Rada
Unii Europejskiej

Bruksela, 17 maja 2016 r.
(OR. en)

Międzyinstytucjonalny numer referencyjny:
2013/0027 (COD)

5581/1/16
REV 1 ADD 1

TELECOM 7
DATAPROTECT 6
CYBER 4
MI 37
CSC 15
CODEC 84
PARLNAT 154

UZASADNIENIE RADY

Dotyczy:	Stanowisko Rady w pierwszym czytaniu w celu przyjęcia DYREKTYWY PARLAMENTU EUROPEJSKIEGO I RADY w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii – Uzasadnienie Rady – Przyjęte przez Radę w dniu 17 maja 2016 r.

I. WPROWADZENIE

1. W dniu 12 lutego 2013 r. Komisja przedłożyła wniosek dotyczący dyrektywy Parlamentu Europejskiego i Rady w sprawie *środków mających na celu zapewnienie wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji w obrębie Unii* (zwanej dalej „dyrektywą"), przy czym podstawą prawną tego aktu jest art. 114 TFUE.

2. Europejski Komitet Ekonomiczno-Społeczny głosował nad swoją opinią w dniu 22 maja 2013 r., a Komitet Regionów – w dniach 3–4 stycznia 2013 r.

3. Parlament Europejski głosował nad rezolucją ustawodawczą w pierwszym czytaniu w dniu 13 marca 2014 r.[1] i przyjął 138 poprawek.

4. W październiku 2014 r. Rada i Parlament Europejski rozpoczęły negocjacje z myślą o osiągnięciu wczesnego porozumienia w drugim czytaniu. Negocjacje zakończyły się pomyślnie w dniu 7 grudnia 2015 r. – Parlament Europejski i Rada osiągnęły wstępne porozumienie co do tekstu kompromisowego.

5. W dniu 18 grudnia 2015 r. Komitet Stałych Przedstawicieli potwierdził kompromisowy tekst dyrektywy w wersji uzgodnionej przez obie instytucje.

6. W dniu 28 stycznia 2016 r. przewodnicząca parlamentarnej Komisji Rynku Wewnętrznego i Ochrony Konsumentów (IMCO) wysłała pismo do przewodniczącego Komitetu Stałych Przedstawicieli, w którym oświadczyła, że w przypadku gdy Rada prześle formalnie Parlamentowi Europejskiemu swoje uzgodnione stanowisko w wersji zweryfikowanej przez prawników lingwistów, zaleci ona, aby na sesji plenarnej stanowisko Rady zostało przyjęte bez poprawek w drugim czytaniu Parlamentu.

7. W dniu 29 lutego 2016 r. Rada potwierdziła porozumienie polityczne co do kompromisowego tekstu dyrektywy.

---

[1] Rezolucja ustawodawcza Parlamentu Europejskiego z dnia 13 marca 2014 r. w sprawie wniosku dotyczącego dyrektywy Parlamentu Europejskiego i Rady w sprawie środków mających na celu zapewnienie wysokiego wspólnego poziomu bezpieczeństwa sieci i informacji w obrębie Unii.

II. CEL

8. Jak wynika z negocjacji, dyrektywa ustanawia środki mające na celu osiągnięcie wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych w obrębie Unii Europejskiej, tak aby poprawić funkcjonowanie rynku wewnętrznego.

III. ANALIZA STANOWISKA RADY W PIERWSZYM CZYTANIU

A. Uwagi ogólne

9. W następstwie głosowania na posiedzeniu plenarnym Parlament Europejski i Rada przeprowadziły negocjacje w celu zawarcia porozumienia w drugim czytaniu na podstawie stanowiska Rady w pierwszym czytaniu, które Parlament byłby w stanie zatwierdzić w jego brzmieniu. Tekst stanowiska Rady w pierwszym czytaniu w pełni odzwierciedla kompromis osiągnięty między tymi dwoma współprawodawcami.

B. Kluczowe kwestie

10. Główne elementy kompromisu osiągniętego z Parlamentem Europejskim przedstawiono poniżej:

a. *Krajowe zdolności*

11. Zgodnie z kompromisem państwa członkowskie mają pewne obowiązki w odniesieniu do swoich krajowych zdolności w zakresie bezpieczeństwa cybernetycznego. Po pierwsze, państwa członkowskie są zobowiązane przyjąć krajową strategię określającą strategiczne cele oraz odpowiednie środki polityczne i regulacyjne służące osiągnięciu i utrzymaniu wysokiego poziomu bezpieczeństwa sieci i systemów informatycznych.

12. Po drugie, państwa członkowskie wyznaczają co najmniej jeden właściwy organ krajowy ds. bezpieczeństwa sieci i systemów informatycznych mający monitorować wdrażanie dyrektywy na szczeblu krajowym.

13. Po trzecie, państwa członkowskie są także zobligowane do wyznaczenia pojedynczego punktu kontaktowego do spraw bezpieczeństwa sieci i systemów informatycznych, który będzie pełnił funkcję łącznikową w celu zapewnienia transgranicznej współpracy z organami państw członkowskich oraz z odpowiednimi organami w innych państwach członkowskich, a także z grupą współpracy i siecią CSIRT. Pojedynczy punkt kontaktowy będzie również przedkładać grupie współpracy roczne sprawozdanie dotyczące otrzymanych zgłoszeń.

