Opinia Europejskiego Komitetu Ekonomiczno-Społecznego w sprawie ataków cybernetycznych w UE

(opinia z inicjatywy własnej)

(2014/C 451/05)

Sprawozdawca: **Thomas McDONOGH**

Dnia 27 lutego 2014 r. Europejski Komitet Ekonomiczno-Społeczny postanowił, zgodnie z art. 29 ust. 2 regulaminu wewnętrznego, sporządzić opinię z inicjatywy własnej w sprawie

ataków cybernetycznych w UE.

Sekcja Transportu, Energii, Infrastruktury i Społeczeństwa Informacyjnego, której powierzono przygotowanie prac Komitetu w tej sprawie, przyjęła swoją opinię 18 czerwca 2014 r.

Na 500. sesji plenarnej w dniach 9–10 lipca 2014 r. (posiedzenie z 10 lipca) Europejski Komitet Ekonomiczno-Społeczny stosunkiem głosów 135 do 1 – nikt nie wstrzymał się od głosu – przyjął następującą opinię:

1. **Wnioski i zalecenia**

1.1 Komitet zaleca utworzenie unijnego organu ds. bezpieczeństwa cybernetycznego, na podobieństwo centralnego organu w lotnictwie, jakim jest Europejska Agencja Bezpieczeństwa Lotniczego (EASA), aby zapewnić silne przywództwo na poziomie UE konieczne do zajęcia się złożonym wdrażaniem skutecznej polityki bezpieczeństwa cybernetycznego na szczeblu europejskim.

1.2 Dobrze poinformowani i świadomi obywatele mają kluczowe znaczenie dla solidnego bezpieczeństwa cybernetycznego w Europie. Kształcenie obywateli w dziedzinie bezpieczeństwa cybernetycznego i ochrony danych osobowych powinno stanowić istotną część szkolnych programów nauczania i szkoleń w środowisku pracy. Ponadto UE powinna prowadzić inicjatywy i programy informacyjne na te tematy w całej Unii.

1.3 Przedsiębiorcy powinni być prawnie zobowiązani do proaktywnego podejścia do ochrony przed atakami cybernetycznymi, w tym do stosowania bezpiecznych i odpornych technologii informacyjnych i komunikacyjnych (ICT) oraz szkolenia personelu w zakresie polityki bezpieczeństwa, podobnie jak szkoli się w zakresie bezpieczeństwa i higieny pracy.

1.4 W każdym państwie członkowskim funkcjonować powinna organizacja, której zadaniem byłoby informowanie, kształcenie i wspieranie sektora MŚP w zakresie najlepszych praktyk związanych z bezpieczeństwem cybernetycznym. Duże przedsiębiorstwa z łatwością mogą zdobyć potrzebną wiedzę, natomiast MŚP potrzebują jednak wsparcia w tym zakresie.

1.5 Należy rozszerzyć mandat Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji (ENISA) i zapewnić finansowanie, tak by podejmowała ona bardziej bezpośrednią odpowiedzialność za kształcenie i programy upowszechniania wiedzy w zakresie bezpieczeństwa cybernetycznego skierowane w szczególności do obywateli oraz małych i średnich przedsiębiorstw (MŚP).

1.6 Przedsiębiorstwa i organizacje muszą zwiększyć świadomość odpowiedzialności za bezpieczeństwo cybernetyczne na szczeblu zarządu. Informacje o ewentualnej odpowiedzialności przedsiębiorstwa wynikającej z nieodpowiedniej polityki bezpieczeństwa cybernetycznego i działań w tym zakresie powinny być wyraźnie przekazywane dyrektorom wszystkich organizacji.

1.7 Ze względu na swą kluczową rolę w świadczeniu usług internetowych wszyscy dostawcy usług internetowych w UE powinni w szczególnym stopniu odpowiadać za ochronę swoich klientów przed atakami cybernetycznymi. Odpowiedzialność ta powinna być określona i zapisana w prawodawstwie na szczeblu UE.

1.8 W celu zapewnienia szybkiego wykorzystania ogromnego potencjału dla wzrostu gospodarczego płynącego z dynamicznego rozwoju chmury obliczeniowej ([1]), na dostawców usług w chmurze obliczeniowej powinny zostać nałożone szczególne wymogi bezpieczeństwa i obowiązki także na szczeblu UE.

