/view).

[11] Deze informatie is gebaseerd op het overzicht van de NCSS dat wordt aangeboden door het Enisa op https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map.

Figuur 1: Vijfstappenplan voor de vaststelling van een NCSS



3. NIS-richtlijn: nationale bevoegde autoriteiten, centrale contactpunten en Computer Security Incident Response Teams (CSIRT's)

Overeenkomstig artikel 8, lid 1, moeten de lidstaten één of meer nationale bevoegde autoriteiten aanwijzen voor ten minste de in bijlage II bij de richtlijn genoemde sectoren en de in bijlage III bedoelde diensten, om de toepassing van de richtlijn te monitoren. De lidstaten mogen deze taak toekennen aan één of meer bestaande autoriteiten.

In dit deel wordt toegelicht op welke manier de paraatheid van de lidstaten wordt versterkt door de in de NIS-richtlijn vastgestelde verplichting om doeltreffende nationale bevoegde autoriteiten en Computer Security Incident Response Teams (CSIRT's) aan te wijzen. Meer bepaald wordt in dit deel ingegaan op de verplichting om nationale bevoegde autoriteiten aan te wijzen, met inbegrip van de rol van het centrale contactpunt. Er komen drie thema's aan bod: a) mogelijke nationale beheersstructuren (bv. gecentraliseerde en gedecentraliseerde modellen, enz.) en andere vereisten; b) de rol van het centrale contactpunt; en c) Computer Security Incident Response Teams.

3.1. Soort autoriteiten

Overeenkomstig artikel 8 van de NIS-richtlijn moeten de lidstaten nationale bevoegde autoriteiten inzake de beveiliging van netwerken en informatiesystemen aanwijzen, waarbij uitdrukkelijk wordt voorzien in de mogelijkheid om "*één of meer nationale bevoegde autoriteiten*" aan te wijzen. Deze beleidskeuze wordt toegelicht in overweging 30: "*Om rekening te houden met de uiteenlopende nationale bestuursstructuren, reeds bestaande sectorale regelingen of toezichthoudende en regelgevende instanties van de Unie ongemoeid te laten en dubbel werk te voorkomen, moeten de lidstaten meer dan één nationale bevoegde autoriteit kunnen aanwijzen die belast is met de uitvoering van de uit deze richtlijn voortvloeiende taken in verband met de beveiliging van de netwerk- en informatiesystemen van aanbieders van essentiële diensten en digitaledienstverleners.*"

Bijgevolg staat het de lidstaten vrij om ofwel één centrale autoriteit aan te wijzen die bevoegd is voor alle sectoren en diensten die onder de richtlijn vallen, ofwel meerdere autoriteiten aan te wijzen, bijvoorbeeld per soort sector.

De lidstaten kunnen bij de keuze van hun aanpak putten uit de opgedane ervaring met de nationale aanpak die werd gebruikt in het kader van de bestaande wetgeving op het gebied van de bescherming van kritieke infrastructuur (CIIP). Zoals beschreven in tabel 1 hebben de lidstaten in het geval van CIIP besloten een gecentraliseerde dan wel gedecentraliseerde aanpak aan te nemen bij de toekenning van bevoegdheden op nationaal niveau. Nationale voorbeelden worden hier louter ter illustratie gebruikt om de bestaande organisatorische kaders onder de aandacht van de lidstaten te brengen. Bijgevolg impliceert de Commissie niet dat het gehanteerde model voor CIIP van de desbetreffende landen gebruikt moet worden met het oog op de omzetting van de NIS-richtlijn.

De lidstaten kunnen ook kiezen voor verschillende hybride regelingen met elementen van zowel de gecentraliseerde als de gedecentraliseerde aanpak. De keuzes kunnen worden afgestemd op eerdere nationale bestuursregelingen voor de verschillende sectoren en diensten die onder de richtlijn vallen, of er kunnen nieuwe keuzes worden gemaakt door de betrokken autoriteiten en de relevante belanghebbenden die zijn geïdentificeerd als aanbieders van essentiële diensten en digitaledienstverleners. De keuzes van de lidstaten kunnen ook worden beïnvloed door andere belangrijke factoren, zoals specialistische expertise op het vlak van cyberbeveiliging, overwegingen in verband met middelen, de verhoudingen tussen de belanghebbenden en de nationale belangen (bijvoorbeeld economische ontwikkeling, openbare veiligheid, enz.).

3.2. Openbaarmaking en andere relevante aspecten

Op grond van artikel 8, lid 7, moeten de lidstaten de Commissie in kennis stellen van de aanwijzing van de nationale bevoegde autoriteiten en hun taken. Dit moet binnen de omzettingstermijn gebeuren.

Overeenkomstig de artikelen 15 en 17 van de NIS-richtlijn moeten de lidstaten ervoor zorgen dat de bevoegde autoriteiten over specifieke bevoegdheden en middelen beschikken om de in deze artikelen vastgestelde taken uit te voeren.

Voorts moet de aanwijzing van specifieke entiteiten als nationale bevoegde autoriteiten openbaar worden gemaakt. In de richtlijn wordt niet nader bepaald op welke manier deze informatie openbaar moet worden gemaakt. Aangezien deze vereiste tot doel heeft een hoog niveau van bewustzijn tot stand te brengen bij de onder de NIS-richtlijn vallende actoren en het brede publiek, en afgaande op de ervaringen in andere sectoren (telecommunicatie, bankwezen, geneesmiddelen), is de Commissie van mening dat dit doel kan worden bereikt door middel van bijvoorbeeld een portaal waaraan veel bekendheid wordt gegeven.

Overeenkomstig artikel 8, lid 5, van de NIS-richtlijn moeten dergelijke autoriteiten over de "nodige middelen" beschikken om de krachtens de richtlijn toegewezen taken uit te voeren.

Tabel 1: Nationale aanpak van de bescherming van kritieke informatie-infrastructuur (CIIP)

In 2016 heeft het Enisa een studie[12] gepubliceerd over de uiteenlopende aanpak die de lidstaten hanteren om hun kritieke informatie-infrastructuren te beschermen. Er worden twee profielen beschreven met betrekking tot het beheer van CIIP in de lidstaten die gebruikt kunnen worden in het kader van de omzetting van de NIS-richtlijn.

Profiel 1: Gedecentraliseerde aanpak – met meerdere sectorspecifieke autoriteiten die bevoegd zijn voor specifieke sectoren en diensten als vermeld in bijlage II en III bij de richtlijn

De gedecentraliseerde aanpak wordt gekenmerkt door:

(i) het subsidiariteitsbeginsel
(ii) nauwe samenwerking tussen overheidsinstanties
(iii) sectorspecifieke wetgeving

Het subsidiariteitsbeginsel

In plaats van één agentschap op te richten of aan te wijzen dat de algehele verantwoordelijkheid draagt, gaat de gedecentraliseerde aanpak uit van het subsidiariteitsbeginsel. Dit betekent dat de verantwoordelijkheid voor de uitvoering wordt toegewezen aan een sectorspecifieke autoriteit, die het beste inzicht heeft in de lokale sector en reeds vaste contacten onderhoudt met belanghebbenden. Volgens dit beginsel worden beslissingen genomen op het niveau dat het dichtst aansluit bij de betrokkenen.

Nauwe samenwerking tussen overheidsinstanties

Aangezien een groot aantal overheidsinstanties actief is op het gebied van CIIP, hebben veel lidstaten samenwerkingsprogramma's ontwikkeld om de werkzaamheden en inspanningen van de verschillende autoriteiten te coördineren. Deze samenwerkingsprogramma's kunnen bestaan uit informele netwerken of meer geïnstitutionaliseerde fora of regelingen. Zij dienen echter alleen om informatie uit te wisselen en de coördinatie tussen de verschillende overheidsinstanties te waarborgen, maar zijn niet bindend ten aanzien van hen.

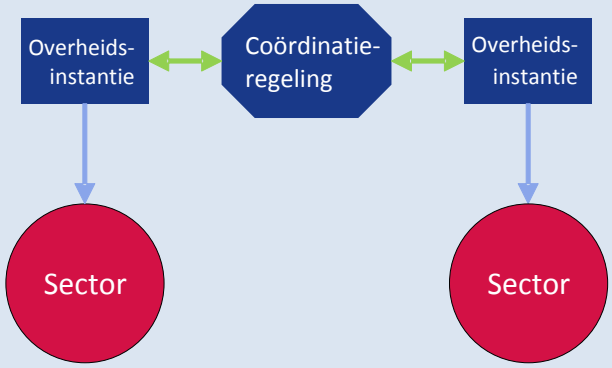
Sectorspecifieke wetgeving

De landen die een gedecentraliseerde aanpak hanteren voor de kritieke sectoren, stellen vaak geen wetgeving vast op het gebied van CIIP. In plaats daarvan blijft de vastgestelde wet- en regelgeving sectorspecifiek en kunnen er grote verschillen bestaan tussen sectoren. Deze aanpak biedt het voordeel dat de maatregelen met betrekking tot de NIS-richtlijn afgestemd kunnen worden op de bestaande sectorspecifieke regelgeving om het draagvlak in de sector te vergroten en de handhaving door de betrokken autoriteit doeltreffender te maken.

[12] Enisa, *Stocktaking, Analysis and Recommendations on the protection of CIIs* (2016). Beschikbaar op: https://www.enisa.europa.eu/publications/stocktaking-analysis-and-recommendations-on-the-protection-of-ciis

Bij een volledig gedecentraliseerde aanpak bestaat er een groot risico dat de richtlijn minder consistent wordt toegepast in diverse sectoren en diensten. In dit geval voorziet de richtlijn in een centraal nationaal contactpunt voor overleg over grensoverschrijdende kwesties, en deze entiteit kan ook door de betrokken lidstaat worden belast met de interne coördinatie en samenwerking tussen de verschillende nationale bevoegde autoriteiten overeenkomstig artikel 10 van de richtlijn.

Figuur 2 – gedecentraliseerde aanpak



Voorbeelden van de gedecentraliseerde aanpak

Zweden is een goed voorbeeld van een land dat een gedecentraliseerde aanpak hanteert op het gebied van CIIP. Het land maakt gebruik van een "systeemperspectief", waarbij verschillende instanties en gemeenten verantwoordelijk zijn voor de belangrijkste taken van CIIP, zoals de identificatie van essentiële diensten en kritieke infrastructuren, de coördinatie en ondersteuning van aanbieders, regelgevingstaken, en maatregelen voor de paraatheid bij noodsituaties. Hierbij gaat het onder meer om het Zweedse agentschap voor civiele noodgevallen (MSB), het Zweedse agentschap voor post en telecommunicatie (PTS) en verschillende Zweedse agentschappen voor defensie, het leger en rechtshandhaving.

Met het oog op de coördinatie tussen de verschillende agentschappen en publieke entiteiten heeft de Zweedse regering een samenwerkingsnetwerk ontwikkeld dat bestaat uit autoriteiten "met specifieke verantwoordelijkheden voor de beveiliging van maatschappelijke informatie". Deze samenwerkingsgroep voor informatiebeveiliging (SAMFI) bestaat uit vertegenwoordigers van de verschillende autoriteiten en komt meerdere keren per jaar bijeen om van gedachten te wisselen over vraagstukken in verband met de nationale informatiebeveiliging. De thematische gebieden van SAMFI zijn voornamelijk van politiek-strategische aard en hebben betrekking op onderwerpen zoals technische aspecten en normalisatie, nationale en internationale ontwikkeling op het gebied van informatiebeveiliging, en het beheer en de preventie van IT-incidenten. (Zweeds agentschap voor civiele noodgevallen (MSB) 2015).

Zweden heeft geen centrale wetgeving op het gebied van CIIP vastgesteld die van toepassing is op aanbieders van kritieke informatie-infrastructuur (CII) in alle sectoren. In plaats daarvan is het de verantwoordelijkheid van de respectieve overheidsinstanties om wetgeving vast te stellen met verplichtingen voor ondernemingen in specifieke sectoren. Zo is het MSB gemachtigd om regelgeving op het gebied van informatiebeveiliging vast te stellen voor overheidsinstanties, en kan het PTS aanbieders opdragen om bepaalde technische en organisatorische beveiligingsmaatregelen uit te voeren op basis van secundaire wetgeving.

Ierland is een ander voorbeeld van een land dat beantwoordt aan de kenmerken van dit profiel. Ierland volgt het "beginsel van subsidiariteit" waarbij elk ministerie verantwoordelijk is voor de identificatie van CII en voor risicobeoordeling in de eigen sector. Daarnaast is er geen specifieke regelgeving op het gebied van CIIP vastgesteld op nationaal niveau. De wetgeving blijft sectoraal en heeft voornamelijk betrekking op de energie- en telecommunicatiesector (2015). Andere voorbeelden zijn Oostenrijk, Cyprus en Finland.

