Wersja: wrzesień 2012

RZECZPOSPOLITA POLSKA
Ministerstwo Administracji i Cyfryzacji,
Agencja Bezpieczeństwa Wewnętrznego

POLITYKA OCHRONY CYBERPRZESTRZENI RZECZYPOSPOLITEJ POLSKIEJ

WARSZAWA
18 Wrzesień 2012

SPIS TREŚCI:

1. GŁÓWNE PRZESŁANKI I ZAŁOŻENIA *POLITYKI* OCHRONY CYBERPRZESTRZENI RP 4

1.1. TERMINY 6
1.2. CEL STRATEGICZNY 8
1.3. CELE SZCZEGÓŁOWE 8
1.4. ADRESACI I ZAKRES ODDZIAŁYWANIA 9
1.5. USTANOWIENIE ODPOWIEDZIALNOŚCI ZA BEZPIECZEŃSTWO CRP 10
1.6. ZGODNOŚĆ ***POLITYKI*** Z AKTAMI PRAWNYMI 11

2. UWARUNKOWANIA I PROBLEMY OBSZARU CYBERPRZESTRZENI 12

3. GŁÓWNE KIERUNKI DZIAŁAŃ 14

3.1 OCENA RYZYKA 14
3.2 BEZPIECZEŃSTWO PORTALI ADMINISTRACJI RZĄDOWEJ 15
3.3 ZAŁOŻENIA DZIAŁAŃ LEGISLACYJNYCH 15
3.4 ZAŁOŻENIA DZIAŁAŃ PROCEDURALNO-ORGANIZACYJNYCH 15
3.4.1 Zarządzanie bezpieczeństwem cyberprzestrzeni RP 16
3.4.2 System zarządzania bezpieczeństwem w jednostce organizacyjnej 16
3.4.3 Rola kierowników jednostek organizacyjnych 17
3.5 ZAŁOŻENIA DOTYCZĄCE KSZTAŁCENIA, SZKOLEŃ I UŚWIADAMIANIA W DZIEDZINIE BEZPIECZEŃSTWA 18
3.5.1. Szkolenia pełnomocników ds. bezpieczeństwa cyberprzestrzeni 18
3.5.2. Wprowadzenie tematyki bezpieczeństwa teleinformatycznego jako stałego elementu kształcenia na uczelniach wyższych. 18
3.5.3. Kształcenie kadry urzędniczej w administracji rządowej 19
3.5.4. Kampania społeczna o charakterze edukacyjno - prewencyjnym 19
3.6 ZAŁOŻENIA DZIAŁAŃ TECHNICZNYCH 21
3.6.1 Programy badawcze 21
3.6.2 Rozbudowa zespołów reagowania na incydenty bezpieczeństwa teleinformatycznego w administracji rządowej 21
3.6.3 Rozbudowa systemu wczesnego ostrzegania oraz wdrażanie *i utrzymanie rozwiązań prewencyjnych* 22
3.6.4 Testowanie poziomu zabezpieczeń i ciągłość działania 22
3.6.5 Rozwój zespołów bezpieczeństwa 22

4. WDROŻENIE I MECHANIZMY REALIZACJI ZAPISÓW DOKUMENTU 24

4.1 NADZÓR I KOORDYNACJA WDROŻENIA 24
4.2 KRAJOWY SYSTEM REAGOWANIA NA INCYDENTY KOMPUTEROWE W CYBERPRZESTRZENI RP 24
4.3 MECHANIZM WYMIANY INFORMACJI 25
4.4 SPOSOBY I FORMY WSPÓŁPRACY 25
4.5 WSPÓŁPRACA Z PRZEDSIĘBIORCAMI 25
4.5.1 Współpraca z producentami urządzeń i systemów teleinformatycznych 26
4.5.2 Współpraca z przedsiębiorcami telekomunikacyjnymi 26
4.6 WSPÓŁPRACA MIĘDZYNARODOWA 26

5. FINANSOWANIE 27

6. OCENA SKUTECZNOŚCI *POLITYKI* 28

6.1 PRZEWIDYWANE EFEKTY ***POLITYKI*** 30
6.2 SKUTECZNOŚĆ DZIAŁAŃ 30
6.3 MONITOROWANIE EFEKTYWNOŚCI DZIAŁAŃ W RAMACH PRZYJĘTEJ ***POLITYKI*** 30
6.4 KONSEKWENCJE NARUSZENIA ZAPISÓW ***POLITYKI*** 31

Niniejszy dokument został opracowany w Ministerstwie Administracji i Cyfryzacji we współpracy z Agencją Bezpieczeństwa Wewnętrznego w oparciu o:

- omówiony 9 marca 2009 r. przez Komitet Stały Rady Ministrów dokument „Rządowy program ochrony cyberprzestrzeni RP na lata 2009-2011 – założenia”,
- okresowe raporty o stanie bezpieczeństwa obszaru gov.pl, publikowane przez Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL,
- decyzję Przewodniczącego Komitetu Rady Ministrów do spraw Cyfryzacji nr 1/2012 z dnia 24 stycznia 2012r. w przedmiocie powołania Zespołu zadaniowego do spraw ochrony portali rządowych.

1. GŁÓWNE PRZESŁANKI I ZAŁOŻENIA *POLITYKI* OCHRONY CYBERPRZESTRZENI RP

W obliczu globalizacji bezpieczeństwo cyberprzestrzeni stało się jednym z podstawowych celów strategicznych w obszarze bezpieczeństwa każdego państwa. W czasie, gdy panuje swoboda przepływu osób, towarów, informacji i kapitału - bezpieczeństwo demokratycznego państwa zależy od wypracowania mechanizmów pozwalających skutecznie zapobiegać i zwalczać zagrożenia dla bezpieczeństwa cyberprzestrzeni.

Z uwagi na wzrost zagrożeń dla systemów teleinformatycznych, od których całkowita separacja jest niemożliwa, a także fakt rozproszonej odpowiedzialności za bezpieczeństwo teleinformatyczne, jest niezbędne skoordynowanie działań, które umożliwią szybkie i efektywne reagowanie na ataki wymierzone przeciwko systemom teleinformatycznym i oferowanym przez nie usługom.

Systemy teleinformatyczne eksploatowane przez administrację rządową, organy władzy ustawodawczej, władzę sądowniczą, samorząd terytorialny, a także systemy strategiczne z punktu widzenia bezpieczeństwa Państwa jak również przedsiębiorcy oraz osoby fizyczne są objęte niniejszą „Polityką Ochrony Cyberprzestrzeni Rzeczpospolitej Polskiej", zwaną dalej ***Polityką***.

Niniejszą ***Polityką*** Rząd Rzeczypospolitej Polskiej przyjmuje, że poprzez swoich przedstawicieli bierze czynny udział w zapewnieniu bezpieczeństwa zasobów informacyjnych Państwa, jego obywateli oraz realizuje swoje konstytucyjne obowiązki.

W ramach ***Polityki*** przyjmuje się wparcie dla inicjatyw społecznych mających na celu realizację zadań zbieżnych z niniejszym dokumentem.

Rząd Rzeczypospolitej Polskiej, przy wypełnianiu obowiązków konstytucyjnych realizowanych za pomocą cyberprzestrzeni, konsultuje się ze zorganizowanymi grupami społeczeństwa, a w szczególności z przedstawicielami przedsiębiorców telekomunikacyjnych oraz dostawców świadczących usługi drogą elektroniczną, celem uzgodnienia akceptowalnego poziomu bezpieczeństwa realizacji przedmiotowych obowiązków.

