I

(Wetgevingshandelingen)

RICHTLIJNEN

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 RAAD VAN DE EUROPESE UNIE,

Gezien het Verdrag betreffende de werking van de Europese Unie, en met name artikel 114,

Gezien het voorstel van de Europese Commissie,

Na toezending van het ontwerp van wetgevingshandeling aan de nationale parlementen,

Gezien het advies van het Europees Economisch en Sociaal Comité ([1]),

Handelend volgens de gewone wetgevingsprocedure ([2]),

Overwegende hetgeen volgt:

(1) Netwerk- en informatiesystemen en -diensten spelen een cruciale rol in de samenleving. De betrouwbaarheid en beveiliging ervan zijn essentieel voor economische en maatschappelijke activiteiten, en met name voor de goede werking van de interne markt.

(2) De omvang, de frequentie en de gevolgen van beveiligingsincidenten nemen toe en vormen een grote bedreiging voor de goede werking van netwerk- en informatiesystemen. Die systemen kunnen ook een doelwit worden van opzettelijke schadelijke acties die bedoeld zijn om de werking van de systemen te verstoren of te onderbreken. Zulke incidenten kunnen de economische bedrijvigheid belemmeren, aanzienlijke financiële verliezen opleveren, het gebruikersvertrouwen ondermijnen en de economie van de Unie ernstige schade toebrengen.

(3) Netwerk- en informatiesystemen, en hoofdzakelijk het internet, spelen een cruciale rol bij het faciliteren van het grensoverschrijdende verkeer van goederen, diensten en personen. Vanwege dat transnationale karakter kan een ernstige verstoring van die systemen, al dan niet opzettelijk en ongeacht waar deze plaatsvindt, individuele lidstaten en de Unie als geheel treffen. De beveiliging van netwerk- en informatiesystemen is daarom essentieel voor de goede werking van de interne markt.

(4) Voortbouwend op de aanzienlijke vooruitgang die in het Europees Forum voor de lidstaten is geboekt bij het bevorderen van gesprekken en de uitwisseling van goede beleidspraktijken, waaronder de ontwikkeling van beginselen voor Europese cybercrisissamenwerking, moet een samenwerkingsgroep worden ingesteld die bestaat uit vertegenwoordigers van de lidstaten, de Commissie en het Agentschap van de Europese Unie voor netwerk- en

([1]) PB C 271 van 19.9.2013, blz. 133.
([2]) Standpunt van het Europees Parlement van 13 maart 2014 (nog niet bekendgemaakt in het Publicatieblad) en standpunt van de Raad in eerste lezing van 17 mei 2016 (nog niet bekendgemaakt in het Publicatieblad). Standpunt van het Europees Parlement van 6 juli 2016 (nog niet bekendgemaakt in het Publicatieblad).

informatiebeveiliging (Enisa) en die tot doel heeft de strategische samenwerking tussen de lidstaten op het gebied van beveiliging van netwerk- en informatiesystemen te ondersteunen en te faciliteren. Om die groep doeltreffend en inclusief te laten zijn, is het van essentieel belang dat alle lidstaten beschikken over minimumcapaciteiten en een strategie om op hun grondgebied een hoog niveau van beveiliging van netwerk- en informatiesystemen te waarborgen. Daarnaast moeten eisen inzake beveiliging en melding van toepassing zijn op aanbieders van essentiële diensten en digitaledienstverleners teneinde een cultuur van risicobeheer te bevorderen en ervoor te zorgen dat de ernstigste incidenten worden gemeld.

(5) De bestaande capaciteiten volstaan niet om een hoog niveau van beveiliging van netwerk- en informatiesystemen in de Unie te waarborgen. Omdat de paraatheidsniveaus van de lidstaten sterk uiteenlopen, is de aanpak in de Unie gefragmenteerd. Dit leidt tot ongelijke niveaus van bescherming van consumenten en bedrijven en ondermijnt het algemene niveau van beveiliging van netwerk- en informatiesystemen in de Unie. Het feit dat er geen gemeenschappelijke eisen voor aanbieders van essentiële diensten en digitaledienstverleners gelden, maakt het dan weer onmogelijk een overkoepelend en doeltreffend mechanisme voor samenwerking op het niveau van de Unie op te zetten. Universiteiten en onderzoekscentra spelen een doorslaggevende rol bij het stimuleren van onderzoek, ontwikkeling en innovatie op deze gebieden.

(6) Om doeltreffend te kunnen reageren op de uitdagingen voor de beveiliging van netwerk- en informatiesystemen is er dus behoefte aan een overkoepelende aanpak op het niveau van de Unie die gemeenschappelijke minimumvereisten inzake capaciteitsopbouw en planning, informatie-uitwisseling, samenwerking en gemeenschappelijke beveiligingseisen voor aanbieders van essentiële diensten en digitaledienstverleners omvat. Het staat aanbieders van essentiële diensten en digitaledienstverleners echter vrij beveiligingsmaatregelen te treffen die strenger zijn dan die waarin in deze richtlijn voorziet.

(7) Om alle relevante incidenten en risico's te bestrijken, dient deze richtlijn van toepassing te zijn op zowel aanbieders van essentiële diensten als digitaledienstverleners. De verplichtingen van aanbieders van essentiële diensten en digitaledienstverleners dienen echter niet van toepassing te zijn op ondernemingen die openbare communicatienetwerken of openbare elektronischecommunicatiediensten in de zin van Richtlijn 2002/21/EG van het Europees Parlement en de Raad ([1]) aanbieden, welke onderworpen zijn aan de in die richtlijn vastgestelde specifieke veiligheids- en integriteitseisen, noch op verleners van vertrouwensdiensten in de zin van Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad ([2]), die onderworpen zijn aan de in die verordening vastgestelde veiligheidseisen.

(8) Deze richtlijn moet de mogelijkheid onverlet laten dat elke lidstaat de nodige maatregelen neemt om de bescherming van de wezenlijke belangen van zijn veiligheid te waarborgen, de openbare orde en de openbare veiligheid te garanderen, en het onderzoek, de opsporing en de vervolging van strafbare feiten mogelijk te maken. Overeenkomstig artikel 346 van het Verdrag betreffende de werking van de Europese Unie (VWEU) mag geen enkele lidstaat verplicht worden inlichtingen te verstrekken waarvan de openbaarmaking naar zijn mening strijdig is met zijn wezenlijke veiligheidsbelangen. In dit verband zijn Besluit 2013/488/EU van de Raad ([3]) en geheimhoudingsovereenkomsten of informele geheimhoudingsovereenkomsten, zoals het verkeerslichtprotocol („Traffic Light Protocol"), van belang.

(9) Bepaalde sectoren van de economie zijn reeds of zullen in de toekomst mogelijk worden gereglementeerd door sectorspecifieke rechtshandelingen van de Unie waarin regels inzake de beveiliging van netwerk- en informatiesystemen zijn opgenomen. Wanneer deze rechtshandelingen van de Unie bepalingen bevatten die eisen inzake de beveiliging van netwerk- en informatiesystemen of de melding van incidenten voorschrijven, moeten die bepalingen gelden voor zover zij eisen bevatten die minstens feitelijk gelijkwaardig zijn aan de in deze richtlijn voorgeschreven verplichtingen. De lidstaten dienen dan de bepalingen van zulke sectorspecifieke rechtshandelingen van de Unie, inclusief die inzake jurisdictie, toe te passen en het in deze richtlijn voorgeschreven identificatieproces voor aanbieders van essentiële diensten niet uit te voeren. In dit verband moeten de lidstaten de Commissie informatie over de toepassing van zulke lex-specialisbepalingen verschaffen. Bij het bepalen of de in sectorspecifieke rechtshandelingen van de Unie opgenomen eisen inzake de beveiliging van netwerk- en informatiesystemen en de melding van incidenten gelijkwaardig zijn aan die in deze richtlijn, dienen uitsluitend de bepalingen van de toepasselijke rechtshandelingen van de Unie en de toepassing daarvan in de lidstaten in acht te worden genomen.

(10) In de sector vervoer over water hebben beveiligingseisen voor ondernemingen, schepen, havenfaciliteiten, havens en scheepvaartbegeleidingsdiensten overeenkomstig rechtshandelingen van de Unie betrekking op alle activiteiten, met inbegrip van de radio- en telecommunicatiesystemen en computersystemen en netwerken. Een deel van de verplichte procedures omvat de melding van alle incidenten en moet derhalve worden beschouwd als lex specialis, voor zover die eisen ten minste gelijkwaardig zijn aan de overeenkomstige bepalingen van deze richtlijn.

([1]) Richtlijn 2002/21/EG van het Europees Parlement en de Raad van 7 maart 2002 inzake een gemeenschappelijk regelgevingskader voor elektronischecommunicatienetwerken en -diensten (kaderrichtlijn) (PB L 108 van 24.4.2002, blz. 33).

([2]) Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG (PB L 257 van 28.8.2014, blz. 73).

([3]) Besluit 2013/488/EU van de Raad van 23 september 2013 betreffende de beveiligingsvoorschriften voor de bescherming van gerubriceerde EU-informatie (PB L 274 van 15.10.2013, blz. 1).

(11) Bij het identificeren van aanbieders in de sector vervoer over water, moeten de lidstaten rekening houden met bestaande en toekomstige internationale codes en richtsnoeren die zijn ontwikkeld door met name de Internationale Maritieme Organisatie, teneinde voor een coherente aanpak voor individuele maritieme aanbieders te zorgen.

(12) De regulering van en het toezicht op bancaire- en financiëlemarktinfrastructuren is in hoge mate geharmoniseerd op Unieniveau, via het gebruik van primaire en secundaire Unierecht en de normen die samen met de Europese toezichthoudende autoriteiten zijn ontwikkeld. Binnen de bankenunie worden de toepassing van en het toezicht op deze eisen gewaarborgd door het gemeenschappelijk toezichtsmechanisme. Voor de lidstaten die geen deel uitmaken van de bankenunie worden deze gewaarborgd door de bevoegde bankentoezichthouders van de lidstaten. Op andere terreinen van de regulering van de financiële sector zorgt het Europees systeem voor financieel toezicht ook voor een grote mate van gemeenschappelijkheid en convergentie in de toezichtpraktijken. De Europese Autoriteit voor effecten en markten heeft ook een rechtstreekse toezichtrol voor bepaalde entiteiten (te weten: ratingbureaus en transactieregisters).

(13) Operationeel risico is een cruciaal onderdeel van de prudentiële regulering en het prudentieel toezicht op bancaire-en financiëlemarktinfrastructuren. Het bestrijkt alle activiteiten, met inbegrip van de beveiliging, de integriteit en de veerkracht van netwerk- en informatiesystemen. De eisen voor deze systemen, die vaak verder gaan dan de eisen van deze richtlijn, zijn opgenomen in een aantal rechtshandelingen van de Unie, met inbegrip van, maar niet beperkt tot regels betreffende toegang tot het bedrijf van kredietinstellingen en het prudentieel toezicht op kredietinstellingen en beleggingsondernemingen en regels betreffende prudentiële vereisten voor kredietinstellingen en beleggingsondernemingen, waaronder eisen inzake het operationele risico; regels betreffende markten voor financiële instrumenten, waaronder eisen inzake risicobeoordeling voor beleggingsondernemingen en gereglementeerde markten; regels betreffende otc-derivaten, centrale tegenpartijen en transactieregisters, waaronder eisen inzake het operationele risico voor centrale tegenpartijen en transactieregisters; en regels betreffende de verbetering van de effectenafwikkeling in de Unie en betreffende centrale effectenbewaarinstellingen, waaronder eisen inzake het operationele risico. Bovendien maken eisen inzake melding van incidenten deel uit van de normale toezichtspraktijken in de financiële sector en zijn zij vaak opgenomen in de handleidingen voor toezicht. De lidstaten moeten deze regels en eisen voor ogen houden bij de toepassing van lex specialis.

(14) Zoals de Europese Centrale Bank in haar advies van 25 juli 2014 ([1]) stelt, laat deze richtlijn de regeling krachtens het Unierecht voor het toezicht op betalings- en afwikkelingssystemen van Eurosysteem onverlet. Het zou een goede zaak zijn als de autoriteiten die verantwoordelijk zijn voor dat toezicht met de voor deze richtlijn bevoegde autoriteiten ervaringen zouden uitwisselen over kwesties in verband met de beveiliging van netwerk- en informatiesystemen. Hetzelfde geldt voor niet tot het eurogebied behorende leden van het Europees Stelsel van centrale banken die dergelijk toezicht op betalings- en afwikkelingssystemen uitoefenen op basis van de nationale wet- en regelgeving.

(15) Een onlinemarktplaats maakt het consumenten en ondernemers mogelijk online verkoop- of dienstenovereenkomsten met ondernemers te sluiten en is de eindbestemming voor het sluiten van deze overeenkomsten. Zij dient geen betrekking te hebben op onlinediensten die slechts als tussenschakel voor diensten van een derde fungeren waarmee uiteindelijk een overeenkomst kan worden gesloten. Derhalve dient zij geen betrekking te hebben op onlinediensten die de prijzen van bepaalde producten of diensten van verschillende ondernemers vergelijken en die de gebruiker vervolgens automatisch naar de geprefereerde ondernemer doorverwijzen om het product te kopen. Tot de computerdiensten die op de onlinemarktplaats worden aangeboden, kunnen de verwerking van transacties, de verzameling van gegevens of de profilering van gebruikers behoren. Applicatiewinkels, die als onlinewinkels de digitale distributie van applicaties of softwareprogramma's van derden mogelijk maken, moeten als een soort onlinemarktplaats worden beschouwd.

(16) Een onlinezoekmachine maakt het de gebruiker mogelijk om in principe over elke website een zoekopdracht over elk mogelijk onderwerp uit te voeren. Er kan ook specifiek op websites in een bepaalde taal mee worden gezocht. De definitie van een onlinezoekmachine in deze richtlijn dient geen betrekking te hebben op zoekfuncties die beperkt zijn tot de inhoud van een specifieke website, ongeacht of de zoekfunctie door een externe zoekmachine wordt aangeboden. Zij dient evenmin betrekking te hebben op onlinediensten die de prijzen van bepaalde producten of diensten van andere ondernemers vergelijken en die de gebruiker vervolgens automatisch doorverwijst naar de geprefereerde ondernemer om het product te kopen.

