KOMISJA WSPÓLNOT EUROPEJSKICH

Bruksela, dnia 30.3.2009
KOM(2009) 149 wersja ostateczna

KOMUNIKAT KOMISJI DO PARLAMENTU EUROPEJSKIEGO, RADY, EUROPEJSKIEGO KOMITETU EKONOMICZNO-SPOŁECZNEGO I KOMITETU REGIONÓW

w sprawie ochrony krytycznej infrastruktury informatycznej

„Ochrona Europy przed zakrojonymi na szeroką skalę atakami i zakłóceniami cybernetycznymi : zwiększenie gotowości, bezpieczeństwa i odporności”

{SEC(2009) 399}
{SEC(2009) 400}

(przedstawiona przez Komisję)

KOMUNIKAT KOMISJI DO PARLAMENTU EUROPEJSKIEGO, RADY, EUROPEJSKIEGO KOMITETU EKONOMICZNO-SPOŁECZNEGO I KOMITETU REGIONÓW

w sprawie ochrony krytycznej infrastruktury informatycznej

„Ochrona Europy przed zakrojonymi na szeroką skalę atakami i zakłóceniami cybernetycznymi: zwiększenie gotowości, bezpieczeństwa i odporności"

1. WPROWADZENIE

Technologie informacyjno-komunikacyjne (ang. *Information and Communication Technologies*, ICT) w coraz większym stopniu stają się nieodłączną częścią naszych codziennych działań. Niektóre systemy, usługi, sieci i infrastruktury ICT (w skrócie – infrastruktury ICT) stanowią istotną część europejskiej gospodarki i społeczeństwa z racji tego, że albo dostarczają niezbędne towary i usługi, albo stanowią bazę dla innych infrastruktur krytycznych. Uważa się je zwykle za krytyczne infrastruktury informatyczne (ang. *critical information infrastructures*, CII)[1], ponieważ zakłócenie ich działalności lub zniszczenie ich miałoby poważne konsekwencje dla kluczowych aspektów funkcjonowania społeczeństwa. Jako ostatnie przykłady wymienić można zakrojone na szeroką skalę ataki cybernetyczne na Estonię w 2007 r. oraz przecięcie kabli transkontynentalnych w 2008 r.

Światowe Forum Gospodarcze oszacowało w 2008 r., że prawdopodobieństwo wystąpienia poważnej awarii CII w ciągu najbliższych 10 lat wynosi 10%–20%, a jej potencjalny koszt dla światowej gospodarki wyniósłby około 250 mld USD[2].

W niniejszym komunikacie skoncentrowano się na zapobieganiu, gotowości i świadomości oraz określono plan natychmiastowych działań mających na celu zwiększenie bezpieczeństwa i odporności CII. Główne poruszone kwestie są zbieżne z tematyką debaty zainicjowanej na wniosek Rady i Parlamentu Europejskiego, poświęconej wyzwaniom i priorytetom w zakresie polityki dotyczącej bezpieczeństwa sieci i informacji (ang. *network and information security*, NIS) oraz najbardziej odpowiednim instrumentom koniecznym do rozwiązania tych problemów na szczeblu UE. Proponowane działania stanowią również uzupełnienie działań mających na celu zapobieganie, zwalczanie i ściganie działalności kryminalnej i terrorystycznej wymierzonej w CII, a także są spójne z bieżącą i przyszłą działalnością badawczą UE w dziedzinie bezpieczeństwa sieci i informacji oraz z międzynarodowymi inicjatywami podejmowanymi w tej dziedzinie.

2. KONTEKST POLITYCZNY

W niniejszym komunikacie opracowano politykę europejską mającą na celu zwiększenie zaufania do społeczeństwa informacyjnego i wzmocnienie jego bezpieczeństwa. Komisja[3] już

---

1 Definicję CII zaproponowano w COM(2005) 576 wersja ostateczna

2 Global Risks 2008 (Globalne zagrożenia 2008)

3 COM (2005) 229

w 2005 r. podkreśliła pilną potrzebę koordynacji działań zmierzających do tego, by zbudować zaufanie zainteresowanych podmiotów do elektronicznych środków komunikacji i usług. W 2006 r. przyjęto w tym celu strategię na rzecz bezpiecznego społeczeństwa informacyjnego[4]. Jej główne elementy, w tym bezpieczeństwo i odporność infrastruktur ICT, zatwierdzono w rezolucji Rady 2007/068/01. Nie wydaje się jednak, aby zainteresowane strony w wystarczającym stopniu poczuwały się do odpowiedzialności za realizację tych działań. Strategia ta wzmacnia również, pod względem taktycznym i operacyjnym, rolę ustanowionej w 2004 r. Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji (ENISA), której zadaniem jest udział w pracach zmierzających do zapewnienia wysokiego i skutecznego poziomu NIS na terenie Wspólnoty oraz rozwijanie kultury NIS z korzyścią dla obywateli UE, konsumentów, przedsiębiorstw i administracji.

