EUROPESE
COMMISSIE

Brussel, 30.5.2016
COM(2016) 363 final

2013/0027 (COD)

MEDEDELING VAN DE COMMISSIE AAN HET EUROPEES PARLEMENT

overeenkomstig artikel 294, lid 6, van het Verdrag betreffende de werking van de Europese Unie

over het

standpunt van de Raad over de vaststelling van een richtlijn van het Europees Parlement en de Raad houdende maatregelen om een hoog gemeenschappelijk niveau van netwerk- en informatiebeveiliging in de Unie te waarborgen

(Voor de EER relevante tekst)

2013/0027 (COD)

MEDEDELING VAN DE COMMISSIE AAN HET EUROPEES PARLEMENT

overeenkomstig artikel 294, lid 6, van het Verdrag betreffende de werking van de Europese Unie

over het

standpunt van de Raad over de vaststelling van een richtlijn van het Europees Parlement en de Raad houdende maatregelen om een hoog gemeenschappelijk niveau van netwerk- en informatiebeveiliging in de Unie te waarborgen

(Voor de EER relevante tekst)

1. ACHTERGROND

Indiening van het voorstel bij het Europees Parlement en de Raad (COM(2013) 48 - 2013/0027/COD):	7.2.2013
Advies van het Europees Economisch en Sociaal Comité:	22.5.2013
Standpunt van het Europees Parlement in eerste lezing:	13.3.2014
Vaststelling van het standpunt van de Raad:	17.5.2016

2. DOEL VAN HET VOORSTEL VAN DE COMMISSIE

In de eerste plaats moet elke lidstaat op grond van het voorstel zorgen voor een minimale nationale capaciteit door:

- voor netwerk- en informatiebeveiliging (NIB) bevoegde autoriteiten aan te wijzen;
- computercrisisteams op te zetten (Computer Emergency Response Teams – CERT's);
- nationale NIB-strategieën en -samenwerkingsplannen vast te stellen.

In de tweede plaats zouden de nationale bevoegde autoriteiten moeten samenwerken in het kader van een netwerk dat beveiligde en doeltreffende coördinatie, inclusief gecoördineerde informatie-uitwisseling, alsmede opsporing en reactie op EU-niveau mogelijk maakt. Via dit netwerk zouden de lidstaten informatie moeten uitwisselen en moeten samenwerken om NIB-dreigingen en -incidenten aan te pakken op basis van het Europese NIB-samenwerkingsplan. Om ervoor te zorgen dat alle bevoegde autoriteiten naar behoren en tijdig worden betrokken, moeten incidenten van criminele aard op grond van het voorstel aan de wetshandhavingsinstanties worden gemeld, en moet Europol worden betrokken bij coördinatiemechanismen binnen de hele EU.

In de derde plaats moet er, uitgaande van het model van de kaderrichtlijn voor elektronische communicatie, voor worden gezorgd dat een cultuur van risicobeheer ingang vindt en dat de particuliere en de openbare sector onderling informatie uitwisselen. Zowel bedrijven uit specifieke kritieke sectoren als overheden zullen ertoe worden verplicht de risico's waarmee

zij worden geconfronteerd, te beoordelen en passende en evenredige maatregelen te nemen om de NIB te waarborgen. Zij zullen aan de bevoegde autoriteiten verslag moeten uitbrengen over incidenten die hun netwerken en informatiesystemen ernstig in gevaar brengen en de continuïteit van kritieke diensten en de levering van goederen significant beïnvloeden.

3. OPMERKINGEN OVER HET STANDPUNT VAN DE RAAD

Algemeen bekrachtigt het standpunt van de Raad de hoofddoelen van het voorstel van de Commissie, namelijk het waarborgen van een hoog gemeenschappelijk niveau van netwerk- en informatiebeveiliging. De Raad brengt echter een aantal wijzigingen aan met betrekking tot de manier om dit doel te bereiken.

Nationale capaciteit voor cyberbeveiliging

Op grond van het standpunt van de Raad zullen de lidstaten een nationale NIB-strategie moeten vaststellen waarin de strategische doelstellingen en passende beleids- en regelgevingsmaatregelen voor cyberveiligheid worden omschreven. De lidstaten zullen ook een nationale bevoegde autoriteit moeten aanwijzen voor de uitvoering en de handhaving van de richtlijn, alsook Computer Security Incident Response Teams (CSIRT's) die verantwoordelijk zijn voor de behandeling van incidenten en risico's.

Hoewel de lidstaten op grond van het standpunt van de Raad geen nationaal NIB-samenwerkingsplan hoeven vast te stellen, zoals gepland in het oorspronkelijke voorstel, kan het standpunt worden gesteund omdat sommige aspecten van het samenwerkingsplan behouden zijn in de bepaling inzake de NIB-strategie.