1.9 Komitet uważa, że środki dobrowolne są niewystarczające i należy nałożyć ścisłe wymogi regulacyjne na państwa członkowskie, aby zapewnić harmonizację cyberbezpieczeństwa, zarządzanie nim i wdrażanie go na szczeblu europejskim. Potrzebne jest także prawodawstwo przewidujące obowiązek zgłaszania istotnych incydentów dotyczących bezpieczeństwa cybernetycznego przez wszystkie organizacje i przedsiębiorstwa, nie tylko dostawców infrastruktury krytycznej. Pomogłoby to poprawić reakcję na zagrożenia w Europie, jak również podnieść poziom wiedzy i zrozumienia ataków cybernetycznych, tak aby można było opracować lepsze środki zaradcze.

([1]) Dz.U. C 24 z 28.1.2012, s. 40; Dz.U. C 76 z 14.3.2013, s. 59.

1.10 Komitet zdecydowanie zaleca, by Unia Europejska przyjęła oparte na projektowaniu podejście do zagrożenia atakami cybernetycznymi i zadbała o to, by wszystkie technologie i usługi wykorzystywane w Europie dla zapewnienia dostępu do internetu i usług internetowych były zaprojektowane tak, by gwarantowały jak najwyższy poziom zabezpieczenia przed atakami cybernetycznymi. Podczas projektowania należy poświęcić szczególną uwagę interfejsowi między użytkownikiem a maszyną.

1.11 EKES oczekuje, że europejskie organizacje normalizacyjne opracują i rozpowszechnią istotne normy bezpieczeństwa cybernetycznego dla wszystkich technologii i usług dotyczących sieci ICT. Normy te powinny zawierać obowiązkowy kodeks dobrych praktyk w celu zapewnienia zgodności wszystkich urządzeń ICT i usług internetowych sprzedawanych obywatelom europejskim z najwyższymi standardami.

1.12 UE musi bez zwłoki zadbać o to, by każde państwo członkowskie dysponowało w pełni sprawnym zespołem reagowania na incydenty komputerowe (CERT), aby chronić siebie i Europę przed atakami cybernetycznymi.

1.13 Komitet domaga się, by Europejskie Centrum ds. Walki z Cyberprzestępczością (EC3) przy Europolu otrzymało dodatkowe środki niezbędne do zwalczania cyberprzestępczości i do zacieśnienia współpracy z siłami policyjnymi w Europie i poza nią w celu zwiększenia zdolności Europy do chwytania i ścigania cyberprzestępców.

1.14 Ogólnie rzecz biorąc EKES uważa, że polityka UE w zakresie bezpieczeństwa cybernetycznego powinna w szczególności uwzględniać następujące aspekty: wzmacnianie wiodącej pozycji UE; opracowywanie strategii w zakresie cyberbezpieczeństwa zwiększających bezpieczeństwo przy jednoczesnej ochronie prywatności oraz innych praw podstawowych; podnoszenie świadomości obywateli i zachęcanie do proaktywnego podejścia do ochrony; kompleksowe zarządzanie ze strony państw członkowskich; świadome i odpowiedzialne działania przedsiębiorstw; ścisłe partnerstwo między władzami, sektorem prywatnym i obywatelami; odpowiedni poziom inwestycji; wysokie standardy techniczne i wystarczające inwestycje w badania, rozwój i innowacje; zaangażowanie międzynarodowe. W tym kontekście Komitet powtarza swoje zalecenia dotyczące polityki bezpieczeństwa cybernetycznego wyrażone w wielu wcześniejszych opiniach ([2]) i zwraca się do Komisji o przeanalizowanie działań, o które w nich apelowano.

2. **Zakres opinii**

2.1 Gospodarka internetowa wytwarza ponad jedną piątą wzrostu PKB w UE, a każdego roku w internecie robi zakupy 200 milionów Europejczyków. Jesteśmy zależni od internetu i związanych z nim technologii cyfrowych, dzięki którym funkcjonują kluczowe usługi energetyczne, zdrowotne, administracji państwowej i finansowe. Jednakże najważniejsza infrastruktura i usługi cyfrowe, które odgrywają tak istotną rolę w naszym życiu gospodarczym i społecznym, są narażone na rosnące ryzyko ataków cybernetycznych zagrażających naszemu dobrobytowi i jakości życia.

2.2 Komitet jest zdania, że coraz większej zależności Unii od internetu i technologii cyfrowej w niewystarczającym stopniu towarzyszą praktyki i polityki zapewniające właściwy poziom bezpieczeństwa cybernetycznego całej Europy teraz i w przyszłości. Celem niniejszej opinii jest zwrócenie uwagi na luki, które Komitet dostrzega w unijnej polityce bezpieczeństwa cybernetycznego, oraz zalecenie usprawnień, które lepiej ograniczałyby ryzyko ataków cybernetycznych.