W 2008 r. mandat Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji został przedłużony na niezmienionych warunkach do marca 2012 r.[5] Równocześnie Rada i Parlament Europejski wezwały do „*dalszej dyskusji nad przyszłością agencji ENISA i nad ogólnym kierunkiem europejskich starań na rzecz większego bezpieczeństwa sieci i informacji*". W celu wsparcia tej debaty w listopadzie ubiegłego roku Komisja zainicjowała internetowe konsultacje publiczne[6], których analiza zostanie wkrótce udostępniona.

Działania zaplanowane w niniejszym komunikacie wpisują się w ramy europejskiego programu ochrony infrastruktury krytycznej (ang. *European Programme for Critical Infrastructure Protection*, EPCIP) i prowadzone są stosunku do niego równolegle[7]. Jednym z kluczowych elementów EPCIP jest dyrektywa[8] w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej[9], w której sektor ICT określono jako przyszły sektor priorytetowy. Kolejnym istotnym elementem EPCIP jest sieć ostrzegania o zagrożeniach infrastruktury krytycznej (ang. *Critical Infrastructure Warning Information Network*, CIWIN)[10].

Od strony prawnej, wniosek Komisji w sprawie reformy ram regulacyjnych sieci i usług łączności elektronicznej[11] zawiera nowe przepisy dotyczące bezpieczeństwa i integralności, które przede wszystkim zwiększają zobowiązania operatorów do podjęcia odpowiednich środków w przypadku zaistnienia określonych zagrożeń, do zagwarantowania ciągłości usług i do powiadamiania o przypadkach naruszenia bezpieczeństwa[12]. Podejście to jest zgodne z ogólnym celem polegającym na zwiększeniu bezpieczeństwa i odporności CII. Parlament Europejski i Rada wyraziły szerokie poparcie dla tych przepisów.

Działania proponowane w niniejszym komunikacie uzupełniają już istniejące i przyszłe środki w dziedzinie współpracy policyjnej i sądowej mające na celu zapobieganie, zwalczanie i ściganie działalności kryminalnej i terrorystycznej wymierzonej w infrastruktury ICT,

---

4 COM (2006) 251
5 Rozporządzenie (WE) nr 1007/2008
6 http://ec.europa.eu/information_society/newsroom/cf/itemlongdetail.cfm?item_id=4464
7 COM(2006) 786 wersja ostateczna
8 2008/114/WE
9 http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/en/er/104617.pdf
10 COM(2008) 676 wersja ostateczna
11 Art. 13 dyrektywy ramowej
12 COM(2007) 697, COM(2007) 698, COM(2007) 699

przewidziane między innymi w decyzji ramowej Rady w sprawie ataków na systemy informatyczne[13] oraz w jej planowanej aktualizacji[14].

W inicjatywie tej uwzględniono działania NATO dotyczące wspólnej polityki obrony przed atakami cybernetycznymi prowadzone przez Organ Zarządzający ds. Obrony przed Atakami Cybernetycznymi (ang. *Cyber Defence Management Authority*) oraz Centrum Doskonałości ds. Współpracy w Dziedzinie Obrony przed Atakami Cybernetycznymi (ang. *Cooperative Cyber Defence Centre of Excellence*).

Należycie uwzględniono również rozwój wydarzeń w polityce międzynarodowej, zwłaszcza opracowane przez państwa grupy G8 zasady dotyczące ochrony krytycznych infrastruktur informatycznych (ang. *Critical Information Infrastructures Protection*, CIIP)[15]; rezolucję Zgromadzenia Ogólnego ONZ 58/199 „Creation of a global culture of cybersecurity and the protection of critical information infrastructures" („Tworzenie globalnej kultury bezpieczeństwa cybernetycznego i ochrona krytycznych struktur informatycznych" oraz opracowane ostatnio zalecenie OECD w sprawie ochrony krytycznych infrastruktur informatycznych.

3. CO PODLEGA ZAGROŻENIOM

3.1. Krytyczne infrastruktury informatyczne są kluczowe dla gospodarki i rozwoju społeczeństwa w UE

W ostatnich sprawozdaniach na temat innowacji i wzrostu gospodarczego podkreślono gospodarczą i społeczną rolę sektora ICT i infrastruktur ICT. Sprawozdania te to m.in. komunikat w sprawie śródokresowego przeglądu i-2010[16], sprawozdanie grupy Aho[17] oraz roczne sprawozdania gospodarcze Unii Europejskiej[18]. OECD podkreśla znaczenie sektora ICT i Internetu „*w zakresie zwiększania wydajności gospodarki i dobrobytu społecznego, a także w zakresie zwiększania zdolności społeczeństw do poprawy jakości życia obywateli na całym świecie*"[19]. OECD zaleca również strategie, które mają zwiększyć zaufanie do infrastruktury internetowej.

