KOMISJA WSPÓLNOT EUROPEJSKICH

Bruksela, dnia 31.5.2006
KOM(2006) 251 wersja ostateczna

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

Strategia na rzecz bezpiecznego społeczeństwa informacyjnego – „Dialog, partnerstwo i przejmowanie inicjatywy”

{SEC(2006) 656}

SPIS TREŚCI

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

Strategia na rzecz bezpiecznego społeczeństwa informacyjnego – „Dialog, partnerstwo i przejmowanie inicjatywy"

1. WPROWADZENIE

W komunikacie „i2010 – Europejskie społeczeństwo informacyjne na rzecz wzrostu i zatrudnienia"[1] podkreślono wagę bezpieczeństwa sieci i informacji dla utworzenia jednolitej europejskiej przestrzeni informacyjnej. Dostępność, niezawodność oraz bezpieczeństwo sieci i systemów informatycznych nabierają kluczowego znaczenia dla gospodarek naszych krajów oraz dla społeczeństwa.

Celem niniejszego komunikatu jest ożywienie strategii Komisji Europejskiej z 2001 r., zawartej w komunikacie „Bezpieczeństwo sieci i informacji: Propozycje na rzecz europejskiego podejścia"[2]. Zawarto w nim przegląd obecnych zagrożeń dla bezpieczeństwa społeczeństwa informacyjnego oraz określono dodatkowe kroki, które należy podjąć w celu poprawy bezpieczeństwa sieci i informacji.

Ambitnym zamierzeniem jest dalszy rozwój dynamicznej, globalnej strategii europejskiej, opartej o kulturę bezpieczeństwa oraz o **dialog, partnerstwo i przejmowanie inicjatywy,** przy wykorzystaniu doświadczeń zgromadzonych zarówno przez Państwa Członkowskie, jak i na szczeblu Wspólnoty Europejskiej.

Podejmując wyzwania dotyczące bezpieczeństwa społeczeństwa informacyjnego, Wspólnota Europejska opracowała podejście nakierowane na trzy elementy: szczególne środki związane z bezpieczeństwem sieci i informacji, ramy regulacyjne dla łączności elektronicznej (w tym zagadnienia dotyczące ochrony prywatności i ochrony danych) oraz zwalczanie przestępczości internetowej. Chociaż każdym z tych trzech aspektów można zajmować się osobno, ze względu na liczne współzależności potrzebna jest jedna skoordynowana strategia. W niniejszym komunikacie określono tę strategię oraz przedstawiono ramy realizacji i dalszego rozwoju spójnego podejścia do bezpieczeństwa sieci i informacji.

Komunikat z 2001 r. definiuje bezpieczeństwo sieci i informacji jako „*zdolność sieci lub systemu informatycznego do oparcia się, w określonym stopniu, skutkom przypadkowych zdarzeń lub złośliwych działań obniżających dostępność, autentyczność, integralność i poufność przechowywanych lub przekazywanych danych oraz związanych z nimi usług oferowanych lub udostępnianych poprzez te sieci lub systemy*". W ostatnich latach Wspólnota Europejska przeprowadziła szereg działań związanych z poprawą bezpieczeństwa sieci i informacji.

Ramy regulacyjne dla łączności elektronicznej, które są obecnie przedmiotem przeglądu, zawierają przepisy związane z bezpieczeństwem. W szczególności dyrektywa o ochronie

---

[1] COM(2005) 229 wersja ostateczna z 1.6.2005 r.

[2] COM(2001) 298 wersja ostateczna z 6.6.2001 r.

prywatności i łączności elektronicznej[3] zobowiązuje dostawców publicznie dostępnych usług łączności elektronicznej do zagwarantowania bezpieczeństwa świadczonych usług. Ustanowiono przepisy przeciwko spamowi[4] oraz programom typu spyware[5].

Zaufanie i bezpieczeństwo są również istotną częścią programów rozwojowo-badawczych Wspólnoty Europejskiej. Kwestie te zostały uwzględnione w szeregu projektów szóstego Programu Ramowego na rzecz badań i rozwoju. Badania związane z bezpieczeństwem zostaną zintensyfikowane w trakcie realizacji siódmego Programu Ramowego dzięki powołaniu europejskiego programu badań nad bezpieczeństwem (European Security Research Programme)[6]. Ponadto program Safer Internet Plus wspiera projekty sieciowe oraz wymianę sprawdzonych rozwiązań w zakresie zwalczania szkodliwych treści krążących w sieciach informatycznych.

