ZAŁOŻENIA STRATEGII CYBERBEZPIECZEŃSTWA DLA RZECZYPOSPOLITEJ POLSKIEJ

Opracował: Zespół zadaniowy Ministerstwa Cyfryzacji

luty 2016 r.

Spis treści

1. Wprowadzenie

Obszar bezpieczeństwa obywateli (również w sieci Internet) powinien być stawiany na równi z ochroną militarną kraju. Ochrona cywilnej cyberprzestrzeni RP jest jednym z głównych priorytetów rządu, jednak do tej pory nie zbudowano silnego ośrodka koordynującego ten niezmiernie istotny obszar, wpływający bezpośrednio na bezpieczeństwo obywateli oraz przedsiębiorców. W sieci Internet coraz częściej dochodzi do naruszania ekonomicznych praw obywateli i przejmowania ich wrażliwych danych – należy temu skutecznie przeciwdziałać. Oczywiście skuteczna ochrona cyberprzestrzeni to nie tylko kwestia ochrony w granicach naszego Państwa, gdyż problem ma charakter ponadgraniczny.

Ogólnoświatowe statystyki mówią same za siebie[1]:

- W roku 2014 pojawiło się 6,5 tys. nowych podatności w oprogramowaniu wykorzystywanym przez strony internetowe,
- 76% przebadanych stron internetowych posiadało podatności, poprzez które można było je zaatakować,
- w przypadku 5 najistotniejszych zidentyfikowanych podatności czas potrzebny producentowi na ich usunięcie wynosił 59 dni, a łączny czas ekspozycji aplikacji zawierających te podatności na ataki typu zero day exploit osiągnął 295 dni,
- codziennie atakowanych było 0,5 mln stron internetowych,
- codziennie generowano 28 mld maili o charakterze spamu,
- jeden na prawie 1000 wysłanych na świecie maili jest mailem o charakterze phishingu,
- rocznie generowanych było 317 mln nowych wariantów malware,
- stwierdzono 35 podatności w systemach sterowników przemysłowych wytwarzanych przez 9 wiodących producentów, w tym w systemach sterowania stosowanych w infrastrukturze krytycznej,
- odnotowano 312 istotnych włamań do systemów teleinformatycznych, w tym w czterech przypadkach istnieje podejrzenie wykradzenia ponad 10 mln tożsamości w każdym z tych włamań; w sumie skradzionych mogło być prawie 350 mln tożsamości,
- w skali świata ok. 2 mln komputerów pracowało w sieciach botnet; **Polska znalazła się na 10 miejscu wśród krajów o największym współczynniku zagrożenia z 2,8% komputerów pracujących w sieciach botnet.**

Według badania Center for Strategic and International Studies (CSIS), każdego roku działania cyberprzestępców powodują w skali światowej straty w wysokości 445 miliardów dolarów.

Takie ataki generowane są zarówno z obszaru podlegającego jurysdykcji RP, a także z obszarów cyberprzestrzeni leżących nie tylko poza jurysdykcją RP, ale także z obszarów, z którymi RP nie ma umów o wzajemnej pomocy prawnej lub z obszarów, w stosunku do których istnieją formalnie umowy o takiej pomocy, jednakże z różnych powodów strona polska pomocy nie uzyskuje. Na koniec należy zauważyć, że z uwagi na stosowanie w cyberprzestrzeni metod anonimizacji użytkowników niekiedy nie jest możliwe ustalenie miejsca położenia atakującego.

[1] *Internet Security Threat Report*, Symantec, 2015 (statystyki za rok 2014)

Potencjalnymi atakującymi mogą być zarówno grupy przestępcze, działające z chęci zysku, jak i grupy za którymi stoją służby specjalne państw obcych, a działania takie służą pozyskaniu informacji, destabilizacji politycznej lub gospodarczej albo wywołaniu niezadowolenia społecznego wobec władz RP. Zwykle atakujący ukrywa swój związek z instytucjami państwowymi, a udowodnienie takiego związku jest praktycznie niemożliwe. Należy mieć również na uwadze fakt, że w cyberprzestrzeni dostępne są narzędzia umożliwiające tworzenie oprogramowania złośliwego przez osoby, które w praktyce nie mają żadnego przygotowania programistycznego, a powstałe oprogramowanie złośliwe rozsyłane jest poprzez cyberprzestrzeń z pobudek chuligańskich, a w przypadku dzieci wręcz nieświadomie.

Szczytową formą wrogich działań obcego państwa może być tak zmasowany atak z cyberprzestrzeni na infrastrukturę informatyczną, że należałoby mówić o działaniach wojennych.

Ataki z cyberprzestrzeni mogą dotyczyć nie tylko systemów informacyjnych sektora prywatnego i administracji publicznej, ale jak wskazują doświadczenia ostatnich lat, dotyczą również systemów automatyki przemysłowej (SCADA), w tym automatyki przemysłowej w obiektach infrastruktury krytycznej. Ataki w tym sektorze mogą prowadzić do zniszczeń fizycznych w obiektach mających istotne znaczenie dla gospodarki, środowiska i obywateli.

W świetle tak zarysowanych zagrożeń, rosnącej komplikacji systemów teleinformatycznych, wzrastającej zależności produkcji, administracji publicznej, a także życia społecznego od tych systemów, niezbędne jest w skali państwa spójne podejście do zapewnienia bezpieczeństwa systemów teleinformatycznych i informacji. Podstawą wszelkich działań powinna być wiedza o tym, czy w danym momencie czasu polskie systemy teleinformatyczne poddawane są atakom oraz jaka jest istota i skala tych ataków.

Opracowany w UE projekt dyrektywy w sprawie środków mających na celu zapewnienie wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji w obrębie Unii (dyrektywa NIS), nad którą prace najprawdopodobniej zakończą się w połowie roku 2016 - kładzie silny akcent na obszar cyberbezpieczeństwa. Nie czekając jednak na wdrożenie tej dyrektywy niezbędne jest zbudowanie minimalnych warunków ochrony cyberprzestrzeni poprzez:

- powołanie w administracji państwowej zespołów reagowania na incydenty komputerowe,
- powołanie w MC Ośrodka Koordynacji Działań związanych z ochroną cyberprzestrzeni zgodnie z zaleceniem NIK do czasu wdrożenia docelowych struktur,
- uzupełnienie Krajowego Planu Zarządzania Kryzysowego o zagrożenia związane z cyberbezpieczeństwem, jak również
- opracowanie i wdrożenie Strategii Ochrony Cyberprzestrzeni Państwa.

Zależność życia społecznego od cyberprzestrzeni będzie stale rosła, tak więc ochrona cyberprzestrzeni przekłada się bezpośrednio na funkcjonowanie państwa i życie codzienne obywateli.

2. Analiza stanu obecnego

2.1. Aktualny stan prawny

W Polce brak jest jednolitego ustawodawstwa regulującego instytucjonalno-prawny system ochrony cyberprzestrzeni. W Polsce funkcjonują jedynie przepisy regulujące jednostkowe, wybrane kwestie bezpieczeństwa teleinformatycznego (szczegółowy wykaz ustaw i dokumentów strategicznych znajduje się w załączniku nr 1). Tak więc jest to jedna z najpilniejszych rzeczy, które należy uporządkować i usystematyzować.

2.2. Aktualny stan organizacyjny

Funkcjonujący w Polsce system ochrony cyberprzestrzeni ma charakter rozproszony, polegający na wzajemnym współdziałaniu odpowiedzialnych podmiotów, zarówno w sferze cywilnej, wojskowej oraz tej związanej z cyberprzestępczością.

Aktualnie w Polsce brak jest jednoznacznych procedur oraz określonych poziomów reakcji na zagrożenia zidentyfikowane w sieciach teleinformatycznych. Kompetencje związane z bezpieczeństwem cyberprzestrzeni dzielone są m.in. pomiędzy Ministerstwo Obrony Narodowej, Rządowe Centrum Bezpieczeństwa, Ministerstwo Cyfryzacji, jak również Radę Ministrów, Agencję Bezpieczeństwa Wewnętrznego, Komendę Główną Policji, Ministerstwo Sprawiedliwości, Urząd Komunikacji Elektronicznej, a także przez CERT Polska znajdujący się w strukturze Naukowej i Akademickiej Sieci Komputerowej (NASK). Ponadto, w Polsce funkcjonują publiczne i prywatne zespoły ds. reagowania na incydenty komputerowe (CERT), obejmujące swoim zakresem m.in. administrację rządową, wojskową oraz Policję, a także zespoły utworzone przez operatorów telekomunikacyjnych oraz środowiska naukowo-badawcze. Warto zauważyć, że podmioty uczestniczące w procesie nie mają jasno określonych progów reakcji.

Prowadzone obecnie ćwiczenia i testy mają charakter wyspowy, niezorganizowany. Podmioty wykorzystują doświadczenia zagraniczne oraz różne, często nieskoordynowane ze sobą inicjatywy krajowe. Niezmiernie ważne jest opracowanie wydajnego systemu szkoleń, prowadzenie ewidencji osób przeszkolonych oraz właściwy system oceny szkoleń. Są to warunki niezbędne do właściwego funkcjonowania systemu.

Oddzielną kwestią jest szacowanie ryzyk, które właściwie nie funkcjonuje. Ryzyka szacowane są zazwyczaj na poziomie instytucji/resortów. Brak jest wydajnego systemu oceny tych ryzyk, a co za tym idzie brak prac badawczo-rozwojowych w celu zminimalizowania ryzyk. Dlatego konieczne jest opracowanie spójnego systemu szacowania ryzyk i wypracowanie właściwych kierunków prac badawczo-rozwojowych. Badania te mogłyby w przyszłości stać się także polską specjalnością z uwagi na polski kadrowy potencjał informatyczny.

Nie prowadzono również analizy architektury sieci pod kątem minimalizowania zagrożeń dla bezpieczeństwa danych i rejestrów.

Faktycznie, do tej pory działania podmiotów państwowych związane z ochroną cyberprzestrzeni były prowadzone w sposób rozproszony i bez spójnej wizji systemowej[2].

[2] NIK: Informacja o wynikach kontroli Informacja o wynikach kontroli: Realizacja przez podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni RP, 2015.

Kluczowym czynnikiem paraliżującym aktywność państwa w tym zakresie był brak jednego ośrodka decyzyjnego, koordynującego działania innych instytucji publicznych. Co szczegółowo opisano w Informacji o wynikach kontroli NIK.

Dopiero ostatnia zmiana Ustawy o działach administracji rządowej[3] dodała do działu informatyzacja sprawy z zakresu bezpieczeństwa cyberprzestrzeni, tym samym przypisując Ministrowi Cyfryzacji obowiązki koordynatora systemu.

2.3. Aktualny podział kompetencji głównych podmiotów

- **Ministerstwo Cyfryzacji** odgrywa kluczową rolę w procesach związanych z ochroną cyberprzestrzeni. Jest strategiczno-politycznym koordynatorem systemu ochrony cyberprzestrzeni RP. We współpracy z ABW opracowało w roku 2013 *Politykę Ochrony Cyberprzestrzeni RP*[4].
- **Agencja Bezpieczeństwa Wewnętrznego** rozpoznaje, zapobiega i zwalcza zagrożenia godzące w bezpieczeństwo wewnętrzne państwa. W ABW funkcjonuje m.in. Departament Bezpieczeństwa Teleinformatycznego, w ramach którego funkcjonuje Rządowy Zespół Reagowania na Incydenty Komputerowe: CERT.GOV.PL.
- **Ministerstwo Spraw Wewnętrznych i Administracji** nadzoruje działania Policji, w zakresie zwalczania cyberprzestępczości.
- **Policja** zajmuje się zwalczaniem cyberprzestępczości. W strukturach Policji funkcjonuje POL-CERT.
- **Ministerstwo Obrony Narodowej** jest odpowiedzialne za wojskową sferę ochrony cyberprzestrzeni RP. W ramach MON funkcjonuje, działający na potrzeby resortu MIL-CERT oraz Narodowe Centrum Kryptologii (NCK).
- **Urząd Komunikacji Elektronicznej** pełni rolę regulatora rynku telekomunikacyjnego i pocztowego, w kontekście bezpieczeństwa w cyberprzestrzeni zapewnia implementację Prawa telekomunikacyjnego.
- **Rządowe Centrum Bezpieczeństwa** pełni wiodącą rolę w obszarze zarządzania kryzysowego i ochrony infrastruktury krytycznej, przygotowuje *Narodowy Program Ochrony Infrastruktury Krytycznej*, a także *Krajowy Plan Zarządzania Kryzysowego oraz Raport o zagrożeniach Bezpieczeństwa Narodowego*. W centrum znajduje się 24 – godzinna służba dyżurna odpowiedzialna za przekazywanie informacji o zagrożeniach z zakresu zarządzania kryzysowego.
- **Ministerstwo Sprawiedliwości** kreuje prawo w zakresie cyberprzestępczości i nadzoruje jego właściwe wykonanie.
- **Ministerstwo Finansów,** odpowiada za kwestie budżetowe, w tym za sprawy związane z cyberbezpieczeństwem.

[3] Ustawa z dnia 22 grudnia 2015r. o zmianie ustawy o działach administracji rządowej oraz niektórych innych ustaw (Dz. U. 2015 poz. 2281).

[4] Uchwała Nr 111/2013 Rady Ministrów z dnia 25 czerwca 2013 roku w sprawie Polityki Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej (nie publikowana)

- **Biuro Bezpieczeństwa Narodowego** jest organem doradczym Prezydenta RP. Opracowało *Doktrynę Cyberbezpieczeństwa Rzeczypospolitej Polskiej.*
- **Naukowa i Akademicka Sieć Komputerowa** jest instytutem badawczym nadzorowanym przez Ministerstwo Cyfryzacji. W ramach NASK funkcjonuje zespół CERT.POLSKA, który pełni *de facto* rolę CERT/CSIRT [5]krajowego.

2.4. Podsumowanie

Żeby zadbać o cyberbezpieczeństwo należy jak najszybciej podjąć spójne i systemowe działania, mające na celu monitorowanie i przeciwdziałanie zagrożeniom występującym w cyberprzestrzeni oraz minimalizowanie skutków incydentów. Musimy skoordynować wszystkie podejmowane dobre inicjatywy, aby wyeliminować ich „wyspowy" charakter. Należy wdrożyć odpowiednie mechanizmy, w tym mechanizmy współpracy podmiotów prywatnych i państwowych (model oparty na współpracy administracji, biznesu i nauki) oraz odpowiedniego finansowania działań związanych z bezpieczeństwem IT. Niezbędne jest określenie systemu finansowania zadań związanych z ochroną cyberprzestrzeni. I najważniejsze: **warunkami efektywnej ochrony cyberprzestrzeni jest przyjęcie ram prawnych krajowego systemu ochrony cyberprzestrzeni oraz wyznaczenie krajowego organu koordynującego działania innych podmiotów w zakresie ochrony cyberprzestrzeni.**

Pilne i niezbędne jest wdrożenie spójnego podziału kompetencji z zakresu obowiązków, procedur oraz szkoleń, treningów i kierunków prac badawczo-rozwojowych.

3. Główne założenia budowy systemu ochrony cyberprzestrzeni RP

Problematyka bezpieczeństwa cyberprzestrzeni powinna być traktowana jako jeden ze strategicznych priorytetów Rzeczpospolitej Polskiej. Ważne jest właściwe zaadresowanie ambicji Polski w cyberprzestrzeni, przy równoczesnym zachowaniu równowagi pomiędzy celami, jakie wyznacza sobie rząd, a dostępnymi zasobami.

Dotąd cyberbezpieczeństwo w Polsce było raczej domeną wąskiej grupy specjalistów IT i sektora prywatnego. Brakowało spójnego, strategicznego podejścia do tego zagadnienia i wyraźniej, umocowanej prawnie koordynacji strategiczno – politycznej.

Przede wszystkim każdy element krajowego systemu teleinformatycznego musi być zaangażowany w proces reagowania na zagrożenia w cyberprzestrzeni.

Co za tym idzie konieczne jest:

1) wypracowanie konkretnych struktur organizacyjnych odpowiedzialnych za obsługę incydentów
2) utworzenie efektywnego system wczesnego ostrzegania, obejmującego wszystkie międzynarodowe i międzyoperatorskie punkty wymiany Internetu
3) stworzenie wielopoziomowych procedur reagowania na incydenty, spójne z już istniejącymi procedurami z zakresu zarządzania kryzysowego. W tym celu konieczne będzie jasne określenie procedur i progów reakcji, zgodnie z następującą hierarchią zagrożeń:
   – KATEGORIA 1: Ograniczenie lub zaprzestanie realizacji istotnych funkcji państwa w sektorach kluczowych (sektor energetyczny, sektor transportowy, sektor

[5] CERT (Computer Emergency Response Team) jest nazwą zastrzeżoną przez Carnegie Mellon University i jej używanie wymaga zgody tego uniwersytetu. Taką zgodę posiada CERT Polska. Projekt dyrektywy NIS posługuje się nazwą CSIRT (Computer Security Incident Response Team).

bankowy, sektor finansowy, sektor zdrowia, produkcja i dystrybucja wody pitnej, sektor telekomunikacyjny, infrastruktury cyfrowej);
- KATEGORIA 2: Kradzież istotnych danych (np. państwowych, bankowych, osobowych);
- KATEGORIA 3: Nieautoryzowany dostęp serwisowy do systemu teleinformatycznego;
- KATEGORIA 4: Zmiana (podmiana) informacji w oficjalnych rejestrach i serwisach (państwowych, bankowych, samorządowych);
- KATEGORIA 5: Utrudnienie dostępu do serwisów i usług.

