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

HET EUROPEES PARLEMENT EN DE RAAD VAN DE EUROPESE UNIE,

Gezien het Verdrag betreffende de werking van de Europese Unie, en met name artikel 83, lid 1,

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) Deze richtlijn heeft ten doel het strafrecht van de lidstaten inzake aanvallen op informatiesystemen onderling af te stemmen door minimumvoorschriften vast te stellen voor de definitie van strafbare feiten en de relevante sancties, en de samenwerking tussen de bevoegde autoriteiten, waaronder de politie en andere gespecialiseerde rechtshandhavingsinstanties van de lidstaten, alsook de bevoegde gespecialiseerde agentschappen en organen van de Unie, zoals Eurojust, Europol en zijn Europees cybercriminaliteitscentrum, en het Europees Agentschap voor netwerk- en informatiebeveiliging (Enisa), te verbeteren.

(2) Informatiesystemen zijn een essentieel onderdeel van de politieke, maatschappelijke en economische interactie in de Unie. De samenleving is sterk en in toenemende mate afhankelijk van dit soort systemen. De goede werking en de veiligheid van die systemen in de Unie is cruciaal voor de ontwikkeling van de interne markt en van een concurrerende en innovatieve economie. Het waarborgen van passende beschermingsniveaus voor informatiesystemen dient deel uit te maken van een effectief alomvattend kader van preventieve maatregelen, in combinatie met strafrechtelijke reacties op cybercriminaliteit.

(3) Aanvallen op informatiesystemen, in het bijzonder aanvallen in het kader van de georganiseerde criminaliteit, vormen een groeiende bedreiging, zowel in de Unie als in de rest van de wereld, en de bezorgdheid over mogelijke terroristische of politiek gemotiveerde aanvallen op informatiesystemen die deel uitmaken van de vitale infrastructuur van de lidstaten en van de Unie neemt toe. Dit brengt de totstandbrenging van een veiliger informatiemaatschappij en een ruimte van vrijheid, veiligheid en recht in gevaar en maakt derhalve een reactie op het niveau van de Unie en betere internationale samenwerking en coördinatie noodzakelijk.

(4) Ontwrichting of vernietiging van een aantal vitale infrastructuren in de Unie zou aanzienlijke grensoverschrijdende gevolgen hebben. Uit de behoefte aan een grotere mate van bescherming van de vitale infrastructuur in de Unie is gebleken dat de maatregelen tegen cyberaanvallen moeten worden aangevuld met zware strafrechtelijke straffen die in verhouding staan tot de ernst van deze aanvallen. Onder „vitale infrastructuur" kan worden verstaan een voorziening, systeem of een deel daarvan op het grondgebied van een lidstaat dat van essentieel belang is voor bijvoorbeeld het behoud van vitale maatschappelijke functies, de gezondheid, de veiligheid, de beveiliging, de economische welvaart of het maatschappelijk welzijn, zoals energiecentrales, vervoersnetwerken of overheidsnetwerken, en waarvan de verstoring of vernietiging in een lidstaat aanzienlijke gevolgen zou hebben doordat die functies ontregeld zouden raken.

(5) Er zijn aanwijzingen dat grootschalige aanvallen op de informatiesystemen die vaak van vitaal belang kunnen zijn voor staten of voor specifieke onderdelen van de publieke of particuliere sector steeds gevaarlijker en frequenter worden. Deze tendens gaat gepaard met de ontwikkeling van steeds geavanceerder methoden, zoals het creëren en gebruiken van zogenaamde „botnets", waarbij de strafbare handeling in verschillende fasen plaatsvindt en iedere fase afzonderlijk een ernstig risico voor openbare belangen kan opleveren. De richtlijn is er onder meer op gericht strafrechtelijke straffen in te voeren voor de fase waar de „botnet" tot stand wordt gebracht, namelijk wanneer controle op afstand over een aanzienlijk aantal computers tot stand wordt gebracht door deze door middel van gerichte cyberaanvallen te besmetten met kwaadaardige software. Als het eenmaal tot stand is gekomen, kan het netwerk van besmette computers, dat de „botnet" vormt, zonder medeweten van de gebruikers ervan worden ingezet om een grootschalige cyberaanval uit te voeren, die gewoonlijk het vermogen heeft om ernstige schade te veroorzaken als bedoeld in deze richtlijn. De lidstaten kunnen bepalen wat overeenkomstig hun nationaal recht en hun nationale praktijk onder ernstige schade wordt verstaan, zoals de ontregeling van systeemdiensten van groot openbaar nut, het veroorzaken van aanzienlijke financiële schade of het verlies van persoonsgegevens of gevoelige informatie.

(6) Grootschalige cyberaanvallen kunnen ernstige economische schade veroorzaken doordat informatiesystemen uitvallen en de communicatie wordt onderbroken en doordat er commercieel belangrijke vertrouwelijke of andere gegevens verloren gaan of worden gewijzigd. Er dient met name op te worden gelet dat innovatieve kleine en middelgrote ondernemingen bewuster worden gemaakt van bedreigingen en zwakke punten in verband met dergelijke aanvallen, vanwege hun grotere afhankelijkheid van de goede werking en beschikbaarheid van informatiesystemen en hun vaak beperkte middelen voor informatiebeveiliging.

