IV

(Zawiadomienia)

ZAWIADOMIENIA INSTYTUCJI I ORGANÓW UNII EUROPEJSKIEJ

RADA

Konkluzji Rady z dnia 27 listopada 2008 r. w sprawie uzgodnionej strategii pracy i konkretnych środków służących zwalczaniu cyberprzestępczości

(2009/C 62/05)

RADA UNII EUROPEJSKIEJ,

ODNOTOWUJĄC, ŻE:

— jednym z celów Unii Europejskiej jest stopniowe ustanawianie przestrzeni wolności, bezpieczeństwa i sprawiedliwości przez podjęcie wspólnych działań państw członkowskich w dziedzinie współpracy policyjnej i sądowej;

— ochrona własnych obywateli to jedno z najważniejszych zadań Europy. Unia musi zatem być w stanie wykrywać pojawiające się formy przestępczości i dostosowywać swoje działania tak, by móc szybko je zwalczać;

— w ostatnich latach stale rośnie liczba przestępstw popełnianych w Internecie i coraz częściej przestępstwa te mają charakter transgraniczny, gdyż Internet sprawia, iż znikają granice;

— Rada Europejska na posiedzeniu w Tampere w październiku 1999 roku priorytetowe znaczenie nadała strategii służącej zwalczaniu przestępczości zorganizowanej i przestępczości komputerowej. Od tego czasu to priorytetowe znaczenie znalazło potwierdzenie w licznych pracach przeprowadzonych przez instytucje europejskie, zwłaszcza w komunikacie Komisji do Parlamentu Europejskiego, Rady i Komitetu Regionów z dnia 22 maja 2007 r. pt. „W kierunku ogólnej strategii zwalczania cyberprzestępczości" oraz w decyzji ramowej 2005/222/WSiSW z dnia 24 lutego 2005 r. w sprawie ataków na systemy informatyczne [1], którą Komisja planuje zaktualizować w 2009 roku;

— najpóźniej do 15 września 2010 r. Komisja dokona oceny wdrażania dyrektywy 2006/24/WE Parlamentu Europejskiego i Rady z dnia 15 marca 2006 r. w sprawie zatrzymywania danych;

— Komisja i Rada Europy zakończyły już prace nad wzmocnieniem partnerstw między organami publicznymi a sektorem prywatnym z myślą o zwalczaniu cyberprzestępczości;

— Komisja przedstawi komunikat na temat przyszłych priorytetów w dziedzinie wolności, bezpieczeństwa i sprawiedliwości w Europie, w którym omówiony zostanie wstępnie przyszły program długoterminowy (na lata 2010–2014) i w którym należy poruszyć kwestię zwalczania cyberprzestępczości;

— przyjęte przez Radę konkluzje w sprawie stworzenia krajowych mechanizmów zasilających europejską platformę, która będzie służyć powiadamianiu o przestępstwach zauważonych w Internecie [2], są wyrazem tej chęci wzmocnienia współpracy policyjnej dzięki zapewnieniu znacznych i skutecznych zasobów organom ścigania;

— ponadto opracowanie całościowego planu zwalczania cyberprzestępczości wydaje się na szczeblu Unii Europejskiej najstosowniejszą metodą, by znaleźć rozwiązanie wszystkich problemów, które pojawiają się lub mogą się pojawić w najbliższej przyszłości w związku z tym zagadnieniem, oraz by zapewnić kontrolę realizacji tych rozwiązań.

RADA:

1) UWAŻA, że należy zwalczać wszelkie aspekty cyberprzestępczości i zachęcać państwa członkowskie i Komisję, by określiły wspólną strategię pracy, która uwzględniać będzie postanowienia konwencji Rady Europy o cyberprzestępczości.

   Wspomnianą strategię należy podporządkować celowi, jakim jest jeszcze skuteczniejsze stawienie czoła różnorodnym działaniom przestępczym dokonywanym za pomocą sieci elektronicznych. Działania te przyjmują tak niepokojącą postać jak pornografia dziecięca, wszelkie formy przemocy seksualnej czy czyny terrorystyczne — w definicji decyzji ramowej 2002/475/WSiSW z dnia 13 czerwca 2002 r.

[1] Dz.U. L 69 z 16.3.2005, s. 67.

[2] Dok. 13243/08 ENFOPOL 162 CRIMORG 140.

Strategia ta powinna również przyczynić się do zwalczania konkretnych niebezpieczeństw, na które narażone są sieci elektroniczne (ataki na masową skalę na systemy informatyczne).