Przyjmując status ***Polityki*** dla przedmiotowego dokumentu należy wskazać, że w ramach obowiązującego systemu rządowych dokumentów strategicznych ***Polityka*** mieści się w grupie dokumentów strategicznych doprecyzowujących kierunki działań wskazanych

w strategiach, programach rozwoju i innych dokumentach programowych, które nie wskazują nowych priorytetów i działań. Określają one wizję rozwoju danego sektora oraz sposoby jej realizacji opierając się na zapisach odpowiednich dokumentów.

Polityka nie obejmuje swoim obszarem zadaniowym niejawnych systemów teleinformatycznych. Należy podkreślić, że obszar ochrony informacji niejawnych posiada własne regulacje prawne i stosowne mechanizmy ochronne. Posiada struktury organizacyjne dedykowane do ochrony informacji niejawnych wytwarzanych, przetwarzanych oraz przechowywanych w wydzielonych systemach teleinformatycznych. Podstawowym aktem prawnym jest ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. Nr 182, poz. 1228).

1.1. Terminy

Użyte w niniejszym dokumencie określenia, skróty oznaczają:

→ Abuse - zwyczajowa nazwa działu bezpieczeństwa u dostawcy usług internetowych, który zarządza procesem reakcji na incydenty komputerowe i rozpatrywaniem skarg dotyczących nadużyć,

→ bezpieczeństwo cyberprzestrzeni - zespół przedsięwzięć organizacyjno-prawnych, technicznych, fizycznych i edukacyjnych mający na celu zapewnienie niezakłóconego funkcjonowania cyberprzestrzeni,

→ CERT (ang. Computer Emergency Response Team), CSIRT (ang. Computer Security Incydent Response Team) - zespół powołany do reakcji na zdarzenia naruszające bezpieczeństwo w sieci Internet,

→ cyberatak - celowe zakłócenie prawidłowego funkcjonowania cyberprzestrzeni,

→ cyberprzestępstwo - czyn zabroniony popełniony w obszarze cyberprzestrzeni,

→ cyberprzestrzeń - przestrzeń przetwarzania i wymiany informacji tworzona przez systemy teleinformatyczne, określone w art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. Nr 64, poz. 565, z późn. zm.) wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami; zgodnie z ustawą z dnia 30 sierpnia 2011 r. o zmianie ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw (Dz. U. Nr 222, poz. 1323),

→ cyberprzestrzeń RP (dalej, jako CRP) - cyberprzestrzeń w obrębie terytorium państwa polskiego i poza jego terytorium, w miejscach gdzie funkcjonują przedstawiciele RP (placówki dyplomatyczne, kontyngenty wojskowe),

→ cyberterroryzm - przestępstwo o charakterze terrorystycznym popełnione w cyberprzestrzeni,

→ incydent związany z bezpieczeństwem informacji - pojedyncze zdarzenie lub seria niepożądanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji - (wg norm serii PN-ISO/IEC 27000),

→ jednostka organizacyjna - jednostka organizacyjna w rozumieniu ustawy z dnia 23 kwietnia 1964 r. - Kodeks cywilny (Dz. U. Nr 16, poz. 93, z późn. zm.),

→ PBC - pełnomocnik ds. bezpieczeństwa cyberprzestrzeni w jednostkach organizacyjnych administracji publicznej,

→ przedsiębiorca - przedsiębiorca w rozumieniu art. 4 ustawy z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej (Dz. U. z 2010 r. Nr 220, poz. 1447, z późn. zm.) lub każda inna jednostka organizacyjna, niezależnie od formy własności,

→ Sektorowy Punkt Kontaktowy - punkt kontaktu pomiędzy podmiotami działającymi w tej samej branży umożliwiający przepływ informacji pomiędzy nimi a właściwymi zespołami CERT lub Abuse,

→ użytkownik cyberprzestrzeni - każda jednostka organizacyjna, urząd obsługujący organ administracji publicznej, przedsiębiorca oraz osoba fizyczna, który korzysta z zasobów cyberprzestrzeni.

1.2. Cel strategiczny

Celem strategicznym *Polityki* jest osiągnięcie akceptowalnego poziomu bezpieczeństwa cyberprzestrzeni Państwa.

Osiągnięcie celu strategicznego jest realizowane poprzez stworzenie ram organizacyjno-prawnych oraz systemu skutecznej koordynacji i wymiany informacji pomiędzy użytkownikami CRP.

Działania podejmowane w celu realizacji celu strategicznego są wynikiem ocen ryzyka prowadzonych przez uprawnione podmioty, w odniesieniu do zagrożeń występujących w cyberprzestrzeni.

Jednocześnie ***Polityka*** jest zgodna z celami zawartymi w:

1) Europejskiej Agendzie Cyfrowej Rady Europejskiej [KOM(2010)245];
2) Strategii Rozwoju Społeczeństwa Informacyjnego;
3) Strategii Bezpieczeństwa Narodowego;
4) Średniookresowej Strategii Rozwoju Kraju;
5) Strategii „Europa 2020";
6) Strategii Sprawne Państwo.

1.3. Cele szczegółowe

1) Zwiększenie poziomu bezpieczeństwa infrastruktury teleinformatycznej Państwa.
2) Zwiększenie zdolności do zapobiegania i zwalczania zagrożeń ze strony cyberprzestrzeni.
3) Zmniejszenie skutków incydentów godzących w bezpieczeństwo teleinformatyczne.
4) Określenie kompetencji podmiotów odpowiedzialnych za bezpieczeństwo cyberprzestrzeni.
5) Stworzenie i realizacja spójnego dla wszystkich podmiotów administracji rządowej systemu zarządzania bezpieczeństwem cyberprzestrzeni oraz ustanowienie wytycznych w tym zakresie dla podmiotów niepublicznych.

6) Stworzenie trwałego systemu koordynacji i wymiany informacji pomiędzy podmiotami odpowiedzialnymi za bezpieczeństwo cyberprzestrzeni oraz użytkownikami cyberprzestrzeni.

7) Zwiększenie świadomości użytkowników cyberprzestrzeni w zakresie metod i środków bezpieczeństwa w cyberprzestrzeni.

Cele ***Polityki*** są realizowane przez:

a) system koordynacji przeciwdziałania i reagowania na zagrożenia i ataki na cyberprzestrzeń, w tym ataki o charakterze terrorystycznym;

b) powszechne wdrożenie wśród jednostek administracji rządowej, a także podmiotów niepublicznych mechanizmów służących zapobieganiu i wczesnemu wykrywaniu zagrożeń dla bezpieczeństwa cyberprzestrzeni oraz właściwemu postępowaniu w przypadku stwierdzonych incydentów;

c) powszechną oraz specjalistyczną edukację społeczną w zakresie bezpieczeństwa CRP.

1.4. Adresaci i zakres oddziaływania

Adresatami ***Polityki*** są wszyscy użytkownicy cyberprzestrzeni w obrębie Państwa i poza jego terytorium, w miejscach gdzie funkcjonują przedstawiciele RP (placówki dyplomatyczne, kontyngenty wojskowe).

Niniejsza ***Polityka*** obowiązuje administrację rządową:

1) urzędy obsługujące naczelne organy administracji rządowej: Prezesa Rady Ministrów, Radę Ministrów, ministrów i przewodniczących określonych w ustawach komitetów;

2) urzędy obsługujące centralne organy administracji rządowej: organy inne niż w/wym, tj. organy podporządkowane Prezesowi Rady Ministrów, bądź poszczególnym ministrom;

3) urzędy obsługujące terenowe organy administracji rządowej: wojewodów, organy administracji zespolonej i niezespolonej;

4) Rządowe Centrum Bezpieczeństwa.