Sektor ICT jest kluczowy dla wszystkich grup społecznych. Przedsiębiorstwa korzystają z sektora ICT zarówno do celów sprzedaży bezpośredniej, jak i w celu zapewnienia wydajności procesów wewnętrznych. Sektor ICT jest niezbędnym elementem innowacji i odpowiada za prawie 40% wzrostu produktywności[20]. ICT są również szeroko obecne w pracy rządów i administracji publicznych: korzystanie z usług e-rządu na wszystkich szczeblach, a także zastosowanie nowoczesnych aplikacji związanych ze zdrowiem, energią i udziałem w życiu politycznym sprawiają, że sektor publiczny jest w dużym stopniu uzależniony od ICT. Równie istotny jest fakt, że w codziennych działaniach także obywatele stają się coraz

---

13 2005/222/WSiSW
14 COM (2008) 712
15 http://www.usdoj.gov/criminal/cybercrime/g82004/G8_CIIP_Principles.pdf
16 COM(2008) 199 wersja ostateczna
17 http://ec.europa.eu/invest-in-research/action/2006_ahogroup_en.htm
18 Przegląd gospodarczy UE za 2007 r. http://ec.europa.eu/economy_finance/publications/publication10130_en.pdf
19 http://www.oecd.org/dataoecd/1/29/40821707.pdf
20 http://epp.eurostat.ec.europa.eu/ - Nauka i technika/Społeczeństwo informacyjne

bardziej zależni od ICT: zwiększenie bezpieczeństwa CII zwiększyłoby zatem zaufanie obywateli do ICT, w szczególności dzięki lepszej ochronie danych osobowych i prywatności.

3.2. Zagrożenia dla krytycznych struktur informatycznych

Zrozumienie zagrożeń wynikających z ataków dokonywanych przez ludzi, katastrof naturalnych i awarii technicznych jest często niepełne, a ich analiza – niewystarczająca. Poziom świadomości wśród zainteresowanych podmiotów jest zatem niewystarczający, by opracować skuteczne zabezpieczenia i środki zaradcze.

Ataki cybernetyczne osiągnęły bezprecedensowy poziom zaawansowania. Zwykłe eksperymenty stają się teraz wyspecjalizowanymi działaniami, które prowadzi się dla zysku lub z powodów politycznych. Niedawne, zakrojone na szeroką skalę ataki cybernetyczne na Estonię, Litwę i Gruzję to najszerzej opisywane przykłady ilustrujące bardziej ogólną tendencję. Duża liczba wirusów, robaków i innych rodzajów złośliwego oprogramowania, coraz częstsze występowanie botnetów i ciągły wzrost ilości spamu potwierdzają skalę tego problemu[21].

Wysoki stopień zależności od CII, ich transgraniczne powiązania oraz współzależności z innymi infrastrukturami, a także ich słabe punkty i grożące im niebezpieczeństwa sprawiają, że konieczne jest podjęcie kwestii ich bezpieczeństwa i odporności w ujęciu systemowym, uznając je za pierwszą linię obrony w przypadku awarii i ataków.

3.3. Bezpieczeństwo i odporność krytycznych infrastruktur informatycznych jako sposób zwiększenia zaufania do społeczeństwa informacyjnego

Aby zapewnić maksymalne wykorzystanie infrastruktur ICT, a tym samym w pełni zrealizować gospodarcze i społeczne możliwości społeczeństwa informacyjnego, wszystkie zainteresowane podmioty muszą mieć do nich duży stopień zaufania. Zależy to od różnych czynników, z których najważniejszy to zapewnienie wysokiego poziomu bezpieczeństwa i odporności infrastruktur ICT. Różnorodność, otwarcie, interoperacyjność, użyteczność, przejrzystość, odpowiedzialność, weryfikowalność różnych elementów składowych i konkurencyjność to kluczowe czynniki zapewniające zwiększenie bezpieczeństwa i zachęcające do wdrażania produktów, procesów i usług zwiększających jego poziom. Jak już wcześniej Komisja podkreślała[22], jest to wspólna odpowiedzialność: żaden zainteresowany podmiot sam nie dysponuje środkami, by zapewnić bezpieczeństwo i odporność wszystkich infrastruktur ICT i by wypełnić wszystkie związane z tym zobowiązania.

Przyjęcie takich zobowiązań wymaga podejścia do zarządzania ryzykiem i kultury zarządzania ryzykiem, które umożliwią reakcję na zagrożenia już rozpoznane i pozwolą przewidzieć przyszłe, jeszcze niezidentyfikowane niebezpieczeństwa, nie popadając przy tym w przesadę i nie hamując rozwoju nowatorskich usług i aplikacji.