Profiel 2: Gecentraliseerde aanpak – met één centrale autoriteit die bevoegd is voor alle sectoren en diensten als vermeld in bijlage II en III bij de richtlijn

De gecentraliseerde aanpak wordt gekenmerkt door:

i) een centrale autoriteit voor alle sectoren
ii) een alomvattende wetgeving

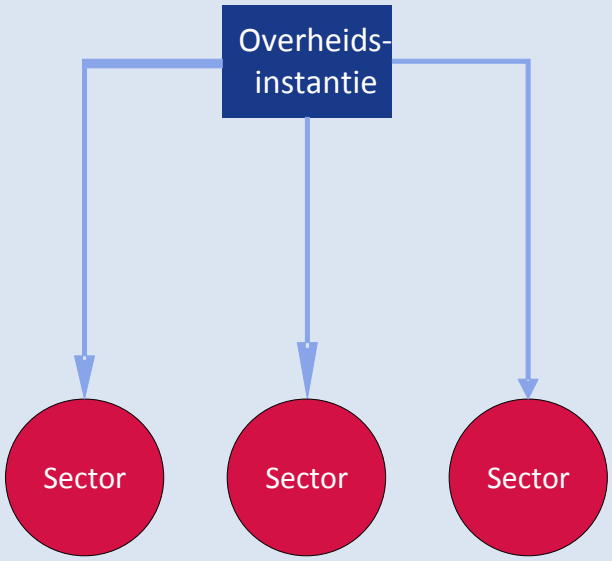
Centrale autoriteit voor alle sectoren

De lidstaten die een gecentraliseerde aanpak hanteren, hebben autoriteiten opgericht met verantwoordelijkheden en ruime bevoegdheden voor meerdere of alle kritieke sectoren, of hebben de bevoegdheden van de bestaande autoriteiten uitgebreid. Deze centrale autoriteiten voor CIIP zijn belast met meerdere taken, zoals noodplanning, crisisbeheersing, regelgevingstaken en de ondersteuning van particuliere aanbieders. In veel gevallen maakt het nationale of gouvernementele CSIRT deel uit van de centrale autoriteit voor CIIP. Een centrale autoriteit beschikt waarschijnlijk over meer expertise op het gebied van cyberbeveiliging in vergelijking met meerdere sectorale autoriteiten, gezien het algemene tekort aan vaardigheden op dit vlak.

Alomvattende wetgeving

Bij alomvattende wetgeving worden verplichtingen en vereisten opgelegd aan alle aanbieders van CII in alle sectoren. Dit kan worden bereikt door nieuwe alomvattende wetgeving vast te stellen of de bestaande sectorspecifieke regelgeving aan te vullen. Met deze aanpak wordt een consistente toepassing van de NIS-richtlijn in alle betrokken sectoren en diensten bevorderd. Hiermee wordt het risico op lacunes in de uitvoering vermeden, dat wel zou kunnen ontstaan indien er meerdere autoriteiten met specifieke bevoegdheden zijn.

Figuur 3 – Gecentraliseerde aanpak



Voorbeelden van de gecentraliseerde aanpak

Frankrijk is een goed voorbeeld van een EU-lidstaat met een gecentraliseerde aanpak. Het Franse nationale agentschap voor de beveiliging van informatiesystemen (Agence Nationale de la Sécurité des Systèmes d'Information - ANSSI) werd in 2011 aangewezen als de centrale nationale autoriteit voor de beveiliging van informatiesystemen. Het ANSSI heeft een sterke toezichthoudende rol ten aanzien van "aanbieders van essentieel belang" (OIV's). Het agentschap kan namelijk beveiligingsmaatregelen opleggen aan OIV's, en het is gemachtigd om ze aan veiligheidscontroles te onderwerpen. Voorts is het agentschap het centrale contactpunt voor OIV's, die verplicht zijn om beveiligingsincidenten hieraan te melden.

In geval van beveiligingsincidenten treedt het ANSSI op als een noodagentschap voor CIIP en neemt het besluiten over de maatregelen die aanbieders moeten nemen als reactie op de crisis. De regeringsmaatregelen worden gecoördineerd in het operatiecentrum van het ANSSI. De opsporing van dreigingen en de respons op incidenten op operationeel niveau wordt verricht door CERT-FR, dat deel uitmaakt van het ANSSI.

Frankrijk heeft een alomvattend rechtskader vastgesteld op het gebied van CIIP. In 2006 heeft de premier de opdracht gegeven om een lijst met sectoren van kritieke infrastructuur op te stellen. Op basis van deze lijst, die bestaat uit twaalf essentiële sectoren, heeft de regering ongeveer 250 OIV's geïdentificeerd. In 2013 werd de wet inzake militaire programmering (LPM)[13] afgekondigd. Hierbij worden verschillende verplichtingen opgelegd aan OIV's, zoals de melding van incidenten en de uitvoering van veiligheidsmaatregelen. Deze vereisten gelden voor alle OIV's in alle sectoren (Franse Senaat 2013).

[13] Loi de programmation militaire.

3.3. Artikel 9 van de NIS-richtlijn: Computer Security Incident Response Teams (CSIRT's)

Overeenkomstig artikel 9 moeten de lidstaten één of meer CSIRT's aanwijzen die worden belast met de behandeling van risico's en incidenten met betrekking tot de in bijlage II bij de NIS-richtlijn genoemde sectoren en de in bijlage III bedoelde diensten. Met inachtneming van het in artikel 3 van de richtlijn opgenomen beginsel van minimumharmonisatie staat het de lidstaten vrij de CSIRT's ook te gebruiken voor andere sectoren die niet onder de richtlijn vallen, zoals overheidsinstanties.

De lidstaten kunnen ervoor kiezen een CSIRT op te zetten binnen de nationale bevoegde autoriteit[14].

3.4. Taken en voorschriften

De in bijlage I bij de NIS-richtlijn vastgestelde taken van aangewezen CSIRT's omvatten onder meer:

- monitoren van incidenten op nationaal niveau;
- ten behoeve van de betrokken belanghebbende partijen zorgen voor vroegtijdige waarschuwingen, alarmmeldingen, aankondigingen en verspreiding van informatie over risico's en incidenten;
- reageren op incidenten;
- zorgen voor een dynamische risico- en incidentanalyse en situatiekennis; en
- deelnemen aan het krachtens artikel 12 ingestelde netwerk van nationale CSIRT's (het CSIRT-netwerk).

In artikel 14, leden 3, 5 en 6, en artikel 16, leden 3, 6 en 7, zijn specifieke bijkomende taken vastgesteld in verband met meldingen van incidenten indien een lidstaat beslist dat CSIRT's dergelijke taken mogen uitvoeren naast of in plaats van nationale bevoegde autoriteiten.

Bij de omzetting van de richtlijn hebben de lidstaten de keuze tussen verschillende opties met betrekking tot welke rol de CSIRT's spelen bij de eisen inzake melding van incidenten. Het is mogelijk om rechtstreekse rapportage aan de CSIRT's verplicht te stellen, wat de administratieve efficiëntie ten goede komt. Daarnaast kunnen de lidstaten ervoor kiezen om rechtstreekse rapportage aan de nationale bevoegde autoriteiten in te voeren, waarbij de CSIRT's toegang krijgen tot de gerapporteerde informatie. De CSIRT's houden zich uiteindelijk bezig met problemen oplossen als het gaat om cyberincidenten ontmoedigen, opsporen, erop reageren en de gevolgen ervan beperken (ook de incidenten waarvoor geen verplichte rapportage geldt) met de belanghebbenden, terwijl de nationale bevoegde autoriteiten zich bezighouden met de naleving van de regelgeving.

Overeenkomstig artikel 9, lid 3, van de richtlijn moeten de lidstaten er ook voor zorgen dat dergelijke CSIRT's toegang hebben tot beveiligde en weerbare ICT-infrastructuur.

[14] Zie artikel 9, lid 1, laatste zin.

Overeenkomstig artikel 9, lid 4, van de richtlijn moeten de lidstaten de Commissie informeren over de bevoegdheid en de voornaamste elementen van de incidentenbehandelingsprocedure van de aangewezen CSIRT's.

De voorschriften voor de door de lidstaten aangewezen CSIRT's zijn vastgesteld in bijlage I bij de NIS-richtlijn. Een CSIRT moet een hoge mate van beschikbaarheid van zijn communicatiediensten garanderen. De lokalen van een CSIRT en de ondersteunende informatiesystemen moeten zich op beveiligde locaties bevinden en bedrijfscontinuïteit kunnen waarborgen. Voorts moeten CSIRT's de mogelijkheid hebben om deel te nemen aan internationale samenwerkingsnetwerken.

3.5. Bijstand voor de ontwikkeling van CSIRT's

Het programma Connecting Europe Facility (CEF) voor digitaleddiensteninfrastructuur op het gebied van cyberbeveiliging kan voorzien in aanzienlijke EU-financiering om de CSIRT's van de lidstaten bij te staan met het oog op verbeterde vermogens en onderlinge samenwerking in het kader van een samenwerkingsmechanisme voor informatie-uitwisseling. Het samenwerkingsmechanisme dat wordt ontwikkeld in het kader van het project SMART 2015/1089, strekt ertoe een snelle en doeltreffende operationele samenwerking op vrijwillige basis tussen de CSIRT's van de lidstaten te bevorderen, namelijk ter ondersteuning van de taken waarmee het CSIRT-netwerk is belast overeenkomstig artikel 12 van de richtlijn.

Nadere informatie over de desbetreffende oproepen tot het indienen van voorstellen voor de capaciteitsopbouw van de CSIRT's van de lidstaten is beschikbaar op de website van het Uitvoerend Agentschap innovatie en netwerken (INEA) van de Europese Commissie[15].

De raad van bestuur van de Connecting Europe Facility (CEF) voor digitaleddiensteninfrastructuur op het gebied van cyberbeveiliging biedt een informele structuur voor begeleiding en bijstand op beleidsniveau aan de CSIRT's van de lidstaten met het oog op capaciteitsopbouw en de invoering van het mechanisme voor vrijwillige samenwerking.

Een nieuwe CSIRT of een CSIRT die is aangewezen om de in bijlage I bij de NIS-richtlijn vastgestelde taken uit te voeren, kan zich baseren op het advies en de expertise van het Enisa om zijn prestaties te verbeteren en zijn werk doeltreffend uit te voeren[16]. In dit verband moet worden opgemerkt dat de CSIRT's van de lidstaten de recente werkzaamheden van het Enisa ten dele als referentie kunnen gebruiken. Zoals vermeld in deel 7 van deze bijlage heeft het agentschap met name een aantal documenten en studies gepubliceerd met goede praktijken, technische aanbevelingen, waaronder beoordelingen van het maturiteitsniveau van CSIRT's, voor diverse vermogens en diensten met betrekking tot CSIRT's. Daarnaast zijn ook richtsnoeren en beste praktijken uitgewisseld door netwerken van CSIRT's op mondiaal (FIRST[17]) en Europees niveau (Trusted Introducer, TI[18]).

[15] Beschikbaar op: https://ec.europa.eu/inea/en/connecting-europe-facility
[16] Zie artikel 9, lid 5, van de NIS-richtlijn.
[17] Forum van Incident Response and Security Teams (https://www.first.org/)

3.6. Rol van het centrale contactpunt

Overeenkomstig artikel 8, lid 3, van de NIS-richtlijn moet elke lidstaat een nationaal centraal contactpunt aanwijzen, dat een verbindingsfunctie vervult bij de grensoverschrijdende samenwerking met de relevante autoriteiten in andere lidstaten en met de samenwerkingsgroep en het CSIRT-netwerk[19], die bij de richtlijn zelf zijn opgericht. In overweging 31 en artikel 8, lid 4, wordt dit vereiste gemotiveerd, namelijk ter bevordering van grensoverschrijdende samenwerking en communicatie. Dit is vooral nodig omdat de lidstaten kunnen beslissen om meer dan één nationale autoriteit aan te wijzen. Bijgevolg zou een centraal contactpunt de identificatie en samenwerking van autoriteiten uit verschillende lidstaten vergemakkelijken.

De verbindingsfunctie van het centrale contactpuntkan interactiet tussen de secretariaten van de samenwerkingsgroep en het CSIRT-netwerk inhouden in gevallen waarin het nationale centrale contactpunt geen CSIRT is en ook geen lid is van de samenwerkingsgroep. Voorts moeten de lidstaten ervoor zorgen dat het centrale contactpunt wordt geïnformeerd over de ontvangen meldingen van aanbieders van essentiële diensten en digitaledienstverleners[20].

In artikel 8, lid 3, van de richtlijn wordt bepaald dat, indien een lidstaat voor een gecentraliseerde aanpak kiest, d.w.z. slechts één bevoegde autoriteit aanwijst, die autoriteit ook de rol van centraal contactpunt op zich neemt. Indien een lidstaat voor een gedecentraliseerde aanpak kiest, kan een van de verschillende bevoegde autoriteiten worden aangewezen om de rol van centraal contactpunt op zich te nemen. Indien een bevoegde autoriteit, het CSIRT en het centrale contactpunt verschillende entiteiten zijn, moeten de lidstaten voor een doeltreffende onderlinge samenwerking zorgen om te voldoen aan de in de richtlijn vastgestelde verplichtingen, ongeacht het gekozen institutionele model[21].

