Instytut
mikroMAKRO
programmamus futura

Fundacja Instytut Mikromakro
ul. Lanciego 13-149
tel. 22 40 72 076
biuro@mikromakro.pl

Warszawa, 20 marca 2013

Opinia Fundacji Instytut Mikromakro w sprawie dokumentu Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń sporządzona w związku z konsultacjami Ministra Administracji i Cyfryzacji

Opublikowany 7 lutego Komunikat, zatytułowany „Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń" został przedstawiony przez Komisję Europejską i Wysokiego Przedstawiciela Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa. To pierwsze kompleksowe ujęcie różnych aspektów bezpieczeństwa informacyjnego, które powinny być przedmiotem polityki wspólnotowej. Dokumentowi towarzyszy projekt dyrektywy w sprawie środków zapewniających wspólny poziom bezpieczeństwa sieci i informacji w Unii Europejskiej, którą zaprezentowała Komisarz Nelie Kroes, odpowiadająca za rozwój rynku sieci i usług telekomunikacyjnych. Podobnie jak w przypadku innych tego rodzaju dokumentów opublikowano również ocenę skutków regulacji (impact assesment).

Dokument określa szereg zadań dla instytucji unijnych i państw członkowskich. Adresatem strategii są również przemysł, organizacje pozarządowe oraz sektor badań i rozwoju.

Wśród wielu zadań do najbardziej istotnych inicjatyw naszym zdaniem należą:

- Zapowiedzi legislacyjne w sprawie mechanizmów koordynacji międzynarodowej współpracy w sprawach zapobiegania, wykrywania, ograniczania i reagowania na naruszenia cyberbezpieczeństwa. Mowa jest też na przykład konkretnie, o potrzebie wymiany informacji pomiędzy krajowymi organami regulacyjnymi w sprawach bezpieczeństwa sieci i informacji, obowiązku zgłaszania naruszeń, które noszą znamiona przestępstw.
- Ukierunkowanie nowych rozwiązań prawnych na zwiększenie gotowości i zaangażowania sektora prywatnego, zachęty do dostarczania wiarygodnych danych na temat naruszeń cyberbezpieczeństwa i ich skutków, stosowania środków zaradczych. Zwraca się przy tym uwagę na konieczność podejścia sektorowego, wprowadzenia zasad dla oceny przeciwdziałania zagrożeniom.
- Wzmocnienie mandatu ENISA. Strategia zawiera wprawdzie formalne zastrzeżenie, że propozycje zadań nie pociągają za sobą takiej konieczności, ale dla ENISA wyznacza się szereg zadań, które poszerzają rolę i status organizacji, włącznie z wyraźną sugestią, że jej relacje z państwami członkowskimi powinny być ściślejsze. Dotyczy to np. zacieśnienia współpracy krajowych CERT.

- Opracowanie ram politycznych dla obrony cybernetycznej w UE.
- Włączenie kwestii ochrony cyberprzestrzeni do polityki zewnętrznej UE oraz wspólnej polityki zagranicznej i bezpieczeństwa w tej dziedzinie.

Niestety , w Strategii zgromadzono najróżniejszej wagi zagadnienia związane z bezpieczeństwem, nie próbując ich właściwie usystematyzować. Tematyka bezpieczeństwa pojawia się w debacie europejskiej w różnych kontekstach i znaczeniach. Zgromadzone prawie wszystkie w jednym dokumencie, tworzą obraz niespójny merytorycznie. Mieszają się i krzyżują bardzo różne wątki. Mówi się o przestępstwach kryminalnych, dziecięcej pornografii, nienawiści rasowej, kradzieży tożsamości, złośliwym oprogramowaniu i jakby na tej samej nucie o ochronie krytycznych zasobów infrastruktury ważnej dla interesów ekonomicznych państw, ochronie informacji rządowych, cyberterroryzmie, szpiegostwie gospodarczym, obronności. Zwraca się uwagę na rosnące znaczenie debaty o swobodach obywatelskich, wolności wypowiedzi, ochronie danych osobowych i prywatności, powszechności dostępu. Wspólna strategia ma również obejmować prace badawczo-rozwojowe w obszarze technologii bezpieczeństwa i produkcję przemysłową.

Trudno zakwestionować potrzebę realizacji któregokolwiek ze wskazanych działań, ale sposób ich ujęcia nie daje spójnego obrazu zagrożeń związanych ze stosowaniem technologii informacyjnych. W takiej sytuacji, proponowane środki zaradcze muszą tworzyć wrażenie koncepcji niekompletnej. Próbując skomunikować się w ten sposób z mieszkańcami Europy i działającymi tu firmami, trudno im zagwarantować bezpieczeństwo.

