Instytut Mikromakro

Warszawa 8 marca 2016 roku

Komentarz fundacji Instytut Mikromakro do dokumentu Założenia strategii cyberbezpieczeństwa dla Rzeczypospolitej Polskiej zaprezentowanej przez Ministra Cyfryzacji do konsultacji 23 lutego 2016 roku

Zaproszenie wystosowane przez Ministra Cyfryzacji do konsultacji założeń strategii cyberbezpieczeństwa dla RP [„Złożenia"] to dobry punkt wyjścia do debaty o roli państwa w zapewnieniu bezpieczeństwa gospodarki i obywateli.

Zakres problematyki cyberbezpieczeństwa

W dotychczasowym systemie bezpieczeństwa systemów informacyjnych, istnieją rozwiązania prawne i organizacyjne, a trzeba wierzyć, że również techniczne, dające podstawy ochrony informacji wrażliwych, w tym informacji istotnych dla bezpieczeństwa i obronności państwa, a także wielu rodzajów innych informacji, wymagających specjalnych środków ochrony. Na osobach odpowiedzialnych za bezpieczeństwo informacji prawnie chronionych spoczywają obowiązki, wynikające wprost z przepisów ustawowych, pragmatyki służb lub zajmowanych stanowisk, regulaminów wewnętrznych, dobrych praktyk, standaryzacji wymagań.

Rozwój technologii informacyjnych wymusił potrzebę dostosowania wielu ustaw, również pod kątem bezpieczeństwa. W większości dziedzin, zmieniających się razem upowszechnieniem technologii informacyjnych, trzeba uwzględniać kwestie bezpieczeństwa. Niektóre dedykowane zastosowania technologii informacyjnych z jednej strony pozwalają, na przykład zwiększyć bezpieczeństwo działania systemów transportowych, ale z drugiej strony mogą one skutkować nowymi zagrożeniami, w związku z ryzykiem ataku z cyberprzestrzeni.

Pojawiły się również nowe koncepcje prawne. Przykłady to prawo o ochronie prywatności, przepisy o handlu elektronicznym, uregulowania dla nowych rozwiązań płatniczych. Niektóre nowe wyzwania technologiczne są uwarunkowane uzgodnieniem nowych zasad prawnych. Dotyczy to takich obszarów tematycznych jak robotyka, bezzałogowe statki, powietrzne, samochody bez kierowcy, sztuczna inteligencja. W każdej z tych dziedzin różne aspekty bezpieczeństwa, w tym również cyberbezpieczeństwa są kwestią o znaczeniu krytycznie ważnym.

Trzeba przy tym zwrócić uwagę, że bezpieczeństwo z reguły musi być ściśle powiązane z pozostałymi cechami systemów. Nawet jeżeli da się wydzielić jako odrębne zagadnienie techniczne, to znacznie lepiej je rozpatrywać w związku wszystkimi podstawowymi funkcjonalnościami systemowymi, cechami fizycznymi, organizacją systemu. Ewidentnym przykładem są waluty wirtualne. Są oparte o

zaawansowane protokoły kryptograficzne, więc system cyberbezpieczeństwa w zasadzie prawie w ogóle nie da się wydzielić jako coś odrębnego.

Relacje z innymi instytucjami odpowiedzialnymi w państwie za bezpieczeństwo

Jeżeli zrozumieć właściwości Ministra Cyfryzacji w zakresie ochrony cyberprzestrzeni jako okazję do budowania politycznego centrum kompetencyjnego, organizującego zadania w szeroko pojętej sferze cywilnej, to jego relacje z innymi z instytucjami, które nie są przez niego nadzorowane, należałoby znacznie lepiej definiować, niż w Założeniach.

Minister Cyfryzacji ma uzupełniać, a nie w alternatywny sposób organizować zadania państwa w zakresie bezpieczeństwa, za które odpowiadają na podstawie odrębnych przepisów krajowa władza bezpieczeństwa, podległe lub nadzorowane organy oraz jednostki organizacyjne, siły zbrojne, operatorzy infrastruktury krytycznej, a także regulatorzy sektorowi. Trudno byłoby sobie na przykład wyobrazić ingerowanie w jakikolwiek sposób w politykę organizacji środków cyberobrony w siłach zbrojnych. Nie można wykluczyć transferu rozwiązań technicznych i wyrobów ze sfery cywilnej do wojskowej, podobnie jak przydatności cywilnego systemu wykrywania zagrożeń i reagowania na incydenty, ale potrzeby armii, szczególnie na szczeblach taktycznym i operacyjnym są odległe od zastosowań cywilnych.

Diagnoza stanu bezpieczeństwa Polski

Założenia rozpoczyna bardzo lakoniczne uzasadnienie zapotrzebowania na przyjęcie strategii cyberbezpieczeństwa. Tymczasem kompleksowa diagnoza stanu bezpieczeństwa Polski pod kątem różnego typu zagrożeń z cyberprzestrzeni powinna stanowić materiał wyjściowy do rozważań o planowanych środkach organizacyjnych, instytucjonalnych, prawnych oraz budżetowych. Powinny być one odpowiadać rzeczywistym, a nie hipotetycznym czynnikom ryzyka.

Należałoby na przykład zdiagnozować powody, dla których dotąd nie udało się przygotować tego rodzaju strategii, w tym na jakich zasadach funkcjonują rozwiązania dotychczasowe, odnosząc je miedzy innymi do dokumentu „Polityka ochrony cyberprzestrzeni RP” przyjęta przez Radę Ministrów w 2013 roku.

Brakuje też odniesienia do dokumentu „Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej” przygotowanego w BBN i podpisanego przez Prezydenta w 2015. Jego konkluzje są na tyle uniwersalne, że trudno je uznać za nieaktualne.

