Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji

Warszawa, dn. 14.08.2019 r.
KIGEiT/2549/08/2019

Sz. P. Marek Zagórski
Minister
Ministerstwo Cyfryzacji
ul. Królewska 27
00-060 Warszawa

Szanowny Panie Ministrze.

Działając w imieniu Krajowej Izby Gospodarczej Elektroniki i Telekomunikacji (dalej „***Izba***" lub „***KIGEiT***"), w związku z przekazanym projektem uchwały Rady Ministrów w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019 – 2024, przesyłam poniższe propozycje uzupełnień do ww. projektu.

Uzupełnienia wstawiono kolorem czerwonym czcionki. Dodatkowo zostały one także naniesione w tekście Załącznika (w trybie recenzji).

1. **W p.1 Wstęp – przesłanki do działań zwiększających cyberbezpieczeństwo**

Proponujemy wprowadzenie odnośnika do infrastruktury krytycznej już we wprowadzeniu. Ponadto w stopce tego punktu proponujemy wprowadzić następujące uzupełnienie:

„Przez cyberprzestrzeń rozumie się przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne i elektroniczne, określone w art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. Nr 64, poz. 565, z późn. zm.2), wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami – art. 1 ust. 1b ustawy z dnia 30 sierpnia 2011 r. o zmianie ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw (Dz. U. Nr 222 z 2011 r., poz. 1323)."

2. **W p. 2 Kontekst strategiczny cyberbezpieczeństwa w Rzeczypospolitej Polskiej (ostatni akapit)**

„Podejmując działania mające na celu wdrożenie *Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019 – 2024*, rząd będzie w pełni ~~respektował~~ gwarantował prawo do prywatności oraz stał na stanowisku, że wolny i otwarty Internet jest istotnym elementem funkcjonowania współczesnego społeczeństwa."

Zwracamy uwagę, że Państwo powinno nie tylko respektować, ale powinno gwarantować prawo do prywatności.

3. **W p. 4.1. Wizja (zdanie 3-cie)**

„Działania uwzględniają systemowe rozwiązania organizacyjne, operacyjne, technologiczne, prawne, kreowanie postaw społecznych, prowadzenie badań naukowych, tak aby zapewnić spełnienie wysokich standardów cyberbezpieczeństwa w obszarze wsparcia/utrzymania sieci, oprogramowania, urządzeń i usług ~~cyfrowych~~."

ul. Stępińska 22/30, 00-739 Warszawa, tel.: +48 22 8510309, 8406522, e-mail: kigeit@kigeit.org.pl
http://www.kigeit.org.pl; NIP 526-00-29-121 Konto: BGŻ BNP Paribas O/Warszawa nr: 52160013740003005222791001

Wizja powinna uwzględniać również fakt, że zagrożenia wynikające z działalności kryminalnej mają zasadniczo różny charakter, skalę i poziom zaawansowania technologicznego od zagrożeń wynikających z ataków dywersyjnych i militarnych przeprowadzanych przez jednostki organizacyjne korzystające ze wsparcia technologicznego, finansowego i ochrony prawnej państwa. To oznacza, że te typy zagrożeń powinny być uwzględnione odrębnie zarówno w Krajowym Systemie Cyberbezpieczeństwa jak i w ramach zmian, jakich wymaga dyrektywa NIS.

4. **W p. 4 Wizja, cel główny, cele szczegółowe (pp.4.3 , 2-gi akapit)**

„Cel szczegółowy 2. Stymulowanie podniesienia poziomu odporności ~~systemów informacyjnych~~ cyberprzestrzeni administracji publicznej i sektora prywatnego oraz osiągnięcie zdolności do skutecznego zapobiegania incydentom."

5. **W p. 5.1. Wdrożenie i ocena funkcjonowania przepisów o Krajowym Systemie Cyberbezpieczeństwa (akapit 2-gi, zdanie 2-gie)**

„Doświadczenia związane ze stosowaniem przepisów prawa w tym zakresie będą również przesłanką do wnioskowania na poziomie Unii Europejskiej w sprawie zmiany przepisów samej Dyrektywy NIS, tak aby zwiększyć skuteczność jej oddziaływania – jednym z obszarów wymagających zmian zwiększających efektywność Dyrektywy NIS będzie doprecyzowanie obowiązków dostawców usług cyfrowych, w szczególności świadczących usługi publicznych chmur obliczeniowych, które w coraz większym stopniu będą wykorzystywane jako model przetwarzania danych dla usług kluczowych."

oraz (akapit 4-ty, zdanie 2-gie)

„Niezbędne będzie również podjęcie prac legislacyjnych mających na celu uregulowanie obszaru z zakresu wytwarzania, posiadania, pozyskiwania oraz wykorzystywania specjalistycznych narzędzi podwójnego zastosowania do prowadzenia działań defensywnych~~o-i~~ofensywnych w cyberprzestrzeni."

