KRAJOWE RAMY POLITYKI CYBERBEZPIECZEŃSTWA RZECZYPOSPOLITEJ POLSKIEJ NA LATA 2017–2022

POSZANOWANIE PRAW I WOLNOŚCI W CYBERPRZESTRZENI
KOMPLEKSOWE PODEJŚCIE DO BEZPIECZEŃSTWA
CYBERBEZPIECZEŃSTWO ISTOTNYM ELEMENTEM POLITYKI PAŃSTWA

Ministerstwo Cyfryzacji
Warszawa 2017

Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej
na lata 2017 - 2022

Spis treści

1. Wstęp

Rozwój społeczny i gospodarczy w coraz większym stopniu zależny jest od szybkiego i nieskrępowanego dostępu do informacji oraz jej wykorzystania w zarządzaniu, produkcji, sektorze usług oraz przez podmioty publiczne. Stały rozwój sieci i systemów informatycznych, w tym operacje na dużych zasobach danych, służą rozwojowi komunikacji, handlu, transportu czy też usług finansowych. W cyberprzestrzeni tworzymy i kształtujemy relacje społeczne, a Internet stał się narzędziem do wpływania na zachowania grup społecznych, a także oddziaływania w sferze politycznej.

Każde znaczące zakłócenie funkcjonowania cyberprzestrzeni, czy to o charakterze globalnym, czy lokalnym, będzie miało wpływ na bezpieczeństwo obrotu gospodarczego, poczucie bezpieczeństwa obywateli, sprawność funkcjonowania instytucji sektora publicznego, przebieg procesów produkcyjnych i usługowych, a w rezultacie na ogólnie pojmowane bezpieczeństwo narodowe.

Informacja jest narażona na utratę dostępności, integralności i poufności w wyniku oddziaływań pochodzących z różnych źródeł, w tym działań zamierzonych, polegających na dystrybucji szkodliwego oprogramowania, włamań do systemów teleinformatycznych, blokowaniu możliwości świadczenia usług. Atakującymi mogą być zarówno grupy przestępcze, działające z chęci zysku, pobudek terrorystycznych, jak i grupy, za którymi mogą stać obce państwa, a działania takie służą pozyskaniu informacji, destabilizacji politycznej lub gospodarczej albo wywołaniu niezadowolenia społecznego.

Zapewnienie bezpieczeństwa informacji jest wyzwaniem dla wszystkich podmiotów tworzących krajowy system cyberbezpieczeństwa, a więc podmiotów gospodarczych świadczących usługi przy wykorzystaniu systemów teleinformatycznych, użytkowników cyberprzestrzeni, organów władzy publicznej, a także wyspecjalizowanych podmiotów zajmujących się bezpieczeństwem teleinformatycznym w sferze operacyjnej. Jest to tym istotniejsze, iż Polska jest ściśle powiązana z innymi państwami poprzez współpracę międzynarodową w ramach takich organizacji jak UE, NATO, ONZ czy OBWE. Współpraca ta odgrywa istotną rolę w walce z rosnącą liczbą incydentów powodowanych nielegalnymi działaniami w cyberprzestrzeni, prowadzącymi do strat materialnych i wizerunkowych.

Niniejszy dokument został opracowany przez grupę składającą się z przedstawicieli resortów: cyfryzacji, obrony narodowej, spraw wewnętrznych i administracji oraz przedstawicieli Agencji Bezpieczeństwa Wewnętrznego, Rządowego Centrum Bezpieczeństwa i Biura Bezpieczeństwa Narodowego.

2. Kontekst strategiczny

Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczpospolitej Polski na lata 2017-2022 to dokument, który wpisuje się w kontynuację działań, podejmowanych w przeszłości przez administrację rządową, mających na celu podniesienie poziomu bezpieczeństwa w cyberprzestrzeni RP, w tym przyjętą przez rząd w 2013 roku *Politykę Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej*.

Zarówno krajowe strategie rozwoju, jak i te odnoszące się do sfery porządku publicznego i bezpieczeństwa narodowego uzależniają swoje powodzenie od zastosowania systemów teleinformatycznych. Cyfryzacja jest nie tylko źródłem rozwoju i innowacji, ale również niesie za sobą ryzyko związane z rosnącą liczbą niebezpieczeństw w sieci. W świetle nowych zagrożeń, rozbudowanej architektury systemów teleinformatycznych, wzrastającej zależności społeczeństwa oraz przedsiębiorców od tych systemów, niezbędna jest rozbudowa krajowego systemu cyberbezpieczeństwa oraz zapewnienie spójnego podejścia w skali całego państwa.

Zamierzeniem niniejszego dokumentu jest określenie ramowych działań, mających na celu uzyskanie wysokiego poziomu odporności krajowych systemów teleinformatycznych, operatorów usług kluczowych, operatorów infrastruktury krytycznej, dostawców usług cyfrowych oraz administracji publicznej na incydenty w cyberprzestrzeni. Proponowane kierunki strategiczne mają również wpływać na zwiększenie skuteczności organów ścigania i wymiaru sprawiedliwości w wykrywaniu i zwalczaniu przestępstw oraz działań o charakterze terrorystycznym i szpiegowskim w cyberprzestrzeni. *Krajowe Ramy Polityki Cyberbezpieczeństwa* są spójne z prowadzonymi działaniami dotyczącymi operatorów infrastruktury krytycznej wykorzystujących systemy teleinformatyczne oraz uwzględnia potrzeby zaangażowania Sił Zbrojnych Rzeczypospolitej Polskiej.

Podejmując działania mające na celu wdrożenie Krajowych Ram Polityki Cyberbezpieczeństwa, Rząd będzie w pełni respektować prawo do prywatności oraz stać na stanowisku, że wolny i otwarty Internet jest istotnym elementem funkcjonowania współczesnego społeczeństwa.

3. Zakres Krajowych Ram Polityki Cyberbezpieczeństwa

Krajowe Ramy Polityki Cyberbezpieczeństwa wskazują, w szczególności:

- cele w zakresie bezpieczeństwa teleinformatycznego,
- główne podmioty zaangażowane we wdrażanie krajowych ram polityki w zakresie bezpieczeństwa teleinformatycznego,

- ramy zarządzania służące realizacji celów krajowych ram polityki w zakresie bezpieczeństwa teleinformatycznego,
- na potrzebę zapobiegania i reagowania w odniesieniu do incydentów oraz przywracania stanu normalnego zakłóconego incydentem, w tym zasady współpracy pomiędzy sektorami publicznym i prywatnym,
- podejście do oceny ryzyka,
- kierunki podejścia do programów edukacyjnych, informacyjnych i szkoleniowych dotyczących cyberbezpieczeństwa,
- działania odnoszące się do planów badawczo-rozwojowych w zakresie bezpieczeństwa teleinformatycznego,
- podejście do współpracy międzynarodowej w zakresie cyberbezpieczeństwa.

Krajowe Ramy Polityki Cyberbezpieczeństwa wprowadzone w drodze uchwały Rady Ministrów, oddziałują w sposób bezpośredni na podmioty administracji rządowej, a w sposób pośredni, po przyjęciu z inicjatywy Rady Ministrów przepisów prawa powszechnego, na pozostałe podmioty władzy publicznej, przedsiębiorców i obywateli.