Jednocześnie ***Polityka*** jest rekomendowana dla administracji samorządowej szczebla gminnego, powiatowego i wojewódzkiego oraz innych urzędów (jednostki nie należące do administracji rządowej i samorządowej), w tym:

a) Kancelarii Prezydenta Rzeczypospolitej Polskiej;
b) Kancelarii Sejmu Rzeczypospolitej Polskiej;
c) Kancelarii Senatu Rzeczypospolitej Polskiej;
d) Biura Krajowej Rady Radiofonii i Telewizji;
e) Biura Rzecznika Praw Obywatelskich;
f) Biura Rzecznika Praw Dziecka;
g) Biura Krajowej Rady Sądownictwa;
h) urzędów organów kontroli państwowej i ochrony prawa;
i) Narodowego Banku Polskiego;
j) urzędu Komisji Nadzoru Finansowego;
k) państwowych osób prawnych i innych niż wymienione wyżej państwowe jednostki organizacyjne.

Polityka stanowi jednocześnie wskazówkę do działań dla wszystkich innych użytkowników cyberprzestrzeni, którzy nie zostali wymienieni powyżej.

1.5. Ustanowienie odpowiedzialności za bezpieczeństwo CRP

Za bezpieczeństwo CRP odpowiada Rada Ministrów, która zadania w tym zakresie wykonuje przez:

1) Ministra Administracji i Cyfryzacji,
2) Ministra Obrony Narodowej,
3) Ministra Spraw Wewnętrznych,
4) Szefa Agencji Bezpieczeństwa Wewnętrznego,
5) Szefa Służby Kontrwywiadu Wojskowego,
6) inne organy administracji rządowej.

Przyjęcie odpowiedzialności za bezpieczeństwo CRP przez Radę Ministrów nie zwalnia użytkowników CRP z obowiązku należytej dbałości o bezpieczeństwo własne oraz zasobów i rozwiązań teleinformatycznych pozostających w ich posiadaniu. Zakłada się, iż

systemy zapewniające bezpieczeństwo, budowane przez administrację rządową oraz przez użytkowników CRP, nawzajem się uzupełniają współtworząc bezpieczeństwo CRP.

Dla sukcesu ***Polityki*** niezbędny jest aktywny udział użytkowników CRP w działaniach mających na celu podniesienie poziomu jej bezpieczeństwa.

Ważne jest także zwiększenie udziału użytkowników CRP w realizacji ***Polityki*** przez konsultowanie jej zawartości oraz udział w koordynacji realizacji ***Polityki*** i jej przeglądów z przedstawicielami społeczeństwa i społeczności teleinformatycznej.

Powszechne stosowanie przez użytkowników CRP rozwiązań mających na celu podniesienie jej bezpieczeństwa będzie wyrazem akceptacji dla działań podejmowanych przez Rząd RP w tym obszarze.

1.6. Zgodność *Polityki* z aktami prawnymi

Polityka jest zgodna z powszechnie obowiązującym prawem Rzeczypospolitej Polskiej (Konstytucja, ustawy, ratyfikowane umowy międzynarodowe oraz rozporządzenia) i nie narusza postanowień żadnego z nich.

2. UWARUNKOWANIA I PROBLEMY OBSZARU CYBERPRZESTRZENI

Funkcjonowanie Państwa i realizacja przez nie obowiązków konstytucyjnych w coraz większym stopniu uzależnione jest od rozwoju nowoczesnych technologii, społeczeństwa informacyjnego oraz niezakłóconego funkcjonowania cyberprzestrzeni. Obecnie bezpieczne funkcjonowanie cyberprzestrzeni w dużej mierze zależne jest od bezpieczeństwa infrastruktury teleinformatycznej umożliwiającej korzystanie z cyberprzestrzeni, zgromadzonych w niej zasobów informacyjnych i usług, które dzięki niej funkcjonują. Infrastruktura funkcjonująca w CRP umożliwia wywiązanie się Państwa z konstytucyjnych obowiązków względem obywateli, zapewnia ciągłość i efektywność działania administracji rządowej oraz niezakłócony i efektywny rozwój gospodarki Rzeczypospolitej Polskiej.

Rząd RP widzi konieczność prowadzenia działań mających na celu zapewnienie bezpieczeństwa infrastruktury teleinformatycznej Państwa, tj. zapewnienie poprawności i ciągłości funkcjonowania systemów teleinformatycznych, obiektów i instalacji wykorzystywanych do realizacji konstytucyjnych zadań Państwa względem obywateli oraz jego bezpieczeństwa wewnętrznego. W tym celu jest niezbędne wyznaczenie minimalnego standardu bezpieczeństwa, który pozwoli na realizację tego celu oraz pozwoli ograniczyć do minimum ewentualne szkody, jakie może nieść za sobą atak na poszczególne elementy cyberprzestrzeni RP. ***Polityka*** stanowi podstawę wypracowania koncepcji zarządzania bezpieczeństwem infrastruktury funkcjonującej w ramach CRP oraz wypracowania wytycznych do opracowania podstawy prawnej służącej wykonywaniu zadań w tym zakresie przez administrację rządową. Zasady zapewnienia bezpieczeństwa cyberprzestrzeni wypracowane w ramach współpracy, o której mowa w pkt 4.4, w zakresie infrastruktury CRP są rekomendowane również przedsiębiorcom.

Działania dotyczące bezpieczeństwa infrastruktury teleinformatycznej będą komplementarne w stosunku do działań mających na celu ochronę infrastruktury krytycznej Państwa. ***Polityka*** w tym zakresie nie narusza postanowień zawartych w Narodowym Programie Ochrony Infrastruktury Krytycznej.

Polityka wskazuje konieczność wypracowania koncepcji zapewnienia bezpieczeństwa infrastruktury funkcjonującej w ramach CRP oraz przygotowania podstaw prawnych do wykonywania zadań w tym zakresie przez administrację rządową.

Infrastruktura teleinformatyczna CRP musi być chroniona przed atakami z cyberprzestrzeni, zniszczeniem, uszkodzeniem i dostępem osób nieuprawnionych.

W ramach działań związanych z realizacją ***Polityki*** jest prowadzona ocena ryzyka z uwzględnieniem identyfikacji zasobów, podsystemów, funkcji i zależności od innych systemów istotnych z punktu widzenia funkcjonowania CRP. Jednocześnie wdrożenie ***Polityki*** pozwoli na opracowanie docelowych wytycznych do realizacji oceny ryzyka oraz szablonów sprawozdań zawierających ogólne dane dotyczące rodzajów ryzyka, zagrożeń oraz słabych punktów stwierdzonych w każdym z sektorów gospodarki RP w odniesieniu do zadań konstytucyjnych realizowanych w oparciu o CRP.

Istnieje potrzeba wypracowania, na podstawie prowadzonej analizy ryzyka, minimalnych standardów bezpieczeństwa zgodnie z którymi będą zabezpieczane zidentyfikowane zasoby i systemy, dzięki którym są realizowane konstytucyjne obowiązki Państwa.

3. GŁÓWNE KIERUNKI DZIAŁAŃ

Polityka będzie realizowana poprzez poniższe działania, zgodnie z priorytetami wynikającymi z przedstawionej kolejności.

3.1 Ocena ryzyka

Ocena ryzyka związana z funkcjonowaniem cyberprzestrzeni jest kluczowym elementem procesu bezpieczeństwa cyberprzestrzeni, determinującym i uzasadniającym działania podejmowane w celu jego obniżenia do akceptowalnego poziomu.

