POLSKIE TOWARZYSTWO INFORMATYCZNE
Zarząd Główny, al. Solidarności 82A m. 5, 01-003 Warszawa, tel.: + 48 22 838 47 05, tel./fax: + 48 22 636 89 87, e-mail: pti@pti.org.pl,
www.pti.org.pl
Adres korespondencyjny: ul. Puławska 39 lok. 4, 02-508 Warszawa

Warszawa, 30 października 2012 r.

Opinia
Polskiego Towarzystwa Informatycznego
do projektu „Polityki Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej"
z dnia 18 września 2012 roku.

Polskie Towarzystwo Informatyczne z zadowoleniem przyjmuje fakt powstania dokumentu „Polityka ochrony cyberprzestrzeni RP" (dalej POCRP, Polityka) i dziękuje za możliwość uczestniczenia w procesie opiniowania tego dokumentu.

Koncepcję stworzenia dokumentu strategicznego mającego na celu osiągnięcie akceptowalnego poziomu bezpieczeństwa teleinformatycznego państwa należy ocenić jako słuszną.

1. Uwagi ogólne

1. Dokument POCRP jest zbyt ogólnikowy. Nie definiuje żadnych standardów ani wymagań minimalnych.

2. Zaletą dokumentu jest rozwiązanie kompetencyjnego sporu w sprawie odpowiedzialności za bezpieczeństwo teleinformatyczne państwa i ustalenie, że za bezpieczeństwo infrastruktury informatycznej państwa odpowiada Ministerstwo Administracji i Cyfryzacji. Należy jednakże mieć na uwadze, że z jego kompetencji wyłączono wojsko, służby, służbę zdrowia, sądownictwo i wymiar sprawiedliwości.

3. Zaletą Polityki jest zapowiedź przeglądu regulacji prawnych związanych z bezpieczeństwem teleinformatycznym oraz określenie założeń proceduralno-organizacyjnych dotyczących bezpieczeństwa teleinformatycznego.

4. Z zadowoleniem należy przyjąć proponowane w POCRP wprowadzenie tematyki bezpieczeństwa teleinformatycznego jako stałego elementu kształcenia: na uczelniach wyższych, kształcenia kadry administracji oraz kampanię społeczną o charakterze edukacyjnym.

2. Uwagi szczegółowe

1. Dokument POCRP mówi, że osiągnięcie akceptowalnego poziomu bezpieczeństwa teleinformatycznego Państwa jest realizowane poprzez „stworzenie ram organizacyjno-prawnych

oraz systemu skutecznej koordynacji i wymiany informacji pomiędzy użytkownikami CRP". To sformułowanie sugeruje, że do zapewnienia bezpieczeństwa cyberprzestrzeni wystarczą działania organizacyjne i proceduralne.

2. Dokument POCRP nie adresuje konieczności opracowania spójnej architektury bezpieczeństwa w skali państwa.

3. Polityka nie przedstawia szczegółów współpracy z przedsiębiorcami w zakresie dostarczania wiedzy i rozwiązań, jak również wspólnej realizacji zadań dotyczących bezpieczeństwa teleinformatycznego.

4. W dokumencie Polityki nie określono źródeł finansowania proponowanych działań. Nie można budować i wdrażać rozwiązań bezpieczeństwa za darmo, bez ponoszenia np. kosztów szkoleń, aktualizacji sprzętu i oprogramowania, usuwanie podatności na zagrożenia. POCRP powinna wskazać potencjalne źródła finansowania przedsięwzięć. Jest to tym ważniejsze, że nie można wprost określić zwrotu z inwestycji w obszarze bezpieczeństwa IT.

5. W dokumencie POCRP kładzie się duży nacisk na reagowanie na incydenty bezpieczeństwa a zbyt mały na działania prewencyjne np. korzystanie z zespołów CERT w celu uprzedzania o możliwych zagrożeniach.

6. Dokument Polityka POCRP nie określa miejsca pełnomocnika bezpieczeństwa cyberprzestrzeni w strukturze jednostki organizacyjnej, nie wskazuje zakresu uprawnień i odpowiedzialności, koniecznego wykształcenia i doświadczenia.