2.3 Motywy ataków cybernetycznych mogą być rozmaite, od bardzo osobistych, np. odwet na osobie lub przedsiębiorstwie, po szpiegostwo uprawiane przez państwa narodowe i wojnę cybernetyczną między krajami. Podczas przygotowywania niniejszej opinii zdecydowano, aby zawęzić jej zakres wyłącznie do ataków cybernetycznych z pobudek przestępczych, tak by skupić się na zaleceniach dotyczących problemów o podstawowym znaczeniu dla większości członków Komitetu. Wielowątkowa debata polityczna na temat ataków cybernetycznych dokonywanych przez państwa członkowskie wobec obywateli i innych państw może być tematem przyszłej opinii.

([2]) Dz.U. C 97 z 28.4. 2007, s. 21;
Dz.U. C 175 z 28.7. 2009, s. 92;
Dz.U. C 255 z 22.9. 2010, s. 98;
Dz.U. C 54 z 19.2. 2011, s. 58;
Dz.U. C 107 z 6.4. 2011, s. 58;
Dz.U. C 229 z 31.7. 2012, s. 90;
Dz.U. C 218 z 23.7. 2011, s. 130;
Dz.U. C 24 z 28.1. 2012, s. 40;
Dz.U. C 229 z 31.7. 2012, s. 1;
Dz.U. C 351 z 15.11. 2012, s. 73;
Dz.U. C 76 z 14.3. 2013, s. 59;
Dz.U. C 271 z 19.9. 2013, s. 127;
Dz.U. C 271 z 19.9.2013, s. 133.

2.4 W niniejszej opinii omówiono tylko ataki cybernetyczne popełniane przez cyberprzestępców dla pieniędzy, co stanowi znakomitą większość ataków. Wprowadzając politykę bezpieczeństwa cybernetycznego i praktyki skutecznego radzenia sobie z atakami cybernetycznymi z pobudek przestępczych, zmniejsza się również zagrożenie związane z atakami cybernetycznymi o motywach politycznych lub bardziej osobistych.

2.5 Mimo iż Unia Europejska poczyniła znaczne postępy w działaniach na rzecz zaufania i bezpieczeństwa w ramach europejskiej agendy cyfrowej oraz opracowała szeroko zakrojoną strategię bezpieczeństwa cybernetycznego, która obejmuje większość celów nakreślonych powyżej, wiele jeszcze pozostaje do zrobienia.

3. **Ataki cybernetyczne i bezpieczeństwo cybernetyczne**

3.1 Atak cybernetyczny jest to wszelkiego rodzaju szkodliwe działanie, którego celem są komputerowe systemy informatyczne, infrastruktury, sieci komputerowe i/lub osobiste urządzenia cyfrowe, prowadzone za pomocą różnego rodzaju czynów dokonywanych w zamiarze kradzieży, zmiany lub zniszczenia określonego celu. Celem mogą być pieniądze, dane lub technologie informacyjne.

3.2 Cyberprzestępcy dokonują ataków cybernetycznych, aby ukraść pieniądze lub dane, dopuścić się oszustwa, prowadzić przestępczą działalność szpiegowską lub w celu dokonania wymuszenia. Ataki cybernetyczne mogą szkodzić podstawowym sieciom i usługom, od których zależy nasze zdrowie, bezpieczeństwo i dobrobyt gospodarczy, w tym sieciom rządowym, transportowym i energetycznym.

3.3 Zagrożenie wynikające z ataków cybernetycznych wzmaga się wraz z naszą rosnącą zależnością od internetu i technologii cyfrowych. Według ostatniego sprawozdania opracowanego przez firmę Symantec, całkowita liczba naruszeń ochrony danych na świecie wzrosła o 62 % w 2013 r., co oznacza ujawnienie ponad 552 mln zapisów. W wyniku tych naruszeń często ujawniano imię i nazwisko, datę urodzenia, numer dowodu tożsamości, dokumentację medyczną czy też informacje finansowe. Ponadto 38 % użytkowników urządzeń mobilnych doświadczyło cyberprzestępczości mobilnej w okresie ostatnich 12 miesięcy.

3.4 Ataki cybernetyczne mogą mieć poważny wpływ na poszczególne przedsiębiorstwa i szerzej rozumianą gospodarkę europejską:

— Sprawozdanie branżowe z 2011 r. sugeruje, że każdego roku na całym świecie ofiary cyberataków tracą około 290 mld EUR, co czyni tę przestępczość bardziej dochodową od światowego handlu marihuaną, kokainą i heroiną łącznie.

