EUROPESE
COMMISSIE

Brussel, 4.10.2017
COM(2017) 476 final

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

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

NL

Inleiding

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), die werd aangenomen op 6 juli 2016, is de eerste horizontale EU-wetgeving waarmee de uitdagingen op het gebied van cyberbeveiliging worden aangepakt en vormt een echte doorbraak voor de weerbaarheid en samenwerking op het vlak van cyberbeveiliging in Europa.

De richtlijn heeft drie hoofddoelstellingen:

- de nationale vermogens op het gebied van cyberbeveiliging verbeteren;
- de samenwerking op EU-niveau opbouwen; en
- een cultuur van risicobeheer en melding van incidenten bevorderen bij belangrijke economische actoren, met name aanbieders van essentiële diensten voor de instandhouding van economische en maatschappelijke activiteiten en digitaledienstverleners.

De NIS-richtlijn vormt een hoeksteen van de EU-respons op de toenemende cyberdreigingen en -uitdagingen die gepaard gaan met de digitalisering van ons economisch en maatschappelijk leven, en de tenuitvoerlegging ervan is bijgevolg een essentieel onderdeel van het cyberbeveiligingspakket dat is gepresenteerd op 13 september 2017. De EU kan niet volledig doeltreffend reageren zolang de NIS-richtlijn niet volledig is omgezet in alle EU-lidstaten. Dit werd ook als een kritiek punt aangemerkt in de mededeling van de Commissie van 2016 over het versterken van het Europese cyberbeveiligingssysteem[2].

Aangezien de NIS-richtlijn nieuw is en de snel evoluerende cyberdreigingen een dringende aanpak vergen, moet bijzondere aandacht worden besteed aan de uitdagingen waarmee alle actoren worden geconfronteerd bij hun inspanningen om de richtlijn tijdig en naar behoren om te zetten. Gezien de omzettingstermijn van 9 mei 2018 en de termijn van 9 november 2018 voor de identificatie van aanbieders van essentiële diensten ondersteunt de Commissie het omzettingsproces van de lidstaten en hun werkzaamheden in de samenwerkingsgroep op dit vlak.

Deze mededeling en de bijbehorende bijlage zijn gebaseerd op de voorbereidende werkzaamheden van de Commissie, de analyse van de tenuitvoerlegging van de NIS-richtlijn tot dusver, de input van het Europees Agentschap voor netwerk- en informatiebeveiliging (Enisa) en de besprekingen met de lidstaten in de omzettingsfase van de richtlijn, met name in

[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.
[2] COM(2016) 410 final.

het kader van de samenwerkingsgroep[3]. Deze mededeling vormt een aanvulling op de aanzienlijke inspanningen die tot dusver zijn geleverd, met name door middel van:

- De intensieve werkzaamheden van de samenwerkingsgroep, die een werkplan heeft afgesproken dat hoofdzakelijk is gericht op de omzetting van de NIS-richtlijn, en met name op de identificatie van aanbieders van essentiële diensten en hun verplichtingen inzake beveiligingseisen en meldingen van incidenten. Hoewel de richtlijn het aan de lidstaten overlaat om omzettingsbepalingen inzake aanbieders van essentiële diensten vast te stellen, erkennen de lidstaten het belang van een geharmoniseerde aanpak op dit vlak[4].
- De invoering en snelle inwerkingtreding van het netwerk van Computer Security Incident Response Teams (CSIRT's) overeenkomstig artikel 12, lid 1, van de richtlijn. Sindsdien legt dit netwerk de basis voor een gestructureerde operationele samenwerking op Europees niveau.

Voor zowel het beleidsmatige als het operationele niveau die in deze twee structuren te onderscheiden zijn, is de volledige inzet van alle lidstaten van essentieel belang met het oog op de doelstelling van een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie.

Die inspanningen zullen worden versterkt door deze mededeling en de bijbehorende bijlage, waarin de beste praktijken van de lidstaten die relevant zijn voor de uitvoering van de richtlijn worden gebundeld en met elkaar worden vergeleken, nadere richtsnoeren worden verstrekt over de wijze van uitvoering van de richtlijn en specifieke bepalingen nader worden toegelicht. De algemene doelstelling bestaat erin de lidstaten ondersteuning te bieden met het oog op een doeltreffende en geharmoniseerde uitvoering van de NIS-richtlijn in de hele EU.

