I

(Rezolucje, zalecenia i opinie)

REZOLUCJE

RADA

REZOLUCJA RADY

z dnia 18 grudnia 2009 r.

w sprawie wspólnego europejskiego podejścia do bezpieczeństwa sieci i informacji

(2009/C 321/01)

RADA UNII EUROPEJSKIEJ,

I. MAJĄC NA UWADZE:

1. Komunikat Komisji z dnia 31 maja 2006 r. „Strategia na rzecz bezpiecznego społeczeństwa informacyjnego" przedstawiający proces „dialogu, partnerstwa i przejmowania inicjatywy" z udziałem państw członkowskich i zainteresowanych podmiotów z sektora prywatnego;

2. Komunikat Komisji z dnia 12 grudnia 2006 r. w sprawie europejskiego programu ochrony infrastruktury krytycznej mający na celu poprawę ochrony takiej infrastruktury w UE oraz tworzący ramy regulacyjne dotyczące ochrony infrastruktury krytycznej;

3. Dyrektywę Rady z dnia 8 grudnia 2008 r. w sprawie rozpoznania i wyznaczenia europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie zwiększenia jej ochrony;

4. Rezolucję Rady z dnia 22 marca 2007 r. w sprawie strategii na rzecz bezpiecznego społeczeństwa informacyjnego w Europie;

5. Konkluzje Rady Europejskiej z dni 19–20 kwietnia 2007 r. w sprawie europejskiego programu ochrony infrastruktury krytycznej;

6. Komunikat Komisji z dnia 30 marca 2009 r. w sprawie ochrony krytycznej infrastruktury informatycznej;

7. Toczącą się debatę, w tym odpowiednie konsultacje publiczne, w sprawie przyszłości Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji (ENISA) oraz jej roli w zakresie ochrony krytycznej infrastruktury informatycznej;

8. Konkluzje prezydencji w sprawie ochrony krytycznej infrastruktury informatycznej z konferencji ministerialnej w Tallinie w dniach 27–28 kwietnia 2009 r.;

9. Cele strategii lizbońskiej dotyczące konkurencyjności i wzrostu gospodarczego oraz prowadzone obecnie prace odnoszące się do przeglądu tej strategii;

10. Środki bezpieczeństwa zaproponowane w procesie przeglądu ram regulacyjnych sieci i usług łączności elektronicznej;

11. Ze względu na efektywność przyszłej polityki w zakresie bezpieczeństwa sieci i informacji w niniejszej rezolucji zakłada się, iż nie ma jeszcze żadnych ustaleń dotyczących jakichkolwiek niezbędnych zmian rozporządzenia w sprawie agencji ENISA. Ponieważ Komisja zajmuje się obecnie przyszłością polityki bezpieczeństwa sieci i informacji, niniejsza rezolucja nie powinna wpływać na wyniki tego przeglądu, odnoszące się do wszelkich zmian rozporządzenia w sprawie agencji ENISA, przed ich opublikowaniem przez Komisję.

II. ODNOTOWUJĄC, ŻE:

1. Ze względu na znaczenie łączności, infrastruktury i usług elektronicznych jako podstawy działalności gospodarczej i społecznej, bezpieczeństwo sieci i informacji przyczynia się do istotnych wartości i celów w społeczeństwie, takich jak demokracja, prywatność, wzrost gospodarczy, swobodny przepływ myśli oraz stabilność gospodarcza i polityczna;

2. Systemy, infrastruktura i usługi informacyjno-komunikacyjne, w tym Internet, odgrywają istotną rolę w społeczeństwie, a zakłócenia ich działania mogą powodować ogromne szkody gospodarcze, co podkreśla znaczenie środków zmierzających do zwiększenia ochrony i odporności w celu zapewnienia ciągłości funkcjonowania usług krytycznych;

3. Incydenty zagrażające bezpieczeństwu mogą naruszać zaufanie użytkowników. Podczas gdy poważne zakłócenia działania sieci i systemów informatycznych mogłyby mieć znaczne skutki społeczno-gospodarcze, codzienne problemy i niedogodności również mogą podkopywać zaufanie społeczeństwa do technologii, sieci i usług;

4. Kalejdoskop zagrożeń zmienia się i rozrasta, co nasila potrzebę zapewnienia użytkownikom końcowym, przedsiębiorstwom i administracji takiej infrastruktury łączności elektronicznej, która z założenia byłaby solidna i odporna, a także określenia właściwych zachęt dla usługodawców, by dokonali tego bez zbędnych opóźnień;