Het centrale contactpunt moet uiterlijk op 9 augustus 2018 en vervolgens eenmaal per jaar bij de samenwerkingsgroep een samenvattend verslag indienen over de ontvangen meldingen, met inbegrip van het aantal en de aard van de gemelde incidenten en de door de autoriteiten genomen maatregelen, zoals kennisgeving van het incident aan de andere getroffen lidstaten of verstrekking van relevante informatie aan de meldende onderneming voor de afhandeling van het incident[22]. Op verzoek van de bevoegde autoriteit of van het CSIRT moet het centraal contactpunt de meldingen van de aanbieders van essentiële diensten doorsturen naar de centrale contactpunten van andere lidstaten die zijn getroffen door de incidenten[23].

De lidstaten moeten de Commissie binnen de omzettingstermijn in kennis stellen van de aanwijzing van het centrale contactpunt en zijn taken. De aanwijzing van het centrale contactpunt moet openbaar worden gemaakt, op dezelfde manier als voor de nationale

---

[18] https://www.trusted-introducer.org/

[19] Een netwerk van nationale CSIRT's voor operationele samenwerking tussen de lidstaten overeenkomstig artikel 12.

[20] Zie artikel 10, lid 3.

[21] Zie artikel 10, lid 1.

[22] Idem.

[23] Zie artikel 14, lid 5.

bevoegde autoriteiten. De Commissie zorgt voor de bekendmaking van de lijst van aangewezen centrale contactpunten.

3.7. Sancties

Op grond van artikel 21 kunnen de lidstaten zelf beslissen over het type en de aard van de toepasselijke sancties, op voorwaarde dat deze doeltreffend, evenredig en afschrikkend zijn. Met andere woorden staat het de lidstaten in principe vrij om te beslissen over het maximumbedrag van de in hun nationale wetgeving vastgestelde sancties, maar het gekozen bedrag of percentage moet de nationale autoriteiten in staat stellen om in elk concreet geval doeltreffende, evenredige en afschrikkende sancties op te leggen, rekening houdend met verschillende factoren zoals de ernst of de frequentie van de inbreuk.

4. Entiteiten met verplichtingen inzake beveiliging en melding van incidenten

Entiteiten die een belangrijke rol spelen in de samenleving en de economie, en die aangemerkt worden als aanbieders van essentiële diensten en digitaledienstverleners in de zin van artikel 4, punt 4, en artikel 4, punt 5, van de richtlijn, moeten passende veiligheidsmaatregelen nemen en ernstige incidenten melden aan de relevante nationale autoriteiten. De redenering hierachter is dat de gevolgen van beveiligingsincidenten in dergelijke diensten een ernstige bedreiging kunnen vormen voor de werking van deze diensten, wat kan leiden tot ernstige verstoringen van de economische activiteiten en van de samenleving in het algemeen, waardoor het gebruikersvertrouwen mogelijk wordt ondermijnd en ernstige schade wordt toegebracht aan de economie van de Unie[24].

Dit deel biedt een overzicht van de entiteiten die binnen het toepassingsgebied van bijlage II en III bij de NIS-richtlijn vallen, en de op hen rustende verplichtingen. De identificatie van aanbieders van essentiële diensten komt uitgebreid aan bod, gezien het belang van dit proces voor de geharmoniseerde uitvoering van de NIS-richtlijn in de hele EU. Daarnaast worden de definities van digitale infrastructuren en digitaledienstverleners uitvoerig toegelicht. In dit deel wordt ook de eventuele opneming van andere sectoren onderzocht en wordt de specifieke aanpak met betrekking tot digitaledienstverleners toegelicht.

4.1. Aanbieders van essentiële diensten

In de NIS-richtlijn is niet expliciet vastgesteld welke entiteiten als aanbieders van essentiële diensten worden beschouwd binnen het toepassingsgebied van de richtlijn. In plaats daarvan voorziet de richtlijn in criteria die de lidstaten moeten toepassen in het identificatieproces en aan de hand waarvan uiteindelijk zal worden bepaald welke individuele ondernemingen van het soort van de in bijlage II vermelde entiteiten worden beschouwd als aanbieders van essentiële diensten, en bijgevolg worden onderworpen aan de verplichtingen uit hoofde van de richtlijn.

[24] Zie overweging 2.

4.1.1. Soort entiteiten als vermeld in bijlage II bij de NIS-richtlijn

In artikel 4, punt 4, worden aanbieders van essentiële diensten gedefinieerd als publieke of private entiteiten waarvan de soort is vermeld in bijlage II en die voldoen aan de criteria van artikel 5, lid 2. Bijlage II bevat een overzicht van de sectoren, deelsectoren en de soort entiteiten waarvoor elke lidstaat een identificatieproces moet uitvoeren overeenkomstig artikel 5, lid 2[25]. Hierbij gaat het om sectoren zoals energie, vervoer, bankwezen, infrastructuur voor de financiële markt, gezondheidszorg, water en digitale infrastructuur.

Voor de meeste entiteiten die behoren tot de "traditionele sectoren", bevat de EU-wetgeving uitgebreide definities, waarnaar wordt verwezen in bijlage II. Dit is echter niet het geval voor de in punt 7 van bijlage II vermelde sector van digitale infrastructuur, met inbegrip van internetknooppunten, domeinnaamsystemen en registers voor topleveldomeinnamen. Daarom worden deze definities hieronder uitvoerig toegelicht.

1) Internetknooppunt (IXP)

De term "internetknooppunt" wordt gedefinieerd in artikel 4, punt 13, en verder toegelicht in overweging 18, en kan worden omschreven als een netwerkinfrastructuur die de onderlinge verbinding van meer dan twee onafhankelijke technisch op zichzelf staande systemen mogelijk maakt, voornamelijk met als doel de uitwisseling van internetverkeer te vergemakkelijken. Een internetknooppunt kan ook worden omschreven als een fysieke locatie waar een aantal netwerken internetverkeer met elkaar uitwisselen via een schakelaar. Een internetknooppunt dient voornamelijk om rechtstreekse interconnectie tussen netwerken mogelijk te maken via het knooppunt, in plaats van via één of meerdere netwerken van derden. De aanbieder van een internetknooppunt is normaal gezien niet verantwoordelijk voor de routing van het internetverkeer. De routing van het verkeer wordt uitgevoerd door de netwerkaanbieders. De rechtstreekse interconnectie heeft veel voordelen, waarvan de kost, latentie en bandbreedte de voornaamste zijn. Het verkeer dat door een knooppunt loopt, wordt doorgaans door geen enkele partij in rekening gebracht, terwijl dit wel het geval is voor verkeer naar een upstream internetprovider. Dankzij de rechtstreekse interconnectie, die zich vaak in dezelfde stad als de beide netwerken bevindt, hoeven de gegevens geen lange afstanden af te leggen van het ene netwerk naar het andere, met een kortere latentie tot gevolg.

Er zij op gewezen dat de definitie van een internetknooppunt geen betrekking heeft op fysieke punten indien slechts twee fysieke netwerken met elkaar interconnecteren (d.w.z. netwerkaanbieders zoals BASE en PROXIMUS). Bij de omzetting van de richtlijn moeten de lidstaten bijgevolg een onderscheid maken tussen aanbieders die de uitwisseling van geaggregeerd internetverkeer tussen meerdere netwerkaanbieders vergemakkelijken, enerzijds, en individuele netwerkaanbieders, die hun netwerk fysiek interconnecteren op basis van een interconnectieovereenkomst, anderzijds. In het laatste geval vallen de

[25] Zie punt 4.1.6 voor meer informatie over het identificatieproces.

netwerkaanbieders niet onder de definitie van artikel 4, punt 13. In overweging 18 wordt verduidelijkt dat een internetknooppunt geen toegang verschaft tot een netwerk en geen dienst doet als dienstverlener of -aanbieder. De laatste categorie aanbieders zijn ondernemingen die openbare communicatienetwerken en/of -diensten aanbieden en onderworpen zijn aan de beveiligings- en meldingsverplichtingen uit hoofde van artikel 13 bis en artikel 13 ter van Richtlijn 2002/21/EG, en bijgevolg buiten het toepassingsgebied van de NIS-richtlijn vallen[26].

2) Domeinnaamsystemen (DNS)

De term "domeinnaamsysteem" wordt in artikel 4, punt 14, gedefinieerd als "*een hiërarchisch opgebouwd adresseringssysteem in een netwerk dat een zoekvraag naar een domeinnaam beantwoordt*". Meer bepaald kan een DNS worden omschreven als een hiërarchisch opgebouwd adresseringssysteem voor computers, diensten en andere met het internet verbonden middelen, waarmee domeinnamen in IP-adressen (Internet Protocol) worden gecodeerd. De hoofdtaak van het systeem bestaat erin toegekende domeinnamen te vertalen in IP-adressen. Daartoe beheert het DNS een databank en maakt het gebruik van naamservers en omzetters om dit soort "vertaling" van domeinnamen in operationele IP-adressen mogelijk te maken. Hoewel de codering van domeinnamen niet de enige taak is van het DNS, is het wel een van de belangrijkste. De juridische definitie in artikel 4, lid 14, is gericht op de hoofdtaak van het systeem vanuit het oogpunt van de gebruiker, zonder al te zeer in te gaan op technische details, zoals het beheer van domeinnamen, naamservers, omzetters, enzovoort. Ten slotte wordt in artikel 4, lid 15, verduidelijkt wie als een DNS-dienstverlener moet worden beschouwd.

3) Register voor topleveldomeinnamen (TLD-naamregister)

Een register voor topleveldomeinnamen wordt in artikel 4, punt 16, gedefinieerd als een entiteit die de internetdomeinnamen van een specifiek topleveldomein registreert en beheert. De registratie en het beheer van domeinnamen omvat de codering van topleveldomeinnamen in IP-adressen.

De Internet Assigned Numbers Authority (IANA) is verantwoordelijk voor de wereldwijde coördinatie van de DNS-root, IP-adressen en andere internetprotocolbronnen. De IANA is met name verantwoordelijk voor de toekenning van algemene topniveaudomeinen (gTLD's) zoals ".com" en landcodetopniveaudomeinen (ccTLD's) zoals ".be" aan aanbieders (registers) en het beheer van de technische en administratieve details ervan. De IANA beheert een mondiaal register van toegekende TLD's en speelt een rol bij de bekendmaking van deze lijst aan internetgebruikers in de hele wereld, en bij de invoering van nieuwe TLD's.

Een belangrijke taak van de registers is de toekenning van domeinnamen op het tweede niveau aan zogenoemde registranten voor hun respectieve TLD. Deze registranten hebben ook de mogelijkheid om zelf domeinnamen op het derde niveau toe te kennen indien zij dit

[26] Zie punt 5.2. voor meer informatie over de verhouding tussen de NIS-richtlijn en Richtlijn 2002/21/EG.

wensen. De ccTLD's dienen om een land of gebied aan te merken op basis van ISO-norm 3166-1. De "algemene" TLD's hebben normaal gezien geen geografische of landbenaming.

Er zij op gewezen dat bij het beheer van het TLD-naamregister DNS-diensten kunnen worden verleend. Zo is in de delegatieregels van de IANA bepaald dat de aangewezen entiteit die zich bezighoudt met ccTLD's – onder meer – toezicht moet houden op de domeinnamen en het DNS van dat land moet beheren[27]. De lidstaten moeten rekening houden met dergelijke omstandigheden bij het identificatieproces voor aanbieders van essentiële diensten in de zin van artikel 5, lid 2.

4.1.2. Identificatie van aanbieders van essentiële diensten

Overeenkomstig de vereisten uit hoofde van artikel 5 van de richtlijn moet elke lidstaat een identificatieproces uitvoeren met betrekking tot alle entiteiten die behoren tot de in bijlage II vermelde soorten en een wettelijke vestiging op het grondgebied van die lidstaat hebben. Op grond van deze beoordeling worden alle entiteiten die voldoen aan de in artikel 5, lid 2, vastgestelde criteria, geïdentificeerd als aanbieders van essentiële diensten en onderworpen aan de beveiligings- en meldingsverplichtingen uit hoofde van artikel 14.

De lidstaten hebben tot 9 november 2018 de tijd om aanbieders te identificeren voor elke sector en deelsector. Om de lidstaten te ondersteunen bij dit proces, werkt de samenwerkingsgroep momenteel aan een richtsnoer met relevante informatie over de nodige stappen en beste praktijken in verband met de identificatie van aanbieders van essentiële diensten.

Overeenkomstig artikel 24, lid 2, zal de samenwerkingsgroep voorts besprekingen houden over de procedure, de inhoud en de soort van nationale maatregelen voor de identificatie van aanbieders van essentiële diensten binnen specifieke sectoren. De lidstaten hebben vóór 9 november 2018 de mogelijkheid om hun nationale ontwerpmaatregelen voor de identificatie van aanbieders van essentiële diensten te bespreken in de samenwerkingsgroep.

