I

(Rezolucje, zalecenia, stanowiska i opinie)

REZOLUCJE

RADA

REZOLUCJA RADY

z dnia 22 marca 2007 r.

w sprawie strategii na rzecz bezpiecznego społeczeństwa informacyjnego w Europie

(2007/C 68/01)

RADA UNII EUROPEJSKIEJ

PRZYJMUJE NINIEJSZĄ REZOLUCJĘ ORAZ

Z ZADOWOLENIEM PRZYJMUJE

Komunikat Komisji do Rady, Parlamentu Europejskiego, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów: Strategia na rzecz bezpiecznego społeczeństwa informacyjnego — „Dialog, partnerstwo i przejmowanie inicjatywy" z dnia 31 maja 2006 r.;

PRZYJMUJE DO WIADOMOŚCI

Komunikat Komisji do Rady, Parlamentu Europejskiego, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów w sprawie walki ze spamem, oprogramowaniem szpiegującym i złośliwym z dnia 15 listopada 2006 r.;

PRZYPOMINA

1. Rezolucję Rady w sprawie wspólnego podejścia i działań szczególnych w dziedzinie bezpieczeństwa sieci i informacji ([1]) z dnia 28 stycznia 2002 r.;

2. Rezolucję Rady w sprawie europejskiego podejścia do kultury bezpieczeństwa sieci i informacji ([2]) z dnia 18 lutego 2003 r.;

3. Konkluzje Rady w sprawie niezamawianych informacji wykorzystywanych do marketingu bezpośredniego czyli „spamu" z dni 8–9 marca 2004 r. oraz konkluzje Rady w sprawie walki ze spamem z 9–10 grudnia 2004 r.;

4. Konkluzje Rady Europejskiej z marca 2005 r. wznawiające strategię lizbońską oraz konkluzje Rady Europejskiej z marca 2006 r., w których apeluje ona do Komisji i państw członkowskich o intensywne wdrażanie nowej strategii i2010;

5. Ramy regulacyjne UE w zakresie łączności elektronicznej ([3]), w szczególności dotyczące bezpieczeństwa, prywatności i poufności łączności, które przyczyniają się do zapewniania wysokiego poziomu ochrony danych osobowych i prywatności oraz do integralności i bezpieczeństwa publicznych sieci łączności;

6. Rozporządzenie (WE) nr 460/2004 Parlamentu Europejskiego i Rady z dnia 10 marca 2004 r. ustanawiające Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji (ENISA) ([4]);

7. Agendę z Tunisu oraz zobowiązanie podjęte podczas Światowego Szczytu Społeczeństwa Informacyjnego w Tunisie, które podkreślają potrzebę zwalczania cyberprzestępczości oraz spamu przy jednoczesnym zapewnieniu ochrony prywatności i wolności wyrażania opinii, a także potrzebę dalszego promowania, rozwoju i wdrażania globalnej kultury cyberbezpieczeństwa we współpracy ze wszystkimi zainteresowanymi stronami;

8. Konkluzje prezydencji w związku ze zorganizowaną w Espoo w Finlandii (27–28 września 2006 r.) Coroczną Europejską Konferencją Społeczeństwa Informacyjnego pod tytułem „i2010 — w kierunku wszechobecnego europejskiego społeczeństwa informacyjnego";

([1]) Dz.U. C 43 z 16.2.2002, str. 2.
([2]) Dz.U. C 48 z 28.2.2003, str. 1.
([3]) Dyrektywy 2002/58/WE (dyrektywa o prywatności i łączności elektronicznej), 2002/20/WE (dyrektywa o zezwoleniach), 2002/22/WE (dyrektywa o usłudze powszechnej) (odpowiednio Dz.U. L 201 z 31.7.2002, str. 37, Dz.U. L 108 z 24.4.2002, str. 21 oraz Dz.U. L 108 z 24.4.2002, str. 51).
([4]) Dz.U. L 77 z 13.3.2004, str. 1.