Deze mededeling zal verder worden aangevuld met de nieuwe uitvoeringsverordening van de Commissie betreffende de nadere specificatie van de elementen en parameters met betrekking tot de eisen inzake beveiliging en melding van incidenten voor digitaledienstverleners, overeenkomstig artikel 16, lid 8, van de NIS-richtlijn. Deze verordening zal de uitvoering van de richtlijn vergemakkelijken wat betreft de verplichtingen met betrekking tot digitaledienstverleners[5].

Deze mededeling presenteert de belangrijkste conclusies van de analyse van de thema's die gelden als belangrijke referentiepunten en mogelijke inspiratiebronnen voor de omzetting in

[3] Een mechanisme voor strategische samenwerking tussen de lidstaten overeenkomstig artikel 11 van de NIS-richtlijn.

[4] De samenwerkingsgroep werkt momenteel aan referentierichtsnoeren over onder meer: de criteria voor het vaststellen van het kritieke karakter van een aanbieder overeenkomstig artikel 5, lid 2, van de richtlijn; de omstandigheden waarin aanbieders van essentiële diensten verplicht zijn incidenten te melden op grond van artikel 14, lid 7, van de richtlijn; en de beveiligingseisen voor aanbieders van essentiële diensten in overeenstemming met artikel 14, leden 1 en 2.

[5] Het ontwerp van uitvoeringsverordening is beschikbaar voor openbare raadpleging op https://ec.europa.eu/info/law/better-regulation/have-your-say_nl.

nationaal recht. Het gaat hier voornamelijk om bepalingen inzake de capaciteiten en verplichtingen van de lidstaten met betrekking tot de onder de richtlijn vallende entiteiten. In de bijlage wordt dieper ingegaan op de gebieden die volgens de Commissie het meest gebaat zijn bij praktische richtsnoeren voor de omzetting, namelijk door specifieke bepalingen van de richtlijn toe te lichten en te interpreteren, en door de beste praktijken en de ervaring tot dusver met de richtlijn voor te stellen.

Naar de doeltreffende uitvoering van de NIS-richtlijn

Het doel van de NIS-richtlijn bestaat erin een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie tot stand te brengen. Dit betekent dat de beveiliging van het internet en de particuliere netwerken en informatiesystemen die de werking van onze samenleving en economie ondersteunen, moet worden verbeterd. Het eerste belangrijke element in dit verband is de paraatheid van de lidstaten, die moet worden gewaarborgd door middel van nationale cyberbeveiligingsstrategieën, zoals omschreven in de richtlijn, en de werkzaamheden van de CSIRT's en de bevoegde nationale autoriteiten.

Volledigheid van de nationale strategieën

Het is belangrijk dat de lidstaten de omzetting van de NIS-richtlijn aangrijpen als een kans om hun nationale cyberbeveiligingsstrategie te herzien in het licht van de in de bijlage vermelde tekortkomingen, beste praktijken en nieuwe uitdagingen.

Hoewel de richtlijn begrijpelijkerwijs is toegespitst op de ondernemingen en diensten die van cruciaal belang zijn, moet de cyberbeveiliging van de economie en de samenleving als geheel worden aangepakt op een holistische en consistente manier in het licht van de steeds toenemende afhankelijkheid van ICT. Bijgevolg zullen integrale nationale strategieën die verder gaan dan de minimumvereisten van de NIS-richtlijn (d.w.z. breder dan de sectoren en diensten als vermeld in respectievelijk bijlage II en III bij de richtlijn) leiden tot een hoger algemeen niveau van beveiliging van netwerk- en informatiesystemen.

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. Met het oog op de doelstellingen van de richtlijn is het dan ook van fundamenteel belang dat er ambitieuze beslissingen worden genomen om toereikende financiële en personele middelen vrij te maken voor de doeltreffende uitvoering van de nationale strategieën, en ook voldoende middelen toe te wijzen aan de nationale bevoegde autoriteiten en de CSIRT's.