4.1.3. Opneming van andere sectoren

Overeenkomstig het in artikel 3 opgenomen beginsel van minimumharmonisatie kunnen de lidstaten wetgeving vaststellen of handhaven waarmee een hoger niveau van beveiliging van netwerk- en informatiesystemen wordt gewaarborgd. In dit opzicht staat het de lidstaten over het algemeen vrij de beveiligings- en meldingsverplichtingen uit hoofde van artikel 14 uit te breiden naar entiteiten die behoren tot sectoren en deelsectoren die niet zijn opgenomen in bijlage II bij de NIS-richtlijn. Meerdere lidstaten hebben besloten of overwegen een aantal van de volgende extra sectoren op te nemen:

i) Overheidsinstanties

Overheidsinstanties kunnen essentiële diensten aanbieden die zijn opgenomen in bijlage II bij de richtlijn en voldoen aan de vereisten uit hoofde van artikel 5, lid 2. Overheidsinstanties die dergelijke diensten aanbieden, worden in deze gevallen onderworpen aan de desbetreffende

[27] Meer informatie beschikbaar op: https://www.icann.org/resources/pages/delegation-2012-02-25-en

beveiligings- en meldingseisen. Indien overheidsinstanties daarentegen diensten aanbieden die niet binnen het bovenstaande toepassingsgebied vallen, gelden deze verplichtingen niet voor dergelijke diensten.

Overheidsinstanties zijn verantwoordelijk voor de goede openbare dienstverlening van overheidsorganen, regionale en lokale autoriteiten, agentschappen en gelieerde ondernemingen. Voor deze diensten moeten vaak persoons- en bedrijfsgegevens over personen en organisaties worden gecreëerd en beheerd, die gedeeld kunnen worden en ter beschikking kunnen worden gesteld aan meerdere publieke entiteiten. In ruimere zin is een hoog niveau van beveiliging van de door overheidsinstanties gebruikte netwerk- en informatiesystemen van groot belang voor de samenleving en de economie in het algemeen. Volgens de Commissie kan het daarom voor de lidstaten nuttig zijn te overwegen om het toepassingsgebied van de nationale wetgeving tot omzetting van de richtlijn te verruimen tot overheidsinstanties en verder te gaanbreder dan de verlening van essentiële diensten zoals vastgesteld in bijlage II en artikel 5, lid 2.

ii) Postsector

De postsector omvat de verlening van postdiensten zoals de ontvangst, de sortering, het vervoer en de verdeling van postzendingen.

iii) Voedingssector

De voedingssector omvat de productie van landbouwproducten en andere levensmiddelen en kan essentiële diensten inhouden, zoals het waarborgen van de voedselzekerheid, -kwaliteit en -veiligheid.

iv) Chemische en nucleaire sector

De chemische en nucleaire sector omvat met name de opslag, productie en verwerking van chemische en petrochemische producten of nucleair materiaal.

v) Milieusector

Milieuactiviteiten omvatten de levering van goederen en diensten die nodig zijn om het milieu te beschermen en hulpbronnen te beheren. Derhalve hebben deze activiteiten tot doel vervuiling te voorkomen, terug te dringen en te beëindigen en de voorraad beschikbare natuurlijke hulpbronnen in stand te houden. In deze sector kunnen het toezicht op en de beheersing van vervuiling (bv. lucht en water) en meteorologische fenomenen essentiële diensten zijn.

vi) Civiele bescherming

De sector van de civiele bescherming heeft de preventie van, de voorbereiding op en de bestrijding van natuurlijke en door de mens veroorzaakte rampen tot doel. De hiertoe verleende diensten omvatten onder meer de activering van noodnummers en maatregelen voor informatieverstrekking over, beheersing van en reactie op noodgevallen.

4.1.4. Jurisdictie

Overeenkomstig artikel 5, lid 1, moet elke lidstaat aanbieders van essentiële diensten met een vestiging op zijn grondgebied identificeren. In de bepaling wordt niet nader ingegaan op het

soort wettelijke vestiging, maar in overweging 21 wordt verduidelijkt dat een dergelijke vestiging de effectieve en daadwerkelijke uitoefening van activiteiten via vaste regelingen verlangt, hoewel de rechtsvorm van zulke regelingen niet doorslaggevend mag zijn. Dit betekent dat een aanbieder van essentiële diensten niet alleen onder de jurisdictie van een lidstaat valt indien de aanbieder zijn hoofdvestiging op het grondgebied van die lidstaat heeft, maar ook indien de aanbieder bijvoorbeeld een bijkantoor of een andere soort wettelijke vestiging heeft.

Dit heeft tot gevolg dat dezelfde entiteit onder de jurisdictie van meerdere lidstaten tegelijk kan vallen.

4.1.5. Aan de Commissie te verstrekken informatie

Met het oog op de evaluatie die de Commissie moet uitvoeren overeenkomstig artikel 23, lid 1, van de NIS-richtlijn moeten de lidstaten uiterlijk op 9 november 2018 en vervolgens om de twee jaar de volgende informatie verstrekken aan de Commissie:

- de nationale maatregelen die de identificatie van aanbieders van essentiële diensten mogelijk maken;
- de lijst van essentiële diensten;
- het aantal aanbieders van essentiële diensten die zijn geïdentificeerd voor elke in bijlage II genoemde sector en het belang van die aanbieders ten aanzien van die sector; en
- de drempels, indien daarvan sprake is, om het niveau van dienstverleningte bepalen wat betreft het aantal gebruikers die van deze dienst afhankelijk zijn, als bedoeld in artikel 6, lid 1, onder a), of het belang van die entiteit overeenkomstig artikel 6, lid 1, onder f).

Uit de evaluatie uit hoofde van artikel 23, lid 1, die voorafgaat aan de algehele evaluatie van de richtlijn, blijkt het belang dat de medewetgevers hechten aan de correcte omzetting van de richtlijn wat betreft de identificatie van aanbieders van essentiële diensten, namelijk om marktversnippering te vermijden.

Om dit proces zo goed mogelijk uit te voeren, moedigt de Commissie de lidstaten aan dit thema te bespreken en relevante ervaringen uit te wisselen in de samenwerkingsgroep. Daarnaast moedigt de Commissie de lidstaten aan de lijsten van geïdentificeerde aanbieders van essentiële diensten (die uiteindelijk werden geselecteerd) te verstrekken aan de Commissie, indien nodig op vertrouwelijke basis, in aanvulling op alle informatie die de lidstaten aan de Commissie moeten verstrekken op grond van de richtlijn. Aan de hand van deze lijsten kan de Commissie makkelijker een kwalitatief betere beoordeling maken van de consistentie van het identificatieproces en kan de aanpak van de lidstaten onderling vergeleken worden, waardoor de doelstellingen van de richtlijn beter worden gerealiseerd.

4.1.6. Hoe moet het identificatieproces worden uitgevoerd?

Zoals blijkt uit figuur 4 moet een nationale autoriteit zes belangrijke vragen onderzoeken bij het identificatieproces voor een bepaalde entiteit. Hieronder komt elke vraag overeen met een

stap die moet worden uitgevoerd overeenkomstig artikel 5 in samenhang met artikel 6, en ook rekening houdend met de toepasbaarheid van artikel 1, lid 7.

Stap 1 – **Behoort de entiteit tot een in bijlage II bij de richtlijn genoemde sector/deelsector en soort?**

Een nationale autoriteit moet nagaan of een op haar grondgebied gevestigde entiteit tot een van de in bijlage II bij de richtlijn genoemde sectoren en deelsectoren behoort. Bijlage II bestrijkt diverse economische sectoren die essentieel worden geacht voor de goede werking van de interne markt. Bijlage II omvat met name de volgende sectoren en deelsectoren:

- Energie: elektriciteit, aardolie en gas
- Vervoer: luchtvervoer, spoorvervoer, vervoer over water en vervoer over de weg
- Bankwezen: kredietinstellingen
- Infrastructuur voor de financiële markt: handelsplatformen en centrale tegenpartijen
- Gezondheidszorg: zorgaanbieders (waaronder ziekenhuizen en privéklinieken)
- Water: levering en distributie van drinkwater
- Digitale infrastructuur: internetknooppunten, DNS-dienstverleners en registers voor topleveldomeinnamen[28]

Stap 2 – **Is een *lex specialis* van toepassing?**

Als volgende stap moet de nationale autoriteit nagaan of de in artikel 1, lid 7, opgenomen lex-specialisbepaling van toepassing is. Hierin is met name bepaald dat, indien een rechtshandeling van de EU aan digitaledienstverleners of aanbieders van essentiële diensten beveiligings- en/of meldingseisen oplegt die ten minste gelijkwaardig zijn aan de overeenkomstige eisen van de NIS-richtlijn, de verplichtingen van de speciale rechtshandeling van toepassing zijn. Daarnaast wordt in overweging 9 verduidelijkt dat, indien wordt voldaan aan de in artikel 1, lid 7, vastgestelde eisen, de lidstaten de bepalingen van de sectorspecifieke rechtshandeling van de EU moeten toepassen, inclusief die inzake jurisdictie. De desbetreffende bepalingen van de NIS-richtlijn zijn daarentegen niet van toepassing. In dit geval mag de bevoegde autoriteit niet doorgaan met het identificatieproces uit hoofde van artikel 5, lid 2[29].

Stap 3 – **Verleent de aanbieder een essentiële dienst in de zin van de Richtlijn?**

Overeenkomstig artikel 5, lid 2, onder a), moet de entiteit die wordt onderworpen aan het identificatieproces, een dienst verlenen die van essentieel belang is voor de instandhouding van kritieke maatschappelijke en/of economische activiteiten. Bij deze beoordeling moeten de lidstaten rekening houden met het feit dat een entiteit zowel essentiële als niet-essentiële diensten kan verlenen. Dit betekent dat de beveiligings- en meldingseisen van de NIS-richtlijn alleen gelden voor een bepaalde aanbieder voor zover deze essentiële diensten verleent.

[28]In punt 4.1.1. wordt dieper ingegaan op deze entiteiten.

[29] In punt 5.1. wordt dieper ingegaan op de toepasbaarheid van *lex specialis.*

Overeenkomstig artikel 5, lid 3, moeten de lidstaten een lijst opstellen van alle essentiële diensten die worden verleend door aanbieders van essentiële diensten op hun grondgebied. Deze lijst moet uiterlijk op 9 november 2018 en vervolgens om de twee jaar worden verstrekt aan de Commissie[30].

Stap 4 - **Is de dienst afhankelijk van een netwerk- en informatiesysteem?**

Voorts moet worden verduidelijkt of deze dienst voldoet aan het tweede criterium van artikel 5, lid 2, onder b), en met name of de verlening van de essentiële dienst afhankelijk is van netwerk- en informatiesystemen zoals omschreven in artikel 4, punt 1.

Stap 5 – **Zou een beveiligingsincident een aanzienlijk verstorend effect hebben?**

Overeenkomstig artikel 5, lid 2, onder c), moet de nationale autoriteit nagaan of een incident een aanzienlijk verstorend effect zou hebben op de verlening van die dienst. In dit verband zijn er in artikel 6, lid 1, een aantal sectoroverschrijdende factoren vastgesteld waarmee rekening moet worden gehouden bij de beoordeling. Voorts is in artikel 6, lid 2, bepaald dat er bij de beoordeling, waar passend, ook rekening moet worden gehouden met sectorspecifieke factoren.

In artikel 6, lid 1, zijn de volgende **sectoroverschrijdende factoren** opgenomen:

- het aantal gebruikers die afhankelijk zijn van de door de betrokken entiteit verleende dienst;
- de afhankelijkheid van andere in bijlage II genoemde sectoren van de door die entiteit verleende dienst;
- de gevolgen die incidenten kunnen hebben, wat betreft mate en duur, voor economische en maatschappelijke activiteiten of de openbare veiligheid;
- het marktaandeel van die entiteit;
- de omvang van het geografische gebied dat door een incident kan worden getroffen;
- het belang van de entiteit voor de instandhouding van een toereikend dienstverleningsniveau, rekening houdend met de beschikbare alternatieven voor het verlenen van die dienst.

Wat **sectorspecifieke factoren** betreft, worden in overweging 28 enkele voorbeelden gegeven (zie tabel 4) die als nuttig richtsnoer kunnen dienen voor nationale autoriteiten.

[30] Zie artikel 5, lid 7, onder b).