Samenwerking tussen de lidstaten

Op grond van het standpunt van de Raad zal de richtlijn een "samenwerkingsgroep" instellen die bestaat uit vertegenwoordigers van de lidstaten, de Commissie en het Agentschap van de Europese Unie voor netwerk- en informatiebeveiliging (ENISA), teneinde strategische samenwerking en de uitwisseling van informatie tussen de lidstaten te ondersteunen en te faciliteren. De richtlijn zal ook een netwerk van Computer Security Incident Response Teams instellen, dat als het CSIRT's-netwerk bekend zal staan, om snelle en doeltreffende operationele samenwerking inzake specifieke cyberveiligheidsincidenten en de uitwisseling van informatie over risico's te bevorderen.

Hoewel dit in wezen verschilt van de benadering die in het oorspronkelijke voorstel werd gevolgd, kan het standpunt van de Raad worden gesteund omdat het algemeen in de lijn ligt van het doel de samenwerking tussen de lidstaten te verbeteren.

Beveiliging- en meldingseisen voor aanbieders van essentiële diensten

Op grond van het standpunt van de Raad zullen "aanbieders van essentiële diensten" (wat gelijkstaat met de "exploitanten van kritieke infrastructuur" in het oorspronkelijke voorstel) passende beveiligingsmaatregelen moeten nemen en ernstige incidenten aan de bevoegde nationale autoriteit moeten melden. De Raad was echter geen voorstander van een verplichting voor de nationale bevoegde autoriteiten om incidenten van criminele aard te melden aan de wetshandhavingsinstanties.

Net als het oorspronkelijke voorstel heeft het standpunt van de Raad betrekking op aanbieders in de sectoren energie, vervoer, het bankwezen, infrastructuur voor de financiële markt en gezondheidszorg. De standpunt van de Raad omvat echter ook de sectoren levering en distributie van drinkwater en digitale infrastructuur.

De lidstaten zullen die aanbieders moeten identificeren aan de hand van bepaalde criteria, bijvoorbeeld of de dienst essentieel is voor de instandhouding van kritieke maatschappelijke en economische activiteiten. Hoewel dit identificatieproces geen deel uitmaakte van het oorspronkelijke voorstel, kan het worden aanvaard, omdat de lidstaten aan de Commissie de informatie moeten verstrekken die nodig is om na te gaan of de lidstaten een consistente benadering volgen om de aanbieders van essentiële diensten te identificeren.

Overheden als zodanig zijn niet in het standpunt van de Raad opgenomen. Als zij aan de in artikel 5 vastgestelde criteria voldoen, zullen zij echter door de lidstaten als een aanbieder van essentiële diensten moeten worden aangewezen, omdat aanbieders van essentiële diensten publieke of private entiteiten kunnen zijn.

Beveiligings- en meldingeisen voor digitaledienstverleners

Op grond van het standpunt van de Raad zullen de lidstaten ervoor moeten zorgen dat digitaledienstverleners passende beveiligingsmaatregelen nemen en incidenten aan de bevoegde autoriteit melden. Het standpunt van de Raad betreft onlinemarktplaatsen (gelijkwaardig met de platforms voor elektronische handel in het oorspronkelijke voorstel), cloudcomputerdiensten en zoekmachines. In vergelijking met het oorspronkelijke voorstel omvat het standpunt van de Raad niet het volgende:

- gateways voor internetbetalingen - die vallen nu onder de herziene richtlijn betalingsdiensten;
- applicatiewinkels - die moeten als een soort onlinemarktplaats worden beschouwd;
- sociale netwerken - zoals in het politieke akkoord van de Raad met het Europees Parlement.

Op grond van het standpunt van de Raad worden aan de Commissie uitvoeringsbevoegdheden toegekend om de procedurele regelingen vast te stellen die noodzakelijk zijn voor de werking van de samenwerkingsgroep, en om de beveiligings- en meldingseisen die van toepassing zijn op digitaledienstverleners, verder te specificeren, waaronder de formats en de procedures voor de meldingseisen voor digitaledienstverleners.

De Commissie steunt de bovenvermelde uitkomsten.

Na de informele tripartiete besprekingen op 14 oktober 2014, 11 november 2014, 30 april 2015, 29 juni 2015, 17 november 2015 en 7 december 2015 hebben het Parlement en de Raad een voorlopig politiek akkoord over de tekst bereikt.

De Raad heeft dit politieke akkoord op 18 december 2015 bevestigd. Op 17 mei 2016 heeft de Raad zijn standpunt in eerste lezing vastgesteld.

4. CONCLUSIE

De Commissie staat achter de resultaten van de interinstitutionele onderhandelingen en kan bijgevolg het standpunt van de Raad in eerste lezing aanvaarden.