W celu zapewnienia właściwego działania procedur konieczne będzie wypracowanie zarówno horyzontalnych jak i wertykalnych kanałów wymiany informacji o incydentach.

Ministerstwo Cyfryzacji będzie pełniło rolę organizatora systemu cyberprzestrzeni. Oznacza to, że będzie nadzorowało tworzenie struktur i wpływało na zakresy kompetencji poszczególnych podmiotów zaangażowanych w proces ochrony cyberprzestrzeni. Ponadto, Ministerstwo będzie prowadziło ewidencję pełnomocników bezpieczeństwa cyberprzestrzeni i ekspertów z zakresu cyberbezpieczeństwa. Ważnym elementem działalności będzie także kształtowanie procesów szkoleniowych, nadzorowanie ćwiczeń i testów z zakresu cyberbezpieczeństwa oraz wyznaczanie kierunków prac badawczo – rozwojowych, tak aby budować potencjał intelektualny i technologiczny.

Konieczne jest wprowadzenie nieustannego procesu oceny ryzyka. Ocena ryzyka w cyberprzestrzeni powinna być prowadzona w taki sposób, aby jej wyniki można było inkorporować do dokumentów diagnozujących bezpieczeństwo Rzeczypospolitej np. do *Raportu o zagrożeniach bezpieczeństwa narodowego*.

Administracja publiczna ma ograniczone siły i środki finansowe, które mogą okazać się niewystarczające w przypadku najbardziej złożonych zagrożeń i problemów. W związku z tym konieczne jest zbudowanie „ostatniej linii obrony”[6] przed cyberzagrożeniami w oparciu o sektor prywatny. Stworzony zostanie mechanizm umów z producentami oprogramowania i wyspecjalizowanymi ośrodkami naukowymi, który będzie pozwalał na skorzystanie z ich wiedzy i umiejętności. Planuje się reorganizację architektury systemu teletransmisyjnego dla kluczowych serwisów państwowych i administracji państwowej i służb zespolonych.

Wszystkie elementy koncepcji zostaną ujęte w ramy prawne tzn. ujęte w aktach prawnych i regulacjach niższego rzędu, dając podstawę i sankcjonując wypracowane rozwiązania. Konieczne jest także ujęcie w budżecie środków finansowych na właściwe zaadresowanie potrzeby obszaru cyberbezpieczeństwa.

3.1. Podział kompetencji i struktura systemu

Wobec kończących się właśnie na forum Unii Europejskiej prac nad *Dyrektywą w sprawie środków mających na celu zapewnienie wspólnego poziomu bezpieczeństwa sieci i informacji w obrębie Unii*, oraz wobec zdiagnozowanych już potrzeb i ambicji RP w cyberprzestrzeni proponuje się następujące rozwiązania w zakresie budowy systemu cyberbezpieczeństwa RP.

- **Utworzenie trzypoziomowej struktury systemu cyberbezpieczeństwa, gdzie odpowiednie instytucje, komórki organizacyjne czy zespoły odpowiadałyby za**

[6] „ostatnia linia obrony” oznacza siły i środki, po których wyczerpaniu ustaje zdolność do odpierania ataku

bezpieczeństwo cyberprzestrzeni w warstwie strategicznej, operacyjnej i technicznej.

Poziom strategiczny	Instytucje odpowiedzialne za wyznaczanie kierunków strategicznych i tworzenie podstaw prawnych oraz standardów funkcjonowania całego systemu cyberbezpieczeństwa
Poziom operacyjny	Instytucje odpowiedzialne za przekazywanie informacji o incydentach transsektorowych oraz agregowanie i analizę informacji o tego typu incydentach.
Poziom techniczny	Instytucje odpowiedzialne za bezpośrednie reagowanie na incydenty w poszczególnych instytucjach (zarówno państwowych, jak i prywatnych)

- **W efekcie powstanie wielopoziomowa struktura reagowania na incydenty, z jasno określonymi kompetencjami, strukturą adekwatną do zagrożeń i czytelnymi procedurami reagowania.[7]**

POZIOM STRATEGICZNO-POLITYCZNY	
Organ właściwy ds. bezpieczeństwa sieci i informacji	Organ ten będzie nadzorował wdrażanie strategii cyberbezpieczeństwa RP i wyznaczał kierunkowe działania dla innych podmiotów zaangażowanych w proces ochrony cyberprzestrzeni. Będzie także tworzył rozwiązania legislacyjne, niezbędne do właściwego funkcjonowania sytemu cyberbezpieczeństwa w Polsce. Oprócz tego, będzie odpowiedzialny za monitorowanie wdrażania dyrektywy NIS na obszarze Rzeczypospolitej Polskiej i negocjowanie aktów delegowanych do tej dyrektywy, a także prowadzenie współpracy międzynarodowej i kreowanie polityki międzynarodowej w dziedzinie cyberbezpieczeństwa. Jest to niezwykle istotne, ponieważ wiele cyberzagrożeń nie ma charakteru narodowego. Instytucja ta będzie ściśle współpracować z już istniejącymi instytucjami, odpowiedzialnymi szerzej za bezpieczeństwo RP, a więc z Biurem Bezpieczeństwa Narodowego oraz Rządowym Centrum Bezpieczeństwa.
POZIOM OPERACYJNY	
Pojedynczy Punkt Kontaktowy(PPK)	Zadaniem Pojedynczego Punktu Kontaktowego będzie agregowanie informacji na temat incydentów w skali całego kraju i kontakt z analogicznymi instytucjami w innych krajach członkowskich w celu wymiany informacji na temat transnarodowych incydentów. Ponieważ będą to informacje

[7]Konieczne jest także nadanie większych kompetencji i przyznanie dodatkowych funduszy na realizacje nowych celów, już istniejącym w Polsce instytucjom.

	o zagrożeniach wysokopoziomowych, wskazane byłoby silne umocowanie takiego organu, tak aby mógł z łatwością uzyskiwać informację od wszystkich krajowych CERT/CSIRT.
Punkt Kontaktowy dla operatorów Infrastruktury Krytycznej **(PKIK)**	Wobec istotności usług, jakie świadczą operatorzy infrastruktury krytycznej oraz z uwagi na zapewnienie tego typu operatorom, wyższego poziomu bezpieczeństwa, niż pozostałym interesariuszom systemu cyberbezpieczeństwa, stworzony zostanie punkt kontaktowy dla operatorów IK. Będzie to instytucja działająca ponad CERT/CSIRT sektorowymi, ułatwiająca przepływ informacji o incydentach pomiędzy operatorami IK. Instytucja ta powinna znajdować się w sferze cywilnej, niemniej jednak powinna ściśle współpracować ze służbami specjalnymi.
Narodowe Centrum Cyberbezpieczeństwa (Centrum Kompetencyjne)	Instytucja odpowiedzialna za przygotowywanie rekomendacji w dziedzinie cyberbezpieczeństwa oraz merytoryczne wsparcie dla wszystkich instytucjonalnych członków systemu, a także zaawansowaną analizę najbardziej złożonych incydentów. Z analizy interesariuszy jasno wynika, że z uwagi na konieczność kontaktowania się z sektorem prywatnym, przede wszystkim z operatorami infrastruktury krytycznej, instytucja taka powinna znajdować się poza służbami specjalnymi.
CERT/CSIRT Narodowy	CERT/CSIRT pełniący rolę „ostatniej szansy" – partner dla CERT/CSIRT sektorowych w rozwiązywaniu najbardziej złożonych incydentów, zapewniający wsparcie analityczne. Instytucja ta będzie miała kompetencje bezpośredniego kierowania realizacją przedsięwzięć z zakresu ochrony cyberprzestrzeni RP. Jednocześnie będzie odpowiadać za krajowy system wczesnego ostrzegania. **Funkcja CSIRT/CERT narodowego powinna być połączona z funkcją Pojedynczego Punktu Kontaktowego, a także z funkcją Narodowego Centrum Cyberbezpieczeństwa– Centrum Kompetencyjnego**.
CERT/CSIRT sektorowe	CERT/CSIRT sektorowe będą odpowiedzialne za obsługę incydentów w poszczególnych sektorach, wspomagając tym samym SOC i Lokalne Zespoły Reagowania na Incydenty Komputerowe w poszczególnych instytucjach. Z uwagi na złożoność procesu tworzenia takich CERT/CSIRT, wskazane jest w pierwszej kolejności tworzenie Centrum Analiz i Dzielenia się Informacjami (ang. Information Sharing and Analysis Center – ISAC[8]). Mogłyby stać się one podstawą systemu cyberbezpieczeństwa w Polsce i stanowić etap poprzedzający

[8] Mechanizm zaproponowany w Stanach Zjednoczonych, mający na celu wspomożenie sektora prywatnego w dziedzinie cyberbezpieczeństwa. ISAC to budowane wokół określonych obszarów gospodarki (np. energetyka, instytucje finansowe) centra wymiany wiedzy dotyczącej zagrożeń sektorowych oraz wymiany dobrych praktyk w zakresie podnoszenia bezpieczeństwa teleinformatycznego. Centra ISAC działają jako instytucje non-profit i służą jako mechanizm dwukierunkowej komunikacji z administracją państwową i innymi ISAC. Mogą przyjmować mniej lub bardziej formalny charakter, np. dysponować wspólnym rozwiązaniem informatycznym do wymiany wiedzy lub działać jako platforma do częstych spotkań ekspertów z danego środowiska. (źródło: *System bezpieczeństwa cyberprzestrzeni RP, Ekspertyza dotycząca rekomendowanego modelu organizacji systemu bezpieczeństwa cyberprzestrzeni w Polsce, wykonana na zlecenie Ministerstwa Administracji i Cyfryzacji*)

	utworzenie sektorowych CERT/CSIRT, wspierających sektory kluczowe w wymianie informacji na temat incydentów oraz reakcji na te incydenty. CERT/CSIRT sektorowe powinny powstać w następujących sektorach: • Sektor energetyczny (m.in. energia elektryczna, ropa naftowa, gaz), • Sektor transportowy (lotniczy, kolejowy, morski), • Sektor bankowy (m.in. instytucje kredytowe), • Sektor finansowy (m.in. giełda), • Sektor zdrowia (m.in. podmioty świadczące opiekę zdrowotną, w tym szpitale), • Sektor zaopatrzenia w wodę, • Sektor telekomunikacyjny, wtymm.in. punkty wymiany ruchu internetowego, dostawcy usług systemu nazw domen oraz rejestry nazw domen najwyższego poziomu
CERT/CSIRT dla administracji rządowej	CERT/CSIRT zapewniający wsparcie SOC/LZR (patrz: Poziom techniczny, tabela niżej) utworzonym w poszczególnych urzędach oraz zapewniający bezpieczeństwo dla instytucji rządowych i urzędów centralnych. CERT/CSIRT ten będzie specjalnym rodzajem CERT/CSIRT sektorowego.

POZIOM TECHNICZNY	
Operacyjne Centra Bezpieczeństwa (ang.: SOC)[9]	Zapewniające bezpieczeństwo w instytucjach, organizacjach i firmach o dużym znaczeniu politycznym, administracyjnym czy gospodarczym i skali przekraczającej kompetencje Lokalnych Zespołów Reagowania (LZR)
Poziom użytkownika	Pełnomocnicy ochrony cyberprzestrzeni i Lokalne Zespoły Reagowania bezpośrednio obsługujące lokalne systemy oraz pracowników w instytucjach publicznych i firmach prywatnych.

[9] SOC(ang. Security Operations Center). To centra monitorujące stan bezpieczeństwa infrastruktury informatycznej i reagujące na pojawiające się incydenty i zagrożenia, w zależności od konkretnych uwarunkowań, zaliczone mogą być do poziomu technicznego albo do poziomu operacyjnego

3.2. System wczesnego ostrzegania i reagowania

3.2.1. Uwarunkowania

Powstały w pierwszych latach 70 ubiegłego wieku wirus komputerowy stworzony został bez złych intencji i był swego rodzaju żartem jego twórcy. Niestety dość szybko stało się jasne, że wirusy komputerowe, a mając na uwadze dzisiejszy stan wiedzy w tym zakresie – oprogramowanie złośliwe, mogą stanowić narzędzie służące działaniom o charakterze destrukcyjnym lub szpiegowskim. Oprogramowanie takie może zostać umieszczone w systemie teleinformatycznym ofiary ataku bezpośrednio z sieci wchodzącej w skład cyberprzestrzeni, jak i pośrednio przez wymienne nośniki informacji zainfekowane tego rodzaju oprogramowaniem. Szczególnym przypadkiem umieszczenia oprogramowania złośliwego w systemie teleinformatycznym jest działanie z zakresu inżynierii społecznej prowadzące do tego, że legalny użytkownik systemu sam nieświadomie umieszcza oprogramowanie złośliwe w systemie lub przyznaje napastnikowi uprawnienia do takiego działania albo do działania w systemie w swoim imieniu. Kolejnym rodzajem zagrożeń pochodzących z cyberprzestrzeni są działania napastnika polegające na wykorzystaniu błędów w oprogramowaniu systemu teleinformatycznego i w ten sposób uzyskanie uprawnień do nieograniczonych działań w systemie. Na koniec należy zwrócić uwagę na zagrożenie dla systemów teleinformatycznych wykorzystujących zdalny dostęp wynikające ze złego zaprojektowania mechanizmu uwierzytelniania i autoryzacji lub złego eksploatowaniu takiego mechanizmu (np. trywialne hasła), co może umożliwić atakującemu działanie w systemie, tak jak legalnemu użytkownikowi. Szczególne ryzyko o takim charakterze związane jest ze zdalnym utrzymywaniem i serwisowaniem systemów.

Podstawą skutecznego zwalczania cyberataku powinien być łańcuch następujących działań:

- wykryj atak lub sprawdź czy jest informacja o możliwości ataku, dystrybuowana w systemie powiadamiania, która może dotyczyć Twojego systemu,
- reaguj jeśli możesz, a jeśli nie potrafisz, to zwróć się o pomoc do z góry określonego podmiotu realizującego wsparcie,
- przekaż informację o ataku na Twój system w systemie powiadamiania,
- oceń skutki ataku,
- opracuj plan naprawczy,
- usuń problem,
- poinformuj o przywróceniu stanu wyjściowego.

3.2.2. Wykrywanie i reagowanie

Wykrywanie rozwijającego się ataku lub odbieranie informacji o możliwości ataku z systemu powiadamiania powinno być kompetencją wyspecjalizowanej komórki organizacyjnej podmiotu, w którym eksploatowany jest system teleinformatyczny. Komórka taka powinna mieć charakter operacyjnego centrum bezpieczeństwa (ang. Security Operation Center - SOC) lub, w przypadku mniejszych organizacji, lokalnego zespołu reagowania (LZR). SOC lub LZR powinny być wyposażone w zasoby umożliwiające ich efektywne funkcjonowanie. Na zasoby te składać się powinny:

- kompetentny personel,
- środki techniczne (w tym rezerwowe środki łączności),

- procedury.

Organizator krajowego systemu cyberbezpieczeństwa powinien zapewnić standaryzacje tych środków, w szczególności w zakresie wymagań dla kwalifikacji personelu oraz stosowanych procedur.

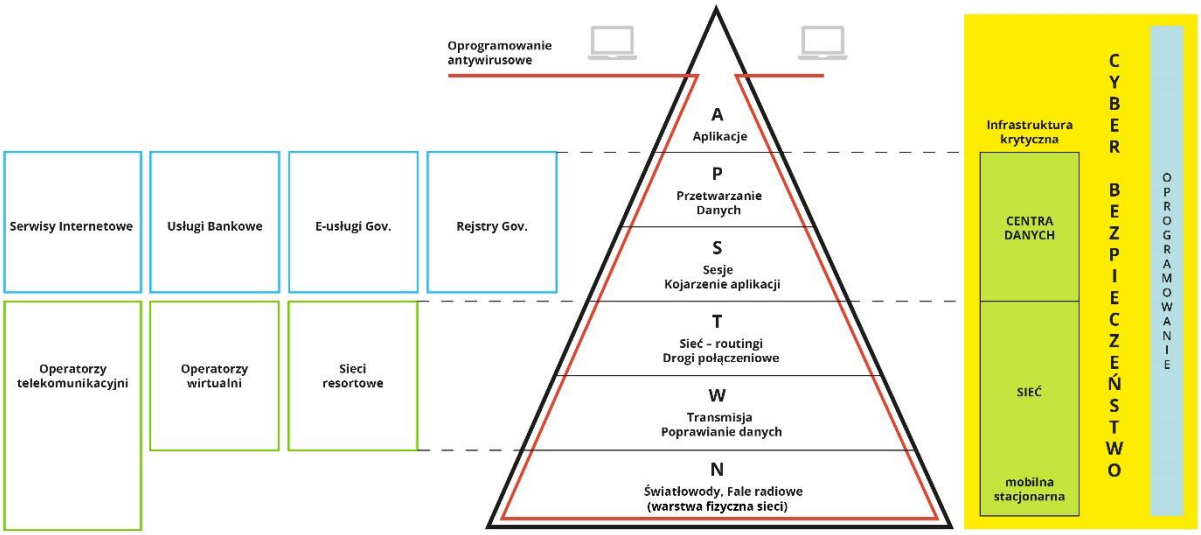
Wykryty atak powinien być zablokowany przez SOC lub LZR, najlepiej jeszcze przed tym jak wyrządzi szkody dla organizacji. W przypadku gdy atak już się powiódł, SOC powinno oszacować jego skutki i rekomendować postępowanie z tymi skutkami. W zależności od skali skomplikowania problemu SOC powinno mieć możliwość skorzystania ze wsparcia Narodowego lub Sektorowego Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego CERT/CSIRT). Krajowa sieć CERT/CSIRT powinna posiadać strukturę hierarchiczną, z warstwą sektorową, warstwą operatorów zapewniających dostęp do Internetu (Internet Service Provider – ISP) oraz CERT/CSIRT narodowym, który powinien posiadać zdolność do komunikowania się na poziomie międzynarodowym(UE, NATO, OECD, ONZ). Szczególną rolę na poziomie CERT/CSIRT Sektorowych odgrywać powinny CERT.GOV.PL i MIL-CERT, każdy w ramach swoich z góry określonych kompetencji.