4. Wizja, cel główny, cele szczegółowe

4.1. Wizja

W roku 2022 Polska będzie krajem bardziej odpornym na ataki i zagrożenia płynące z cyberprzestrzeni. Dzięki synergii działań wewnętrznych i międzynarodowych cyberprzestrzeń RP stanowić będzie bezpieczne środowisko umożliwiające realizowanie wszystkich funkcji państwa i pozwalać na pełne wykorzystywanie potencjału gospodarki cyfrowej, przy równoczesnym poszanowaniu praw i wolności obywateli.

4.2. Cel główny

Zapewnienie wysokiego poziomu bezpieczeństwa sektora publicznego, sektora prywatnego oraz obywateli w zakresie świadczenia lub korzystania z usług kluczowych oraz usług cyfrowych.

4.3. Cele szczegółowe

Cel szczegółowy 1. Osiągnięcie zdolności do skoordynowanych w skali kraju działań służących zapobieganiu, wykrywaniu, zwalczaniu oraz minimalizacji skutków incydentów naruszających bezpieczeństwo systemów teleinformatycznych istotnych dla funkcjonowania państwa.

Cel szczegółowy 2. Wzmocnienie zdolności do przeciwdziałania cyberzagrożeniom.

Cel szczegółowy 3. Zwiększanie potencjału narodowego oraz kompetencji w zakresie bezpieczeństwa w cyberprzestrzeni.

Cel szczegółowy 4. Zbudowanie silnej pozycji międzynarodowej RP w obszarze cyberbezpieczeństwa.

5. Cel szczegółowy 1 – Osiągnięcie zdolności do skoordynowanych w skali kraju działań służących zapobieganiu, wykrywaniu, zwalczaniu oraz minimalizacji skutków incydentów naruszających bezpieczeństwo systemów teleinformatycznych istotnych dla funkcjonowania państwa

5.1. Dostosowanie otoczenia prawnego do potrzeb i wyzwań w obszarze cyberbezpieczeństwa

Rozbudowa krajowego systemu cyberbezpieczeństwa wymaga zmian prawnych. W związku z tym zostanie dokonany przegląd istniejących przepisów prawa w celu ich harmonizacji, zwiększenia efektywności działania i poprawy przepływu informacji pomiędzy wszystkimi interesariuszami zaangażowanymi w aktywne budowanie krajowego systemu cyberbezpieczeństwa.

Najdalej idące zmiany będą wynikać z obowiązku implementacji do polskiego porządku prawnego *Dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii*[1] zwanej dalej Dyrektywą NIS. Zawiera ona dyspozycje do określenia wymagań bezpieczeństwa w odniesieniu do podmiotów prywatnych i państwowych z sektorów energetycznego, transportowego, bankowości i infrastruktury rynków finansowych, służby zdrowia, zaopatrzenia w wodę oraz infrastruktury cyfrowej, świadczących usługi kluczowe. Zapewnienie skuteczności krajowego systemu cyberbezpieczeństwa wymaga włączenia do niego sektora publicznego oraz telekomunikacyjnego, a także uwzględnienia kwestii związanych z usługami zaufania i usługami publicznymi świadczonymi przez sektor prywatny. Ponadto Dyrektywa NIS wprowadza minimalne wymagania dla dostawców usług cyfrowych, to jest internetowych platform handlowych, wyszukiwarek internetowych i usług przetwarzania w chmurze.

Za przygotowanie propozycji zmian prawnych w zakresie cyberbezpieczeństwa w swych obszarach kompetencyjnych odpowiadają właściwi ministrowie.

W ramach prac legislacyjnych minister właściwy do spraw informatyzacji, we współpracy z innymi resortami, dokona przeglądu regulacji sektorowych i szczególnych, które dotyczą omawianej problematyki oraz regulacji prawnych, które mogą mieć oddziaływanie na inne obszary, na przykład

[1] Dz. U. UE 2016 L194

na ochronę danych osobowych, czy infrastrukturę krytyczną w kontekście Narodowego Programu Ochrony Infrastruktury Krytycznej. Niezbędne będzie również podjęcie prac legislacyjnych mających na celu uregulowanie obszaru z zakresu wytwarzania, posiadania, pozyskiwania oraz wykorzystywania specjalistycznych narzędzi z zakresu prowadzenia działań militarnych w cyberprzestrzeni przez resort obrony narodowej.

Uregulowane zostaną kwestie współpracy operacyjnej, w tym właściwej koordynacji działań i wymiany informacji pomiędzy instytucjami odpowiedzialnymi za bezpieczeństwo narodowe, działania antyterrorystyczne oraz bezpieczeństwo wewnętrzne i porządek publiczny.

Z uwagi na dynamikę procesów zachodzących w obszarze cyberbezpieczeństwa niezbędne będzie okresowe monitorowanie zjawisk tam zachodzących i inicjowanie ewentualnych zmian w przepisach prawa.

5.2. Udoskonalenie struktury krajowego systemu cyberbezpieczeństwa

Wobec dynamicznego rozwoju społeczeństwa informacyjnego, elektronicznej administracji i gospodarki cyfrowej, jak również w świetle zagrożeń w cyberprzestrzeni zostaną wzmocnione struktury krajowego systemu ochrony cyberprzestrzeni.

W świetle planowanych zmian prawa zadaniem organów państwowych będzie określenie zakresu odpowiedzialności podmiotu koordynującego krajowy system cyberbezpieczeństwa, obowiązków i uprawnień uczestników systemu oraz sposobów oddziaływania koordynatora na uczestników systemu. Należy również określić kompetencje organów właściwych, odpowiedzialnych za sprawowanie nadzoru w zakresie systemów teleinformatycznych w sektorach, w których świadczone są usługi kluczowe i usługi cyfrowe.

Dotychczasowe działania w obszarze cyberbezpieczeństwa podmiotów ze sfery cywilnej, wojskowej, sektora publicznego i prywatnego oraz instytucji odpowiedzialnych za zwalczanie cyberprzestępczości miały charakter rozproszony, co bezpośrednio wpływało na niską efektywność tego systemu. Wdrożenie skutecznego systemu cyberbezpieczeństwa będzie możliwe poprzez skonsolidowanie i zharmonizowanie działań wszystkich interesariuszy. W tym celu niezbędne będzie zastosowanie podejścia procesowego, poprzez dokonanie identyfikacji procesów, ról poszczególnych interesariuszy i ich zasobów.

Rozwój krajowego systemu cyberbezpieczeństwa wiąże się również z rozbudową struktur zajmujących się cyberbezpieczeństwem na poziomie operacyjnym, w tym Narodowego Centrum Cyberbezpieczeństwa (NCC), CSIRT Narodowego, sektorowych zespołów reagowania na incydenty (CSIRT sektorowe), centrów wymiany i analizy informacji oraz potrzebą właściwego umocowania kompetencyjnego na poziomie ustawy odpowiednich struktur, w tym NCC oraz CSIRT Narodowego. Niezbędne jest ustanowienie systemowych rozwiązań pozwalających na wymianę informacji pomiędzy interesariuszami i dzielenie się wiedzą, co do zagrożeń i incydentów.