— Obywatele są stale zagrożeni kradzieżą tożsamości w wyniku ataków cybernetycznych. W maju 2014 r. baza danych zawierająca dane osobowe 145 mln posiadaczy kont w witrynie eBay została skradziona podczas pojedynczego ataku. Zgodnie z przeprowadzonym przez Uniwersytet Kent w 2013 r. badaniem na temat bezpieczeństwa cybernetycznego w ciągu zaledwie jednego roku (2012–2013) włamano się na konta internetowe ponad 9 milionów dorosłych mieszkańców Wielkiej Brytanii, 8 % ludności wskutek cyberprzestępczości straciło pieniądze, a w wypadku 2,3 % mieszkańców Zjednoczonego Królestwa straty przekraczały 10 tys. GBP.

— W brytyjskim sprawozdaniu rządowym z 2011 r. oszacowano, że ogólny koszt cyberprzestępczości dla gospodarki Zjednoczonego Królestwa wyniósł 27 mld GBP:

  — oszustwa internetowe: 1,5 mld GBP;

  — kradzież tożsamości: 1,7 mld GBP;

  — kradzież własności intelektualnej: 9,2 mld EUR;

  — szpiegostwo: 7,6 mld GBP;

  — utrata danych klientów: 1 mld GBP;

  — kradzież (bezpośrednia) z przedsiębiorstw przez internet: 1,3 mld GBP;

  — wymuszenia: 2,2 mld GBP;

  — oszustwa podatkowe: 2,3 mld GBP.

— Każdego roku w Europie ataki cybernetyczne powodują ogromne straty gospodarcze. Szacunki dotyczące kosztów muszą uwzględniać:

  — utratę własności intelektualnej i danych szczególnie chronionych;

  — koszty utraconych korzyści, w tym koszty zakłóceń w zatrudnieniu i świadczeniu usług;

  — szkody dla wizerunku marki i reputacji przedsiębiorstwa;

  — kary i płatności wyrównawcze dla klientów (za niedogodności lub pośrednie straty) bądź odszkodowania umowne (w przypadku opóźnienia itp.);

  — koszty środków zaradczych i ubezpieczenia;

  — koszty strategii łagodzących i usuwania szkód wynikających z ataków cybernetycznych;

  — straty handlowe i utratę konkurencyjności;

  — zakłócenia obrotu handlowego;

  — utratę miejsc pracy.

— Zgodnie z opublikowanym przez rząd brytyjski badaniem na temat przypadków naruszenia bezpieczeństwa informacyjnego z 2014 r w 2013 r. tego rodzaju naruszeń doświadczyło 81 % dużych przedsiębiorstw oraz 60 % MŚP.

— W tym samym sprawozdaniu rządowym oszacowano, że przeciętny koszt najpoważniejszego naruszenia bezpieczeństwa cybernetycznego może sięgać nawet 1,4 mln EUR w wypadku wielkich organizacji i 140 tys. EUR w wypadku MŚP.

— Nawet jeśli ataki nie są skuteczne, koszty łagodzenia ich skutków szybko wzrastają. W 2014 r. wzrost rynku bezpieczeństwa informacji na całym świecie przyspieszy do 8,6 % i przekroczy wartość 73 mld USD.

3.5 Metody dokonywania ataków cybernetycznych nieustannie się zmieniają:

— Atak cybernetyczny zazwyczaj polega na zastosowaniu wektora ataku, za pomocą którego przestępca cybernetyczny może uzyskać dostęp do internetowych danych uwierzytelniających bądź też do komputera lub serwera sieciowego w celu zrealizowania złych zamiarów. Powszechnie wykorzystywane wektory ataku to urządzenia USB, załączniki do poczty elektronicznej, strony internetowe, okna dialogowe, komunikatory, czaty internetowe i oszustwa, takie jak wyłudzanie informacji.

— Najbardziej powszechną formą ataku jest zainstalowanie złośliwego oprogramowania. Złośliwe oprogramowanie to tego rodzaju oprogramowanie, które w celach przestępczych przejmuje kontrolę nad urządzeniem cyfrowym, na przykład w celu kradzieży danych uwierzytelniających użytkownika lub jego pieniędzy bądź do rozprzestrzenienia się na inne urządzenia. Do złośliwego oprogramowania należą wirusy komputerowe (w tym robaki komputerowe i konie trojańskie), ransomeware, programy szpiegujące, adware, scareware i inne złośliwe programy. Na przykład oprogramowanie typu ransom blokuje dostęp do zarażonego przez siebie systemu komputerowego, a następnie żąda od użytkownika okupu za zniesienie blokady.