Doeltreffendheid van de uitvoering en handhaving

Overeenkomstig artikel 8 van de richtlijn moeten respectieve nationale bevoegde autoriteiten en centrale contactpunten worden aangewezen, wat essentieel is om de NIS-richtlijn en de grensoverschrijdende samenwerking efficiënt uit te voeren. Op dit vlak hebben de lidstaten een meer gecentraliseerde dan wel gedecentraliseerde aanpak gekozen. Wanneer lidstaten een meer gedecentraliseerde aanpak hanteren om nationale bevoegde autoriteiten aan te wijzen,

blijken regelingen voor nauwe samenwerking tussen de verschillende autoriteiten en het centrale contactpunt uiterst belangrijk (*zie tabel 1 in punt 3.2. in de bijlage*). Dit zal de uitvoering doeltreffender en de handhaving gemakkelijker maken.

Er kan worden voortgebouwd op de eerder opgedane ervaring met de bescherming van kritieke informatie-infrastructuur (CIIP) om een optimaal bestuursmodel te ontwikkelen voor de lidstaten, zodat de NIS-richtlijn een doeltreffende sectorale uitvoering krijgt en een coherente horizontale benadering wordt aangenomen (*zie punt 3.1. in de bijlage*).

Versterkte capaciteiten van de nationale CSIRT's

Zonder doeltreffende nationale CSIRT's in de hele EU die over de nodige middelen beschikken, zoals voorgeschreven in artikel 9 van de NIS-richtlijn, zal de EU te kwetsbaar blijven voor grensoverschrijdende cyberdreigingen. Derhalve kunnen de lidstaten overwegen de werkingssfeer van de CSIRT's uit te breiden naar andere sectoren en diensten waarop de richtlijn niet van toepassing is (*zie punt 3.3. in de bijlage*). Hierdoor kunnen de nationale CSIRT's operationele ondersteuning bieden in geval van cyberincidenten in ondernemingen en organisaties waarop de richtlijn niet van toepassing is, maar die ook belangrijk zijn voor de samenleving en de economie. Daarnaast kunnen de lidstaten ten volle gebruik maken van de aanvullende financieringsmogelijkheden die worden geboden door het programma van de Connecting Europe Facility (CEF) voor digitaleddiensteninfrastructuren op het gebied van cyberbeveiliging, dat is opgezet om de capaciteiten van de nationale CSIRT's en de onderlinge samenwerking te versterken (*zie punt 3.5 in de bijlage*).

Consistentie van het identificatieproces voor aanbieders van essentiële diensten

Overeenkomstig artikel 5 van de NIS-richtlijn moeten de lidstaten uiterlijk op 9 november 2018 de entiteiten identificeren die als aanbieders van essentiële diensten zullen worden beschouwd. Voor deze taak kunnen de lidstaten overwegen de definities en richtsnoeren in deze mededeling consistent toe te passen, zodat soortgelijke entiteiten die een soortgelijke rol spelen in de interne markt op consistente wijze worden geïdentificeerd als aanbieders van essentiële diensten in andere lidstaten. De lidstaten kunnen eveneens overwegen het toepassingsgebied van de NIS-richtlijn uit te breiden naar overheidsinstanties, gezien de rol die deze spelen in de samenleving en de economie in het algemeen (*zie de punten 2.1. en 4.1.3 in de bijlage*).

Het zou zeer nuttig zijn om de nationale aanpak van de identificatie van aanbieders van essentiële diensten zo veel mogelijk op elkaar af te stemmen, met name aan de hand van de door de samenwerkingsgroep opgestelde richtsnoeren (*zie punt 4.1.2 in de bijlage*), omdat dit zal leiden tot een meer geharmoniseerde toepassing van de bepalingen van de richtlijn en bijgevolg tot een lager risico op marktversnippering. Indien aanbieders van essentiële diensten in twee of meer lidstaten essentiële diensten verlenen, moet worden gestreefd naar een overeenkomst tussen de lidstaten in het kader van de overlegprocedure in de zin van artikel 5, lid 4, over de consistente identificatie van entiteiten (*zie punt 4.1.7 in de bijlage*), om te

voorkomen dat dezelfde entiteit wordt onderworpen aan verschillende regelgeving in verschillende lidstaten.