([1]) PB C 218 van 23.7.2011, blz. 130.

([2]) Standpunt van het Europees Parlement van 4 juli 2013 (nog niet bekendgemaakt in het Publicatieblad) en besluit van de Raad van 22 juli 2013.

(7) Gemeenschappelijke definities op dit gebied zijn van belang om te garanderen dat de richtlijn in de lidstaten coherent wordt toegepast.

(8) Teneinde tot een gemeenschappelijke aanpak van de bestanddelen van strafbare feiten te komen, moet een gemeenschappelijk begrip van de strafbare feiten „onrechtmatige toegang tot een informatiesysteem", „onrechtmatige systeemverstoring", „onrechtmatige gegevensverstoring" en „onrechtmatige onderschepping" worden ingevoerd.

(9) Onderschepping omvat, maar is niet noodzakelijkerwijs beperkt tot, het afluisteren van, monitoren van of houden van toezicht op de inhoud van communicatie, en het ofwel rechtstreeks, door middel van toegang tot en gebruik van de informatiesystemen, ofwel indirect, door middel van het gebruik van een technisch hulpmiddel, zoals elektronische afluister- of aftapapparatuur, verkrijgen van de inhoud van gegevens.

(10) De lidstaten dienen met betrekking tot aanvallen op informatiesystemen in straffen te voorzien. Die straffen dienen doeltreffend, evenredig en afschrikkend te zijn en dienen gevangenisstraffen en/of geldboeten te omvatten.

(11) Deze richtlijn voorziet in elk geval in strafrechtelijke straffen voor gevallen die niet onbeduidend zijn. De lidstaten kunnen volgens hun nationaal recht en hun nationale praktijk bepalen welke gevallen onbeduidende gevallen zijn. Een geval kan bijvoorbeeld als onbeduidend worden beschouwd, wanneer de door het strafbare feit aangerichte schade aan en/of het risico voor openbare of particuliere belangen, zoals de integriteit van een computersysteem of computergegevens, of de integriteit, de rechten of andere belangen van een persoon, te verwaarlozen zijn of van dien aard zijn dat het binnen de wettelijke grenzen opleggen van een strafrechtelijke sanctie of het strafrechtelijk aansprakelijk stellen voor deze feiten niet noodzakelijk is.

(12) Het onderkennen en rapporteren van bedreigingen en risico's die uitgaan van cyberaanvallen en de kwetsbaarheid van informatiesystemen in dat verband, is een belangrijk element om cyberaanvallen daadwerkelijk te voorkomen en te bestrijden en om de beveiliging van informatiesystemen te verbeteren. Door het rapporteren van beveiligingslacunes te stimuleren kan op dit gebied nog meer effect worden gesorteerd. De lidstaten moeten mogelijkheden trachten aan te reiken voor de wettige opsporing en rapportering van beveiligingslacunes.

(13) Het is passend te voorzien in zwaardere straffen voor aanvallen op een informatiesysteem die gepleegd zijn door een criminele organisatie in de zin van Kaderbesluit 2008/841/JBZ van de Raad van 24 oktober 2008 ter bestrijding van georganiseerde criminaliteit [1], of voor grootschalige cyberaanvallen, die een aanzienlijk aantal informatiesystemen treffen, met inbegrip van aanvallen die tot doel hebben een „botnet" te creëren, of voor cyberaanvallen die ernstige schade veroorzaken, inclusief wanneer die worden uitgevoerd door middel van een „botnet". Het is tevens passend te voorzien in zwaardere straffen voor aanvallen op een vitale infrastructuur van de lidstaten of van de Unie.

(14) Het nemen van doeltreffende maatregelen tegen identiteitsdiefstal en andere identiteitsgerelateerde strafbare feiten is een ander belangrijk onderdeel van een geïntegreerde aanpak van cybercriminaliteit. De behoefte aan een optreden van de Unie tegen dit soort crimineel gedrag kan eveneens worden nagegaan in het kader van het onderzoek naar de noodzaak van een alomvattend horizontaal instrument van de Unie.

(15) De conclusies van de Raad van 27 tot en met 28 november 2008 hielden in dat er binnen de lidstaten en de Commissie een nieuwe strategie dient te worden ontwikkeld, waarbij rekening wordt gehouden met de inhoud van het uit 2001 daterende Verdrag inzake cybercriminaliteit van de Raad van Europa. Dat verdrag is het wettelijke referentiekader voor de bestrijding van cybercriminaliteit, waaronder aanvallen op informatiesystemen. Deze richtlijn bouwt daarop voort. Het zo spoedig mogelijk afronden van het proces van ratificering van dat verdrag door alle lidstaten moet als een prioriteit worden beschouwd.