W odpowiedzi na zagrożenia dla bezpieczeństwa Wspólnota Europejska postanowiła w 2004 r. utworzyć Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji (ENISA). ENISA przyczynia się do rozwoju kultury bezpieczeństwa sieci i informacji, przynosząc korzyści obywatelom, konsumentom, przedsiębiorstwom oraz instytucjom sektora publicznego w Unii Europejskiej.

UE odgrywa również aktywna role na arenie międzynarodowej poruszając te tematy miedzy innymi na forum OECD, Rady Europy czy ONZ. Na Światowym Szczycie Społeczeństwa Informacyjnego w Tunisie UE zdecydowanie poparła dyskusje nad dostępnością, niezawodnością i bezpieczeństwem sieci i informacji. W programie z Tunisu[7], który wraz ze zobowiązaniami z Tunisu wytycza dalsze kroki w debacie politycznej poświęconej globalnemu Społeczeństwu Informacyjnemu poparte przez światowych przywódców, podkreślono potrzebę dalszego zwalczania przestępczości internetowej i spamu przy jednoczesnym zapewnieniu ochrony prywatności i wolności wypowiedzi. Wyrażono w nim również potrzebę porozumienia w zakresie zagadnień związanych z bezpieczeństwem Internetu oraz dalszej współpracy nad gromadzeniem i rozpowszechnianiem informacji związanych z bezpieczeństwem, a także wymiany między zainteresowanymi podmiotami sprawdzonych rozwiązań w zakresie walki z zagrożeniami dla bezpieczeństwa.

2. POPRAWA BEZPIECZEŃSTWA SPOŁECZEŃSTWA INFORMACYJNEGO: GŁÓWNE WYZWANIA

Mimo działań podejmowanych na poziomie międzynarodowym, europejskim i krajowym kwestia bezpieczeństwa nadal stanowi poważne wyzwanie.

Po pierwsze, ataki na systemy informatyczne są coraz częściej powodowane chęcią zysku, a nie wyłącznie pragnieniem zakłócenia pracy systemu. Dane są nielegalnie eksplorowane, coraz częściej bez wiedzy użytkowników, a liczba wersji (i tempo rozwoju) szkodliwego

---

3 Dyrektywa 2002/58/WE.

4 czyli niezamówionym informacjom reklamowym.

5 Spyware to oprogramowanie szpiegujące, instalowane bez odpowiedniej wiedzy, zgody lub kontroli użytkownika.

6 Program ten jest przygotowywany w ramach działania przygotowawczego na rzecz badań nad bezpieczeństwem w latach 2004-2006.

7 *Ku globalnemu partnerstwu w społeczeństwie informacyjnym - Kontynuacja drugiej fazy Światowego Szczytu Społeczeństwa Informacyjnego*, COM(2006) 181 wersja ostateczna z 27.4.2006 r.

oprogramowania (malware)[8] szybko wzrasta. Dobrym przykładem takiej ewolucji jest spam, który staje się nośnikiem wirusów i narzędziem oszustw lub działań przestępczych, takich jak stosowanie programów wywiadowczych (spyware), oszustwa mające na celu wyłudzenie cennych informacji (phishing)[9] i inne formy szkodliwego oprogramowania. Ich szerokie rozpowszechnienie coraz bardziej opiera się na sieciach „botów",[10] tj. serwerach i komputerach osobistych, nad którymi przejęto kontrolę w celu użycia ich jako przekaźniki bez wiedzy użytkowników.

Coraz szersze zastosowanie urządzeń przenośnych (w tym telefonów komórkowych 3G, przenośnych gier wideo itd.) oraz usług sieciowych opartych na urządzeniach przenośnych będzie wiązać się z nowymi wyzwaniami ze względu na szybki rozwój usług opartych na protokole IP. W ostatecznym rozrachunku mogą się one okazać bardziej powszechną drogą ataków niż komputery osobiste, gdyż te ostatnie już dziś charakteryzuje wysoki poziom bezpieczeństwa. W istocie wszystkie nowe formy platform komunikacyjnych i systemów informatycznych w sposób stwarzają nowe możliwości dla złośliwych ataków.