Warunkiem prawidłowego działania systemu będzie również doprecyzowanie wzajemnych powiązań pomiędzy poszczególnymi interesariuszami krajowego systemu cyberbezpieczeństwa, w tym organów odpowiedzialnych za bezpieczeństwo narodowe, działania antyterrorystyczne, bezpieczeństwo wewnętrzne oraz porządek publiczny, prokuraturę oraz sądownictwo.

Rząd w ramach współpracy administracji rządowej z administracją samorządową będzie rekomendował i działał na rzecz jednostek samorządu terytorialnego w zakresie tworzenia klastrów bezpieczeństwa dla tej administracji.

5.3. Zwiększenie efektywności współdziałania podmiotów zapewniających bezpieczeństwo cyberprzestrzeni RP

Podstawą skutecznej reakcji na zagrożenia i ataki jest funkcjonowanie niezawodnych i bezpiecznych mechanizmów wymiany informacji pomiędzy interesariuszami krajowego systemu cyberbezpieczeństwa. Z drugiej strony powszechnie występującym problemem jest niechęć tych podmiotów do dzielenia się informacją na temat zauważonych zagrożeń, incydentów oraz szacowanych strat. Niezależnie od rozwiązań prawnych określających jednoznaczne mechanizmy wymiany informacji o cyberbezpieczeństwie, w pierwszym okresie konieczne jest utworzenie lub rozbudowa krajowej sieci CSIRT (narodowy, sektorowe, komercyjne i przedsiębiorców), które wymieniałyby kluczowe informacje o zagrożeniach bezpieczeństwa i incydentach w danym sektorze bądź dziale administracji rządowej.

Mechanizmy systemu wymiany informacji zostaną skonstruowane tak, aby podmiotom uczestniczącym zapewnić ochronę interesów, w tym ochronę tajemnicy przedsiębiorstwa, ochronę wizerunku oraz ochronę innych istotnych wartości.

Krytycznym czynnikiem procesu zwiększenia efektywności współdziałania podmiotów zapewniających bezpieczeństwo cyberprzestrzeni RP, jak i doskonalenia systemu reagowania na incydenty, będą ćwiczenia i treningi pozwalające na sprawdzenie skuteczności działania w skali krajowej i międzynarodowej.

Na poziomie krajowym będą organizowane kompleksowe ćwiczenia symulujące ogólnokrajowy incydent. Równolegle będą organizowanie ćwiczenia o mniejszym zasięgu, w tym sektorowe, w odpowiedzi na bieżące wydarzenia i incydenty w celu ciągłego doskonalenia personelu, narządzi i procedur. W ramach ćwiczeń krajowych i międzynarodowych będą także podnoszone zdolności Sił Zbrojnych Rzeczypospolitej Polskiej (SZ RP) do prowadzenia działań militarnych w cyberprzestrzeni.

W obszarze współpracy międzynarodowej Polska będzie aktywnie włączać się w ćwiczenia prowadzone zarówno przez organizacje krajowe, podmioty UE i NATO oraz inne podmioty międzynarodowe.

Na podstawie przeprowadzonych ćwiczeń i treningów opracowane będą wytyczne i zalecenia służące doskonaleniu systemu cyberbezpieczeństwa.

Doskonalenie systemu możliwe jest także poprzez uczestnictwo w zaufanych międzynarodowych forach wymiany informacji o zagrożeniach w cyberprzestrzeni. Fora takie mają często charakter nieformalny lub powstają w ramach organizacji typu non-profit.

5.4. Zwiększenie bezpieczeństwa teleinformatycznego usług kluczowych i cyfrowych oraz infrastruktury krytycznej

Technologie informacyjno-komunikacyjne stały się obecnie fundamentem rozwoju gospodarczego. Z uwagi na wykorzystywanie tych technologii przez operatorów usług kluczowych, dostawców usług cyfrowych oraz operatorów infrastruktury krytycznej, stanowią one element krytyczny w zapewnianiu bezpieczeństwa obywatelom i ciągłości działania państwa. Z tego też powodu zapewnienie bezpieczeństwa teleinformatycznego będzie traktowane przez Radę Ministrów jako priorytet. Mając na uwadze, że odpowiedzialność za zapewnienie bezpieczeństwa usług leży przede wszystkim po stronie podmiotów je świadczących, rząd podejmie działania wspierające budowanie zdolności i kompetencji w zakresie cyberbezpieczeństwa wśród operatorów usług kluczowych, operatorów infrastruktury krytycznej oraz dostawców usług cyfrowych, uwzględniając

ich różnorodną specyfikę i różny stopień dojrzałości w zakresie cyberbezpieczeństwa. Ponadto rząd będzie wspierał wszystkie te podmioty w reagowaniu na poważne incydenty, przede wszystkim w przypadku wystąpienia incydentów ponadsektorowych. W pierwszej kolejności zostanie zapewniona spójność działań w zakresie opracowywania kryteriów identyfikacji operatorów infrastruktury krytycznej i usług kluczowych, uwzględniająca potrzebę włączenia tych podmiotów do systemu zarządzania kryzysowego. Proces ten przebiegał będzie we współpracy ze wszystkimi sektorami. Następnie opracowane zostaną minimalne wymagania w zakresie bezpieczeństwa teleinformatycznego z uwzględnianiem zarządzania ciągłością działania. Osobnym reżimem objęci zostaną dostawcy usług cyfrowych. Rząd ma pełną świadomość międzynarodowej specyfiki tych podmiotów, oraz konieczności zapewnienia takich regulacji, które będą sprzyjały rozwojowi rynku cyfrowego w Polsce.

Ważnym elementem struktury krajowego systemu cyberbezpieczeństwa na poziomie technicznym staną się bezpieczne sieci typu intranet, oferujące połączenia wewnątrz sieci, usługi bezpieczeństwa oraz bezpieczny dostęp do sieci Internet, zwane klastrami bezpieczeństwa. Priorytetowym przedsięwzięciem będzie zbudowanie takiego klastra dla centralnej administracji rządowej.

5.5. Opracowanie i wdrożenie standardów oraz dobrych praktyk bezpieczeństwa sieci i systemów informatycznych

Na wszystkich etapach życia systemu teleinformatycznego, w odniesieniu do zapewnienia bezpieczeństwa tych systemów, zastosowanie powinny mieć Polskie Normy, normy międzynarodowe, powszechnie uznawane standardy, a także tak zwane dobre praktyki. Na podstawie obowiązujących przepisów prawa podmioty realizujące zadania publiczne są zobowiązane do stosowania takiego podejścia. Rząd dołoży starań, aby przepisy te były w pełni wdrożone w tych podmiotach. Istotne jest również wspieranie wdrożenia rekomendacji wydawanych przez regulatorów rynkowych.

Wykorzystując potencjał intelektualny ekspertów zgromadzonych w komitetach technicznych Polskiego Komitetu Normalizacyjnego, ośrodkach naukowych, akademickich i instytutach badawczych, a także w zainteresowanych podmiotach, opracowane zostaną nowe standardy lub nastąpi przełożenie istniejących norm i standardów na konkretne rekomendacje w zakresie ich wdrażania.