(16) Gelet op de verschillende manieren waarop aanvallen kunnen worden uitgevoerd, en gelet op de snelle ontwikkelingen op het gebied van hardware en software, wordt er in deze richtlijn verwezen naar „instrumenten" die kunnen worden gebruikt voor het plegen van de in deze richtlijn opgesomde strafbare feiten. Onder instrumenten wordt bijvoorbeeld kwaadaardige software verstaan, zoals die voor het vervaardigen van botnets, waarmee cyberaanvallen worden gepleegd. Zelfs als een instrument geschikt of zelfs specifiek geschikt is voor het plegen van de in deze richtlijn opgesomde strafbare feiten, kan het toch voor legitieme doeleinden zijn vervaardigd. Aangezien strafbaarstelling moet worden voorkomen wanneer dergelijke instrumenten worden vervaardigd en in de handel worden gebracht voor legitieme doeleinden, zoals het testen van de betrouwbaarheid van informatietechnologieproducten of de beveiliging van informatiesystemen, moet er, naast het algemene vereiste van opzet, ook een bijzonder oogmerk zijn vereist om deze hulpmiddelen te gebruiken voor het plegen van een van de in deze richtlijn opgesomde strafbare feiten.

(17) Deze richtlijn verplicht niet tot strafbaarstelling wanneer aan de objectieve bestanddelen van de in deze richtlijn opgesomde strafbare feiten is voldaan, maar er geen sprake is van criminele opzet, bijvoorbeeld wanneer een persoon zich er niet bewust van was dat de toegang niet was toegestaan, of in het geval van het gemachtigd testen of beschermen van informatiesystemen, zoals wanneer een persoon door een bedrijf of een verkoper is aangewezen om de sterkte van zijn beveiligingssysteem te testen. In de context van deze richtlijn mogen contractuele verplichtingen of overeenkomsten om de toegang tot informatiesystemen door middel van gebruikersbeleid of functievoorwaarden te beperken, alsook arbeidsconflicten met betrekking tot de toegang tot en het gebruik van informatiesystemen van een werkgever voor privé-gebruik, geen strafrechtelijke gevolgen hebben indien de toegang onder die omstandigheden ongeoorloofd wordt geacht en derhalve de enige grondslag voor een strafprocedure zou vormen. Deze richtlijn doet niet af aan het recht van toegang tot informatie zoals dat is vastgelegd in het nationale recht en het recht van de Unie maar dat recht mag tegelijkertijd niet worden ingeroepen om onrechtmatige of willekeurige toegang tot informatie te rechtvaardigen.

[1] PB L 300 van 11.11.2008, blz. 42.

(18) Cyberaanvallen kunnen door verschillende omstandigheden in de hand worden gewerkt, zoals wanneer de dader uit hoofde van zijn functie toegang heeft tot de beveiligingsmechanismen van de getroffen informatiesystemen. In het kader van het nationale recht moet in strafprocedures voor zover nodig rekening worden gehouden met dergelijke omstandigheden.

(19) De lidstaten moeten in hun nationaal recht verzwarende omstandigheden opnemen overeenkomstig de in hun rechtsstelsels vastgestelde regels die hierop van toepassing zijn. Zij dienen ervoor te zorgen dat rechters deze verzwarende omstandigheden bij de straftoemeting van daders kunnen laten meewegen. Het behoort tot de beoordelingsvrijheid van de rechter deze omstandigheden samen met de andere feiten en omstandigheden van de zaak te beoordelen.

(20) Deze richtlijn betreft niet de voorwaarden voor de uitoefening van rechtsmacht met betrekking tot een van de daarin genoemde strafbare feiten, zoals een aangifte door het slachtoffer op de plaats waar de feiten zijn gepleegd, een aanklacht die is geformuleerd door de staat van de plaats waar de feiten zijn gepleegd of het feit dat de dader niet vervolgd is op de plaats waar de feiten zijn gepleegd.

(21) Staten en overheidsorganen moeten in het kader van deze richtlijn de eerbiediging van de mensenrechten en de fundamentele vrijheden onverkort blijven waarborgen, overeenkomstig bestaande internationale verplichtingen.

(22) Deze richtlijn vergroot het belang van netwerken, zoals dat van de G-8 of het netwerk van contactpunten van de Raad van Europa, die vierentwintig uur per dag en zeven dagen per week bereikbaar zijn. Die contactpunten moeten effectieve bijstand kunnen verlenen en aldus bijvoorbeeld uitwisseling van beschikbare relevante gegevens of verstrekking van technisch advies of juridische informatie ten behoeve van onderzoeken of procedures inzake strafbare feiten op het gebied van informatiesystemen en daarmee samenhangende gegevens, die de verzoekende lidstaat betreffen, vergemakkelijken. Met het oog op een goede werking van de netwerken moet elk contactpunt over de capaciteit beschikken om snel met het contactpunt van een andere lidstaat te communiceren, mede dankzij de ondersteuning van daartoe opgeleid en toegerust personeel. Gelet op de snelheid waarmee grootschalige cyberaanvallen kunnen worden uitgevoerd, dienen de lidstaten onverwijld te kunnen reageren op dringende bijstandsverzoeken van dit netwerk van contactpunten. In zulke gevallen kan het passend zijn dat naast het verzoek tot het verstrekken van gegevens telefonisch contact wordt opgenomen, teneinde te waarborgen dat het verzoek spoedig door de aangezochte staat in behandeling wordt genomen en dat binnen acht uur respons wordt gegeven.

