BEZPIECZEŃSTWO CYBERPRZESTRZENI

REKOMENDACJE STOWARZYSZENIA EURO-ATLANTYCKIEGO

Tezy:

Postęp w dziedzinie technologii informacyjnych i komunikacyjnych (ICT) przyniósł rozwój społeczeństwa informacyjnego i nowy wymiar działania – cyberprzestrzeń. Na początku lat 90. ubiegłego wieku cyberprzestrzeń uznano za nowy wymiar pola walki i bezpieczeństwa narodowego (międzynarodowego). Przyniosło to koncepcje takie, jak infowar, cyberwar, netwar oraz realne zagrożenia cyberterrorystyczne. Do istotnych współczesnych problemów politycznych i badawczych należy zaliczyć następujące: swoistość cyberprzestrzeni i specyfikacja zagrożeń cybernetycznych dla bezpieczeństwa narodowego, ryzyko zagrożeń cybernetycznych dla bezpieczeństwa narodowego RP, bezpieczeństwo Europejskiej Przestrzeni Cybernetycznej, uwarunkowania organizacyjne i prawne bezpieczeństwa cybernetycznego UE, NATO i RP, możliwość „cybernetycznego Pearl Harbor", wnioski z Rządowego Programu Ochrony Cyberprzestrzeni RP na lata 2011-2016, warunki i możliwość ogłoszenia stanu wyjątkowego z powodu zagrożeni cybernetycznego.

Rekomendacje:

W celu zapewnienia pożądanego poziomu bezpieczeństwa cyberprzestrzeni państwa właściwe jest podjęcie działań w obszarach:

Uregulowań prawnych:

- Powierzenie Ministerstwu Administracji i Cyfryzacji odpowiedzialności za koordynację ogólnej polityki bezpieczeństwa cyberprzestrzeni RP.

- Uchwalenie Rządowego Programu Ochrony Cyberprzestrzeni RP na lata 2011-2016
- Uchwalenie Narodowego Programu Ochrony Infrastruktury Krytycznej, w którym zagrożenia teleinformatyczne i ochrona przed nimi są traktowane jako integralny element jej ochrony
- Dokonanie zmian w istniejących aktach prawnych w celu precyzyjnego określenia roli, odpowiedzialności oraz uprawnień w zakresie prowadzenia działań w cyberprzestrzeni przez instytucje oraz organizacje państwowe i prywatne, a także osoby prywatne.
- Wprowadzenie zmian prawnych regulujących zasadę wymiany informacji oraz współpracę pomiędzy instytucjami państwowymi a podmiotami prywatnymi (przedsiębiorstwa telekomunikacyjne, wiodący dostawcy sprzętu, wiodący dostawcy usług informatycznych itp).
- Wprowadzenie zmian legislacyjnych określających zasady wykorzystania instrumentów cybernetycznych do prowadzenia aktywnej obrony cyberprzestrzeni, oraz stworzenie możliwości wykorzystania tych instrumentów w podejmowaniu działań wyprzedzających;
- Dokonanie precyzyjnego podziału obszarów kompetencji i odpowiedzialności w odniesieniu do bezpieczeństwa cyberprzestrzeni RP oraz stworzenie podstaw prawnych współpracy z sektorem prywatnym w tym zakresie.

Badań i rozwoju systemu cyberobrony:

- Zaktywizować ośrodki naukowo-badawcze do prowadzenia badań naukowych, rozwoju technologii bezpieczeństwa, metodyk analiz i oceny bezpieczeństwa cyberprzestrzeni RP itp.
- Wspomóc przedsiębiorców w prowadzeniu prac badawczo-rozwojowych
- w tym zakresie i stworzyć mechanizmy regulujące wdrożenie wyników tych prac do działań administracji publicznej.
- Stworzenie programu *Edukacja dla bezpieczeństwa w cyberprzestrzeni* skierowanego do obywateli, urzędników oraz funkcjonariuszy mającego na celu zwiększenie świadomości potrzeby indywidualnego bezpieczeństwa

podczas wykorzystywania sieci komputerowych i Internetu jako składowej bezpieczeństwa państwa.

- W ramach tego programu uznać rok 2012 za Rok Ochrony Cyberprzestrzeni (ROC) i prosić Prezydenta RP o patronat, by pod jego auspicjami podjąć publiczną debatę, jakimi przesłankami musi się on kierować, by wprowadzić jeden ze stanów nadzwyczajnych po cyberataku.
- Rozwijać programy nauczania we wszystkich typach szkół w zakresie podstaw bezpiecznej eksploatacji systemów informatycznych – budowanie powszechnej świadomości bezpieczeństwa cyberprzestrzeni.