Sugerujemy, że legislacja w dziedzinie narzędzi podwójnego zastosowania powinna odbyć się na poziomie ogólnoeuropejskim (tak jak na poziomie europejskim regulowany jest eksport dóbr podwójnego zastosowania). Legislacja zagrożeń o charakterze militarnym i dywersyjnym powinna być spójna w ramach systemu cyberobrony NATO.

oraz (akapit 6-ty, zdanie 1-wsze)

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

6. **W p. 5.2 Podniesienie efektywności funkcjonowania Krajowego Systemu Cyberbezpieczeństwa (2-gi akapit)**

„Organy właściwe, odpowiedzialne za sprawowanie nadzoru ~~w zakresie systemów teleinformatycznych~~ nad bezpieczeństwem cyberprzestrzeni w sektorach, w których świadczone są usługi kluczowe i usługi cyfrowe, będą prowadziły działania mające wspierać operatorów i dostawców w zapewnieniu bezpieczeństwa świadczonych przez nich usług. Organy właściwe będą mogły w tym celu wydawać zalecenia organizacyjne i techniczne, a także udostępniać narzędzia i wiedzę dotyczącą najlepszych praktyk sektorowych i ponadsektorowych podnoszących cyberbezpieczeństwo."

Do tego akapitu nasuwa się pytanie o procedurę w jakiej organy te będą wyznaczone? Ponadto sugerujemy wypracowanie definicji/katalogu usług kluczowych.

oraz (4-ty akapit)

„Rząd w ramach współpracy administracji rządowej z administracją samorządową będzie rekomendował i działał na rzecz jednostek samorządu terytorialnego w zakresie podnoszenia kompetencji w doborze, wdrażaniu i utrzymaniu środków technicznych zwiększających cyberbezpieczeństwo, w tym korzystania z nowoczesnych i bezpiecznych modeli przetwarzania w chmurach obliczeniowych, tworzenia bezpiecznych aplikacji wykorzystujących technologie mikroelektroniczne oraz korzystania z bezpiecznych systemów mobilnych."

oraz (5-ty akapit, zdanie drugie)

„Standaryzacja i wymagania cyberbezpieczeństwa, opracowane i wykorzystywane przez administrację publiczną w ramach Narodowych Standardów Cyberbezpieczeństwa, powinny stać się także wyznacznikiem dobrych praktyk dla sektora prywatnego oraz dla obywateli."

W tym miejscu pojawia się pytanie, czy sektor prywatny automatycznie przyjmie/zaakceptuje standardy wprowadzone przez administrację publiczną? Opracowane standardy mogą stać się obligatoryjne tylko wtedy, gdy zostaną wprowadzone jako specyfikacje techniczne poprzez odpowiednie rozporządzenia. To wymaga również postawienia pytania o delegację ustawową do takich rozporządzeń i ich spójność w ramach systemu prawnego UE.

7. **W p. 5.3. Rozbudowa systemu wymiany informacji na potrzeby kierowania bezpieczeństwem narodowym**

„W celu usprawnienia zarządzania bezpieczeństwem, prowadzone będą działania mające na celu wymianę informacji i uzgadnianie reakcji, tak na poziomie strategicznym jak i poziomie operacyjnym, w szczególności pomiędzy podmiotami sferyą cywilneją, policją i służbami przeciwdziałającymi przestępczości oraz służbami odpowiadającymi za bezpieczeństwo wewnętrzne i obronność ~~i sferą wojskową~~. Niezbędna jest budowa odpornego na cyberzagrożenia systemu wymiany informacji dla potrzeb administracji publicznej wykorzystującego najnowocześniejsze technologie wymiany informacji, technologie mikroelektroniczne, uwzględniające konieczność wysokiej mobilności. System ten będzie wykorzystywany w różnych stanach nadzwyczajnych oraz stanach podwyższonej gotowości obronnej państwa."

8. **W p.5.4 Zwiększenie cyberbezpieczeństwa usług kluczowych i cyfrowych oraz infrastruktury krytycznej (1-szy akapit)**

„Technologie informatyczne (IT)[6] wykorzystywane przez operatorów usług kluczowych, dostawców usług cyfrowych, operatorów infrastruktury krytycznej (w tym operatorów telekomunikacyjnych), stanowią element krytyczny dla ciągłości działania państwa oraz zapewniania bezpieczeństwa obywatelom. Co więcej, bezpieczeństwo najważniejszych sektorów gospodarki, ze szczególnym uwzględnieniem sektora energii, zależy od zapewnienia niezakłóconego działania przemysłowych systemów sterowania (OT)[7]. Dlatego zapewnienie cyberbezpieczeństwa zarówno IT, jak i OT, w tym rozwiązań systemowych mających na celu podnoszenie bezpieczeństwa sprzętowych mikroelektronicznych komponentów systemów teleinformatycznych będzie traktowane przez Radę Ministrów jako priorytet. ..."

9. **W p. 5.5. Wypracowanie i wdrożenie metodyki szacowania ryzyka na poziomie krajowym**

W opinii KIGEiT jest to bardzo ważny punkt, dlatego w miarę możliwości postulujemy o jak najszybsze (jeszcze przed 2020) wypracowanie takiej metodyki i narzędzi.