W KONSEKWENCJI PODKREŚLA, ŻE:

1. Nasze społeczeństwa w szybkim tempie wchodzą w nową fazę rozwoju, prowadzącą do wszechobecnego społeczeństwa informacyjnego, w której coraz więcej codziennych czynności obywateli opiera się na wykorzystaniu technologii informacyjno-komunikacyjnych (TIK) oraz sieci łączności elektronicznej; bezpieczeństwo sieci i informacji powinno być uważane za kluczowy czynnik umożliwiający ten rozwój i jego powodzenie;

2. Zaufanie jest zasadniczym elementem sukcesu nowego społeczeństwa informacyjnego; zaufanie związane jest także z doświadczeniami użytkowników oraz potrzebą poszanowania ich prywatności; dlatego też bezpieczeństwo sieci i informacji nie powinno być uważane jedynie za kwestię techniczną;

3. Bezpieczeństwo sieci i informacji jest niezbędnym elementem tworzenia europejskiej przestrzeni informacyjnej w ramach inicjatywy i2010, przyczyniając się do powodzenia odnowionej strategii lizbońskiej; TIK są również decydującym elementem innowacyjności, wzrostu gospodarczego i zatrudnienia w całej gospodarce;

4. Nowe technologie, które poprowadzą nas ku wszechobecnemu społeczeństwu informacyjnemu, już są opracowywane; pojawienie się przełomowych technologii (takich jak szybkie sieci bezprzewodowe, urządzenia identyfikacji radiowej — RFID, sieci sensorów) oraz nowatorskich usług o bogatych zasobach treści (takich jak telewizja internetowa — IPTV, telefonia internetowa — VoIP, telewizja przenośna i inne usługi mobilne) wymaga odpowiednich poziomów bezpieczeństwa sieci i informacji już od pierwszych faz rozwoju, aby mogły one nabrać rzeczywistej wartości handlowej; szybkie przyjęcie nowych obiecujących wynalazków jest bardzo ważne dla rozwoju społeczeństwa informacyjnego oraz dla konkurencyjności Europy; organy rządowe i przedsiębiorstwa powinny jak najszybciej zacząć stosować bezpieczne nowo powstające technologie i usługi, aby przyspieszyć ich powszechne przyjęcie;

5. Dla UE strategiczne znaczenie ma fakt, że europejski przemysł jest zarówno wymagającym użytkownikiem, jak i konkurencyjnym dostawcą sieci oraz produktów i usług związanych z bezpieczeństwem; różnorodność, otwartość i interoperacyjność stanowią integralne elementy bezpieczeństwa i należy je wspierać;

6. Wiedza o bezpieczeństwie sieci i informacji oraz umiejętności z nim związane muszą stać się integralną częścią codziennego życia każdej osoby i zainteresowanej strony funkcjonującej w społeczeństwie; na szczeblu krajowym i UE przeprowadzono szereg kampanii na rzecz zwiększenia świadomości, lecz nadal należy podejmować działania w tej dziedzinie, zwłaszcza jeśli chodzi o użytkowników oraz małe i średnie przedsiębiorstwa (MŚP); szczególną uwagę poświęcić należy użytkownikom o szczególnych potrzebach lub ograniczonej wiedzy w zakresie bezpieczeństwa sieci i informacji; wszystkie zainteresowane strony powinny mieć świadomość, że stanowią element globalnego łańcucha bezpieczeństwa, i mieć możliwość działania w takim charakterze; kwestie bezpieczeństwa sieci i informacji powinny być uwzględniane we wszelkich działaniach edukacyjnych i szkoleniowych związanych z TIK;

7. Utworzenie ENISA jest bardzo ważnym krokiem naprzód w staraniach UE mających na celu sprostanie wyzwaniom dotyczącym bezpieczeństwa sieci i informacji; zakres, cele, zadania i okres działania agencji ENISA określa rozporządzenie (WE) nr 460/2004;

8. Zasoby przeznaczane na badania i rozwój oraz innowacje zarówno na poziomie krajowym, jak i UE, są jednym z głównych elementów podnoszenia poziomu bezpieczeństwa informacji i sieci w obrębie nowych systemów, aplikacji i usług; na szczeblu UE należy wzmocnić starania w zakresie badań i innowacyjności związanych z bezpieczeństwem, w szczególności poprzez siódmy program ramowy oraz program ramowy w zakresie konkurencyjności i innowacji; należy także podejmować działania w zakresie sposobów rozpowszechniania wyników i zachęcania do ich komercyjnego wykorzystania, w tym także oceny ich przydatności dla szerszych kręgów społeczeństwa; zwiększy to możliwości dostarczania przez europejskich dostawców takich rozwiązań w zakresie bezpieczeństwa, które będą zaspokajały szczególne potrzeby rynku europejskiego;

