Rada
Unii Europejskiej

Bruksela, 31 maja 2016 r.
(OR. en)

9690/16

Międzyinstytucjonalny numer referencyjny:
2013/0027 (COD)

TELECOM 107
DATAPROTECT 58
CYBER 61
MI 401
CSC 166
CODEC 789

PISMO PRZEWODNIE

Od:	Sekretarz Generalny Komisji Europejskiej, podpisał dyrektor Jordi AYET PUIGARNAU
Data otrzymania:	30 maja 2016 r.
Do:	Jeppe TRANHOLM-MIKKELSEN, Sekretarz Generalny Rady Unii Europejskiej
Nr dok. Kom.:	COM(2016) 363 final
Dotyczy:	KOMUNIKAT KOMISJI DO PARLAMENTU EUROPEJSKIEGO na podstawie art. 294 ust. 6 Traktatu o funkcjonowaniu Unii Europejskiej dotyczący stanowiska Rady w sprawie przyjęcia dyrektywy Parlamentu Europejskiego i Rady w sprawie środków mających na celu zapewnienie wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji w obrębie Unii

Delegacje otrzymują w załączeniu dokument COM(2016) 363 final.

Zał.: COM(2016) 363 final

KOMISJA
EUROPEJSKA

Bruksela, dnia 30.5.2016 r.
COM(2016) 363 final

2013/0027 (COD)

KOMUNIKAT KOMISJI DO PARLAMENTU EUROPEJSKIEGO

na podstawie art. 294 ust. 6 Traktatu o funkcjonowaniu Unii Europejskiej

dotyczący

stanowiska Rady w sprawie przyjęcia dyrektywy Parlamentu Europejskiego i Rady w sprawie środków mających na celu zapewnienie wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji w obrębie Unii

(Tekst mający znaczenie dla EOG)

2013/0027 (COD)

KOMUNIKAT KOMISJI
DO PARLAMENTU EUROPEJSKIEGO

na podstawie art. 294 ust. 6 Traktatu o funkcjonowaniu Unii Europejskiej

dotyczący

stanowiska Rady w sprawie przyjęcia dyrektywy Parlamentu Europejskiego i Rady w sprawie środków mających na celu zapewnienie wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji w obrębie Unii

(Tekst mający znaczenie dla EOG)

1. PRZEBIEG PROCEDURY

Data przekazania wniosku Parlamentowi Europejskiemu i Radzie (COM(2013) 48 – 2013/0027/COD)	7.2.2013
Data wydania opinii przez Europejski Komitet Ekonomiczno-Społeczny:	22.5.2013
Data uchwalenia stanowiska Parlamentu Europejskiego w pierwszym czytaniu:	13.3.2014
Data przyjęcia stanowiska Rady:	17.5.2016

2. PRZEDMIOT WNIOSKU KOMISJI

Po pierwsze, wniosek zobowiązuje wszystkie państwa członkowskie do zagwarantowania minimalnego poziomu krajowych zdolności poprzez:

- ustanowienie właściwych organów ds. bezpieczeństwa sieci i informacji (BSI);
- powołanie zespołów reagowania na incydenty komputerowe (CERT)
- oraz przyjęcie krajowych strategii i planów współpracy w zakresie bezpieczeństwa sieci i informacji.

Po drugie, właściwe organy krajowe powinny współpracować w ramach sieci umożliwiającej bezpieczną i skuteczną koordynację, w tym skoordynowaną wymianę informacji, jak również wykrywanie i reagowanie na poziomie UE. Poprzez tę sieć państwa członkowskie powinny wymieniać się informacjami i współpracować ze sobą w celu zwalczania zagrożeń i incydentów w zakresie bezpieczeństwa sieci i informacji (BSI) na podstawie europejskiego planu współpracy w tej dziedzinie. Celem zapewnienia należytego i terminowego zaangażowania wszystkich zainteresowanych organów wniosek zobowiązuje je do zgłaszania

organom ścigania poważnych incydentów, które mogą mieć charakter przestępczy, jednocześnie przewidując zaangażowanie Europolu w ramach ogólnounijnego mechanizmu koordynacji.

Po trzecie, opierając się na modelu, jakim jest dyrektywa ramowa w sprawie łączności elektronicznej, wniosek ma na celu zapewnienie rozwoju kultury wspierającej przeciwdziałanie zagrożeniom oraz wymiany informacji między sektorem prywatnym i publicznym. Przedsiębiorstwa w określonych krytycznych sektorach oraz organy administracji publicznej będą zobowiązane do dokonania oceny zagrożeń, na jakie są narażone, oraz do przyjęcia odpowiednich i proporcjonalnych środków mających na celu zapewnienie bezpieczeństwa sieci i informacji. Będą one zobowiązane do zgłaszania właściwym organom wszelkich incydentów poważnie zagrażających ich sieciom i systemom informatycznym oraz mogących znacząco zakłócić ciągłość krytycznych usług i dostaw towarów.

3. UWAGI DOTYCZĄCE STANOWISKA RADY

Stanowisko Rady jest zasadniczo zgodne z głównymi celami wniosku Komisji, który zmierza do zapewnienia wspólnego wysokiego poziomu bezpieczeństwa sieci i systemów informatycznych. Rada wprowadza jednak pewne zmiany co do sposobu osiągnięcia tego celu.

Krajowe zdolności w zakresie bezpieczeństwa cybernetycznego

Zgodnie ze stanowiskiem Rady państwa członkowskie będą zobowiązane do uchwalenia krajowych strategii BSI, określających strategiczne cele i odpowiednie założenia polityki wraz ze środkami regulacyjnymi w dziedzinie bezpieczeństwa cybernetycznego. Państwa członkowskie będą również zobowiązane do wyznaczenia właściwych organów krajowych odpowiedzialnych za wdrażanie i egzekwowanie przepisów dyrektywy, jak również do powołania zespołów reagowania na incydenty komputerowe (CERT) odpowiedzialnych za reagowanie w przypadku wystąpienia incydentów i zagrożeń.