Innym ważnym procesem jest nadejście ery „inteligentnego otoczenia", której inteligentne urządzenia oparte na technologiach komputerowych i sieciowych staną się wszechobecne (np. poprzez technologie RFID[11], IPv6 i sieci sensorów). Życie codzienne umożliwiające swobodne wzajemne łączenie się i przekazywanie danych między sieciami oferuje szerokie możliwości. Z drugiej jednak strony będzie wiązać się również z dodatkowym ryzykiem w zakresie bezpieczeństwa i ochrony prywatności. Mimo iż powszechnie używane platformy i aplikacje pozytywnie wpływają na interoperacyjność oraz popyt na technologie teleinformatyczne, mogą one również powodować wzrost ryzyka. Przykładowo, im szersze wykorzystanie oprogramowania standardowego, tym większe ryzyko naruszenia ochrony w przypadku wykrycia słabych punktów lub wystąpienia błędów. Powstawanie określonych „monokultur" w obrębie platform oprogramowania i aplikacji może znacznie przyczynić się do zwiększenia i rozprzestrzenienia się zagrożeń dla bezpieczeństwa, takich jak aplikacje typu malware i wirusy. **Różnorodność, otwartość i interoperacyjność stanowią integralne elementy bezpieczeństwa i należy je wspierać**.

Znaczenie teleinformatyki dla europejskiej gospodarki i społeczeństwa jako całości jest bezsporne. Technologie teleinformatyczne są kluczowym elementem innowacyjności i odpowiadają za niemal 40 % wzrostu wydajności. Ponadto sektor ten, cechujący się wysokim poziomem nowatorskich rozwiązań, pochłania ponad jedną czwartą całkowitych europejskich nakładów na prace badawczo-rozwojowe. Pełni on również kluczową rolę w zapewnieniu wzrostu gospodarczego i nowych miejsc pracy w całej gospodarce. Coraz więcej Europejczyków żyje w prawdziwym społeczeństwie opartym na informacji, w którym nastąpiło szybkie zwiększenie wykorzystania technologii teleinformatycznych stanowiących kluczowy element stosunków społeczno-gospodarczych. Eurostat podaje, że 89 % przedsiębiorstw na obszarze Wspólnoty aktywnie korzystało z Internetu w 2004 r., a około 50 % konsumentów korzystało w ostatnim czasie z Internetu[12].

---

8 Malware (ang. „malicious software") oznacza szkodliwe oprogramowanie.

9 Phishing jest formą oszustwa internetowego mającego na celu kradzież cennych informacji, takich jak numery kart kredytowych i rachunków bankowych oraz nazwy i hasła użytkowników.

10 Sieć botów (ang. „botnet") to sieć aplikacji przejmujących zdalną kontrolę nad komputerem, zainstalowanych potajemnie na komputerze ofiary.

11 Sposób identyfikacji za pomocą fal radiowych (ang. Radio Frequency Identification).

12 Eurostat, *Internet activities in the European Union* (Internet w Unii Europejskiej), 40/2005.

Naruszenie bezpieczeństwa sieci i informacji może mieć skutki wykraczające poza wymiar gospodarczy. W istocie, powszechne są obawy, że problemy bezpieczeństwa mogą zniechęcić użytkowników i zmniejszyć popyt na technologie teleinformatyczne, podczas gdy dostępność, niezawodność i bezpieczeństwo są niezbędnym warunkiem zapewnienia ochrony praw podstawowych w Internecie.

Ponadto z uwagi na coraz większe zależności pomiędzy sieciami, również inne kluczowe infrastruktury (takie jak transport, energetyka itp.) stają się coraz bardziej zależne od integralności stosownych systemów informatycznych.

Zarówno przedsiębiorcy, jak i obywatele w Europie nadal lekceważą ryzyko. Ma to wiele przyczyn, jednak w przypadku przedsiębiorstw wynika to głównie z tego, że w niewielkim stopniu uświadamiają sobie one zwrot z inwestycji w rozwiązania w zakresie bezpieczeństwa, a w przypadku obywateli z faktu, że nie są świadomi swej odpowiedzialności w globalnym łańcuchu bezpieczeństwa.