W krytycznych przypadkach, jeżeli SOC lub LZR nie ma możliwości bezpośredniego oddziaływania na źródło ataku, w szczególności jeżeli jest ono położone poza obszarem jego odpowiedzialności, SOC lub LZR musi być wyposażone w kompetencję pozwalającą na izolowanie systemu lub jego części od cyberprzestrzeni – szczegółowy sposób postępowania należy określić w procedurach postępowania.

W sytuacji gdy atak dotyczy nie pojedynczego podmiotu, ale odnosi się do całego sektora gospodarki narodowej lub części terytorium RP, muszą istnieć mechanizmy izolowania takiego sektora lub terytorium. Należy przy tym zauważyć, że pojęcie „terytorium" nie zawsze należy rozumieć w sensie słownikowym, albowiem w cyberprzestrzeni nie zawsze jest ono adekwatne i może na przykład oznaczać segment sieci, w tym całą sieć konkretnego operatora.

W procesie wykrywania ataków i reagowania na nie, należy uwzględnić wszystkie warstwy modelu sieciowego OSI[10]. Każde wykorzystanie sieci teleinformatycznej lub skorzystanie z usług dostępnych w sieci wiąże się z wykorzystaniem wszystkich warstw modelu OSI, dlatego cyberbezpieczeństwo należy postrzegać jako sumę bezpieczeństwa poszczególnych poziomów modelu OSI. Część modelu określająca warstwę fizyczną sieci, obwody połączeniowe i stacje teletransmisyjne pomimo tego, że posiada elementy oprogramowania podatne na zagrożenia cybernetyczne, jednak zaliczana jest głównie do infrastruktury krytycznej. W tych warstwach dominują operatorzy telekomunikacyjni, wirtualni operatorzy telekomunikacyjni i operatorzy resortowi. Warstwy górne to głównie rejestry państwowe, e-usługi i serwisy internetowe. Na szczycie modelu OSI znajdują się najbardziej podatne na zagrożenia aplikacje i oprogramowanie indywidualnych użytkowników. Choć wszystkie warstwy są jednakowo istotne, jednak najsłabszym ogniwem wydają się najwyższe warstwy i to one w dużej mierze decydują o bezpieczeństwie całego systemu.

[10] ISO OSI Reference Model - standard zdefiniowany przez ISO oraz ITU-T opisujący strukturę komunikacji sieciowej

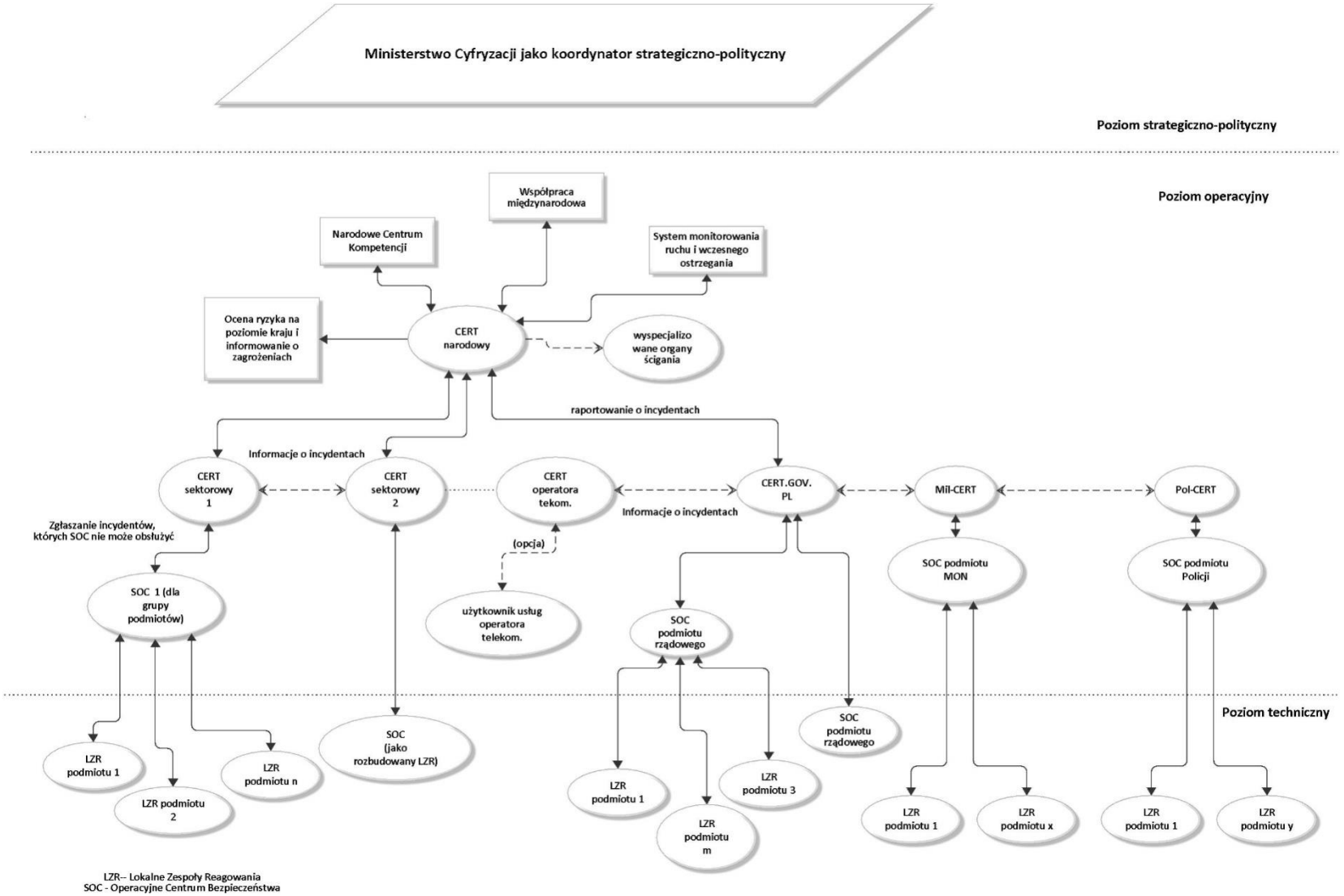


Rysunek 1 Bezpieczeństwo w kontekście modelu sieciowego OSI

Ważnym problemem, wymagającym rozwiązania, jest wyznaczenie progów, od przekroczenia których następuje reagowanie określonego komponentu systemu cyberbezpieczeństwa. Należy również określić jakiego rodzaju incydenty podlegają notyfikacji na wyższy poziom hierarchii systemu zapewnienia cyberbezpieczeństwa.

3.2.3. Ostrzeganie i informowanie

System ostrzegania i informowania powinien składać się z dwóch komponentów. Pierwszym z nich powinien być podsystem zbierania informacji o zaistniałych incydentach bezpieczeństwa przez ogniwo danego poziomu hierarchii w systemie cyberbezpieczeństwa od współpracujących ogniw poziomu niższego, agregowania tych informacji i ich oceniania pod kątem ryzyk jakie raportowane incydenty stwarzają dla bezpieczeństwa cyberprzestrzeni. Ostrzeżenia o trwających lub mogących nastąpić atakach powinny być komunikowane w dół hierarchii, w taki sposób aby skutecznie docierała do ogniw wykonawczych jakimi są SOC. Z drugiej strony zagregowane informacje, po przekroczeniu określonego poziomu powinny być przekazywane na kolejny poziom hierarchii do CERT/CSIRT narodowego, łącznie.

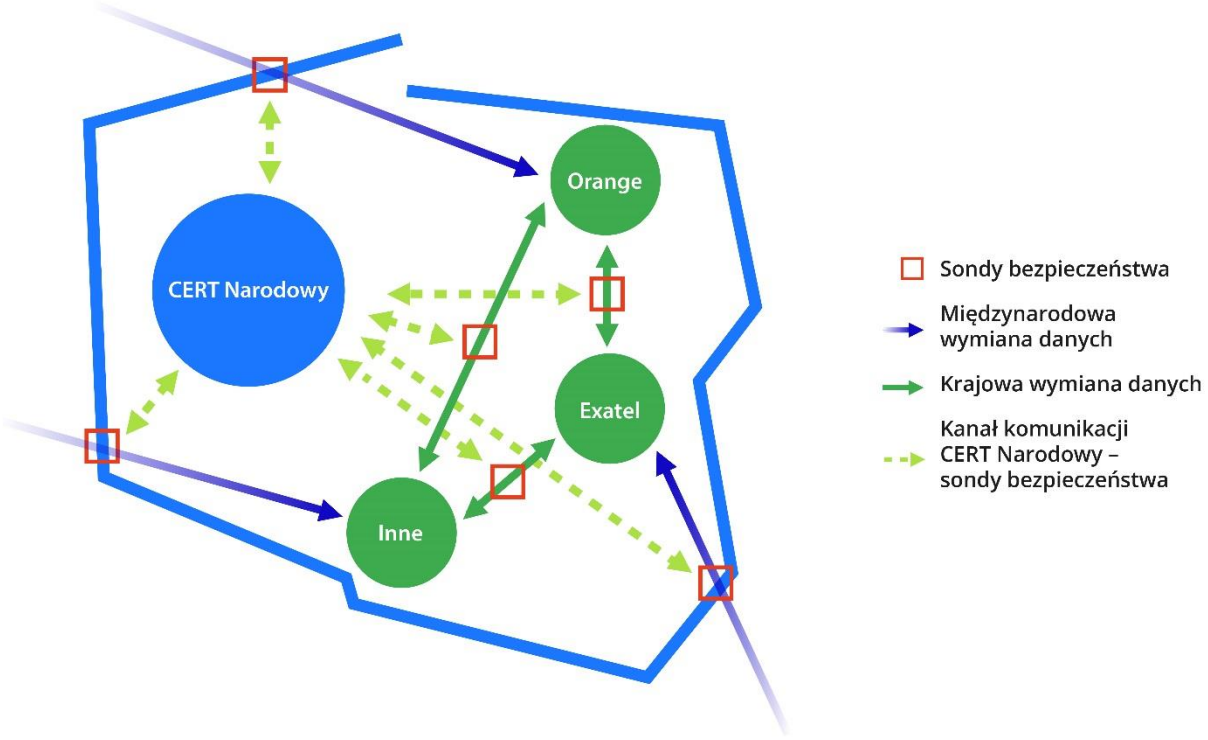


Rysunek 2Proponowana struktura krajowego systemu cyberbezpieczeństwa

Jednocześnie należy zapewnić na poziomie wykonawczym dostęp do wiarygodnej informacji o wykrytych podatnościach w urządzeniach i oprogramowaniu, tak komunikowanych przez wytwórców, jak i ośrodki niezależne, a także o sposobach postępowania z takimi podatnościami. Mówiąc o wiarygodności należy mieć na uwadze fałszywe zgłoszenia o podatnościach, a w szczególności o sposobach usuwania takich podatności, które mogą być w istocie formami ataku (np. tzw. fakeAV).

Drugim komponentem systemu ostrzegania i informowania powinien być system monitorowania ruchu w punktach wymiany ruchu internetowego (*Internet Exchange Point* – IXP -Rysunek. 3) Przy czym pod pojęciem IXP należy rozumieć zarówno punkt wymiany pomiędzy operatorami krajowymi jak i punkty wymiany z operatorami zagranicznym. W IXP powinno następować monitorowanie ruchu w poszukiwaniu anomalii, które mogą być symptomem rozwijającego się rozległego ataku. Jednakże mimo tego, że powyższy postulat wydaje się być racjonalny, jego realizacja nie jest prosta. Po pierwsze zidentyfikowaniu muszą podlegać wszystkie wspomniane punkty wymiany, a w szczególności punkty wymiany z operatorami zagranicznymi. Jednakże mimo dochowania niezbędnej staranności może okazać się, że w krajowej sieci pojawią się punkty wymiany realizowane *ad hoc*, np. z wykorzystaniem łącza satelitarnego. Kolejną trudnością związaną z realizacją monitorowania ruchu sieciowego w punktach wymiany jest wolumen wymienianego ruchu. Monitorowanie nie może prowadzić do obniżenia przepustowości punktu wymiany, a zatem wymagać to będzie zastosowania urządzeń o bardzo dużej mocy obliczeniowej. Odrębnym zagadnieniem jest ustanowienie kryteriów, według których identyfikowane byłyby zjawiska występujące w punkcie wymiany, kwalifikujące je do anomalii stanowiącej zagrożenie dla użytkowników sieci krajowej. Wykrycie anomalii może być podstawą do decyzji o izolowaniu sieci generującej taką anomalię.

CERT/CSIRT narodowy powinien posiadać możliwość umieszczania własnych sond w IXP lub korzystania z narzędzi stosowanych przez operatora.



Rysunek 3 Monitorowanie ruchu internetowego

SOC/LZR będą realizowały swoje zadania w sposób efektywny jedynie w sytuacji, gdy będą dysponować pełną wiedzą o aktualnych zagrożeniach, zarówno potencjalnych jak i o atakach będących w toku. Niezbędne jest zatem stworzenie działającego w czasie rzeczywistym systemu powiadamiania na poziomie Narodowego CERT/CSIRT. Z jednej strony system taki musi być w sposób efektywny zasilany informacyjnie, z drugiej zaś strony musi dystrybuować zweryfikowane i zagregowane informacje o zagrożeniach do komórek wykonawczych.

Zasilanie takiego systemu informacją musi odbywać się z każdego poziomu hierarchii krajowego systemu cyberbezpieczeństwa, w tym informacją pochodzącą z:

- operacyjnych centrów bezpieczeństwa podmiotów eksploatujących systemy teleinformatyczne,
- CERT/CSIRT sektorowych,
- własnych działań rozpoznawczych CERT/CSIRT Narodowego.

Dystrybucja informacji o aktualnej sytuacji powinna obejmować:

- komunikaty o wykrytych podatnościach w stosowanym oprogramowaniu systemowym i aplikacyjnym wraz z informacją o sposobach postępowania z tymi podatnościami,
- komunikaty o potencjalnych atakach oraz o atakach będących w toku wraz z informacją o środkach przeciwdziałania, ze szczególnym uwzględnieniem ataków prowadzonych środkami, które nie zostały jeszcze wzięte pod uwagę w automatycznych systemach obronnych typu AV, IPS i in.

3.3. Procedury, progi reakcji, kanały wymiany informacji

Mając na uwadze to, że w przypadku ataku na systemy teleinformatyczne o powodzeniu takiego ataku mogą decydować wręcz milisekundy, niezbędne jest zapewnienie automatyzacji reakcji obronnych. Jeżeli reakcja automatyczna okaże się zawodna, zwykle pozostaje już jedynie podjęcie działań mających na celu określenie strat, jakie zostały poniesione w wyniku takiego ataku oraz działań ograniczających zasięg tych strat (w tym strat wtórnych) i działań przywracających sprawność zaatakowanego systemu. Z uwagi na konieczność reakcji w czasie rzeczywistym, reakcje takie muszą następować według z góry ustalonych scenariuszy ujętych w stosowne procedury. Należy dążyć do tego, aby procedury reakcji zostały ustandaryzowane we wszystkich podmiotach danego poziomu hierarchii reagowania. Standaryzacji powinna polegać nie tylko treść procedury, ale również sposób jej oznaczania. Standaryzacja oznaczeń procedur pozwoli ułatwić sterowanie wyzwalaniem procedur przez jednostkę nadrzędną w hierarchii systemu reagowania wobec jednostek położonych na niższym poziomie hierarchii.

Wyzwolenie realizacji procedury powinno następować według jednoznacznie określonego kryterium. Wiąże się to z ustaleniem progów wyzwolenia, przy ustalaniu których należy wziąć pod uwagę istotność skutków, jakie powoduje lub może spowodować dany rodzaj ataku, w tym rozległość terytorialna, istotność dla życia i zdrowia obywateli, bezpieczeństwo środowiska, wpływ na gospodarkę narodową itp. W ustalaniu progów wyzwolenia mogą pojawić się trudności związane z „ciemną liczbą”[11] ataków. Dotyczy to w szczególności ataków na komputery osobiste i urządzenia mobilne pojedynczych obywateli lub podmiotów sektora MŚP. Konieczne jest zatem opracowanie metod szacowania wspomnianej „ciemnej liczby” ataków metodami statystycznymi, operującymi na próbce populacji.

Podstawą skutecznej reakcji na ataki jest istnienie niezawodnego systemu łączności pomiędzy ogniwami krajowego systemu cyberbezpieczeństwa, poprzez który z jednej strony mogą być zbierane informacje o prowadzonych atakach, a z drugiej strony rozsyłane polecenia określonych działań w odpowiedzi na zgłoszenia o atakach. Należy zauważyć, że w stanie normalnym jako elementy systemu łączności wykorzystywane są te komponenty, które w przypadku ataku mogą stać się jego celem, a zatem nie będzie możliwości wykorzystania tych środków łączności na potrzeby zarządzania incydentem, jakim jest atak. Należy zatem ustanowić alternatywny system łączności na potrzeby zarządzania incydentami w cyberprzestrzeni. Jednocześnie należy zauważyć, że żaden system nie zapewni bezwzględnego bezpieczeństwa i prędzej czy później wystąpić może sytuacja, w której zawiodą mechanizmy ochronne. W takich przypadkach na wszystkich poziomach zarządzania muszą być stworzone warunki do podjęcia pracy przez zespoły zarządzania kryzysowego.