— Złośliwe oprogramowanie może również zamienić komputer w komputer zombie podłączony do botneta przestępcy cybernetycznego lub do sieci zombie, które przestępca kontroluje w celu atakowania ofiar.

— Atak spam ma miejsce, gdy przestępca wysyła niechciane wiadomości do dużej liczby odbiorców, często, by skłonić ofiary do wydania pieniędzy na podrabiane towary. Do wysyłania większości niechcianych wiadomości wykorzystuje się botnety.

— Ataki mające na celu wyłudzenie informacji (phishing) to próba wykradzenia nazwy użytkownika, hasła i szczegółów dotyczących karty kredytowej poprzez wzbudzenie zaufania, tak by przestępca mógł przejąć kontrolę nad kontem poczty elektronicznej, sieciami społecznościowymi i rachunkami bankowymi ofiary. Z punktu widzenia przestępcy tego rodzaju ataki są szczególnie skuteczne, ponieważ 70 % użytkowników internetu wybiera to samo hasło w odniesieniu do prawie wszystkich usług sieciowych, z których korzystają.

— Cyberprzestępcy stosują czasami atak typu „odmowa usługi" (DoS) w celu wymuszenia pieniędzy od przedsiębiorstwa lub organizacji. Atak typu DoS to próba zablokowania dostępu do maszyny lub zasobów sieciowych użytkownikom, dla których są one przeznaczone, przez nasycenie celu zewnętrznymi żądaniami komunikacji, tak że nie może on odpowiedzieć na uprawnione żądania dostępu lub odpowiada tak powoli, że staje się zasadniczo niedostępny. W atakach typu DoS przestępcy stosują powszechnie botnety.

3.6 Między organizacjami bezpieczeństwa cybernetycznego istnieje powszechna zgoda co do priorytetowych działań, które obywatele i przedsiębiorstwa powinni przedsięwziąć, aby się ochronić przed atakami cybernetycznymi. Praktyki te powinny być przekazywane w każdym programie uświadamiającym i edukacyjnym na temat bezpieczeństwa cybernetycznego:

a. Obywatele powinni:

— korzystać z trudnych do złamania, zapadających w pamięć haseł;

— zainstalować oprogramowanie antywirusowe na nowych urządzeniach;

— sprawdzać ustawienia dotyczące prywatności w mediach społecznościowych;

— robić bezpieczne zakupy online, dbając zawsze o sprawdzenie, czy portale sprzedaży detalicznej są zabezpieczone;

— pobierać aktualizacje naprawcze oprogramowania i aplikacji po ogłoszeniu ich udostępnienia.

b. Przedsiębiorstwa powinny:

— stosować białe listy aplikacji;

— stosować standardowe, bezpieczne konfiguracje systemów;

— instalować aktualizacje naprawcze oprogramowania użytkowego w ciągu 48 godzin;

— instalować aktualizacje naprawcze oprogramowania systemowego w ciągu 48 godzin;

— zmniejszyć liczbę użytkowników posiadających uprawnienia administratora.

3.7 Małym przedsiębiorstwom często brakuje wystarczającego wsparcia IT, by uzyskać bieżące informacje o potencjalnych zagrożeniach cybernetycznych, w związku z czym potrzebują specjalnej pomocy w ochronie przed atakami cybernetycznymi.

3.8 Ujawnianie ataków cybernetycznych i słabości systemu ma zasadnicze znaczenie dla zwalczania ataków cybernetycznych, zwłaszcza w zwalczaniu tzw. ataków zero-day, czyli nowych odmian ataków, które nie były wcześniej znane społeczności zajmującej się bezpieczeństwem cybernetycznym. Jednak przedsiębiorstwa często nie podają ataków cybernetycznych do wiadomości publicznej ze względu na obawy związane z utratą reputacji lub odpowiedzialnością prawną. To nieujawnianie informacji naraża na szwank zdolność Europy do szybkiego i skutecznego reagowania na zagrożenia cybernetyczne oraz do poprawy ogólnego bezpieczeństwa cybernetycznego dzięki uczeniu się od siebie nawzajem.