9. Wszechobecne społeczeństwo informacyjne obok ogromnych korzyści przynosi także istotne wyzwania, stwarzając w ten sposób nowe spektrum potencjalnych zagrożeń; zagrożenia bezpieczeństwa i prywatności, także spowodowane nielegalnym przechwytywaniem i wykorzystywaniem danych, stają się coraz poważniejsze, bardziej ukierunkowane i wyraźnie nacechowane dążeniem do korzyści finansowych; należy w nowatorski sposób znajdować nowe odpowiedzi na pojawiające się i już istniejące zagrożenia, tak aby uwzględnić w nich także zagadnienia wynikające ze złożoności systemów, błędów, nieprzewidzianych wypadków lub niejasnych wytycznych; należy zachęcać do tworzenia i rozwoju krajowych jednostek reagowania na sytuacje nadzwyczajne związane z komputerami, ukierunkowanych na wiele podmiotów, zachęcać do współpracy pomiędzy tymi jednostkami oraz między nimi a innymi odpowiednimi zainteresowanymi stronami, a także promować powyższe działania;

10. Na szczególną uwagę w polityce UE na rzecz bezpieczeństwa sieci i informacji zasługują normalizacja i certyfikacja produktów usług i systemów zarządzania — w szczególności przeprowadzana przez istniejące instytucje — stanowiące sposób rozpowszechniania dobrej praktyki i profesjonalizmu w dziedzinie bezpieczeństwa sieci i informacji; na terminowym przyjęciu ewentualnych nowych norm, o charakterze otwartym i interoperacyjnym, skorzystałyby zwłaszcza nowo pojawiające się technologie, takie jak RFID i telewizja przenośna; należy zachęcać europejskie organy normalizacyjne do działania w tej dziedzinie;

11. Ze względu na to, że sieci elektroniczne i systemy informacyjne odgrywają coraz większą rolę w ogólnym działaniu infrastruktury krytycznej, ich dostępność i integralność stają się niezbędne dla bezpieczeństwa i jakości funkcjonowania administracji, przedsiębiorstw i obywateli, dla jakości życia oraz dla ogólnego funkcjonowania społeczeństw;

12. Bardziej niż kiedykolwiek dotąd potrzebne są współpraca i podejścia praktyczne; różne zainteresowane strony powinny określić i uznać nawzajem swoje role, obowiązki i prawa.

I DLATEGO ZWRACA SIĘ DO PAŃSTW CZŁONKOWSKICH O:

1. Wspieranie programów szkoleń oraz zwiększanie ogólnej wiedzy na temat kwestii bezpieczeństwa sieci i informacji, np. poprzez przeprowadzanie kampanii informacyjnych dotyczących zagadnień bezpieczeństwa sieci i informacji, skierowanych do wszystkich obywateli/użytkowników i sektorów gospodarki, w szczególności MŚP oraz użytkowników o szczególnych potrzebach lub niewielkiej wiedzy w tym zakresie; do roku 2008 należy wybrać dzień, który stanie się ogólnoeuropejskim dniem zwiększania świadomości (np. „dzień bezpieczeństwa informacji i sieci") i który w każdym państwie członkowskim będzie mógł co roku być organizowany na zasadzie dobrowolności;

2. Zwiększenie wkładu w związane z bezpieczeństwem badania i rozwój oraz stworzenie większych możliwości wykorzystania uzyskanych w ten sposób wyników, a także lepsze ich rozpowszechnianie; zachęcanie do rozwijania nowatorskich partnerstw w celu przyspieszenia wzrostu europejskiej branży bezpieczeństwa TIK oraz w celu upowszechniania szybszego stosowania nowych technologii i usług w zakresie bezpieczeństwa sieci i informacji, co zwiększy ich wartość komercyjną;