W strategii należy ponadto zaproponować środki walki z tradycyjnymi formami przestępczości popełnianymi w Internecie, takimi jak podszywanie się pod inną osobę, kradzież tożsamości, oszukańcze sprzedaże, przestępstwa finansowe, nielegalny handel prowadzony przez Internet, zwłaszcza handel środkami odurzającymi i bronią.

2) WYRAŻA OPINIĘ, że poszukiwanie skutecznej odpowiedzi na te różnorakie zagrożenia związane z sieciami elektronicznymi powinno się przełożyć na działania horyzontalne, takie jak:

   a) wzmocnienie partnerstwa między organami publicznymi a sektorem prywatnym z myślą o wspólnym wypracowaniu metod wykrywania szkód spowodowanych przez działania przestępcze i zapobiegania tym szkodom, a także z myślą o przekazywaniu organom ścigania istotnych informacji dotyczących częstotliwości przestępstw przez przedsiębiorstwa, które padły ich ofiarą. W szczególności Komisja powinna przeprowadzić prace nad szczegółami wytycznych przyjętych podczas konferencji poświęconej globalnej współpracy na rzecz zwalczania cyberprzestępczości, która odbyła się pod auspicjami Rady Europy w dniach 1–2 kwietnia 2008 r.; miała ona na celu zacieśnienie partnerstwa między organami publicznymi a sektorem prywatnym w ramach zwalczania cyberprzestępczości. W tym kontekście Rada przyjmuje do wiadomości zalecenia poczynione na zakończenie spotkania ekspertów, które Komisja zorganizowała w dniach 25–26 września br.; zalecenia te znajdują się w dodatku do niniejszego projektu konkluzji;

   b) zwiększenie wiedzy i poprawienie stopnia wyszkolenia podmiotów zaangażowanych w walkę z cyberprzestępczością w Europie. W szczególności pożądane byłoby ustanowienie sieci szefów policji ds. zwalczania cyberprzestępczości. Prace tej sieci uzupełniałyby prace podjęte działające w tej dziedzinie grupy ekspertów i dotyczyłyby nie tylko przyszłych zagrożeń, ale również procedur w przypadku działań podejmowanych w pilnym trybie w odpowiedzi na poważne zdarzenia, podobnie jak ma to miejsce w przypadku grupy powołanej pod auspicjami Europolu lub wspólnych centrów badawczych ustanowionych przez Komisję;

   c) wzmocnienie technicznej i międzynarodowej współpracy z państwami trzecimi, które coraz częściej borykają się z tą przestępczą plagą, a także zwiększenie pomocy technicznej;

3) z tego względu ZACHĘCA państwa członkowskie i Komisję do wprowadzenia środków opracowanych na podstawie studiów przypadku i uwzględniających postęp techniczny, które to środki umożliwią przygotowanie — w krótkiej lub średniej perspektywie — narzędzi operacyjnych, takich jak:

   a) w krótkiej perspektywie

      — stworzenie europejskiej platformy ostrzegania o czynach o charakterze przestępczym popełnianych w Internecie;

      — opracowanie, w porozumieniu z podmiotami prywatnymi, europejskiego wzoru umowy o współpracy między organami ścigania a podmiotami prywatnymi;

      — stworzenie zgodnego z przepisami krajowymi opisu przestępstwa polegającego na kradzieży tożsamości w Internecie;

      — stworzenie krajowych ram i prowadzenie wymiany dobrych praktyk odnoszących się do cyberpatroli, będących nowoczesnym narzędziem zwalczania przestępczości w Internecie, co pozwoli na dzielenie się informacjami o pseudonimach na szczeblu europejskim zgodne z krajowymi przepisami dotyczącymi wymiany danych;

      — wykorzystanie wspólnych zespołów dochodzeniowo-śledczych;

      — znalezienie rozwiązania problemów powodowanych przez roaming w sieciach elektronicznych i anonimowy charakter użytkowania przedpłaconych produktów telekomunikacyjnych;

   b) w średniej perspektywie

      — wprowadzenie wymiany informacji o systemach blokowania/zamykania stron zawierających pornografię dziecięcą w państwach członkowskich. Należy zachęcić do zastosowania tych środków dostawców dostępu. W razie potrzeby europejska platforma mogłaby posłużyć sporządzeniu wspólnej „czarnej listy";

      — ułatwianie zdalnego przeszukiwania, jeśli przewidują je przepisy krajowe i za zgodą państwa przyjmującego, co umożliwi ekipom dochodzeniowym szybki dostęp do informacji;

      — opracowanie tymczasowych definicji kategorii przestępstw oraz wskaźników statystycznych, które ułatwią tworzenie porównywalnych statystyk odnoszących się do różnych form cyberprzestępczości; należy przy tym uwzględnić prace, które Unia Europejska już prowadzi w tej dziedzinie.