W celu osiągnięcia akceptowalnego poziomu bezpieczeństwa, zakłada się, iż każda jednostka administracji rządowej, o której mowa w pkt 1.4 (punkty 1-4), w terminie do 31 stycznia każdego roku przekaże do ministra właściwego ds. informatyzacji sprawozdanie podsumowujące oceny ryzyka (wg wzorca opracowanego przez ministra właściwego ds. informatyzacji). Sprawozdanie powinno zawierać ogólne dane dotyczące rodzajów ryzyka, zagrożeń i słabych punktów zdiagnozowanych w każdym z sektorów, w których poszczególna instytucja działa i za które odpowiada. W sprawozdaniu winny być przedstawione także informacje o sposobach postępowania z ryzykiem.

Zadaniem ministra właściwego ds. informatyzacji powinno być przekazanie, do Prezesa Rady Ministrów, w terminie do 31 marca każdego roku, sprawozdania zawierającego ogólne dane dotyczące rodzajów zagrożeń i słabych punktów zdiagnozowanych w cyberprzestrzeni RP.

Minister właściwy ds. informatyzacji we współpracy z zaangażowanymi instytucjami określi jednolitą metodykę przeprowadzania analiz ryzyka. Istnieje konieczność, aby używanie tej metodyki było docelowo obligatoryjne dla instytucji administracji rządowej.

Zalecane jest, aby Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL przedstawił ministrowi właściwemu ds. informatyzacji, w celu zunifikowanego podejścia, opracowane katalogi zawierające specyfikację zagrożeń oraz możliwych podatności godzących w bezpieczeństwo cyberprzestrzeni.

3.2 Bezpieczeństwo portali administracji rządowej

Głównym miejscem wymiany informacji pomiędzy jednostkami administracji a obywatelem, w e-społeczeństwie, są strony internetowe. Winny one spełniać podstawowe wymagania bezpieczeństwa, to jest zapewniać odpowiednią dostępność, integralność oraz poufność danych. Każda jednostka organizacyjna powinna samodzielnie ocenić ryzyko (o którym mowa w pkt. 3.1) dla swoich portali. Zakłada się, iż na tej podstawie zostaną zaimplementowane odpowiednie (w zależności od typu portalu i wyników oceny ryzyka) rozwiązania organizacyjno-techniczne pozwalające na zapewnienie odpowiedniego poziomu bezpieczeństwa. Ze względu na różne typy stron i różne ich priorytety, rozwiązania te będą się różnić od siebie.

Proponuje się, aby jednostki administracji rządowej prowadzące portale internetowe, poza spełnieniem minimalnych wymogów, wdrożyły również odpowiednie zalecenia oraz dobre praktyki z zakresu bezpieczeństwa, które przygotuje Zespół zadaniowy do spraw ochrony portali rządowych we współpracy z Rządowym Zespołem Reagowania na Incydenty Komputerowe CERT.GOV.PL.

3.3 Założenia działań legislacyjnych

Podstawowym elementem realizacji ***Polityki***, przewidzianym niezwłocznie do wykonania, są działania legislacyjne. Rada Ministrów, rozumiejąc wysoki priorytet tych działań, widzi potrzebę ich zainicjowania przez ministra właściwego ds. informatyzacji, aby stworzyć regulacje prawne, dające podstawy do podejmowania dalszych działań w ramach wdrożenia zapisów ***Polityki***. Konieczny jest przegląd obecnie obowiązujących regulacji prawnych mających na względzie przygotowanie rozwiązań w celu zwiększenia poczucia bezpieczeństwa nie tylko instytucji rządowych ale wszystkich użytkowników cyberprzestrzeni.

3.4 Założenia działań proceduralno-organizacyjnych

Ważnym etapem realizacji ***Polityki*** będą działania proceduralno-organizacyjne. Ich celem jest optymalizacja funkcjonowania CRP poprzez wprowadzenie w życie najlepszych

praktyk i standardów w tym zakresie. Na tym etapie konieczne jest wykorzystanie zarówno narzędzi prawnych stworzonych w pierwszym etapie, jak i mechanizm „miękkich"[1] regulacji.

Wykonanie tego etapu nastąpi dzięki uruchomieniu oddzielnych projektów szczegółowych.

3.4.1 Zarządzanie bezpieczeństwem cyberprzestrzeni RP

W ramach zarządzania bezpieczeństwem cyberprzestrzeni RP, a także w celu usprawnienia procesu realizacji celów ***Polityki*** oraz zapewnienia skuteczności działań organów władzy państwowej w zakresie bezpieczeństwa CRP jest niezbędne powołanie przez Prezesa Rady Ministrów zespołu odpowiedzialnego za przygotowywanie rekomendacji dla właściwego ministra z zakresu wykonania czy koordynacji wszelkich działań związanych z jej bezpieczeństwem (zwanego dalej Zespołem).

Zespół może zostać zorganizowany poprzez rozwinięcie istniejącego Zespołu zadaniowego do spraw ochrony portali rządowych, powołanego przez Przewodniczącego Komitetu Rady Ministrów do spraw Cyfryzacji decyzją nr 1/2012 z dnia 24 stycznia 2012 r.

Zaleca się, aby Zespół, w terminie 30 dni od dnia powołania, przygotował i przedstawił do zatwierdzenia Radzie Ministrów plan działań w zakresie bezpieczeństwa cyberprzestrzeni RP.

Podstawowym zadaniem Zespołu powinno być rekomendowanie działań mających na celu koordynowanie działań instytucji realizujących zadania nałożone przez Politykę, organizacja cyklicznych spotkań, rekomendowanie proponowanych rozwiązań z zakresu bezpieczeństwa CRP.

Zakłada się, że w zakresie realizacji zadań związanych z bezpieczeństwem CRP w obszarze administracji rządowej i obszarze cywilnym, rolę głównego zespołu CERT pełni Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL. Analogicznie, w obszarze militarnym, rolę taką pełni „Resortowe Centrum Zarządzania Bezpieczeństwem Sieci i Usług Teleinformatycznych".

3.4.2 System zarządzania bezpieczeństwem w jednostce organizacyjnej

W każdej jednostce organizacyjnej administracji rządowej, w ramach zapewnienia bezpieczeństwa cyberprzestrzeni, kierownik jednostki powinien ustanowić system

[1] Jako miękką regulację rozumie się np. kodeksy dobrych praktyk, wytyczne, zalecenia, kodeks etyczny, etykietę, dobre praktyki czy też normy itp.

zarządzania bezpieczeństwem informacji, w oparciu o obowiązujące przepisy i najlepsze praktyki.

Zakłada się, że podmiot publiczny będzie opracowywał i modyfikował w zależności od potrzeb, a także wdrażał politykę bezpieczeństwa dla systemów teleinformatycznych używanych przez niego do realizacji zadań publicznych. Przy opracowywaniu ***Polityki*** bezpieczeństwa podmiot publiczny uwzględnia 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.

W celu zapewnienia spójności polityk bezpieczeństwa informacji jednostek organizacyjnych, zakłada się, że minister właściwy ds. informatyzacji w porozumieniu z Ministrem Obrony Narodowej i Szefem Agencji Bezpieczeństwa Wewnętrznego może przygotować wytyczne dotyczące systemów zarządzania bezpieczeństwem informacji.

3.4.3 Rola kierowników jednostek organizacyjnych

W ramach jednostek organizacyjnych administracji rządowej powinna zostać określona rola pełnomocnika ds. bezpieczeństwa cyberprzestrzeni (dalej jako PBC).

