Raad van de
Europese Unie

Brussel, 21 april 2016
(OR. en)

5581/16
ADD 1

Interinstitutioneel dossier:
2013/0027 (COD)

TELECOM 7
DATAPROTECT 6
CYBER 4
MI 37
CSC 15
CODEC 84

ONTWERP-MOTIVERING VAN DE RAAD

Betreft:	Standpunt van de Raad in eerste lezing met het oog op de vaststelling van een RICHTLIJN VAN HET EUROPEES PARLEMENT EN DE RAAD houdende maatregelen voor een hoog gemeenschappelijk niveau van netwerk- en informatiebeveiliging in de Unie – Ontwerpmotivering van de Raad

I. INLEIDING

1. De Commissie heeft haar voorstel voor 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* (hierna "de richtlijn") op 12 februari 2013 ingediend met artikel 114 VWEU als rechtsgrond.

2. Het Europees Economisch en Sociaal Comité heeft op 22 mei 2013 advies uitgebracht en het Comité van de Regio's op 3-4 juli 2013.

3. Het Europees Parlement heeft op 13 maart 2014[1] in eerste lezing over zijn wetgevingsresolutie gestemd en heeft 138 amendementen aangenomen.

4. De Raad en het Europees Parlement zijn in oktober 2014 onderhandelingen aangegaan om tot een akkoord in vervroegde tweede lezing te komen. De onderhandelingen werden op 7 december 2015 met succes afgerond toen het Europees Parlement en de Raad een voorlopig akkoord over een compromistekst bereikten.

5. Op 18 december 2015 heeft het Comité van permanente vertegenwoordigers de compromistekst van de richtlijn, zoals die door de twee instellingen is overeengekomen, bevestigd.

6. De voorzitter van de Commissie IMCO van het Europees Parlement heeft op 28 januari 2016 in een brief aan de voorzitter van het Comité van permanente vertegenwoordigers laten weten dat zij, indien de Raad zijn aldus overeengekomen en door de juristen-vertalers bijgewerkte standpunt formeel aan het Europees Parlement doet toekomen, de plenaire vergadering zal aanbevelen het standpunt van de Raad tijdens de tweede lezing van het Parlement zonder amendementen te aanvaarden.

7. Op 29 februari 2016 heeft de Raad zijn politiek akkoord over de compromistekst van de richtlijn bevestigd.

---

[1] Wetgevingsresolutie van het Europees Parlement van 13 maart 2014 over het voorstel voor een richtlijn van het Europees Parlement en de Raad houdende maatregelen om een hoog gemeenschappelijk niveau van netwerk- en informatiebeveiliging (NIB) in de Unie te waarborgen.

II. DOELSTELLING

8. Uit het resultaat van de onderhandelingen blijkt dat deze richtlijn maatregelen bevat die moeten leiden tot een hoog gemeenschappelijk niveau van beveiliging van netwerken en informatiesystemen in de Europese Unie, teneinde de werking van de interne markt te verbeteren.

III. ANALYSE VAN HET STANDPUNT VAN DE RAAD IN EERSTE LEZING

A. Algemeen

9. Na de stemming in de plenaire vergadering hebben het Europees Parlement en de Raad onderhandelingen gevoerd met als doel een akkoord in tweede lezing te sluiten op basis van een standpunt van de Raad in eerste lezing dat het Parlement ongewijzigd kan goedkeuren. In de tekst van het standpunt van de Raad in eerste lezing komt het tussen de medewetgevers bereikte compromis volledig tot uiting.

B. Belangrijkste punten

10. De belangrijkste elementen van het met het Europees Parlement bereikte compromis worden hieronder toegelicht:

a. *Nationale capaciteiten*

11. Overeenkomstig het compromis hebben de lidstaten bepaalde verplichtingen met betrekking tot hun nationale cyberbeveiligingscapaciteiten. Allereerst moeten zij een nationale strategie vaststellen waarin de strategische doelstellingen en passende beleids- en regelgevingsmaatregelen worden omschreven, met het oog op het bereiken en behouden van een hoog niveau van beveiliging van netwerken en informatiesystemen.

12. Ten tweede wijzen zij een of meer nationale bevoegde autoriteiten voor de beveiliging van netwerk- en informatiesystemen aan om toezicht te houden op de toepassing van de richtlijn op nationaal niveau.

13. Ten derde wijzen zij een nationaal centraal contactpunt voor de beveiliging van netwerken en informatiesystemen aan dat een verbindingsfunctie vervult en moet zorgen voor grensoverschrijdende samenwerking van hun autoriteiten met de betrokken autoriteiten in andere lidstaten en met de samenwerkingsgroep en het CSIRT-netwerk. Het centraal contactpunt zal ook jaarlijks bij de samenwerkingsgroep een verslag indienen over ontvangen meldingen.