(23) Om aanvallen op informatiesystemen te voorkomen en te bestrijden, is het van groot belang dat de overheidsinstanties zowel onderling als met de particuliere sector en het maatschappelijke middenveld samenwerken. De samenwerking tussen serviceproviders, producenten, rechtshandhavingsinstanties en justitiële autoriteiten moet worden gestimuleerd en verbeterd, met volledige inachtneming van de rechtsstaat. Deze samenwerking kan steun door serviceproviders omvatten om mogelijk bewijsmateriaal te helpen bewaren, om elementen aan te leveren die kunnen helpen bij de identificatie van daders, en om, in laatste instantie, informatiesystemen of -functies die zijn besmet of voor illegale doeleinden zijn gebruikt, overeenkomstig het nationale recht en de nationale praktijk geheel of gedeeltelijk buiten werking te stellen. De lidstaten moeten tevens de oprichting overwegen van samenwerkingsverbanden en partnerschappen met serviceproviders en producenten voor de uitwisseling van informatie in verband met strafbare feiten die onder het toepassingsgebied van deze richtlijn vallen.

(24) Er is behoefte aan het verzamelen van vergelijkbare gegevens over in deze richtlijn bedoelde strafbare feiten. Relevante gegevens moeten ter beschikking worden gesteld van de bevoegde gespecialiseerde agentschappen en organen van de Unie, zoals Europol en Enisa, naar gelang hun taken en informatiebehoeften, opdat er een vollediger beeld ontstaat van de problematiek van cybercriminaliteit en netwerk- en informatiebeveiliging op het niveau van de Unie en er een doeltreffender reactie kan worden geformuleerd. De lidstaten moeten aan Europol en zijn Europees centrum inzake cybercriminaliteit gegevens over de modus operandi van de daders verstrekken met het oog op dreigingsevaluatie en strategische analyses van cybercriminaliteit in overeenstemming met Besluit 2009/371/JBZ van de Raad van 6 april 2009 tot oprichting van de Europese politiedienst (Europol) ([1]). Het verstrekken van informatie kan een beter inzicht bevorderen in huidige en toekomstige bedreigingen, en aldus bijdragen tot een meer passende en gerichte besluitvorming over het bestrijden en voorkomen van aanvallen op informatiesystemen.

(25) De Commissie moet een verslag over de toepassing van deze richtlijn presenteren en de nodige wetgevingsvoorstellen indienen die zouden kunnen leiden tot een verruiming van de werkingssfeer ervan, rekening houdend met ontwikkelingen op het gebied van cybercriminaliteit. Deze ontwikkelingen kunnen technologische ontwikkelingen zijn, die bijvoorbeeld een effectievere handhaving op het gebied van aanvallen op informatiesystemen mogelijk maken, de voorkoming ervan vergemakkelijken of de gevolgen ervan tot een minimum beperken. Daartoe dient de Commissie rekening te houden met de beschikbare analyses en verslagen van betrokken actoren, meer bepaald Europol en Enisa.

(26) Om cybercriminaliteit op een effectieve manier te bestrijden, is het eveneens van belang de weerstandscapaciteit van informatiesystemen te verhogen door deze beter te beschermen tegen cyberaanvallen en de juiste maatregelen te nemen om dit te doen. De lidstaten moeten de nodige maatregelen treffen om vitale infrastructuur te beschermen tegen cyberaanvallen, en in het kader daarvan moeten zij de bescherming van hun informatiesystemen en daarmee samenhangende gegevens overwegen.

([1]) PB L 121 van 15.5.2009, blz. 37.

Het waarborgen van een passend niveau van bescherming en beveiliging van informatiesystemen door rechtspersonen, bijvoorbeeld in het kader van het verstrekken van openbaar beschikbare elektronische communicatiediensten overeenkomstig bestaande wetgeving van de Unie inzake de persoonlijke levenssfeer en elektronische communicatie en gegevensbescherming, is een wezenlijk bestanddeel van een alomvattende aanpak voor de doeltreffende bestrijding van cybercriminaliteit. Er moet worden gezorgd voor passende niveaus van bescherming tegen op een redelijke manier te identificeren bedreigingen en kwetsbaarheden, overeenkomstig de allernieuwste technieken voor specifieke sectoren en specifieke gegevensverwerkingssituaties. De kosten en lasten van dergelijke bescherming dienen evenredig te zijn met de waarschijnlijke schade die een cyberaanval voor de betrokkenen veroorzaakt. De lidstaten worden ertoe aangemoedigd om in het kader van hun nationaal recht te voorzien in aansprakelijkheidsmaatregelen ingeval een rechtspersoon duidelijk geen passend niveau van bescherming tegen cyberaanvallen heeft ingesteld.