3. Zwrócenie należnej uwagi na potrzebę zapobiegania nowym i istniejącym zagrożeniom dla sieci łączności elektronicznej i zwalczania takich zagrożeń, które obejmują także nielegalne przechwytywanie i wykorzystywanie danych; rozpoznawanie i zmniejszanie zagrożeń z tym związanych oraz zachęcanie, w odpowiednich przypadkach we współpracy z agencją ENISA, do efektywnej wymiany informacji oraz do współpracy między odpowiednimi organizacjami i agencjami na szczeblu krajowym; zaangażowanie w walkę ze spamem, programami szpiegującymi i złośliwym oprogramowaniem, w szczególności poprzez poprawę współpracy właściwych organów na szczeblu krajowym i międzynarodowym;

4. Zwiększanie wzajemnej współpracy w ramach strategii i2010 w celu określenia skutecznych i nowatorskich praktyk mających na celu zwiększenie bezpieczeństwa sieci i informacji oraz dobrowolne rozpowszechnianie wiedzy o takich praktykach na terenie całej UE;

5. Zachęcanie do stałego udoskonalania krajowych jednostek reagowania na sytuacje nadzwyczajne związane z komputerami;

6. Wspieranie środowiska sprzyjającego świadczeniu klientom przez dostawców usług i operatorów sieci solidnych usług oraz zapewnieniu przez nich odporności tych usług i rozwiązań w zakresie bezpieczeństwa, a także oferowaniu klientowi odpowiedniego wyboru w tym zakresie; zachęcanie lub w stosownych przypadkach obligowanie operatorów sieci i dostawców usług do zapewniania swym klientom odpowiedniego poziomu bezpieczeństwa sieci i informacji;

7. Kontynuację strategicznych rozmów w ramach Grupy Wysokiego Szczebla ds. Strategii i2010, z jednoczesnym uwzględnieniem stałego rozwoju społeczeństwa informacyjnego, oraz zapewnienie konsekwentnego podejścia obejmującego wymiary: regulacji, współregulacji, badań i rozwoju oraz administracji elektronicznej (e-Rząd), łączności i edukacji;

8. Zgodnie z planem działania na rzecz administracji elektronicznej w ramach inicjatywy i2010 zapewnienie uruchomienia niezawodnych usług administracji elektronicznej, promowanie interoperacyjnych rozwiązań w zakresie zarządzania tożsamością oraz wprowadzanie wszelkich niezbędnych zmian w organizacji sektora publicznego; rządy i administracje publiczne powinny stanowić model najlepszych praktyk, promując bezpieczne usługi administracji elektronicznej dla wszystkich obywateli;

Z ZADOWOLENIEM PRZYJMUJE PLANOWANE PRZEZ KOMISJĘ:

1. Dalsze opracowywanie kompleksowej i dynamicznej ogólnounijnej strategii na rzecz bezpieczeństwa sieci i informacji. Szczególne znaczenie ma zaproponowane przez Komisję podejście całościowe;

2. Zajęcie się kwestią bezpieczeństwa sieci i informacji poprzez uczynienie z niej jednego z celów przeglądu ram regulacyjnych UE dotyczących komunikacji elektronicznej;

3. Dalsze pełnienie swej roli w celu zwiększania świadomości potrzeby ogólnego politycznego zaangażowania na rzecz zwalczania spamu, programów szpiegujących i złośliwego oprogramowania; wzmacnianie dialogu i współpracy z państwami trzecimi, w szczególności poprzez zawieranie z nimi umów uwzględniających kwestię zwalczania spamu, programów szpiegujących i złośliwego oprogramowania;

4. Zwiększenie zaangażowania agencji ENISA we wspieranie strategii na rzecz bezpiecznego społeczeństwa informacyjnego w Europie, przedstawionej w niniejszej rezolucji, zgodnie z celami i zadaniami wyznaczonymi w rozporządzeniu (WE) nr 460/2004 oraz przy bliższej współpracy i ściślejszych kontaktach roboczych z państwami członkowskimi i zainteresowanymi stronami;

5. Opracowanie — w oparciu o ramy i2010, we współpracy z państwami członkowskimi i wszystkimi zainteresowanymi stronami, w szczególności z ekspertami w dziedzinie statystyki i ekspertami z państw członkowskich w dziedzinie bezpieczeństwa informacji — odpowiednich wskaźników do wspólnotowych badań aspektów związanych z bezpieczeństwem i zaufaniem;