Zadania pełnomocnika w zakresie bezpieczeństwa cyberprzestrzeni winny obejmować swoim zakresem przede wszystkim:

1) realizację obowiązków wynikających z przepisów aktów prawnych właściwych dla zapewnienia bezpieczeństwa cyberprzestrzeni;
2) opracowanie i wdrożenie procedur reagowania na incydenty komputerowe, które będą obowiązywały w organizacji;
3) identyfikowanie i prowadzenie cyklicznych analiz ryzyka;
4) przygotowanie planów awaryjnych oraz ich testowanie;
5) opracowanie procedur zapewniających informowanie właściwych zespołów CERT o:
    a) wystąpieniu incydentów komputerowych,
    b) zmianie lokalizacji jednostki organizacyjnej, danych kontaktowych, itp.;

Polityka nie wskazuje miejsca usytuowania pełnomocnika ds. bezpieczeństwa cyberprzestrzeni w strukturze jednostki organizacyjnej, jednak rola pełnomocnika powinna

zostać przypisana osobie odpowiedzialnej za realizację procesu bezpieczeństwa teleinformatycznego.

3.5 Założenia dotyczące kształcenia, szkoleń i uświadamiania w dziedzinie bezpieczeństwa

W ramach realizacji ***Polityki*** Rada Ministrów widzi potrzebę rozpoczęcia prac nad wdrożeniem działań edukacyjnych. Zakłada się, że działania z tego zakresu będą prowadzone wśród obecnych oraz przyszłych użytkowników CRP. Mają one na celu wzmocnienie efektu dwóch poprzednich działań, utrwalenie ich wśród użytkowników, a także stworzenie możliwości przejścia do następnego etapu realizacji ***Polityki***.

3.5.1. Szkolenia pełnomocników ds. bezpieczeństwa cyberprzestrzeni

W celu podniesienia kwalifikacji istnieje konieczność opracowania systemu szkoleń dla pełnomocników ds. bezpieczeństwa cyberprzestrzeni. W projekcie szkoleń szczególny nacisk powinien być położony na kwestię reagowania na incydenty związane z bezpieczeństwem informacji.

3.5.2. Wprowadzenie tematyki bezpieczeństwa teleinformatycznego jako stałego elementu kształcenia na uczelniach wyższych.

Jednym z podstawowych aspektów zapewnienia bezpieczeństwa CRP jest posiadanie wysoko wykwalifikowanych kadr w sektorze publicznym i prywatnym odpowiadających za utrzymanie systemów teleinformatycznych ze szczególnym uwzględnieniem zasobów kluczowych dla bezpieczeństwa państwa. Aby zapewnić ciągły dopływ odpowiednio wyszkolonych specjalistów z dziedziny bezpieczeństwa teleinformatycznego jest konieczne zaangażowanie szkół wyższych w realizację założeń ***Polityki***. Zagadnienia związane z bezpieczeństwem cyberprzestrzeni powinny stać się stałym elementem nauczania. W szczególności dotyczy to uczelni technicznych kształcących informatyków. Nie można dopuszczać do sytuacji, w której projektanci, programiści skupiają się wyłącznie na funkcjonalności, zapominając o zasadach tworzenia bezpiecznego kodu, a administratorzy systemów za priorytet uznają dostępność zasobów użytkowników zapominając o konieczności ochrony przetwarzanych informacji przed intruzami. W tym celu konieczne jest umieszczenie tematyki bezpieczeństwa teleinformatycznego na liście efektów kształcenia „Krajowych Ram Kwalifikacji", na wszystkich etapach kształcenia.

3.5.3. Kształcenie kadry urzędniczej w administracji rządowej

Rada Ministrów widzi konieczność edukacji pracowników administracji rządowej, mającej dostęp oraz korzystającej z CRP, w zakresie zagadnień dotyczących bezpieczeństwa systemów teleinformatycznych - odpowiednio do zajmowanego stanowiska i ryzyka z nim związanego.

3.5.4. Kampania społeczna o charakterze edukacyjno - prewencyjnym

Powszechność korzystania przez obywateli z systemów dołączonych do sieci Internet oraz zwiększające się znaczenie dostępności usług oferowanych przez cyberprzestrzeń, wymuszają konieczność podnoszenia świadomości odnośnie bezpiecznych metod korzystania z Internetu oraz uwrażliwienia obywateli na pojawiające się zagrożenia.

Świadomość i wiedza na temat sposobów przeciwdziałania i zwalczania zagrożeń stanowią kluczowe elementy walki z tymi zagrożeniami. Jedynie odpowiedzialne zachowanie odpowiednio wyedukowanego użytkownika może skutecznie minimalizować ryzyko wynikające z istniejących zagrożeń. Należy podkreślić, iż we współczesnym świecie zapewnienie bezpieczeństwa teleinformatycznego w dużej mierze zależy od wiedzy i działań każdego użytkownika cyberprzestrzeni.

Ze względu na fakt, że przestępczością w cyberprzestrzeni są zagrożeni zarówno osoby fizyczne, jak również instytucje publiczne, przedsiębiorcy, organizacje społeczne, to kampania będzie miała charakter wielowymiarowy i uwzględniać będzie konieczne zróżnicowanie form i treści przekazu w zależności od potrzeb jej adresatów. Zakłada się, że kampania społeczna będzie miała charakter długofalowy i powszechny.

Ze względu na bezpieczeństwo teleinformatyczne warunkujące realizację zadań publicznych, adresatami akcji informacyjnych będą w szczególności pracownicy administracji rządowej oraz podmioty, których zasoby należą do infrastruktury teleinformatycznej CRP.

Zakłada się, że kampania edukacyjno-prewencyjna skierowana będzie do ogółu społeczeństwa, a w szczególności:

1) dzieci i młodzieży - jako grupy najbardziej podatnej na wpływy. Edukacja powinna rozpocząć się już od najmłodszych lat celem wytworzenia nawyków, które uchronią młodych ludzi przed zagrożeniami czyhającymi na nich w sieci (np. przed zjawiskiem zwanym cyberbullying - przemocy w sieci, zawieraniem niebezpiecznych znajomości, niecenzuralnymi treściami, piractwem, uzależnieniem od Internetu).

Wiedzę na temat zagrożeń z cyberprzestrzeni dziecko powinno uzyskiwać przede wszystkim w szkole na wszystkich poziomach edukacji (szkoła podstawowa, gimnazjum, szkoła średnia);

2) rodziców - jako osoby odpowiedzialne za wychowanie kolejnych pokoleń. To na rodzicach spoczywa odpowiedzialność za przygotowanie dzieci do funkcjonowania w społeczeństwie, również w społeczeństwie informacyjnym. Celem skutecznego nadzoru nad działalnością dziecka w Internecie rodzice powinni zdobyć odpowiednią wiedzę na temat zagrożeń z cyberprzestrzeni oraz metod ich eliminowania.

3) nauczycieli - od roku 2004 kształcenie nauczycieli w ramach specjalizacji odbywa się zgodnie z rozporządzeniem. Ministra Edukacji Narodowej, określającym standardy kształcenia nauczycieli[2]. W ramach zajęć obowiązkowych na studiach wyższych nauczyciele uzyskują podstawową wiedzę z zakresu technologii informacyjnej, w tym również bezpiecznego i świadomego korzystania z systemów teleinformatycznych.

Kampania społeczna adresowana do dzieci, młodzieży i ich rodziców w dużej mierze powinna być realizowana w placówkach oświatowych wszystkich szczebli.