(27) Aanzienlijke lacunes en verschillen in de wetgeving en de strafrechtelijke procedures van de lidstaten op het gebied van aanvallen op informatiesystemen kunnen een belemmering vormen voor de bestrijding van georganiseerde criminaliteit en terrorisme, en kunnen doeltreffende politiële en justitiële samenwerking op dit gebied bemoeilijken. Het transnationale en grensloze karakter van moderne informatiesystemen houdt in dat aanvallen op deze systemen een grensoverschrijdende dimensie hebben, wat tot gevolg heeft dat er dringend behoefte bestaat aan verdere onderlinge afstemming van het strafrecht op dit gebied. Bovendien dient de coördinatie van de vervolging van aanvallen op informatiesystemen te worden vergemakkelijkt door de passende uitvoering en toepassing van Kaderbesluit 2009/948/JBZ van de Raad van 30 november 2009 over het voorkomen en beslechten van geschillen over de uitoefening van rechtsmacht bij strafprocedures ([1]). De lidstaten moeten in samenwerking met de Unie tevens streven naar een betere internationale samenwerking op het gebied van de beveiliging van informatiesystemen, computernetwerken en computergegevens. In elke internationale overeenkomst die betrekking heeft op gegevensuitwisseling, moet passende aandacht worden besteed aan de beveiliging van het verzenden en het opslaan van gegevens.

(28) Een verbeterde samenwerking tussen de bevoegde rechtshandhavingsinstanties en justitiële autoriteiten in de hele Unie is van wezenlijk belang voor de effectieve bestrijding van cybercriminaliteit. In dit verband moet er meer werk worden gemaakt van een passende opleiding voor de betrokken instanties, met als doel een beter begrip te kweken van cybercriminaliteit en de gevolgen daarvan, en samenwerking en uitwisseling van „best practices" te bevorderen, bijvoorbeeld via de bevoegde gespecialiseerde agentschappen en organen van de Unie. Die opleiding moet onder meer de verschillende nationale rechtsstelsels, de mogelijke juridische en technische uitdagingen bij strafrechtelijke onderzoeken of de bevoegdheidsverdeling tussen de betrokken nationale autoriteiten onder de aandacht brengen.

(29) Deze richtlijn eerbiedigt de mensenrechten en de fundamentele vrijheden en is in overeenstemming met de beginselen die met name bij het Handvest van de grondrechten van de Europese Unie en het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden zijn erkend, waaronder de bescherming van persoonsgegevens, de eerbiediging van de persoonlijke levenssfeer, de vrijheid van meningsuiting en van informatie, het recht op een eerlijk proces, het beginsel van het vermoeden van onschuld en de rechten van de verdediging, alsmede het legaliteitsbeginsel en het evenredigheidsbeginsel inzake delicten en straffen. Deze richtlijn beoogt in het bijzonder de onverkorte eerbiediging van deze rechten en beginselen te waarborgen en moet dienovereenkomstig worden uitgevoerd.

(30) De bescherming van persoonsgegevens is een grondrecht overeenkomstig artikel 16, lid 1, VWEU en artikel 8 van het Handvest van de grondrechten van de Europese Unie. Derhalve moet elke verwerking van persoonsgegevens in het kader van de uitvoering van deze richtlijn volledig voldoen aan de op grond van de Verdragen aangenomen EU-wetgeving inzake gegevensbescherming.

(31) Overeenkomstig artikel 3 van het Protocol betreffende de positie van het Verenigd Koninkrijk en Ierland ten aanzien van de ruimte van vrijheid, veiligheid en recht, dat gehecht is aan het Verdrag betreffende de Europese Unie en het Verdrag betreffende de werking van de Europese Unie, hebben die lidstaten te kennen gegeven dat zij aan de vaststelling en toepassing van deze richtlijn wensen deel te nemen.

(32) Overeenkomstig de artikelen 1 en 2 van het Protocol betreffende de positie van Denemarken, dat gehecht is aan het Verdrag betreffende de Europese Unie en het Verdrag betreffende de werking van de Europese Unie, neemt Denemarken niet deel aan de vaststelling van deze richtlijn; deze richtlijn is niet bindend voor noch van toepassing in deze lidstaat.

(33) Aangezien de doelstellingen van deze richtlijn, namelijk aanvallen op informatiesystemen in alle lidstaten te bestraffen met doeltreffende, evenredige en afschrikkende straffen en de justitiële samenwerking te verbeteren en te bevorderen, niet voldoende door de lidstaten kunnen worden verwezenlijkt, en derhalve, vanwege de omvang en de gevolgen ervan, beter door de Unie kunnen worden verwezenlijkt, kan de Unie maatregelen nemen overeenkomstig het subsidiariteitsbeginsel van artikel 5 van het Verdrag betreffende de Europese Unie. Overeenkomstig het in hetzelfde artikel neergelegde beginsel van evenredigheid, gaat deze richtlijn niet verder dan nodig is om deze doelstellingen te verwezenlijken.

(34) Deze richtlijn strekt tot wijziging en uitbreiding van de bepalingen van Kaderbesluit 2005/222/JBZ van de Raad van 24 februari 2005 over aanvallen op informatiesystemen ([2]). Aangezien de aan te brengen wijzigingen zowel in aantal als wat betreft hun inhoud substantieel zijn, dient het Kaderbesluit 2005/222/JBZ ter wille van de duidelijkheid integraal te worden vervangen voor de lidstaten die aan de vaststelling van deze richtlijn deelnemen,

([1]) PB L 328 van 15.12.2009, blz. 42.