(17) Cloudcomputerdiensten bestrijken een breed scala aan activiteiten die volgens verschillende modellen kunnen worden verricht. Voor de toepassing van deze richtlijn wordt onder „cloudcomputerdiensten" verstaan: diensten die toegang tot een schaalbare en elastische groep van gedeelde computercapaciteit geven. Die „computercapaciteit" heeft betrekking op capaciteit zoals netwerken, servers en andere infrastructuur, opslag, applicaties en diensten. Met „schaalbaar" wordt bedoeld: computercapaciteit die, ongeacht de geografische locatie van de capaciteit, op flexibele wijze door aanbieders van cloudcomputerdiensten wordt toegewezen teneinde met schommelingen in de vraag te kunnen omgaan. Met „elastische groep" wordt bedoeld: de computercapaciteit die afhankelijk van de vraag ter beschikking wordt gesteld en wordt vrijgegeven teneinde deze beschikbare capaciteit

([1]) PB C 352 van 7.10.2014, blz. 4.

snel te kunnen verhogen en verlagen naargelang van het werkvolume. Met „gedeeld" wordt bedoeld: de computercapaciteit die ter beschikking wordt gesteld aan meerdere gebruikers die een gemeenschappelijke toegang tot de dienst hebben, maar waarbij de verwerking voor elke gebruiker afzonderlijk plaatsvindt, hoewel de dienst door middel van dezelfde elektronische uitrusting wordt verleend.

(18) Een internetknooppunt kenmerkt zich door zijn functie netwerken met elkaar te interconnecteren. Een internetknooppunt verschaft geen toegang tot een netwerk of doet dienst als dienstverlener of -aanbieder. Een internetknooppunt verleent evenmin andere diensten die geen verband houden met interconnectie, wat niet uitsluit dat een internetknooppuntaanbieder dergelijke diensten mag verlenen. Een internetknooppunt is er om technisch en organisatorisch afzonderlijke netwerken met elkaar te verbinden. De term „autonoom systeem" wordt gebruikt ter aanduiding van een technisch op zichzelf staand netwerk.

(19) Het dient aan de lidstaten te zijn om te bepalen welke entiteiten aan de criteria van de definitie van aanbieder van essentiële diensten voldoen. Met het oog op een consistente benadering moeten de lidstaten de definitie van aanbieder van essentiële diensten op coherente wijze toepassen. Daartoe voorziet de richtlijn in de beoordeling van de entiteiten die actief zijn in de specifieke sectoren en deelsectoren, de opstelling van een lijst van essentiële diensten, het in overweging nemen van een gemeenschappelijke lijst van sectoroverschrijdende factoren om te bepalen of een potentieel incident een aanzienlijk verstorend effect zou hebben, een raadplegingsproces waaraan betrokken lidstaten deelnemen in het geval van entiteiten die in meer dan één lidstaat diensten verlenen, en de ondersteuning van de samenwerkingsgroep bij het identificatieproces. Opdat eventuele veranderingen in de markt nauwkeurig weerspiegeld zouden worden, moet de lijst van geïdentificeerde aanbieders op regelmatige basis door de lidstaten worden geëvalueerd en, indien nodig, geactualiseerd. Ten slotte moeten de lidstaten aan de Commissie de informatie verstrekken die nodig is om na te gaan in hoeverre deze gemeenschappelijke methodologie heeft bijgedragen tot de consistente toepassing van de definitie door de lidstaten.

(20) Bij het identificatieproces voor aanbieders van essentiële diensten moeten de lidstaten, ten minste voor elke in deze richtlijn vermelde deelsector, nagaan welke diensten als essentieel voor de instandhouding van kritieke maatschappelijke en economische activiteiten moeten worden beschouwd en moeten zij beoordelen of de in de sectoren en deelsectoren in deze richtlijn bedoelde entiteiten die deze diensten verlenen, aan de identificatiecriteria voor aanbieders voldoen. Bij de beoordeling of een entiteit een voor de instandhouding van kritieke maatschappelijke of economische activiteiten essentiële dienst verleent, volstaat het na te gaan of die entiteit verlener is van een in de lijst van essentiële diensten opgenomen dienst. Voorts moet worden aangetoond dat de verlening van de essentiële dienst afhankelijk is van netwerk- en informatiesystemen. Bij de beoordeling of een incident een aanzienlijk verstorend effect op de verlening van de dienst zou hebben, ten slotte, moeten de lidstaten rekening houden met een aantal sectoroverschrijdende factoren evenals, in voorkomend geval, met sectorspecifieke factoren.

(21) Voor het vaststellen van de identiteit van aanbieders van essentiële diensten wordt voor de vestiging in een lidstaat de effectieve en daadwerkelijke uitoefening van activiteiten via vaste regelingen verlangd. De rechtsvorm van zulke regelingen, of het nu om een bijkantoor of om een dochteronderneming met rechtspersoonlijkheid gaat, is daarbij niet doorslaggevend.

(22) Entiteiten die actief zijn in de in deze richtlijn bedoelde sectoren en deelsectoren kunnen zowel essentiële als niet-essentiële diensten verlenen. In de luchtvaartsector, bijvoorbeeld, kunnen luchthavens diensten verlenen die door een lidstaat als essentieel beschouwd zouden kunnen worden, zoals het beheer van de start- en landingsbanen. Daarnaast kunnen luchthavens ook een aantal diensten verlenen die als niet-essentieel beschouwd zouden kunnen worden, zoals de inrichting van winkelcentra. Aanbieders van essentiële diensten dienen enkel met betrekking tot deze als essentieel beschouwde diensten aan de specifieke beveiligingsvereisten onderworpen te worden. Voor de identificatie van aanbieders moeten de lidstaten derhalve een lijst van als essentieel beschouwde diensten opstellen.

(23) Alle op het grondgebied van de lidstaat verleende diensten die aan de voorschriften van deze richtlijn voldoen, moeten in de dienstenlijst worden opgenomen. De lidstaten moeten de bestaande lijst kunnen aanvullen met nieuwe diensten. De dienstenlijst moet dienen als referentiepunt voor de lidstaten om aanbieders van essentiële diensten te identificeren. Zij heeft tot doel de soorten essentiële diensten in een bepaalde in deze richtlijn bedoelde sector te identificeren en deze zodoende te onderscheiden van niet-essentiële activiteiten waarvoor een in een bepaalde sector werkzame entiteit verantwoordelijk kan zijn. De door de lidstaten opgestelde dienstenlijsten zouden dienen als bijkomende inbreng bij de beoordeling van de regelgevingspraktijken van de lidstaten met het oog op het waarborgen van de algehele samenhang van het identificatieproces tussen de lidstaten.

(24) Indien een entiteit een essentiële dienst in twee of meer lidstaten verleent, moeten deze lidstaten bilaterale of multilaterale besprekingen met elkaar voeren. Dit overlegproces heeft tot doel de lidstaten bij te staan bij het beoordelen van het kritieke karakter van de aanbieder wat betreft de grensoverschrijdende gevolgen, en biedt elke betrokken lidstaat de mogelijkheid zijn standpunt bekend te maken betreffende de risico's die aan de door aanbieder verleende diensten verbonden zijn. In het kader van dit proces moeten de betrokken lidstaten rekening houden met elkaars standpunten. De betrokken lidstaten kunnen in dit verband om de bijstand van de samenwerkingsgroep verzoeken.

(25) Ingevolge het identificatieproces moeten de lidstaten nationale maatregelen vaststellen waarin bepaald wordt welke entiteiten onderworpen zijn aan verplichtingen in verband met beveiliging van netwerk- en informatiesystemen. Dit kan door het vaststellen van een lijst van alle aanbieders van essentiële diensten of door het vaststellen van nationale maatregelen, met inbegrip van objectieve kwantificeerbare criteria (zoals de output van de aanbieder of het aantal gebruikers) op basis waarvan bepaald kan worden welke entiteiten onderworpen zijn aan verplichtingen in verband met beveiliging van netwerk- en informatiesystemen en welke niet. De nationale maatregelen, zowel de reeds bestaande als de in het kader van deze richtlijn aangenomen maatregelen, moeten de wettelijke, administratieve en beleidsmaatregelen omvatten die de identificatie van aanbieders van essentiële diensten uit hoofde van deze richtlijn mogelijk maken.

(26) Om een indicatie te geven van het belang van de geïdentificeerde aanbieders van essentiële diensten voor de betrokken sector moeten de lidstaten rekening houden met het aantal en de omvang van deze aanbieders, bijvoorbeeld wat betreft marktaandeel of geproduceerde of aanwezige hoeveelheid, zonder dat zij verplicht zijn informatie vrij te geven waaruit zou blijken welke aanbieders geïdentificeerd zijn.

(27) Om te bepalen of een incident een aanzienlijk verstorend effect op een essentiële dienst heeft, moeten de lidstaten rekening houden met een aantal verschillende factoren, zoals het aantal gebruikers dat afhankelijk is van die dienst. Het gebruik van die dienst kan direct, indirect of door bemiddeling geschieden. Bij de beoordeling van de mogelijke gevolgen, wat betreft omvang en duur, van een incident op economische en maatschappelijke activiteiten of op de openbare veiligheid moeten de lidstaten ook inschatten hoe lang het zal duren voordat de discontinuïteit een negatief effect begint te sorteren.

(28) Om te bepalen of een incident een aanzienlijk verstorend effect op de verlening van een dienst zou hebben, dienen niet alleen sectoroverschrijdende maar ook sectorspecifieke factoren in aanmerking genomen te worden. Voor energieleveranciers omvatten zulke factoren mogelijk het volume of het aandeel in de hoeveelheid nationaal geproduceerde energie; voor olieleveranciers het dagelijkse volume; voor het luchtvervoer (inclusief luchthavens en luchtvaartmaatschappijen), het spoorvervoer en de zeehavens het aandeel in het nationaal verkeersvolume en het jaarlijks aantal reizigers of vrachtactiviteiten; voor bancaire- of financiëlemarktinfrastructuren hun systemisch belang op basis van de totale activa of de verhouding tussen de totale activa en het bbp; voor de gezondheidssector het jaarlijks aantal patiënten die door een aanbieder worden behandeld; voor de waterproductie, -zuivering en -voorziening het volume en het aantal en type gebruikers (zoals ziekenhuizen, openbare diensten, organisaties of individuen) en het bestaan van alternatieve waterbronnen om hetzelfde geografische gebied van water te voorzien.

(29) Om een hoog niveau van beveiliging van netwerk- en informatiesystemen te bereiken en te handhaven, moet elke lidstaat beschikken over een nationale strategie voor de beveiliging van netwerk- en informatiesystemen waarin de te verwezenlijken strategische doelstellingen en concrete beleidsmaatregelen zijn vastgesteld.

(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.

(31) Ter bevordering van de grensoverschrijdende samenwerking en communicatie, en om de richtlijn doeltreffend te kunnen uitvoeren, is het echter nodig dat iedere lidstaat, ongeacht de sectorale regelingen, een centraal contactpunt aanwijst dat verantwoordelijk is voor de coördinatie van zaken die verband houden met de beveiliging van netwerk- en informatiesystemen en voor de grensoverschrijdende samenwerking op Unieniveau. Bevoegde autoriteiten en centrale contactpunten moeten de nodige technische, financiële en personele middelen krijgen om de hun toegewezen taken op doeltreffende en efficiënte wijze te kunnen verrichten en aldus de doelstellingen van deze richtlijn te verwezenlijken. Aangezien met deze richtlijn wordt beoogd de werking van de interne markt te verbeteren door het scheppen van vertrouwen, moeten de instanties van de lidstaten in staat zijn doeltreffend samen te werken met economische actoren en dienovereenkomstig worden gestructureerd.

(32) Incidenten moeten worden gemeld bij de bevoegde autoriteiten of de computer security incident response teams (CSIRT's). De centrale contactpunten dienen niet rechtstreeks alle meldingen van incidenten te ontvangen, tenzij zij ook optreden als bevoegde autoriteit of CSIRT. Een bevoegde autoriteit of een CSIRT moet het centraal contactpunt echter kunnen opdragen incidenten door te melden aan de centrale contactpunten van andere betrokken lidstaten.

(33) Om ervoor te zorgen dat de lidstaten en de Commissie doeltreffend worden geïnformeerd, moet een samenvattend verslag door het centraal contactpunt bij de samenwerkingsgroep worden ingediend, en worden geanonimiseerd met het oog op de bescherming van de vertrouwelijkheid van de meldingen en de identiteit van de aanbieders van essentiële diensten en digitaledienstverleners. Informatie over de identiteit van de meldende entiteiten is immers niet vereist voor de uitwisseling van goede praktijken in de samenwerkingsgroep. Het samenvattend verslag moet informatie bevatten over het aantal ontvangen meldingen, en een indicatie betreffende de aard van de gemelde incidenten, zoals de soorten inbreuken in verband met beveiliging, de ernst of de duur ervan.

(34) De lidstaten moeten zowel technisch als organisatorisch voldoende zijn toegerust voor het voorkomen en opsporen van, het reageren op en verlichten van incidenten en risico's met betrekking tot netwerk- en informatiesystemen. De lidstaten moeten er daarom voor zorgen dat zij over goed functionerende, aan essentiële eisen beantwoordende CSIRT's, ook bekend als computer emergency response teams (CERT's), beschikken die voor doeltreffende en compatibele capaciteiten voor de aanpak van incidenten en risico's moeten zorgen en doeltreffende samenwerking op Unieniveau moeten waarborgen. Opdat deze capaciteiten en deze samenwerking ten goede zouden komen aan alle soorten aanbieders van essentiële diensten en digitaledienstverleners, moeten de lidstaten ervoor zorgen dat alle soorten onder een aangewezen CSIRT vallen. Gezien het belang van internationale samenwerking op het gebied van cyberbeveiliging, moeten CSIRT's kunnen deelnemen aan internationale samenwerkingsnetwerken naast het bij deze richtlijn ingestelde CSIRT-netwerk.

(35) Aangezien de meeste netwerk- en informatiesystemen privaat worden geëxploiteerd, is samenwerking tussen de publieke en de private sector essentieel. Aanbieders van essentiële diensten en digitaledienstverleners moeten worden aangemoedigd om hun eigen informele samenwerkingsmechanismen na te streven om de beveiliging van netwerk- en informatiesystemen te waarborgen. De samenwerkingsgroep moet in voorkomend geval belanghebbenden kunnen uitnodigen om aan de beraadslagingen deel te nemen. Om de uitwisseling van informatie en beste praktijken effectief te stimuleren is het essentieel ervoor te zorgen dat aanbieders van essentiële diensten en digitaledienstverleners die deelnemen aan een dergelijke uitwisseling, geen nadelen ondervinden van hun samenwerking.

(36) Het Enisa moet de lidstaten en de Commissie met deskundigheid en advies bijstaan en de uitwisseling van beste praktijken faciliteren. Met name bij de toepassing van deze richtlijn moet de Commissie het Enisa raadplegen, en moeten de lidstaten hiertoe de mogelijkheid hebben. Om capaciteit en kennis bij de lidstaten op te bouwen, moet de samenwerkingsgroep ook fungeren als instrument voor de uitwisseling van beste praktijken, besprekingen over capaciteiten en paraatheid van de lidstaten en, op vrijwillige basis, om haar leden bijstand te verlenen bij de evaluatie van nationale strategieën voor de beveiliging van netwerk- en informatiesystemen, bij capaciteitsopbouw en bij de evaluatie van oefeningen in verband met de evaluatie van de beveiliging van netwerk- en informatiesystemen.