7. Polityka Dokument POCRP zaleca wzmocnienie zespołów reagowania na cyberataki, przy ABW i NASK. Natomiast w niewielkim stopniu porusza tematykę działań i rozwiązań zapobiegającym atakom. Atak jest najczęściej skutkiem uprzednich zaniedbań lub przyjęcia nieuzasadnionych – zbyt optymistycznych założeń w szacowaniu ryzyka.

8. Polityka bezpieczeństwa teleinformatycznego państwa nie może być realizowana za wszelką cenę. Nie powinna ona naruszać wolności słowa, czy też anonimowej komunikacji w sieci. Zapisy przedstawione w pkt 3.6.3 budzą obawy, że do ochrony cyberprzestrzeni mogą w przyszłości zostać wykorzystane mechanizmy i narzędzia umożliwiające monitorowanie zachowań użytkowników lub filtrowanie bądź blokowanie treści, nawet mogą być stosowane niejawnie.

9. Dokument POCRP nie wskazuje miejsca usytuowania pełnomocnika bezpieczeństwa cyberprzestrzeni strukturze jednostki organizacyjnej, jednak rola pełnomocnika powinna zostać przypisana osobie odpowiedzialnej za realizację procesu bezpieczeństwa teleinformatycznego. Nasuwa się pytanie czy ustanowienie PBC na dowolnym szczeblu struktury organizacyjnej umożliwi mu realizację obowiązków.

10. Dokument nie bierze pod uwagę zmian zachodzących w technikach informatycznych. Np. w dokumencie nie uwzględniono faktu, że coraz więcej procesów realizowanych jest z wykorzystanie urządzeń mobilnych lub rozwiązań opartych na technologii chmury. POCRP

powinna być przeglądana przez kompetentne i poinformowane osoby aby stwierdzić czy w kolejnych latach jest jeszcze przydatna.

11. W punkcie 3.4.2 ”System zarządzania bezpieczeństwem w jednostce” autorzy dokumentu powołują się na „*obowiązki wynikające z ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. Nr, poz. 565, z późn. zm.) dotyczące minimalnych wymagań dla systemów teleinformatycznych w zakresie bezpieczeństwa informacji.*” natomiast nie nawiązuje do Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. 2012, pozycja 526). Rozporządzenie to określa metody i wytyczne do budowania systemów teleinformatycznych administracji publicznej i zawiera szereg wytycznych dotyczących bezpieczeństwa teleinformatycznego (z odwołaniem do norm z serii 27000). Rozporządzenie KRI przejęło także funkcje wcześniejszego rozporządzenia o minimalnych wymaganiach wobec systemów teleinformatycznych (Dz. U. z dnia 28 października 2005).

12. W wielu miejscach dokumentu POCRP i występują pojęcia „ocena ryzyka” i „analiza ryzyka”. Proponujemy oprzeć się na terminologii polskich norm z serii 27000, a w szczególności normy PN-ISO/IEC 27005:2010 „Technika informatyczna -- Techniki bezpieczeństwa -- Zarządzanie ryzykiem w bezpieczeństwie informacji”, gdzie *analiza* ryzyka i *ocena* ryzyka to dwa etapy *szacowania ryzyka*.

3. Wnioski

Zdaniem Polskiego Towarzystwa Informatycznego przedłożony projekt Polityki należy poddać istotnym modyfikacjom. Wśród nich powinny się znaleźć:

1. Uspójnienie z obowiązującymi aktami prawnymi (np. Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych).
2. Konsekwentne przyjęcie terminologii z norm serii PN ISO/IEC 27000.
3. Zdefiniowanie odpowiedzialności i uprawnień osób związanych z zapewnieniem bezpieczeństwa cyberprzestrzeni.
4. Określenie realnych źródeł finansowania działań zdefiniowanych w Polityce.

Projekt opinii przygotował zespół ekspertów Polskiego Towarzystwa Informatycznego.