([2]) PB L 69 van 16.3.2005, blz. 67.

HEBBEN DE VOLGENDE RICHTLIJN VASTGESTELD:

Artikel 1

Onderwerp

Deze richtlijn stelt minimumvoorschriften vast voor de definitie van strafbare feiten en sancties op het gebied van aanvallen op informatiesystemen. Zij strekt er tevens toe de preventie van deze strafbare feiten te vergemakkelijken en de samenwerking tussen de justitiële en de andere bevoegde autoriteiten te verbeteren.

Artikel 2

Definities

In deze richtlijn wordt verstaan onder:

a) „informatiesysteem": apparaat of groep van onderling verbonden of samenhangende apparaten, waarvan er één of meer op basis van een programma automatisch computergegevens verwerken, alsmede de computergegevens die met dat apparaat of die groep van apparaten worden opgeslagen, verwerkt, opgehaald of verzonden met het oog op de werking, het gebruik, de beveiliging en het onderhoud daarvan;

b) „computergegevens": een weergave van feiten, gegevens of begrippen in een vorm die geschikt is voor verwerking in een informatiesysteem, met inbegrip van programma's die een informatiesysteem een bepaalde functie kunnen laten vervullen;

c) „rechtspersoon": een entiteit die krachtens het toepasselijke recht de hoedanigheid van rechtspersoon bezit, met uitzondering van staten of overheidsentiteiten die handelen in de uitoefening van het openbaar gezag of van publiekrechtelijke internationale organisaties;

d) „onrechtmatig": een gedraging waarnaar in deze richtlijn wordt verwezen, waaronder toegang, verstoring, onderschepping, die niet is toegestaan door de eigenaar of een andere houder van rechten op het systeem of op een deel daarvan, of niet is toegestaan krachtens het nationale recht.

Artikel 3

Onrechtmatige toegang tot informatiesystemen

De lidstaten treffen de nodige maatregelen om opzettelijke, onrechtmatige toegang tot een informatiesysteem of tot een deel daarvan, strafbaar te stellen wanneer het strafbaar feit is gepleegd door een beveiligingsmaatregel te doorbreken, althans voor gevallen die niet onbeduidend zijn.

Artikel 4

Onrechtmatige systeemverstoring

De lidstaten treffen de nodige maatregelen om het ernstig hinderen of het onderbreken van de werking van een informatiesysteem, door de invoer, de transmissie, het beschadigen, wissen, verminken, wijzigen, onderdrukken of ontoegankelijk maken van computergegevens, indien dat opzettelijk en op onrechtmatige wijze geschiedt, strafbaar te stellen, althans voor gevallen die niet onbeduidend zijn.

Artikel 5

Onrechtmatige gegevensverstoring

De lidstaten treffen de nodige maatregelen om het wissen, beschadigen, verminken, wijzigen, onderdrukken of ontoegankelijk maken van computergegevens in een informatiesysteem, indien dat opzettelijk en op onrechtmatige wijze geschiedt, strafbaar te stellen, althans voor gevallen die niet onbeduidend zijn.

Artikel 6

Onrechtmatige onderschepping

De lidstaten treffen de nodige maatregelen om het met technische middelen onderscheppen van niet-openbare transmissies van computergegevens naar, vanuit of binnen een informatiesysteem, met inbegrip van elektromagnetische emissies uit een informatiesysteem dat zulke computergegevens draagt, indien dat opzettelijk en op onrechtmatige wijze geschiedt, strafbaar te stellen, althans voor gevallen die niet onbeduidend zijn.

Artikel 7

Instrumenten voor het plegen van strafbare feiten

De lidstaten treffen de nodige maatregelen om het opzettelijk vervaardigen, verkopen, verkrijgen voor gebruik, invoeren, verspreiden of op andere wijze beschikbaar maken van één van de volgende instrumenten, indien dat opzettelijk geschiedt en met het oogmerk deze te gebruiken voor het plegen van een van de in de artikelen 3 tot en met 6 bedoelde feiten, strafbaar te stellen, althans voor gevallen die niet onbeduidend zijn:

a) een computerprogramma, dat hoofdzakelijk ontworpen of geschikt gemaakt is voor het plegen van de in de artikelen 3 tot en met 6 bedoelde strafbare feiten;

b) een computerwachtwoord, toegangscode of soortgelijke gegevens waarmee toegang kan worden verkregen tot een informatiesysteem of een deel daarvan.

Artikel 8

Uitlokking, medeplichtigheid en poging

1. De lidstaten zorgen ervoor dat uitlokking van of medeplichtigheid aan een van de in de artikelen 3 tot en met 7 genoemde feiten strafbaar wordt gesteld.

2. De lidstaten zorgen ervoor dat poging tot het plegen van een van de in de artikelen 4 en 5 genoemde feiten strafbaar wordt gesteld.

Artikel 9

Straffen

1. De lidstaten treffen de nodige maatregelen om ervoor te zorgen dat op de in de artikelen 3 tot en met 8 bedoelde strafbare feiten doeltreffende, evenredige en afschrikkende straffen worden gesteld.