Odrębnym zagadnieniem jest potrzeba wypracowania rekomendacji w zakresie zabezpieczeń technicznych, konfiguracji systemów, procedur bezpiecznej eksploatacji i bezpiecznego użytkowania. Opracowane rekomendacje będą dotyczyć podmiotów, które nie są lub nie będą z mocy prawa zobowiązane do stosowania określonych rozwiązań, jak również obywateli. Zostaną również przygotowane polityki informacyjne dopasowane do potrzeb poszczególnych grup odbiorców.

5.6. Wypracowanie i wdrożenie systemu zarządzania ryzykiem na poziomie krajowym

Na potrzeby zarządzania bezpieczeństwem państwa w cyberprzestrzeni opracowana zostanie spójna metodyka szacowania ryzyka, uwzględniająca specyfikę poszczególnych sektorów, a także operatorów infrastruktury krytycznej, usług kluczowych i dostawców usług cyfrowych. Zapewni to porównywalność szacowań, w tym określenie poziomu ryzyka, w szczególności na potrzeby raportu o zagrożeniach bezpieczeństwa narodowego, sporządzanego na podstawie przepisów o zarządzaniu kryzysowym. Aby uzyskać dane niezbędne do szacowania ryzyka, konieczne będzie opracowanie modelu zależności, opisującego wpływ incydentu w jednym podmiocie na realizację usług przez inne podmioty.

Minister właściwy ds. informatyzacji zapewni działanie systemu analizy i bieżącego zarządzania ryzykiem w cyberprzestrzeni RP. W obszarze operacyjnym informacje z systemu przekazywane będą zainteresowanym stronom w trybie online. Dostęp do tego systemu będą miały instytucje odpowiedzialne za bezpieczeństwo cyberprzestrzeni RP oraz instytucja koordynująca zarządzanie kryzysowe.

Opracowany zostanie również system dynamicznego zarządzania ryzykiem wynikającym ze zidentyfikowanych w skali globalnej podatności w oprogramowaniu i sprzęcie.

5.7. Zapewnienie bezpiecznego łańcucha dostaw

Zapewnienie wysokiego poziomu bezpieczeństwa systemów teleinformatycznych wymaga, aby w procesie ich budowy, eksploatacji oraz wycofywania zapewniony był tak zwany bezpieczny łańcuch dostaw. Pod pojęciem łańcucha dostaw należy rozumieć system, na który składają się podsystemy produkcji, dystrybucji, transportu, magazynowania oraz recyklingu komponentów systemów teleinformatycznych.

Ważnym elementem zapewnienia jakości w łańcuchu dostaw jest ocena i certyfikacja produktów. Priorytetowe w tym zakresie będzie utworzenie krajowego systemu oceny, co będzie sprzyjać uzyskaniu narodowej niezależności w wymiarze sprzętowym, programistycznym i kryptologicznym.

Z uwagi na procesy globalizacyjne niezbędne jest włączenie Polski w międzynarodowy system oceny i certyfikacji oparty na międzynarodowych normach i standardach. Polska aktywnie włączy się w ustanowienie europejskiego systemu oceny i certyfikacji produktów oraz usług sektora technologii informatycznych i komunikacyjnych. Polska ubiegać się będzie o członkostwo w międzynarodowych organizacjach skupiających organy certyfikujące, takich jak SOGIS MRA[2] oraz CCRA[3].

5.8. Zbudowanie systemu ostrzegania użytkowników cyberprzestrzeni w zakresie ryzyka wynikającego z cyberzagrożeń

Kluczowym warunkiem zapewnienia bezpieczeństwa systemów teleinformatycznych jest dostęp do informacji o zagrożeniach oraz dzielenie się informacjami o występujących lub mogących nastąpić atakach. W tym celu zbudowany zostanie system bieżącego zarządzania bezpieczeństwem cyberprzestrzeni. System ten umożliwi zgłaszanie informacji o zagrożeniach i podatnościach, ich agregowane, analizowanie i korelowanie. Na podstawie przeprowadzonych analiz przekazywane będą ostrzeżenia do zainteresowanych stron na temat zagrożeń i podatności, w taki sposób, aby zachowane zostały zasady poufności informacji przekazywanych w zgłoszeniach, ze szczególnym uwzględnieniem tajemnicy przedsiębiorstwa, którego dane zgłoszenie dotyczy.

W celu ochrony użytkowników końcowych przed skutkami zidentyfikowanych zagrożeń zostanie utworzony dodatkowy system informacyjny dla obywateli.

[2] SOG-IS MRA – Senior Officials Group Information Systems Security Mutual Recognition Agreement

[3] CCRA - Common Criteria Recognition Arrangement

6. Cel szczegółowy 2 – Wzmocnienie zdolności do przeciwdziałania cyberzagrożeniom

6.1. Zwiększanie zdolności do zwalczania cyberprzestępczości, w tym cyberszpiegostwa i zdarzeń o charakterze terrorystycznym, występującej w cyberprzestrzeni

W zakresie zwiększania zdolności do zwalczania cyberprzestępczości, w tym cyberszpiegostwa, zdarzeń o charakterze terrorystycznym oraz działań o charakterze hybrydowym, ważne jest zapewnienie wsparcia dla operatorów usług kluczowych, dostawców usług cyfrowych oraz operatorów infrastruktury krytycznej w wykrywaniu oraz zwalczaniu incydentów we wszystkich ich fazach. Wymagana jest współpraca oraz koordynacja działań organów ścigania niezależnie od motywów, którymi kierują się sprawcy przestępstw. Istotne znaczenie ma zabezpieczenie dowodów elektronicznych.

Zwiększenie efektywności czynności procesowych lub operacyjnych wymaga także poszerzenia współdziałania organów ścigania z innymi podmiotami, które mogą posiadać wiedzę w zakresie ustalenia istoty przestępstwa lub mogą przyczynić się do ustalenia jego sprawcy. Dotyczy to współpracy z krajowymi oraz międzynarodowymi podmiotami prywatnymi, szczególnie z sektora telekomunikacyjnego, bankowego oraz ubezpieczeniowego. Niezbędne jest zaangażowanie przedstawicieli organów ścigania, w tym Policji, w prace krajowych oraz międzynarodowych forów wymiany informacji o zagrożeniach i podatnościach.

Mając na uwadze specyfikę cyberprzestrzeni zwalczanie cyberprzestępczości wymaga transgranicznej współpracy organów ścigania oraz podmiotów typu CERT/CSIRT. W czynnościach procesowych lub w procesie rozpoznania operacyjnego dotyczących przestępstw dokonywanych w cyberprzestrzeni krytyczny jest upływ czasu. Oznacza to, że wymagane są sprawne i zaufane kanały wymiany informacji pomiędzy organami ścigania różnych państw.