3.4. Rola organizatora systemu

Rola ośrodka koordynacji działań związanych z ochroną cyberprzestrzeni RP oraz krajowego systemu reagowania na incydenty komputerowe będzie powierzona Ministerstwu Cyfryzacji. Została zmieniona ustawa o działach administracji rządowej, która przypisuje nowe zadania koordynacji bezpieczeństwa cyberprzestrzeni ministrowi właściwemu ds. informatyzacji[12]. Ponadto w nowym statucie Ministerstwa[13] został przewidziany Departament Cyberbezpieczeństwa, który będzie nadzorował specjalnie powołany do tego obszaru wiceminister.

[11] liczba skutecznych ataków, które nie zostały rozpoznane przez zaatakowanego
[12] Dz. U. z 2015 r., poz. 2281.
[13] M.P. z 2015 r., poz. 1290.

Na **poziomie strategicznym** rolą organizatora systemu będzie przygotowanie **krajowej strategii cyberbezpieczeństwa**, obejmującej administrację państwową i sektory rynkowe tj. energetykę, transport, bankowość i instytucje finansowe, sektory zdrowia, zaopatrzenia w wodę, infrastrukturę cyfrową i dostawców usług cyfrowych, co wynika z projektu dyrektywy NIS. Organizator systemu opracuje jeden dokument strategiczny, jednocześnie zostanie przeprowadzona ewaluacja i uspójnienia dotychczasowych dokumentów strategicznych odnoszących się do problematyki cyberbezpieczeństwa tj. *Polityki ochrony cyberprzestrzeni RP, Strategii bezpieczeństwa narodowego, Doktryny cyberbezpieczeństwa RP, Narodowego Program Ochrony Infrastruktury Krytycznej*. Strategia określi środki w zakresie gotowości, reagowania i przywracania stanu normalnego w zakresie bezpieczeństwa sieci i informacji, mechanizmy współpracy pomiędzy sektorami publicznym i prywatnym, a ponadto wskaże pożądany sposób przeprowadzania szacowania ryzyka dla wszystkich sektorów.

Ministerstwo Cyfryzacji będzie odpowiedzialne za tworzenie, konsultowanie i przedstawianie odpowiednich rozwiązań legislacyjnych pozwalających na funkcjonowanie całego systemu bezpieczeństwa cyberprzestrzeni. Będzie odpowiedzialne za przygotowywania projektów **aktów prawnych** (ustaw i rozporządzeń dotyczących ochrony cyberprzestrzeni) **o charakterze międzysektorowym**, a także harmonizacji z prawodawstwem Unii Europejskiej w tym obszarze. W oparciu o przyjęte akty prawne i Ministerstwo Cyfryzacji będzie pełnić role instytucjonalne i koordynacyjne odnośnie współpracy międzynarodowej przewidziane w projekcie dyrektywy NIS tj. rolę organu właściwego ds. bezpieczeństwa sieci i informacji i rolę pojedynczego punktu kontaktowego.

Organizator systemu będzie nadzorował tworzenie struktur bezpieczeństwa sieci i informacji w administracji publicznej i kluczowych sektorach gospodarki (np. CERT/CSIRT sektorowych), wpływał na zakresy kompetencji, ewidencjonował dane o pełnomocnikach i ekspertach z zakresu bezpieczeństwa teleinformatycznego z koordynowanych sektorów. Założeniem będzie tworzenie zespołów, które będą w stanie rozwiązywać problemy bezpieczeństwa teleinformatycznego na poziomie instytucji. Zespoły będą uczestniczyć w kompleksowym **programie szkoleń dotyczącym bezpieczeństwa teleinformatycznego**, a dodatkowo w ogólnokrajowych ćwiczeniach cybernetycznych, weryfikujących posiadane i nabyte kompetencje. Organizator systemu będzie stymulować powstawanie **partnerstw publiczno-prywatnych** w dziedzinie ochrony teleinformatycznej bądź ukierunkowanych na podniesienie bezpieczeństwa świadczonych usług (centra typu SOC, ISAC), które z racji kosztów nie są w Polsce powszechne.

Ministerstwo zapewni obsługę prac **Zespołu zadaniowego ds. bezpieczeństwa cyberprzestrzeni RP** w ramach KRMC[14], podejmującego decyzje dotyczące problemów systemowych (np. luk w systemie bezpieczeństwa cyberprzestrzeni), opracowujących wieloletnie programy działania i wydającego rekomendacje dla uczestników systemu. Organizator systemu we współpracy z Zespołem zadaniowym wypracuje propozycje koordynacji/eskalacji problemów dotyczących bezpieczeństwa cyberprzestrzeni na poziom organów decyzyjnych zajmujących się problematyką bezpieczeństwa narodowego i zarządzania kryzysowego (Rada Ministrów, Rządowe Centrum Bezpieczeństwa, Biuro Bezpieczeństwa Narodowego).

Wśród zadań horyzontalnych Ministerstwo Cyfryzacji - organizator systemu, we współpracy z Ministerstwem Nauki i Szkolnictwa Wyższego, Narodowym Centrum Badań i Rozwoju oraz Ministerstwem Edukacji Narodowej - zapewni odpowiednie warunki i ramy dla realizacji **programów krajowych w dziedzinie badań** oraz edukacji na temat bezpieczeństwa

[14]W ramach Komitetu Rady Ministrów ds. Cyfryzacji.

cyberprzestrzeni. Będą wspierane badania prowadzące do powstawania narzędzi, w tym narodowych, umożliwiających zaawansowane monitorowanie zagrożeń i skuteczna reakcję.

Na **poziomie operacyjnym** rolą organizatora systemu bezpieczeństwa cyberprzestrzeni, czyli Ministerstwa Cyfryzacji, będzie powołanie oficjalnego zespołu reagującego na zagrożenia i incydenty bezpieczeństwa w cyberprzestrzeni na poziomie krajowym – CERT/CSIRT krajowego oraz określenie kompetencji, zasad współpracy z uczestnikami systemu, w tym CERT/CSIRT sektorowymi, punktem kontaktowym dla operatorów Infrastruktury Krytycznej, centrami ISAC i zespołami ds. bezpieczeństwa. Minister Cyfryzacji zapewni funkcjonowanie krajowego systemu reagowania na incydenty komputerowe, będącego w stanie zarządzać aktualnymi zagrożeniami w cyberprzestrzeni. Z jednej strony zostaną wzmocnione, przewidziane *Polityką ochrony cyberprzestrzeni RP*[15] dotychczasowe kanały współpracy z Rządowym Zespołem Reagowania na Incydenty Komputerowe CERT.GOV.PL, Resortowym Centrum Zarządzania Bezpieczeństwem Sieci i Usług Teleinformatycznych (MIL-CERT) i Urzędem Komunikacji Elektronicznej. Z drugiej strony w wymianę informacji zostaną włączone powołany CSIRT Narodowy, CSIRT sektorowe, zespoły ds. bezpieczeństwa teleinformatycznego funkcjonujące w sektorach wskazanych w dyrektywie NIS, a także organy ścigania oraz organy właściwe w zakresie ochrony danych osobowych. Organizator będzie wspierać rozwój współpracy, a także reagować na problemy współpracy pomiędzy CERT/CSIRT Narodowym, CERT.GOV.PL, CERT/CSIRT sektorowymi oraz centrami ISAC. Minister Cyfryzacji określi **jednoznaczne mechanizmy wymiany informacji** o cyberbezpieczeństwie pomiędzy wymienionymi elementami systemu, a także pomiędzy podmiotami administracji państwowej czy podmiotami prywatnymi kluczowych sektorów gospodarki.

W krótkim okresie czasu opisany wyżej ośrodek koordynacyjny zostanie zbudowany na bazie pojedynczego punktu kontaktowego i będzie pełnił rolę brokera przetworzonych informacji z zakresu bezpieczeństwa sieci i informacji z całego systemu cyberprzestrzeni RP, obejmującego administrację publiczną, sektor telekomunikacji oraz inne sektory rynkowe wskazane w dyrektywie NIS. W krótkim okresie punkt kontaktowy miałby za zadanie zapewnić zwiększenie kultury bezpieczeństwa teleinformatycznego w administracji publicznej i sektorach rynkowych, natomiast w dłuższym okresie koncepcja będzie poszerzona o koordynację działań w przypadku cyberataku, współpracę z partnerami zagranicznymi oraz użytkownikami i administratorami cyberprzestrzeni, wymianę informacji na temat zagrożeń z podmiotami państwowymi i prywatnymi.

W dłuższym okresie, w oparciu o organizatora systemu i CSIRT-krajowy, uznane w kraju ośrodki badawcze oraz we współpracy z producentami urządzeń i systemów teleinformatycznych, zostanie powołane **Narodowe Centrum Cyberbezpieczeństwa**, które będzie gromadzić dane o zagrożeniach i podatnościach z zakresu bezpieczeństwa teleinformatycznego. Charakter Centrum ma umożliwić pogłębioną analizę niektórych zjawisk (np. do analizy złośliwego kodu), co jednocześnie zracjonalizuje sposób działania zespołów ds. bezpieczeństwa.

Zaproponowane zostaną również działania z zakresu **reorganizacji systemu teletransmisyjnego** pod kątem zwiększenia **bezpieczeństwa rejestrów** i istotnych danych będących w zasobach administracji państwowej, służb zespolonych oraz części sektora prywatnego.

[15] Docelowo Polityka ochrony cyberprzestrzeni RP zostanie zastąpiona Strategią Cyberbezpieczeństwa.

3.5. Aspekty prawne i finansowe

Rozbudowa krajowego systemu cyberbezpieczeństwa będzie wymagała licznych zmian prawnych. Najszersze zmiany będą związane z wdrożeniem do polskiego porządku prawnego, będącego obecnie na etapie projektu, dyrektywy Parlamentu Europejskiego i Rady w sprawie środków mających na celu zapewnienie wspólnego wysokiego poziomu bezpieczeństwa sieci i systemów informatycznych w Unii Europejskiej. Dyrektywa zawiera podstawy do ustanowienia wymienionych w dokumencie **elementów struktury krajowego systemu cyberbezpieczeństwa**: właściwych organów ds. bezpieczeństwa sieci i informacji, powołania struktury zespołów reagowania na incydenty komputerowe typu CERT/CSIRT, przyjęcia krajowych strategii w zakresie bezpieczeństwa sieci i informacji i przewidzianych nią działań, ustanowienia jednolitego punktu kontaktowego służącego wymianie informacji międzysektorowej i międzynarodowej. Projekt zawiera zobowiązania wobec operatorów kluczowych usług, którzy będą dokonywać oceny zagrożeń cybernetycznych, na jakie są narażeni, oraz do przyjęcia odpowiednich i proporcjonalnych środków mających na celu zapewnienie bezpieczeństwa sieci i informacji. Podmioty te będą zobowiązane do zgłaszania wszelkich incydentów poważnie zagrażających ich sieciom i systemom informatycznym oraz mogących znacząco zakłócić ciągłość działania kluczowych usług. Ograniczonym reżimem regulacyjnym zostaną objęci dostawcy usług cyfrowych, a więc platformy handlu elektronicznego, internetowe portale płatnicze, wyszukiwarki, usługi chmurowe, sklepów z aplikacjami[16].

Dyrektywa będzie implementowana poprzez przyjęcie ustawy o krajowym systemie cyberbezpieczeństwa, a powyższe zostało zgłoszone do programu prac legislacyjnych Rady Ministrów. Ustawa obejmie **swoim zakresem także organy władzy publicznej** oraz będzie zawierać **przepisy szczególne wobec elementów informatycznych służących ochronie infrastruktury krytycznej**, aby stworzyć spójny krajowy system wymiany informacji o incydentach i zapobiegania zagrożeniom teleinformatycznym. Przyjęta koncepcja krajowego systemu cyberbezpieczeństwa oznacza przebudowanie **definicji cyberprzestrzeni** i jej rozciągnięcie na sferę kluczowych operatorów funkcjonujących w sferze gospodarczej[17]. Dotychczasowa definicja była ograniczona do sektora publicznego (administracja państwowa, sądownictwo, administracja rządowa, część podmiotów z sektora finansów publicznych). Wprowadzenie szczególnych wymogów wobec elementów teleinformatycznych ochrony infrastruktury krytycznej może również oznaczać potrzebę uzupełnienia definicji infrastruktury krytycznej, tak aby nie pozostawiała wątpliwości, że obejmuje również infrastrukturę wirtualną (informacyjną).

Do uporządkowania pozostaje część uregulowań prawnych w zakresie wdrożenia kompleksowego **mechanizmu wymiany informacji** o cyberbezpieczeństwie pomiędzy elementami systemu. Przyjęte rozwiązanie powinno pozwalać na pełną automatyzację procesu wymiany informacji, być „*userfriendly*", z drugiej strony co najmniej zapewnić opcję klasyfikacji informacji (wzorem dystrybucji protokołem TLP[18]). Przepisy prawne muszą zapewnić ochronę tajemnic prawnie chronionych, np. tajemnicy przedsiębiorstwa, mają umożliwić ściganie przestępstw, z drugiej strony zostaną przewidziane wyłączenia wymiany informacji w wymiarze międzynarodowym o ile będą dotyczyć sfery bezpieczeństwa narodowego. Tym samym strategia i ustawa dotyczące krajowego systemu

[16]Ograniczony reżim regulacyjny oznacza mniejszą ilość wymagań bezpieczeństwa wobec dostawców usług cyfrowych, niższą niż stosowaną względem operatorów kluczowych usług (np. dobrowolna notyfikacja incydentów bezpieczeństwa).

[17]Definicja mogłaby zostać wprowadzona do ustawy o krajowym systemie cyberbezpieczeństwa bądź ustawy o świadczeniu usług drogą elektroniczną.

[18]Patrz decyzja Rady 2011/292/UE z 31 marca 2011 r. w sprawie przepisów bezpieczeństwa dotyczących ochrony informacji niejawnych UE w sprawie zasad bezpieczeństwa ochrony informacji.

cyberbezpieczeństwa, które obejmują sfery bezpieczeństwa administracji publicznej i gospodarki będą zawierać łączniki ze sferą bezpieczeństwa narodowego.

Spójność ze sferą bezpieczeństwa narodowego zostanie również zachowana poprzez uregulowanie np. w ustawie o zamówieniach publicznych i ustawie o Agencji Bezpieczeństwa Wewnętrznego **procesu weryfikacji producentów** i stosowanych rozwiązań w ramach sieci teleinformatycznych organów administracji państwowej oraz świadczonych usług, m.in. w zakresie: zapór sieciowych (firewall), oprogramowania antywirusowego, antyszpiegowskiego, rozwiązań uwierzytelniających, filtrujących, archiwizujących, szyfrujących, rozwiązań monitorujących i wykrywających włamania. Do wypracowania pozostanie nałożenie wymagań regulacyjnych i kontrolnych na dostawców rozwiązań systemów sterowania przemysłowego (OT – ang. *Operational Technology*) i systemów informatycznych (IT – ang. *Information Technology*) dla operatorów kluczowych usług.

Finansowanie krajowego systemu cyberbezpieczeństwa musi mieć odzwierciedlenie w budżetach odpowiednich instytucji. W krótkim okresie należy zapewnić finansowanie Departamentowi Cyberbezpieczeństwa Ministerstwa Cyfryzacji, podmiotu realizującego funkcję CERT/CSIRT Narodowego, CERT.GOV.PL, i jednolitego punktu kontaktowego w wersji wstępnej. W dłuższym okresie wydatki muszą obejmować wydatki związane z utrzymaniem platformy wymiany informacji między uczestnikami systemu i jednolitego punktu kontaktowego w wersji maksymalnej, a więc pełniącego funkcję systemu wczesnego ostrzegania oraz odpowiednio zabezpieczonego, stale aktualizowanego rejestru usług kluczowych i podmiotów je świadczących. Przy tworzeniu platformy wymiany informacji należy wykorzystać narzędzia już zbudowane przez instytuty badawcze zajmujące się cyberbezpieczeństwem (NASK, Wojskowy Instytut Łączności), np. w ramach projektów UE i NCBR. Istotnym elementem będzie kontynuacja finansowania **programów krajowych w dziedzinie badań** oraz edukacji na temat bezpieczeństwa cyberprzestrzeni. Wszystkie wymienione kategorie kosztów znajdą się w nowej kategorii budżetu zadaniowego w ramach budżetu państwa. Proponuje się również dalsze doskonalenie budżetowania administracji rządowej w dziedzinie cyberbezpieczeństwa, np. poprzez racjonalizację wydatków sprzętowo-utrzymaniowych, i centralizacji finansowania na szkolenia, utrzymania wykwalifikowanych zasobów ludzkich, ćwiczenia cybernetyczne i testy penetracyjne – wspomniane w pkt. 3.4 programu.[19] W przypadku prawnego uregulowania kwestii **CERT/CSIRT prywatnych i dla danego sektora gospodarki** w uzgodnieniu z regulatorami rynku oraz przedsiębiorcami na nich działającymi zostanie ustalony optymalny sposób funkcjonowania. Operatorzy kluczowych usług, o ile nie są już objęci przepisami dotyczącymi sektora publicznego, będą zobowiązani do przyjmowania minimalnych wymagań z zakresu bezpieczeństwa teleinformatycznego, co będzie wiązało się poniesieniem dodatkowych kosztów, np. na wdrożenie standardów bezpieczeństwa teleinformatycznego. Założeniem rozwiązań przyjętych na poziomie krajowym będzie jednak **zapewnienie konkurencyjności polskich podmiotów** w stosunku do podmiotów z innych krajów.