2. De lidstaten treffen de nodige maatregelen om ervoor te zorgen dat op de in de artikelen 3 tot en met 7 bedoelde strafbare feiten een maximale gevangenisstraf van ten minste twee jaar wordt gesteld, althans voor gevallen die niet onbeduidend zijn.

3. De lidstaten nemen de nodige maatregelen om ervoor te zorgen dat op de in de artikelen 4 en 5 bedoelde strafbare feiten, wanneer deze opzettelijk worden gepleegd, een maximale gevangenisstraf van ten minste drie jaar wordt gesteld, wanneer

een aanzienlijk aantal informatiesystemen getroffen zijn door het gebruik van een in artikel 7 bedoeld instrument, dat hoofdzakelijk voor dit doel is ontworpen of geschikt gemaakt.

4. De lidstaten nemen de nodige maatregelen om ervoor te zorgen dat op de in de artikelen 4 en 5 bedoelde strafbare feiten een maximale gevangenisstraf van ten minste vijf jaar wordt gesteld wanneer het strafbare feit:

a) is gepleegd in het kader van een criminele organisatie zoals omschreven in Kaderbesluit 2008/841/JBZ van de Raad, ongeacht de daarin aangegeven straf, of

b) ernstige schade teweegbrengt, of

c) is gepleegd tegen een informatiesysteem van een vitale infrastructuur.

5. De lidstaten treffen de nodige maatregelen om ervoor te zorgen dat wanneer de in de artikelen 4 en 5 bedoelde strafbare feiten worden gepleegd door misbruik te maken van persoonsgegevens van een andere persoon met het oogmerk het vertrouwen van een derde te winnen, waardoor de rechtmatige bezitter van een identiteit schade wordt berokkend, dit, overeenkomstig de betrokken bepalingen van het nationale recht, kan worden beschouwd als verzwarende omstandigheden, tenzij deze omstandigheden reeds worden bestreken door een ander feit dat overeenkomstig het nationaal recht strafbaar is.

Artikel 10

Aansprakelijkheid van rechtspersonen

1. De lidstaten treffen de nodige maatregelen om ervoor te zorgen dat rechtspersonen aansprakelijk kunnen worden gesteld voor de in de artikelen 3 tot en met 8 genoemde strafbare feiten wanneer die feiten ten voordele van die rechtspersonen zijn gepleegd door personen die hetzij individueel, hetzij als lid van een orgaan van de rechtspersoon handelen en die in de rechtspersoon een leidende functie bekleden op grond van:

a) de bevoegdheid om de rechtspersoon te vertegenwoordigen, of

b) de bevoegdheid om namens de rechtspersoon beslissingen te nemen, of

c) de bevoegdheid om binnen de rechtspersoon toezicht uit te oefenen.

2. De lidstaten treffen de nodige maatregelen om ervoor te zorgen dat rechtspersonen aansprakelijk kunnen worden gesteld indien het gebrek aan toezicht of controle door een in lid 1 bedoelde persoon het voor een persoon die onder het gezag van de rechtspersoon staat, mogelijk heeft gemaakt ten voordele van die rechtspersoon een van de in de artikelen 3 tot en met 8 bedoelde strafbare feiten te plegen.

3. De aansprakelijkheid van rechtspersonen krachtens de leden 1 en 2 sluit strafvervolging van natuurlijke personen die als daders, uitlokkers of medeplichtigen betrokken zijn bij een in de artikelen 3 tot en met 8 bedoeld strafbaar feit, niet uit.

Artikel 11

Sancties tegen rechtspersonen

1. De lidstaten treffen de nodige maatregelen om ervoor te zorgen dat tegen een rechtspersoon die uit hoofde van artikel 10, lid 1, aansprakelijk is gesteld, doeltreffende, evenredige en afschrikkende sancties kunnen worden opgelegd. Deze sancties omvatten al dan niet strafrechtelijke geldboetes en kunnen andere sancties omvatten, zoals:

a) uitsluiting van door de overheid verleende uitkeringen of steun;

b) een tijdelijk of permanent verbod op het uitoefenen van commerciële activiteiten;

c) plaatsing onder toezicht van de rechter;

d) een gerechtelijk bevel tot ontbinding;

e) tijdelijke of permanente sluiting van vestigingen die zijn gebruikt voor het plegen van het strafbare feit.

2. De lidstaten treffen de nodige maatregelen om ervoor te zorgen dat aan een rechtspersoon die volgens artikel 10, lid 2, aansprakelijk is, sancties of andere maatregelen kunnen worden opgelegd die doeltreffend, evenredig en afschrikkend zijn.

Artikel 12

Rechtsmacht

1. De lidstaten vestigen hun rechtsmacht ten aanzien van de in de artikelen 3 tot en met 8 bedoelde strafbare feiten indien deze:

a) geheel of gedeeltelijk op hun grondgebied zijn gepleegd, of

b) door een van hun onderdanen zijn gepleegd, in elk geval voor zover het feit op de plaats waar het is gepleegd strafbaar is gesteld.