(37) De lidstaten moeten bij de toepassing van deze richtlijn, waar van toepassing, bestaande organisatiestructuren of strategieën kunnen gebruiken of aanpassen.

(38) De respectieve taken van de samenwerkingsgroep en het Enisa zijn onderling afhankelijk en complementair. In het algemeen moet het Enisa de samenwerkingsgroep bijstaan bij de uitvoering van haar taken, overeenkomstig de doelstelling van het Enisa die is vastgesteld in Verordening (EU) nr. 526/2013 van het Europees Parlement en de Raad ([1]), namelijk „bijstand verlenen aan de instellingen, organen en instanties van de Unie en de lidstaten bij de tenuitvoerlegging van het beleid dat nodig is voor de naleving van wettelijke of regelgevende eisen aangaande beveiliging van netwerk- en informatiesystemen uit hoofde van de bestaande en toekomstige rechtshandelingen van de Unie". In het bijzonder dient het Enisa bijstand te verlenen op de gebieden die overeenstemmen met zijn eigen taken, als bepaald in Verordening (EU) nr. 526/2013, te weten de analyse van strategieën voor beveiliging van netwerk- en informatiesystemen, het verlenen van ondersteuning voor het organiseren en uitvoeren van uniale oefeningen in verband met de beveiliging van netwerk- en informatiesystemen en de uitwisseling van informatie en beste praktijken op het gebied van bewustmaking en opleiding. Het Enisa moet ook worden betrokken bij het opstellen van richtsnoeren voor sectorspecifieke criteria voor het bepalen van de aanzienlijkheid van de gevolgen van een incident.

([1]) Verordening (EU) nr. 526/2013 van het Europees Parlement en de Raad van 21 mei 2013 inzake het Agentschap van de Europese Unie voor netwerk- en informatiebeveiliging (Enisa) en tot intrekking van Verordening (EG) nr. 460/2004 (PB L 165 van 18.6.2013, blz. 41).

(39) Met het oog op de bevordering van geavanceerde netwerk- en informatiebeveiligingssystemen moet de samenwerkingsgroep, waar nodig, samenwerken met de bevoegde instellingen, organen en instanties van de Unie, om kennis en beste praktijken uit te wisselen en advies te verlenen over de veiligheidsaspecten van netwerk- en informatiebeveiligingssystemen die een effect kunnen hebben op hun werkzaamheden, met inachtneming van bestaande regelingen voor de uitwisseling van niet-openbare informatie. Bij de samenwerking met rechtshandhavingsautoriteiten inzake de beveiligingsaspecten van netwerk- en informatiesystemen die van invloed kunnen zijn op hun werkzaamheden, moet de samenwerkingsgroep bestaande informatiekanalen en gevestigde netwerken respecteren.

(40) Informatie over incidenten wordt steeds waardevoller voor het grote publiek en bedrijfsleven, met name het midden- en kleinbedrijf. In sommige gevallen is deze informatie al verstrekt via websites op nationaal niveau, in de taal van het betreffende land en voornamelijk gericht op incidenten en voorvallen met een nationale dimensie. Aangezien bedrijven in toenemende mate grensoverschrijdend actief zijn en burgers gebruik maken van onlinediensten, moet informatie over incidenten in pakketvorm op Unieniveau worden verstrekt. Het secretariaat van het CSIRT-netwerk wordt aangemoedigd een website te hebben of een specifieke pagina op een bestaande website te hosten waar algemene informatie met betrekking tot belangrijke incidenten die in de hele Unie plaatsvonden, ter beschikking wordt gesteld van het grote publiek, met speciale aandacht voor de belangen en de behoeften van het bedrijfsleven. CSIRT's die deelnemen aan het CSIRT-netwerk, worden aangespoord om op vrijwillige basis de informatie te verstrekken die op deze website moet worden gepubliceerd, maar geen vertrouwelijke of gevoelige informatie.

(41) Wanneer informatie volgens uniale en nationale voorschriften inzake de vertrouwelijkheid van bedrijfsinformatie als vertrouwelijk wordt beschouwd, moet die vertrouwelijkheid worden gewaarborgd tijdens de activiteiten die noodzakelijk zijn ter verwezenlijking van de doelstellingen van deze richtlijn.

(42) Oefeningen inzake cyberbeveiliging, waarbij incidentenscenario's in realtime worden gesimuleerd, zijn van essentieel belang voor het testen van de paraatheid en de samenwerking van de lidstaten op het gebied van de beveiliging van netwerk- en informatiesystemen. De door het Enisa gecoördineerde CyberEurope-cyclus van oefeningen, waaraan de lidstaten deelnemen, is een nuttig instrument voor het testen en het formuleren van aanbevelingen om de incidentenrespons op Unieniveau mettertijd te verbeteren. Overwegende dat de lidstaten momenteel niet verplicht zijn oefeningen te plannen of eraan deel te nemen, moet de oprichting van het CSIRT-netwerk op grond van deze richtlijn de lidstaten in staat stellen deel te nemen aan oefeningen op basis van een nauwkeurige planning en strategische keuzes. De krachtens deze richtlijn ingestelde samenwerkingsgroep moet de strategische beslissingen inzake oefeningen nemen, met name maar niet uitsluitend wat betreft de regelmatigheid van de oefeningen en het ontwerp van de scenario's. Het Enisa moet, overeenkomstig zijn taakopdracht, de organisatie en uitvoering van oefeningen in de hele Unie ondersteunen door expertise en advies te verlenen aan de samenwerkingsgroep en het CSIRT-netwerk.

(43) Gezien het mondiale karakter van veiligheidsproblemen in verband met netwerk- en informatiebeveiligingssystemen is er behoefte aan nauwere internationale samenwerking om beveiligingsnormen en informatieuitwisseling te verbeteren en een gemeenschappelijke internationale aanpak van veiligheidskwesties te bevorderen.

(44) De verantwoordelijkheid voor het waarborgen van de veiligheid van netwerk- en informatiesystemen ligt voor een groot deel bij aanbieders van essentiële diensten en digitaledienstverleners. Aan de hand van passende regelgevingseisen en vrijwillige sectorconvenanten moet een cultuur van risicobeheer worden bevorderd en ontwikkeld, die risicobeoordeling en de uitvoering van risicogerichte beveiligingsmaatregelen behelst. Ook de totstandbrenging van een betrouwbaar gelijk speelveld is essentieel om te waarborgen dat alle lidstaten doeltreffend samenwerken in de samenwerkingsgroep en het CSIRT-netwerk.

(45) Deze richtlijn is alleen van toepassing op overheidsdiensten die aangemerkt worden als aanbieders van essentiële diensten. Het is bijgevolg de verantwoordelijkheid van de lidstaten om te zorgen voor de beveiliging van netwerken informatiesystemen van overheidsdiensten die niet binnen de werkingssfeer van deze richtlijn vallen.

(46) Maatregelen voor risicobeheer omvatten maatregelen om incidentrisico's in beeld te brengen, incidenten te voorkomen, op te sporen en aan te pakken en de gevolgen ervan te beperken; de beveiliging van netwerk- en informatiesystemen behelst de beveiliging van opgeslagen, doorgegeven en verwerkte gegevens.

(47) De bevoegde autoriteiten moeten nationale richtsnoeren kunnen blijven vaststellen met betrekking tot de omstandigheden waarin aanbieders van essentiële diensten incidenten moeten melden.

(48) Veel bedrijven in de Unie vertrouwen voor de verlening van hun eigen diensten op de digitaledienstverleners zoals gedefinieerd in deze richtlijn. Aangezien sommige digitale diensten een belangrijk hulpmiddel kunnen zijn voor hun gebruikers, met inbegrip van aanbieders van essentiële diensten, en aangezien deze gebruikers niet altijd over alternatieven beschikken, moet deze richtlijn ook van toepassing zijn op de verleners van dergelijke diensten. De beveiliging, continuïteit en betrouwbaarheid van het soort digitale diensten bedoeld in deze richtlijn zijn van essentieel belang voor de vlotte werking van tal van bedrijven. Een verstoring van een dergelijke digitale dienst kan verhinderen dat andere diensten worden verleend die daarvan afhankelijk zijn, en kan dus gevolgen hebben voor belangrijke economische en maatschappelijke activiteiten in de Unie. Dergelijke digitale diensten kunnen derhalve van cruciaal belang zijn voor de goede werking van ondernemingen die daarvan afhankelijk zijn, en tevens voor de deelname van deze ondernemingen aan de interne markt en de grensoverschrijdende handel in de hele Unie. Digitaledienstverleners als bedoeld in deze richtlijn zijn die welke geacht worden digitale diensten aan te bieden waarop steeds meer bedrijven in de Unie vertrouwen.

(49) Digitaledienstverleners moeten zorgen voor een niveau van beveiliging dat in verhouding staat tot de risicograad voor de beveiliging van de digitale diensten die ze verlenen, gezien het belang van hun diensten voor de activiteiten van andere ondernemingen binnen de Unie. In de praktijk zal de risicograad voor aanbieders van essentiële diensten, die vaak van essentieel belang zijn voor het behoud van kritieke maatschappelijke en economische activiteiten, hoger zijn dan voor digitaledienstverleners. Daarom moeten de beveiligingseisen voor digitaledienstverleners lichter zijn. Digitaledienstverleners moeten de vrijheid behouden om maatregelen te treffen die zij passend achten ter beheersing van de risico's voor de beveiliging van hun netwerk- en informatiesystemen. Vanwege hun grensoverschrijdende aard moet voor digitaledienstverleners een meer geharmoniseerde aanpak op Unieniveau worden gehanteerd. Uitvoeringshandelingen moeten de invulling en tenuitvoerlegging van deze maatregelen vergemakkelijken.

(50) Hoewel hardwareproducenten en softwareontwikkelaars geen aanbieders van essentiële diensten of digitaledienstverleners zijn, bevorderen hun producten de beveiliging van netwerk- en informatiesystemen. Zij hebben derhalve een belangrijke rol omdat zij de aanbieders van essentiële diensten en digitaledienstverleners in staat stellen hun netwerk- en informatiesystemen te beveiligen. Voor dergelijke hardware en software gelden reeds bestaande regels betreffende productaansprakelijkheid.

(51) In de technische en organisatorische maatregelen die aan aanbieders van essentiële diensten en digitaledienstverleners worden opgelegd, mag niet de eis worden gesteld dat een bepaald commercieel informatie- en communicatietechnologieproduct op een bepaalde wijze wordt ontworpen, ontwikkeld of vervaardigd.

(52) Aanbieders van essentiële diensten en digitaledienstverleners moeten zorgen voor de beveiliging van de netwerk- en informatiesystemen die zij gebruiken. Het gaat daarbij voornamelijk om private netwerk- en informatiesystemen die door hun intern IT-personeel worden beheerd of waarvan de beveiliging is uitbesteed. De beveiligings- en meldingsvereisten moeten van toepassing zijn op de betrokken aanbieders van essentiële diensten en digitaledienstverleners, ongeacht of zij het onderhoud van hun netwerk- en informatiesystemen zelf verrichten dan wel uitbesteden.

(53) Om te voorkomen dat aan aanbieders van essentiële diensten en digitaledienstverleners onevenredige financiële en administratieve lasten worden opgelegd, moeten de eisen, rekening houdend met de stand van de techniek, in verhouding staan tot het risico dat verbonden is aan het netwerk- en informatiesysteem in kwestie. In het geval van digitaledienstverleners mogen deze eisen niet van toepassing zijn op micro-ondernemingen en kleine ondernemingen.

(54) Wanneer overheidsdiensten in de lidstaten gebruik maken van diensten die worden aangeboden door digitaledienstverleners, met name cloudcomputerdiensten, is het mogelijk dat zij van de verleners van die diensten extra beveiligingsmaatregelen verlangen naast datgene wat de digitaledienstverleners normaliter zouden aanbieden conform de eisen van deze richtlijn. Dit moeten zij kunnen doen door middel van contractuele verplichtingen.

(55) De definities van onlinemarktplaatsen, onlinezoekmachines en cloudcomputerdiensten in deze richtlijn gelden voor de specifieke toepassing van deze richtlijn, onverminderd andere instrumenten.

(56) Deze richtlijn mag de lidstaten niet beletten nationale maatregelen te nemen op grond waarvan openbare lichamen verplicht worden specifieke beveiligingseisen te stellen wanneer zij contracten sluiten voor cloudcomputerdiensten. Dergelijke nationale maatregelen moeten gelden voor het betrokken openbare lichaam en niet voor de aanbieder van cloudcomputerdiensten.

(57) Gezien de fundamentele verschillen tussen aanbieders van essentiële diensten, met name wat betreft hun rechtstreekse band met de fysieke infrastructuur, en digitaledienstverleners, met name hun grensoverschrijdende karakter, moet deze richtlijn ten aanzien van deze twee categorieën entiteiten een gedifferentieerde aanpak volgen met betrekking tot de mate van harmonisatie. Voor aanbieders van essentiële diensten moeten de lidstaten kunnen achterhalen wie de betreffende aanbieders zijn en strengere eisen kunnen opleggen dan die welke in deze richtlijn zijn vastgelegd. De lidstaten hoeven niet te achterhalen wie digitaledienstverleners zijn, aangezien deze richtlijn van toepassing moet zijn op alle digitaledienstverleners die binnen de werkingssfeer ervan vallen. Bovendien moeten deze richtlijn en de op grond daarvan vastgestelde uitvoeringshandelingen zorgen voor een hoge mate van harmonisatie van de beveiligings- en meldingseisen voor digitaledienstverleners. Deze elementen moeten een uniforme aanpak van digitaledienstverleners in de gehele Unie mogelijk maken, die in verhouding staat tot de aard en de graad van het risico dat zij kunnen lopen.

(58) Deze richtlijn mag de lidstaten niet verhinderen beveiligings- en meldingseisen op te leggen aan entiteiten die geen digitaledienstverleners in de zin van deze richtlijn zijn, onverminderd de verplichtingen van de lidstaten uit hoofde van het Unierecht.

(59) De bevoegde autoriteiten moeten de nodige aandacht besteden aan de instandhouding van informele en betrouwbare kanalen voor informatie-uitwisseling. Bij de bekendmaking van aan de bevoegde autoriteiten gemelde incidenten moet het belang van het publiek om te worden geïnformeerd over bedreigingen worden afgewogen tegen mogelijke commerciële en imagoschade voor de aanbieders van essentiële diensten en digitaledienstverleners die incidenten melden. Bij het nakomen van de meldingsverplichtingen moeten de bevoegde autoriteiten en de CSIRT's bijzondere aandacht besteden aan de noodzaak om informatie over de kwetsbare punten van producten strikt vertrouwelijk te houden tot er passende herstel- en beveiligingsmaatregelen zijn genomen.