Biorąc pod uwagę wszechobecność technologii teleinformatycznych i systemów informatycznych, bezpieczeństwo sieci i informacji stanowi wyzwanie dla wszystkich:

- **Jednostki administracji publicznej** powinni zająć się kwestią bezpieczeństwa swoich systemów, nie tylko w celu ochrony informacji sektora publicznego, ale także by służyć innym dobrym przykładem ;

- **Przedsiębiorcy** powinni postrzegać bezpieczeństwo sieci i informacji bardziej jako atut i element przewagi konkurencyjnej niż w kategorii kosztów;

- **Użytkownicy indywidualni** powinni zrozumieć, że ich domowe systemy mają zasadnicze znaczenie dla całego „łańcucha bezpieczeństwa”.

Aby z powodzeniem stawić czoła problemom opisanym powyżej, wszystkie zainteresowane podmioty muszą dysponować wiarygodnymi danymi na temat incydentów i tendencji związanych z bezpieczeństwem informacji. Jednak z wielu powodów wiarygodne i wyczerpujące dane na temat takich incydentów są trudne do zdobycia, począwszy od szybkości rozprzestrzeniania się takich zdarzeń, a skończywszy na niechęci niektórych podmiotów do ujawniania i upubliczniania przypadków naruszenia bezpieczeństwa. Mimo wszystko jednym z kamieni węgielnych rozwoju kultury bezpieczeństwa jest **zwiększenie naszej wiedzy na temat problemu**.

Ważne jest, by programy uświadamiające wagę zagrożeń bezpieczeństwa nie zachwiały zaufania konsumentów i użytkowników poprzez skupianie się wyłącznie na negatywnych aspektach bezpieczeństwa. Z tego względu i w miarę możliwości, **bezpieczeństwo sieci i informacji należy przedstawiać raczej jako zaletę i szansę** niż obciążenie i koszty. Musi być ono postrzegane jako atut w budowaniu zaufania konsumentów, element przewagi konkurencyjnej dla przedsiębiorstw zajmujących się obsługą systemów informatycznych oraz kwestia jakości usług zarówno dla usługodawców z sektora publicznego, jak i prywatnego.

Głównym wyzwaniem dla decydentów politycznych jest wypracowanie kompleksowego podejścia, uznającego stosowne role różnych zainteresowanych podmiotów. Musi ono zapewnić odpowiednią koordynację całej gamy posunięć politycznych oraz przepisów prawa, które w sposób bezpośredni lub pośredni wpływają na bezpieczeństwo sieci i informacji. Procesy liberalizacji, deregulacji i konwergencji spowodowały zwiększenie różnorodności

uczestników wśród rozmaitych grup zainteresowanych stron, co czyni zadania łatwiejszym. ENISA może w znaczącym stopniu przyczynić się do osiągnięcia tego celu. Może służyć jako centrum wymiany informacji, współpracy pomiędzy wszystkimi zainteresowanymi stronami oraz wymiany godnych polecenia rozwiązań, zarówno w Europie, jak i we współpracy z innymi państwami na świecie, tak aby przyczynić się do wzrostu konkurencyjności sektora teleinformatycznego oraz osiągnięcia sprawnego rynku wewnętrznego.

3. W KIERUNKU DYNAMICZNEGO PODEJŚCIA DO BEZPIECZNEGO SPOŁECZEŃSTWA INFORMACYJNEGO

Bezpieczne społeczeństwo informacyjne musi opierać się na **zwiększonym bezpieczeństwie sieci i informacji** oraz powszechnej **kulturze bezpieczeństwa**. W tym celu Komisja Europejska proponuje **dynamiczne, zintegrowane podejście** obejmujące wszystkie zainteresowane podmioty, oparte na **dialogu, partnerstwie i przejmowaniu inicjatywy**. Biorąc pod uwagę wzajemne uzupełnianie się sektora publicznego i prywatnego w tworzeniu kultury bezpieczeństwa, inicjatywy związane z polityką w tej dziedzinie muszą być oparte na **otwartym dialogu obejmującym szereg zainteresowanych podmiotów.**

Podejście to i powiązane z nim działania stanowić będą uzupełnienie oraz rozszerzenie powziętego przez Komisję planu kontynuacji i rozbudowy całościowej i dynamicznej polityki, na której realizację składa się szereg inicjatyw przewidzianych na 2006 r.:

(1) opracowanie komunikatu dotyczącego szczegółowych zagadnień związanych z rozwojem spamu i zagrożeń takich jak programy typu spyware i inne rodzaje szkodliwego oprogramowania;

(2) opracowanie propozycji poprawy współpracy między organami odpowiedzialnymi za egzekwowanie prawa oraz reakcji na nowe formy działalności przestępczej z użyciem Internetu, pogarszających funkcjonowanie infrastruktury krytycznej. Zagadnienia te będą przedmiotem oddzielnego komunikatu dotyczącego przestępczości internetowej.