Szybko zmieniające się metody popełniania przestępstw wymagają rozwijania badań naukowych w obszarze zwalczania cyberprzestępczości, których wyniki zapewnią wsparcie dla organów ścigania. Wyniki tych badań będą wykorzystywane w pracy organów ścigania i wymiaru sprawiedliwości, jak też będą stanowić materiał do opracowania działań profilaktycznych. Wdrożone zostaną, skierowane do społeczeństwa, programy informacyjne o zagrożeniach cyberprzestępczością oraz metodach unikania skutków tych zagrożeń. Wskazane zostaną sposoby postępowania dla osób

dotkniętych przestępstwem. Ważną rolę do odegrania w tego typu działalności będą mieli operatorzy usług kluczowych, dostawcy usług cyfrowych, dostawcy usługi dostępu do Internetu oraz organizacje pozarządowe.

6.2. Uzyskanie zdolności do prowadzenia pełnego spektrum działań militarnych w cyberprzestrzeni

SZ RP, jako podstawowy element systemu obronnego państwa, muszą prowadzić działania w cyberprzestrzeni[4] tak samo skutecznie jak w powietrzu, na lądzie i na morzu. Zdolności do prowadzenia pełnego spektrum działań militarnych w cyberprzestrzeni muszą więc obejmować: rozpoznawanie zagrożeń, ochronę i obronę systemów teleinformatycznych oraz zwalczanie źródeł zagrożeń.

Działania w cyberprzestrzeni włączone zostaną w planowanie operacyjne oraz stanowić będą integralną część operacji prowadzonych przez SZ RP samodzielnie, jak i w układzie sojuszniczym oraz koalicyjnym. Udoskonalone zostaną struktury wojskowe, które zapewnią skuteczniejsze planowanie, dowodzenie i zarządzanie zasobami, umiejętnościami i zdolnościami. Umiejętności personelu prowadzącego działania militarne w cyberprzestrzeni będą stale podnoszone w ramach szkoleń wewnętrznych, jak i wysoce specjalistycznych szkoleń zewnętrznych przygotowywanych na potrzeby resortu obrony narodowej. Jednocześnie prowadzone będzie na bieżąco rozpoznanie zagrożeń oraz ocena sytuacji w celu podjęcia właściwych środków ochrony lub aktywnego przeciwdziałania źródłom zagrożeń. Mając na uwadze dynamikę rozwoju technologii tworzących środowisko, jakim jest cyberprzestrzeń, resort obrony narodowej będzie dążyć do wytworzenia, bądź pozyskania nowatorskiego zestawu narzędzi, który podniesie ich skuteczność działania w tej domenie

6.3. Zbudowanie zdolności w zakresie analizy zagrożeń na poziomie krajowym

Niezbędnym elementem systemu bezpieczeństwa cyberprzestrzeni jest utrzymywanie i rozwijanie krajowych zdolności analitycznych w zakresie ogólnej oceny sytuacji w obszarze cyberzagrożeń oraz weryfikacji i dogłębnej analizy konkretnych zagrożeń i incydentów.

---

[4] Cyberprzestrzeń uznana została przez NATO jako kolejna domena działań operacyjnych na Szczycie NATO w Warszawie w 2016 r.

W tym celu, w krajowym systemie cyberbezpieczeństwa, będzie uwzględniony komponent, który na podstawie materiałów ze źródeł krajowych i zagranicznych oraz badań własnych i podmiotów współpracujących, będzie realizował zadania analityczne. Rolę tą będzie pełniło Narodowe Centrum Cyberbezpieczeństwa.

6.4. Zbudowanie systemu bezpiecznej komunikacji na potrzeby bezpieczeństwa narodowego

Zbudowany zostanie spójny system łączności jawnej i niejawnej całej administracji rządowej na potrzeby systemu kierowania bezpieczeństwem narodowym. System ten będzie obejmował użytkowników administracji publicznej różnych szczebli, zapewniając niezwodną łączność w ramach kierowania bezpieczeństwem narodowym, we wszystkich fazach zarządzania kryzysowego oraz gotowości obronnej państwa. System zapewni bezpieczną, terminową i niezawodną wymianę informacji w relacjach wewnętrznych oraz zewnętrznych, w tym z dowództwami, strukturami polityczno-wojskowymi NATO i UE. Dostarczy on niezbędne usługi telekomunikacyjne, takie jak telefonia, transmisja danych, poczta elektroniczna, wideo i telekonferencje, dostęp do Internetu, dostęp do baz danych rejestrów państwowych. Usługom systemu zapewniony zostanie wymagany poziom bezpieczeństwa.

6.5. Audyty i testy bezpieczeństwa

Jednym ze środków, który pozwala na dokonanie oceny skuteczności wdrożonych systemów zarządzania bezpieczeństwem i adekwatności ustanowionych zabezpieczeń, są okresowe audyty. Na podstawie norm i dobrych praktyk oraz uwzględniając specyfiki poszczególnych sektorów, opracowane zostaną spójne metodyki audytów. Celem takiego podejścia jest uzyskanie porównywalności wyników audytów.

Kolejnym środkiem oceny bezpieczeństwa są testy penetracyjne, które pozwalają na rzeczywistą ocenę odporności systemu na zagrożenia. Ich wyniki stanowią podstawę weryfikacji przyjętych założeń w zakresie ustanowionych zabezpieczeń.

Testowanie zabezpieczeń wymaga posiadania specjalistycznych narzędzi. Niezbędne jest podjęcie prac legislacyjnych, które na nowo uregulują ten obszar. Należy również rozpatrzeć możliwość prawnego uregulowania tzw. *bug-bounty*[5].

[5] Bug-bounty – poszukiwanie podatności w oprogramowaniu przez osoby niezwiązane z producentem tego oprogramowania, zwykle za jego zgodą generalną.

7. Cel szczegółowy 3 – Zwiększanie potencjału narodowego oraz kompetencji w zakresie bezpieczeństwa w cyberprzestrzeni

7.1. Rozbudowa zasobów przemysłowych i technologicznych na potrzeby cyberbezpieczeństwa

Rząd Polski stawia sobie za cel inwestowanie w rozbudowę zasobów przemysłowych i technologicznych na potrzeby cyberbezpieczeństwa poprzez stwarzanie warunków dla rozwoju przedsiębiorstw, ośrodków naukowo-badawczych, jak i *start-upów*, których przedmiotem działalności jest tworzenie nowych rozwiązań, tym w obszarze cyberbezpieczeństwa. W ramach rozwoju kompetencji powstanie program *Cyberpark Enigma* dysponujący potencjałem pozwalającym konkurować na europejskim rynku specjalistycznych usług z zakresu teleinformatyki. Projekt zakłada odtworzenie i rozbudowę kompetencji w obszarze budowy zdolności do kompleksowego wytwarzania urządzeń i oprogramowania wykorzystywanych we wszystkich gałęziach przemysłu. Pozyskiwanie nowych technologii dla rozwoju rodzimych przedsięwzięć będzie realizowane również poprzez udział w inicjatywach europejskich kładących nacisk na innowacyjność, w drodze współpracy dwustronnej oraz w ramach organizacji międzynarodowych.