5. Istnieje potrzeba zwiększenia bezpieczeństwa sieci i informacji oraz uwzględniania tego zagadnienia we wszystkich dziedzinach polityki i sektorach społecznych, a także stawienia czoła wyzwaniu, jakim jest zapewnienie wystarczających umiejętności za pomocą działań krajowych i europejskich oraz kampanii uświadamiających wśród użytkowników technologii informacyjno-komunikacyjnych (TIK);

6. Urzeczywistnienie i funkcjonowanie rynku wewnętrznego wymagać będzie ponadgranicznej współpracy właścicieli sieci i usługodawców, jako że potencjalne zakłócenia w jednym państwie członkowskim mogą również oddziaływać na inne państwa członkowskie i całą UE;

7. Nowe schematy użytkowania, takie jak „cloud computing" czy oprogramowanie jako usługa, dodatkowo zwiększają znaczenie bezpieczeństwa sieci i informacji;

8. Bezpieczeństwo sieci i informacji służy celowi wszystkich zainteresowanych stron, we wszystkich sektorach społeczeństwa, by móc zaufać systemom informatycznym, w związku z czym potrzebne jest podejście międzysektorowe i transgraniczne;

9. Wraz z rosnącym wykorzystaniem TIK w społeczeństwie bezpieczeństwo sieci i informacji staje się niezbędnym warunkiem niezawodnego i bezpiecznego świadczenia usług publicznych, takich jak e-administracja;

10. Agencja ENISA może wykorzystać ważną rolę, jaką odgrywa już w dziedzinie bezpieczeństwa sieci i informacji.

III. PODKREŚLA, ŻE:

1. Potrzeba wysokiego poziomu bezpieczeństwa sieci i informacji w UE w celu wspierania:

   a) swobód i praw obywatelskich, w tym prawa do prywatności;

   b) społeczeństwa efektywnego pod względem jakości przetwarzania informacji;

   c) zyskowności oraz rozwoju handlu i przemysłu;

   d) zaufania obywateli i organizacji do przetwarzania informacji i systemów TIK;

2. Sektor TIK jest nieodzowny dla większości sektorów społeczeństwa, co czyni bezpieczeństwo sieci i informacji wspólnym zadaniem wszystkich zainteresowanych stron, w tym operatorów, usługodawców, producentów sprzętu i oprogramowania, użytkowników końcowych, organów publicznych i rządów krajowych.

IV. UZNAJE:

1. Znaczenie aktywnej i posiadającej odpowiednią wiedzę europejskiej społeczności bezpieczeństwa sieci i informacji, która przyczynia się do ściślejszej współpracy między państwami członkowskimi a sektorem prywatnym;

2. Korzyści płynące ze zharmonizowanego stosowania, w odpowiednich przypadkach, międzynarodowych standardów bezpieczeństwa w całej UE na potrzeby bezpieczeństwa sieci i informacji;

3. Potrzebę wspólnego europejskiego podejścia do bezpieczeństwa sieci i informacji na arenie międzynarodowej, ponieważ mamy do czynienia z wyzwaniem o zasięgu globalnym;

4. Znaczenie dla państw członkowskich i instytucji UE, jakie ma dostępność rzetelnych danych statystycznych na temat stanu bezpieczeństwa sieci i informacji w Europie;

5. Potrzebę większej świadomości oraz narzędzi zarządzania ryzykiem dla wszystkich zainteresowanych stron;

6. Znaczenie wzmożonych wysiłków wśród państw członkowskich w celu podnoszenia świadomości, wymiany sprawdzonych rozwiązań oraz opracowywania wytycznych dla państw członkowskich;

7. Znaczenie modeli z udziałem wielu zainteresowanych stron, takich jak partnerstwa publiczno-prywatne (PPP), opartych na długookresowym działaniu oddolnym w celu ograniczenia określonych zagrożeń w przypadkach, gdy tego rodzaju podejście przynosi wartość dodaną, przyczyniając się do zapewnienia wysokiego poziomu odporności sieci;

8. Kluczową rolę, jaką odgrywają usługodawcy w zapewnianiu społeczeństwu solidnej i odpornej infrastruktury łączności elektronicznej;

9. Przydatność organizowanych w Europie ćwiczeń w dziedzinie bezpieczeństwa sieci i informacji, które mogą być wartościową lekcją dla operatorów sieci, usługodawców i administracji;