Dokument proponuje przede wszystkim strategię stawiania zapór i poprawiania odporności na zagrożenia oraz reagowania na incydenty głównie w kontekście organizacyjno-technicznym. Zastosowano typową wspólnotową pragmatykę dochodzenia do wspólnych rozwiązań poprzez harmonizowanie procedur, standardów i współpracę instytucjonalną. Tak jak w każdym innym obszarze polityki wspólnotowej przyjęto, że mechanizmy współpracy i zrozumienie dla niej będą budowane stopniowo, razem ze wzrostem akceptacji dla jednolitego podejścia. Takie posunięcia są bezsprzecznie potrzebne. Niezbędne jest ujednolicenie zasad funkcjonowania zespołów CERT, sklasyfikowanie rodzajów infrastruktury krytycznej, ale już formalna klasyfikacja rodzajów działalności gospodarczej w Internecie (załącznik II do projektu dyrektywy) budzi poważne wątpliwości, biorąc pod uwagę dynamikę zmian w tym sektorze w ostatnich latach. Wbrew deklaracjom Strategii, trudno dostrzec bodźce i zachęty do budowania partnerstwa publiczno-prywatnego dla wzmacniania strategicznego bezpieczeństwa europejskiej gospodarki.

Postulowane wzmacnianie mechanizmów współpracy jest wpasowane w typową dla instytucji unijnych inercję. Wyraźnie brakuje refleksji nad znaczeniem dynamiki zmian na rynku usług i zastosowań technologii informacyjnych, nowych i przyszłych obszarów zagrożeń.

Pojawia się ryzyko utrwalenia luk w instytucjonalnym systemie bezpieczeństwa. Utworzone niedawno w ramach Europolu Europejskie Centrum ds. Walki z Cyberprzestępczością, zajmuje się przede wszystkim przestępczością kryminalną. Uwagę Europolu w coraz większym stopniu absorbuje doskonale sobie radząca w Internecie przestępczość zorganizowana, ale nie wszystkie potencjalne zagrożenia da się penalizować. Rola CEPOLU i Eurojustu sprowadza się podobnie jak w innych dziedzinach do planowania i znoszenia barier we współpracy międzynarodowej.

ENISA jest często przywoływana w Strategii, ma jak na razie dosyć ograniczone możliwości wpływania na politykę bezpieczeństwa cyberprzestrzeni w państwach członkowskich, pełniąc rolę czegoś w rodzaju eksperckiego think-tanku i organizatora bardzo potrzebnych ćwiczeń międzynarodowych. Wbrew zastrzeżeniom Strategii, nie powinno się uciekać od wyraźnego wzmocnienia mandatu tej organizacji. Wiele potencjalnych zagrożeń w Internecie będzie przekraczać granice geograficzne państw.

Organizatorem nowych instrumentów polityki na szczeblu Komisji Europejskiej ma być Dyrekcja Generalna ds. Sieci, Treści i Technologii Telekomunikacyjnych. W Strategii wymienia się zagrożenia z arsenału szeroko pojętego szpiegostwa przemysłowego, ale głównie w kontekście fizycznych zabezpieczeń dostępu do sieci korporacyjnych i przemysłowych. W bardzo niewielkim stopniu odnosi się to do wykorzystania technologii informacyjnych do nieprzyjaznego państwom europejskim wpływania na procesy w gospodarce i działań, które należy podejmować dla zmniejszania ich skutków zarówno w sferze analitycznej, jak i przeciwdziałania. W sprawach zagrożeń o charakterze militarnym rola Europejskiej Agencji Obrony nie wykracza poza obecny ostrożny mandat planowania wspólnych obszarów dla polityki obronnej i wymiany informacji. O ile w sprawach militarnych zagrożeń konwencjonalnych taka ograniczona polityka obronna może być uzasadniona, to w sferze zagrożeń z cyberprzestrzeni nie przystaje do bardzo realnych wyzwań.

Proponowana obecnie Strategia nie pasuje do charakteru i zakresu zagrożeń związanych z powszechną dostępnością technologii informacyjnych. Nie odpowiada na bieżące problemy, związane z ryzykiem wykorzystania wszelkich narzędzi technologii informacyjnych do zdobywania w sposób nieczysty rynkowej przewagi, nie uwzględnia zagrożeń związanych z naturalnym ryzykiem wtórnych skutków awarii i katastrof w systemach, które zależą od wykorzystania technologii informacyjnych. To podejście zupełnie inne, niż np. obecne planowanie w Stanach Zjednoczonych, gdzie określono np. konieczność przygotowań do działań ofensywnych w przypadku ataków na systemy informacyjne amerykańskich firm. W unijnej strategii zakłada się ewolucję wspólnotowej polityki. W takim rozumieniu Strategia jest zachowawcza, zakładając, że państwa członkowskie są same w stanie chronić siebie, obywateli i gospodarkę.

Sławomir Kosieliński
Prezes Zarządu
Fundacji „Instytut Mikromakro”

Piotr Rutkowski
Wiceprezes Zarządu
Fundacji „Instytut Mikromakro”