Kampania będzie realizowana także za pośrednictwem środków masowego przekazu. Media - jako istotny partner w promowaniu zagadnień bezpieczeństwa, CRP oraz popularyzacji przedsięwzięć zawartych w Polityce - zwiększą skuteczność realizacji założonych celów. Dzięki ich pomocy w trakcie realizacji ***Polityki*** będzie możliwe przeprowadzenie również akcji informacyjnych i kampanii edukacyjnych. W tym celu zostaną zaangażowane media ogólnopolskie, regionalne oraz lokalne. Założeniem jest, że w ramach kampanii społecznej informacje dotyczące bezpieczeństwa teleinformatycznego oraz przedsięwzięć edukacyjnych i organizacyjno-prawnych podejmowanych w ramach ***Polityki*** będą prezentowane na stronach internetowych Ministerstwa Administracji i Cyfryzacji oraz na stronie Rządowego Zespołu Reagowania na Incydenty Komputerowe CERT.GOV.PL Jednocześnie zakłada się efektywne komunikowanie treści, inicjatyw i rezultatów prowadzenia ***Polityki*** wobec szerokich kręgów społecznych i zawodowych.

[2] rozporządzenie Ministra Edukacji Narodowej i. Sportu z dnia 7 września 2004 r. w sprawie standardów kształcenia nauczycieli (Dz. U. Nr 207 poz. 2110)

3.6 Założenia działań technicznych

Na podstawie działań proceduralno-organizacyjnych (np. planu postępowania z ryzykiem), ostatnim etapem realizacji ***Polityki*** powinny być działania techniczne. Ich celem będzie zmniejszenie ryzyka wystąpienia zagrożeń z CRP. Wykonanie tego etapu nastąpi poprzez uruchomienie projektów szczegółowych.

3.6.1 Programy badawcze

Niezwykle istotne dla skutecznej realizacji ***Polityki*** jest wspieranie inicjatyw badawczych dotyczących bezpieczeństwa teleinformatycznego. Formuła wsparcia powinna zachęcić do wspólnego prowadzenia badań przez podmioty zajmujące się bezpieczeństwem teleinformatycznym ze sfery administracji publicznej, ośrodki naukowe oraz przedsiębiorców telekomunikacyjnych i dostawców świadczących usługi drogą elektroniczną.

Przyjmuje się, że podmiotem koordynującym wdrażanie zapisów ***Polityki*** w tym zakresie będzie Ministerstwo Nauki i Szkolnictwa Wyższego (MNiSW), jako właściwe w sprawach badań naukowych i prac rozwojowych. Wykaz inicjatyw uwzględniających dynamikę stanu wiedzy określony zostanie na poziomie projektów szczegółowych, opracowanych na podstawie ***Polityki*** i może być uzupełniany z inicjatywy właściwych podmiotów odpowiedzialnych za jego realizację.

3.6.2 Rozbudowa zespołów reagowania na incydenty bezpieczeństwa teleinformatycznego w administracji rządowej

Aby było możliwe skuteczne prowadzenie działań związanych z zapewnieniem bezpieczeństwem CRP, w tym reagowanie na incydenty bezpieczeństwa teleinformatycznego, jest konieczne zapewnienie odpowiedniego zaplecza technicznego nie tylko umożliwiającego realizację bieżących zadań, ale również uwzględniającego wzrastające zapotrzebowanie na specjalizowane systemy teleinformatyczne w przyszłości.

Wszystkie zespoły po unifikacji zakresów obowiązków oraz procedur reagowania, jak również określenia obszaru zadaniowego (ang. constituency), tworzyłyby krajowy system reagowania na incydenty komputerowe, który oprócz współdziałania obejmowałby również wspólne konferencje, szkolenia i ćwiczenia.

3.6.3 Rozbudowa systemu wczesnego ostrzegania oraz wdrażanie i utrzymanie rozwiązań prewencyjnych

Departament Bezpieczeństwa Teleinformatycznego ABW wraz z Zespołem CERT Polska, działającym w ramach Naukowej i Akademickiej Sieci Komputerowej (NASK), wdrożył system wczesnego ostrzegania przed zagrożeniami z sieci Internet - ARAKIS-GOV. Rozbudowa systemu będzie realizowana zgodnie z projektem szczegółowym.

Jednocześnie mając na uwadze postęp zachodzący w technologiach teleinformatycznych i związaną z nim tendencję pojawiania się coraz bardziej wyrafinowanych zagrożeń, podczas wdrażania ***Polityki*** zakłada się podejmowanie inicjatyw promujących tworzenie coraz nowocześniejszych rozwiązań wspierających bezpieczeństwo teleinformatyczne.

Należy dążyć do stosowania jak najszerszego spektrum różnych rodzajów systemów zabezpieczeń w celu zapewnienia bezpieczeństwa krytycznych zasobów teleinformatycznych.

3.6.4 Testowanie poziomu zabezpieczeń i ciągłość działania

W ramach testowania poziomu zabezpieczeń i zapewnienia nieprzerwanej realizacji procesów CRP, PBC winien organizować i koordynować okresowe testy zarówno poziomu zabezpieczeń technicznych, organizacyjnych jak i rozwiązań proceduralnych (np. procedur ciągłości działania czy współpracy ponadresortowej). Wyniki ćwiczeń będą służyć ocenie aktualnej odporności cyberprzestrzeni na ataki, natomiast wnioski stanowić będą podstawę do przygotowania zaleceń do dalszych działań prewencyjnych.

3.6.5 Rozwój zespołów bezpieczeństwa

Zespoły typu CERT są centrami kompetencyjnymi służącymi pomocą merytoryczną na etapie tworzenia właściwych struktur i procedur. Dodatkowo służą również do rozwiązywania problemów w trakcie ich eksploatacji w poszczególnych jednostkach organizacyjnych administracji rządowej, czy też przedsiębiorców. Każda instytucja w ramach własnych zasobów osobowych i posiadanych środków technicznych może ustanowić własny, lokalny zespół reagowania na incydenty, którego działanie jest koordynowane zgodnie z pkt. 4.2.

Ponadto, do zadań Zespołów Reagowania na Incydenty Komputerowe należeć powinno utrzymywanie wewnętrznych witryn informacyjnych. Witryny będą stanowiły główne źródła informacji o bezpieczeństwie teleinformatycznym dla osób zajmujących się

bezpieczeństwem teleinformatycznych w instytucjach administracji rządowej, a także innych osób zainteresowanych tą tematyką.

W szczególności witryny będą miejscem publikacji następujących informacji:

1) aktualności związanych z bezpieczeństwem teleinformatycznym;
2) informacji o potencjalnych ryzykach i zagrożeniach;
3) biuletynów bezpieczeństwa;
4) różnego rodzaju poradników, dobrych praktyk, ftp.;
5) raportów oraz informacji na temat trendów i statystyk;
6) forum wymiany informacji oraz doświadczeń osób zaangażowanych w działania związane z bezpieczeństwem teleinformatycznym.

Witryny będą pełnić rolę punktów zgłaszania incydentów bezpieczeństwa teleinformatycznego. Witryna będzie tak skonstruowana, by użytkownik bez większej wiedzy z zakresu informatyki mógł zgłosić incydent lub znaleźć informację gdzie dane zdarzenie można zgłosić.

4. WDROŻENIE I MECHANIZMY REALIZACJI ZAPISÓW DOKUMENTU

Zakłada się, że cele i założenia ***Polityki*** będą wdrożone z uwzględnieniem analizy ryzyka i realizowane w ramach projektów szczegółowych.