3.9 Obywatele i przedsiębiorstwa kupują dostęp do internetu i usług za pośrednictwem dostawców usług internetowych (ISP). Ze względu na ich kluczową rolę w świadczeniu usług online jest istotne, by dostawcy usług internetowych zapewniali możliwie najwyższy poziom ochrony przed atakami na swoich klientów. Oprócz dbania o to, by ich własne usługi i infrastruktura były zaprojektowane i utrzymywane w taki sposób, by zapewniały najwyższy poziom bezpieczeństwa cybernetycznego, dostawcy usług internetowych powinni służyć swoim klientom doskonałej jakości poradami na temat bezpieczeństwa cybernetycznego oraz powinni dysponować specjalnymi protokołami w celu bieżącego wykrywania i zwalczania ataków cybernetycznych na klientów. Odpowiedzialność ta powinna być określona i zapisana w prawodawstwie na szczeblu UE.

3.10 Przyspieszenie rozpowszechnienia chmury obliczeniowej wśród obywateli i przedsiębiorstw w Europie jest bardzo istotne dla gospodarki UE ([3]). Ze względu na to, że korzystanie z chmury obliczeniowej w aplikacjach osobistych i biznesowych staje się coraz powszechniejsze, istotne jest zwłaszcza, aby Europa zapewniła bezpieczeństwo cybernetyczne dostawców usług w chmurze. Niepewność co do bezpieczeństwa usług w chmurze ma negatywny wpływ na tempo przyjmowania tej dynamicznej technologii. Komitet życzyłby sobie, aby UE nałożyła specjalne wymogi bezpieczeństwa i obowiązki na dostawców usług w chmurze, aby wspierać rozwój chmury obliczeniowej w Europie.

([3]) Dz.U. C 24 z 28.1.2012, s. 40; Dz.U. C 76 z 14.3.2013, s. 59.

3.11 Należy podjąć szczególne wysiłki w celu rekrutacji pracowników do przemysłu bezpieczeństwa cybernetycznego w Europie. Oczekuje się, że zapotrzebowanie na pracowników posiadających dyplom studiów dotyczących bezpieczeństwa informacji wzrośnie ponad dwukrotnie w stosunku do wskaźnika wzrostu w odniesieniu do ogółu branży komputerowej. W tym kontekście Komitet zwraca uwagę Komisji na popularność konkursów i zawodów organizowanych w USA i w niektórych państwach członkowskich oraz ich skuteczność w kwestii podnoszenia świadomości bezpieczeństwa cybernetycznego i z punktu widzenia kształcenia następnego pokolenia specjalistów w dziedzinie bezpieczeństwa cybernetycznego.

3.12 Jedną z najlepszych strategii ochrony przed cyberatakami jest przyjęcie opartego na projektowaniu podejścia, tak by dopilnować, by wszystkie technologie i usługi wykorzystywane w Europie do łączności internetowej i usług internetowych były zaprojektowane tak, by gwarantowały jak najwyższy poziom ochrony przed atakami cybernetycznymi. Podczas projektowania należy poświęcić szczególną uwagę interfejsowi między użytkownikiem a maszyną. Wymagałoby to współpracy między producentami technologii, dostawcami usług internetowych, przemysłem bezpieczeństwa cybernetycznego, EC3, ENISA, agencjami obrony narodowej i bezpieczeństwa państw członkowskich oraz obywatelami. Tego typu podejście do bezpieczeństwa cybernetycznego mogłoby zostać wprowadzone na poziomie UE przez Komisję i – być może – koordynowane przez ENISA.

4. **Polityka UE w zakresie bezpieczeństwa cybernetycznego**

4.1 UE opracowuje kompleksową strategię na rzecz zwiększenia bezpieczeństwa cybernetycznego obywateli Europy ([4]):

— W ramach europejskiej agendy cyfrowej filar zaufanie i bezpieczeństwo obejmuje 14 działań ukierunkowanych na zwiększenie bezpieczeństwa cybernetycznego i ochrony danych.

— W dyrektywie dotyczącej ataków cybernetycznych ([5]), która musi zostać przetransponowana do prawa krajowego do dnia 4 września 2015 r., określono wytyczne dotyczące definicji przestępstw w tej dziedzinie i sankcji wobec osób je popełniających.

— Aby zwiększyć wiedzę na temat bezpieczeństwa cybernetycznego oraz ułatwić współpracę transgraniczną między państwami członkowskimi, UE wzmocniła mandat Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji (ENISA).

— W Europolu utworzono Europejskie Centrum ds. Walki z Cyberprzestępczością (EC3).

— Inicjatywa polityczna w sprawie ochrony krytycznej infrastruktury informatycznej (CIIP) skupia się na ochronie Europy przed zakłóceniami cybernetycznymi, w tym atakami, dzięki zwiększeniu bezpieczeństwa cybernetycznego i odporności całej UE.