(60) Digitaledienstverleners moeten worden onderworpen aan licht en reactief toezicht achteraf dat te rechtvaardigen is door de aard van hun diensten en activiteiten. De betrokken bevoegde autoriteit moet daarom alleen maatregelen nemen als zij over bewijzen beschikt (bijvoorbeeld verstrekt door de digitaledienstverlener zelf, door een andere bevoegde autoriteit, met inbegrip van een bevoegde autoriteit van een andere lidstaat, of door een gebruiker van de dienst) dat een digitaledienstverlener niet voldoet aan de eisen van deze richtlijn, met name nadat een incident zich heeft voorgedaan. Voor de bevoegde autoriteit moet er daarom geen algemene verplichting zijn om toezicht te houden op digitaledienstverleners.

(61) De bevoegde autoriteiten moeten over de nodige middelen beschikken om hun taken uit te voeren, met inbegrip van bevoegdheden om voldoende informatie te kunnen verzamelen om na te gaan in hoeverre netwerk- en informatiesystemen beveiligd zijn.

(62) Incidenten kunnen het resultaat zijn van criminele activiteiten, waarvan de voorkoming, het onderzoek en de vervolging wordt ondersteund door coördinatie en samenwerking tussen aanbieders van essentiële diensten, digitaledienstverleners, bevoegde autoriteiten en rechtshandhavingsinstanties. Indien vermoed wordt dat een incident gerelateerd is aan ernstige criminele activiteiten volgens het Unierecht of het nationale recht, dienen de lidstaten aanbieders van essentiële diensten en digitaledienstverleners ertoe aan te sporen incidenten van vermoedelijk ernstig criminele aard zelf te melden aan de bevoegde rechtshandhavingsinstanties. In voorkomend geval is het wenselijk dat de coördinatie tussen bevoegde autoriteiten en de rechtshandhavingsinstanties van verschillende lidstaten wordt bevorderd door het Centrum voor de bestrijding van cybercriminaliteit van het Europees Centrum voor de bestrijding van cybercriminaliteit (EC3) en het Enisa.

(63) In veel gevallen worden persoonsgegevens aangetast als gevolg van incidenten. Daarom moeten de bevoegde autoriteiten en de autoriteiten voor gegevensbescherming samenwerken en informatie over alle relevante zaken uitwisselen om inbreuken in verband met persoonsgegevens als gevolg van incidenten aan te pakken.

(64) De jurisdictie ten aanzien van digitaledienstverleners mag aan slechts één lidstaat worden verleend, te weten die waar de betrokken digitaledienstverlener zijn hoofdvestiging heeft in de Unie; in beginsel is dat de plaats waar de dienstverlener zijn hoofdkantoor heeft in de Unie. Vestiging veronderstelt het effectief en daadwerkelijk uitoefenen van activiteiten via vaste regelingen. De rechtsvorm van dergelijke regelingen, of het nu gaat om een bijkantoor of om een dochteronderneming met rechtspersoonlijkheid, is daarbij niet doorslaggevend. Dit criterium mag niet

zitten in het feit of de netwerk- en informatiesystemen fysiek zijn ondergebracht op in die plaats; de aanwezigheid en het gebruik van die systemen zijn op zich onvoldoende om te kunnen spreken van hoofdvestiging en zijn dan ook geen criteria voor het bepalen van de hoofdvestiging.

(65) Wanneer een digitaledienstverlener die niet gevestigd is in de Unie diensten aanbiedt in de Unie, moet hij een vertegenwoordiger aanwijzen. Om te bepalen of een dergelijke digitaledienstverlener diensten aanbiedt in de Unie, moet worden nagegaan of hij kennelijk voornemens is diensten aan te bieden aan personen in één of meer lidstaten. Het loutere feit van toegankelijkheid van de website van de digitaledienstverlener of van een tussenpersoon in de Unie of van een e-mailadres of van andere contactgegevens of het gebruik van een taal die algemeen wordt gebruikt in het derde land waar de digitaledienstverlener is gevestigd, is op zich ontoereikend om een dergelijk voornemen vast te stellen. Uit factoren zoals het gebruik van een taal of een valuta die in één of meer lidstaten algemeen wordt gebruikt, met de mogelijkheid om in die taal diensten te bestellen, of de vermelding van klanten of gebruikers die zich in de Unie bevinden, kan evenwel blijken dat de digitaledienstverlener voornemens is diensten aan te bieden in de Unie. De vertegenwoordiger dient namens de digitaledienstverlener te handelen, en de bevoegde autoriteiten of de CSIRT's moeten contact kunnen opnemen met de vertegenwoordiger. De vertegenwoordiger dient via een schriftelijk mandaat van de digitaledienstverlener uitdrukkelijk te worden aangewezen om, in het kader van deze richtlijn, namens laatstgenoemde op te treden met betrekking tot diens verplichtingen, waaronder de melding van incidenten.

(66) De normalisatie van beveiligingseisen is een marktgestuurd proces. Met het oog op een eenvormige toepassing van de beveiligingsnormen moeten de lidstaten naleving van of afstemming op specifieke normen aanmoedigen om een hoog niveau van beveiliging van netwerk- en informatiesystemen op Unieniveau te waarborgen. Het Enisa dient de lidstaten bij te staan met advies en richtsnoeren. Daartoe kan het nuttig zijn geharmoniseerde normen op te stellen, hetgeen moet gebeuren overeenkomstig Verordening (EU) nr. 1025/2012 van het Europees Parlement en de Raad ([1]).

(67) Entiteiten die buiten het toepassingsgebied van deze richtlijn vallen, kunnen worden geconfronteerd met incidenten die aanzienlijke gevolgen hebben voor de door hen verleende diensten. Wanneer deze entiteiten van mening zijn dat het melden van deze incidenten het openbaar belang dient, moeten zij in staat zijn dat op vrijwillige basis te doen. Zulke meldingen moeten door de bevoegde autoriteit of het CSIRT worden verwerkt wanneer die verwerking geen onevenredige of overmatige belasting voor de betrokken lidstaat vormt.

(68) Om eenvormige voorwaarden te waarborgen voor de uitvoering van deze richtlijn, moeten aan de Commissie uitvoeringsbevoegdheden worden toegekend om de procedurele regelingen vast te stellen die noodzakelijk zijn voor de werking van de samenwerkingsgroep en de beveiligings- en meldingseisen die van toepassing zijn op digitaledienstverleners. Die bevoegdheden moeten worden uitgeoefend in overeenstemming met Verordening (EU) nr. 182/2011 van het Europees Parlement en de Raad ([2]). Bij de vaststelling van uitvoeringshandelingen met betrekking tot de procedurele regelingen die noodzakelijk zijn voor de werking van de samenwerkingsgroep, moet de Commissie zo veel mogelijk rekening houden met het advies van het Enisa.

(69) Bij het vaststellen van uitvoeringshandelingen inzake de beveiligingseisen voor digitaledienstverleners, moet de Commissie zo veel mogelijk rekening houden met het advies van het Enisa en zij betrokken belanghebbenden raadplegen. Bovendien wordt de Commissie aangemoedigd om rekening te houden met de volgende voorbeelden: met betrekking tot de beveiliging van systemen en voorzieningen: fysieke en omgevingsbeveiliging, bevoorradingszekerheid, controle op de toegang tot netwerk- en informatiesystemen en integriteit van netwerk- en informatiesystemen; met betrekking tot incidentbeheer: procedures voor incidentbeheer, capaciteit voor incidentdetectie, incidentrapportage en -communicatie; met betrekking tot het beheer van de bedrijfscontinuïteit: strategie inzake continuïteit van de dienstverlening en rampenplannen, uitwijkcapaciteiten; en op het gebied van toezicht, controle en testen: toezicht- en registratiebeleid, oefenen rampenplannen, testen van de netwerk- en informatiesystemen, beoordelingen van de beveiliging en toezicht op de naleving.

(70) Bij de tenuitvoerlegging van deze richtlijn moet de Commissie waar passend met de bevoegde sectorale comités en de op Unieniveau opgerichte bevoegde organen contacten onderhouden op de onder deze richtlijn vallende gebieden.

([1]) Verordening (EU) nr. 1025/2012 van het Europees Parlement en de Raad van 25 oktober 2012 betreffende Europese normalisatie, tot wijziging van de Richtlijnen 89/686/EEG en 93/15/EEG van de Raad alsmede de Richtlijnen 94/9/EG, 94/25/EG, 95/16/EG, 97/23/EG, 98/34/EG, 2004/22/EG, 2007/23/EG, 2009/23/EG en 2009/105/EG van het Europees Parlement en de Raad en tot intrekking van Beschikking 87/95/EEG van de Raad en Besluit nr. 1673/2006/EG van het Europees Parlement en de Raad (PB L 316 van 14.11.2012, blz. 12).

([2]) Verordening (EU) nr. 182/2011 van het Europees Parlement en de Raad van 16 februari 2011 tot vaststelling van de algemene voorschriften en beginselen die van toepassing zijn op de wijze waarop de lidstaten de uitoefening van de uitvoeringsbevoegdheden door de Commissie controleren (PB L 55 van 28.2.2011, blz. 13).

(71) De Commissie moet deze richtlijn in overleg met alle belanghebbenden op gezette tijden evalueren, met name om na te gaan of zij in het licht van de veranderende maatschappelijke, politieke, technologische of marktomstandigheden moet worden gewijzigd.

(72) Voor de uitwisseling van informatie over risico's en incidenten in de samenwerkingsgroep en het CSIRT-netwerk en de naleving van de voorschriften inzake het melden van incidenten aan de nationale bevoegde autoriteiten of het CSIRT, kan de verwerking van persoonsgegevens worden verlangd. Die verwerking moet gebeuren in overeenstemming met Richtlijn 95/46/EG van het Europees Parlement en de Raad ([1]) en Verordening (EG) nr. 45/2001 van het Europees Parlement en de Raad ([2]). Waar zulks passend is, moet bij de toepassing van deze richtlijn Verordening (EG) nr. 1049/2001 van het Europees Parlement en de Raad ([3]) van toepassing zijn.

(73) De Europese Toezichthouder voor gegevensbescherming is geraadpleegd overeenkomstig artikel 28, lid 2, van Verordening (EG) nr. 45/2001 en heeft op 14 juni 2013 advies uitgebracht ([4]).

(74) Daar de doelstelling van deze richtlijn, namelijk het komen tot een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie, niet voldoende door de lidstaten alleen kan worden verwezenlijkt maar vanwege de gevolgen van de maatregelen beter door de Unie kan worden verwezenlijkt, kan de Unie, overeenkomstig het in artikel 5 van het Verdrag betreffende de Europese Unie neergelegde subsidiariteitsbeginsel, maatregelen nemen. Overeenkomstig het in hetzelfde artikel neergelegde evenredigheidsbeginsel gaat deze richtlijn niet verder dan nodig is om die doelstelling te verwezenlijken.

(75) Deze richtlijn is in overeenstemming met de grondrechten en beginselen die door het Handvest van de grondrechten van de Europese Unie worden erkend, met name het recht op eerbiediging van het privéleven en communicatie, de bescherming van persoonsgegevens, de vrijheid van ondernemerschap, het recht op eigendom, het recht op een doeltreffende voorziening in rechte en het recht te worden gehoord. Deze richtlijn moet overeenkomstig deze rechten en beginselen ten uitvoer worden gelegd,

HEBBEN DE VOLGENDE RICHTLIJN VASTGESTELD:

HOOFDSTUK I

ALGEMENE BEPALINGEN

Artikel 1

Onderwerp en toepassingsgebied

1. Bij deze richtlijn worden maatregelen vastgesteld met het oog op het tot stand brengen van een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie, teneinde de werking van de interne markt te verbeteren.

2. Daartoe wordt bij deze richtlijn in het volgende voorzien:

a) de vaststelling van verplichtingen voor alle lidstaten om een nationale strategie voor beveiliging van netwerk- en informatiesystemen vast te stellen;

b) de instelling van een samenwerkingsgroep die de strategische samenwerking en informatie-uitwisseling tussen de lidstaten moet ondersteunen en onderling vertrouwen moet scheppen;

c) de totstandbrenging van een netwerk van computer security incident response teams („CSIRT's-netwerk") dat mede vertrouwen moet scheppen tussen de lidstaten en snelle en doeltreffende operationele samenwerking moet bevorderen;

([1]) Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (PB L 281 van 23.11.1995, blz. 31).

([2]) Verordening (EG) nr. 45/2001 van het Europees Parlement en de Raad van 18 december 2000 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de communautaire instellingen en organen en betreffende het vrije verkeer van die gegevens (PB L 8 van 12.1.2001, blz. 1).

([3]) Verordening (EG) nr. 1049/2001 van het Europees Parlement en de Raad van 30 mei 2001 inzake de toegang van het publiek tot documenten van het Europees Parlement, de Raad en de Commissie (PB L 145 van 31.5.2001, blz. 43).

([4]) PB C 32 van 4.2.2014, blz. 19.

d) de vaststelling van beveiligings- en meldingseisen voor aanbieders van essentiële diensten en voor digitaledienstverleners;

e) de vaststelling van verplichtingen voor de lidstaten om nationale bevoegde autoriteiten, centrale contactpunten en CSIRT's aan te wijzen, met taken in verband met de beveiliging van netwerk- en informatiesystemen.

3. De beveiligings- en meldingseisen bedoeld in deze richtlijn zijn niet van toepassing op ondernemingen die zijn onderworpen aan de eisen van de artikelen 13 bis en 13 ter van Richtlijn 2002/21/EG, noch op verleners van vertrouwensdiensten die zijn onderworpen aan de eisen van artikel 19 van Verordening (EU) nr. 910/2014.

4. Deze richtlijn laat Richtlijn 2008/114/EG van de Raad ([1]) en de Richtlijnen 2011/93/EU ([2]) en 2013/40/EU ([3]) van het Europees Parlement en de Raad onverlet.

5. Onverminderd artikel 346 VWEU wordt informatie die als vertrouwelijk wordt beschouwd krachtens uniale en nationale voorschriften, zoals voorschriften inzake de vertrouwelijkheid van bedrijfsinformatie, uitsluitend met de Commissie en andere betrokken autoriteiten uitgewisseld wanneer die uitwisseling noodzakelijk is voor de toepassing van deze richtlijn. De uitgewisselde informatie wordt beperkt tot hetgeen relevant is voor en evenredig is met het doel van die uitwisseling. Bij die uitwisseling van informatie wordt de vertrouwelijkheid van de informatie gewaarborgd en de bescherming van de veiligheids- en commerciële belangen van aanbieders van essentiële diensten en digitaledienstverleners beschermd.