3.4. Wyzwania dla Europy

Aby zwiększyć bezpieczeństwo i odporność CII, oprócz wszystkich działań związanych z wdrażaniem dyrektywy w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury

---

[21] COM(2006) 688 wersja ostateczna

[22] COM(2006) 251 wersja ostateczna

krytycznej, zwłaszcza w zakresie określania kryteriów związanych z sektorem CII, należy zająć się kilkoma poważniejszymi problemami.

3.4.1. Zróżnicowane i nieskoordynowane podejścia krajowe

Choć wśród zaistniałych wyzwań i problemów jest wiele podobieństw, środki i systemy mające na celu zapewnienie bezpieczeństwa i odporności CII, a także poziom wiedzy specjalistycznej i gotowości, są w poszczególnych państwach członkowskich zróżnicowane.

Przyjęcie podejścia wyłącznie w skali krajowej niesie ze sobą ryzyko spowodowania rozdrobnienia i nieefektywności w Europie. Różnice w podejściach krajowych i brak usystematyzowanej współpracy transgranicznej znacznie zmniejszają efektywność krajowych środków zaradczych, ponieważ – między innymi – ze względu na powiązania między CII, niski poziom bezpieczeństwa i odporności CII w jednym kraju może potencjalnie zwiększyć podatność na zagrożenia i stopień ryzyka w innych krajach.

W celu rozwiązania tego problemu konieczne jest podjęcie działań na szczeblu europejskim, które – wspierając zwiększanie świadomości i powszechne zrozumienie charakteru wyzwań, zachęcając do przyjmowania wspólnych celów polityki i priorytetów, wzmacniając współpracę między państwami członkowskimi i wpisując polityki krajowe w bardziej europejskie i globalne ramy – będą stanowić wartość dodaną dla polityk i programów krajowych.

3.4.2. Potrzeba nowego europejskiego modelu zarządzania dla CII

Zwiększenie bezpieczeństwa i odporności CII wiąże się z powstaniem szczególnych problemów dotyczących zarządzania. Choć ostateczną odpowiedzialność za określanie polityki związanej z CII ponoszą państwa członkowskie, jej wdrażanie uzależnione jest od zaangażowania sektora prywatnego, który posiada lub kontroluje dużą liczbę CII. Z drugiej strony, rynki nie zawsze w wystarczającym stopniu zachęcają sektor prywatny do inwestowania w ochronę CII na poziomie odpowiadającym oczekiwaniom rządów.

Aby rozwiązać ten problem dotyczący zarządzania, na szczeblu krajowym pojawiły się jako model odniesienia partnerstwa publiczno-prywatne (PPP). Jednak mimo zgody co do tego, że PPP byłyby również pożądane na szczeblu europejskim, europejskie PPP jak do tej pory jeszcze się nie pojawiły. Za pomocą europejskich wielostronnych ram zarządzania, w których zwiększoną rolę odgrywać może agencja ENISA, można by wspierać zaangażowanie sektora prywatnego w określanie strategicznych celów polityki publicznej oraz priorytetów i środków operacyjnych. Ramy te zapełniłyby lukę między działaniami politycznymi na szczeblu krajowym a rzeczywistą sytuacją operacyjną w terenie.

3.4.3. Ograniczona europejska zdolność wczesnego ostrzegania i reagowania

Mechanizmy zarządzania będą efektywne tylko wtedy, gdy wszyscy uczestnicy będą działać w oparciu o wiarygodne informacje. Ma to szczególne znaczenie dla rządów, które ponoszą ostateczną odpowiedzialność za bezpieczeństwo i dobrobyt obywateli.

Procesy i praktyki dotyczące monitorowania przypadków naruszenia bezpieczeństwa sieci i składania na ten temat sprawozdań są jednak w poszczególnych państwach członkowskich różne. W niektórych nie istnieje organizacja referencyjna pełniąca funkcję punktu monitorującego. Co ważne, współpraca między państwami członkowskimi i wymiana informacji dotyczących wiarygodnych i konkretnych danych na temat przypadków naruszenia

bezpieczeństwa wydaje się być słabo rozwinięta – jest albo nieformalna, albo ogranicza się do wymian dwustronnych lub wielostronnych w ograniczonym zakresie. Ponadto kluczowe znaczenie dla zwiększenia bezpieczeństwa i odporności CII mają symulacje przypadków naruszenia bezpieczeństwa i prowadzenie ćwiczeń sprawdzających zdolność reagowania, w szczególności wtedy, kiedy koncentrują się one na elastycznych strategiach i procesach uwzględniających nieprzewidywalność potencjalnych kryzysów. Ćwiczenia w zakresie bezpieczeństwa cybernetycznego w UE są jeszcze w zalążku. Liczba ćwiczeń przeprowadzanych na szczeblu ponadnarodowym jest bardzo ograniczona. Jak pokazały ostatnie wydarzenia[23], wzajemna pomoc jest kluczowym elementem właściwej reakcji na zakrojone na szeroką skalę zagrożenia i ataki na CII.