Celem podnoszenia kompetencji ośrodków naukowych w obszarze cyberbezpieczeństwa planowane jest powstanie Naukowego Klastra Cyberbezpieczeństwa (NKC). Będzie to platforma naukowa złożona z uczelni wyższych oraz ośrodków naukowo-badawczych specjalizujących się w technologiach cyberbezpieczeństwa.

W celu wyrównania szans polskich przedsiębiorców na globalnym rynku oraz wspierając rozwój polskiego biznesu w uzyskiwaniu zdolności cyfrowych, powstaną huby innowacyjności[6], które będą oferować kompleksową obsługę dla firm i *start-up'ów*, w tym testowanie nowych rozwiązań, badanie rynku, pomoc w ubieganiu się o środki na rozwój innowacyjnych rozwiązań innowacyjnych, doradztwo w dostępie do nowych rynków jak i pomoc w nawiązaniu współpracy z innymi przedsiębiorcami.

[6]środowisko technologiczne i organizacyjne, w którym osoby nie dysponujące zasobami mogą przetestować wymyślone przez siebie innowacyjne rozwiązania oraz uzyskać pełne wsparcie w zakresie komercjalizacji tego rozwiązania

7.2. Zbudowanie mechanizmów współpracy między sektorem publicznym i prywatnym

Zapewnienie bezpieczeństwa w cyberprzestrzeni wymaga wspólnego wysiłku sektora prywatnego, publicznego oraz obywateli. Rząd będzie dążył do zbudowania efektywnego systemu partnerstwa publiczno-prywatnego opartego na zaufaniu i wspólnej odpowiedzialności za bezpieczeństwo w cyberprzestrzeni. Jednocześnie administracja publiczna będzie doskonaliła swój potencjał w zakresie doradzania sektorom rynkowym w dziedzinie bezpieczeństwa teleinformatycznego. Rząd będzie również aktywnie angażować się w istniejące i powstające formy europejskiej współpracy publiczno-prywatnej i tym samym promować polski biznes na arenie międzynarodowej.

Realizując nową wizję rozwoju kraju i wspierając innowacyjność polskiej gospodarki, istotna będzie budowa systemu wsparcia przedsięwzięć badawczo-rozwojowych w dziedzinie cyberbezpieczeństwa, w tym projektów realizowanych we współpracy ze światem nauki oraz z przedsiębiorstwami komercyjnymi.

7.3. Stymulowanie badań i rozwoju w obszarze bezpieczeństwa systemów teleinformatycznych

W związku z dynamicznie rozwijającym się rynkiem informatycznym, w szczególności w związku z perspektywą zmiany aktualnie użytkowanego w sieci Internet protokołu IPv4 na rzecz protokołu IPv6, a także w związku z rozwojem idei Internetu Rzeczy, Inteligentnych Miast, Przemysłu 4.0, jak również Chmury Obliczeniowej, czy Megadane (*Big Data)* zachodzi konieczność intensyfikacji działań badawczych i rozwojowych oraz wytwórczych w zakresie cyberbezpieczeństwa.

W tym celu wspólnie z Narodowym Centrum Badań i Rozwoju uruchomiony zostanie program badawczy, mający na celu przygotowanie i wdrożenie nowych metod ochrony przed zagrożeniami pochodzącymi z cyberprzestrzeni.

Ponadto we współpracy ze środowiskiem naukowo-akademickim zostaną opracowane programy badawcze mające na celu:

- ocenę skuteczności zabezpieczeń i odporności cyberprzestrzeni RP na cyberzagrożenia,
- ocenę skuteczności reagowania za zagrożenia,
- analizę tendencji w zakresie nowych cyberprzestępstw, cyberterroryzmu i metod ich zwalczania,

- badanie metod ataków i sposobów przeciwdziałania tym atakom.

Ważne zadania w systemie zapewnienia cyberbezpieczeństwa mają organizacje pozarządowe, które mogą być użyteczne jako organizatorzy działań edukacyjnych w społeczeństwie, a także jako dostawcy analiz i opinii dla administracji publicznej. Możliwe jest także pozyskiwanie specjalistów o unikatowych umiejętnościach przez ośrodki analityczne na potrzeby rozwiązywania skomplikowanych problemów z zakresu cyberbezpieczeństwa.

7.4. Zwiększanie kompetencji kadry podmiotów istotnych dla funkcjonowania bezpieczeństwa cyberprzestrzeni

Podnoszenie kompetencji kadry podmiotów istotnych dla funkcjonowania bezpieczeństwa cyberprzestrzeni RP będzie realizowane poprzez stworzenie i wdrożenie takiego modelu funkcjonowania systemu edukacji akademickiej i doskonalenia zawodowego, który zapewni odpowiednie do wyzwań kwalifikacje pracowników.

Uczelnie będą zachęcane do tego, aby rozwijane były specjalizacje interdyscyplinarne obejmujące między innymi zarządzanie bezpieczeństwem informacji, ochronę danych osobowych, ochronę własności intelektualnej w Internecie oraz zagadnienia związane z rozwojem nowych technologii i wyzwaniami, które są tego pochodnymi.

W ramach szeroko rozumianej edukacji eksperckiej, aby skuteczniej przeciwdziałać rozwijającej się cyberprzestępczości, zostanie wzmocniony system szkoleń dla wszystkich pracowników podmiotów istotnych dla funkcjonowania bezpieczeństwa w cyberprzestrzeni oraz dla przedstawicieli organów ścigania i wymiaru sprawiedliwości.

W celu zatrzymania w administracji publicznej pracowników o wysokich kompetencjach, równolegle z wykorzystaniem innych instrumentów wspierających ich aktywność, uruchomione zostaną programy motywacyjne, w tym rządowy program „Złota Setka”. Program będzie skierowany do specjalistów z obszaru IT i bezpieczeństwa teleinformatycznego, zatrudnionych w administracji publicznej, mający na celu utrzymywanie i promowanie najlepiej wykwalifikowanych specjalistów. Za przygotowanie i wdrożenie programu odpowiadać będzie minister właściwy do spraw informatyzacji.

W celu zapewnienia merytorycznego wsparcia dla kierowników jednostek administracji rządowej w zakresie zarządzania cyberbezpieczeństwem utrzymana zostanie zasada powoływania w tych jednostkach Pełnomocników do spraw bezpieczeństwa cyberprzestrzeni.

Dla optymalnego wykorzystania zasobów ludzkich w obszarze cyberbezpieczeństwa zostanie opracowany model zarządzania tymi zasobami.

7.5. Stworzenie warunków do bezpiecznego korzystania z cyberprzestrzeni przez obywateli

Edukację w zakresie cyberbezpieczeństwa należy rozpoczynać już na etapie kształcenia wczesnoszkolnego. Uwzględniając tematykę bezpiecznego korzystania z cyberprzestrzeni zakłada się opracowanie i wdrożenie zmian do podstaw programowych nauczania. Planuje się także opracowanie i uruchomienie kursów doszkalających dla nauczycieli informatyki oraz wdrożenie adekwatnych zmian w kształceniu podyplomowym nauczycieli.