6. Deze richtlijn laat onverlet de maatregelen van de lidstaten ter bescherming van hun essentiële staatsfuncties, in het bijzonder ter bescherming van de nationale veiligheid (met inbegrip van maatregelen ter bescherming van informatie waarvan de lidstaten de verbreiding strijdig achten met de wezenlijke belangen van hun veiligheid), en ter handhaving van de openbare orde, met name om het onderzoek, de opsporing en de vervolging van strafbare feiten mogelijk te maken.

7. Wanneer een sectorspecifieke rechtshandeling van de Unie vereist dat aanbieders van essentiële diensten of digitaledienstverleners zorgen voor de beveiliging van hun netwerk- en informatiesystemen of de melding van incidenten, op voorwaarde dat die eisen ten minste feitelijk gelijkwaardig zijn aan de verplichtingen van deze richtlijn, zijn de bepalingen van die sectorspecifieke rechtshandeling van de Unie van toepassing.

Artikel 2

Bescherming en verwerking van persoonsgegevens

1. De verwerking van persoonsgegevens krachtens deze richtlijn gebeurt overeenkomstig Richtlijn 95/46/EG.

2. De verwerking van persoonsgegevens door instellingen en organen van de Unie krachtens deze richtlijn gebeurt overeenkomstig Verordening (EG) nr. 45/2001.

Artikel 3

Minimumharmonisatie

Onverminderd artikel 16, lid 10, en de krachtens het recht van de Unie op hen rustende verplichtingen, kunnen de lidstaten bepalingen vaststellen of handhaven met het oog op het tot stand brengen van een hoger niveau van beveiliging van netwerk- en informatiesystemen.

([1]) Richtlijn 2008/114/EG van de Raad van 8 december 2008 inzake de identificatie van Europese kritieke infrastructuren, de aanmerking van infrastructuren als Europese kritieke infrastructuren en de beoordeling van de noodzaak de bescherming van dergelijke infrastructuren te verbeteren (PB L 345 van 23.12.2008, blz. 75).

([2]) Richtlijn 2011/93/EU van het Europees Parlement en de Raad van 13 december 2011 ter bestrijding van seksueel misbruik en seksuele uitbuiting van kinderen en kinderpornografie, en ter vervanging van Kaderbesluit 2004/68/JBZ van de Raad (PB L 335 van 17.12.2011, blz. 1).

([3]) Richtlijn 2013/40/EU van het Europees Parlement en de Raad van 12 augustus 2013 over aanvallen op informatiesystemen en ter vervanging van Kaderbesluit 2005/222/JBZ van de Raad (PB L 218 van 14.8.2013, blz. 8).

Artikel 4

Definities

Voor de toepassing van deze richtlijn wordt verstaan onder:

1) „netwerk- en informatiesysteem”:

   a) een elektronisch communicatienetwerk in de zin van artikel 2, onder a), van Richtlijn 2002/21/EG;

   b) een apparaat of groep van geïnterconnecteerde of bij elkaar behorende apparaten, waarvan een of meer, overeenkomstig een programma, digitale gegevens automatisch verwerkt of verwerken, of

   c) digitale gegevens die via in de punten a) en b) bedoelde elementen worden opgeslagen, verwerkt, opgehaald of verzonden met het oog op de werking, het gebruik, de beveiliging en het onderhoud ervan;

2) „beveiliging van netwerk- en informatiesystemen”: 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;

3) „nationale strategie voor de beveiliging van netwerk- en informatiesystemen”: een kader met strategische doelstellingen en prioriteiten op het gebied van de beveiliging van netwerk- en informatiesystemen op nationaal niveau;

4) „aanbieder van essentiële diensten”: een publieke of private entiteit waarvan de soort is vermeld in bijlage II en die voldoet aan de criteria van artikel 5, lid 2;

5) „digitale dienst”: een dienst in de zin van artikel 1, lid 1, onder b), van Richtlijn (EU) 2015/1535 van het Europees Parlement en de Raad ([1]), waarvan de soort is vermeld in bijlage III;

6) „digitaledienstverlener”: elke rechtspersoon die een digitale dienst aanbiedt;

7) „incident”: elke gebeurtenis met een daadwerkelijk schadelijk effect op de beveiliging van netwerk- en informatiesystemen;

8) „incidentenbehandeling”: alle procedures ter ondersteuning van de opsporing, analyse en beheersing van en reactie op een incident;

9) „risico”: elke redelijkerwijs vast te stellen omstandigheid of gebeurtenis met een mogelijk schadelijk effect op de beveiliging van netwerk- en informatiesystemen;

10) „vertegenwoordiger”: elke in de Unie gevestigde natuurlijke of rechtspersoon die uitdrukkelijk is aangewezen om voor rekening van een niet in de Unie gevestigde digitaledienstverlener te handelen, waartoe een nationale bevoegde autoriteit of een CSIRT zich kan wenden in plaats van tot de digitaledienstverlener, wat de verplichtingen van de digitaledienstverlener uit hoofde van deze richtlijn betreft;

11) „norm”: een norm in de zin van artikel 2, punt 1, van Verordening (EU) nr. 1025/2012;

12) „specificatie”: een technische specificatie in de zin van artikel 2, punt 4, van Verordening (EU) nr. 1025/2012;

13) „internetknooppunt”: een netwerkinfrastructuur die de onderlinge verbinding van meer dan twee onafhankelijke autonome systemen mogelijk maakt, voornamelijk met als doel de uitwisseling van internetverkeer te vergemakkelijken; een internetknooppunt zorgt voor onderlinge verbinding enkel voor autonome systemen; een internetknooppunt vereist niet dat het internetverkeer tussen twee deelnemende autonome systemen via een derde autonoom systeem verloopt noch dat het internetknooppunt dergelijk verkeer wijzigt of anderszins daartussen komt;

14) „domeinnaamsysteem” of „DNS”: een hiërarchisch opgebouwd adresseringssysteem in een netwerk dat een zoekvraag naar een domeinnaam beantwoordt;

([1]) Richtlijn (EU) 2015/1535 van het Europees Parlement en de Raad van 9 september 2015 betreffende een informatieprocedure op het gebied van technische voorschriften en regels betreffende de diensten van de informatiemaatschappij (PB L 241 van 17.9.2015, blz. 1).

15) „DNS-dienstverlener": een entiteit die DNS-diensten op het internet verleent;

16) „register voor topleveldomeinnamen": een entiteit die de internetdomeinnamen van een specifiek topleveldomein registreert en beheert;

17) „onlinemarktplaats": een digitale dienst die het consumenten en/of ondernemers, zoals gedefinieerd in artikel 4, lid 1, onder a) respectievelijk onder b), van Richtlijn 2013/11/EU van het Europees Parlement en de Raad ([1]), mogelijk maakt online verkoop- of dienstenovereenkomsten met ondernemers te sluiten op de website van de onlinemarktplaats of op de website van een ondernemer die gebruikmaakt van door de onlinemarktplaats aangeboden informaticadiensten;

18) „onlinezoekmachine": een digitale dienst die het gebruikers mogelijk maakt zoekacties uit te voeren op in beginsel alle websites of websites in een bepaalde taal op basis van een zoekvraag over om het even welk onderwerp in de vorm van een trefwoord, frase of andere input; het resultaat zijn hyperlinks naar informatie over de opgevraagde inhoud;

19) „cloudcomputerdienst": een digitale dienst die toegang mogelijk maakt tot een schaalbare en elastische pool van deelbare computercapaciteit.

Artikel 5

Identificatie van aanbieders van essentiële diensten

1. Uiterlijk op 9 november 2018 wijzen de lidstaten voor elke in bijlage II genoemde sector en deelsector de aanbieders van essentiële diensten met een vestiging op hun grondgebied aan.

2. De in artikel 4, punt 4, bedoelde criteria voor de identificatie van aanbieders van essentiële diensten luiden als volgt:

a) een entiteit verleent een dienst die van essentieel belang is voor de instandhouding van kritieke maatschappelijke en/of economische activiteiten;

b) de verlening van die dienst is afhankelijk van netwerk- en informatiesystemen, en

c) een incident zou aanzienlijke verstorende effecten hebben voor de verlening van die dienst.

3. Voor de toepassing van lid 1 stelt iedere lidstaat een lijst op van de in lid 2, onder a), bedoelde diensten.

4. Indien een entiteit een in lid 2, onder a), bedoelde dienst verleent in twee of meer lidstaten, plegen die lidstaten voor de toepassing van lid 1 overleg. Dat overleg vindt plaats alvorens een besluit inzake aanwijzing wordt genomen.

5. De lidstaten voeren op regelmatige basis en uiterlijk op 9 mei 2018 een evaluatie uit en zij actualiseren, in voorkomend geval, de lijst van geïdentificeerde aanbieders van essentiële diensten.

6. De samenwerkingsgroep ondersteunt overeenkomstig de in artikel 11 genoemde taken de lidstaten in het hanteren van een samenhangende aanpak voor de identificatie van aanbieders van essentiële diensten.

7. Voor de uitvoering van de in artikel 23 bedoelde evaluatie en uiterlijk op 9 november 2018, en vervolgens om de twee jaar, verstrekken de lidstaten de Commissie de informatie die zij nodig heeft voor de beoordeling van de uitvoering van deze richtlijn, met name wat betreft de samenhang van de aanpak van de lidstaten voor de identificatie van aanbieders van essentiële diensten. Deze informatie omvat ten minste:

a) de nationale maatregelen die de identificatie van aanbieders van essentiële diensten mogelijk maken;

([1]) Richtlijn 2013/11/EU van het Europees Parlement en de Raad van 21 mei 2013 betreffende alternatieve beslechting van consumentengeschillen en tot wijziging van Verordening (EG) nr. 2006/2004 en Richtlijn 2009/22/EG (richtlijn ADR consumenten) (PB L 165 van 18.6.2013, blz. 63).

b) de in lid 3 bedoelde lijst van diensten;

c) het aantal aanbieders van essentiële diensten die zijn geïdentificeerd voor elke in bijlage II genoemde sector en een indicatie van hun belang ten aanzien van die sector;

d) de drempels, waar zij voorkomen, voor het bepalen van het relevante verleningsniveau ten aanzien van het aantal gebruikers dat afhankelijk is van deze dienst als bedoeld in artikel 6, lid 1, onder a), of het belang van die bepaalde aanbieder van essentiële diensten overeenkomstig artikel 6, lid 1, onder f).

Ter bevordering van het verstrekken van vergelijkbare informatie kan de Commissie, zo veel mogelijk rekening houdend met het Enisa, passende technische richtsnoeren vaststellen betreffende de parameters voor de in dit lid bedoelde informatie.

Artikel 6

Aanzienlijk verstorend effect

1. Bij het bepalen van de omvang van een verstorend effect als bedoeld in artikel 5, lid 2, onder c), houden de lidstaten rekening met ten minste de volgende sectoroverschrijdende factoren:

a) het aantal gebruikers dat afhankelijk is van de door de betrokken entiteit verleende dienst;

b) de afhankelijkheid van andere in bijlage II genoemde sectoren van de door die entiteit verleende dienst;

c) de gevolgen die incidenten kunnen hebben, wat betreft mate en duur, voor economische en maatschappelijke activiteiten of de openbare veiligheid;

d) het marktaandeel van die entiteit;

e) de omvang van het geografische gebied dat door een incident kan worden getroffen;

f) het belang van de entiteit voor de instandhouding van een toereikend dienstverleningsniveau, rekening houdend met de beschikbare alternatieven voor het verlenen van die dienst.

2. Bij het bepalen of een incident een aanzienlijk verstorend effect zou hebben, houden de lidstaten waar passend ook rekening met sectorspecifieke factoren.

HOOFDSTUK II

NATIONALE KADERS VOOR DE BEVEILIGING VAN NETWERK- EN INFORMATIESYSTEMEN

Artikel 7

Nationale strategie voor de beveiliging van netwerk- en informatiesystemen

1. Elke lidstaat stelt een nationale strategie voor de beveiliging van netwerk- en informatiesystemen vast waarin de strategische doelstellingen en passende beleids- en regelgevingsmaatregelen worden bepaald met het oog op het tot stand brengen en handhaven van een hoog niveau van beveiliging van netwerk- en informatiesystemen, en waarin ten minste de in bijlage II genoemde sectoren en de in bijlage III bedoelde diensten aan bod komen. De nationale strategie voor de beveiliging van netwerk- en informatiesystemen voorziet met name in het volgende:

a) de doelstellingen en de prioriteiten van de nationale strategie voor de beveiliging van netwerk- en informatiesystemen;

b) een governancekader ter verwezenlijking van de doelstellingen en de prioriteiten van de nationale strategie voor de beveiliging van netwerk- en informatiesystemen, met inbegrip van de taken en verantwoordelijkheden van de overheidsorganen en de andere betrokken actoren;

c) de bepaling van maatregelen inzake paraatheid, reactie en herstel, met inbegrip van samenwerking tussen de publieke en de particuliere sector;

d) een vermelding van de onderwijs-, bewustmakings- en opleidingsprogramma's met betrekking tot de nationale strategie voor de beveiliging van netwerk- en informatiesystemen;

e) een vermelding van de plannen voor onderzoek en ontwikkeling met betrekking tot de nationale strategie voor de beveiliging van netwerk- en informatiesystemen;

f) een risicobeoordelingsplan om risico's vast te stellen;

g) een lijst van de verschillende actoren die betrokken zijn bij de uitvoering van de nationale strategie voor de beveiliging van netwerk- en informatiesystemen.

2. De lidstaten kunnen het Enisa om bijstand vragen bij de ontwikkeling van hun nationale strategie voor de beveiliging van netwerk- en informatiesystemen.

3. De lidstaten delen hun nationale strategie voor de beveiliging van netwerk- en informatiesystemen binnen drie maanden na de vaststelling ervan aan de Commissie mede. Daarbij mogen de lidstaten elementen van de strategie die verband houden met de nationale veiligheid, weglaten.

Artikel 8

Nationale bevoegde autoriteiten en centraal contactpunt

1. Elke lidstaat wijst één of meer nationale bevoegde autoriteiten inzake de beveiliging van netwerk- en informatiesystemen („bevoegde autoriteit") aan voor ten minste de in bijlage II genoemde sectoren en de in bijlage III bedoelde diensten. De lidstaten mogen deze taak toekennen aan één of meer bestaande autoriteiten.

2. De bevoegde autoriteiten monitoren de toepassing van deze richtlijn op nationaal niveau.

3. Elke lidstaat wijst een nationaal centraal contactpunt voor de beveiliging van netwerk- en informatiesystemen („centraal contactpunt") aan. De lidstaten mogen deze taak toekennen aan een bestaande autoriteit. Indien een lidstaat slechts één bevoegde autoriteit aanwijst, is die bevoegde autoriteit tevens het centraal contactpunt.