14. Ponadto państwa członkowskie wyznaczają co najmniej jeden Zespół Reagowania na Incydenty związane z Bezpieczeństwem Komputerowym (CSIRT) odpowiedzialny za postępowanie w odniesieniu do incydentów i ryzyk. Tekst kompromisowy przewiduje wymogi i zadania CSIRT zawarte w załączniku I.

b. *Współpraca*

15. Aby wesprzeć i ułatwić strategiczną współpracę pomiędzy państwami członkowskimi w celu wzmocnienia zaufania i pewności oraz z myślą o osiągnięciu wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych w Unii, w tekście kompromisowym ustanawia się grupę współpracy. Grupa będzie się składać z przedstawicieli państw członkowskich, Komisji i Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA) i będzie miała konkretne zadania wymienione w tekście, takie jak wymiana najlepszych praktyk i informacji na temat szeregu kwestii lub omawianie zdolności i gotowości państw członkowskich.

16. Ponadto w tekście kompromisowym ustanawia się sieć krajowych CSIRT w celu przyczyniania się do rozwoju pewności i zaufania między państwami członkowskimi oraz w celu propagowania szybkiej i skutecznej współpracy. W skład sieci wchodzić będą przedstawiciele CSIRT państw członkowskich i CERT-UE, a Komisja będzie w niej uczestniczyć w roli obserwatora. ENISA będzie zapewniać sekretariat i aktywnie wspierać współpracę między CSIRT. Tekst zawiera wykaz zadań do wykonania przez sieć, takich jak wymiana informacji na temat usług, operacji i zdolności współpracy CSIRT, wspieranie państw członkowskich w zajmowaniu się incydentami transgranicznymi lub, pod pewnymi warunkami, wymiana i omawianie informacji związanych z incydentami i powiązanymi ryzykami.

c. *Wymogi dotyczące bezpieczeństwa i zgłaszania*

17. W dyrektywie ustanawia się pewne obowiązki dla dwóch grup podmiotów rynkowych: operatorów usług podstawowych i dostawców usług cyfrowych.

18. Załącznik II do dyrektywy wymienia w wykazie różne sektory istotne dla społeczeństwa i gospodarki, mianowicie sektory: energetyczny, transportowy, bankowy, infrastruktury rynków finansowych, opieki zdrowotnej, zaopatrzenia w wodę pitną i jej dystrybucji oraz infrastruktury cyfrowej. W obrębie tych sektorów państwa członkowskie wskażą operatorów usług podstawowych w oparciu o precyzyjne kryteria określone w dyrektywie.

19. Załącznik III do dyrektywy wymienia w wykazie trzy typy usług cyfrowych, których dostawcy będą musieli spełnić wymogi dyrektywy: internetowe platformy handlowe, wyszukiwarki internetowe oraz usługi przetwarzania w chmurze. Wszyscy dostawcy usług cyfrowych świadczący wymienione usługi będą musieli spełniać wymogi dyrektywy, z wyłączeniem mikroprzedsiębiorstw i małych przedsiębiorstw.

20. Obie grupy podmiotów rynkowych będą zobowiązane przyjmować środki organizacyjne i techniczne w celu zarządzania ryzykami, na jakie narażone jest bezpieczeństwo sieci i systemów informatycznych, oraz w celu minimalizowania wpływu incydentów związanych z bezpieczeństwem tych systemów. Ponadto incydenty, które charakteryzuje pewien poziom wpływu na odnośne usługi, będą musiały być zgłaszane do właściwych organów krajowych lub CSIRT. Dyrektywa zawiera kryteria określania poziomu wpływu takich incydentów.

21. Przyjęto w niej zróżnicowane podejście w odniesieniu do tych dwu kategorii podmiotów. Wymogi dotyczące bezpieczeństwa i zgłaszania są mniej restrykcyjne dla dostawców usług cyfrowych niż dla operatorów usług podstawowych, co odzwierciedla stopień ryzyka, jakie zakłócenie tych usług może stanowić dla społeczeństwa i gospodarki. Ponadto, biorąc pod uwagę, że dostawcy usług cyfrowych często są aktywni w wielu państwach członkowskich, oraz w celu zapewnienia wysokiego poziomu harmonizacji, dyrektywa uniemożliwia państwom członkowskim nakładanie na tych usługodawców dodatkowych wymogów dotyczących bezpieczeństwa i zgłaszania.

22. Tekst kompromisowy przewiduje również, że podmioty, które nie zostały wskazane jako operatorzy podstawowych usług i nie są dostawcami usług cyfrowych, mogą zgłaszać pewne incydenty na zasadzie dobrowolności.

d. *Transpozycja*

23. Państwa członkowskie będą musiały dokonać transpozycji dyrektywy w terminie 21 miesięcy od daty jej wejścia w życie i będą miały 6 dodatkowych miesięcy na wskazanie swoich operatorów usług podstawowych.

IV. PODSUMOWANIE

24. Stanowisko Rady w pełni odzwierciedla kompromis osiągnięty w negocjacjach między Parlamentem Europejskim a Radą, prowadzonych w porozumieniu z Komisją. Kompromis ten został potwierdzony pismem przewodniczącej parlamentarnej komisji IMCO do przewodniczącego Komitetu Stałych Przedstawicieli z dnia 28 stycznia 2016 r.