Równolegle, we współpracy z organizacjami pozarządowymi oraz ośrodkami akademickimi, administracja publiczna podejmie systemowe działania uwrażliwiające społeczeństwo na zagrożenia płynące z w cyberprzestrzeni, a także działania edukacyjne w zakresie praw i wolności w środowisku cyfrowym. Uruchomione zostaną m.in. kampanie społeczne, skierowane do różnych grup docelowych (między innymi dzieci, rodziców, seniorów).

Administracja publiczna będzie wspierać wszelkie działania, zarówno operatorów usług kluczowych jak i dostawców usług cyfrowych, w zakresie podejmowania działań edukacyjnych i informacyjnych. Celem działań będzie zapewnienie użytkownikom końcowym dostępu do wiedzy pozwalającej na zrozumienie zagrożeń w cyberprzestrzeni i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami.

8. Cel szczegółowy 4 – Zbudowanie silnej pozycji międzynarodowej Polski w obszarze cyberbezpieczeństwa

8.1. Aktywna współpraca międzynarodowa na poziomie strategiczno-politycznym

W obliczu wszechobecnych procesów globalizacyjnych i związanych z nimi współzależności państw, międzynarodowa współpraca jest kluczowa dla osiągnięcia bezpieczeństwa globalnej cyberprzestrzeni.

Realizując te zadania na poziomie europejskim Polska zintensyfikuje działania na rzecz zapewnienia bezpieczeństwa Jednolitego Rynku Cyfrowego jako motoru wzrostu gospodarczego i innowacyjności. Ponadto istotne jest dążenie do szerszego uwzględnienia aspektów cyberbezpieczeństwa w pracach nad pogłębieniem Wspólnej Polityki Zagranicznej i Bezpieczeństwa Unii Europejskiej.

Członkostwo w Sojuszu Północnoatlantyckim jest istotnym filarem bezpieczeństwa Polski jak i bezpieczeństwa euroatlantyckiego. Nasilające się ataki o charakterze hybrydowym czynią nieodzownym inwestowanie w zdolności odstraszania i obronne, w tym doskonalenia swojej odporności i zdolności do szybkiego i skutecznego reagowania na cyberataki.

Współpracując w ramach systemu Organizacji Narodów Zjednoczonych Polska będzie dążyła do kontynuacji debaty dotyczącej sprawnie funkcjonującego systemu międzynarodowego zarządzania siecią globalną oraz zagadnień związanych z prawną oceną cyberataków, w celu wypracowania spójnych rozwiązań, gwarantujących pewność międzynarodowej wymiany informacji w Internecie. Polska będzie angażować się we wzmacnianie środków budowy zaufania i bezpieczeństwa w ramach istniejących forów międzynarodowych, w tym OBWE. Rząd będzie włączał się również w działania na rzecz skutecznego zwalczania cyberprzestępczości w wymiarze międzynarodowym.

Istotna jest również współpraca z krajami regionu, w tym wzmocnienie współpracy w ramach Grupy Wyszehradzkiej, jak i z państwami Morza Bałtyckiego.

Wzmocnienie polskiej pozycji międzynarodowej będzie możliwe tylko na drodze wewnętrznej ścisłej kooperacji pomiędzy instytucjami i agencjami odpowiadającymi w Polsce za zapewnienie cyberbezpieczeństwa, w tym szczególnie pomiędzy ministrem właściwym ds. informatyzacji oraz z ministrem spraw zagranicznych odpowiadającym za całokształt polskiej polityki zagranicznej.

Silna pozycja międzynarodowa Polski w obszarze cyberbezpieczeństwa nie będzie możliwa bez odpowiedniego zaplecza merytorycznego. Zasób kadrowy wsparty odpowiednim finansowaniem będzie podstawą do zbudowania wizerunku Polski jako kompetentnego gracza na arenie międzynarodowej. W tym kontekście istotne jest, aby eksperci z Polski aktywnie uczestniczyli w dyskusjach prowadzonych na forach regionalnych i globalnych oraz odgrywali kluczowe role w organizacjach międzynarodowych, przyczyniając się w ten sposób do skutecznej realizacji polityki zagranicznej w zakresie cyberbezpieczeństwa. Celem zdobywania umiejętności, rozwijania wiedzy i wymiany najlepszych praktyk Polska będzie przykładała jeszcze większą wagę do współpracy międzynarodowej, dwu- i wielostronnej, w kwestiach edukacji, szkoleń i ćwiczeń jak i budowania świadomości.

8.2. Aktywna współpraca międzynarodowa na poziomie operacyjnym i technicznym

Współpraca międzynarodowa na poziomie operacyjno-technicznym realizowana będzie między innymi w ramach Sieci CSIRT na poziomie Unii Europejskiej, na innych forach wymiany informacji i dokonywania analiz sytuacji bezpieczeństwa IT danego sektora, poprzez inne międzynarodowe sieci współpracy typu FIRST, czy TF-CSIRT, platformy wymiany informacji typu MISP, czy n6 oraz w ramach współpracy dwu- i wielostronnej. W tym kontekście szczególne znaczenie będzie miało wypracowanie wspólnych procedur działania w ramach UE i NATO oraz Grupy Wyszehradzkiej. Współpraca na tym poziomie będzie służyła nie tylko skutecznemu przeciwdziałaniu zagrożeniom w cyberprzestrzeni, ale przyczyni się do wymiany doświadczeń pomiędzy personelem technicznym w ramach wspólnych przedsięwzięć. Będzie również okazją do promowania polskich rozwiązań technologicznych i polskiej kadry eksperckiej.

9. Zarządzanie Krajowymi Ramami Polityki Bezpieczeństwa

Krajowe Ramy Polityki Cyberbezpieczeństwa uchwalane są na okres 5 lat. Koordynatorem wdrażania Krajowych Ram Polityki Cyberbezpieczeństwa jest minister właściwy do spraw informatyzacji. Po dwóch latach od przyjęcia oraz w czwartym roku obowiązywania dokument podlega przeglądowi i ocenie efektów jego oddziaływania. Wyniki przeglądu przedstawiane są Radzie Ministrów. W wyniku dokonanego przeglądu minister właściwy do spraw informatyzacji opracowuje propozycję działań korygujących lub projekt dokumentu na kolejny okres pięcioletni. W przypadku wystąpienia uzasadnionych okoliczności Krajowe Ramy Polityki Cyberbezpieczeństwa mogą być aktualizowane w innych terminach, niż te o których mowa powyżej.

Koordynator w terminie do sześciu miesięcy od przyjęcia Krajowych Ram Polityki Cyberbezpieczeństwa we współpracy z członkami Rady Ministrów, kierownikami urzędów centralnych, Dyrektorem Rządowego Centrum Bezpieczeństwa opracuje *Plan działań na rzecz wdrożenia Krajowych Ram Polityki Cyberbezpieczeństwa*. Przy opracowywaniu *Planu* wymienione powyżej organy uwzględniają w swoich działaniach problematykę cyberbezpieczeństwa w zakresie zgodnym z ustawowymi kompetencjami. *Plan działań* obejmować będzie w szczególności:

1) nazwę celu szczegółowego,
2) nazwę zadania,
3) typ działania – działanie: legislacyjne, organizacyjne, technologiczne, edukacyjne, informacyjne, promocyjne, inne,
4) podejmowane przedsięwzięcia lub narzędzia realizacji,
5) harmonogram – termin rozpoczęcia i termin zakończenia podejmowanej inicjatywy,
6) organ lub organy – organ wiodący i organy współpracujące przy realizacji zadania,
7) oczekiwane efekty wynikające z realizacji zadania,
8) szacunkowy koszt realizacji zadania.