10. Że krajowe lub rządowe zespoły ds. reagowania kryzysowego w dziedzinie informatycznej (ang. „Computer Emergency Response Team", CERT) bądź inne mechanizmy reagowania wobec zagrożeń i eliminowania słabych punktów mogą przyczynić się do zapewnienia wysokiego poziomu odporności oraz zdolności do przetrwania i wyeliminowania zakłóceń w działaniu sieci i systemów informatycznych;

11. Znaczenie analizy strategicznych skutków, zagrożeń i perspektyw dla instytucji UE związanych ze stworzeniem CERT oraz znaczenie rozważenia możliwej przyszłej roli agencji ENISA w tym zakresie;

12. Dotychczasowe osiągnięcia agencji ENISA w dziedzinie bezpieczeństwa sieci i informacji oraz potrzebę dalszego rozwoju tej agencji, by uczynić z niej efektywny organ zapewniający wyraźne korzyści w dziedzinie europejskiego bezpieczeństwa sieci i informacji.

V. PODKREŚLA, ŻE:

1. Rozszerzona, całościowa europejska strategia bezpieczeństwa sieci i informacji, z wyraźnym rozgraniczeniem obowiązków Komisji Europejskiej, państw członkowskich i agencji ENISA, ma kluczowe znaczenie dla tego, by stawić czoła aktualnym i przyszłym wyzwaniom;

2. Po przeprowadzeniu odpowiednich konsultacji i analiz należy rozważyć w procesie legislacyjnym kwestię modernizacji i wzmocnienia agencji ENISA, której mandat byłby elastyczny i przewidywałby nadzór ze strony państw członkowskich oraz Komisji, a także efektywną rolę przedstawicieli zainteresowanych stron z sektora prywatnego. Mandat agencji ENISA powinien uwzględniać ramy regulacyjne sieci i usług łączności elektronicznej oraz pozostawać w zgodzie z ambitnymi zamierzeniami określonymi w strategii lizbońskiej oraz celami w zakresie badań, innowacji, konkurencyjności, wzrostu gospodarczego i zapewniania zaufania;

3. Agencja ENISA mogłaby wspierać Komisję i państwa członkowskie w rozwijaniu i wdrażaniu polityki, w szczególności poprzez wypełnianie luki między światem technologii a światem polityki, oraz powinna współpracować ściśle z państwami członkowskimi i innymi zainteresowanymi stronami, by ich działania były odpowiednio dostosowane do priorytetów UE;

4. Agencja ENISA, działająca na podstawie zmienionego mandatu, powinna pełnić rolę unijnego ośrodka wiedzy specjalistycznej w sprawach związanych z bezpieczeństwem sieci i informacji w UE. W związku z tym instytucje europejskie powinny występować do niej o opinię oraz uwzględniać tę opinię przy opracowywaniu i wdrażaniu strategii politycznych mających potencjalny wpływ na tę dziedzinę;

5. Na wniosek państw członkowskich agencja ENISA mogłaby również wspierać je w rozbudowie ich własnego potencjału w dziedzinie bezpieczeństwa sieci i informacji oraz poprawie ich umiejętności radzenia sobie z incydentami zagrażającymi bezpieczeństwu.

VI. ZACHĘCA PAŃSTWA CZŁONKOWSKIE DO:

1. Kontynuowania prac mających na celu zwiększanie zaufania użytkowników końcowych do TIK poprzez kampanie uświadamiające;

2. Organizowania krajowych ćwiczeń lub udziału w regularnych europejskich ćwiczeniach w dziedzinie bezpieczeństwa sieci i informacji, odnotowując potrzebę szeroko zakrojonego planowania ze względu na złożoność tej kwestii oraz zaangażowanie sektora prywatnego. Na wniosek państw członkowskich agencja ENISA mogłaby wspierać państwa członkowskie w tym zakresie. Przedmiot oraz geograficzny zasięg takich ćwiczeń powinny z czasem naturalnie ewoluować oraz powinny opierać się na rozpoznanych zagrożeniach;

3. Stworzenia zespołów ds. reagowania kryzysowego w dziedzinie informatycznej (CERT) w państwach członkowskich, które nie dysponują jeszcze takimi strukturami, oraz do zacieśnienia współpracy między krajowymi CERT na szczeblu europejskim. Agencja ENISA mogłaby wspierać państwa członkowskie w tym zakresie;