Stanowisko Rady nie wymaga wprawdzie uzgodnienia przez każde państwo członkowskie krajowego planu współpracy w zakresie bezpieczeństwa sieci i informacji (BSI), jak przewidziano w pierwotnym wniosku, stanowisko to można poprzeć, jako że pewne aspekty planu współpracy zachowano w przepisach dotyczących strategii BSI.

Współpraca pomiędzy państwami członkowskimi

W myśl stanowiska Rady, na mocy dyrektywy powstanie grupa współpracy, złożona z przedstawicieli państw członkowskich, Komisji i Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji („ENISA"), służąca wspieraniu i ułatwianiu współpracy strategicznej między państwami członkowskimi w zakresie bezpieczeństwa sieci i informacji. Dyrektywa ma również być podstawą dla utworzenia zespołów reagowania na incydenty komputerowe (CERT), współdziałających jako sieć CERT, aby zapewnić szybką i skuteczną współpracę operacyjną w przypadku wystąpienia incydentów w sferze cyberbezpieczeństwa i wymianę informacji o zagrożeniach.

Jakkolwiek w znacznym stopniu odmienne od koncepcji przyjętej w pierwotnym wniosku, stanowisko Rady można poprzeć, jako wpisujące się ogólnie w dążenie do poprawy współpracy między państwami członkowskimi.

Wymogi dotyczące bezpieczeństwa i zgłaszania incydentów dla operatorów usług podstawowych

Zgodnie ze stanowiskiem Rady przewidywanych pierwotnie „najważniejszych dostawców internetu“ mają zastąpić „operatorzy usług podstawowych”, których obowiązkiem ma być podejmowanie odpowiednich działań mających na celu przeciwdziałanie zagrożeniom bezpieczeństwa oraz zgłaszanie poważnych incydentów właściwym organom krajowym. Rada nie poparła jednak proponowanego nałożenia na właściwe organy krajowe obowiązku zgłaszania organom ścigania poważnych incydentów, które mogą mieć charakter przestępczy.

W zgodzie z pierwotnym wnioskiem stanowisko Rady obejmuje analogicznych operatorów w sektorach energetyki, transportu, bankowości, infrastruktury rynków finansowych i opieki zdrowotnej. Rada postanowiła jednak w swym stanowisku uwzględnić również sektor wodny i infrastruktury cyfrowej.

Obowiązkiem państw członkowskich ma być wskazanie takich operatorów na podstawie określonych kryteriów, na przykład w zależności od tego, czy dana usługa ma podstawowe znaczenie dla utrzymania istotnych funkcji gospodarczych bądź społecznych. Proces wskazywania operatorów, jakkolwiek nieuwzględniony w pierwotnym wniosku, może być zaakceptowany, zważywszy na spoczywający na państwach członkowskich obowiązek przedkładania Komisji informacji niezbędnych dla oceny spójności metod stosowanych przez państwa członkowskie w celu wyznaczenia operatorów usług podstawowych.

Organy administracji publicznej jako takie nie są ujęte w stanowisku Rady. Gdyby jednak spełniały one kryteria wyszczególnione w art. 5, powinny być traktowane przez państwa członkowskie jako operatorzy usług podstawowych, skoro operatorem usług podstawowych może być zarówno podmiot prywatny, jak i publiczny.

Wymogi dotyczące bezpieczeństwa i zgłaszania incydentów dla operatorów usług cyfrowych

W świetle stanowiska Rady państwa członkowskie będą musiały zagwarantować, że operatorzy usług cyfrowych podejmują odpowiednie działania mające na celu przeciwdziałanie zagrożeniom bezpieczeństwa oraz zgłaszają poważne incydenty właściwym organom krajowym. W stanowisku Rady uwzględniono rynki online (odpowiadające platformom handlu elektronicznego z pierwotnego wniosku), usługi przetwarzania w chmurze obliczeniowej i wyszukiwarki internetowe. W stosunku do pierwotnego wniosku stanowisko Rady pomija:

- internetowe portale płatnicze, obecnie uregulowane zmienioną dyrektywą w sprawie usług płatniczych;
- sklepy z aplikacjami – które należy definiować jako rodzaj rynków online;
- portale społecznościowe – zgodnie z porozumieniem politycznym osiągniętym przez Parlament Europejski i Radę.

Zgodnie ze stanowiskiem Rady Komisji powierza się uprawnienia wykonawcze w celu określenia procedur niezbędnych do funkcjonowania grupy współpracy, jak również w celu doprecyzowania pewnych elementów dotyczących operatorów usług cyfrowych, w tym formatów i procedur mających zastosowanie do obowiązków operatorów usług cyfrowych w zakresie informowania.

Komisja popiera powyższe rozstrzygnięcia.

W wyniku nieformalnych rozmów trójstronnych w dniach 14 października 2014 r., 11 listopada 2014 r., 30 kwietnia 2015 r., 29 czerwca 2015 r., 17 listopada 2015 r. i 7 grudnia 2015 r. Parlament i Rada osiągnęły tymczasowe porozumienie polityczne w sprawie brzmienia tekstu.

Osiągnięte porozumienie polityczne zostało potwierdzone przez Radę w dniu 18 grudnia 2015 r. W dniu 17 maja 2016 r. Rada przyjęła stanowisko w pierwszym czytaniu.

4. PODSUMOWANIE

Komisja popiera wyniki negocjacji międzyinstytucjonalnych i może zatem przyjąć stanowisko Rady w pierwszym czytaniu.