Rada
Európskej únie

V Bruseli 21. apríla 2016
(OR. en)

Medziinštitucionálny spis:
2013/0027 (COD)

5581/16
ADD 1

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

NÁVRH ODÔVODNENÉHO STANOVISKA RADY

Predmet:	Pozícia Rady v prvom čítaní na účely prijatia SMERNICE EURÓPSKEHO PARLAMENTU A RADY o opatreniach na zaistenie vysokej spoločnej úrovne bezpečnosti sieťových a informačných systémov v celej Únii – návrh odôvodneného stanoviska Rady

I. ÚVOD

1. Komisia 12. februára 2013 predložila návrh smernice Európskeho parlamentu a Rady o opatreniach na zabezpečenie vysokej úrovne bezpečnosti sietí a informácií v Únii (ďalej len „smernica“), ktorého právnym základom je článok 114 ZFEÚ.

2. Európsky hospodársky a sociálny výbor odhlasoval svoje stanovisko 22. mája 2013 a Výbor regiónov odhlasoval svoje stanovisko 3. – 4. júla 2013.

3. Európsky parlament hlasoval o svojom legislatívnom uznesení v prvom čítaní 13. marca 2014[1], pričom prijal 138 pozmeňujúcich návrhov.

4. Rada a Európsky parlament začali v októbri 2014 rokovania s cieľom dosiahnuť skorú dohodu v druhom čítaní. Rokovania sa úspešne ukončili 7. decembra 2015, pričom Európsky parlament a Rada dosiahli predbežnú dohodu o kompromisnom znení.

5. Výbor stálych predstaviteľov 18. decembra 2015 potvrdil kompromisné znenie smernice, na ktorom sa dohodli tieto dve inštitúcie.

6. Predsedníčka Výboru Európskeho parlamentu pre vnútorný trh a ochranu spotrebiteľa (IMCO) zaslala 28. januára 2016 predsedovi Výboru stálych predstaviteľov list, v ktorom uviedla, že ak Rada formálne zašle Európskemu parlamentu svoju pozíciu v dohodnutom znení, s výhradou revízie právnikov lingvistov odporučí plénu, aby v druhom čítaní Parlamentu akceptovalo pozíciu Rady bez pozmeňujúcich návrhov.

7. Rada 29. februára 2016 potvrdila svoju politickú dohodu o kompromisnom znení smernice.

[1] Legislatívne uznesenie Európskeho parlamentu z 13. marca 2014 k návrhu smernice Európskeho parlamentu a Rady o opatreniach na zabezpečenie vysokej úrovne bezpečnosti sietí a informácií v Únii.

II. CIEĽ

8. Z výsledku rokovaní vyplýva, že touto smernicou sa stanovujú opatrenia na dosiahnutie vysokej spoločnej úrovne bezpečnosti sieťových a informačných systémov v Európskej únii s cieľom zlepšiť fungovanie vnútorného trhu.

III. ANALÝZA POZÍCIE RADY V PRVOM ČÍTANÍ

A. Všeobecne

9. Po hlasovaní v pléne sa uskutočnili rokovania Európskeho parlamentu a Rady s cieľom uzavrieť dohodu v druhom čítaní na základe pozície Rady v prvom čítaní, ktorú by Parlament mohol schváliť. V znení pozície Rady v prvom čítaní sa v plnej miere odzrkadľuje kompromis, ktorý dosiahli spoluzákonodarcovia.

B. Hlavné otázky

10. Hlavné prvky kompromisu dosiahnutého s Európskym parlamentom sú tieto:

a. Vnútroštátne spôsobilosti

11. Podľa kompromisu majú členské štáty určité povinnosti vo vzťahu k svojim vnútroštátnym spôsobilostiam v oblasti kybernetickej bezpečnosti. Po prvé, členské štáty sú povinné prijať národnú stratégiu, v ktorej sa vymedzia strategické ciele a vhodné politické a regulačné opatrenia na dosiahnutie a udržanie vysokej úrovne bezpečnosti sieťových a informačných systémov.

12. Po druhé, členské štáty určia jeden alebo viaceré vnútroštátne príslušné orgány pre bezpečnosť sieťových a informačných systémov, ktoré budú monitorovať uplatňovanie smernice na vnútroštátnej úrovni.

13. Po tretie, členské štáty sú taktiež povinné určiť vnútroštátne jednotné kontaktné miesto pre bezpečnosť sieťových a informačných systémov, ktoré bude plniť styčnú úlohu, aby zabezpečilo cezhraničnú spoluprácu orgánov členských štátov s príslušnými orgánmi v iných členských štátoch, so skupinou pre spoluprácu a sieťou jednotiek CSIRT. Jednotné kontaktné miesto bude tiež skupine pre spoluprácu predkladať výročnú správu o oznámeniach, ktoré dostane.