4. Wzmożenia wysiłków w dziedzinie programów kształcenia, szkolenia i badań dotyczących bezpieczeństwa sieci i informacji, aby zapewnić dostępność w UE niezbędnych umiejętności technicznych i profesjonalnej kadry, jak również aby podnieść poziom profesjonalizmu osób działających w tej dziedzinie;

5. Podejmowania wspólnych działań w wypadku incydentów o charakterze transgranicznym oraz rozwijania możliwości takiego współdziałania, co wymaga wzmocnienia dialogu między właściwymi decydentami, zwłaszcza w kwestiach dotyczących poufności.

VII. ZWRACA SIĘ DO KOMISJI, BY:

1. W stosownych przypadkach wspierała państwa członkowskie we wdrażaniu niniejszej rezolucji;

2. Regularnie informowała Parlament Europejski i Radę o inicjatywach podejmowanych na szczeblu UE dotyczących bezpieczeństwa sieci i informacji;

3. We współpracy z agencją ENISA inicjowała kampanie uświadamiające społeczeństwo europejskie oraz podmioty prywatne o znaczeniu odpowiedniego zarządzania ryzykiem w odniesieniu do bezpieczeństwa sieci i informacji;

4. Kontynuowała, we współpracy z państwami członkowskimi, działania zmierzające do określenia zachęt dla operatorów infrastruktury łączności elektronicznej, by infrastruktura oferowana przez nich użytkownikom końcowym, przedsiębiorstwom i administracji była z założenia solidna i odporna;

5. We współpracy z państwami członkowskimi opracowała metody, które umożliwią ocenę porównawczą na szczeblu UE społeczno-gospodarczych skutków incydentów oraz efektywności środków zapobiegawczych;

6. Zachęcała do stosowania i rozwoju modeli z udziałem wielu zainteresowanych stron, które to modele powinny cechować się wyraźną wartością dodaną z korzyścią dla użytkowników końcowych oraz przemysłu;

7. Przygotowała całościową strategię bezpieczeństwa sieci i informacji, w tym [1] propozycje dotyczące wzmocnionego i elastycznego mandatu agencji ENISA, jak również wzmocnionego nadzoru ze strony państw członkowskich i Komisji;

8. Przeprowadziła, we współpracy z państwami członkowskimi, analizę dotyczącą zespołów ds. reagowania kryzysowego w dziedzinie informatycznej (CERT), tak aby określić, w których obszarach wymagana jest dalsza współpraca;

9. Nadal badała możliwości wypracowania wspólnego lub wzajemnie zgodnego podejścia instytucji UE do zamówień dotyczących bezpiecznych systemów i usług TIK.

VIII. WZYWA AGENCJĘ ENISA DO:

1. Dalszego aktywnego wspierania państw członkowskich, Komisji Europejskiej i innych właściwych zainteresowanych stron we wdrażaniu europejskiej polityki bezpieczeństwa sieci i informacji oraz w realizacji planu działania w sprawie ochrony krytycznej infrastruktury informatycznej;

2. Współpracy z państwami członkowskimi, Komisją i urzędami statystycznymi nad stworzeniem ram regulacyjnych dotyczących danych statystycznych na temat stanu bezpieczeństwa sieci i informacji w Europie.

IX. ZACHĘCA ZAINTERESOWANE STRONY DO:

1. Wzmożenia wysiłków zmierzających do podniesienia poziomu bezpieczeństwa sieci i informacji, w szczególności poprzez zapewnianie niezawodnych, godnych zaufania i łatwych w użyciu produktów i usług;

2. Należytego informowania użytkowników o zagrożeniach bezpieczeństwa związanych z produktami i usługami oraz o możliwych sposobach ochrony przed takimi zagrożeniami;

3. Podjęcia wszelkich właściwych środków technicznych i organizacyjnych w celu zagwarantowania ciągłości funkcjonowania, integralności i poufności sieci i usług łączności elektronicznej;

4. Dalszych prac normalizacyjnych w dziedzinie bezpieczeństwa sieci i informacji w celu znalezienia zharmonizowanych i współdziałających ze sobą rozwiązań;

5. Udziału wraz z państwami członkowskimi w ćwiczeniach mających zapewnić odpowiednią gotowość na wypadek stanów zagrożenia.

---

[1] Komisja sugeruje, by dodać tutaj słowa „być może".