Do czasu wdrożenia docelowego, kompleksowego systemu bezpieczeństwa teleinformatycznego, a więc przyjęcia ustawy o krajowym systemie cyberbezpieczeństwa, zadania realizowane we współpracy z UKE, NASK, CERT.GOV.PL będą realizowane w oparciu umowy, porozumienia wynikające z dotychczasowych przepisów prawa (przepisy prawa administracyjnego, ustawa o finansach publicznych, ustawa o instytutach badawczych).

[19]W ramach *Polityki ochrony cyberprzestrzeni* w 2015 r. dokonano przeglądu finansowania wydatków na cyberbezpieczeństwo w administracji rządowej (urzędach wskazanych w *Polityce*). W przypadku programu szkoleń można wykorzystać środki UE z PO PC.

3.6. Ocena ryzyk

Z uwagi na to, że wybór obiektu ataku, jego momentu w czasie oraz rodzaju ataku zawsze będzie pozostawał po stronie atakującego, broniący się musi racjonalizować zaangażowanie środków w obronę przed atakiem. Podstawę takiej racjonalizacji powinien stanowić ciągły proces szacowania ryzyka. Dla potrzeb tego procesu niezbędne jest zapewnienie:

- ustanowienie jednolitej metodyki szacowania ryzyka,
- prowadzenia w czasie rzeczywistym bazy informacji o zidentyfikowanych zagrożeniach,
- prowadzenie w czasie rzeczywistym bazy informacji o zidentyfikowanych podatnościach,
- wyznaczenie dla każdego poziomu hierarchii systemu cyberbezpieczeństwa progów dla poziomów ryzyka od których wymagane jest raportowanie na wyższy poziom.

Raportowanie o ryzykach na wyższy poziom hierarchii systemu cyberbezpieczeństwa ma za zadanie optymalizacji środków ochrony w skali sektora lub w skali całego kraju.

Przyjęty w *Polityce Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej* system oceny ryzyk na poziomie kraju, polegający na agregowaniu przez urząd obsługujący ministra właściwego ds. cyfryzacji sprawozdań z poszczególnych podmiotów administracji rządowej okazał się nieskuteczny i nie pozwala na realną ocenę stanu bezpieczeństwa w cyberprzestrzeni w czasie rzeczywistym. System ten wymaga gruntownej przebudowy.

3.7. Ostatnia linia obrony

Mankamentem obecnie funkcjonującego systemu jest brak systemowych rozwiązań dających możliwość rozwiązywania trudnych problemów z odziałem operatora, dostawcy usługi czy producenta oprogramowania. Nie ma zawartych na szczeblu strategicznym umów zobowiązujących wyżej wymienione podmioty do uczestnictwa w procesie zapewnienia bezpieczeństwa cybernetycznego lub przywracania funkcji systemów utraconych lub uszkodzonych w wyniku niepożądanych działań w cyberprzestrzeni.

4. Stan proponowany

4.1. Proponowany podział kompetencji i struktury

Wypełniając jedno z podstawowych założeń budowy efektywnego systemu cyberbezpieczeństwa należy obowiązki w zakresie ochrony cyberprzestrzeni rozdzielić pomiędzy uczestników procesu w taki sposób, by żaden element systemu nie pozostał bez nadzoru odpowiedniej struktury organizacyjnej.

POZIOM STRATEGICZNO-POLITYCZNY	
Organ właściwy ds. bezpieczeństwa sieci i informacji	**Minister właściwy do spraw informatyzacji**

Organ właściwy w sprawie stanowienia prawa dotyczącego cyberprzestępczości	**Minister właściwy do spraw sprawiedliwości**
Organ nadzorujący pracę organów ścigania	**Minister właściwy do spraw wewnętrznych**
POZIOM OPERACYJNY	
Pojedynczy Punkt Kontaktowy(PPK)	**Ministerstwo obsługujące ministra właściwego ds. informatyzacji (w tym na potrzeby implementacji dyrektywy NIS)**
Punkt Kontaktowy dla operatorów Infrastruktury Krytycznej(PKIK)	**Stanowisko w ramach Centrum Operacyjno-Analitycznego działającego w Rządowym Centrum Bezpieczeństwa, merytorycznie powiązane z CERT/CSIRT Krajowym/Narodowym**
Narodowe Centrum Cyberbezpieczeństwa (Centrum Kompetencyjne)	**Organizacyjne włączone w strukturę Naukowej i Akademickiej Sieci Komputerowej, korzystające z zasobów i środków akademickich, Narodowego Centrum Kryptologii, CERT.GOV.PL, MIL-CERT i CERT/CSIRT kluczowych dostawców usługi dostępu do Internetu**
CERT/CSIRT Narodowy	**CERT Polska (NASK)**
Organ regulacyjny ds. integralności sieci i usług telekomunikacyjnych	**Urząd Komunikacji Elektronicznej**
Krajowy Punkt Kontaktowy do celów wymiany informacji odnoszących się do cyberprzestępstw	**CERT.GOV.PL (ABW)**
Komórki zajmujące się zwalczaniem cyberprzestępczości	**Wydziały ds. walki z cyberprzestępczością Komendy Głównej Policji, komend wojewódzkich Policji**
CERT/CSIRT sektorowe	**Operatorzy usług kluczowych, operatorzy telekomunikacyjni, operatorzy usług zaufania, certyfikacji**
CERT/CSIRT dla administracji rządowej	**CERT.GOV.PL (dla obszaru cywilnego), MIL-CERT (dla obszaru militarnego)**
CERT/CSIRT dla Policji	**POL-CERT (dla systemów IT Policji)**
POZIOM TECHNICZNY	
Operacyjne Centra Bezpieczeństwa (ang.: SOC)[20]	**Podmioty utrzymujące systemy teleinformatyczne o kluczowym znaczeniu dla cyberbezpieczeństwa albo grupy podmiotów eksploatujących systemy teleinformatyczne**
Poziom użytkownika	**Lokalne Zespoły Reagowania ustanowione w podmiotach eksploatujących systemy teleinformatyczne**

[20] SOC, w zależności od konkretnych uwarunkowań, zaliczone mogą być do poziomu technicznego albo do poziomu operacyjnego

Niezależnie od powyższych struktur wykonawczych na poziomie technicznym, w podmiotach realizujących zadania publiczne, muszą zostać wydzielone komórki organizacyjne, podległe bezpośrednio kierownikowi podmiotu, których zadaniem będzie organizacja i utrzymywanie systemu zarządzania bezpieczeństwem informacji zgodnie z wymaganiami zawartymi w *rozporządzeniu Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych*. Do zadań takiej komórki powinno należeć w szczególności realizacja zadań w zakresie:

1) systemu zarządzania bezpieczeństwem informacji,
2) opracowania i aktualizacji polityki bezpieczeństwa w podmiocie,
3) kontroli przestrzegania polityki bezpieczeństwa we wszystkich komórkach i jednostkach organizacyjnych podmiotu w tym, kontroli efektywności uzyskanego poziomu bezpieczeństwa do założonych celów,
4) zarządzania ryzykiem bezpieczeństwa informacyjnego,
5) standaryzacji poziomu bezpieczeństwa zasobów informacyjnych,
6) określania obowiązków osób odpowiedzialnych za bezpieczeństwo informacji każdego szczebla zarządzania.

Ponadto komórka organizacyjna, o której mowa powyżej, może realizować zadania w zakresie:

1) organizacja ochrony fizycznej i zabezpieczenia technicznego,
2) określania obowiązujących zasad ochrony i przetwarzania danych osobowych,
3) wykonywania ustawowych obowiązków Administratora Bezpieczeństwa Informacji przez pracowników struktury bezpieczeństwa, zatrudnionych w podmiocie,
4) nadzoru i koordynacji wdrożenia, aktualizacji i testowania planów zapewnienia ciągłości działania w podmiocie oraz wykonywania i koordynacji zadań z zakresu planowania obronnego i zarządzania kryzysowego,
5) zapewnienia wykonywania przepisów określonych w ustawie o ochronie informacji niejawnej i aktach wykonawczych do ustawy,
6) prowadzenia kancelarii tajnej,
7) szkolenia pracowników z zakresu polityki bezpieczeństwa, obronności, działań kryzysowych i informacji niejawnych.

4.2. Organizacja systemu wczesnego ostrzegania i reagowania

CERT/CSIRT narodowy musi posiadać możliwość zbierania informacji o anomaliach w ruchu sieciowym odbywającym się zarówno w wymianie międzynarodowej, jak i w wymianie pomiędzy operatorami krajowymi, których usługi zaliczone zostaną do tzw. usług kluczowych. Centralne prowadzenie monitorowania ma na celu wykrycie takich anomalii, które w przypadku pojedynczego węzła wymiany nie osiągają progu alarmowania, jednak w skali całej wymiany mogą być symptomem poważnego ataku. Analiza ruchu sieciowego

może być prowadzona z wykorzystaniem doświadczeń projektu ARAKIS (docelowo ARAKIS2) realizowanego przez Naukową i Akademicką Sieć Komputerową. W tym celu niezbędne jest przeprowadzenie inwentaryzacji wszystkich punktów wymiany międzyoperatorskiej, ze szczególnym uwzględnieniem wymiany międzynarodowej.

Zagregowana informacja o zagrożeniach powinna być przekazywana do CERT/CSIRT sektorowych poprzez z góry ustalone kanały komunikacyjne, w tym, jeśli zajdzie taka potrzeba, poprzez środki łączności zapasowej. Informacja o zagrożeniach powinna być również dostępna dla wszystkich użytkowników cyberprzestrzeni za pośrednictwem dedykowanej strony internetowej.

W przypadku stwierdzenia, że polski obszar cyberprzestrzeni jest atakowany ze źródeł położonych poza terytorium kraju CERT/CSIRT musi posiadać zdolność do przekazania operatorowi węzła wymiany ruchu żądania wprowadzenia filtrowania ruchu według określonych zasad, a w przypadkach krytycznych żądania odłączenia węzła wymiany.

Według wyżej wymienionych zasad powinno się również monitorować ruch sieciowy pomiędzy operatorami wewnątrz kraju, po to by odpowiednio wcześniej identyfikować źródła ataku.

4.3. Proponowane procedury, progi reakcji, kanały wymiany informacji

W odpowiedzi na zidentyfikowane zagrożenia, a w szczególności w odpowiedzi na zagrożenia zmaterializowane, należy wypracować scenariusze reakcji. W skład scenariusza reakcji powinien wchodzić łańcuch procedur powoływanych w miarę rozwoju sytuacji. Scenariusz reakcji musi opisywać kto i w jakiej sytuacji uruchamia konkretne procedury, kogo powiadania o uruchomieniu procedury, z kim współpracuje i kogo powiadamia o skutkach realizacji procedury, a w szczególności o przywróceniu stanu normalnego albo o dalszej eskalacji incydentu, co powinno skutkować powołaniem kolejnych procedur.

Przykładowy scenariusz reagowania na incydent zawarty jest w Załączniku nr 2. Zaprezentowany scenariusz prezentuje metodę podejścia do problemu reagowania na incydenty oraz ich komunikowania i wymaga dopracowania w drodze konsultacji z zainteresowanymi podmiotami, a w szczególności z Rządowym Centrum Bezpieczeństwa, CERT Polska oraz reprezentacją wszystkich sektorów. W wyniku tych konsultacji powinny powstać scenariusze reagowania na incydenty wszystkich kategorii dla wszystkich sektorów .

Podstawą opracowania scenariuszy, a w dalszej konsekwencji procedur postępowania, jest zidentyfikowanie zagrożeń pochodzących z cyberprzestrzeni i wpływu ich materializacji na konkretne systemy teleinformatyczne.

Szczególne miejsce w zbiorze takich scenariuszy zajmie scenariusz postępowania w sytuacji, gdy dane zagrożenie nie było dotąd zidentyfikowane albo stosowane procedury okazują się nieskuteczne, co *de facto* oznacza wdrożenie procedury kryzysowej. Dotyczy to również sytuacji gdy incydenty mają charakter masowy.

Istotnym problemem, którego rozwiązanie nie jest w pełni możliwe na obecnym etapie tworzenia krajowego systemu cyberbezpieczeństwa, jest ustalenie progów podziału na kategorie incydentów, o których mowa w Rozdziale 3. Z jednej strony pożądane by było, aby progi podziału były obiektywne, oparte na mierzalnych wskaźnikach. Jednak z drugiej strony wprowadzenie ostrych granic podziału może powodować, że w konkretnym przypadku może dojść do nieodpowiedniej kwalifikacji incydentu. Oznacza to, że wprowadzając kryteria

podziału nie uniknie się potrzeby stosowania wiedzy eksperckiej. Istotne jest, aby powstała baza takiej wiedzy obejmująca dotychczasowe doświadczenia, uwzględniająca zarówno przypadki decyzji trafionych, jak i decyzji błędnych.

Krajowy system cyberbezpieczeństwa musi posiadać podsystem powiadamiania działający w dwóch trybach: aktywnym i pasywnym. W trybie aktywnym podmiot, który posiadł wiedzę o potencjalnym ataku lub zidentyfikował atak, który już trwa, powiadamia o tym fakcie inne podmioty według z góry ustalonego schematu. W trybie pasywnym podmiot zainteresowany sytuacją w obszarze cyberbezpieczeństwa uzyskuje wiedzę o tym stanie z bazy wiedzy utrzymywanej przez CERT/CSIRT narodowy.

Mając na uwadze to, że incydent może dotyczyć systemu komunikacji należy zapewnić kanały łączności zasadniczej i alternatywnej. System łączności ma służyć powiadamianiu o incydentach, wyzwalaniu procedur reakcji i raportowaniu o skutkach incydentu. Przewiduje się, że jako zasadniczy kanał komunikacji wykorzystany zostanie system kierowania bezpieczeństwem narodowym (SKBN).

W ramach studium dla ENISA (opracowanie "Actionable Information for Security Incident Response"), zespół CERT Polska zidentyfikował aż 53 standardy wymiany informacji cyberbezpieczeństwa oraz 16 przykładowych darmowych narzędzi (na licencji open source) do zarządzania nimi. Platforma wymiany informacji może się składać z wielu elementów, charakteryzujących się obsługą różnych typów informacji. Z doświadczeń budowy podobnych systemów (projekty FISHA/NISHA czy platforma n6) wynika bowiem, że charakter wymienianych informacji (w tym ich ilość oraz możliwe zastosowanie) jest tak różnorodny, że jest mało prawdopodobne, aby mogło powstać jedno efektywne rozwiązanie do ich wymiany.

Wśród wymienianych informacji powinny znajdować się m.in.:

- ostrzeżenia (alerty) o nowych zagrożeniach czy podatnościach [NISHA],
- zalecenia dotyczące zagrożeń i podatności [NISHA],
- opracowania "najlepszych praktyk" w zakresie zagadnień cyberbezpieczeństwa [NISHA],
- materiały typu "awareness" [NISHA],
- informacje o wykrytej złośliwej aktywności (np. komputery zainfekowane botami, biorące udział w ataku DDoS czy przechowujące złośliwe strony WWW itp.) [n6],
- informacje o źle skonfigurowanej, otwartej lub podatnej infrastrukturze (np. otwarte systemy DNS, NTP itp.) [n6],
- informacje o wskaźnikach "IoC" (Indicators of Compromise) [n6],
- istotne próbki złośliwego oprogramowania (do ewentualnej wspólnej analizy),
- informacje o TTP (ang. Tactics, Techniques and Procedures) i ew. aktorach stojących za atakami (w szczególności Advanced Persistent Threats - APT),
- logi systemowe, sieciowe, kopie dysków i inne materiały mogące być przedmiotem analizy forensics,
- informacje o nielegalnych treściach w sieci.

4.4. Projekt kompetencji organizatora systemu

Kompetencje i uprawnienia Ministra Cyfryzacji jako organizatora systemu cyberbezpieczeństwa określi ustawa o krajowym systemie cyberbezpieczeństwa. Ustawa usankcjonuje prawnie rolę Ministra w zakresie:

a) opracowania **krajowej strategii** cyberbezpieczeństwa,

b) przygotowywania projektów **aktów prawnych** z zakresu **cyberbezpieczeństwa**, w tym:

- ustalenia ustawowych wymagań i powinności z zakresu cyberbezpieczeństwa w obszarze organizacyjnym i technologicznym,
- opracowania kryteriów kwalifikacji podmiotów gospodarki narodowej jako świadczących usługi kluczowe z punktu widzenia przepisów prawa dotyczących cyberbezpieczeństwa,
- opracowania, prowadzenia i aktualizacji wykazu usług kluczowych i podmiotów świadczących takie usługi w rozumieniu przepisów prawa,
- opracowania propozycji progów istotności incydentu bezpieczeństwa dla podmiotów z administracji publicznej i każdego z sektorów zobowiązanych do notyfikacji incydentów,
- opracowania uregulowań i wytycznych dotyczących mechanizmów wymiany informacji z zakresu cyberbezpieczeństwa w administracji publicznej, sferze gospodarki narodowej, zarządzania kryzysowego a także w zakresie relacji z organami ścigania i organami odpowiedzialnymi za zapewnienie bezpieczeństwa narodowego,
- przygotowania wytycznych w zakresie ustanowienia odpowiednich i proporcjonalnych środków ochrony systemów teleinformatycznych i informacji na podstawie procesu zarządzania ryzykiem,

c) prowadzenia **kontroli** przestrzegania przepisów z zakresu cyberbezpieczeństwa w administracji publicznej i podmiotach świadczących usługi kluczowe,

d) prowadzenia spraw związanych z uruchomieniem i sprawowaniem **nadzoru nad krajową siecią CSIRT/CERT** i **CSIRT Narodowym**, w tym zapewnieniem mu odpowiednich zasobów technicznych, ludzkich i finansowych,

e) ustanowienia i zapewnienia funkcjonowania **pojedynczego punktu kontaktowego**, w tym zagwarantowania mu odpowiednich zasobów technicznych, ludzkich i finansowych,

f) zapewnienia funkcjonowania krajowego systemu reagowania na incydenty komputerowe w wymiarze operacyjnym, przy czym powyższa funkcjonalność będzie mogła być zbudowana na bazie pojedynczego punktu kontaktowego.