4. Het centraal contactpunt vervult een verbindingsfunctie om te zorgen voor grensoverschrijdende samenwerking van de autoriteiten van de lidstaten en met de betrokken autoriteiten in andere lidstaten en met de in artikel 11 bedoelde samenwerkingsgroep en het in artikel 12 bedoelde CSIRT-netwerk.

5. De lidstaten zorgen ervoor dat de bevoegde autoriteiten en de centrale contactpunten over de nodige middelen beschikken om de taken die aan hen zijn toegewezen op doeltreffende en efficiënte wijze uit te voeren en aldus de doelstellingen van deze richtlijn te verwezenlijken. De lidstaten zorgen ervoor dat de aangewezen vertegenwoordigers op doeltreffende, efficiënte en beveiligde wijze samenwerken binnen de samenwerkingsgroep.

6. De bevoegde autoriteiten en het centrale contactpunt plegen overleg en werken samen met de betrokken nationale rechtshandhavingsinstanties en de nationale autoriteiten voor gegevensbescherming waar dat passend is en in overeenstemming is met het nationale recht.

7. Elke lidstaat stelt de Commissie onverwijld in kennis van de aanwijzing van de bevoegde autoriteit en het centraal contactpunt, van hun taken, en van elke latere wijziging daarvan. Elke lidstaat maakt zijn aanwijzing van de bevoegde autoriteit en het centraal contactpunt openbaar. De Commissie zorgt voor de bekendmaking van de lijst van aangewezen centrale contactpunten.

Artikel 9

Computer security incident response teams („CSIRT's")

1. Elke lidstaat wijst één of meer CSIRT's aan die voldoen aan de voorschriften in bijlage I, punt 1, voor ten minste de in bijlage II genoemde sectoren en de in bijlage III bedoelde diensten, die verantwoordelijk zijn voor de behandeling van risico's en incidenten volgens een welomschreven proces. Een CSIRT mag binnen een bevoegde autoriteit worden opgezet.

2. De lidstaten zorgen ervoor dat de CSIRT's over de nodige middelen beschikken om hun in bijlage I, punt 2, vastgelegde taken doeltreffend uit te voeren.

De lidstaten zorgen ervoor dat hun CSIRT's op doeltreffende, efficiënte en beveiligde wijze samenwerken binnen het in artikel 12 bedoelde CSIRT-netwerk.

3. De lidstaten zorgen ervoor dat de aangewezen CSIRT's toegang hebben tot passende, beveiligde en weerbare communicatie- en informatie-infrastructuur op nationaal niveau.

4. De lidstaten informeren de Commissie over de bevoegdheid van de CSIRT's, en over de voornaamste elementen van de incidentenbehandelingsprocedure van de CSIRT's.

5. De lidstaten mogen het Enisa om bijstand vragen bij de ontwikkeling van nationale CSIRT's.

Artikel 10

Samenwerking op nationaal niveau

1. Wanneer de bevoegde autoriteit, het centraal contactpunt en het CSIRT van een lidstaat verschillend van elkaar zijn, werken zij samen inzake het vervullen van de in deze richtlijn vastgestelde verplichtingen.

2. De lidstaten zorgen ervoor dat de bevoegde autoriteiten of de CSIRT's de overeenkomstig deze richtlijn ingediende meldingen van incidenten ontvangen. Wanneer een lidstaat besluit dat CSIRT's geen meldingen mogen ontvangen, wordt de CSIRT's, in de mate die nodig is om hun taken uit te voeren, toegang verleend tot gegevens over incidenten die zijn gemeld door aanbieders van essentiële diensten, overeenkomstig artikel 14, leden 3 en 5, of door digitaledienstverleners, overeenkomstig artikel 16, leden 3 en 6.

3. De lidstaten zorgen ervoor dat de bevoegde autoriteiten of de CSIRT's de centrale contactpunten informeren over de overeenkomstig deze richtlijn ingediende meldingen van incidenten.

Het centraal contactpunt dient uiterlijk op 9 augustus 2018 en vervolgens eenmaal per jaar bij de samenwerkingsgroep een samenvattend verslag in over de ontvangen meldingen, met inbegrip van het aantal en de aard van de gemelde incidenten, en van de maatregelen die zijn genomen overeenkomstig artikel 14, leden 3 en 5, en artikel 16, leden 3 en 6.

HOOFDSTUK III

SAMENWERKING

Artikel 11

Samenwerkingsgroep

1. Er wordt een samenwerkingsgroep opgericht om de strategische samenwerking en de uitwisseling van informatie tussen de lidstaten te ondersteunen en te faciliteren, vertrouwen te scheppen, en een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie tot stand te brengen.

De samenwerkingsgroep verricht haar taken op basis van tweejarige werkprogramma's als bedoeld in lid 3, tweede alinea.

2. De groep bestaat uit vertegenwoordigers van de lidstaten, de Commissie en het Enisa.

Waar nodig kan de samenwerkingsgroep vertegenwoordigers van de belanghebbenden uitnodigen om deel te nemen aan haar werkzaamheden.

Het secretariaat wordt verzorgd door de diensten van de Commissie.

3. De samenwerkingsgroep heeft de volgende taken:

a) strategische richtsnoeren bepalen voor de activiteiten van het CSIRT-netwerk als bedoeld in artikel 12;

b) beste praktijken uitwisselen inzake de uitwisseling van informatie over de melding van incidenten als bedoeld in artikel 14, leden 3 en 5, en artikel 16, leden 3 en 6;

c) beste praktijken uitwisselen tussen de lidstaten en, in samenwerking met het Enisa, de lidstaten bijstaan bij het opbouwen van capaciteit op het gebied van de beveiliging van netwerk- en informatiesystemen;

d) de capaciteiten en de paraatheid van de lidstaten bespreken en, op vrijwillige basis, de nationale strategieën voor de beveiliging van netwerk- en informatiesystemen en de doeltreffendheid van de CSIRT's evalueren, en beste praktijken identificeren;

e) informatie en beste praktijken uitwisselen op het gebied van bewustmaking en opleiding;

f) informatie en beste praktijken uitwisselen inzake onderzoek en ontwikkeling op het gebied van de beveiliging van netwerk- en informatiesystemen;

g) waar nodig ervaringen op gebied van de beveiliging van netwerk- en informatiesystemen uitwisselen met de betrokken instellingen, organen, bureaus en agentschappen van de Unie;

h) de in artikel 19 bedoelde normen en specificaties bespreken met vertegenwoordigers van de betrokken Europese normalisatie-instellingen;

i) informatie over beste praktijken verzamelen inzake risico's en incidenten;

j) jaarlijks de in artikel 10, lid 3, tweede alinea, bedoelde samenvattende verslagen bestuderen;

k) de werkzaamheden met betrekking tot oefeningen in verband met de beveiliging van netwerk- en informatiesystemen, onderwijsprogramma's en opleiding, met inbegrip van de werkzaamheden van het Enisa, bespreken;

l) met de hulp van het Enisa beste praktijken uitwisselen inzake de identificatie door de lidstaten van aanbieders van essentiële diensten, onder meer wat betreft grensoverschrijdende afhankelijkheid inzake risico's en -incidenten;

m) de nadere bepalingen bespreken voor de rapportage betreffende incidentmeldingen als bedoeld in de artikelen 14 en 16.

Uiterlijk op 9 februari 2018, en vervolgens om de twee jaar, stelt de samenwerkingsgroep een werkprogramma op over te nemen maatregelen ter uitvoering van de doelstellingen en taken, die in overeenstemming moeten zijn met de doelstellingen van deze richtlijn.

4. Met het oog op de in artikel 23 bedoelde evaluatie stelt de samenwerkingsgroep uiterlijk op 9 augustus 2018, en daarna om de anderhalf jaar, een verslag op ter beoordeling van de ervaringen die zijn opgedaan met de strategische samenwerking die bij dit artikel wordt beoogd.

5. De Commissie stelt uitvoeringshandelingen vast waarin de procedurele regelingen zijn opgenomen die nodig zijn voor de werking van de samenwerkingsgroep. Die uitvoeringshandelingen worden volgens de in artikel 22, lid 2, bedoelde onderzoeksprocedure vastgesteld.

Voor de toepassing van de eerste alinea dient de Commissie het eerste ontwerp van uitvoeringshandeling uiterlijk op 9 februari 2017 in bij het in artikel 22, lid 1, bedoelde comité.

Artikel 12

Het CSIRT-netwerk

1. Om bij te dragen tot het opbouwen van vertrouwen tussen de lidstaten en om snelle en doeltreffende operationele samenwerking te bevorderen, wordt een netwerk van nationale CSIRT's ingesteld.

2. Het CSIRT-netwerk bestaat uit vertegenwoordigers van de CSIRT's van de lidstaten en CERT-EU. De Commissie zal als waarnemer deel uitmaken van het CSIRT-netwerk. Het Enisa zorgt voor het secretariaat en voor een actieve ondersteuning van de samenwerking tussen de CSIRT's.

3. Het CSIRT-netwerk heeft tot taak:

a) informatie uit te wisselen over diensten, activiteiten en samenwerkingscapaciteiten van de CSIRT's;

b) op verzoek van een vertegenwoordiger van een CSIRT van een lidstaat die mogelijk door een incident is getroffen, informatie die niet commercieel gevoelig is en verband houdt met het betreffende incident uit te wisselen en de daaraan verbonden risico's te bespreken; elk CSIRT van een lidstaat kan echter weigeren tot die bespreking bij te dragen als er een risico is dat het onderzoek naar het incident in gevaar wordt gebracht;

c) op vrijwillige basis niet-vertrouwelijke informatie over afzonderlijke incidenten uit te wisselen en beschikbaar te maken;

d) op verzoek van de vertegenwoordiger van het CSIRT van een lidstaat, een incident dat binnen de jurisdictie van die zelfde lidstaat heeft plaatsgevonden te bespreken en, indien mogelijk, een gecoördineerde reactie daarop te bepalen;

e) de lidstaten op basis van de vrijwillige wederzijdse bijstand te ondersteunen bij de aanpak van grensoverschrijdende incidenten;

f) andere vormen van operationele samenwerking te bespreken, te verkennen en vast te stellen, onder andere met betrekking tot:

   i) risico- en incidentcategorieën,

   ii) vroegtijdige waarschuwingen,

   iii) wederzijdse bijstand,

   iv) coördinatiebeginselen en -regelingen voor gevallen waarin de lidstaten reageren op grensoverschrijdende risico's en -incidenten;

g) de samenwerkingsgroep te informeren over zijn werkzaamheden en over de overeenkomstig punt f) besproken andere vormen van operationele samenwerking, en te verzoeken om sturing hieromtrent;

h) de lessen die uit oefeningen in verband met de beveiliging van netwerk- en informatiesystemen — waaronder de door het Enisa georganiseerde oefeningen — getrokken zijn, te bespreken;

i) op verzoek van een afzonderlijk CSIRT, de capaciteiten en paraatheid van dat CSIRT te bespreken;

j) richtsnoeren uit te vaardigen ter bevordering van de harmonisatie van de (operationele) praktijken inzake de toepassing van de bepalingen van dit artikel met betrekking tot de operationele samenwerking.

4. Met het oog op de in artikel 23 bedoelde evaluatie stelt het CSIRT-netwerk uiterlijk op 9 augustus 2018, en daarna om de anderhalf jaar, een verslag met conclusies en aanbevelingen op waarin het de ervaringen beoordeelt die zijn opgedaan met de operationele samenwerking die in dit artikel wordt beoogd. Dat verslag wordt tevens voorgelegd aan de samenwerkingsgroep.

5. Het CSIRT-netwerk stelt zijn eigen reglement van orde vast.

Artikel 13

Internationale samenwerking

De Unie kan overeenkomstig artikel 218 VWEU internationale overeenkomsten met derde landen of internationale organisaties sluiten waarbij deelname aan bepaalde activiteiten van de samenwerkingsgroep mogelijk wordt gemaakt en georganiseerd. In dergelijke overeenkomsten wordt rekening gehouden met de noodzaak om gegevens afdoende te beschermen.

HOOFDSTUK IV

BEVEILIGING VAN DE NETWERK- EN INFORMATIESYSTEMEN VAN AANBIEDERS VAN ESSENTIELE DIENSTEN

Artikel 14

Beveiligingseisen en melding van incidenten

1. De lidstaten zorgen ervoor dat aanbieders van essentiële diensten passende en evenredige technische en organisatorische maatregelen nemen om de risico's voor de beveiliging van netwerk- en informatiesystemen die zij bij hun activiteiten gebruiken, te beheersen. Deze maatregelen zorgen, gezien de stand van de techniek, voor een niveau van beveiliging van netwerk- en informatiesystemen dat is afgestemd op de risico's die zich voordoen.

2. De lidstaten zorgen ervoor dat aanbieders van essentiële diensten passende maatregelen nemen om de gevolgen van incidenten die de beveiliging van de voor de verlening van die essentiële diensten gebruikte netwerk- en informatiesystemen aantasten, te voorkomen en te minimaliseren zulks om de continuïteit van deze diensten te waarborgen.

3. De lidstaten zorgen ervoor dat aanbieders van essentiële diensten incidenten met aanzienlijke gevolgen voor de continuïteit van de door hen verleende essentiële diensten onverwijld aan de bevoegde autoriteit of het CSIRT melden. De meldingen bevatten informatie die de bevoegde autoriteit of het CSIRT in staat stelt de eventuele grensoverschrijdende gevolgen van het incident te bepalen. Melding leidt voor de meldende partij niet tot een verhoogde aansprakelijkheid.

4. Om te bepalen of een incident aanzienlijke gevolgen heeft, worden met name de volgende parameters in aanmerking genomen:

a) het aantal gebruikers dat door de verstoring van de essentiële dienst wordt getroffen;

b) de duur van het incident;

c) de omvang van het geografische gebied dat door het incident is getroffen.

5. Op basis van de informatie in de melding van de aanbieder van essentiële diensten informeert de bevoegde autoriteit of het CSIRT de andere getroffen lidstaat (of lidstaten) als het incident aanzienlijke gevolgen heeft voor de continuïteit van essentiële diensten in die lidstaat (of lidstaten). De bevoegde autoriteit of het CSIRT beschermt daarbij, overeenkomstig het Unierecht of nationale wetgeving die met het Unierecht in overeenstemming is, de veiligheids- en commerciële belangen van de aanbieder van essentiële diensten alsook de vertrouwelijkheid van de informatie in diens melding.

Indien de omstandigheden dit toelaten, verstrekt de bevoegde autoriteit of het CSIRT de aanbieder van essentiële diensten die de melding indient, relevante informatie over de follow-up van diens melding, zoals informatie die tot een doeltreffende behandeling van het incident kan bijdragen.

Op verzoek van de bevoegde autoriteit of van het CSIRT stuurt het centraal contactpunt de in de eerste alinea bedoelde meldingen door naar de centrale contactpunten van andere getroffen lidstaten.