Te inicjatywy polityczne stanowią również uzupełnienie działań planowanych dla osiągnięcia celów Zielonej księgi w sprawie europejskiego programu ochrony infrastruktury krytycznej (EPCIP)[13], opracowanej w odpowiedzi na wniosek Rady z grudnia 2004 r. Proces związany z Zieloną księgą prawdopodobnie doprowadzi do powstania planu działań łączącego kompleksowe podejście do ochrony infrastruktury krytycznej z konieczną polityką uwzględniającą potrzeby poszczególnych sektorów, w tym sektora teleinformatycznego. Przedmiotem szczegółowej polityki dla sektora teleinformatycznego byłoby przeanalizowanie, w drodze **dialogu obejmującego wiele zainteresowanych stron**, odpowiednich czynników gospodarczych, biznesowych i społecznych w celu zwiększenia bezpieczeństwa oraz odporności sieci i systemów informatycznych.

Ponadto w 2006 r. w ramach przeglądu ram regulacyjnych dla łączności elektronicznej zostaną uwzględnione elementy poprawy bezpieczeństwa sieci i informacji, tj. środki techniczne i organizacyjne podejmowane przez operatorów, przepisy związane z powiadamianiem o przypadkach naruszenia bezpieczeństwa oraz szczegółowe działania naprawcze i kary związane z niedotrzymaniem zobowiązań.

---

[13] COM(2005) 576 wersja ostateczna z 17.11.2005 r.

Dostarczanie użytkownikom rozwiązań, usług i produktów związanych z bezpieczeństwem to przede wszystkim zadanie dla sektora prywatnego. Z tego względu niezwykle istotne jest, by **przemysł europejski był zarówno wymagającym użytkownikiem, jak i konkurencyjnym dostawcą** produktów i usług związanych z bezpieczeństwem.

Rządy krajowe muszą być w stanie określić i wdrożyć najlepsze rozwiązania w zakresie tworzenia polityki, a także wykazać zaangażowanie w realizację tych celów polityki poprzez administrowanie własnymi systemami informatycznymi w sposób bezpieczny. Organy władzy publicznej w państwach członkowskich i na szczeblu UE mają do odegrania kluczową rolę we właściwym informowaniu użytkowników, tak by mogli oni przyczynić się do poprawy własnego bezpieczeństwa. Priorytetem powinno być zwiększanie wiedzy na temat zagadnień związanych z bezpieczeństwem sieci i informacji oraz odpowiednie i terminowe informowanie na temat zagrożeń, ryzyka, ostrzeżeń oraz najlepszych rozwiązań za pośrednictwem portali poświęconych bezpieczeństwu sieci elektronicznych. W tym celu należy zbadać możliwość stworzenia **europejskiego wielojęzycznego systemu ostrzegania i wymiany informacji**, który polegałby na połączeniu i wykorzystaniu istniejących lub planowanych inicjatyw publicznych lub prywatnych, co mogłoby stanowić ważny cel dla ENISA.

Globalny wymiar bezpieczeństwa sieci i informacji stanowi dla Komisji ważne wyzwanie, zarówno na poziomie międzynarodowym, jak i w przypadku współpracy z państwami członkowskimi, do zwiększenia wysiłków we **wspieraniu globalnej współpracy nad bezpieczeństwem sieci i informacji**, przede wszystkim poprzez realizację planu przyjętego na Światowym Szczycie Społeczeństwa Informacyjnego w listopadzie 2005 r.

Prace badawczo-rozwojowe, w szczególności na poziomie UE, również pomogą stworzyć nowatorskie partnerstwa na rzecz szybszego rozwoju całej europejskiej branży teleinformatycznej, a w szczególności jej podsektorów związanych z bezpieczeństwem. Z tego względu Komisja będzie dążyć do zapewnienia odpowiednich środków finansowych na badania nad bezpieczeństwem sieci i informacji oraz niezawodnymi technologiami, prowadzone w ramach siódmego programu ramowego UE.