Skuteczna europejska zdolność w zakresie wczesnego ostrzegania i reagowania powinna opierać się na sprawnie działających (tzn. posiadających wspólne podstawy w zakresie zdolności) krajowych/rządowych zespołach ds. reagowania kryzysowego w dziedzinie informatycznej (ang. *Computer Emergency Response Team*, CERT). Organy te powinny być krajowymi katalizatorami dla interesów zainteresowanych podmiotów i dla działań podejmowanych w sferze polityki publicznej (w tym działań dotyczących systemów wymiany informacji i ostrzeżeń o zasięgu obejmującym obywateli i MŚP) oraz powinny w efektywny sposób prowadzić współpracę i wymianę informacji na szczeblu transgranicznym, wykorzystując przy tym ewentualnie istniejące już organizacje, takie jak Europejska Grupa Rządowych CERT (ang. *European Governmental CERTs Group*, EGC)[24].

3.4.4. Współpraca międzynarodowa

Wzrost znaczenia Internetu, który jest jedną z kluczowych CII, powoduje, że należy zwrócić szczególną uwagę na jego odporność i stabilność. Dzięki swemu rozproszonemu i redundantnemu charakterowi Internet dał się poznać jako bardzo solidna infrastruktura. Jego fenomenalny rozwój dał jednak początek nowym usługom i zastosowaniom oraz spowodował, że jego fizyczna i logiczna struktura staje się coraz bardziej skomplikowana: kwestionowanie odporności Internetu na coraz większą liczbę zakłóceń i ataków cybernetycznych jest więc uzasadnione.

Rozbieżność opinii na temat znaczenia elementów składowych Internetu częściowo wyjaśnia różnorodność stanowisk przyjmowanych przez rządy na międzynarodowych forach i często sprzeczne opinie dotyczące wagi tej kwestii. Może to utrudnić właściwe zapobieganie zagrożeniom dotyczącym Internetu, przygotowanie się do nich oraz przywrócenie sprawności Internetu w przypadku ich wystąpienia. Przykładowo, konsekwencje przejścia z IPv4 na IPv6 również należy ocenić w kontekście bezpieczeństwa CII.

Internet jest globalną i wysoce rozproszoną siecią sieci, której centra kontroli nie są zawsze zlokalizowane według klucza państwowego. Zapewnienie odporności i stabilności wymaga więc szczególnego, ukierunkowanego podejścia, opartego na dwóch połączonych ze sobą środkach. Pierwszy z nich to osiągnięcie konsensusu w sprawie europejskich priorytetów dotyczących odporności i stabilności Internetu, zarówno w zakresie polityki publicznej, jak i w zakresie działań operacyjnych. Drugi to włączenie społeczności międzynarodowej w opracowanie zestawu zasad dotyczących odporności i stabilności Internetu, zgodnych z podstawowymi europejskimi wartościami i wpisanych w ramy naszego strategicznego dialogu

---

23 http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/large_scale/

24 http://www.egc-group.org/

i współpracy z krajami trzecimi i organizacjami międzynarodowymi. Działania te byłyby konsekwencją uznania kluczowego znaczenia stabilności Internetu na Światowym Szczycie Społeczeństwa Informacyjnego[25].

4. KOLEJNY ETAP: DZIAŁANIA NA RZECZ WIĘKSZEJ KOORDYNACJI I WSPÓŁPRACY NA SZCZEBLU UE

Ze względu na wspólnotowy i międzynarodowy wymiar problemu, zintegrowane podejście UE na rzecz zwiększenia bezpieczeństwa i odporności CII uzupełniłoby i wzbogaciłoby programy krajowe oraz istniejące już dwustronne i wielostronne programy współpracy między państwami członkowskimi.

W wyniku dyskusji poświęconych polityce publicznej przeprowadzonych po wydarzeniach w Estonii uznano, że skutki podobnych ataków można ograniczyć za pomocą środków zapobiegawczych i skoordynowanych działań w trakcie trwania kryzysu. Bardziej usystematyzowana wymiana informacji i dobrych praktyk w obrębie całej UE mogłaby znacznie ułatwić zwalczanie transgranicznych zagrożeń.

Konieczne jest wzmocnienie istniejących już instrumentów współpracy, w tym agencji ENISA, oraz, w razie potrzeby, stworzenie nowych narzędzi. Niezbędne jest przyjęcie wielostronnego i wielopoziomowego podejścia na szczeblu europejskim, które będzie w pełni respektowało i uzupełniało zobowiązania krajowe.