6. Wanneer publieke bewustwording nodig is om een incident te voorkomen of een lopend incident te beheersen, kan de bevoegde autoriteit of het CSIRT na raadpleging van de aanbieder van essentiële diensten die de melding heeft ingediend, het publiek over afzonderlijke incidenten informeren.

7. Bevoegde autoriteiten die samen optreden binnen de samenwerkingsgroep kunnen richtsnoeren opstellen en aannemen over de omstandigheden waarin aanbieders van essentiële diensten verplicht zijn incidenten te melden, onder andere over de in lid 4 bedoelde parameters om te bepalen of de gevolgen van een incident aanzienlijk zijn.

Artikel 15

Uitvoering en handhaving

1. De lidstaten zorgen ervoor dat de bevoegde autoriteiten over de nodige bevoegdheden en middelen beschikken om de naleving van de krachtens artikel 14 op aanbieders van essentiële diensten rustende verplichtingen en de effecten daarvan op de beveiliging van netwerk- en informatiesystemen te beoordelen.

2. De lidstaten zorgen ervoor dat de bevoegde autoriteiten over de bevoegdheden en middelen beschikt om van aanbieders van essentiële diensten te eisen dat zij:

a) de informatie verschaffen die nodig is om de beveiliging van hun netwerk- en informatiesystemen te beoordelen, met inbegrip van gedocumenteerde beleidsmaatregelen op het gebied van beveiliging;

b) het bewijs leveren dat het beveiligingsbeleid daadwerkelijk wordt uitgevoerd, bijvoorbeeld de resultaten van een beveiligingsaudit die door de bevoegde autoriteit of een bevoegde auditor is uitgevoerd en, in het laatste geval, de resultaten daarvan, met inbegrip van de onderliggende gegevens, ter beschikking te stellen van de bevoegde autoriteit.

Bij het toezenden van die eis tot informatie of bewijs vermelden de bevoegde autoriteiten het doel van de eis en specificeren zij welke informatie moet worden verstrekt.

3. Na de beoordeling van de informatie of het resultaat van de in lid 2 bedoelde audits, kan de bevoegde autoriteit aan de aanbieders van essentiële diensten bindende aanwijzingen geven om de vastgestelde tekortkomingen te verbeteren.

4. De bevoegde autoriteit werkt nauw samen met de autoriteiten voor gegevensbescherming om incidenten aan te pakken die inbreuken in verband met persoonsgegevens tot gevolg hebben.

HOOFDSTUK V

BEVEILIGING VAN DE NETWERK- EN INFORMATIESYSTEMEN VAN DIGITALEDIENSTVERLENERS

Artikel 16

Beveiligingseisen en melding van incidenten

1. De lidstaten zorgen ervoor dat digitaledienstverleners de risico's voor de beveiliging van netwerk- en informatiesystemen die zij gebruiken voor het aanbieden van diensten in de Unie zoals genoemd in bijlage III, identificeren en passende en evenredige technische en organisatorische maatregelen nemen om die risico's te beheersen. Deze maatregelen zorgen, gezien de stand van de techniek, voor een niveau van beveiliging van netwerk- en informatiesystemen dat is afgestemd op de risico's die zich voordoen, en houden rekening met de volgende aspecten:

a) de beveiliging van systemen en voorzieningen,

b) behandeling van incidenten,

c) het beheer van de bedrijfscontinuïteit,

d) toezicht, controle en testen,

e) inachtneming van de internationale normen.

2. De lidstaten zorgen ervoor dat digitaledienstverleners maatregelen nemen om de gevolgen van incidenten die de beveiliging van hun netwerk- en informatiesystemen aantasten, voor de in bijlage III bedoelde diensten die in de Unie worden aangeboden, te voorkomen en te minimaliseren, zulks om de continuïteit van die diensten te waarborgen.

3. De lidstaten zorgen ervoor dat digitaledienstverleners ieder incident dat substantiële gevolgen heeft voor de verlening van een door hen in de Unie aangeboden dienst als bedoeld in bijlage III, onverwijld aan de bevoegde autoriteit of het CSIRT melden. De meldingen bevatten informatie die de bevoegde autoriteit of het CSIRT in staat stelt te bepalen of de grensoverschrijdende impact van het incident aanzienlijk is. Melding leidt voor de meldende partij niet tot een verhoogde aansprakelijkheid.

4. Om te bepalen of een incident aanzienlijke gevolgen heeft, worden met name de volgende parameters in aanmerking genomen:

a) het aantal gebruikers dat door het incident wordt getroffen, in het bijzonder gebruikers die de dienst nodig hebben voor de verlening van hun eigen diensten;

b) de duur van het incident;

c) de omvang van het geografische gebied dat door het incident is getroffen;

d) de omvang van de verstoring van de werking van de dienst;

e) de omvang van de impact op de economische en maatschappelijke activiteiten.

De verplichting om een incident te melden, geldt alleen wanneer de digitaledienstverlener toegang heeft tot de informatie die nodig is om de gevolgen van een incident ten aanzien van de eerste alinea bedoelde parameters te beoordelen.

5. Wanneer een aanbieder van essentiële diensten afhankelijk is van een derde digitaledienstverlener voor de verlening van een dienst die van essentieel belang is voor de instandhouding van kritieke maatschappelijke en economische activiteiten, meldt die aanbieder alle gevallen waarin een incident bij de digitaledienstverlener aanzienlijke gevolgen heeft voor de continuïteit van de essentiële diensten.

6. De bevoegde autoriteit of het CSIRT stelt in voorkomend geval, en in het bijzonder indien het in lid 3 bedoelde incident op twee of meer lidstaten betrekking heeft, de andere getroffen lidstaten in kennis. De bevoegde autoriteiten, de CSIRT's en het centrale contactpunt beschermen daarbij, overeenkomstig het Unierecht van de Unie of de nationale wetgeving die met het Unierecht in overeenstemming is, de veiligheids- en commerciële belangen van de digitaledienstverlener alsook de vertrouwelijkheid van de verstrekte informatie.

7. Wanneer publieke bewustwording nodig is om een incident te voorkomen of een lopend incident te beheersen, of wanneer de openbaarmaking van het incident anderszins in het algemeen belang is, kunnen de bevoegde autoriteit of het in kennis gestelde CSIRT en, in voorkomend geval, de autoriteiten of CSIRT's van andere betrokken lidstaten na overleg met de betrokken digitaledienstverlener het publiek informeren over afzonderlijke incidenten of verlangen dat de digitaledienstverlener dit doet.

8. De Commissie stelt uitvoeringshandelingen vast waarin de in lid 1 genoemde aspecten, alsmede de in lid 4 van dit artikel genoemde parameters, nader worden gespecificeerd. Deze uitvoeringshandelingen worden uiterlijk op 9 augustus 2017 volgens de in artikel 22, lid 2, bedoelde onderzoeksprocedure vastgesteld.

9. De Commissie kan uitvoeringshandelingen vaststellen waarin de formats en de procedures voor meldingseisen worden opgenomen. Die uitvoeringshandelingen worden volgens de in artikel 22, lid 2, bedoelde onderzoeksprocedure vastgesteld.

10. Onverminderd artikel 1, lid 6, leggen de lidstaten digitaledienstverleners geen andere beveiligings- of meldingseisen op.

11. Hoofdstuk V is niet van toepassing op kleine en micro-ondernemingen, zoals gedefinieerd in Aanbeveling 2003/361/EG van de Commissie ([1]).

([1]) Aanbeveling 2003/361/EG van de Commissie van 6 mei 2003 betreffende de definitie van kleine, middelgrote en micro-ondernemingen (PB L 124 van 20.5.2003, blz. 36).

Artikel 17

Uitvoering en handhaving

1. De lidstaten zorgen ervoor dat de bevoegde autoriteiten, indien nodig door middel van toezichtmaatregelen achteraf, maatregelen nemen wanneer zij bewijs in handen krijgen dat een digitaledienstverlener niet voldoet aan de in artikel 16 vastgestelde eisen. Dit bewijs kan worden voorgelegd door een bevoegde autoriteit van een andere lidstaat waar de dienst wordt verleend.

2. Voor de toepassing van lid 1 beschikken de bevoegde autoriteiten over de nodige bevoegdheden en middelen om te eisen dat digitaledienstverleners:

a) hen de informatie verstrekken die nodig is om de beveiliging van hun netwerk- en informatiesystemen te beoordelen, met inbegrip van gedocumenteerde beleidsmaatregelen op het gebied van beveiliging;

b) iedere niet-naleving van de in artikel 16 vastgestelde eisen rechtzetten.

3. Indien een digitaledienstverlener zijn hoofdvestiging of een vertegenwoordiger in een lidstaat heeft maar zijn netwerk- en informatiesystemen in één of meer andere lidstaten, werken de bevoegde autoriteit van de lidstaat van de hoofdvestiging of van de vertegenwoordiger samen met de bevoegde autoriteiten van die andere lidstaten en staan zij elkaar waar nodig bij. Deze bijstand en samenwerking kunnen betrekking hebben op de uitwisseling van informatie tussen de betrokken bevoegde autoriteiten en op verzoeken om de in lid 2 bedoelde toezichtmaatregelen.

Artikel 18

Jurisdictie en territorialiteit

1. Voor de toepassing van deze richtlijn wordt een digitaledienstverlener geacht te vallen onder de jurisdictie van de lidstaat waar hij zijn hoofdvestiging heeft. Een digitaledienstverlener wordt geacht zijn hoofdvestiging in een lidstaat te hebben als zijn hoofdkantoor zich in die lidstaat bevindt.

2. Een digitaledienstverlener die niet in de Unie is gevestigd, maar wel binnen de Unie diensten aanbiedt als bedoeld in bijlage III, wijst een vertegenwoordiger in de Unie aan. De vertegenwoordiger is gevestigd in één van de lidstaten waar de diensten worden aangeboden. De digitaledienstverlener wordt geacht te vallen onder de jurisdictie van de lidstaat waar zijn vertegenwoordiger is gevestigd.

3. De aanwijzing van een vertegenwoordiger door de digitaledienstverlener laat onverlet dat tegen de digitaledienstverlener rechtsvorderingen kunnen worden ingesteld.

HOOFDSTUK VI

NORMALISATIE EN VRIJWILLIGE MELDING

Artikel 19

Normalisatie

1. Ter bevordering van een geharmoniseerde uitvoering van artikel 14, leden 1 en 2, en artikel 16, leden 1 en 2, moedigen de lidstaten het gebruik van Europese of internationaal aanvaarde normen en/of specificaties voor de beveiliging van netwerk- en informatiesystemen aan, zonder het gebruik van een bepaald soort technologie op te leggen of te bevoorrechten.

2. Het Enisa vaardigt in samenwerking met de lidstaten adviezen en richtsnoeren uit betreffende de technische gebieden die in verband met lid 1 moeten worden bezien, alsook betreffende reeds bestaande normen, met inbegrip van de nationale normen van de lidstaten, die op deze gebieden zouden kunnen gaan gelden.

Artikel 20

Vrijwillige melding

1. Onverminderd artikel 3 mogen entiteiten die niet zijn geïdentificeerd als aanbieders van essentiële diensten en geen digitaledienstverleners zijn, op vrijwillige basis incidenten melden die aanzienlijke gevolgen hebben voor de continuïteit van de door hen verleende diensten.

2. Bij de behandeling van meldingen handelen de lidstaten overeenkomstig de in artikel 14 vastgestelde procedure. De lidstaten mogen verplichte meldingen prioritair verwerken ten opzichte van vrijwillige meldingen. Vrijwillige meldingen worden enkel verwerkt wanneer die verwerking geen onevenredige of overmatige belasting voor de betrokken lidstaat vormt.

Vrijwillige melding mag niet leiden tot het opleggen aan de meldende entiteit van verplichtingen waaraan zij niet zou zijn onderworpen als zij die melding niet had gedaan.

HOOFDSTUK VII

SLOTBEPALINGEN

Artikel 21

Sancties

De lidstaten stellen de voorschriften vast ten aanzien van de sancties die van toepassing zijn op overtredingen op nationale bepalingen die zijn vastgesteld op grond van deze richtlijn, en nemen alle nodige maatregelen om ervoor te zorgen dat deze sancties worden uitgevoerd. De sancties moeten doeltreffend, evenredig en afschrikkend zijn. De lidstaten stellen de Commissie uiterlijk op 9 mei 2018 van die voorschriften en deze maatregelen in kennis en delen haar latere wijzigingen onverwijld mede.

Artikel 22

Comitéprocedure

1. De Commissie wordt bijgestaan door het Comité beveiliging netwerk- en informatiesystemen. Dat comité is een comité in de zin van Verordening (EU) nr. 182/2011.

2. Wanneer naar dit lid wordt verwezen, is artikel 5 van Verordening (EU) nr. 182/2011 van toepassing.

Artikel 23

Evaluatie

1. De Commissie dient uiterlijk op 9 mei 2019 bij het Europees Parlement en de Raad een verslag in, waarin zij de coherentie beoordeelt van de aanpak van de lidstaten met betrekking tot de identificatie van aanbieders van essentiële diensten.

2. De Commissie evalueert op gezette tijden de werking van deze richtlijn en brengt daarover verslag uit aan het Europees Parlement en de Raad. Met dit doel en met het oog op de verdere bevordering van de strategische en operationele samenwerking, houdt de Commissie rekening met de verslagen van de samenwerkingsgroep en het CSIRT's-netwerk over de ervaringen die op strategisch en operationeel niveau zijn opgedaan. In haar evaluatie beoordeelt de Commissie ook de lijst in bijlagen II en III, en de coherentie van de identificatie van aanbieders van essentiële diensten en van diensten in de in bijlage II bedoelde sectoren. Het eerste verslag wordt uiterlijk op 9 mei 2021 ingediend.

Artikel 24

Overgangsmaatregelen

1. Onverminderd artikel 25 en teneinde de lidstaten tijdens de omzettingsperiode aanvullende mogelijkheden voor doeltreffende samenwerking te geven, vangen de samenwerkingsgroep en het CSIRT-netwerk uiterlijk op 9 februari 2017 aan met de uitvoering van de in artikel 11, lid 3, respectievelijk artikel 12, lid 3, opgenomen taken.

2. Om de lidstaten te ondersteunen inzake een coherente aanpak bij de identificatie van aanbieders van essentiële diensten, bespreekt de samenwerkingsgroep in de periode vanaf 9 februari 2017 tot 9 november 2018 de procedure, de inhoud en de soort van nationale maatregelen voor de identificatie van aanbieders van essentiële diensten binnen een specifieke sector overeenkomstig de in de artikelen 5 en 6 opgenomen criteria. Daarnaast bespreekt de samenwerkingsgroep op verzoek van een lidstaat diens specifieke ontwerpen van nationale maatregelen die het mogelijk maken aanbieders van essentiële diensten binnen een specifieke sector te identificeren overeenkomstig de in de artikelen 5 en 6 vastgestelde criteria.