Tabel 4: Voorbeelden van in aanmerking te nemen sectorspecifieke factoren bij de beoordeling van een aanzienlijk verstorend effect in geval van een incident

Sector	Voorbeelden van sectorspecifieke factoren
Energieleveranciers	volume of aandeel in de hoeveelheid nationaal geproduceerde energie
Olieleveranciers	dagelijkse volume van geleverde olie
Luchtvervoer (inclusief luchthavens en luchtvaartmaatschappijen) **Spoorvervoer** **Zeehavens**	aandeel in het nationale verkeersvolume; jaarlijkse aantal reizigers of vrachtactiviteiten
Bancaire- of financiëlemarktinfrastructuren	systemisch belang op basis van de totale activa; verhouding tussen de totale activa en het bbp
Gezondheidssector	jaarlijkse aantal patiënten die door een aanbieder worden behandeld
Waterproductie, -zuivering en -voorziening	volume en aantal en type gebruikers (zoals ziekenhuizen, openbare diensten, organisaties of individuen); bestaan van alternatieve waterbronnen om hetzelfde geografische gebied van water te voorzien

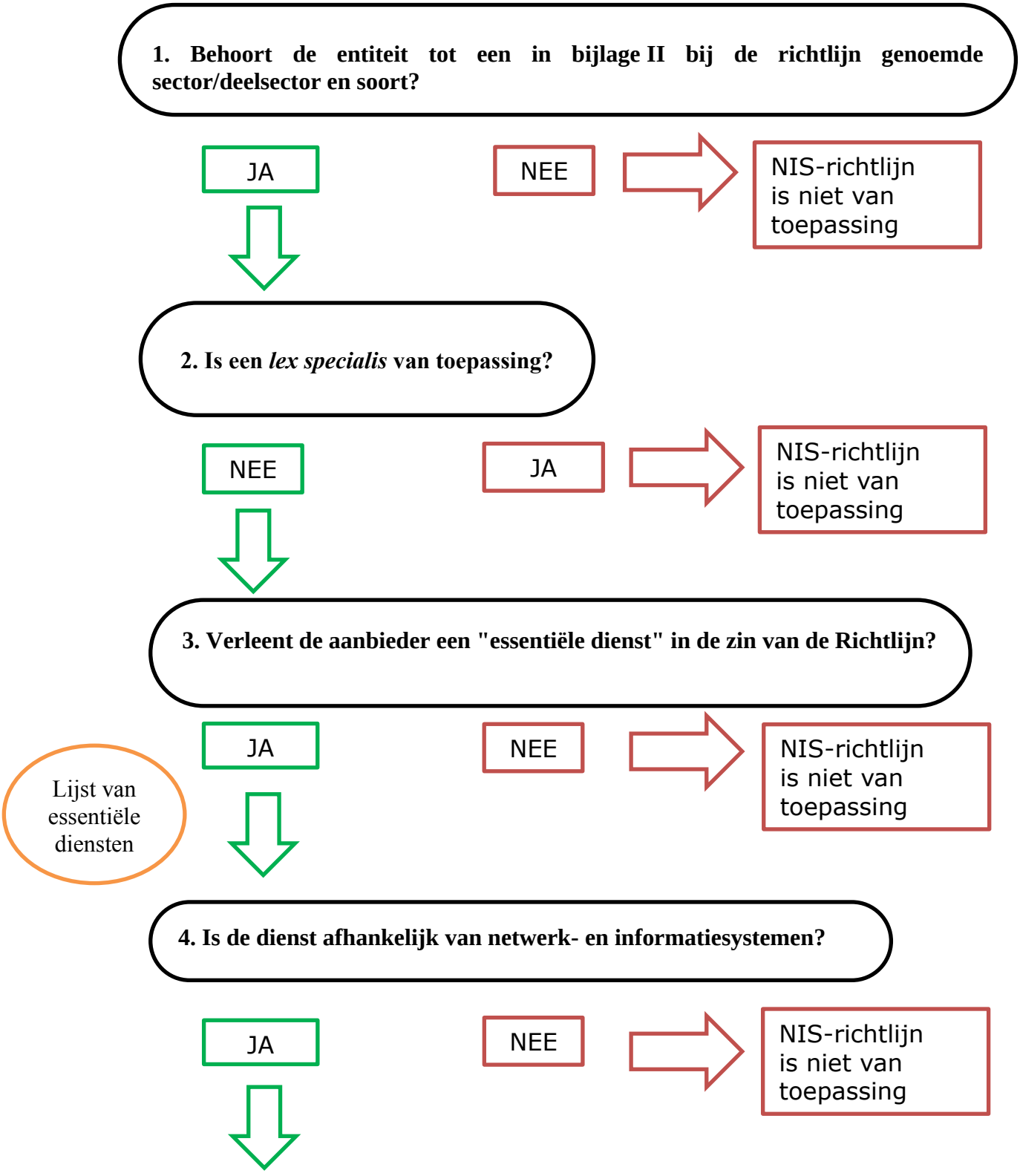
Er moet worden opgemerkt dat de lidstaten bij de beoordeling uit hoofde van artikel 5, lid 2, geen extra criteria mogen toevoegen bovenop die welke zijn opgenomen in deze bepaling, omdat dit zou kunnen leiden tot een lager aantal geïdentificeerde aanbieders van essentiële diensten en de in artikel 3 van de richtlijn opgenomen minimumharmonisatie voor aanbieders van essentiële diensten in gevaar zou kunnen brengen.

Stap 6 - **Verleent de betrokken aanbieder essentiële diensten in andere lidstaten?**

Stap 6 heeft betrekking op gevallen waarin een aanbieder essentiële diensten verleent in twee of meer lidstaten. Voordat het identificatieproces wordt afgerond, moeten de betrokken lidstaten overleg plegen overeenkomstig artikel 5, lid 4[31].

[31] Zie punt 4.1.7. voor meer informatie over de overlegprocedure.

Figuur 4: Identificatieproces in zes stappen



5. Zou een beveiligingsincident een aanzienlijk verstorend effect hebben?

Sectoroverschrijdende factoren (artikel 6, lid 1)

- **Aantal gebruikers** die afhankelijk zijn van de diensten
- **Afhankelijkheid** van andere essentiële diensten van de dienst
- Gevolgen die incidenten kunnen hebben voor **economische en maatschappelijke activiteiten** of de **openbare veiligheid**
- Mogelijke **omvang van het geografische gebied**

Sectorspecifieke factoren (in overweging 28 vermelde voorbeelden)

- **Energie**: volume of aandeel in de hoeveelheid nationaal geproduceerde energie
- **Vervoer**: aandeel in het nationale verkeersvolume en jaarlijkse aantal vrachtactiviteiten
- **Gezondheidszorg**: jaarlijkse aantal patiënten die door een aanbieder worden behandeld

JA

NEE → NIS-richtlijn is niet van toepassing

6. Verleent de betrokken aanbieder essentiële diensten in andere lidstaten?

JA

NEE → NIS-richtlijn is niet van toepassing

Verplicht overleg met de betrokken lidsta(a)t(en)

Vaststelling van nationale maatregelen (bv. lijst van aanbieders van essentiële diensten, beleids- en juridische maatregelen)

4.1.7. Grensoverschrijdend overlegproces

Indien een aanbieder essentiële diensten verleent in twee of meer lidstaten, moeten deze lidstaten onderling overleg plegen overeenkomstig artikel 5, lid 4, voordat het identificatieproces wordt afgerond. Dit overleg heeft tot doel het kritieke karakter van de aanbieder wat betreft de grensoverschrijdende gevolgen makkelijker te beoordelen.

Het beoogde resultaat van het overleg is dat de betrokken nationale autoriteiten hun argumenten en standpunten uitwisselen en bij voorkeur tot dezelfde conclusie komen wat betreft de identificatie van de betrokken aanbieder. De NIS-richtlijn sluit echter niet uit dat lidstaten uiteenlopende conclusies trekken over de vraag of een bepaalde entiteit al dan niet wordt geïdentificeerd als een aanbieder van essentiële diensten. In overweging 24 wordt vermeld dat de lidstaten in dit verband om de bijstand van de samenwerkingsgroep kunnen verzoeken.

De Commissie is van mening dat de lidstaten ernaar moeten streven overeenstemming te bereiken over deze vraagstukken om te voorkomen dat dezelfde onderneming een verschillende juridische status heeft in verschillende lidstaten. Afwijkingen zouden alleen in zeer uitzonderlijke gevallen mogen voorkomen, bijvoorbeeld indien een entiteit die als een aanbieder van essentiële diensten is geïdentificeerd in de ene lidstaat, marginale en geringe activiteiten heeft in de andere.

4.2. Beveiligingseisen

Overeenkomstig artikel 14, lid 1, moeten de lidstaten ervoor zorgen dat aanbieders van essentiële diensten gezien de stand van de techniek passende en evenredige technische en organisatorische maatregelen nemen om de risico's voor de beveiliging van netwerk- en informatiesystemen die zij bij het verstrekken van hun diensten gebruiken, te beheersen. Overeenkomstig artikel 14, lid 2, moeten passende maatregelen de gevolgen van een incident voorkomen en minimaliseren.

In een specifieke actielijn buigt de samenwerkingsgroep zich momenteel over niet-bindende richtsnoeren betreffende beveiligingsmaatregelen voor aanbieders van essentiële diensten[32]. De richtsnoeren worden door de groep voltooid in het vierde kwartaal van 2017. De Commissie moedigt de lidstaten aan om de door de samenwerkingsgroep te ontwikkelen richtsnoeren nauwgezet te volgen zodat de nationale bepalingen inzake beveiligingseisen zoveel mogelijk onderling afgestemd worden. Harmonisatie van deze eisen zou erg bevorderlijk zijn om aanbieders van essentiële diensten die vaak essentiële diensten aanbieden in meer dan één lidstaat, te helpen bij de nakoming ervan en zou het toezicht door nationale bevoegde autoriteiten en CSIRT's sterk vereenvoudigen.

[32] Voor de realisatie van deze actielijn werden lijsten van internationale normen, goede praktijken en methoden voor risicobeoordeling/-beheer verspreid voor alle onder de NIS-richtlijn vallende sectoren en deze werden gebruikt als input voor de voorgestelde beveiligingsaspecten en -maatregelen.

4.3 Meldingseisen

Overeenkomstig artikel 14, lid 3, moeten de lidstaten ervoor zorgen dat aanbieders van essentiële diensten "*incidenten met aanzienlijke gevolgen voor de continuïteit van de door hen verleende essentiële diensten*" melden. Bijgevolg moeten aanbieders van essentiële diensten geen kleine incidenten melden maar alleen ernstige incidenten die de continuïteit van de essentiële diensten verstoren. In artikel 4, punt 7, wordt een incident gedefinieerd als "*elke gebeurtenis met een daadwerkelijk schadelijk effect op de beveiliging van netwerk- en informatiesystemen*". De term "beveiliging van netwerk- en informatiesystemen" wordt in artikel 4, punt 2, verder gedefinieerd als "*het vermogen van netwerk- en informatiesystemen om met een bepaalde mate van betrouwbaarheid bestand te zijn tegen acties die de beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid van de opgeslagen, verzonden of verwerkte gegevens of de daaraan gerelateerde diensten die via die netwerk- en informatiesystemen worden aangeboden of toegankelijk zijn, in gevaar brengen*". Bijgevolg kan elke gebeurtenis die een schadelijk effect heeft niet alleen op de beschikbaarheid maar ook op de authenticiteit, integriteit of vertrouwelijkheid van gegevens of van gerelateerde diensten, potentieel de meldingsverplichting activeren. In feite is het mogelijk dat de continuïteit van de dienst als bedoeld in artikel 14, lid 3, in gevaar wordt gebracht, niet alleen in gevallen waarin er sprake is van fysieke beschikbaarheid, maar ook door een ander beveiligingsincident dat de behoorlijke werking van de dienst aantast[33].

Binnen de samenwerkingsgroep worden momenteel via een specifieke actielijn niet-bindende richtsnoeren voorbereid voor de melding van incidenten, met betrekking tot omstandigheden waarin aanbieders van essentiële diensten incidenten moeten melden overeenkomstig artikel 14, lid 7, alsmede het formaat en de procedure volgens welke nationale meldingen moeten plaatsvinden. Het is de bedoeling dat deze richtsnoeren in het vierde kwartaal van 2017 worden afgewerkt.

Uiteenlopende nationale meldingseisen kunnen leiden tot gebrekkige rechtszekerheid, meer complexe en omslachtige procedures en aanzienlijke administratieve kosten voor aanbieders die grensoverschrijdend actief zijn. De Commissie verheugt zich derhalve over de werkzaamheden van de samenwerkingsgroep. Zoals voor de beveiligingseisen moedigt de Commissie de lidstaten aan om de door de samenwerkingsgroep te ontwikkelen richtsnoeren nauwgezet te volgen zodat de nationale bepalingen inzake melding van incidenten zoveel mogelijk onderling afgestemd worden.

4.4. NIS-richtlijn, bijlage III: digitaledienstverleners

De digitaledienstverleners vormen de tweede categorie entiteiten die binnen het toepassingsgebied van de NIS-richtlijn vallen. Deze entiteiten worden beschouwd als belangrijke economische spelers wegens het feit dat zij door tal van ondernemingen worden gebruikt voor de verlening van eigen diensten, en verstoringen van de digitale dienstverlening zouden gevolgen hebben voor cruciale economische en maatschappelijke activiteiten.

[33] Hetzelfde geldt voor digitaledienstverleners.