Konieczne jest pełne zrozumienie środowiska i ograniczeń. Przykładowo, zaniepokojenie budzi fakt, że ze względu na rozproszony charakter Internetu, węzły brzegowe mogą być wykorzystane jako wektory ataku, jak ma to miejsce np. w przypadku botnetów. Rozproszony charakter Internetu jest też jednak kluczowym elementem jego stabilności oraz odporności i może pomóc w szybszym odzyskaniu sprawności operacyjnej niż miałoby to miejsce w przypadku przesadnie sformalizowanych, odgórnie sterowanych procedur. Taki stan rzeczy wymaga uważnej, jednostkowej analizy polityk publicznych i procedur operacyjnych, które planuje się wprowadzić w życie.

Ważna jest również kwestia czasu. Konieczne jest natychmiastowe podjęcie działań i szybkie wdrożenie elementów niezbędnych do stworzenia ram, które umożliwią nam reakcję na obecne zagrożenia i które będą się wpisywać w przyszłą strategię dotyczącą bezpieczeństwa sieci i informacji.

W celu rozwiązania tych problemów proponuje się pięć filarów:

(1) gotowość i zapobieganie: zapewnienie gotowości na wszystkich szczeblach;

(2) wykrywanie i reagowanie: zapewnienie odpowiednich mechanizmów wczesnego ostrzegania;

(3) łagodzenie skutków i przywracanie sprawności operacyjnej: wzmocnienie unijnych mechanizmów obronnych dla CII;

---

[25] Program z Tunisu na rzecz społeczeństwa informacyjnego http://www.itu.int/wsis/docs2/tunis/off/6rev1.html

(4) współpraca międzynarodowa: propagowanie priorytetów UE na scenie międzynarodowej;

(5) kryteria dla sektora ICT: wspieranie wdrażania dyrektywy w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej[26].

5. PLAN DZIAŁANIA

5.1. Gotowość i zapobieganie:

Podstawowe zdolności i usługi w zakresie współpracy ogólnoeuropejskiej. Komisja zwraca się do państw członkowskich i zainteresowanych podmiotów, by:

- w ramach wspierania współpracy na szczeblu ogólnoeuropejskim określiły, przy pomocy agencji ENISA, minimalny poziom zdolności i usług w odniesieniu do krajowych/rządowych zespołów CERT i operacji reagowania na przypadki naruszenia bezpieczeństwa;

- zapewniły krajowym/rządowym zespołom CERT status kluczowego elementu krajowej zdolności w zakresie gotowości, wymiany informacji, koordynacji i reagowania.

Cel: porozumienie w sprawie minimalnych standardów do końca 2010 r.; powołanie we wszystkich państwach członkowskich sprawnie działających krajowych/rządowych zespołów CERT do końca 2011 r.

Europejskie partnerstwo publiczno-prywatne na rzecz odporności (ang. *European Public Private Partnership for Resilience* , EP3R). Komisja będzie

- wspierać współpracę między sektorem publicznym a sektorem prywatnym w zakresie celów dotyczących bezpieczeństwa i odporności, podstawowych wymogów, dobrych praktyk i środków politycznych. Działania EP3R będą się w głównej mierze koncentrować na płaszczyźnie europejskiej i będą mieć charakter strategiczny (np. dobre praktyki polityczne) oraz taktyczny/operacyjny (np. udział podmiotów gospodarczych). EP3R powinno stanowić kontynuację i uzupełnienie istniejących już inicjatyw krajowych i działań operacyjnych agencji ENISA.

Cel: opracowanie mapy drogowej i planu dotyczącego EP3R do końca 2009 r.; ustanowienie EP3R do połowy 2010 r.; przedstawienie pierwszych efektów działań EP3R do końca 2010 r.

Europejskie forum wymiany informacji między państwami członkowskimi. Komisja

- ustanowi europejskie forum, w ramach którego państwa członkowskie będą się wymieniać informacjami i dobrymi praktykami politycznymi dotyczącymi bezpieczeństwa i odporności CII. Forum to będzie korzystało z efektów prac innych organizacji, zwłaszcza agencji ENISA.

Cel: zainicjowanie działalności forum do końca 2009 r.; przedstawienie pierwszych efektów działań forum do końca 2010 r.

[26] Dyrektywa Rady 2008/114/WE

5.2. Wykrywanie i reagowanie

Europejski system wymiany informacji i wczesnego ostrzegania (EISAS). Komisja wspiera

rozwój i wdrożenie europejskiego systemu wymiany informacji i wczesnego ostrzegania (ang. *European Information Sharing and Alert System*, EISAS), obejmującego swym zasięgiem obywateli oraz MŚP i opartego na krajowych oraz prywatnych systemach wymiany informacji i wczesnego ostrzegania. Komisja wspiera finansowo dwa uzupełniające się projekty w dziedzinie prototypowania[27]. Do agencji ENISA skierowano prośbę o podsumowanie wyników tych projektów i innych inicjatyw krajowych oraz o przygotowanie mapy drogowej dalszego rozwoju i wdrażania EISAS.