4.1 Nadzór i koordynacja wdrożenia

Ze względu na międzyinstytucjonalny charakter ***Polityki*** organem nadzorującym jego wdrożenie jest Rada Ministrów. Podmiotem koordynującym realizację ***Polityki***, w imieniu Rady Ministrów, jest minister właściwy ds. informatyzacji.

4.2 Krajowy System Reagowania na Incydenty Komputerowe w CRP

Rząd RP ustanawia trzypoziomowy Krajowy System Reagowania na Incydenty Komputerowe w CRP:

1) Poziom I - poziom koordynacji - minister właściwy ds. informatyzacji;
2) Poziom II - reagowania na Incydenty komputerowe:
   a) Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL - realizujący jednocześnie zadania głównego narodowego zespołu odpowiadającego za koordynację procesu obsługi incydentów komputerowych w obszarze CRP,
   b) Resortowe Centrum Zarządzania Bezpieczeństwem Sieci i Usług Teleinformatycznych realizujące zadania w sferze militarnej,
3) Poziom III - poziom realizacji - administratorzy odpowiadający za poszczególne systemy teleinformatyczne funkcjonujące w cyberprzestrzeni.

Ustanowiony system reagowania zapewnia wymianę informacji pomiędzy zespołami administracji publicznej oraz zespołami CERT (CERT Polska, TP CERT, PIONIERCERT), CSIRT, ABUSE, przedsiębiorcami telekomunikacyjnymi w rozumieniu ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z późn. zm.) i usługodawcami świadczących usługi drogą elektroniczną w rozumieniu ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. Nr 144, poz. 1204, z późn. zm.), zgodnie z obowiązującymi przepisami prawa, a w szczególności zgodnie z ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926, z

późn. zm.) oraz ustawą z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. Nr 182, poz. 1228).

4.3 Mechanizm wymiany informacji

Sprawny system koordynacji zapewni wymianę informacji pozyskanych ze współpracy międzynarodowej, pomiędzy zespołami rządowymi, wojskowymi i cywilnymi, zgodnie z obowiązującymi przepisami prawa, a w szczególności zgodnie z ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.) oraz ustawą z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. Nr 182, poz. 1228).

System ten między innymi określi alternatywne kanały wymiany informacji oraz wprowadzi okresowe testy skuteczności procesów wymiany informacji.

4.4 Sposoby i formy współpracy

W ramach realizacji ***Polityki*** powinny zostać wypracowane formy współpracy pomiędzy organami odpowiedzialnymi za bezpieczeństwo cyberprzestrzeni oraz odpowiedzialnymi za zwalczanie przestępczości komputerowej o charakterze kryminalnym. Powyższe formy współpracy będą miały zarówno postać roboczą, w celu zminimalizowania opóźnień reakcji na incydenty komputerowe, jak i sformalizowaną - służącą eliminowaniu problemów kompetencyjnych.

4.5 Współpraca z przedsiębiorcami

Niezbędne jest zaktywizowanie przedsiębiorców, których ochrona przed zagrożeniami z cyberprzestrzeni jest istotna z punktu widzenia prawidłowego funkcjonowania Państwa.

Należy do tej grupy zaliczyć przedsiębiorców działających w szczególności w ramach sektorów:

1) zaopatrzenia w energię, surowce energetyczne i paliwa,
2) łączności,
3) sieci teleinformatycznych,
4) finansowego.

Polityka zakłada podjęcie działań aktywizujących współpracę pomiędzy przedsiębiorcami zarządzającymi własną teleinformatyczną infrastrukturą zaliczoną do infrastruktury teleinformatycznej CRP o podobnym charakterze, a przez to narażoną na podobne typy podatności i metody ataków. Jedną z form współpracy będzie tworzenie gremiów powoływanych do wewnętrznej wymiany informacji i doświadczeń oraz współpracy z administracją publiczną w zakresie bezpieczeństwa infrastruktury teleinformatycznej CRP.

4.5.1 Współpraca z producentami urządzeń i systemów teleinformatycznych

Ważnymi partnerami dla instytucji rządowych i innych podmiotów odpowiedzialnych za bezpieczeństwo teleinformatyczne i zwiększenie bezpieczeństwa w cyberprzestrzeni są producenci sprzętu i oprogramowania. Rozwój współpracy z tymi partnerami, w tym wymiana doświadczeń i oczekiwań, stanowić powinien jeden z ważniejszych czynników mających duży wpływ zarówno na system edukacji społecznej i specjalistycznej, jak i na jakość tworzonych systemów. Szczególne znaczenie dla rozszerzenia spektrum dostępnych narzędzi winna mieć współpraca podmiotów odpowiedzialnych za bezpieczeństwo teleinformatyczne z producentami systemów zabezpieczeń.

Należy dążyć do udostępniania użytkownikom jak największego wachlarza rozwiązań służących szeroko rozumianemu bezpieczeństwu teleinformatycznemu oraz ochronie informacji.

4.5.2 Współpraca z przedsiębiorcami telekomunikacyjnymi

Ze względu na globalny charakter zagrożeń wymagana jest ścisła skoordynowana współpraca w zakresie bezpieczeństwa cyberprzestrzeni pomiędzy Urzędem Komunikacji Elektronicznej (UKE), przedsiębiorcami telekomunikacyjnymi i użytkownikami CRP.

4.6 Współpraca międzynarodowa

Ze względu na globalny charakter problemów związanych z bezpieczeństwem cyberprzestrzeni, istotnym elementem jest utrzymanie i rozwijanie współpracy międzynarodowej w tym zakresie.

Rząd RP widzi potrzebę, aby Polska, poprzez swoich przedstawicieli, organy rządowe, instytucje państwowe oraz współpracę z instytucjami pozarządowymi inicjowała i prowadziła aktywne działania zmierzające do zwiększenia bezpieczeństwa CRP oraz międzynarodowej.

5. FINANSOWANIE

Polityka nie będzie implikować dodatkowych środków z budżetu państwa na sfinansowanie założonych działań w roku jej wejścia w życie, ponieważ aktualnie jednostki organizacyjne administracji publicznej realizują już częściowo cele wymienione w Polityce. W związku z tym przyjmuje się, że po jej zaakceptowaniu każda jednostka organizacyjna wyraźnie wskaże zadania już realizowane i środki finansowe na nie wydatkowane.

Niniejszy dokument zakłada kontynuację działań realizowanych oraz zaplanowanych przez Zespół, o którym mowa w pkt 3.4.1.

Zakłada się, że od chwili wejścia w życie ***Polityki*** poszczególne jednostki będą szacowały koszty realizowanych już zadań, pokrywających się z zadaniami nałożonymi niniejszą ***Polityką***.

Przedstawione szacunki kosztów pozwolą na ich ujęcie w planie następnego roku budżetowego z wyraźnym wskazaniem, iż dotyczą bezpieczeństwa cyberprzestrzeni.

Poszczególne jednostki organizacyjne dane o oszacowanych przez siebie kosztach realizacji zadań przekazują do ministra właściwego ds. informatyzacji. Koszty realizacji zadań będą zdeterminowane analizą ryzyka i przedstawione w projektach szczegółowych z przypisaniem poszczególnym jednostkom i wskazaniem źródeł finansowania.

Konieczne wydatki, związane z realizacją ***Polityki*** będą finansowane w ramach limitu wydatków budżetowych przewidzianych we właściwej części budżetowej w ustawie budżetowej na dany rok.

6. OCENA SKUTECZNOŚCI *POLITYKI*

Ze względu na nowatorski charakter niniejszego dokumentu szczegółowe wskaźniki realizacji założeń ***Polityki*** będą opracowane po przeprowadzeniu oceny ryzyka.