14. Ten slotte wijzen de lidstaten een of meer "Computer Security Incident Response Teams" (CSIRT's) aan die verantwoordelijk zijn voor de behandeling van incidenten en risico's. In bijlage I van de compromistekst worden vereisten en taken voor de CSIRT's vermeld.

b. *Samenwerking*

15. Om de strategische samenwerking tussen de lidstaten te ondersteunen en te faciliteren, vertrouwen te scheppen en een hoog gemeenschappelijk niveau van beveiliging van netwerken en informatiesystemen in de Unie tot stand te brengen, wordt in de compromistekst een samenwerkingsgroep ingesteld. De groep zal bestaan uit vertegenwoordigers van de lidstaten, de Commissie en het Agentschap van de Europese Unie voor netwerk- en informatiebeveiliging (het Enisa) en zal de in de tekst genoemde specifieke taken hebben, zoals het uitwisselen van beste praktijken en informatie over een aantal kwesties of het bespreken van de capaciteiten en paraatheid van de lidstaten.

16. Voorts beoogt het compromis de instelling van een netwerk van nationale CSIRT's, dat vertrouwen tussen de lidstaten moet helpen te creëren en mede snelle en doeltreffende operationele samenwerking moet bevorderen.Het netwerk zal bestaan uit vertegenwoordigers van de CSIRT's van de lidstaten en het EU-CERT; de Commissie zal als waarnemer aan het netwerk deelnemen. Het Enisa verzorgt het secretariaat en zorgt voor actieve ondersteuning van de samenwerking tussen de CSIRT's. In de tekst wordt een aantal taken opgesomd die moeten worden uitgevoerd door het netwerk, zoals het uitwisselen van informatie over de diensten, de activiteiten en de samenwerkings-capaciteit van de CSIRT's, het ondersteunen van de lidstaten bij het aanpakken van grensoverschrijdende incidenten of, onder bepaalde voorwaarden, het uitwisselen en bespreken van informatie in verband met incidenten en de daaraan verbonden risico's.

c. *Beveiligings- en meldingsvereisten*

17. In de richtlijn worden bepaalde verplichtingen vastgelegd voor de twee categorieën marktdeelnemers, nl. aanbieders van essentiële diensten en digitaledienstverleners.

18. Bijlage II bij de richtlijn bevat een opsomming van een aantal sectoren die van belang zijn voor de samenleving en de economie, te weten energie, vervoer, het bankwezen, infrastructuur voor de financiële markt, gezondheidszorg, drinkwatervoorziening en -distributie en digitale infrastructuur. Binnen deze sectoren zullen de lidstaten aan de hand van nauwkeurige, in de richtlijn vastgelegde, criteria bepalen welke exploitanten essentiële diensten verrichten.

19. Bijlage III bij de richtlijn vermeldt drie soorten digitale diensten waarvan de aanbieders zullen moeten voldoen aan de vereisten van de richtlijn: onlinemarktplaatsen, online-zoekmachines en cloudcomputingdiensten. Alle digitaledienstverleners die de genoemde diensten aanbieden, moeten voldoen aan de vereisten van de richtlijn, met uitzondering van micro- en kleine ondernemingen.

20. De twee soorten marktdeelnemers moeten organisatorische en technische maatregelen nemen om de risico's voor de beveiliging van netwerken en informatiesystemen te beheersen en de gevolgen van incidenten die van invloed zijn op de beveiliging van de systemen te voorkomen en zo veel mogelijk te beperken. Bovendien moeten incidenten met een zekere mate van invloed op de betrokken diensten gemeld worden aan de nationale bevoegde autoriteiten of de CSIRT's. De richtlijn geeft criteria voor het bepalen van de mate van invloed van dergelijke incidenten.

21. In de richtlijn is gekozen voor een gedifferentieerde aanpak met betrekking tot de twee categorieën marktdeelnemers. De vereisten inzake beveiliging en melding zijn lichter voor digitaledienstverleners dan voor exploitanten van essentiële diensten, hetgeen overeenstemt met het risiconiveau van verstoring van de dienstverlening voor de samenleving en de economie. Voorts zorgt de richtlijn ervoor, gelet op het feit dat aanbieders van digitale diensten vaak in veel lidstaten actief zijn, en met het oog op het garanderen van een hoge mate van harmonisatie, dat lidstaten geen extra beveiligings- en meldingseisen kunnen stellen aan deze aanbieders.

22. De compromistekst bepaalt dat entiteiten die niet als exploitanten van essentiële diensten zijn aangemerkt en die geen digitaledienstverleners zijn, bepaalde incidenten op vrijwillige basis kunnen melden.

d. *Omzetting*

23. De lidstaten moeten de richtlijn omzetten binnen een termijn van 21 maanden na de datum van inwerkingtreding, en beschikken over nog eens zes maanden om te bepalen welke hun exploitanten van essentiële diensten zijn.

IV. CONCLUSIE

24. In het standpunt van de Raad komt het compromis dat is bereikt in de onderhandelingen tussen het Europees Parlement en de Raad, met de goedkeuring van de Commissie, volledig tot uiting. Dit compromis is bevestigd door de brief van 28 januari 2016 van de voorzitter van de Commissie IMCO aan de voorzitter van het Comité van permanente vertegenwoordigers.