Organizator systemu będzie odpowiedzialny za przygotowywanie krajowej strategii z zakresu cyberbezpieczeństwa zawierającą cele i priorytety w oparciu o aktualną analizę zagrożeń i incydentów oraz przeprowadzone szacowanie ryzyka bezpieczeństwa cyberprzestrzeni dla wszystkich wskazanych w niej sektorów. Tym samym organizator będzie przygotowywał **roczne raporty o zagrożeniach cyberprzestrzeni w ujęciu sektorowym** przy wykorzystaniu danych sektorowych jak i uzyskanych i współpracy z innymi instytucjami, które

już obecnie opracowują raporty dotyczące cyberbezpieczeństwa, cyberprzestępczości czy sfery bezpieczeństwa narodowego tj. CERT Polska[21], CERT.GOV.PL[22], raport MSWiA o stanie bezpieczeństwa[23], raporty RCB o stanie zagrożenia bezpieczeństwa narodowego[24]. Strategia wyposaży Ministerstwo Cyfryzacji w ramy zarządzania służące realizacji celów i priorytetów, w tym jasne określenie funkcji i zakresu obowiązków organów rządowych i innych właściwych podmiotów. Przy określeniu środków w zakresie gotowości, reagowania i przywracania stanu normalnego w zakresie bezpieczeństwa sieci i informacji, mechanizmów współpracy pomiędzy sektorami publicznym i prywatnym organizator systemu wykorzysta wymagania określone w normie ISO 22301:2012 dotyczącej Systemu Zarządzania Ciągłością Działania wspieranej przez normy ISO/IEC 24762:2008 i ISO/IEC 27031:2011 oraz wymagania dotyczące systemów zarządzania bezpieczeństwem informacji opartych na normach z rodziny ISO 27000. Organizator systemu wspólnie z Ministerstwem Nauki i Szkolnictwa Wyższego, Narodowym Centrum Badań i Rozwoju oraz Ministerstwem Edukacji określi w strategii odpowiednie warunki i ramy dla realizacji kilkuletnich programów krajowych w dziedzinie badań oraz edukacji, w tym specjalistycznej na temat bezpieczeństwa cyberprzestrzeni. Ministerstwo Cyfryzacji będzie odpowiedzialne za przygotowanie i stały rozwój analizy ryzyka z zakresu bezpieczeństwa teleinformatycznego, dla wszystkich wskazanych w strategii sektorów. Ministerstwo wykorzysta doświadczenia szacowania ryzyka prowadzone na potrzeby „*Polityki ochrony cyberprzestrzeni RP*" oraz zaangażuje się szerzej w działalność Platformy NIS[25] Komisji Europejskiej i agencji ENISA, stanowiącej platformę wymiany informacji nt. działań systemowych w dziedzinie edukacji, działalności badawczo-rozwojowej i prowadzenia szacowania ryzyka.

Jednym z podstawowych zadań o charakterze operacyjnym organizatora będzie powołanie i zapewnienie działania oficjalnego zespołu reagującego na zagrożenia i incydenty bezpieczeństwa w cyberprzestrzeni na poziomie krajowym – **CSIRT/CERT Narodowy** oraz zapewnienia funkcjonowania sieci CSIRT/CERT sektorowych. Założeniem funkcjonowania systemu będzie, że działania operacyjne będą realizowane w wymiarze sektorowym (CERT sektorowe, SOC, ISAC i lokalne zespoły reagowania), przy jednoczesnym umocowaniu CERT Narodowego jako głównego punktu kontaktowego w wymiarze techniczno-operacyjnym (tzw. CERT „of the last resort"). CSIRT Narodowy będzie koordynować pracę CSIRT sektorowych i będzie stanowić punkt wymiany informacji z podobnymi jednostkami w innych krajach (w ramach sieci CSIRT). Powyższe podejście oznacza przypisanie odpowiedzialności wobec koordynatora systemu w zakresie zdefiniowania katalogu usług, które winny być świadczone przez CSIRT/CERT Narodowy oraz poziomu, na jakim winny być świadczone.[26]

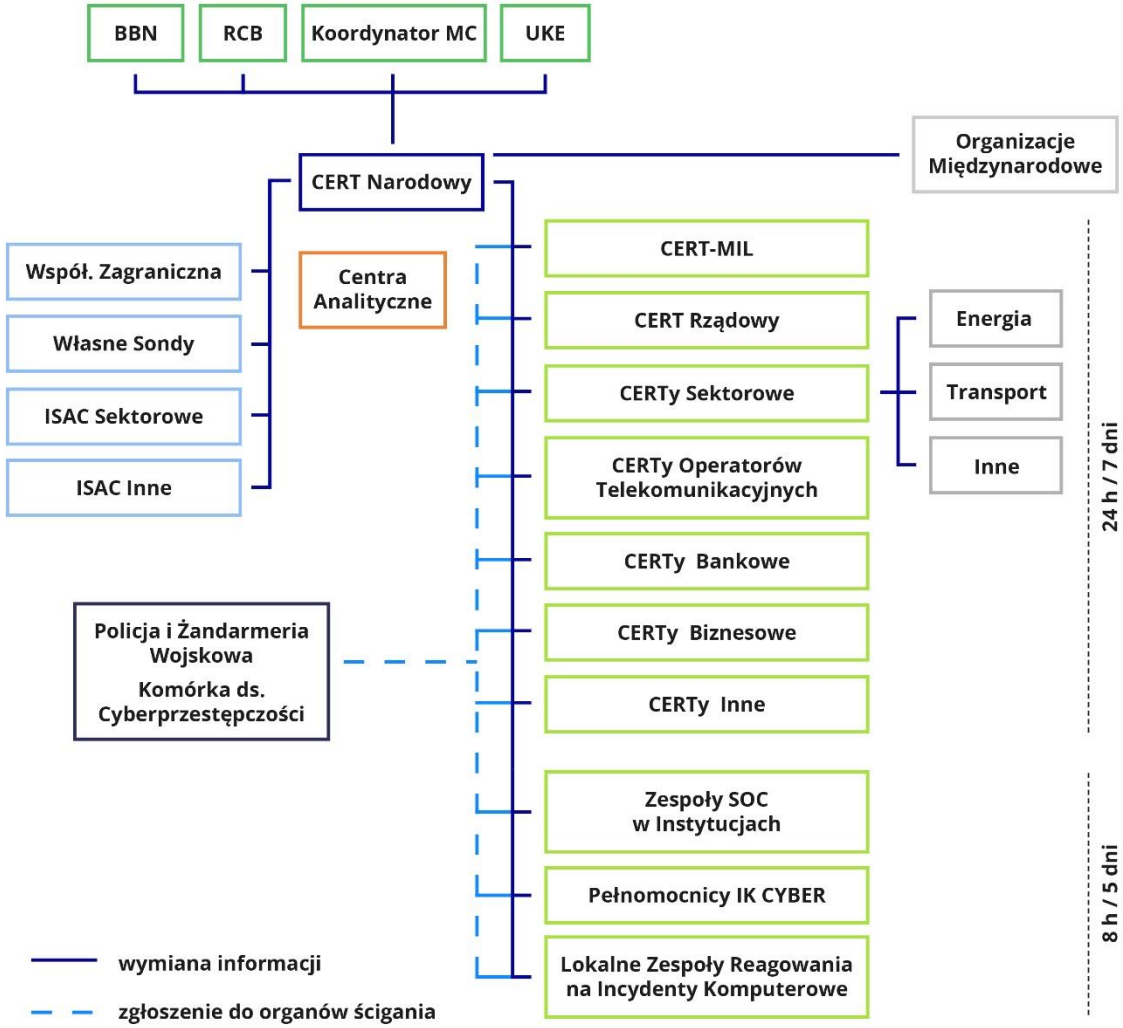
Zgodnie z publikacją Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji (ENISA) pt. *„ENISA – CERT Inventory Inventoryof CERT teams and activities in Europe"*[27] dominującą cechą charakterystyczną rozwiązań występujących w krajach członkowskich UE jest umiejscowienie CSIRT/CERT Narodowego w strukturach cywilnych oraz łączenie funkcji CSIRT krajowego i rządowego. Znane wyjątki umiejscowienia CSIRT krajowego w strukturach służb specjalnych to Grecja i Hiszpania, a w strukturach wojska to Dania i Łotwa.

[21] http://www.cert.pl/raporty
[22] http://www.cert.gov.pl/cer/publikacje
[23] http://bip.mswia.gov.pl/bip/raport-o-stanie-bezpie/18405,Raport-o-stanie-bezpieczenstwa.html
[24] http://rcb.gov.pl/
[25] https://resilience.enisa.europa.eu/nis-platform
[26] Opisane w ekspertyzie NASK na s. 98-106 oraz publikacji agencji ENISA „National/governmental CERT. ENISA's recommendations on baseline capabilities"https://www.enisa.europa.eu/activities/cert/support/baseline-capabilities/national-governmental-certs-enisas-recommendations-on-baseline-capabilities
[27] https://www.enisa.europa.eu/activities/cert/background/inv/files/inventory-of-cert-activities-in-europe

Do kompetencji organizatora należeć będzie **budowa funkcjonalności pojedynczego punktu kontaktowego** w wersji wstępnej, a następnie jego rozbudowa do wersji rozszerzonej, a więc krajowego systemu reagowania na incydenty komputerowe, będącego w stanie zarządzać aktualnymi zagrożeniami w cyberprzestrzeni. W ramach tej funkcji jednolity punkt kontaktowy będzie:

- informować w wymiarze międzysektorowym i międzynarodowym (w związku z dyrektywą NIS) o incydentach dużej skali,
- eskalować za pośrednictwem właściwych organów (np. RCB) o najpoważniejszych problemach bezpieczeństwa teleinformatycznego na poziom Rady Ministrów,
- prowadzić katalog zagrożeń wraz ze scenariuszami reakcji na te zagrożenia przez podmioty państwowe, uwzględniającego również rolę podmiotów prywatnych,
- stanowić punkt kontaktowy dla Komisji Europejskiej na Polskę (po przyjęciu Dyrektywy NIS). Taki punkt będzie sporządzał raport nt. notyfikacji poważnych incydentów z sektorów objętych dyrektywą NIS, rodzajów naruszeń i czasu ich trwania.

W dłuższym okresie do kompetencji Ministerstwa Cyfryzacji będzie należało opracowanie studium wykonalności odnośnie utworzenia Narodowego Centrum Cyberbezpieczeństwa, zdefiniowanie jego zadań i funkcji. Centrum gromadziłoby dane o zagrożeniach i podatnościach. Proponuje się połączenie roli CERT Narodowego i Narodowego Centrum Cyberbezpieczeństwa.



Rysunek 4 System wczesnego ostrzegania

4.5. Niezbędne zmiany kompetencyjne, organizacyjne i legislacyjne

Zasadnicza część zmian organizacyjnych w krajowym systemie cyberbezpieczeństwa będzie związana z precyzyjnym zdefiniowaniem roli organizatora systemu, czyli Ministerstwa Cyfryzacji w ustawie o krajowym systemie cyberbezpieczeństwa. Częściowa centralizacja systemu, za którą opowiadają się kluczowi interesariusze, oznacza, że Ministerstwo Cyfryzacji jako koordynator strategiczno-polityczny będzie ustalać politykę i cele do realizacji, proponować i wdrażać rozwiązania legislacyjne, oddziaływać prawnie na inne instytucje, opracowywać wieloletnie programy działania (np. w zakresie działalności badawczo-rozwojowej) i koordynować współpracę międzynarodową. Równocześnie przy projektowaniu systemu przyjęto założenie, aby nie naruszać kompetencji i dotychczasowych zdolności podmiotów tworzących system bezpieczeństwa cybernetycznego RP, ale nazwać faktycznie pełnione role przez podmioty i ich miejsce w systemie. Oznacza to m.in. usankcjonowanie na poziomie ustawowym funkcjonującego w ABW Rządowego Zespołu CERT.GOV.PL, jego

kompetencji i procedur. Wobec powyższego niezbędne będzie wprowadzenie odpowiednich zmian w art. 5 ustawy z dnia 24 maja 2002 roku o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, poprzez wskazanie, że jednym z zadań Agencji Bezpieczeństwa Wewnętrznego jest pełnienie funkcji rządowego zespołu reagowania na incydenty komputerowe. Niezbędne będzie również nowelizowanie Ustawy Prawo Telekomunikacyjne ze względu na konieczność uzupełnienia zapisów dotyczących obowiązków UKE i ABW.

Rozbudowa krajowego systemu cyberbezpieczeństwa w wymiarze operacyjnym będzie związana ze zbudowaniem przez organizatora systemu nowych instytucji **CSIRT Narodowego** i **funkcjonalności pojedynczego punktu kontaktowego**. Do czasu przyjęcia ustawy o krajowym systemie cyberbezpieczeństwa i wobec braku umocowania ustawowego CERT.GOV.PL preferowaną formułą będzie powierzenie roli CERT Narodowego zespołowi CERT Polska, działającego w ramach NASK. Powierzenie CERT Polska/NASK roli Narodowego CSIRT powinno się odbyć z wykorzystaniem procedury opisanej w art. 37 ustawy z dnia 30 kwietnia 2010 roku o instytutach badawczych. Na podstawie powołanego przepisu Minister Cyfryzacji może nałożyć na NASK jako instytut badawczy zadanie, zgodnie z zakresem działania określonym w statucie instytutu, jeżeli jest to niezbędne ze względu na potrzeby obronności lub bezpieczeństwa publicznego, w przypadku stanu klęski żywiołowej lub w celu wykonania zobowiązań międzynarodowych. Zakres działania NASK określony w § 8 Statutu z dnia 25 marca 2011 roku obejmuje m.in. prowadzenie badań naukowych i prac rozwojowych w zakresie bezpieczeństwa sieci i systemów teleinformatycznych. Realizacja zadania w postaci obowiązku utworzenia i pełnienia funkcji CSIRT Narodowego oraz funkcjonalności punktu kontaktowego powinna odbywać się, na podstawie umowy pomiędzy NASK a Ministrem Cyfryzacji. Umowa będzie określać zarówno szczegółowe obowiązki CERT Narodowego, w tym obowiązek prowadzenia platformy wymiany informacji, zasady składania raportów i przekazywania bieżących informacji do organizatora systemu, jak również zasady współpracy z CSIRT rządowym, CSIRT sektorowymi i Policją. Dodatkowo w NASK, jako instytucie badawczym mogłoby powstać akredytowane laboratorium dokonujące oceny lub certyfikacji produktów informatycznych (sprzętu lub oprogramowania) stosowanych w systemach podmiotów sfery publicznej i w zainteresowanych podmiotach prywatnych.

Organizacja przez Ministra Cyfryzacji systemu cyberbezpieczeństwa na poziomie technicznym, oznacza standaryzację kompetencji zasobów ludzkich umożliwiających efektywne funkcjonowanie SOC, lokalnych zespołów reagowania (LZR) pełnomocników ds. bezpieczeństwa cyberprzestrzeni, pełnomocników ds. infrastruktury krytycznej, kompetencji dyrektorów generalnych w zakresie bezpieczeństwa teleinformatycznego. Powyższe zmiany organizacyjne będą wymagały przeprowadzenia w ramach prac legislacyjnych zmian w przepisach dotyczących funkcjonowania administracji rządowej (m.in. ustawa o służbie cywilnej, rozporządzenie w sprawie stanowisk urzędniczych, ustawa o zarządzaniu kryzysowym).

Planuje się również ustanowienie programu motywacyjnego dla specjalistów z obszaru cyberbezpieczeństwa **pod roboczą nazwą „Złota Setka”;** celem programu będzie zapewnienie stosownych dodatków motywacyjnych dla specjalistów spełniających najwyższe kryteria fachowości potwierdzone stosownymi certyfikatami. Ocenia się że ok. 100 specjalistów z różnych dziedzin informatyki będących w zasobach państwowych struktur (resortów)zaliczonych do programu „Złota Setka” może mieć istotny wpływ na zapewnienie wymaganego poziomu bezpieczeństwa teleinformatycznego sektora rządowego i skutecznie wspierać ważne sektory pozarządowe. Ustanowienie programu zapobiegnie, a co najmniej zmniejszy, odpływ specjalistów o najwyższych kwalifikacjach z instytucji rządowych do sektora cywilnego. Ocenia się że koszty programu to ok. 6 mln zł/rok.