2. Bij het vestigen van zijn rechtsmacht overeenkomstig lid 1, onder a), zorgt elke lidstaat ervoor dat deze zich uitstrekt tot gevallen waarin:

a) de dader het strafbare feit pleegt terwijl hij zich fysiek op zijn grondgebied bevindt, ongeacht of het strafbare feit is gericht tegen een informatiesysteem op dat grondgebied, of

b) het strafbare feit gericht is tegen een informatiesysteem op zijn grondgebied, ongeacht of de dader het strafbare feit pleegt terwijl hij zich fysiek op dat grondgebied bevindt.

3. Elke lidstaat stelt de Commissie ervan in kennis wanneer hij besluit om ook over een strafbaar feit als bedoeld in de artikelen 3 tot en met 8 dat buiten zijn grondgebied is gepleegd zijn rechtsmacht te vestigen, bijvoorbeeld indien het strafbare feit is gepleegd:

a) door iemand die zijn vaste woon- of verblijfplaats op zijn grondgebied heeft, of

b) ten voordele van een rechtspersoon die gevestigd is op zijn grondgebied.

Artikel 13

Uitwisseling van informatie

1. Voor informatie-uitwisseling over strafbare feiten in de zin van de artikelen 3 tot en met 8 zorgen de lidstaten ervoor dat zij beschikken over een operationeel nationaal contactpunt en gebruikmaken van het bestaande netwerk van operationele contactpunten die vierentwintig uur per dag en zeven dagen per week bereikbaar zijn. De lidstaten zorgen er tevens voor dat zij over procedures beschikken waarmee zij in geval van dringende verzoeken voor bijstand binnen maximaal acht uur na ontvangst ten minste kunnen aangeven of het verzoek om bijstand zal worden ingewilligd, alsmede de vorm en het tijdstip waarop dit naar verwachting zal gebeuren.

2. De lidstaten stellen de Commissie in kennis van het in lid 1 bedoelde contactpunt dat is aangewezen. De Commissie geeft deze informatie door aan de overige lidstaten en aan de bevoegde gespecialiseerde agentschappen en organen van de Unie.

3. De lidstaten treffen de nodige maatregelen om ervoor te zorgen dat passende rapportagekanalen ter beschikking worden gesteld om het rapporteren zonder onnodige vertraging van de in de artikelen 3 tot en met 6 genoemde strafbare feiten aan de bevoegde nationale autoriteiten te vergemakkelijken.

Artikel 14

Toetsing en statistieken

1. De lidstaten zorgen voor een systeem voor het registreren, aanmaken en verstrekken van statistische gegevens over de in de artikelen 3 tot en met 7 bedoelde strafbare feiten.

2. De in lid 1 bedoelde statistieken vermelden ten minste de beschikbare gegevens over het aantal in de artikelen 3 tot en met 7 bedoelde strafbare feiten die door de lidstaten zijn geregistreerd en het aantal personen dat is vervolgd en veroordeeld in verband met de in de artikelen 3 tot en met 7 bedoelde strafbare feiten.

3. De lidstaten verstrekken de overeenkomstig dit artikel verzamelde gegevens aan de Commissie. De Commissie zorgt ervoor dat een geconsolideerd overzicht van hun statistische verslagen wordt gepubliceerd en aan de bevoegde gespecialiseerde agentschappen en organen van de Unie wordt toegezonden.

Artikel 15

Vervanging van Kaderbesluit 2005/222/JBZ

Kaderbesluit 2005/222/JBZ wordt vervangen voor de lidstaten die aan de vaststelling van deze richtlijn deelnemen, onverminderd de verplichtingen van de lidstaten wat betreft de termijn voor de omzetting van het kaderbesluit in intern recht.

Voor de lidstaten die aan de vaststelling van deze richtlijn deelnemen, gelden verwijzingen naar Kaderbesluit 2005/222/JBZ als verwijzingen naar deze richtlijn.

Artikel 16

Omzetting

1. De lidstaten doen de nodige wettelijke en bestuursrechtelijke bepalingen in werking treden om uiterlijk 4 september 2015 aan deze richtlijn te voldoen.

2. De lidstaten delen aan de Commissie de tekst mede van alle bepalingen waarmee zij hun verplichtingen uit hoofde van deze richtlijn in intern recht omzetten.

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

Artikel 17

Rapportering

De Commissie dient uiterlijk 4 september 2017 bij het Europees Parlement en de Raad een verslag in waarin wordt beoordeeld in hoeverre de lidstaten de nodige maatregelen hebben genomen om aan deze richtlijn te voldoen, indien nodig vergezeld van wetgevingsvoorstellen. De Commissie houdt tevens rekening met de technische en juridische ontwikkelingen op het vlak van cybercriminaliteit, met name met betrekking tot het toepassingsgebied van deze richtlijn.

Artikel 18

Inwerkingtreding

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

Artikel 19

Adressaten

Deze richtlijn is overeenkomstig de Verdragen gericht tot de lidstaten.

Gedaan te Brussel, 12 augustus 2013.

Voor het Europees Parlement	*Voor de Raad*
De voorzitter	*De voorzitter*
M. SCHULZ	L. LINKEVIČIUS