4.4.1. Categorieën digitaledienstverleners

Artikel 4, punt 5, dat de "digitale dienst" definieert, verwijst naar de wettelijke definitie in punt b) van artikel 1, lid 1, van Richtlijn (EU) 2015/1535, door het toepassingsgebied te versmallen tot de in bijlage III vermelde soorten diensten. In punt b) van artikel 1, lid 1, van Richtlijn (EU) 2015/1535 wordt deze dienst met name omschreven als "*elke dienst die gewoonlijk tegen vergoeding, langs elektronische weg, op afstand en op individueel verzoek van een afnemer van diensten wordt verricht*" en in bijlage III bij deze richtlijn worden drie specifieke soorten diensten vermeld: onlinemarktplaatsen, onlinezoekmachines en cloudcomputerdiensten. In vergelijking met de aanbieders van essentiële diensten zijn de lidstaten krachtens de richtlijn niet verplicht de digitaledienstverleners te identificeren, die in dat geval onderworpen zouden worden aan de desbetreffende verplichtingen. De toepasselijke verplichtingen van de richtlijn, namelijk de in artikel 16 voorgeschreven beveiligings- en meldingseisen, zullen van toepassing zijn op alle binnen haar toepassingsgebied vallende digitaledienstverleners.

In de volgende onderdelen wordt nadere toelichting gegeven over drie soorten digitale diensten die onder de richtlijn vallen.

1. Aanbieders van onlinemarktplaats

Via een onlinemarktplaats wordt aan een grote groep en een breed gamma van ondernemingen de mogelijkheid geboden hun handelsactiviteiten ten aanzien van de consumenten te ontplooien en zakelijke relaties tussen ondernemingen aan te gaan. Hiermee wordt aan ondernemingen de basisinfrastructuur geboden om online en over de grenzen heen handel te drijven. Marktplaatsen spelen een belangrijke rol in de economie met name door kleine en middelgrote ondernemingen toegang te verlenen tot de ruimere digitale eengemaakte markt in de EU. De activiteiten van een aanbieder van onlinemarktplaats kunnen ook bestaan in het verstrekken van computerdiensten op afstand die de economische activiteit van de cliënt vergemakkelijken, onder meer door verwerking van transacties en aggregatie van gegevens over kopers, aanbieders en producten, zoals ook de ondersteuning van de zoekoperatie naar de passende producten, het leveren van deze producten, de deskundigheid in het sluiten van transacties en het samenbrengen van kopers en verkopers, tot die activiteiten kunnen behoren.

Het begrip "onlinemarktplaats" wordt gedefinieerd in artikel 4, punt 17, en nader toegelicht in overweging 15. Het wordt omschreven als een dienst die het consumenten en ondernemers mogelijk maakt online verkoop- of dienstenovereenkomsten met ondernemers te sluiten en het is de eindbestemming voor het sluiten van deze overeenkomsten. Een aanbieder als *E-bay* bijvoorbeeld kan worden beschouwd als een onlinemarktplaats omdat deze anderen de mogelijkheid biedt op zijn platform winkels op te zetten om producten en diensten online beschikbaar te stellen aan consumenten of bedrijven. Ook voor onlinewinkels voor applicaties die de distributie van applicaties en software verzorgen, wordt aangenomen dat zij onder de definitie van onlinemarktplaats vallen omdat ze ontwikkelaars van applicaties in staat stellen hun diensten aan consumenten of andere bedrijven te verkopen of beschikbaar te stellen. Daarentegen vallen diensten die fungeren als tussenschakel voor diensten van derden, zoals

Skyscanner, en diensten voor prijsvergelijking, die de gebruiker doorsturen naar de website van de handelaar waar het eigenlijke contract voor de dienst of het product wordt gesloten, niet onder de definitie van artikel 4, punt 17.

2. Aanbieders van onlinezoekmachines

Het begrip "onlinezoekmachine" wordt gedefinieerd in artikel 4, punt 18, en nader toegelicht in overweging 16. Het wordt omschreven als een digitale dienst die het gebruikers mogelijk maakt zoekacties te verrichten op in beginsel alle websites of websites in een bepaalde taal op basis van een zoekvraag. Zoekfuncties die beperkt zijn tot de inhoud van een specifieke website en websites voor prijsvergelijking vallen niet onder de definitie. Het soort zoekmachine als die welke EUR-LEX[34] ter beschikking stelt, kan niet worden beschouwd als zoekmachine in de zin van de richtlijn aangezien de zoekfunctie beperkt is tot de inhoud van die concrete website.

3. Aanbieders van cloudcomputerdiensten

Artikel 4, punt 19, definieert een "cloudcomputerdienst" als een digitale dienst die toegang mogelijk maakt tot een schaalbare en elastische pool van deelbare computercapaciteit en in overweging 17 wordt nadere toelichting gegeven over de termen "computercapaciteit", "schaalbare en elastische pool".

Cloudcomputing kan in het kort worden omschreven als een bijzonder soort computerdienst die gebruikmaakt van gedeelde capaciteit om gegevens op verzoek te verwerken, waarbij gedeelde capaciteit verwijst naar elk soort hardware- of softwarecomponenten (bv. netwerken, servers of andere infrastructuur, opslagcapaciteit, applicaties en diensten) die op verzoek aan gebruikers worden vrijgegeven voor de verwerking van gegevens. De term "deelbaar" definieert computercapaciteit waarin een groot aantal gebruikers dezelfde fysieke infrastructuur gebruiken voor de verwerking van gegevens. De computercapaciteit kan als deelbaar worden omschreven indien de pool van middelen die de aanbieder gebruikt, te allen tijde kan worden uitgebreid of beperkt naargelang van de behoeften van de gebruiker. De mogelijkheid bestaat dus dat datacentra of afzonderlijke componenten in één datacentrum toegevoegd of verwijderd worden indien de totale hoeveelheid van de computing- of opslagcapaciteit een update nodig heeft. De term "elastische pool" kan worden omschreven als veranderingen in het werkvolume door het automatisch aanmaken of afbouwen van capaciteit, zodat de beschikbare middelen op elk ogenblik zoveel mogelijk overeenstemmen met de bestaande vraag[35].

Momenteel bestaan er drie belangrijke soorten modellen van clouddiensten die een aanbieder kan verstrekken:

[34] Beschikbaar op: http://eur-lex.europa.eu/homepage.html.

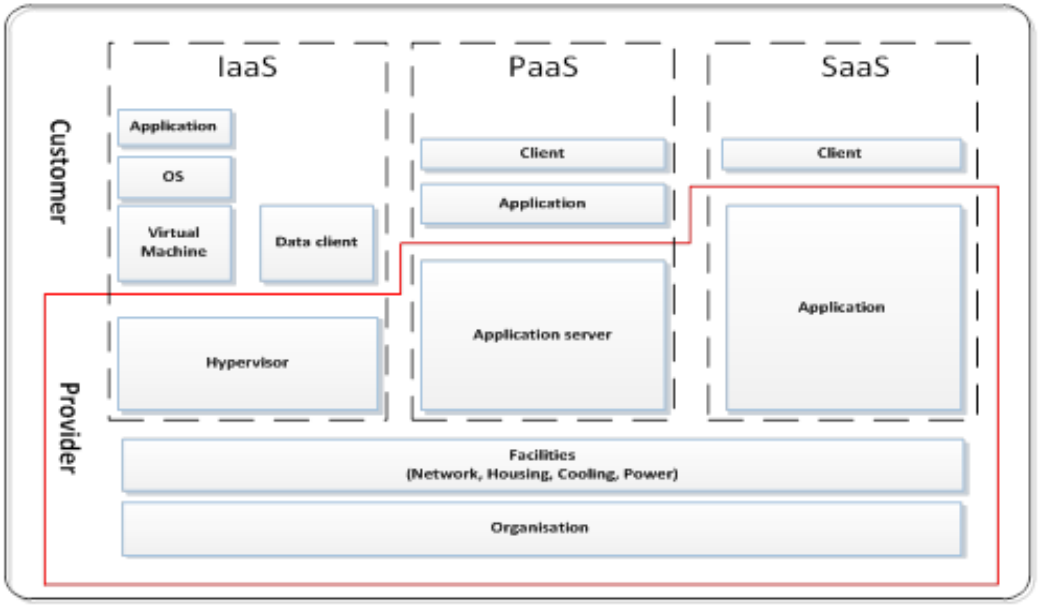
[35] Nikolas Roman Herbst, Samuel Kounev, Ralf Reussner, Karlsruhe Institute of Technology, "Elasticity in Cloud Computing: What It Is, and What It Is Not", beschikbaar op: https://sdqweb.ipd.kit.edu/publications/pdfs/HeKoRe2013-ICAC-Elasticity.pdf. Zie ook blz. 2-5 van COM(2012) 529.

- Infrastructuur als dienst (Infrastructure as a Service – IaaS): een categorie clouddiensten waarin het soort cloudcapaciteit dat aan de klant wordt geboden, een infrastructuur is. Deze omvat onder meer de virtuele levering van computercapaciteit in de vorm van hardware-, netwerk- en opslagdiensten. IaaS bedient server-, opslag-, netwerk- en besturingssystemen. Er wordt ondernemingsinfrastructuur geboden waarin een onderneming haar gegevens kan opslaan en de applicaties kan draaien die nodig zijn voor haar dagelijkse werking.

- Platform als dienst (Platform as a Service – PaaS): een categorie clouddiensten waarin het soort cloudcapaciteit dat aan de klant wordt geboden, een platform is. Deze omvat onder meer onlinecomputerplatforms waarop ondernemingen bestaande applicaties kunnen draaien of nieuwe applicaties kunnen ontwikkelen en testen.

- Software als dienst (Software as a service – SaaS): een categorie clouddiensten waarin het soort cloudcapaciteit dat aan de klant wordt geboden, een applicatie of computersoftware is die over het internet is opgezet. Dit type clouddiensten maakt dat het voor de eindgebruiker niet meer noodzakelijk is software te kopen, te installeren en te beheren, en heeft het voordeel dat de software door middel van een internetverbinding van op het even welke plaats toegankelijk kan worden gesteld.

Figuur 5: Dienstverleningsmodellen en activa in cloud computing



Uitvoerige richtsnoeren over specifieke thema's met betrekking tot de cloud[36] en een leidraad over de basisbeginselen voor cloud computing[37] zijn verstrekt door het Enisa.

[36] Beschikbaar op: https://www.enisa.europa.eu/topics/cloud-and-big-data/cloud-security.
[37] Enisa, *Cloud Security Guide for SMEs* (2015). Beschikbaar op: https://www.enisa.europa.eu/publications/cloud-security-guide-for-smes.

4.4.2. Beveiligingseisen

Overeenkomstig artikel 16, lid 1, moeten de lidstaten ervoor zorgen dat digitaledienstverleners passende technische en organisationele maatregelen nemen om de risico's voor de beveiliging van netwerk- en informatiesystemen die zij bij hun activiteiten gebruiken, te beheersen. Voor de beveiligingsmaatregelen moet rekening worden gehouden met de stand van de techniek en met de volgende vijf elementen: i) beveiliging van systemen en voorzieningen; ii) afhandeling van incidenten; iii) het beheer van de bedrijfscontinuïteit; iv) toezicht, controle en tests; v) naleving van internationale normen.

In dit verband is de Commissie gemachtigd overeenkomstig artikel 16, lid 8, uitvoeringshandelingen vast te stellen waarin genoemde aspecten nader worden gespecificeerd en een hoog niveau van harmonisatie wordt gegarandeerd voor deze dienstenaanbieders. De uitvoeringshandeling zal door de Commissie naar verwachting worden vastgesteld in het najaar van 2017. Voorts moeten de lidstaten ervoor zorgen dat digitaledienstverleners de nodige maatregelen nemen om de gevolgen van incidenten te voorkomen en te minimaliseren ter waarborging van de continuïteit van hun diensten.

4.4.3. Meldingseisen

Digitaledienstverleners moeten ernstige incidenten melden aan de bevoegde autoriteiten of de CSIRT's. Overeenkomstig artikel 16, lid 3, van de NIS-richtlijn wordt de meldingsverplichting voor digitaledienstverleners geactiveerd in gevallen waarin het beveiligingsincident substantiële gevolgen heeft voor de verlening van de dienst. Wat de vaststelling van de gevolgen betreft, worden in artikel 16, lid 4, met name vijf parameters vermeld die de digitaledienstverleners in aanmerking moeten nemen. In dit verband is de Commissie overeenkomstig artikel 16, lid 8, gemachtigd uitvoeringshandelingen vast te stellen om de parameters nader te omschrijven. De nadere specificatie van deze parameters zal deel uitmaken van de uitvoeringshandeling tot nadere omschrijving van de in punt 4.4.2 vermelde beveiligingseisen, die de Commissie voornemens is aan te nemen in het najaar.

4.4.4. Risicogebaseerde regelgevende aanpak

Artikel 17 bepaalt dat digitaledienstverleners onderworpen zijn aan regelgevingstoezicht achteraf door de bevoegde nationale autoriteiten. De lidstaten moeten ervoor zorgen dat de bevoegde autoriteiten maatregelen nemen wanneer zij bewijs in handen krijgen dat een digitaledienstverlener niet voldoet aan de in artikel 16 van de richtlijn vastgestelde eisen.