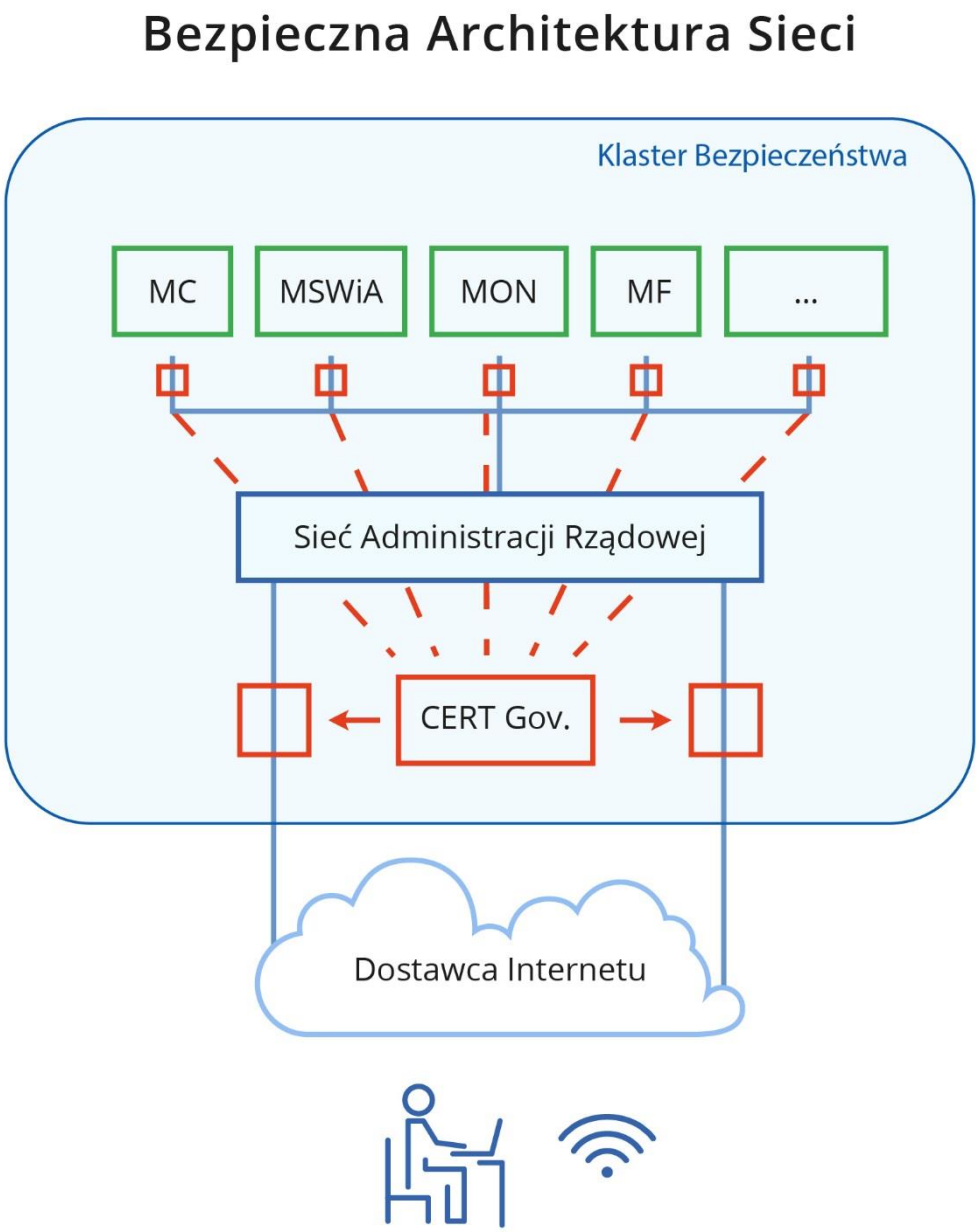
Bez uszczerbku dla dotychczasowych zdolności podmiotów tworzących system bezpieczeństwa cybernetycznego RP najważniejsze zmiany kompetencyjne będą dotyczyć powiązań i zależności pomiędzy instytucjami sektorowymi, tj. regulatorami rynkowymi odpowiedzialnymi za funkcjonowanie podmiotów z sektorów, w przypadku których naruszenia bezpieczeństwa teleinformatycznego mogą nieść zagrożenia istotnych funkcji państwa (patrz KATEGORIA 1 Rozdział 3) a kompetencjami podmiotów odpowiedzialnych za sferę zarządzania kryzysowego (Rządowe Centrum Bezpieczeństwa) i szerzej sfery bezpieczeństwa narodowego (Biuro Bezpieczeństwa Narodowego).

Istotne dla całego procesu organizowania systemu bezpieczeństwa cyberprzestrzeni jest przyjęcie optymalnego podejścia do zagadnienia infrastruktury krytycznej we wszystkich kluczowych sektorach, a więc unikanie powielania kompetencji i dublowania wymiany informacji. Z jednej bowiem strony każdy z kluczowych sektorów opiera się na infrastrukturze teleinformatycznej, która powinna być odpowiednio chroniona (taka koncepcja została przyjęta w dyrektywie NIS). Z drugiej zaś strony istnieje pojęcie informatycznej infrastruktury krytycznej (ang. *Critical Information Infrastructure* - CII) jako często najważniejszej kategorii systemów (niezależnie jaką branżę reprezentują) podlegających skoordynowanej ochronie. W polskim systemie prawnym nie istnieje odrębna kategoria teleinformatycznej infrastruktury krytycznej, funkcjonuje natomiast system sieci teleinformatycznych. Minister Cyfryzacji jako odpowiedzialny za powyższy system, współpracuje z operatorami powyższej infrastruktury w zakresie jej ochrony i utrzymania (przy założeniu, że są to powinności operatora) oraz Rządowym Centrum Bezpieczeństwa, odpowiedzialnym za koordynację ochrony całego systemu IK na poziomie kraju. Dodatkowo system sieci teleinformatycznych charakteryzuje najwyższa skala powiązań z innymi kluczowymi sektorami. Dlatego też bezpieczeństwo powinno być widziane całościowo (na wskroś poszczególnych sektorów) poprzez przypisanie roli w zakresie zarządzania bezpieczeństwa warstwy sieci („teleinformatycznej infrastruktury krytycznej") jednej instytucji, a więc Rządowemu Centrum Bezpieczeństwa bądź Urzędowi Komunikacji Elektronicznej, przy zapewnieniu wymiany informacji z organizatorem systemu i CSIRT Narodowym CERT.GOV.PL[28]. Natomiast w każdym sektorze kluczowym z osobna, powinny istnieć kompetencje służące identyfikacji poważnych zagrożeń w warstwie sieci i usług teleinformatycznych, wymianie informacji z RCB bądź UKE, a CSIRT Narodowym i organizatorem systemu. Konsekwentnie plany zarządzania kryzysowego odnosiłyby się odrębnie do „teleinformatycznej infrastruktury krytycznej", a odrębnie do warstwy usług i aplikacji.

Poszerzenie aspektów ochrony cyberprzestrzeni na sferę podmiotów rynkowych będzie wymagało stworzenia podstaw formalnych prowadzonej współpracy (np. incydentach), w tym zagwarantowania w przepisach sektorowych wymagań w zakresie ochrony tajemnicy przedsiębiorstwa i podstaw funkcjonowania CSIRT sektorowych. W tak zbudowanym systemie Ministerstwo Cyfryzacji pełniąc rolę urzędu ds. bezpieczeństwa sieci i informacji prowadziłoby natomiast rejestr usług kluczowych i podmiotów je świadczących.

Kolejnym istotnym elementem nowego podejścia do ochrony cyberprzestrzeni RP jest propozycja **tworzenia Klastrów Bezpieczeństwa**, polegająca na dostosowaniu konfiguracji sieci do wymogów bezpieczeństwa.

[28] CERT.GOV.PL podpisuje umowy z operatorami infrastruktury krytycznej, którzy są zainteresowani wymianą informacji o incydentach.



Rysunek 5 Klaster bezpieczeństwa centralnej administracji rządowej

Główną ideą jest stworzenie dwustopniowego systemu zabezpieczeń rejestrów państwowych, systemów bankowych i regionalizacja ochrony cybernetycznej dla jednostek samorządowych i służb zespolonych. Rozwiązania takie są z powodzeniem stosowane na świecie i w NATO. Uporządkowany i zorganizowany dostęp do ogólnodostępnej sieci Internet daje możliwość ochrony istotnych danych i serwisów rządowych przed działaniami cyberprzestępców. Rozwiązanie takie nie eliminuje zagrożeń, jednak znacznie ogranicza ich potencjalne skutki.

4.6. Organizacja systemu oceny ryzyk

Z punktu widzenia centralnego organu odpowiedzialnego za ochronę cyberprzestrzeni konieczna jest wiedza, jak incydent powstały w jednym z podmiotów oddziałuje lub może oddziaływać na inne podmioty i jakie skutki wywołuje w skali całego kraju. System oceny ryzyk musi posiadać zdolność do prezentowania organom decyzyjnym stanu ryzyk w czasie rzeczywistym. System musi uwzględniać zarówno zagrożenia potencjalne, jak i zagrożenia zmaterializowane, siatkę powiązań skutków incydentu pomiędzy poszczególnymi podmiotami oraz siłę oddziaływania incydentu w jednym z podmiotów na inne podmioty.

Za punkt wyjścia do opracowania takiego systemu może być przyjęty produkt projektu pod nazwą: *System ewaluacji zagrożeń bezpieczeństwa cyberprzestrzeni RP na potrzeby systemu zarządzania bezpieczeństwem narodowym Rzeczypospolitej Polskiej*, prowadzonego w NCBR przez konsorcjum, w którym rolę lidera pełnił Wojskowy Instytut Łączności.

Dla proponowanego systemu niezbędne jest ustanowienie punktu równowagi pomiędzy szczegółowością, a uogólnieniem, tak aby istniała możliwość podejmowania skutecznych decyzji na poziomie krajowym.

Jednocześnie w każdym z podmiotów wchodzących w skład krajowego systemu cyberbezpieczeństwa powinna być prowadzone zarządzanie ryzykiem z uwzględnieniem Polskiej Normy PN ISO/IEC 27005. Szacowanie ryzyka powinno stanowić podstawę do wdrażania zabezpieczeń. Należy przy tym wskazać, że zarządzanie ryzykiem musi być procesem ciągłym, uwzględniającym dynamikę, jaką cechują się zjawiska zachodzące w cyberprzestrzeni. Planuje się, że analizy ryzyka prowadzone będą przez podmioty uczestniczące w procesie ochrony cyberprzestrzeni ale jednocześnie przewiduje się wykorzystanie (zlecanie) analiz z ośrodków naukowych i specjalistycznych firm zajmujących się tą problematyką. Istotnym elementem wzmacniającym poziom świadomości będą fora wymiany informacji i konsultacji organizowane minimum raz w roku. Wnioski wypracowywane w procesie oceny ryzyk będą uwzględniane w procesie planowania prac naukowo-badawczych i badawczo rozwojowych, tak by minimalizować skutki zidentyfikowanych ryzyk.

4.7. Finansowanie

Oszacowanie finansowania wdrożenia, a następnie utrzymywania krajowego systemu cyberbezpieczeństwa jest przedsięwzięciem złożonym i ustalenie kosztów tego finansowania możliwe będzie dopiero po uszczegółowieniu Strategii. Niewątpliwie takie uszczegółowienie zawarte będzie w ustawie o krajowym systemie cyberbezpieczeństwa i aktach wykonawczych do tej ustawy. Na etapie niniejszych założeń możliwe jest jedynie wskazanie źródeł tego finansowania. Źródłami tymi będą:

1. budżet państwa, a szczególności:
    1) plan finansowy Ministerstwa Cyfryzacji – w zakresie związanym z organizacją systemu cyberbezpieczeństwa, a następnie z utrzymywaniem centralnych struktur tego systemu,
    2) plany finansowe jednostek administracji państwowej (w tym jednostek samorządu terytorialnego) – w zakresie organizacji, a następnie utrzymywania komponentów krajowego systemu cyberbezpieczeństwa zlokalizowanych w tych jednostkach,

3) dofinansowanie prac badawczych i rozwojowych w zakresie cyberbezpieczeństwa, głównie poprzez Narodowe Centrum Badań i Rozwoju,

4) dofinansowanie podmiotów publicznych na podstawie art. 12c ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne,

2. projekty posiadające dofinansowanie z UE (w miarę pojawienia się takich możliwości),
3. budżety podmiotów prywatnych zobowiązanych do określonych działań przepisami ustawy.

4.8. Przewidywane korzyści

Wdrożenie Strategii Cyberbezpieczeństwa RP powinno skutkować nie tylko zapewnieniem wymaganego poziomu zabezpieczeń przed atakami cyberterrorystów i cyberprzestępców ale powinno również wpłynąć pozytywnie na aspekty gospodarcze kraju.

Specjalizacja narodowa – obszar cyberbezpieczeństwa staje się coraz bardziej doceniany w krajach o zwiększającym się wykorzystaniu usług świadczonych drogą elektroniczną. Potencjał krajowych wytwórców oprogramowania może być podstawą do rozwoju sektora cyberbezpieczeństwa, tym bardziej że obecnie znaczna część oprogramowania jest dostarczana przez rodzime firmy. Budowa uporządkowanego kompetencyjnie i proceduralnie środowiska bezpieczeństwa będzie wymagała wdrożenia nowych narzędzi monitorowania, zapobiegania i przeciwdziałania w cyberprzestrzeni, co powinno być paliwem **innowacyjności** sektora cyberbezpieczeństwa. Taką stymulację procesów wytwórczych należy wykorzystać nie tylko dla rynku krajowego ale również wypracować mechanizmy pozwalające eksportować wytworzone produkty na rynek Europejski i rynki światowe tak, by były one **konkurencyjne** pod względem jakości i ceny. Oznacza to stosowne klasyfikowanie produktów, które mogą być stosowane tylko w kraju i tych na rynki zewnętrzne.

Wdrożenie Strategii Cyberbezpieczeństwa RP to również **inwestycje** w infrastrukturę teleinformatyczną i środowisko badawcze pozwalające testować nowe rozwiązania i ich skuteczność w semi-realnym układzie. Dostosowanie konfiguracji sieci do wymagań bezpieczeństwa od szczebla województw w dół będzie skutkowało efektywniejszym wykorzystaniem infrastruktury telekomunikacyjnej szczególnie tej, w której udziały mają samorządy, a która obecnie nie zawsze wykorzystywana jest optymalnie. Uporządkowanie struktur odpowiedzialnych za cyberbezpieczeństwo na wszystkich szczeblach organizacyjnych, zorganizowanie procesu szkoleń testów i treningów to z jednej strony wzrost zatrudnienia w tym sektorze, ale z drugiej oszczędności wynikające ze skuteczniejszego mechanizmu wykrywania, przeciwdziałania i minimalizacji skutków cyberprzestępczości. W procesie uwzględnić należy również ośrodki specjalizujące się w ocenie ryzyk oraz ośrodki będące centrami eksperckimi, których rozwój powinien wspierać krajowe struktury reagowania i przeciwdziałania incydentom komputerowym.

5. Harmonogram opracowania Strategii Cyberbezpieczeństwa RP

Celem niniejszego dokumentu jest wypracowanie zdolności państwa do przeciwdziałania zagrożeniom pochodzącym z cyberprzestrzeni, które mogłyby spowodować szkody dla jego interesów politycznych i gospodarczych, a także interesów obywateli i przedsiębiorców. Mając na uwadze, że cyberbezpieczeństwo musi być wbudowane w procesy wszystkich interesariuszy istnieje potrzeba skonsultowania dokumentu w szerokim gronie. Ważne jest aby uzyskać powszechny konsensus wobec proponowanych rozwiązań, albowiem tyko w takim przypadku uzyska się synergię działań cząstkowych.

5.1. Tryb opracowania

Etap uzgodnień wewnętrznych

Przyjęto, że dokument strategii zostanie przygotowany według uzgodnionego na posiedzeniach Grupy Eksperckiej ds. Cyberbezpieczeństwa[29] harmonogramu. Poszczególne rozdziały i działania składające się na strukturę dokumentu będą omawiane na posiedzeniach Grupy Eksperckiej po to, by zapewnić maksymalną spójność działań na wszystkich szczeblach administracji rządowej. Strategia Cyberbezpieczeństwa RP będzie również omawiana i uzgadniana na posiedzeniach Zespołu Zadaniowego ds. Cyberbezpieczeństwa.

Etap konsultacji publicznych

Uzgodniony wewnętrznie projekt strategii będzie procedowany, zgodnie z Regulaminem Prac Rady Ministrów, wg. trybu postępowania z projektami dokumentów rządowych i przyjęty uchwałą Rady Ministrów.

W ramach konsultacji publicznych projekt strategii będzie przekazany do uzgodnień z interesariuszami spoza administracji publicznej (operatorzy telekomunikacyjni, fundacje, operatorzy IK i inne kluczowe podmioty).

Etap uzgodnień międzyresortowych

Wypracowany w ramach konsultacji publicznych i zatwierdzony przez Komitet Rady Ministrów ds. Cyfryzacji, projekt Strategii zostanie następnie przekazany do uzgodnień międzyresortowych.

Dalsza ścieżka legislacyjna

Po uwzględnieniu uwag resortów, projekt Strategii zostanie przedłożony pod obrady Stałego Komitetu Rady Ministrów w celu zatwierdzenia. Ostatnim etapem procesu legislacyjnego jest przyjęcie projektu przez Radę Ministrów i opublikowanie tekstu Strategii w Dzienniku Urzędowym „Monitor Polski”.

5.2. Harmonogram opracowania Strategii Cyberbezpieczeństwa RP

Lp.	Zadanie	Realizator/ Współrealizator	Termin realizacji
1.	Przygotowanie projektu koncepcji Strategii Cyberbezpieczeństwa RP	DSI-WPBC	do 16 lutego 2016 r.
2.	Przedstawienie zarysu koncepcji Strategii Cyberbezpieczeństwa RP na posiedzeniu	Grupa Ekspercka ds. Cyberbezpieczeństwa	19 lutego 2016 r.