Niezbędnym jest, aby od chwili wejścia w życie ***Polityki***, poszczególne jednostki organizacyjne analizowały i sugerowały wskaźniki realizacji zadań, na podstawie których zostaną zagregowane informacje i wypracowane globalne wskaźniki celów niniejszego dokumentu. Zakłada się, że przedstawione propozycje globalnych wskaźników będą wykorzystane w ramach aktualizacji ***Polityki*** i pozwolą na ocenę stopnia realizacji założonych celów i zadań w zakresie bezpieczeństwa CRP.

Stopnie realizacji przedsięwzięć związanych z realizacją celu strategicznego oraz celów szczegółowych ***Polityki*** będą oceniane w ramach projektów szczegółowych pod kątem następujących kryteriów:

1) stopnia nasycenia wszystkich jednostek organizacyjnych, posiadających systemy ochrony i wczesnego ostrzegania w stosunku do liczby urzędów administracji publicznej;
2) poziomu integracji:
   a) sposobu i trybu wymiany informacji między zespołami z zapewnieniem poufności, integralności i dostępności,
   b) możliwości i zakresu osiągania wspólnego, dynamicznego zobrazowania cyberprzestrzeni objętej niniejszym ***Polityką,***
3) stopnia standaryzacji - stopnia wdrożenia norm, kategorii incydentów i procedur;
4) stopnia wyposażenia systemów w kompleksowe oprogramowanie antywirusowe, firewalle, antyspamowe w stosunku do wymaganych objęciem taką ochroną (szacowanie zasobów).

Do oceny skuteczności projektów szczegółowych, utworzonych na podstawie niniejszej ***Polityki,*** zostaną wykorzystane następujące mierniki:

1. Mierniki skuteczności - mierzą stopień osiągnięcia zamierzonych celów i mogą mieć zastosowanie na wszystkich szczeblach klasyfikacji zadaniowej.

Przykładowy miernik produktu:

- liczba zamkniętych incydentów w stosunku do ogólnej liczby sklasyfikowanych incydentów.

2. Mierniki produktu - odzwierciedlają wykonanie danego zadania w krótkim okresie i pokazują konkretne dobra oraz usługi wyprodukowane przez sektor publiczny. Mierniki produktu - mierzą stopień wykonania celów operacyjnych.

Przykładowe mierniki produktu:

- liczba odpowiedzi na zgłoszone przez obywateli incydenty,
- liczba obsłużonych incydentów,

3. Mierniki rezultatu - mierzą efekty uzyskane w wyniku działań objętych zadaniem lub pod zadaniem, realizowanych za pomocą odpowiednich wydatków, na poziomie zadania/podzadania/działania. Mierzą skutki podejmowanych działań. Mierniki rezultatu - mierzą bezpośrednie skutki podejmowanych działań w krótkiej lub średniej perspektywie czasowej.

Przykładowe mierniki rezultatu:

- skrócenie czasu obsługi incydentu,
- średni czas odpowiedzi na incydent.

4. Mierniki oddziaływania - mierzą długofalowe konsekwencje realizacji zadania. Mogą one mierzyć bezpośrednie skutki wdrażania zadania, które ujawniają się po upływie dłuższego okresu czasu. Mierniki oddziaływania odnoszą się czasem do wartości, które tylko w części są efektem realizacji zadania (na efekty wpływają także inne, zewnętrzne czynniki).

Przykładowy miernik oddziaływania:

- zwiększenie poczucia bezpieczeństwa w sieci Internet w Polsce (badania CBOS). Stopień realizacji zostanie oceniony w procentach, przy czym za 100% rozumie się realizację wszystkich zadań wynikających z projektów szczegółowych opracowanych na podstawie ***Polityki***.

W ciągu roku od wejścia ***Polityki*** w życie, każda zaangażowana jednostka, o której mowa w pkt. 1.4 ust. 1 niniejszego dokumentu, oszacuje (w %) w jakim stopniu są już zrealizowane założenia przedmiotowej ***Polityki***.

6.1 Przewidywane efekty *Polityki*

Przewiduje się następujące długofalowe efekty działań wynikających z wdrożenia niniejszej ***Polityki*** oraz projektów szczegółowych opracowanych na jej podstawie:

- większy poziom bezpieczeństwa CRP oraz większy poziom odporności państwa na ataki w CRP,
- spójną dla wszystkich zaangażowanych podmiotów politykę dotyczącą bezpieczeństwa cyberprzestrzeni,
- mniejszą skuteczność ataków terrorystycznych w CRP i mniejsze koszty usuwania następstw ataków cyberterrorystycznych,
- skuteczny system koordynacji i wymiany informacji pomiędzy publicznymi i prywatnymi podmiotami odpowiedzialnymi za zapewnianie bezpieczeństwa cyberprzestrzeni oraz tymi, które dysponują zasobami stanowiącymi krytyczną infrastrukturę teleinformatyczną państwa,
- większą kompetencję podmiotów zaangażowanych w bezpieczeństwo infrastruktury teleinformatycznej Państwa funkcjonującej w cyberprzestrzeni,
- większe zaufanie obywateli do właściwego zabezpieczenia usług państwa świadczonych drogą elektroniczną,
- większą świadomość obywateli, co do metod bezpiecznego użytkowania systemów dostępnych elektronicznie i sieci teleinformatycznych.

6.2 Skuteczność działań

Miarą skuteczności podjętych w ramach ***Polityki*** działań będzie ocena stworzonych regulacji, instytucji i relacji, które umożliwią rzeczywiste zaistnienie skutecznego systemu bezpieczeństwa cyberprzestrzeni. Jedną z podstawowych metod wpływania na skuteczność założonych działań wykonywanych przez wiele instytucji jest ustalenie zakresu zadań każdego z podmiotów oraz ustalenie odpowiedzialności za ich realizację.

6.3 Monitorowanie efektywności działań w ramach przyjętej *Polityki*

Raporty o postępach w realizacji ***Polityki*** będą przesyłane przez jednostki wyszczególnione w pkt. 1.4 do ministra właściwego ds. informatyzacji.

6.4 Konsekwencje naruszenia zapisów *Polityki*

Każdy podmiot administracji rządowej stosuje się do zapisów niniejszej ***Polityki*** niezależnie od odpowiedzialności określonej w przepisach prawa powszechnie obowiązującego.

Naruszenie zasad określonych w niniejszej Polityce może być przyczyną wykluczenia się podmiotu ze społeczności informacyjnej i powstania utrudnień w dostępie do informacji publicznej. Odpowiednie zabezpieczenia, ochrona przetwarzanych danych oraz niezawodność funkcjonowania systemów teleinformatycznych są najwyższymi wartościami stawianymi współczesnym systemom. Podmioty realizujące przedmiotową Politykę powinny wskazać sposoby zabezpieczenia systemów informatycznych, procedury postępowania w sytuacji naruszenia bezpieczeństwa teleinformatycznego w systemach informatycznych w ***Polityka***ch bezpieczeństwa tych systemów. Wykonywanie zapisów niniejszego dokumentu ma zapewnić właściwą reakcję, ocenę i udokumentowanie przypadków naruszenia bezpieczeństwa systemów oraz zapewnić właściwy sposób reagowania na incydenty w celu przywrócenia akceptowalnego poziomu bezpieczeństwa. Istotnym obowiązkiem jest niezwłoczne informowanie administratora lub właściwego Zespołu CERT o wykryciu incydentu oraz podjęcie lub zaniechanie czynności mających na celu jego obsłużenie.