Voorts is de Commissie overeenkomstig artikel 16, leden 8 en 9, gemachtigd om uitvoeringshandelingen vast te stellen met betrekking tot de eisen inzake melding en beveiliging, hetgeen voor digitaledienstverleners een hoger niveau van harmonisatie zal meebrengen. Daarnaast is het overeenkomstig artikel 16, lid 10, de lidstaten niet toegestaan digitaledienstverleners andere beveiligings- of meldingseisen op te leggen dan die waarin de richtlijn voorziet, tenzij voor gevallen waarin deze maatregelen noodzakelijk zijn om essentiële staatsfuncties te beschermen, in het bijzonder ter bescherming van de nationale veiligheid, en om het onderzoek, de opsporing en de vervolging van strafbare feiten mogelijk te maken.

Rekening houdend met het grensoverschrijdende karakter van digitaledienstverleners volgt de richtlijn ten slotte niet het model van meerdere parallelle rechtsmachten maar is de aanpak gebaseerd op het criterium van de voornaamste vestiging van de onderneming in de EU[38]. Deze aanpak maakt het mogelijk om één enkele reeks voorschriften op digitaledienstverleners toe te passen, met één bevoegde autoriteit die belast is met het toezicht, hetgeen erg belangrijk is omdat tal van digitaledienstverleners hun diensten tegelijk in meerdere lidstaten aanbieden. Door de toepassing van deze aanpak wordt de nalevingslast voor digitaledienstverleners tot een minimum beperkt en wordt de goede werking van de digitale eengemaakte markt gegarandeerd.

4.4.5. Jurisdictie

Zoals hierboven vermeld, valt de onderneming overeenkomstig artikel 18, lid 1, van de richtlijn onder de jurisdictie van de lidstaat waar zij haar hoofdvestiging heeft. In gevallen waarin de concrete digitaledienstverlener diensten aanbiedt in de EU maar niet op het grondgebied van de EU is gevestigd, is hij krachtens artikel 18, lid 2, verplicht een vertegenwoordiger in de Unie aan te wijzen. In dat geval zal de lidstaat waar de vertegenwoordiger is gevestigd, jurisdictie uitoefenen over de onderneming. In gevallen waarin een digitaledienstverlener diensten in een lidstaat aanbiedt maar geen vertegenwoordiger in de Unie heeft aangewezen, kan de lidstaat in principe optreden tegen de dienstverlener omdat deze zijn uit de richtlijn voortvloeiende verplichtingen niet nakomt.

4.4.6. Vrijstelling van beveiligings- en meldingsverplichtingen voor digitaledienstverleners van beperkte omvang

Overeenkomstig artikel 16, lid 11, zijn digitaledienstverleners die kleine en micro-ondernemingen zijn, zoals gedefinieerd in Aanbeveling 2003/361/EG van de Commissie[39], uitgesloten van het toepassingsgebied van de in artikel 16 omschreven beveiligings- en meldingseisen. Dit betekent dat ondernemingen met minder dan 50 werknemers die een jaarlijkse omzet en/of een jaarlijks balanstotaal van minder dan 10 miljoen EUR hebben, niet aan deze verplichtingen onderworpen zijn. Bij het bepalen van de omvang van de entiteit heeft het geen belang of de betrokken onderneming uitsluitend digitale diensten in de zin van de NIS-richtlijn dan wel ook andere diensten verstrekt.

5. Verhouding tussen NIS-richtlijn en andere wetgeving

In dit onderdeel wordt ingegaan op de bepalingen betreffende *lex specialis*, waarin artikel 1, lid 7, van de NIS-richtlijn voorziet. De drie voorbeelden van *lex specialis* die de Commissie tot dusver heeft beoordeeld, worden van uitleg voorzien en de beveiligings- en meldingseisen die van toepassing zijn op aanbieders van telecommunicatiediensten en van vertrouwensdiensten, worden nader toegelicht.

[38] Zie met name artikel 18 van de richtlijn.
[39] PB L 24 van 20.5.2003, blz. 36.

5.1. NIS-richtlijn, artikel 1, lid 7: *lex specialis*-bepaling

Overeenkomstig artikel 1, lid 7, van de NIS-richtlijn zijn de bepalingen inzake beveiligings- en/of meldingseisen voor digitaledienstverleners of aanbieders van essentiële diensten krachtens de richtlijn niet van toepassing indien een sectorspecifieke wetgeving van de Unie in beveiligings- en meldingseisen voorziet die ten minste feitelijk gelijkwaardig zijn aan de overeenkomstige verplichtingen van de NIS-richtlijn. De lidstaten moeten rekening houden met artikel 1, lid 7, bij de algemene omzetting van de richtlijn en de Commissie informatie verschaffen over de toepassing van de *lex specialis*-bepalingen.

Methodiek

Bij de beoordeling van de gelijkwaardigheid van een onderdeel van Europese sectorspecifieke wetgeving met de desbetreffende bepalingen van de NIS-richtlijn moet bijzondere aandacht worden geschonken aan de vraag of de beveiligingsverplichtingen in de sectorspecifieke wetgeving maatregelen bevatten die de beveiliging van netwerk- en informatiesystemen zoals gedefinieerd in artikel 4, punt 2, van de richtlijn verzekeren.

Wat meldingseisen betreft, wordt in artikel 14, lid 3, en artikel 16, lid 3, van de NIS-richtlijn bepaald dat aanbieders van essentiële diensten en digitaledienstverleners incidenten met aanzienlijke gevolgen voor de verlening van de dienst onverwijld aan de bevoegde autoriteiten of het CSIRT moeten melden. Bijzondere aandacht moet hierbij worden besteed aan de verplichtingen van de aanbieder/digitaledienstverlener om in de melding informatie op te nemen die de bevoegde autoriteit of het CSIRT in staat stelt de grensoverschrijdende gevolgen van het beveiligingsincident te beoordelen.

Momenteel bestaat er geen sectorspecifieke wetgeving voor de categorie van de digitaledienstverleners die in beveiligings- en meldingseisen voorziet welke vergelijkbaar zijn met de in artikel 16 van de NIS-richtlijn omschreven eisen, en die in aanmerking komt voor de toepassing van artikel 1, lid 7, van de NIS-richtlijn[40].

Wat aanbieders van essentiële diensten betreft, zijn de financiële sector en met name het bankwezen en de infrastructuur voor de financiële markt als bedoeld in de punten 3 en 4 van bijlage II momenteel onderworpen aan beveiligings- en/of meldingseisen uit hoofde van sectorspecifieke EU-wetgeving. Dit is te danken aan het feit dat de veiligheid en soliditeit van door financiële instellingen gebruikte IT- en netwerk- en informatiesystemen een belangrijk onderdeel vormt van de eisen inzake operationele risico's die financiële instellingen moeten nakomen op basis van Europese wetgeving.

Voorbeelden

i) Richtlijn betalingsdiensten 2

Met betrekking tot de banksector en met name voor zover het gaat om de levering van betalingsdiensten door kredietinstellingen als bedoeld in punt 1) van artikel 4 van

[40] Dit geldt onverminderd de melding van een inbreuk in verband met persoonsgegevens aan de toezichthoudende autoriteit in de zin van artikel 33 van de algemene verordening gegevensbescherming.

Verordening (EU) nr. 575/2013, voorziet de zogenoemde richtlijn betalingsdiensten 2 (hierna "PSD 2")[41] in beveiligings- en meldingseisen, die omschreven zijn in de artikelen 95 en 96 van deze richtlijn.

Artikel 95, lid 1, schrijft meer bepaald voor dat betalingsdienstaanbieders een regeling moeten treffen die voorziet in passende risicobeperkende maatregelen en controlemechanismen ter beheersing van de operationele en beveiligingsrisico's die verbonden zijn aan de door hen aangeboden betalingsdiensten. Deze maatregelen moeten onder meer voorzien in de vaststelling en handhaving van doelmatige procedures voor het beheersen van incidenten, waaronder detectie en classificatie van grote operationele incidenten en veiligheidsincidenten. In de overwegingen 95 en 96 van de PSD 2 wordt de aard van deze beveiligingsmaatregelen verder toegelicht. Blijkens de voorschriften hebben de maatregelen tot doel de veiligheidsrisico's met betrekking tot de bij het aanbieden van betalingsdiensten gebruikte netwerk- en informatiesystemen te beheren. Deze beveiligingsvoorschriften kunnen derhalve worden beschouwd als ten minste feitelijk gelijkwaardig aan de overeenkomstige bepaling van artikel 14, leden 1 en 2, van de NIS-richtlijn.

Wat de meldingseisen betreft, legt artikel 96, lid 1, van de PSD 2 aanbieders van betalingsdiensten de verplichting op de bevoegde autoriteit onverwijld in kennis te stellen van ernstige beveiligingsincidenten. Zoals artikel 14, lid 5, van de NIS-richtlijn, legt artikel 96, lid 2, van de PSD 2 de bevoegde autoriteit de verplichting op de bevoegde autoriteiten van andere lidstaten op de hoogte te brengen indien het incident voor hen relevant is. Deze verplichting impliceert tegelijkertijd dat de melding van beveiligingsincidenten informatie moet bevatten zodat de autoriteiten de grensoverschrijdende gevolgen van een incident kunnen beoordelen. Krachtens artikel 96, lid 3, onder a), van de PSD 2 is EBA in dit verband gemachtigd in samenwerking met de ECB richtsnoeren op te stellen over de precieze inhoud en het formaat van de melding.

Bijgevolg kan worden geconcludeerd dat overeenkomstig artikel 1, lid 7, van de NIS-richtlijn de in de artikelen 95 en 96 van de PSD 2 bepaalde beveiligingseisen en meldingseisen toegepast moeten worden in plaats van de overeenkomstige bepalingen van artikel 14 van de NIS-richtlijn voor zover er sprake is van het aanbieden van betalingsdiensten door kredietinstellingen.

ii) Verordening (EU) nr. 648/2012 van het Europees Parlement en de Raad van 4 juli 2012 betreffende otc-derivaten, centrale tegenpartijen en transactieregisters

Wat de financiëlemarktinfrastructuur betreft, bevat Verordening (EU) nr. 648/2012 in samenhang met Gedelegeerde Verordening (EU) 153/2013 van de Commissie voorschriften voor beveiliging voor centrale tegenpartijen, die beschouwd kunnen worden als *lex specialis*. Deze wetgeving bevat met name technische en organisatorische maatregelen met betrekking tot de beveiliging van netwerk- en informatiesystemen die zelfs gedetailleerder zijn en verder

[41] Richtlijn (EU) 2015/2366, PB L 337 van 23.12.2015, blz. 35.

gaan dan de vereisten van artikel 14, leden 1 en 2, van de NIS-richtlijn en derhalve geacht kunnen worden overeen te stemmen met de voorschriften van artikel 1, lid 7, van de NIS-richtlijn wat de veiligheidseisen betreft.

Volgens artikel 26, lid 1, van Verordening (EU) nr. 648/2012 moet de entiteit beschikken over "*solide governancesystemen, waaronder een duidelijke organisatiestructuur met duidelijk omschreven, transparante en samenhangende verantwoordelijkheden, effectieve procedures voor het vaststellen, beheren, bewaken en rapporteren van de risico's waaraan zij blootstaat of bloot kan komen te staan, en adequate interne controlemechanismen, zoals goede administratieve en boekhoudkundige procedures*". Volgens artikel 26, lid 3, moet de CTP zorgen voor een organisatiestructuur die de continuïteit en ordelijke werking bij het verrichten van haar diensten en activiteiten garandeert, en moet zij gebruikmaken van passende en evenredige systemen, middelen en procedures.

Verder verduidelijkt artikel 26, lid 6, dat een CTP moet zorgen voor "*informatietechnologiesystemen die zijn aangepast aan de complexiteit, de diversiteit en het soort diensten en activiteiten die worden verricht, teneinde te garanderen dat strenge normen in acht worden genomen op het gebied van beveiliging en integriteit en vertrouwelijkheid van de bijgehouden informatie*". Artikel 34, lid 1, voorziet in de verplichte vaststelling, toepassing en instandhouding van een passend plan voor bedrijfscontinuïteit en noodherstel dat moet zorgen voor een tijdig herstel van de bedrijfsactiviteiten.

Deze verplichtingen zijn verder gespecificeerd in Gedelegeerde Verordening EU/153/2013 van de Commissie van 19 december 2012 tot aanvulling van Verordening (EU) nr. 648/2012 van het Europees Parlement en de Raad met betrekking tot technische reguleringsnormen inzake vereisten voor centrale tegenpartijen[42]. Artikel 4 van deze verordening legt CTP's met name de verplichting op passende instrumenten voor risicobeheer te ontwikkelen om het beheer van en de rapportering over alle relevante risico's mogelijk te maken, en het soort maatregelen verder te omschrijven (bijvoorbeeld gebruik van robuuste informatie- en risicobeheersystemen, beschikbaarstelling van middelen, deskundigheid en toegang tot alle relevante informatie voor de functie van risicobeheer, beschikbaarheid van toereikende interne controlemechanismen zoals degelijke administratieve en boekhoudkundige procedures ter ondersteuning van de raad van een CTP om de toereikendheid en effectiviteit van de gedragslijnen, procedures en systemen voor risicobeheer te bewaken en te beoordelen).