14. Napokon, členské štáty určia jednu alebo viacero jednotiek pre riešenie počítačových incidentov (CSIRT), ktoré budú zodpovedné za riešenie incidentov a rizík. Požiadavky na CSIRT a ich úlohy sa ustanovujú v prílohe I ku kompromisnému zneniu.

b. Spolupráca

15. S cieľom podporiť a uľahčiť strategickú spoluprácu medzi členskými štátmi, rozvíjať dôveru a dosiahnuť vysokú spoločnú úroveň bezpečnosti sieťových a informačných systémov v Únii sa v kompromisnom znení zriaďuje skupina pre spoluprácu. Táto skupina sa bude skladať zo zástupcov členských štátov, Komisie a Agentúry Európskej únie pre sieťovú a informačnú bezpečnosť (ENISA) a bude mať osobitné úlohy uvedené v znení, ako je napríklad výmena najlepších postupov a informácií o určitých oblastiach alebo prerokúvanie spôsobilostí a pripravenosti členských štátov.

16. Okrem toho sa v kompromisnom znení ustanovuje sieť vnútroštátnych jednotiek CSIRT s cieľom prispieť k rozvoju dôvery medzi členskými štátmi a presadzovať rýchlu a účinnú operačnú spoluprácu. Táto sieť sa bude skladať zo zástupcov jednotiek CSIRT členských štátov a jednotky CERT-EU, pričom Komisia sa bude zúčastňovať na činnosti siete ako pozorovateľ. Agentúra ENISA bude zabezpečovať sekretariát a aktívne podporovať spoluprácu medzi jednotkami CSIRT. V znení sa ustanovuje zoznam úloh siete, ako je napríklad výmena informácií o službách, operáciách a kooperačných spôsobilostiach jednotiek CSIRT, podpora členských štátov pri riešení cezhraničných incidentov či za určitých podmienok aj výmena a prediskutovanie informácií o incidentoch a súvisiacich rizikách.

c. *Bezpečnostné požiadavky a požiadavky na oznamovanie*

17. V smernici sa stanovujú určité povinnosti pre dve skupiny účastníkov trhu: prevádzkovatelia základných služieb a poskytovatelia digitálnych služieb.

18. V prílohe II k smernici sa uvádza niekoľko dôležitých odvetví pre spoločnosť a hospodárstvo, a to energetika, doprava, bankovníctvo, infraštruktúry finančných trhov, zdravotníctvo, dodávka a distribúcia pitnej vody a digitálna infraštruktúra. Členské štáty identifikujú v rámci týchto odvetví na základe presných kritérií stanovených v smernici prevádzkovateľov základných služieb.

19. V prílohe III k smernici sa uvádzajú tri druhy digitálnych služieb, ktorých poskytovatelia budú musieť spĺňať požiadavky smernice: online trhy, internetové vyhľadávače a služby cloud computingu. Požiadavky smernice budú musieť spĺňať všetci poskytovatelia uvedených digitálnych služieb s výnimkou mikropodnikov a malých podnikov.

20. Uvedené dve skupiny účastníkov trhu budú musieť prijať organizačné a technické opatrenia na riadenie rizík spojených s bezpečnosťou sieťových a informačných systémov a na prevenciu a minimalizovanie vplyvu incidentov ovplyvňujúcich bezpečnosť týchto systémov. Okrem toho incidenty, ktoré majú určitý stupeň vplyvu na dané služby, sa budú musieť oznámiť príslušným vnútroštátnym orgánom alebo jednotkám CSIRT. V smernici sa stanovujú kritériá na určenie stupňa vplyvu takýchto incidentov.

21. V smernici sa uplatňuje diferencovaný prístup vo vzťahu k uvedeným dvom kategóriám účastníkov trhu. Bezpečnostné a oznamovacie požiadavky na poskytovateľov digitálnych služieb sú nižšie ako na poskytovateľov základných služieb, čo je odrazom stupňa rizika, ktoré môže pri narušení ich služieb vzniknúť pre spoločnosť a hospodárstvo. Okrem toho vzhľadom na to, že poskytovatelia digitálnych služieb často pôsobia v mnohých členských štátoch, a s cieľom zabezpečiť vysokú mieru harmonizácie smernica bráni členským štátom v tom, aby týmto poskytovateľom ukladali ďalšie bezpečnostné a oznamovacie požiadavky.

22. V kompromisnom znení sa tiež ustanovuje, že subjekty, ktoré sa neidentifikovali ako prevádzkovatelia základných služieb a ktoré nie sú poskytovateľmi digitálnych služieb, môžu oznamovať určité incidenty na dobrovoľnom základe.

d. *Transpozícia*

23. Členské štáty budú musieť transponovať smernicu do 21 mesiacov od nadobudnutia jej účinnosti, pričom budú mať ďalších 6 mesiacov na identifikáciu svojich prevádzkovateľov základných služieb.

IV. ZÁVER

24. V pozícii Rady sa plne zohľadňuje kompromis, ktorý sa dosiahol počas rokovaní medzi Európskym parlamentom a Radou so súhlasom Komisie. Kompromis potvrdila predsedníčka výboru IMCO v liste predsedovi Výboru stálych predstaviteľov z 28. januára 2016.