— Strategia na rzecz lepszego internetu dla dzieci ma na celu stworzenie bezpiecznego środowiska dla dzieci w internecie oraz zwalczanie seksualnego wykorzystywania dzieci i dostępnych on-line materiałów związanych z seksualnym wykorzystywaniem dzieci.

— Przedstawiony wniosek dotyczący dyrektywy w sprawie bezpieczeństwa sieci i informacji (NIS) wymaga, aby państwa członkowskie wprowadziły systemowe rozwiązania w zakresie bezpieczeństwa sieci i informacji, np. dobrze funkcjonujący zespół reagowania na incydenty komputerowe (CERT). Sprecyzowano w niej również wymogi dotyczące bezpieczeństwa sieci i sprawozdawczości dla dostawców infrastruktury krytycznej.

4.2 EKES zdecydowanie zareagował na wniosek Komisji dotyczący dyrektywy w sprawie bezpieczeństwa sieci i informacji (NIS) ([6]), ponieważ proponowane środki zostały uznane za zbyt łagodne i nieskłaniające państw członkowskich w wystarczającym stopniu do ochrony obywateli i przedsiębiorstw przed atakami cybernetycznymi. Tymczasem przyjmując proponowaną dyrektywę, Parlament dodatkowo osłabił jej przydatność, ściśle ograniczając zakres jej stosowania do dostawców „infrastruktury krytycznej", przez co wykluczono jej stosowanie do wyszukiwarek, platform mediów społecznościowych, internetowych portali płatniczych i dostawców usług w chmurze obliczeniowej.

4.3 Proponowana dyrektywa NIS obecnie nie wystarczy, aby zapewnić przepisy konieczne do zwiększenia świadomości zagrożenia i zdolności reagowania na ataki cybernetyczne w Unii. Komitet pragnie, by przyjęto nowe przepisy przewidujące obowiązek zgłaszania wszystkich istotnych incydentów dotyczących bezpieczeństwa cybernetycznego, które miałyby zastosowanie nie tylko wobec dostawców infrastruktury krytycznej. Brak obowiązku zgłaszania pomaga cyberprzestępcom wykorzystywać niewiedzę wrażliwych celów.

([4]) JOIN/2013/01 final.
([5]) Dz.U. L 218 z 14.8.2013, s. 8–14.
([6]) Dz.U. C 271 z 19.9.2013, s. 133.

4.4 UE powinna rozważyć rozszerzenie mandatu ENISA, by zwiększyć świadomość zagrożenia atakami cybernetycznymi i usprawnić reagowanie na nie w całej Unii. Być może rolę ENISA można by rozszerzyć w taki sposób, by odpowiadała ona bardziej bezpośrednio za programy szkoleń i upowszechniania wiedzy w dziedzinie bezpieczeństwa cybernetycznego skierowane w szczególności do obywateli i MŚP.

4.5 W 2013 r. utworzono Europejskie Centrum ds. Walki z Cyberprzestępczością (EC3) przy Europolu w celu zwiększenia zdolności Europy do walki z cyberprzestępczością. EC3 działa jako centrum wywiadu kryminalnego w Europie i wspiera prowadzone w państwach członkowskich działania i dochodzenia dotyczące ataków cybernetycznych. Jednakże w swoim pierwszym sprawozdaniu rocznym EC3 ostrzega, że jego obecne zasoby już ograniczają możliwości postępu w dochodzeniach i że nie będzie w stanie uporać się z dochodzeniami na dużą skalę, które do niego trafiają.

4.6 UE powinna zwrócić się do europejskich organizacji normalizacyjnych (CEN, CENELEC i ETSI) o opracowanie norm bezpieczeństwa cybernetycznego dla wszelkiego oprogramowania, sprzętu ICT lub usług internetowych przeznaczonych do sprzedaży w UE. Normy te powinny być stale aktualizowane, by uwzględniać nowe zagrożenia.

4.7 Potrzebne jest prawodawstwo przewidujące obowiązek zgłaszania istotnych incydentów dotyczących bezpieczeństwa cybernetycznego przez wszystkie organizacje i przedsiębiorstwa, nie tylko dostawców infrastruktury krytycznej. Pomogłoby to zwiększyć możliwości łagodzenia zagrożeń internetowych, jak również podnieść poziom wiedzy i zrozumienia dokonywanych ataków cybernetycznych, co pomogłoby władzom, branży bezpieczeństwa cybernetycznego, przedsiębiorstwom i obywatelom poprawiać bezpieczeństwo cybernetyczne oraz zwalczać zagrożenia. Aby zachęcić do wymiany informacji o atakach, przepisy prawne powinny zapewniać przedsiębiorstwom i organizacjom informującym o ataku odpowiedni poziom anonimowości. Należy również zwrócić uwagę w stosownych przypadkach na zapewnienie ochrony przed odpowiedzialnością.