Cel: zakończenie prac nad projektami w dziedzinie prototypowania do końca 2010 r.; opracowanie mapy drogowej EISAS do końca 2010 r.

5.3. Łagodzenie skutków i przywracanie sprawności operacyjnej

Krajowe plany i ćwiczenia awaryjne. Komisja wzywa państwa członkowskie do:

- opracowania krajowych planów awaryjnych i regularnej organizacji ćwiczeń w zakresie reagowania w przypadku zakrojonych na szeroką skalę incydentów zagrażających bezpieczeństwu sieci oraz przywracania sprawności operacyjnej w przypadku awarii, co będzie stanowić krok w kierunku bliższej współpracy ogólnoeuropejskiej. Krajowe/rządowe zespoły CERT/CSIRT mogą otrzymać zadanie przeprowadzania ćwiczeń i testów w zakresie krajowych planów awaryjnych, przy udziale zainteresowanych podmiotów z sektora prywatnego i publicznego. Do agencji ENISA skierowano prośbę o wsparcie procesu wymiany dobrych praktyk pomiędzy państwami członkowskimi.

Cel: przeprowadzenie co najmniej jednego ćwiczenia krajowego w każdym państwie członkowskim do końca 2010 r.

Ogólnoeuropejskie ćwiczenia na wypadek zakrojonych na szeroką skalę incydentów zagrażających bezpieczeństwu sieci . Komisja będzie

- wspierać finansowo prace nad ogólnoeuropejskimi ćwiczeniami na wypadek incydentów zagrażających bezpieczeństwu Internetu[28], które to prace mogą również stanowić platformę operacyjną dla ogólnoeuropejskiego udziału w międzynarodowych ćwiczeniach na wypadek incydentów zagrażających bezpieczeństwu sieci, takich jak amerykańskie ćwiczenia „Cyber Storm".

Cel: opracowanie i przeprowadzenie pierwszego ogólnoeuropejskiego ćwiczenia do końca 2010 r.; ogólnoeuropejski udział w ćwiczeniach międzynarodowych do końca 2010 r.

Zwiększona współpraca między krajowymi/rządowymi zespołami CERT. Komisja wzywa państwa członkowskie do:

---

27 W ramach programu WE „Zapobieganie, gotowość i zarządzanie skutkami w zakresie terroryzmu i innych rodzajów zagrożeń dla bezpieczeństwa" http://ec.europa.eu/justice_home/funding/cips/funding_cips_en.htm

28 *Supra* 27

- zwiększenia współpracy między krajowymi/rządowymi zespołami CERT, również dzięki wykorzystaniu i rozbudowaniu istniejących już mechanizmów współpracy, takich jak np. EGC[29]. Do agencji ENISA skierowano prośbę o aktywne promowanie i wspieranie ogólnoeuropejskiej współpracy między krajowymi/rządowymi zespołami CERT, co powinno zaowocować zwiększoną gotowością, wzmocnieniem zdolności Europy w zakresie reagowania na incydenty zagrażające bezpieczeństwu oraz przeprowadzeniem ćwiczeń w skali ogólnoeuropejskiej (lub regionalnej).

Cel: podwojenie liczby organów krajowych biorących udział w pracach ECG do końca 2010 r.; przygotowanie przez agencję ENISA materiałów referencyjnych wspierających współpracę na szczeblu ogólnoeuropejskim do końca 2010 r.

5.4. Współpraca międzynarodowa

Odporność i stabilność Internetu. Przewiduje się trzy uzupełniające się działania:

- Europejskie priorytety dotyczące długoterminowej odporności i stabilności Internetu. Komisja przeprowadzi ogólnoeuropejską debatę z udziałem wszystkich zainteresowanych podmiotów publicznych i prywatnych, której celem będzie określenie priorytetów UE dotyczących długoterminowej odporności i stabilności Internetu.

Cel: określenie priorytetów UE w zakresie kluczowych elementów i problemów dotyczących Internetu do końca 2010 r.

- Zasady i wytyczne dotyczące odporności i stabilności Internetu (na szczeblu europejskim). Komisja będzie współpracować z państwami członkowskimi nad określeniem wytycznych dotyczących odporności i stabilności Internetu, biorąc pod uwagę między innymi regionalne działania naprawcze, porozumienia o wzajemnej pomocy, skoordynowane strategie przywracania sprawności operacyjnej i zapewniania ciągłości usług, geograficzne rozmieszczenie krytycznych zasobów internetowych, zabezpieczenia technologiczne w architekturze i protokołach internetowych oraz powielanie i różnorodność usług i danych. Komisja finansuje już grupę zadaniową ds. odporności protokołu DNS, która, przy udziale innych stosownych projektów, pomoże osiągnąć konsensus[30].