6. Zachęcanie państw członkowskich do zbadania, poprzez dialog obejmujący wiele zainteresowanych stron, czynników gospodarczych, biznesowych i społecznych w celu opracowania polityki dla sektora TIK zmierzającej do zwiększenia bezpieczeństwa oraz odporności sieci i systemów informatycznych, co może stanowić wkład w planowany europejski program ochrony infrastruktury strategicznej;

7. Kontynuację prowadzonych w porozumieniu z państwami członkowskimi działań mających na celu propagowanie dialogu z odpowiednimi partnerami i organizacjami międzynarodowymi z myślą o wspieraniu globalnej współpracy w dziedzinie bezpieczeństwa sieci i informacji, w szczególności poprzez realizację linii działania wytyczonych przez Światowy Szczyt Społeczeństwa Informacyjnego oraz regularne składanie sprawozdań Radzie;

ORAZ WZYWA:

1. Agencję ENISA — do dalszego działania w bliskiej współpracy z państwami członkowskimi, Komisją i innymi odpowiednimi zainteresowanymi stronami w celu realizacji zadań i celów określonych w rozporządzeniu (WE) nr 460/2004, a także do wspomagania podejmowanych przez Komisję i państwa członkowskie działań zmierzających do sprostania wymaganiom bezpieczeństwa sieci i informacji, przyczyniając się w ten sposób do realizacji i dalszego rozwoju strategii na rzecz bezpiecznego społeczeństwa informacyjnego w Europie, przedstawionej w niniejszej rezolucji;
2. Wszystkie zainteresowane strony — do poprawy bezpieczeństwa oprogramowania oraz bezpieczeństwa i odporności sieci i systemów informacyjnych zgodnie ze strategią na rzecz bezpiecznego społeczeństwa informacyjnego w Europie, przedstawioną w niniejszej rezolucji, a także do udziału w zorganizowanej debacie z udziałem wielu zainteresowanych stron na temat sposobów najlepszego wykorzystania istniejących narzędzi i instrumentów regulacyjnych;
3. Przedsiębiorstwa — do zajęcia pozytywnego stanowiska wobec bezpieczeństwa informacji i sieci w celu stworzenia bardziej zaawansowanych i bezpieczniejszych produktów i usług, do rozważania inwestycji w takie produkty i usługi jako sposób osiągnięcia przewagi nad konkurencją;
4. Producentów i dostawców usług — do projektowania produktów i usług oraz wdrażania infrastruktury sieciowej, aplikacji i oprogramowania — w stosownych przypadkach — z uwzględnieniem wymogów w zakresie bezpieczeństwa, prywatności i poufności, a także do wdrażania i monitorowania rozwiązań w dziedzinie bezpieczeństwa;
5. Zainteresowane strony — do współpracy oraz tworzenia środowisk doświadczalnych służących do testowania i pilotażu nowych technologii i usług w sposób bezpieczny; do przyjmowania nowych bezpiecznych technologii i usług bez zbędnych opóźnień po ich wprowadzeniu do obrotu;
6. Wszystkie zainteresowane strony — do zaangażowania w dalsze starania zmierzające do zwalczania spamu i innych nieprawidłowych działań w sieci oraz do aktywnej współpracy z właściwymi organami na szczeblu krajowym i międzynarodowym;
7. Dostawców usług oraz sektor TIK — do skupienia się na zwiększeniu bezpieczeństwa, prywatności i możliwości korzystania z produktów, procesów i usług, w celu zapewnienia niezawodności, zapobiegania kradzieżom tożsamości i innym naruszającym prywatność atakom oraz zwalczania takich zjawisk;
8. Operatorów sieci, dostawców usług oraz sektor prywatny — do wzajemnego udostępniania oraz do realizacji dobrych praktyk w dziedzinie bezpieczeństwa, a także do propagowania kultury analizy ryzyka i zarządzania ryzykiem w organizacjach i firmach poprzez wspieranie odpowiednich programów szkoleń, rozwój planowania awaryjnego oraz udostępnianie klientom w ramach swych usług rozwiązań w dziedzinie bezpieczeństwa.