Indiening bij de Commissie van informatie over de identificatie van aanbieders van essentiële diensten

Overeenkomstig artikel 5, lid 7, moeten de lidstaten de Commissie informatie verstrekken over de nationale maatregelen die de identificatie van aanbieders van essentiële diensten mogelijk maken, de lijst van essentiële diensten, het aantal geïdentificeerde aanbieders van essentiële diensten en het belang van die aanbieders ten aanzien van de sector. Daarnaast wordt de lidstaten verzocht om melding te maken van de drempels, waar zij voorkomen, die in het identificatieproces worden gebruikt voor het bepalen van het relevante verleningsniveau of het belang van die bepaalde aanbieder voor de instandhouding van een toereikend dienstverleningsniveau. De lidstaten kunnen eveneens overwegen de lijsten van geïdentificeerde aanbieders van essentiële diensten te verstrekken aan de Commissie, indien nodig op vertrouwelijke basis, aangezien dit zou leiden tot een nauwkeurigere en kwalitatief betere beoordeling door de Commissie (*zie de punten 4.1.5. en 4.1.6. in de bijlage*).

Onderling afgestemde aanpak van de eisen inzake beveiliging en melding van incidenten voor aanbieders van essentiële diensten

Wat betreft de verplichtingen inzake beveiligingseisen en melding van incidenten voor aanbieders van essentiële diensten (artikel 14, leden 1 tot en met 3), kan een onderling afgestemde aanpak met betrekking tot beveiligingseisen en melding van incidenten, als ondersteuning voor aanbieders van essentiële diensten om te voldoen aan hun verplichtingen inzake grensoverschrijdende naleving, een maximaal effect op de eengemaakte markt teweegbrengen. In dit opzicht blijven de werkzaamheden van de samenwerkingsgroep met het oog op een richtsnoer de referentie (*zie de punten 4.2. en 4.3. in de bijlage*).

In geval van een grootschalig cyberincident waarbij meerdere lidstaten zijn betrokken, is het zeer waarschijnlijk dat de verplichte melding van het incident wordt verricht door een aanbieder van essentiële diensten of een digitaledienstverlener overeenkomstig artikel 14, lid 3, en artikel 16, lid 3, of op vrijwillige basis door een andere entiteit waarop de richtlijn niet van toepassing is, overeenkomstig artikel 20, lid 1. In overeenstemming met de aanbeveling van de Commissie voor een gecoördineerde respons op grootschalige cyberincidenten en -crises kunnen de lidstaten overwegen hun nationale aanpak op elkaar af te stemmen zodat zij op basis van deze meldingen zo spoedig mogelijk relevante informatie kunnen verstrekken aan de bevoegde autoriteiten of het CSIRT van andere betrokken lidstaten. Nauwkeurige en bruikbare informatie is van cruciaal belang om het aantal besmettingen terug te dringen of zwakke punten aan te pakken voordat deze verder worden uitgebuit.

In de geest van partnerschap om de NIS-richtlijn ten volle te benutten, is de Commissie voornemens in het kader van de Connecting Europe Facility steun te verlenen aan alle relevante belanghebbenden die betrokken zijn bij deze wetgeving. Hoewel de nadruk werd

gelegd op de capaciteitsopbouw van de CSIRT's en een platform voor snelle en doeltreffende operationele samenwerking met het oog op een versterkt CSIRT-netwerk, zal de Commissie nu nagaan hoe de financiering in het kader van de Connecting Europe Facility ook ten goede kan komen aan de nationale bevoegde autoriteiten, de aanbieders van essentiële diensten en digitaledienstverleners.

Conclusie

In het licht van de naderende termijn van 9 mei 2018 voor de omzetting van de NIS-richtlijn in nationaal recht en de termijn van 9 november 2018 voor de identificatie van aanbieders van essentiële diensten moeten de lidstaten passende maatregelen nemen om ervoor te zorgen dat de in de NIS-richtlijn vastgestelde bepalingen en samenwerkingsmodellen de best mogelijke instrumenten op EU-niveau opleveren om een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie tot stand te brengen. De Commissie verzoekt de lidstaten bij dit proces rekening te houden met de relevante informatie, richtsnoeren en aanbevelingen in deze mededeling.

Deze mededeling kan verder worden aangevuld met andere maatregelen, waaronder de maatregelen die worden ontwikkeld bij de lopende werkzaamheden in het kader van de samenwerkingsgroep.