3.1. Dialog

3.1.1. *Jako pierwszy krok do intensyfikacji dialogu między organami publicznymi Komisja proponuje rozpocząć działanie polegające na **analizie porównawczej krajowych polityk związanych z bezpieczeństwem sieci i informacji**, włącznie ze szczegółową polityką bezpieczeństwa dla sektora publicznego. Działanie to pozwoli określić najbardziej skuteczne rozwiązania celem ich upowszechnienia w całej UE i uczynić z administracji krajowych kluczowe podmioty wspierające sprawdzone rozwiązania w dziedzinie bezpieczeństwa. Prace nad identyfikacją elektroniczną, prowadzone np. w ramach przyjętego ostatnio planu działania na rzecz administracji elektronicznej, mogą odegrać pod tym względem ważną rolę.*

Pod warunkiem odpowiedniego przeprowadzenia, wyniki takiej analizy porównawczej pozwolą **określić najlepsze rozwiązania w zakresie informowania MŚP oraz obywateli o konieczności** zwrócenia uwagi na ich własne potrzeby i wyzwania związane z bezpieczeństwem sieci i informacji oraz o tym, że są w stanie zająć się tą kwestią. ENISA powinna odgrywać aktywną rolę w tym dialogu oraz w gromadzeniu i wymianie najlepszych rozwiązań.

*3.1.2. Istnieje potrzeba zorganizowania **usystematyzowanej debaty obejmującej wiele zainteresowanych podmiotów**, dotyczącej najlepszego wykorzystania istniejących narzędzi i instrumentów regulacyjnych w celu uzyskania odpowiedniej równowagi społecznej między bezpieczeństwem a ochroną podstawowych praw, w tym prawa do prywatności. Wkład w tę debatę zapewni planowana konferencja „i2010 – Towards a Ubiquitous European Information Society", organizowana przez zbliżającą się prezydencję fińską, oraz konsultacje dotyczące bezpieczeństwa i wpływu identyfikacji radiowej RFID na prywatność, stanowiące część szerszych konsultacji rozpoczętych niedawno przez Komisję. Ponadto Komisja zorganizuje:*

- spotkanie z przedstawicielami świata biznesu, którego celem będzie stymulowanie zaangażowania branży w przyjęcie skutecznych koncepcji wdrożenia kultury bezpieczeństwa **w branży**;

- seminarium poświęcone sposobom zwiększania świadomości na temat bezpieczeństwa oraz zwiększenia zaufania **użytkowników** do korzystania z sieci elektronicznych i systemów informatycznych.

3.2. Partnerstwo

*3.2.1. Do skutecznego tworzenia polityki potrzebne jest jasne zrozumienie charakteru oraz zakresu wyzwań. Oznacza to nie tylko konieczność posiadania wiarygodnych i aktualnych danych statystycznych i ekonomicznych na temat przypadków naruszenia bezpieczeństwa informatycznego oraz poziomu zaufania konsumentów i użytkowników, lecz również aktualnych danych o wielkości i tendencjach w części europejskiej branży teleinformatycznej zajmującej się bezpieczeństwem. Komisja zamierza poprosić agencję ENISA o budowanie **opartego na zaufaniu partnerstwa z państwami członkowskimi i zainteresowanymi podmiotami** w celu opracowania **odpowiednich ram dla gromadzenia danych**, włącznie z procedurami i mechanizmami gromadzenia i analizy danych na temat incydentów związanych z bezpieczeństwem oraz poziomu zaufania konsumentów w całej UE.*

Jednocześnie z uwagi na znaczne rozdrobnienie rynku w UE i jego dość specyficzny charakter, Komisja zaprosi państwa członkowskie, podmioty sektora prywatnego i środowisko naukowe do **utworzenia strategicznego partnerstwa** na rzecz zapewnienia dostępności danych z części sektora teleinformatycznego zajmującej się bezpieczeństwem oraz danych na temat rozwoju tendencji rynkowych w odniesieniu do produktów i usług w UE.

3.2.2. W celu poprawy europejskiej zdolności reagowania na zagrożenia dla bezpieczeństwa sieci Komisja poprosi agencję ENISA o przeprowadzenie badania ***wykonalności europejskiego systemu wymiany informacji i ostrzegania*** *służącego ułatwieniu podejmowania skutecznych działań w obliczu istniejących i pojawiających się zagrożeń dla sieci elektronicznych. Wymaganym elementem takiego systemu byłby* ***wielojęzyczny portal UE*** *dostarczający konkretnych informacji o zagrożeniach, ryzyku i ostrzeżeniach.*

3.3. Przejmowanie inicjatywy

W kontekście wspierania bezpieczeństwa sieci i informacji warunkiem wstępnym zwiększania świadomości na temat potrzeb i ryzyka jest przejęcie inicjatywy przez każdą grupę zainteresowanych podmiotów.