4.8 Pomimo inicjatyw podejmowanych przez UE państwa członkowskie reprezentują bardzo różny poziom zdolności i gotowości, co prowadzi do niejednolitych reakcji na ataki cybernetyczne w całej UE. Biorąc pod uwagę fakt, że sieci i systemy są ze sobą połączone, te państwa członkowskie, które prowadzą bardzo słabą politykę bezpieczeństwa cybernetycznego, zmniejszają ogólną zdolność UE do zwalczania ataków cybernetycznych. Należy podjąć działania zmierzające do zapewnienia akceptowalnego poziomu bezpieczeństwa cybernetycznego we wszystkich państwach członkowskich. Trzeba szczególnie zadbać o to, by każde państwo członkowskie dysponowało sprawnie funkcjonującym zespołem reagowania na incydenty komputerowe (CERT).

4.9 Zgodnie z zaleceniami zawartymi we wcześniejszych opiniach ([7]) EKES uważa, że dobrowolne działania są nieskuteczne, jeśli chodzi o poprawę ochrony UE przed atakami cybernetycznymi, i że należy nałożyć na państwa członkowskie zdecydowane zobowiązania regulacyjne, by zapewnić harmonizację, zarządzanie i egzekwowanie w zakresie europejskiego bezpieczeństwa cybernetycznego.

4.10 Podsumowując: aby Unia Europejska była w stanie zapewnić rzeczywistą i aktualizowaną ochronę obywateli i przedsiębiorstw przed atakami, jej polityka w zakresie bezpieczeństwa cybernetycznego powinna koncentrować się na następujących działaniach:

— silnym przywództwie UE ustanawiającej polityki, prawa i instytucje w celu wspierania wysokiego poziomu bezpieczeństwa cybernetycznego w całej Unii;

— politykach bezpieczeństwa cybernetycznego, które zwiększają bezpieczeństwo zbiorowe i indywidualne, jednocześnie zachowując prawo obywateli do prywatności i chroniąc inne podstawowe wartości i wolności;

— wysokiej świadomości wszystkich obywateli o ryzyku związanym z korzystaniem z internetu, oraz zachęcaniu do proaktywnego podejścia do ochrony swoich urządzeń cyfrowych, tożsamości, prywatności i transakcji on-line;

— kompleksowym systemie zarządzania we wszystkich państwach członkowskich gwarantującym bezpieczeństwo i odporność krytycznej infrastruktury teleinformatycznej;

— przemyślanych i odpowiedzialnych działaniach wszystkich przedsiębiorstw w celu zapewnienia, że ich systemy ICT są bezpieczne i odporne, aby chronić ich działalność i interesy klientów;

— proaktywnym podejściu dostawców usług internetowych do ochrony swoich klientów przed atakami cybernetycznymi;

— podejściu do bezpieczeństwa cybernetycznego opartym na głębokim partnerstwie w całej UE między rządami, sektorem prywatnym i obywatelami, na poziomie strategicznym i operacyjnym;

— opartym na projektowaniu podejściu do wbudowanego bezpieczeństwa cybernetycznego przy opracowywaniu technologii i usług internetowych;

([7]) Dz.U. C 255 z 22.9.2010, s. 98; Dz.U. C 218 z 23.7.2011, s. 130; Dz.U. C 271 z 19.9.2013, s. 133.

— odpowiednim poziomie inwestycji w rozwój wiedzy i umiejętności dotyczących bezpieczeństwa cybernetycznego, aby wykształcić solidnych specjalistów od bezpieczeństwa cybernetycznego;

— dobrych normach technicznych bezpieczeństwa cybernetycznego i wystarczających inwestycjach w B+R+I, aby wspierać rozwój silnego sektora bezpieczeństwa cybernetycznego oraz tworzenie rozwiązań światowej klasy;

— aktywnym zaangażowaniu międzynarodowym wraz z państwami spoza UE w prace nad skoordynowaną globalną polityką i systemem reagowania wobec zagrożeń cybernetycznych.

Bruksela, 10 lipca 2014 r.

Przewodniczący
Europejskiego Komitetu Ekonomiczno-Społecznego
Henri MALOSSE