W stosunku do pozycji *Planu* zawierających informacje o charakterze niejawnym zastosowanie mają przepisy ustawy o ochronie informacji niejawnych.

Koordynator będzie corocznie przygotowywał sprawozdanie o postępach wdrażania Krajowych Ram Polityki Cyberbezpieczeństwa za rok poprzedni na podstawie informacji otrzymywanych od podmiotów zaangażowanych w jej realizację. Sprawozdania będą przedkładane Radzie Ministrów.

10.Finansowanie

Już obecnie, na mocy obowiązujących przepisów, podmioty realizujące zadania publiczne są zobowiązane do ujmowania w swoich planach finansowych nakładów na cyberbezpieczeństwo. Koszty te powiększą się o nakłady przeznaczone na działania integracyjne związane z budową krajowego systemu cyberbezpieczeństwa oraz o nakłady ponoszone na realizację pozostałych przedsięwzięć *Planu działań na rzecz wdrożenia Krajowych Ram Polityki Cyberbezpieczeństwa*. Szczegółowa wielkość i struktura kosztów poszczególnych przedsięwzięć będzie określona w procesie inicjowania konkretnych projektów. Oszacowanie kosztów finansowania wdrażania Krajowych Ram Polityki Cyberbezpieczeństwa nastąpi w ramach *Planu działań*. Źródłami finansowania realizacji działań opisanych w dokumencie będą plany finansowe poszczególnych jednostek zaangażowanych we wdrażanie Krajowych Ram Polityki Cyberbezpieczeństwa, a także środki pochodzące z Narodowego Centrum Badań i Rozwoju oraz środki Unii Europejskiej, w miarę zaistnienia takich możliwości.

Docelowo niezbędne jest ustanowienie w ramach budżetu państwa Wieloletniego Programu dedykowanego budowie i rozwojowi przedsięwzięć w obszarze cyberbezpieczeństwa.

11.Słownik

Na potrzeby niniejszego dokumentu stosuje się następujące definicje:

1) „sieci i systemy informatyczne” lub inaczej „systemy teleinformatyczne” oznaczają:
    a) sieci łączności elektronicznej w rozumieniu art. 2 lit. a) dyrektywy 2002/21/WE,
    b) wszelkie urządzenia lub grupy wzajemnie połączonych lub powiązanych urządzeń, z których jedno lub większa ich liczba, wykonując program, dokonuje automatycznego przetwarzania danych cyfrowych; lub
    c) dane cyfrowe przechowywane, przetwarzane, odzyskiwane lub przekazywane przez elementy określone w lit. a) i b) w celu ich eksploatacji, użycia, ochrony i utrzymania,
2) „cyberprzestrzeń” oznacza przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami,
3) „bezpieczeństwo sieci i systemów informatycznych” lub inaczej „cyberbezpieczeństwo” lub inaczej „bezpieczeństwo teleinformatyczne” oznacza odporność systemów teleinformatycznych, przy danym poziomie zaufania, na wszelkie działania naruszające dostępność, autentyczność, integralność lub poufność przechowywanych lub przekazywanych, lub przetwarzanych danych, lub związanych z nimi usług oferowanych lub dostępnych poprzez te sieci i systemy informatyczne,
4) „operator usługi kluczowej” oznacza podmiot publiczny lub prywatny, należący do jednego z rodzajów, o których mowa w załączniku II dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148, spełniający kryteria określone w odrębnych przepisach,
5) „usługa cyfrowa” oznacza usługę w rozumieniu art. 1 ust. 1 lit. b) dyrektywy Parlamentu Europejskiego i Rady (UE) 2015/1535, która należy do jednego z rodzajów wymienionych w załączniku III dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148,
6) „incydent” oznacza każde zdarzenie, które ma rzeczywiście niekorzystny wpływ na bezpieczeństwo systemów teleinformatycznych,
7) „poważny incydent” oznacza incydent lub grupa incydentów, które powodują lub mogą spowodować znaczną szkodę dla bezpieczeństwa publicznego, interesów międzynarodowych RP, w tym interesów gospodarczych, poziomu zaufania do instytucji publicznych, swobód obywatelskich lub zdrowia obywateli RP,

8) „ryzyko” oznacza każdą dającą się racjonalnie określić okoliczność lub zdarzenie, które ma potencjalny niekorzystny wpływ na bezpieczeństwo sieci i systemów informatycznych,
9) „norma” oznacza normę w rozumieniu art. 2 pkt 1 rozporządzenia (UE) nr 1025/2012,
10) „usługa przetwarzania w chmurze” lub „Cloud Computing” oznacza usługę cyfrową umożliwiającą dostęp do skalowalnego i elastycznego zbioru zasobów obliczeniowych do wspólnego wykorzystywania,
11) „CSIRT” lub „CERT”[7] lub „Zespół reagowania na incydenty komputerowe” oznacz grupę osób składającą się z analityków bezpieczeństwa, zorganizowaną w celu opracowywania, rekomendowania i koordynowania działań mających na celu wykrywanie, powstrzymywanie i zwalczanie skutków wynikających z incydentów, a także pozyskanie informacji na temat istoty tych incydentów,
12) „Sieć CSIRT” oznacza strukturę organizacyjną, o której mowa w art. 12 Dyrektywy NIS,
13) „CSIRT Narodowy” oznacza strukturę na poziomie krajowym pełniącą rolę i posiadającą kompetencje w zakresie CSIRT w odniesieniu do incydentów i zagrożeń o charakterze ponadsektorowym, międzynarodowym oraz dużej skali odziaływania na poziomie kraju,
14) „Krajowy system cyberbezpieczeństwa” oznacza system, w skład którego wchodzą krajowe podmioty lub struktury organizacyjne podmiotów wraz z relacjami pomiędzy tymi podmiotami lub strukturami, służący zapewnieniu wysokiego poziomu bezpieczeństwa cyberprzestrzeni RP,
15) „Narodowe Centrum Cyberbezpieczeństwa” oznacza element krajowego systemu cyberbezpieczeństwa, którego rola polega na monitorowaniu stanu bezpieczeństwa cyberprzestrzeni na poziomie krajowym, koordynowaniu działań mających na celu zapobieganie, przeciwdziałanie i analizowanie istoty oraz skutków poważnych incydentów,
16) „klaster bezpieczeństwa” oznacza wydzieloną sieć typu intranet, łączącą podmioty należące do tego klastra, udostępniającą usługi bezpieczeństwa, w tym usługę bezpiecznego dostępu do Internetu.

[7] CERT (Computer Emergency Response Team) jest nazwą zastrzeżoną przez Carnegie Mellon University i jej używanie wymaga zgody tego uniwersytetu. Zgodę taką posiada CERT Polska. Dyrektywa NIS posługuje się nazwą CSIRT.