3. Uiterlijk op 9 februari 2017 zorgen de lidstaten met het oog op de toepassing van dit artikel voor passende vertegenwoordiging in de samenwerkingsgroep en het CSIRT-netwerk.

Artikel 25

Omzetting

1. De lidstaten dienen uiterlijk op 9 mei 2018 de nodige wettelijke en bestuursrechtelijke bepalingen vast te stellen en bekend te maken om aan deze richtlijn te voldoen. Zij delen de Commissie de tekst van die bepalingen onverwijld mede.

Zij passen die bepalingen toe vanaf 10 mei 2018.

Wanneer de lidstaten die bepalingen aannemen, wordt in die bepalingen zelf of bij de officiële bekendmaking ervan naar deze richtlijn verwezen. De regels voor die verwijzing worden vastgesteld door de lidstaten.

2. De lidstaten delen de Commissie de tekst van de belangrijkste bepalingen van intern recht mede die zij op het onder deze richtlijn vallende gebied vaststellen.

Artikel 26

Inwerkingtreding

Deze richtlijn treedt in werking op de twintigste dag na die van de bekendmaking ervan in het *Publicatieblad van de Europese Unie*.

Artikel 27

Adressaten

Deze richtlijn is gericht tot de lidstaten.

Gedaan te Straatsburg, 6 juli 2016.

Voor het Europees Parlement	*Voor de Raad*
De voorzitter	*De voorzitter*
M. SCHULZ	I. KORČOK

BIJLAGE I

VOORSCHRIFTEN EN TAKEN VOOR COMPUTER SECURITY INCIDENT RESPONSE TEAMS (CSIRT's)

De voorschriften en taken voor CSIRT's moeten adequaat en duidelijk worden gedefinieerd en worden ondersteund door nationale beleids- en/of regelgevingsmaatregelen. Deze dienen het volgende te omvatten:

1) voorschriften voor CSIRT's:

   a) CSIRT's garanderen een hoge mate van beschikbaarheid van hun communicatiediensten door zwakke punten (single points of failure) te voorkomen, en beschikken over diverse kanalen waarlangs te allen tijde contact met hen kan worden opgenomen en contact met anderen kan worden opgenomen. De communicatiekanalen moeten voorts duidelijk worden gespecificeerd en bekend zijn bij de gebruikersgroep en de samenwerkingspartners;

   b) de lokalen van CSIRT's en de ondersteunende informatiesystemen moeten zich op beveiligde locaties bevinden;

   c) bedrijfscontinuïteit:

      i) de CSIRT's worden, met het oog op vlotte overdrachten, uitgerust met een adequaat systeem voor het beheren en routeren van verzoeken,

      ii) CSIRT's krijgen voldoende personeel om een volcontinue beschikbaarheid te garanderen,

      iii) CSIRT's doen een beroep op infrastructuur waarvan de continuïteit gewaarborgd is. Hiertoe wordt voorzien in redundante systemen en reservewerkruimten;

   d) CSIRT's kunnen indien zij dit wensen, deelnemen aan internationale samenwerkingsnetwerken.

2) Taken van de CSIRT's:

   a) de taken van de CSIRT's behelzen ten minste het volgende:

      i) monitoren van incidenten op nationaal niveau;

      ii) ten bate van de betrokken belanghebbende partijen zorgen voor vroegtijdige waarschuwingen, alarmmeldingen, aankondigingen en verspreiding van informatie over risico's en incidenten;

      iii) reageren op incidenten;

      iv) zorgen voor een dynamische risico- en incidentanalyse en situatiekennis;

      v) deelnemen aan het CSIRT-netwerk;

   b) CSIRT's zorgen voor op samenwerking gerichte contacten met de particuliere sector;

   c) ter bevordering van de samenwerking stimuleren de CSIRT's de vaststelling en het gebruik van gemeenschappelijke of gestandaardiseerde praktijken op het gebied van:

      i) procedures voor de behandeling van incidenten en risico's;

      ii) systemen voor de classificatie van incidenten, risico's en informatie.

BIJLAGE II

SOORT ENTITEITEN VOOR DE TOEPASSINGEN VAN ARTIKEL 4, PUNT 4

Sector	Deelsector	Soort entiteit
1. Energie	a) Elektriciteit	— Elektriciteitsbedrijf zoals gedefinieerd in artikel 2, punt 35, van Richtlijn 2009/72/EG van het Europees Parlement en de Raad ([1]), dat de functie verricht van „levering" zoals gedefinieerd in artikel 2, punt 19, van die richtlijn
		— Distributiesysteembeheerders zoals gedefinieerd in artikel 2, punt 6, van Richtlijn 2009/72/EG
		— Transmissiesysteembeheerders zoals gedefinieerd in artikel 2, punt 4, van Richtlijn 2009/72/EG
	b) Aardolie	— Exploitant van oliepijpleidingen
		— Exploitanten van voorzieningen voor de productie, raffinage en behandeling van olie, opslag en transport
	c) Gas	— Leveringsbedrijven zoals gedefinieerd in artikel 2, punt 8, van Richtlijn 2009/73/EG van het Europees Parlement en de Raad ([2])
		— Distributiesysteembeheerders zoals gedefinieerd in artikel 2, punt 6, van Richtlijn 2009/73/EG
		— Transmissiesysteembeheerders zoals gedefinieerd in artikel 2, punt 4, van Richtlijn 2009/73/EG
		— Opslagsysteembeheerders zoals gedefinieerd in artikel 2, punt 10, van Richtlijn 2009/73/EG
		— LNG-systeembeheerders zoals gedefinieerd in artikel 2, punt 12, van Richtlijn 2009/73/EG
		— Aardgasbedrijven zoals gedefinieerd in artikel 2, punt 1, van Richtlijn 2009/73/EG
		— Exploitanten van voorzieningen voor de raffinage en behandeling van aardgas
2. Vervoer	a) Luchtvervoer	— Luchtvaartmaatschappijen zoals gedefinieerd in artikel 3, punt 4, van Verordening (EG) nr. 300/2008 van het Europees Parlement en de Raad ([3])
		— Luchthavenbeheerders zoals gedefinieerd in artikel 2, punt 2, van Richtlijn 2009/12/EG van het Europees Parlement en de Raad ([4]); luchthavens zoals gedefinieerd in artikel 2, punt 1, van die richtlijn, inclusief de tot het kernnetwerk behorende luchthavens die in afdeling 2 van bijlage II van Verordening (EU) nr. 1315/2013 van het Europees Parlement en de Raad ([5]); zijn opgenomen, alsook de entiteiten die bijbehorende installaties bedienen welke zich op luchthavens bevinden

Sector	Deelsector	Soort entiteit
		— Luchtverkeersleidingsdiensten zoals gedefinieerd in artikel 2, punt 1, van Verordening (EG) nr. 549/2004 van het Europees Parlement en de Raad ([6])
	b) Spoorvervoer	— Infrastructuurbeheerders zoals gedefinieerd in artikel 3, punt 2, van Richtlijn 2012/34/EU van het Europees Parlement en de Raad ([7])
		— Spoorwegondernemingen zoals gedefinieerd in artikel 3, punt 1, van Richtlijn 2012/34/EU, inclusief exploitanten van dienstvoorzieningen zoals gedefinieerd in artikel 3, punt 12, van Richtlijn 2012/34/EU
	c) Vervoer over water	— Bedrijven voor vervoer over water (binnenvaart, kust- en zeevervoer) van passagiers en vracht die in bijlage I bij Verordening (EG) nr. 725/2004 van het Europees Parlement en de Raad ([8]) als bedrijven voor maritiem vervoer worden gedefinieerd, met uitzondering van de door deze bedrijven geëxploiteerde individuele vaartuigen
		— Beheerders van havens zoals gedefinieerd in artikel 3, punt 1, van Richtlijn 2005/65/EG van het Europees Parlement en de Raad ([9]), inclusief hun havenfaciliteiten zoals gedefinieerd in artikel 2, punt 11, van Verordening (EG) nr. 725/2004; alsook entiteiten die werken en uitrusting in havens beheren
		— Exploitanten van verkeersbegeleidingssystemen zoals gedefinieerd in artikel 3, onder o), van Richtlijn 2002/59/EG van het Europees Parlement en de Raad ([10])
	d) Vervoer over de weg	— Wegenautoriteiten zoals gedefinieerd in artikel 2, punt 12, van gedelegeerde Verordening (EU) 2015/962 van de Commissie ([11]) verantwoordelijk voor het verkeersbeheer
		— Exploitanten van intelligente vervoerssystemen zoals gedefinieerd in artikel 4, punt 1, van Richtlijn 2010/40/EU van het Europees Parlement en de Raad ([12])
3. Bankwezen:		Kredietinstellingen zoals gedefinieerd in artikel 4, punt 1, van Verordening (EU) nr. 575/2013 van het Europees Parlement en de Raad ([13])
4. Infrastructuur voor de financiële markt		— Exploitanten van handelsplatformen zoals gedefinieerd in artikel 4, punt 24, van Richtlijn 2014/65/EU van het Europees Parlement en de Raad ([14])
		— Centrale tegenpartijen zoals gedefinieerd in artikel 2, punt 1, van Verordening (EU) nr. 648/2012 van het Europees Parlement en de Raad ([15])
5. Gezondheidszorg	Zorginstellingen (waaronder ziekenhuizen en privéklinieken)	Zorgaanbieders zoals gedefinieerd in artikel 3, onder g), van Richtlijn 2011/24/EU van het Europees Parlement en de Raad ([16])

Sector	Deelsector	Soort entiteit
6. Levering en distributie van drinkwater		Leveranciers en distributeurs van „voor menselijke consumptie bestemd water" zoals gedefinieerd in artikel 2, punt 1, onder a), van Richtlijn 98/83/EG van de Raad ([17]), maar met uitzondering van distributeurs voor wie de distributie van water voor menselijke consumptie slechts een deel is van hun algemene activiteit van distributie van andere waren en goederen die niet worden beschouwd als essentiële diensten
7. Digitale infrastructuur		— Internetknooppunten
		— DNS-dienstverleners
		— Register voor topleveldomeinnamen

([1]) Richtlijn 2009/72/EG van het Europees Parlement en de Raad van 13 juli 2009 betreffende gemeenschappelijke regels voor de interne markt voor elektriciteit en tot intrekking van Richtlijn 2003/54/EG (PB L 211 van 14.8.2009, blz. 55).
([2]) Richtlijn 2009/73/EG van het Europees Parlement en de Raad van 13 juli 2009 betreffende gemeenschappelijke regels voor de interne markt voor aardgas en tot intrekking van Richtlijn 2003/55/EG (PB L 211 van 14.8.2009, blz. 94).
([3]) Verordening (EG) nr. 300/2008 van het Europees Parlement en de Raad van 11 maart 2008 inzake gemeenschappelijke regels op het gebied van de beveiliging van de burgerluchtvaart en tot intrekking van Verordening (EG) nr. 2320/2002 (PB L 97 van 9.4.2008, blz. 72).
([4]) Richtlijn 2009/12/EG van het Europees Parlement en de Raad van 11 maart 2009 inzake luchthavengelden (PB L 70 van 14.3.2009, blz. 11).
([5]) Verordening (EU) nr. 1315/2013 van het Europees Parlement en de Raad van 11 december 2013 betreffende richtsnoeren van de Unie voor de ontwikkeling van het trans-Europees vervoersnetwerk en tot intrekking van Besluit nr. 661/2010/EU (PB L 348 van 20.12.2013, blz. 1).
([6]) Verordening (EG) nr. 549/2004 van het Europees Parlement en de Raad van 10 maart 2004 tot vaststelling van het kader voor de totstandbrenging van het gemeenschappelijke Europese luchtruim („de kaderverordening") (PB L 96 van 31.3.2004, blz. 1).
([7]) Richtlijn 2012/34/EU van het Europees Parlement en de Raad van 21 november 2012 tot instelling van één Europese spoorwegruimte (PB L 343 van 14.12.2012, blz. 32).
([8]) Verordening (EG) nr. 725/2004 van het Europees Parlement en de Raad van 31 maart 2004 betreffende de verbetering van de beveiliging van schepen en havenfaciliteiten (PB L 129 van 29.4.2004, blz. 6).
([9]) Richtlijn 2005/65/EG van het Europees Parlement en de Raad van 26 oktober 2005 betreffende het verhogen van de veiligheid van havens (PB L 310 van 25.11.2005, blz. 28).
([10]) Richtlijn 2002/59/EG van het Europees Parlement en de Raad van 27 juni 2002 betreffende de invoering van een communautair monitoring- en informatiesysteem voor de zeescheepvaart en tot intrekking van Richtlijn 93/75/EEG van de Raad (PB L 208 van 5.8.2002, blz. 10).
([11]) Gedelegeerde Verordening (EU) 2015/962 van de Commissie van 18 december 2014 ter aanvulling van Richtlijn 2010/40/EU van het Europees Parlement en de Raad wat de verlening van EU-wijde realtimeverkeersinformatiediensten betreft (PB L 157 van 23.6.2015, blz. 21).
([12]) Richtlijn 2010/40/EU van het Europees Parlement en de Raad van 7 juli 2010 betreffende het kader voor het invoeren van intelligente vervoerssystemen op het gebied van wegvervoer en voor interfaces met andere vervoerswijzen (PB L 207 van 6.8.2010, blz. 1).
([13]) Verordening (EU) nr. 575/2013 van het Europees Parlement en de Raad van 26 juni 2013 betreffende prudentiële vereisten voor kredietinstellingen en beleggingsondernemingen en tot wijziging van Verordening (EU) nr. 648/2012 (PB L 176 van 27.6.2013, blz. 1).
([14]) 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 (PB L 173 van 12.6.2014, blz. 349).
([15]) Verordening (EU) nr. 648/2012 van het Europees Parlement en de Raad van 4 juli 2012 betreffende otc-derivaten, centrale tegenpartijen en transactieregisters (PB L 201 van 27.7.2012, blz. 1).
([16]) Richtlijn 2011/24/EU van het Europees Parlement en de Raad van 9 maart 2011 betreffende de toepassing van de rechten van patiënten bij grensoverschrijdende gezondheidszorg (PB L 88 van 4.4.2011, blz. 45).
([17]) Richtlijn 98/83/EG van de Raad van 3 november 1998 betreffende de kwaliteit van voor menselijke consumptie bestemd water (PB L 330 van 5.12.1998, blz. 32).

BIJLAGE III

SOORTEN DIGITALE DIENSTEN VOOR DE TOEPASSING VAN ARTIKEL 4, PUNT 5

1. Onlinemarktplaats
2. Onlinezoekmachine
3. Cloudcomputerdiensten