Brakuje oceny jak funkcjonują obowiązujące rozwiązania Prawa telekomunikacyjnego, dlaczego np. niedomaga działa system zgłaszania incydentów do UKE.

Cele strategii cyberbezpieczeństwa RP należałoby też odnieść zarówno do celów strategii gospodarczej państwa (Plan na rzecz odpowiedzialnego rozwoju), jak i stanu bezpieczeństwa państwa, zarówno wewnętrznego, jak i w kontekście regionalnym, europejskim, globalnym.

Istotne wydaje się na przykład planowanie zadań, które dopasują strategię cyberbezpieczeństwa do planów zapewnienia bezpieczeństwa energetycznego, zarówno w kontekście krajowym (przecież mowa o części infrastruktury krytycznej), jak i starań Polski o wspólną politykę bezpieczeństwa energetycznego UE.

Powiązanie strategii rozwoju gospodarczego z cyberbezpieczeństwem trzeba identyfikować w związku z budową systemów transportowych, inteligentnych miast, systemów komunalnych. W takim kontekście powinny się ujawnić braki, błędy lub zaniechania w planowaniu zamówień na

systemy inteligentnego transportu, systemów kontroli ruchu kolejowego (GSM-R), systemów przetwarzania informacji dla potrzeb zarządzania infrastrukturą miejską itp.

Istotne jest również powiązanie cyberbezpieczeństwa z bezpieczeństwem powszechnym. Można wskazać takie zagadnienia jak stan edukacji w zakresie rozwiązań zapewniających bezpieczeństwo, dostępność do narzędzi wzmacniających zarówno poczucie bezpieczeństwa, jak i rzeczywiste bezpieczeństwo.

W Założeniach w kilku miejscach wspomniany jest temat potrzeby stworzenia specjalnie uodpornionych systemów łączności rządowej. Zalecalibyśmy zdiagnozowanie, co stało dotąd na przeszkodzie w organizacji tego typu systemów? Jaki jest stan organizacji łączności kryzysowej? Dlaczego od kilkunastu lat nie udaje się w Polsce stworzyć jednolitego systemu łączności radiowej dla służb ratunkowych i porządku publicznego, a zamiast niego powstają rozwiązania doraźne o charakterze wyspowym?

Zakres Założeń

W Założeniach przyjęto podejście, które skupia plan Ministra Cyfryzacji na stworzeniu systemu reagowania na incydenty w cyberprzestrzeni. Nie negując potrzeby zorganizowania specjalizowanych CERT/ CSIRT, oceniamy go jako zbyt ograniczony. Uzupełnia go system wymiany informacji. Cenny, bo poszkodowany wreszcie powinien wiedzieć, gdzie zgłaszać przypadki naruszeń. Nie wyczerpuje on jednak wyzwań związanych z bezpieczeństwem.

W tym systemie kluczową rolę ma odgrywać NASK, od niedawna nadzorowany przez Ministra Cyfryzacji. Nie negując w najmniejszym stopniu wysokich kompetencji zespołu NASK w sprawach wykrywania i analizowania zagrożeń z cyberprzestrzeni, trzeba zauważyć, że brakuje komentarza w sprawach organizacji NASK, w tym jego innych rodzajów działalności, również komercyjnej, co może stać w konflikcie z zadaniami instytucji standaryzującej i nadzorującej operacyjnie sprawy cyberbezpieczeństwa. Nie są w szczególności wyjaśnione kwestie ewentualnych uprawnień do zarządzania wyłączaniem ruchu w sieciach przedsiębiorców, uprawnieniem do umieszczania w nich sond ruchu. Wydaje się, że tego typu uprawnienia powinny mieć mocne utwierdzenie ustawowe.

Współpraca z sektorem prywatnym

Założenia bardzo lakonicznie odnoszą się do kwestii współpracy z podmiotami komercyjnymi, organizacjami pozarządowymi i ośrodkami badawczo-rozwojowymi. Liczne niezależne inicjatywy, konferencje oraz ćwiczenia wyglądają na ignorowane w ogólnym planie Założeń lub wręcz niesprawiedliwie lekceważone. To element, który należy bezwzględnie poprawić, bo dzięki niezależnym inicjatywom stan współpracy w sprawach wymiany informacji o zagrożeniach i doświadczeniach wygląda w Polsce wcale nie tak źle, jak by to wynikało z oficjalnego obrazu polityki instytucji rządowych, podsumowany w raporcie NIK z 2014 roku.

Współpraca zagraniczna

Założenia pomijają również lub nie komentują, istniejących okazji do współpracy zagranicznej, np. z ENISA, EC3 w Europolu, udziału w inicjatywach Komisji Europejskiej, w tym inicjatywach partnerstwa publiczno-prywatnego w badaniach na temat cyberbezpieczeństwa.

W Założeniach w wielu miejscach przewija się natomiast sprawa konieczności wdrożenia dyrektywy NIS. Można powiedzieć, że koncepcja Założeń, wraz z utworzeniem systemu CSIRT, jest temu zadaniu podporządkowana. Sprawa dyrektywy NIS, która jeszcze nie jest jeszcze obowiązująca, a ponadto ma długi 21 miesięczny okres transpozycji, wymaga jednak bezwzględnie odrębnego szerszego

komentarza i analizy. Dlaczego prace nad dyrektywą trwały tak długo? Jak się mają do unijnej strategii ochrony cyberprzestrzeni, zwalczania cyberprzestępczości? Jak należy oceniać skuteczność współpracy międzynarodowej, ewentualnych przyszłych regulacji uzupełniających koncepcję dyrektywy NIS?

Piotr Rutkowski
wiceprezes fundacji Instytut Mikromakro