3.3.1. Mając to na uwadze, Komisja zaprasza ***państwa członkowskie*** *do:*

- aktywnego uczestnictwa w proponowanej analizie porównawczej krajowych polityk w zakresie bezpieczeństwa sieci i informacji;
- wspierania, w ścisłej współpracy z agencją ENISA, kampanii informacyjnych poświęconych zaletom, korzyściom i pozytywnym aspektom przyjęcia skutecznych technologii, rozwiązań i sposobów działania związanych z bezpieczeństwem;
- wykorzystywania wdrożonych elektronicznych usług administracji we wspieraniu dobrych praktyk i przekazywaniu odpowiednich informacji w dziedzinie bezpieczeństwa, które można by później rozszerzyć na inne sektory;
- stymulowania rozwoju programów dotyczących bezpieczeństwa sieci i informacji poprzez włączenie ich do programów kształcenia wyższego.

3.3.2. Komisja zaprasza również zainteresowane podmioty z ***sektora prywatnego*** *do podejmowania działań związanych z:*

- opracowaniem odpowiedniej definicji obowiązków producentów oprogramowania i dostawców usług internetowych dotyczących zapewnienia właściwego i możliwego do skontrolowania poziomu bezpieczeństwa. W tym zakresie potrzebne jest wsparcie w opracowaniu ustandaryzowanych procesów, spełniających powszechnie uznane normy bezpieczeństwa i zasady wynikające ze sprawdzonych rozwiązań;
- wspieraniem różnorodności, otwartości, interoperacyjności, użyteczności i konkurencji jako czynników kluczowych dla bezpieczeństwa oraz stymulowanie wdrażania produktów, procesów i usług zwiększających bezpieczeństwo, w celu zapobiegania kradzieżom tożsamości i innym atakom na prywatność oraz w celu ich zwalczania;
- upowszechnianiem sprawdzonych rozwiązań w zakresie bezpieczeństwa wśród operatorów sieci, dostawców usług oraz MŚP jako punktu odniesienia dla zapewnienia bezpieczeństwa i ciągłości funkcjonowania przedsiębiorstwa;

- wspieraniem programów szkoleniowych wśród przedsiębiorstw, w szczególności MŚP, w celu zapewnienia pracownikom wiedzy i umiejętności niezbędnych do skutecznego stosowania rozwiązań w dziedzinie bezpieczeństwa;

- pracami nad stworzeniem przystępnych cenowo systemów certyfikacji bezpieczeństwa produktów, procesów i usług, dopasowanych do konkretnych potrzeb UE (w szczególności w odniesieniu do prywatności);

- zaangażowaniem sektora ubezpieczeń w opracowanie odpowiednich narzędzi i metod zarządzania ryzykiem w odniesieniu do rodzajów ryzyka związanego z technologiami teleinformatycznymi oraz rozwojem kultury zarządzania ryzykiem w organizacjach i przedsiębiorstwach (w szczególności MŚP).

4. WNIOSKI

Zdefiniowanie wyzwań związanych z bezpieczeństwem sieci i systemów informatycznych w UE oraz stawienie im czoła wymaga pełnego zaangażowania wszystkich zainteresowanych podmiotów. Podejście zaproponowanie w niniejszym komunikacie zmierza do tego celu poprzez zaakcentowanie **zaangażowania wielu zainteresowanych podmiotów**. Oznacza ono rozwój w oparciu o wspólne interesy, określenie odpowiednich ról i opracowanie dynamicznych ram dla skutecznego tworzenia polityki społecznej i inicjatyw sektora prywatnego.

W połowie 2007 r. Komisja sporządzi sprawozdanie dla Rady i Parlamentu dotyczące rozpoczętych działań, wstępnych wyników i stanu realizacji poszczególnych inicjatyw, włącznie z inicjatywami agencji ENISA oraz podjętymi na poziomie państw członkowskich i w sektorze prywatnym. Jeżeli okaże się to stosowne, Komisja zaproponuje zalecenie dotyczące bezpieczeństwa sieci i informacji.