[29] nieformalny zespół wspomagający pracę Zespołu ds. Bezpieczeństwa Cyberprzestrzeni Komitetu Rady Ministrów ds. Cyfryzacji

Lp.	Zadanie	Realizator/ Współrealizator	Termin realizacji
	Grupy Eksperckiej ds. Cyberbezpieczeństwa		
3.	Rozesłanie członkom Grupy Eksperckiej ds. Cyberbezpieczeństwa projektu koncepcji Strategii Cyberbezpieczeństwa RP w celu uzgodnienia	DSI-WPBC	19 lutego 2016 r.
4.	Opracowanie koncepcji Strategii Cyberbezpieczeństwa RP uwzględniającej uwagi Grupy Eksperckiej ds. Cyberbezpieczeństwa – publikacja do konsultacji w dniu 23.02.	DSI-WPBC	do 22 lutego 2016 r.
5.	Zaprezentowanie koncepcji Strategii Cyberbezpieczeństwa RP przez kierownictwo Ministerstwa Cyfryzacji na konferencji organizowanej przez Computerworld – „Państwo 2.0”	Doradca Minister Cyfryzacji	25 lutego 2016 r., Konferencja „Państwo 2.0”, Warszawa
6.	Konsultacje i uzgodnienia projektu Strategii – spotkanie nr I	Grupa Ekspercka ds. Cyberbezpieczeństwa	26 lutego 2016 r.
7.	Opracowanie projektu Strategii uwzględniającej uwagi Grupy Eksperckiej ds. Cyberbezpieczeństwa	Grupa Ekspercka ds. Cyberbezpieczeństwa	do 2 marca 2016 r.
8.	Konsultacje i uzgodnienia projektu Strategii – spotkanie nr I	Zespół Zadaniowy ds. Bezpieczeństwa Cyberprzestrzeni RP	3 marca 2016 r.
9.	Konsultacje i uzgodnienia projektu Strategii – spotkanie nr II	Grupa Ekspercka ds. Cyberbezpieczeństwa	4 marca 2016 r.
10.	Opracowanie uwag zgłoszonych przez Grupę Ekspercką ds. Cyberbezpieczeństwa	DC	do 10 marca 2016 r.
11.	Konsultacje i uzgodnienia projektu Strategii – spotkanie nr III	Grupa Ekspercka ds. Cyberbezpieczeństwa	11 marca 2016 r.
12.	Opracowanie uwag zgłoszonych przez Grupę Ekspercką ds. Cyberbezpieczeństwa	DC	do 16 marca 2016 r.
13.	Konsultacje i uzgodnienia projektu Strategii – spotkanie nr II	Zespół Zadaniowy ds. Bezpieczeństwa Cyberprzestrzeni RP	16 marca 2016 r.
14.	Konsultacje i uzgodnienia projektu Strategii – spotkanie nr IV	Grupa Ekspercka ds. Cyberbezpieczeństwa	18 marca 2016 r.

Lp.	Zadanie	Realizator/ Współrealizator	Termin realizacji
15.	Opracowanie uwag zgłoszonych przez Grupę Ekspercką ds. Cyberbezpieczeństwa	DC	do 24 marca 2016 r.
16.	Konsultacje i uzgodnienia projektu Strategii – spotkanie nr V	Grupa Ekspercka ds. Cyberbezpieczeństwa	25 marca 2016 r.
17.	Opracowanie uwag zgłoszonych przez Grupę Ekspercką ds. Cyberbezpieczeństwa	DC	do 30 marca 2016 r.
18.	Konsultacje i uzgodnienia projektu Strategii – spotkanie nr III	Zespół Zadaniowy ds. Bezpieczeństwa Cyberprzestrzeni RP	30 marca 2016 r.
19.	Konsultacje i uzgodnienia projektu Strategii –spotkanie nr VI	Grupa Ekspercka ds. Cyberbezpieczeństwa	1 kwietnia 2016 r.
20.	Opracowanie uwag zgłoszonych przez Grupę Ekspercką ds. Cyberbezpieczeństwa	DC	do 7 kwietnia 2016 r.
21.	Konsultacje i uzgodnienia projektu Strategii – spotkanie nr VII	Grupa Ekspercka ds. Cyberbezpieczeństwa	8 kwietnia 2016 r.
22.	Opracowanie uwag zgłoszonych przez Grupę Ekspercką ds. Cyberbezpieczeństwa	DC	do 13 kwietnia 2016 r.
23.	Konsultacje i uzgodnienia projektu Strategii – spotkanie nr IV	Zespół Zadaniowy ds. Bezpieczeństwa Cyberprzestrzeni RP	14 kwietnia 2016 r.
24.	Konsultacje i uzgodnienia projektu Strategii – spotkanie nr VIII	Grupa Ekspercka ds. Cyberbezpieczeństwa	15 kwietnia 2016 r.
25.	Opracowanie uwag zgłoszonych przez Grupę Ekspercką ds. Cyberbezpieczeństwa	DC	do 21 kwietnia 2016 r.
26.	Konsultacje i uzgodnienia projektu Strategii – spotkanie nr IX	Grupa Ekspercka ds. Cyberbezpieczeństwa	22 kwietnia 2016 r.
27.	Opracowanie uwag zgłoszonych przez Grupę Ekspercką ds. Cyberbezpieczeństwa	DC	do 28 kwietnia 2016 r.
28.	Konsultacje i uzgodnienia projektu Strategii – spotkanie nr V	Zespół Zadaniowy ds. Bezpieczeństwa Cyberprzestrzeni RP	27 kwietnia 2016 r.
29.	Opracowanie ostatecznego projektu Strategii	DC	do 4 maja 2016 r.

Lp.	Zadanie	Realizator/ Współrealizator	Termin realizacji
30.	Uzgodnienia projektu Strategii z członkami Grupy Eksperckiej ds. Cyberbezpieczeństwa	DC	do 10 maja 2016 r.
31.	Przedłożenie projektu Strategii do zatwierdzenia przez Zespół Zadaniowy ds. Cyberbezpieczeństwa	Zespół Zadaniowy ds. Bezpieczeństwa Cyberprzestrzeni RP	11 maja 2016 r.
32.	Zaprezentowanie i omówienie projektu Strategii	Kierownictwo Ministerstwa Cyfryzacji	19 maja 2016 r. Konferencja „CyberGov 2016”, Warszawa
33.	Uzgodnienia wewnętrzne projektu Strategii	DC/komórki MC	do 9 czerwca 2016 r.
34.	Opracowanie uwag zgłoszonych w ramach uzgodnień wewnętrznych	DC	do 15 czerwca 2016 r.
35.	Konsultacje publiczne projektu Strategii	Ministerstwo Cyfryzacji / podmioty publiczne z branży IT (stowarzyszenia, fundacje, izby gospodarcze)	do 30 czerwca 2016 r.
36.	Opracowanie uwag zgłoszonych w ramach konsultacji publicznych	DC	do 8 lipca 2016 r.
37.	Strategia działań koalicyjnych w cyberprzestrzeni w kontekście wzmocnienia wschodniej flanki Sojuszu Północnoatlantyckiego	Ministerstwo Obrony Narodowej /Ministerstwo Cyfryzacji	8-9 lipca 2016 r., Szczyt NATO, Warszawa
38.	Przedłożenie projektu Strategii do zatwierdzenia przez Komitet Rady Ministrów ds. Cyfryzacji	DC/ KRMC	do 27 lipca 2016 r.
39.	Uzgodnienia międzyresortowe projektu Strategii	Ministerstwo Cyfryzacji/ międzyresort	do 29 lipca 2016 r.
40.	Opracowanie uwag zgłoszonych w ramach uzgodnień międzyresortowych	DC	do 11 sierpnia 2016 r.
41.	Opracowanie ostatecznej wersji Strategii	DC	do 31 sierpnia 2016 r.
42.	Przedłożenie Strategii do zatwierdzenia przez Radę Ministrów	Ministerstwo Cyfryzacji/ Rada Ministrów	do 10 września 2016 r.

Lp.	Zadanie	Realizator/ Współrealizator	Termin realizacji
43.	Opublikowanie tekstu Strategii w Dzienniku Urzędowym „Monitor Polski”	Ministerstwo Cyfryzacji/ Rada Ministrów/ Rządowe Centrum Legislacji	do 30 września 2016 r.

Załącznik nr 1 – Wykaz aktów prawnych jednostkowo odnoszących się do kwestii cyberbezpieczeństwa

Przepisy określające minimalne wymagania z zakresu bezpieczeństwa teleinformatycznego w administracji publicznej:

1. ustawa z dnia 17 lutego 2005r. *o informatyzacji działalności podmiotów realizujących zadania publiczne*[1];
2. rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012r. *w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych*[2]

Przepisy określające wymagania w zakresie zarządzania bezpieczeństwem sieci i informacji systemów teleinformatycznych (dotyczące zarówno podmiotów prywatnych jak i jednostek sektora finansów publicznych):

1. ustawa z dnia 6 czerwca 1997r. *Kodeks karny*
2. ustawa z dnia 29 sierpnia 1997r. *o ochronie danych osobowych*[4]
3. ustawa z dnia 27 sierpnia 2009r. *o finansach publicznych*[5]
4. ustawa z dnia 29 września 1994r. *o rachunkowości*[6]
5. ustawa z dnia 6 września 2001r. *o dostępie do informacji publicznej*[7]
6. ustawa z dnia 15 kwietnia 2011r. *o systemie informacji oświatowej*[8]
7. ustawa z dnia 28 kwietnia 2011r. *o systemie informacji w ochronie zdrowia*[9]
8. ustawa z dnia 14 lipca 1983r. *o narodowym zasobie archiwalnym i archiwach*[10]
9. ustawa z dnia 29 sierpnia 199 r. *Prawo bankowe*[11]
10. ustawa z dnia 18 września 2001r. *o podpisie elektronicznym*[12]
11. rozporządzenie PE i Rady z dnia 23 lipca 2014 r. *w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym*[13]
12. ustawa z dnia 18 lipca 2002r. *o świadczeniu usług drogą elektroniczną*[14]
13. ustawa z dnia 29 czerwca 1995 r. *o statystyce publicznej*[15]
14. ustawa z dnia 16 kwietnia 1993 r. *o zwalczaniu nieuczciwej konkurencji*[16]

[1] Dz. U. z 2014 r., Nr 1114 j.t.
[2] Dz. U. z 2012 r. Nr 526 z późn. zm.
[4] Dz. U. z 2014 r. Nr 1182 j. t. z późn. zm.
[5] Dz. U. z 2013 r. Nr 885 j.t.
[6] Dz. U. z 2013 r. Nr 330 j.t. z późn. zm.
[7] Dz. U. z 2014 r. Nr 782 j.t. z późn. zm.
[8] Dz. U. z 2015 r. Nr 45 j.t. z późn. zm.
[9] Dz. U. z 2015 r. Nr 636 j.t.
[10] Dz. U. z 2011 r. Nr 123 poz. 698 j.t. z późn. zm.
[11] Dz. U. z 2015 r. Nr 128 j.t.
[12] Dz. U. z 2013 r. Nr 262 j.t.
[13] Nr 910/2014 – Dz. U. L 257 z 2014 r.
[14] Dz.U.2013.1422 j.t.
[15] Dz. U. z 2012 r. Nr 591 j.t. z późn. zm.
[16] Dz. U. z 2003 r. Nr 153 poz. 1503 j.t. z późn. zm.

15. ustawa z dnia 29 stycznia 2004 r. Prawo zamówień publicznych[30]

Przepisy odnoszące się do rozwiązań instytucjonalnych związanych z bezpieczeństwem teleinformatycznym:

1. Ustawa z dnia 16 lipca 2004r. *Prawo telekomunikacyjne*[18] - przepisy regulują m.in. kwestie wymagań bezpieczeństwa teleinformatycznego w sektorze telekomunikacji oraz warunki zgłaszania najważniejszych incydentów cybernetycznych w sieciach telekomunikacyjnych[19].
2. Ustawa z dnia 26 kwietnia 2007r. *o zarządzaniu kryzysowym*[21] - RCB przygotowuje m.in. Narodowy Program Ochrony Infrastruktury Krytycznej, oficjalnie przyjmowany przez Radę Ministrów.
3. Ustawa z dnia z dnia 24 maja 2002 r. *o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu*[31] - przepisy regulują zadania obu służb specjalnych, m.in. w zakresie ochrony przed zagrożeniami dla bezpieczeństwa Państwa.
4. Ustawa z dnia 30 kwietnia 2010 r. *o instytutach badawczych*[32] – przepisy regulują zakres kompetencji tego typu jednostek, w tym odnoszących się do zagadnień z zakresu obronności lub bezpieczeństwa publicznego
5. Ustawa z dnia 21 listopada 2008 r. *o służbie cywilnej*[33]określa m.in. zasady organizacji, funkcjonowania i rozwoju służby cywilnej, w tym kompetencje dyrektorów generalnych urzędów.
6. Rozporządzenie Prezesa Rady Ministrów z dnia 9 grudnia 2009 r. *w sprawie określenia stanowisk urzędniczych, wymaganych kwalifikacji zawodowych, stopni służbowych urzędników służby cywilnej, mnożników do ustalania wynagrodzenia oraz szczegółowych zasad ustalania i wypłacania innych świadczeń przysługujących członkom korpusu służby cywilnej*[34].
7. Ustawa z dnia 30 kwietnia 2010 r. *o Narodowym Centrum Badań i Rozwoju*[35], określa zadania tej instytucji z zakresu polityki naukowej, naukowo-technicznej i innowacyjnej państwa
8. Kwestii instytucjonalnych oraz wymagań prawnych związanych z bezpieczeństwem cyberprzestrzeni, dotyczy projekt dyrektywy w sprawie środków mających na celu zapewnienie wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji w obrębie Unii (dyrektywa NIS).

Ponadto, w Polsce, funkcjonują dokumenty o charakterze strategicznym, tj.

1. *Polityka Ochrony Cyberprzestrzeni RP;*
2. *Strategia Bezpieczeństwa Narodowego;*
3. *Doktryna Cyberbezpieczeństwa RP*.

[30] Dz. U. z 2015 r. Nr 2164 j. t.

[18] Dz. U. z 2004r. Nr 171 poz. 1800 z późn. zm.

[19] Do dnia 30 kwietnia każdego roku Prezes UKE przekazuje sprawozdania z działalności do Ministra Administracji i Cyfryzacji.

[21] Dz. U. z 2013 r. Nr 1166 j.t.

[31] Dz. U. z 2015 r. Nr 1929 j.t.

[32] Dz. U. z 2015 r. Nr 1095 j.t.

[33] Dz. U. z 2014 r. Nr 1111 j.t.

[34] Dz. U. z 2009. Nr 211 poz. 1630 z późn. zm.

[35] Dz. U. z 2014 r. Nr 1788.

Załącznik nr 2 Przykładowy scenariusz reagowania na incydent

Zdarzenie Kategorii [1]: Ograniczenie lub zaprzestanie realizacji istotnych funkcji państwa w sektorach kluczowych (sektor energetyczny, sektor bankowy, sektor transportowy, sektor zdrowia, produkcja i dystrybucja wody pitnej, sektor telekomunikacyjny, infrastruktury cyfrowej);

[1.1]Sektor elektroenergetyczny

[1.1.3]Skutek lokalny

Incydent: Wprowadzenie malware do systemu sterowania Głównego Punktu Zasilania (GPZ);

Skutek: Brak możliwości zasilania linii średniego napięcia (ŚN) na obszarze powiatu;

Reakcja:

- Powiadomienie odbiorców energii elektrycznej;
- Zaatakowany GPZ powiadamia o incydencie CSIRT sektora energetyki;
- CSIRT sektora energetyki powiadamia wszystkie GPZ o możliwości zainfekowania systemu sterowania;
- LZR powiadomionych GPZ przeprowadzają inspekcję systemów sterowania;
- Zaatakowany GPZ powiadomienia o incydencie Krajową Dyspozycję Mocy (KDM);
- Zaatakowany GPZ powiadomienia o incydencie Centrum Operacyjno-Analityczne Rządowego Centrum Bezpieczeństwa (COA RCB);
- Wykonanie przez Lokalny Zespół Reagowania (LZR) procedury odtworzenia systemu sterowania z kopii zapasowej.

Eskalacja incydentu na duży obszar

[1.1.2]Skutek w dużej skali

Incydent: Wprowadzenie malware do systemu sterowania kilku GPZ;

Skutek: Brak możliwości zasilania linii ŚN na obszarze województwa;

Reakcja:

- Zaatakowane GPZ postępują zgodnie z [1.1.3];
- KDM powiadomienia o incydencie COA RCB;
- RCB podejmuje działania według właściwego planu reagowania kryzysowego;
- KDM aktywizuje CSIRT sektora energetycznego z zadaniem rozwiązania problemu;
- CSIRT sektora energetycznego zawiadamia CSIRT Narodowy.

Eskalacja incydentu na skalę kraju

[1.1.1] Skutek w skali całego kraju

Incydent: W wyniku zdjęcia obciążenia w wyniku awarii w wielu GPZ następuje awaryjne wyłączenie dużej elektrowni;

Skutek: Brak zasilania na obszarze kilku województw;

Reakcja: Incydent pierwotnie wywołany przez zdarzenie o charakterze incydentu bezpieczeństwa w systemie teleinformatycznym GPZ przekształca się w incydent w infrastrukturze krytycznej, zatem uruchomiony zostaje za pośrednictwem RCB plan reagowania kryzysowego.

Przywrócenie stanu normalnego – przywrócenie pracy we wszystkich GPZ

Działania następcze:

- Analiza przypadku przez zespół CSIRT sektora energetycznego, z ewentualnym udziałem Narodowego Centrum Cyberbezpieczeństwa, mających na celu ustalenie łańcucha wydarzeń, które spowodowały incydent;
- Wypracowanie działań naprawczych i korygujących.