Cel: opracowanie mapy drogowej dla zasad i wytycznych dotyczących odporności i stabilności Internetu do końca 2009 r.; osiągnięcie porozumienia w sprawie pierwszej wersji zasad i wytycznych do końca 2010 r.

- Zasady i wytyczne dotyczące odporności i stabilności Internetu (na szczeblu światowym). Komisja będzie współpracować z państwami członkowskimi nad mapą drogową dotyczącą wspierania zasad i wytycznych na szczeblu światowym. Rozwijana będzie strategiczna współpraca z krajami trzecimi, zwłaszcza w formie dialogów na rzecz społeczeństwa informacyjnego, która posłuży do osiągnięcia konsensusu na szczeblu światowym[31].

Cel: opracowanie mapy drogowej dla współpracy międzynarodowej w dziedzinie zasad i wytycznych dotyczących bezpieczeństwa i odporności Internetu do początku 2010 r.;

---

29 *Supra* 24
30 *Supra* 27
31 COM(2008) 588 wersja ostateczna

przeprowadzenie do końca 2010 r. dyskusji nad pierwszą, zaakceptowaną na szczeblu międzynarodowym wersją zasad i wytycznych z krajami trzecim i na stosownych forach, w tym na Forum Zarządzania Internetem.

Ćwiczenia w skali światowej obejmujące przywracanie sprawności operacyjnej i łagodzenie skutków zakrojonych na szeroką skalę incydentów zagrażających bezpieczeństwu Internetu. Komisja wzywa europejskie zainteresowane podmioty do:

- zastanowienia się nad praktycznym sposobem rozszerzenia w skali światowej ćwiczeń przeprowadzanych w ramach filaru poświęconego łagodzeniu skutków i przywracaniu sprawności operacyjnej, tak aby były one uzupełnieniem regionalnych planów awaryjnych i zdolności reakcji.

Cel: przygotowanie przez Komisję ram i mapy drogowej w celu wsparcia zaangażowania i udziału Europy w światowych ćwiczeniach obejmujących przywracanie sprawności operacyjnej i łagodzenie skutków zakrojonych na szeroką skalę incydentów zagrażających bezpieczeństwu Internetu.

5.5. Kryteria rozpoznawania europejskich infrastruktur krytycznych w sektorze ICT

Kryteria dotyczące sektora ICT. Opierając się na wstępnych działaniach przeprowadzonych w 2008 r., Komisja będzie

- w dalszym ciągu pracować, wspólnie z państwami członkowskimi i wszystkimi zainteresowanymi podmiotami, nad określeniem kryteriów rozpoznawania europejskich infrastruktur krytycznych w sektorze ICT. Informacje niezbędne do tego celu będą pochodzić z przeprowadzanej obecnie specjalnej analizy[32].

Cel: określenie przez Komisję do końca pierwszej połowy 2010 r. kryteriów rozpoznawania europejskich infrastruktur krytycznych w sektorze ICT.

6. WNIOSKI

Bezpieczeństwo i odporność CII stanowią pierwszą linię obrony w przypadku awarii i ataków. Wzmocnienie bezpieczeństwa i odporności CII w całej UE jest niezbędne do tego, by w pełni odnieść korzyści płynące ze społeczeństwa informacyjnego. Aby osiągnąć ten ambitny cel proponuje się plan działania, mający na celu zwiększenie taktycznej i operacyjnej współpracy na szczeblu europejskim. Sukces tych działań zależy od ich efektywności w zakresie wykorzystywania i wspomagania działań sektora publicznego i prywatnego oraz od zaangażowania i pełnego udziału państw członkowskich, instytucji europejskich i zainteresowanych podmiotów.

W związku z tym w dniach 27–28 kwietnia 2009 r. zorganizowana zostanie konferencja ministerialna, której celem będzie omówienie zaproponowanych inicjatyw z państwami członkowskimi i potwierdzenie ich zaangażowania w debatę na temat unowocześnionej i wzmocnionej polityki dotyczącej NIS w Europie.

---

[32] *Supra* 27

Ponieważ zwiększenie bezpieczeństwa i odporności CII jest celem długoterminowym, związana z nim strategia i środki wymagają regularnej oceny. Z tego względu – a także ponieważ cel ten jest zgodny z ogólną debatą na temat przyszłej strategii dotyczącej bezpieczeństwa sieci i informacji w UE po 2012 r. – pod koniec 2010 r. Komisja rozpocznie procedurę przeglądu, której celem będzie ocena pierwszej fazy działań oraz w razie konieczności określenie i zaproponowanie dalszych środków.