4) ZWRACA SIĘ do Komisji, by oceniła postępy w przygotowaniach do realizacji działań, o których mowa w powyższych pkt 2 i 3. W związku z powyższym wzywa państwa członkowskie do informowania Komisji o swoich działaniach.

5) APELUJE o to, by w dłuższej perspektywie wprowadzone zostały środki uzupełniające w ramach kolejnego długoterminowego programu w dziedzinie wolności, bezpieczeństwa i sprawiedliwości (2010–2014).

ZAŁĄCZNIK

1. Należy zachęcić organy ścigania oraz sektor prywatny ([1]) do zaangażowania się w wymianę informacji operacyjnych i strategicznych, która pozwoli wzmocnić ich zdolności w zakresie identyfikowania i zwalczania pojawiających się rodzajów cyberprzestępczości. Należy zachęcać organy ścigania do informowania dostawców dostępu o nowych tendencjach w cyberprzestępczości.
2. W szczególności państwa członkowskie są proszone o ustanowienie znormalizowanego systemu poufnej wymiany informacji operacyjnych i strategicznych między organami ścigania i sektorem prywatnym. Taki system powinien koniecznie obejmować następujące struktury i procedury:
3. stałe punkty kontaktowe: należy ustanowić stałe punkty kontaktowe w ramach organów ścigania i ich odpowiedniki w sektorze prywatnym, tak by poprawić jasność i wydajność procesu składania wniosków i odpowiedzi na nie. Punkty kontaktowe w sektorze prywatnym powinny działać również poza godzinami pracy przedsiębiorstw, tak by mogły odpowiadać na pilne wnioski ze strony organów ścigania. Kwestię tego, które wnioski należy uznać za pilne, powinny między sobą ustalić organy ścigania i sektor prywatny.
4. Sektor prywatny i organy ścigania są proszone o wzajemną pomoc w zakresie edukacji, szkolenia i innego wsparcia swoich służb i działań.
5. Standardowy formularz wniosku: na szczeblu krajowym, a w miarę możliwości również w kontaktach z państwami trzecimi, organy ścigania powinny określić standardy i strukturę formularza wykorzystywanego do przesyłania wniosków i odpowiadania na nie. Sektor prywatny powinien korzystać z tego formularza, odpowiadając na wnioski organów ścigania. Wnioski ze strony organów ścigania powinny być przynajmniej składane na piśmie, najlepiej w formie elektronicznej, i zawierać następujące informacje:
   — numer referencyjny,
   — odniesienie do podstaw prawnych,
   — informacje o tym, jakich danych wniosek dotyczy,
   — strefa czasowa,
   — informacje, które umożliwiają zweryfikowanie źródła wniosku.
6. Poziomy priorytetu wniosku: organy ścigania i sektor prywatny powinny między sobą ustalić system nadawania priorytetu wnioskom przekazywanym przez organy ścigania do sektora prywatnego.
7. Organy ścigania i sektor prywatny powinny brać pod uwagę koszty, jakie wiążą się ze sformułowaniem wniosku i odpowiedzią na niego. Procedury należy opracowywać, uwzględniając skutki finansowe tych działań, należy również wziąć pod uwagę kwestię zwrotu kosztów lub sprawiedliwej rekompensaty dla stron.
8. Wzywa się Komisję Europejską, państwa członkowskie i podmioty sektora prywatnego, by wspierały wymianę dobrych praktyk w odniesieniu do powyższych pkt. 1–7, tak by możliwe było zbliżenie działania mechanizmów krajowych, a w dalszej perspektywie — stworzenie systemu wymiany informacji operacyjnych i strategicznych na szczeblu UE.

([1]) Termin „sektor prywatny" obejmuje nie tylko przedsiębiorstwa sektora prywatnego, ale również odpowiednie podmioty branży technologii informacyjno-komunikacyjnych, w tym zespoły CERT (*Computer Emergency Response Teams*, komputerowe zespoły szybkiego reagowania).