Organizacyjnym i funkcjonalnym:

- Racjonalizacja struktury systemu podejmowania decyzji strategiczno-politycznych w kontekście możliwych i prawdopodobnych zagrożeń bezpieczeństwa w cyberprzestrzeni oraz konsolidacja struktur w poszczególnych resortach i na szczeblu rządowym.
- Uznać konieczność współpracy i podziału odpowiedzialności za obszary cyberprzestrzeni między CERT.GOV.PL (administracja publiczna), MIL CERT (wojsko), a CERT Polska, TP CERT, CERT PIONIER, CERT PLIX oraz innymi zespołami CERT istniejącymi w Polsce (biznes i osoby prywatne).
- Wykonywać cykliczne, kompleksowe, wielopoziomowe (od szczebla strategicznego do podstaw fizycznej realizacji) analizy ryzyka zakłócenia funkcjonowania infrastruktury krytycznej z uwzględnieniem zagrożeń cybernetycznych, ze szczególnym uwzględnieniem systemów SCADA (z ang. *Supervisory Control And Data Acquisition*).
- W ramach programów ochrony infrastruktury krytycznej kraju wykonywać cykliczne kompleksowe wielopoziomowe (od szczebla strategicznego do podstaw fizycznej realizacji) analizy ryzyka zagrożeń bezpieczeństwa infrastruktury krytycznej z uwzględnieniem zagrożeń cybernetycznych (np. sterowanie systemami przesyłu energii, informacji powietrznej, zakładów produkcyjnych).
- Stworzenie systemu wymiany informacji (on-line) operacyjnych pomiędzy poszczególnymi podmiotami zarówno państwowymi jak i prywatnymi oraz

rozwój struktury systemu ochrony i aktywnej obrony cyberprzestrzeni we współpracy z nauką i przemysłem.

- Rozwój zdolności do działań w cyberprzestrzeni dzięki planowaniu i realizacji ćwiczeń międzyresortowych, międzypaństwowych, wraz z podmiotami prywatnymi i organizacjami pozarządowymi (operatorzy telekomunikacyjni, przedsiębiorcy teleinformatyczni, stowarzyszenia fundacje) ukierunkowanych na zbieranie doświadczeń i doskonalenie struktur i procedur w odpieraniu ataków teleinformatycznych na infrastrukturę krytyczna państwa. Pierwszy taki trening/ćwiczenie winno mieć miejsce we wrześniu 2012 r. i łączyć zagadnienia klasycznego zarządzania kryzysowego z ochroną cyberprzestrzeni zgodnie z przeświadczeniem, że dzisiaj mamy do czynienia z pięcioma żywiołami: wodą, ogniem, powietrzem, ziemią i cyberprzestrzenią.

Dostrzega się konieczność uruchomienia „Strategicznego programu osłony kryptograficznej systemów bezpieczeństwa państwa". W ramach programu należy przewidzieć:

- Doskonalenie narodowych rozwiązań z zakresu kryptografii we współpracy sfery nauki z firmami komercyjnymi (tworzenie konsorcjów),
- Wdrożenie wytworzonych urządzeń kryptograficznych dla potrzeb Sił Zbrojnych RP i bezpieczeństwa państwa.
- Skrócenie prac certyfikacyjnych w zakresie kryptologii i urządzeń kryptograficznych (np. poprzez tworzenie laboratoriów prowadzących badania wspierające proces certyfikacji).
- Międzynarodową współpracę nad rozwojem metod ewaluacji ryzyka zagrożeń bezpieczeństwa cyberprzestrzeni oraz analizy podatności na zagrożenia systemów krytycznej infrastruktury państwa itp.

Możliwość incydentu w cyberprzestrzeni, mającego charakter zewnętrznego zagrożenia państwa jest obecnie możliwa i bardzo prawdopodobna. Informatyzacja różnych dziedzin życia społecznego spowodowała silne uzależnienie ich funkcjonowania od sieci teleinformatycznych. Mają one wielki wpływ na bezpieczeństwo pojedynczych ludzi, firmy i koncerny, gospodarkę narodową oraz system obronności państwa.

Współczesne systemy informatyczne oraz systemy łączności radiowej ze względu na ogólną dostępność narażone są na ataki zarówno ze strony cyberprzestępców, organizacji terrorystycznych, jak i służb obcych państw. Ataki te najczęściej mają na celu sprawdzenie i praktyczne zweryfikowanie własnej wiedzy atakującego, rozpoznanie obcego systemu informatycznego, kradzież danych wrażliwych lub nawet wykonanie dywersji przez pojedynczych osobników. Zadaniem systemu bezpieczeństwa cyberprzestrzeni RP, w tym ochrony kryptograficznej i aktywnego nadzoru administratorów sieci, jest niedopuszczenie do takich ataków, reagowanie na bieżące zagrożenia oraz wykrywanie sprawców.

Z powyższych powodów oczywistym jest, że: *w sytuacji szczególnego zagrożenia konstytucyjnego ustroju państwa, bezpieczeństwa obywateli lub porządku publicznego, w tym spowodowanego działaniami o charakterze terrorystycznym lub działaniami w cyberprzestrzeni, które nie może być usunięte poprzez użycie zwykłych środków konstytucyjnych, Rada Ministrów może podjąć uchwalę o skierowaniu do Prezydenta Rzeczypospolitej Polskiej wniosku o wprowadzenie stanu wyjątkowego.* Należy jednak uznać obecny stan prawny za niezadowalający w zakresie oceny i kwalifikacji czynów godzących w bezpieczeństwo informacyjne podmiotów oraz bezpieczeństwo cyberprzestrzeni państwa. Stan ten dotyczy także obecnie stosowanej terminologii oraz ogólnych zasad współpracy międzynarodowej i międzyresortowej w zakresie bezpieczeństwa cyberprzestrzeni RP. Proponowana debata publiczna w ramach Roku Ochrony Cyberprzestrzeni miałaby szansę zintegrować działania i zwiększyć świadomość konieczności zapewnienia powszechnego bezpieczeństwa teleinformatycznego.