Daarnaast maakt artikel 9 uitdrukkelijk melding van de beveiliging van informatietechnologiesystemen en worden concrete technische en organisatorische maatregelen opgelegd om een robuust kader van informatiebeveiliging te onderhouden voor het beheer van IT-veiligheidsrisico's. Deze maatregelen moeten passende mechanismen en procedures omvatten om de beschikbaarheid van de diensten te garanderen en om de authenticiteit, integriteit en vertrouwelijkheid van gegevens te beschermen.

[42] PB L 52 van 23.2.2013, blz. 41.

- **iii) Richtlijn 2014/65/EU van het Europees Parlement en de Raad van 15 mei 2014 betreffende markten voor financiële instrumenten en tot wijziging van Richtlijn 2002/92/EG en Richtlijn 2011/61/EU[43]**
-

Wat handelsplatformen betreft, zijn exploitanten daarvan krachtens artikel 48, lid 1, van Richtlijn 2014/65/EU verplicht de continuïteit van de bedrijfsuitoefening te verzekeren in geval van een storing van hun handelssystemen. Deze algemene verplichting is onlangs nader gepreciseerd en aangevuld bij Gedelegeerde Verordening (EU) 2017/584[44] van 14 juli 2016 houdende aanvulling van Richtlijn 2014/65/EU van het Europees Parlement en de Raad met betrekking tot technische reguleringsnormen ter specificatie van de organisatorische vereisten voor handelsplatformen[45]. Artikel 23, lid 1, van deze verordening bepaalt met name dat handelsplatformen moeten beschikken over procedures en regelingen voor fysieke en elektronische beveiliging om hun systemen tegen misbruik of onbevoegde toegang te beschermen en om de integriteit van gegevens te waarborgen. Deze maatregelen moeten het mogelijk maken de risico's van aanvallen op informatiesystemen te voorkomen of tot een minimum te beperken.

Artikel 23, lid 2, schrijft verder voor dat de maatregelen en regelingen van de exploitanten het mogelijk moeten maken risico's onverwijld te omschrijven en te beheren wanneer deze betrekking hebben op onbevoegde toegang, interferenties tussen systemen waardoor de werking van informatiesystemen ernstig wordt belemmerd of afgebroken, en interferenties tussen gegevens waardoor de beschikbaarheid, de integriteit of de authenticiteit van gegevens in gevaar komt. Daarnaast moeten handelsplatformen krachtens artikel 15 van de verordening over doeltreffende regelingen voor bedrijfscontinuïteit beschikken om een toereikende stabiliteit van het systeem te garanderen en verstorende incidenten te bestrijden. Deze maatregelen dienen de exploitant met name in staat te stellen de handel binnen ongeveer twee uur na een verstorend incident te hervatten en moeten er ook voor zorgen dat de hoeveelheid gegevens die verloren is gegaan, nagenoeg tot nul wordt beperkt.

Voorts moeten volgens artikel 16 de omschreven maatregelen voor de bestrijding en het beheer van verstorende incidenten deel uitmaken van het bedrijfscontinuïteitsplan van het handelsplatform en moeten door de exploitant een bepaald aantal elementen in aanmerking worden genomen wanneer het bedrijfscontinuïteitsplan wordt aangenomen (bijvoorbeeld de oprichting van een specifiek team voor veiligheidsoperaties dat een regelmatig te hernieuwen effectbeoordeling verricht voor de omschrijving van de risico's).

Uit de inhoud van deze beveiligingsmaatregelen kan worden opgemaakt dat zij bedoeld zijn om het risico met betrekking tot de beschikbaarheid, de authenticiteit, de integriteit en de vertrouwelijkheid van gegevens of verleende diensten te bestrijden. Bijgevolg kan worden geconcludeerd dat de hierboven bedoelde sectorspecifieke EU-wetgeving

[43] PB L 173 van 12.6.2014, blz. 349.
[44] PB L 87 van 31.3.2017, blz. 350.
[45] http://ec.europa.eu/finance/securities/docs/isd/mifid/rts/160714-rts-7_en.pdf.

beveiligingsverplichtingen bevat die ten minste feitelijk evenwaardig zijn met de overeenkomstige verplichtingen van artikel 14, leden 1 en 2, van de NIS-richtlijn.

5.2. NIS-richtlijn, artikel 1, lid 3: telecomaanbieders en verleners van vertrouwensdiensten

Overeenkomstig artikel 1, lid 3, zijn de in de richtlijn voorgeschreven beveiligings- en meldingseisen niet van toepassing op aanbieders die onderworpen zijn aan de voorschriften van de artikelen 13 bis en 13 ter van Richtlijn 2002/21/EG. De artikelen 13 bis en 13 ter zijn van toepassing op ondernemingen die openbare communicatienetwerken of openbaar beschikbare elektronischecommunicatiediensten aanbieden. Voor het aanbieden van openbare communicatienetwerken of openbaar beschikbare elektronischecommunicatiediensten moet de onderneming bijgevolg voldoen aan de verplichtingen inzake veiligheid en kennisgeving van Richtlijn 2002/21/EG.

Indien dezelfde onderneming ook andere diensten aanbiedt, zoals digitale diensten (bv. cloudcomputing of een onlinemarktplaats) vermeld in bijlage III bij de NIS-richtlijn, of diensten zoals DNS- of IXP-diensten bedoeld in punt 7 van bijlage II bij de NIS-richtlijn, zal zij onderworpen zijn aan de beveiligings- en meldingseisen van de NIS-richtlijn voor het aanbieden van deze bijzondere diensten. Er zij opgemerkt dat aangezien aanbieders van diensten vermeld in punt 7 van bijlage II tot de categorie van aanbieders van essentiële diensten behoren, de lidstaten verplicht zijn het identificatieproces krachtens artikel 5, lid 2, te verrichten om uit te maken welke individuele aanbieders van DNS-, IXP- of TLD-diensten aan de voorschriften van de NIS-richtlijn dienen te voldoen. Dit betekent dat na afloop van deze beoordeling alleen de DNS-, IXP- of TLD-aanbieders die aan de criteria van artikel 5, lid 2, van de NIS-richtlijn voldoen, verplicht zullen zijn te voldoen aan de voorschriften van de NIS-richtlijn.

In artikel 1, lid 3, wordt voorts bepaald dat de in de richtlijn bedoelde beveiligings- en meldingseisen niet van toepassing zijn op verleners van vertrouwensdiensten die krachtens artikel 19 van Verordening (EU) nr. 910/2014 aan soortgelijke eisen zijn onderworpen.

6. Bekendgemaakte documenten in verband met nationale cyberbeveiligingsstrategieën

	Lidstaat	Titel van strategie en beschikbare links
1.	Oostenrijk	*Austrian Cybersecurity Strategy* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/AT_NCSS.pdf (EN)
2.	België	*Securing Cyberspace* (2012) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/ncss-be-fr (FR)
3.	Bulgarije	*Cyber Resilient Bulgaria 2020* (2016) http://www.cyberbg.eu/ (BG)
4.	Kroatië	*The national cyber security strategy of the republic of Croatia* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CRNCSSEN.pdf (EN)
5.	Tsjechië	*National cyber security strategy of the Czech Republic for the period from 2015 to 2020* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CzechRepublic_Cyber_Security_Strategy.pdf (EN)
6.	Cyprus	*Cybersecurity Strategy of the Republic of Cyprus* (2012) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CybersecurityStrategyoftheRepublicofCyprusv10_English.pdf (EN)

7.	Denemarken	*The Danish Cyber and Information Security Strategy* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/DK_NCSS.pdf (EN)
8.	Estland	*Cyber Security Strategy* (2014) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Estonia_Cyber_security_Strategy.pdf (EN)
9.	Finland	*Finland´s Cyber security Strategy* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/FinlandsCyberSecurityStrategy.pdf (EN)
10.	Frankrijk	*French national digital security strategy* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/France_Cyber_Security_Strategy.pdf (EN)
11.	Ierland	*National Cyber Security Strategy 2015-2017* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS_IE.pdf (EN)
12.	Italië	*National Strategic Framework for Cyberspace Security* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/IT_NCSS.pdf (EN)
13.	Duitsland	*Cyber-security Strategy for Germany* (2016) http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/ModerneVerwaltung-OeffentlicherDienst/Informationsgesellschaft/cybersicherheitsstrategie-2016.pdf?__blob=publicationFile (DE)

14.	Hongarije	*National Cyber Security Strategy of Hungary* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/HU_NCSS.pdf (EN)
15.	Letland	*Cyber Security Strategy of Latvia 2014–2018* (2014) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/lv-ncss (EN)
16.	Litouwen	*The programme for the development of electronic information security (cyber-security) for 2011–2019* (2011) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Lithuania_Cyber_Security_Strategy.pdf (EN)
17.	Luxemburg	*National Cybersecurity Strategy II (2015)* https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Luxembourg_Cyber_Security_strategy.pdf (EN)
18.	Malta	*National Cyber Security Strategy Green Paper* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSSGreenPaper.pdf (EN)
19.	Nederland	*National Cyber Security Strategy 2* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS2Engelseversie.pdf (EN)
20.	Polen	*Cyberspace Protection Policy of the Republic of Poland* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/copy_of_PO_NCSS.pdf (EN)

21.	Roemenië	*Cybersecurity Strategy of Romania* (2011) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/StrategiaDeSecuritateCiberneticaARomaniei.pdf (RO)
22.	Portugal	*National Cyberspace Security Strategy* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/portuguese-national-cyber-security-strategy/view (EN)
23.	Slowakije	*Cyber Security Concept of the Slovak Republic for 2015 – 2020* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/cyber-security-concept-of-the-slovak-republic-1 (EN)
24.	Slovenië	*Cyber Security Strategy establishing a system to ensure a high level of cyber security* (2016) http://www.uvtp.gov.si/fileadmin/uvtp.gov.si/pageuploads/Cyber_Security_Strategy_Slovenia.pdf (EN)
25.	Spanje	*National Cyber Security Strategy* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS_ESen.pdf (EN)
26.	Zweden	*The Swedish National Cybersecurity Strategy* (2017) http://www.government.se/49edf4/contentassets/b5f956be6c50412188fb4e1d72a5e501/fact-sheet-a-national-cyber-security-strategy.pdf (EN)
27.	Verenigd Koninkrijk	*National Cyber Security Strategy (2016-2021)* (2016) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national_cyber_security_strategy_2016.pdf (EN)

7. Lijst van goede praktijken en aanbevelingen van het Enisa

Voor respons bij incidenten

- ✓ Strategieën voor respons bij incidenten en samenwerking in geval van cybercrisis[46]

Voor afhandeling van incidenten

- ✓ Project voor automatisering van incidentafhandeling[47]
- ✓ Gids voor goede praktijken inzake incidentbeheer[48]

Voor indeling en taxonomie van incidenten

- ✓ Overzicht van bestaande taxonomieën[49]
- ✓ Gids voor goede praktijken bij het gebruik van taxonomieën in voorkoming en opsporing van incidenten[50]

Voor maturiteit van CSIRT's

- ✓ Uitdagingen voor nationale CSIRT's in Europa in 2016: studie over maturiteit van CSIRT's[51]
- ✓ Studie over maturiteit van CSIRT's – Evaluatieproces[52]
- ✓ Richtsnoeren voor wijze van beoordeling van maturiteit voor nationale en gouvernementele CSIRT's[53]

Voor capaciteitsopbouw en opleiding van CSIRT's

- ✓ Gids voor goede praktijken inzake opleidingsmethoden[54]

Om informatie te vinden over bestaande CSIRT's in Europa – Overzicht van CSIRT's per land[55]

[46] Enisa, *Strategies for incident response and cyber crisis cooperation* (2016). Beschikbaar op:https://www.enisa.europa.eu/publications/strategies-for-incident-response-and-cyber-crisis-cooperation
[47] Meer informatie: https://www.enisa.europa.eu/topics/csirt-cert-services/community-projects/incident-handling-automation
[48] Enisa, *Good Practice Guide for Incident Management* (2010). Beschikbaar op:https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management
[49] Meer informatie: https://www.enisa.europa.eu/topics/csirt-cert-services/community-projects/existing-taxonomies
[50] Enisa, *A good practice guide of using taxonomies in incident prevention and detection* (2017). Beschikbaar op:https://www.enisa.europa.eu/publications/using-taxonomies-in-incident-prevention-detection
[51] Enisa, *Challenges for National CSIRTs in Europe in 2016: Study on CSIRT Maturity* (2017). Beschikbaar op:https://www.enisa.europa.eu/publications/study-on-csirt-maturity
[52] Enisa, *Study on CSIRT Maturity – Evaluation Process* (2017). Beschikbaar op:https://www.enisa.europa.eu/publications/study-on-csirt-maturity-evaluation-process
[53] Enisa, CSIRT Capabilities. *How to assess maturity? Guidelines for national and governmental CSIRTs* (2016). Beschikbaar op: https://www.enisa.europa.eu/publications/csirt-capabilities
[54] Enisa, *Good Practice Guide on Training Methodologies* (2014). Beschikbaar op:https://www.enisa.europa.eu/publications/good-practice-guide-on-training-methodologies
[55] Meer informatie: https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map