10. W p. 5.6. Zwiększanie zdolności do zwalczania cyberprzestępczości, w tym cyberszpiegostwa i zdarzeń o charakterze terrorystycznym (1-szy akapit))

„W zakresie zwiększania zdolności do zwalczania cyberprzestępczości, w tym cyberszpiegostwa, zdarzeń o charakterze terrorystycznym (w tym działań o charakterze hybrydowym), ważne jest zapewnienie wsparcia dla operatorów usług kluczowych, dostawców usług cyfrowych oraz operatorów infrastruktury krytycznej w wykrywaniu oraz zwalczaniu incydentów we wszystkich ich fazach. W tym celu wymagana jest współpraca oraz koordynacja działań organów ścigania niezależnie od motywów, którymi kierują się sprawcy przestępstw, a szczególnie istotne znaczenie ma prawidłowe zabezpieczenie dowodów cyfrowych wykorzystujących bezpieczne krajowe rozwiązania mikroelektroniczne, oraz zapewnienie „łańcucha zaufania”.”

11. W p. 6.1. Opracowanie i wdrożenie Narodowych Standardów Cyberbezpieczeństwa oraz promowanie dobrych praktyk i zaleceń (1-szy akapit)

„Wykorzystując potencjał intelektualny ekspertów zgromadzonych w komitetach technicznych Polskiego Komitetu Normalizacyjnego, ośrodkach naukowych, akademickich i instytutach badawczych, instytutach Sieci Badawczej Łukasiewicz a także w zainteresowanych podmiotach publicznych i prywatnych, opracowane zostaną nowe standardy lub nastąpi przełożenie istniejących norm do ~~i~~ standardów ~~na konkretne rekomendacje w zakresie~~ definiujących zakres ich wdrażania.”

Ponadto dla systemów/produktów dla których istnieją odpowiednie normy międzynarodowe powinny być one bezpośrednio przyjęte poprzez ich umieszczenie w odpowiednich standardach (specyfikacjach technicznych). Sugerujemy zatem odpowiednią zmianę zapisu wskazującą, że: PKN we współpracy z ośrodkami akademickimi (…) powinien skatalogować istniejące normy międzynarodowe dla poszczególnych kategorii oraz przyjąć konkretne rekomendacje w zakresie ich wdrażania.

Proponujemy również w tym punkcie następujące uzupełnienie:

„W celu zwiększenia odporności systemów informacyjnych administracji publicznej na cyberzagrożenia niezbędne jest opracowanie Narodowych Standardów Cyberbezpieczeństwa jako zbioru wymagań organizacyjnych i technicznych dotyczących w szczególności bezpieczeństwa:

1) aplikacji,
2) urządzeń mobilnych,
3) stacji roboczych,
4) serwerów i sieci,
5) modeli chmur obliczeniowych,
6) wsparcia i utrzymania sieci/systemów teleinformatycznych”

12. W p. 6.2. Bezpieczeństwo łańcucha dostaw

Proponujemy dodać paragraf o konieczności weryfikowania poziomu zaufania sprzętu przeznaczonego do infrastruktury, uwzględniając jego podatność na cyberataki. Ponadto w akapicie 2-gim proponuje uzupełnienie:

„Ważnym elementem zapewnienia jakości w łańcuchu dostaw jest ocena i certyfikacja produktów i systemów (w szczególności oprogramowania, urządzeń i usług).”

Natomiast w ostatnim akapicie tego punktu:

„Efektem tych działań będzie uzyskanie na poziomie krajowym zdolności do wspierania ~~polskich~~ producentów, którzy uzyskując europejskie certyfikaty cyberbezpieczeństwa będą mogli skuteczniej konkurować na jednolitym rynku cyfrowym UE.”

13. **W p. 7.1. Rozbudowa zasobów przemysłowych i technologicznych na potrzeby cyberbezpieczeństwa (1-szy akapit)**

„Rząd Polski stawia sobie za cel inwestowanie w rozbudowę zasobów przemysłowych i technologicznych na potrzeby cyberbezpieczeństwa poprzez stwarzanie warunków dla rozwoju działających w Polsce przedsiębiorstw, ośrodków naukowo-badawczych, jak i *start-upów*, których przedmiotem działalności jest tworzenie nowych rozwiązań w obszarze cyberbezpieczeństwa. Jednym z priorytetów jest wzrost zdolności w obszarze projektowania i wytwarzania oprogramowania, projektowania i wytwarzania mikroelektronicznych przyrządów półprzewodnikowych w tym bezpiecznych układów scalonych, urządzeń i usług wykorzystywanych we wszystkich gałęziach polskiego przemysłu, zwiększających jego konkurencyjność."

14. KIGEiT proponuje rozważenie włączenia nowego elementu strategii jako punkt 7.5. skupionego na poprawie cyberbezpieczeństwa sektora Public Safety (bezpieczeństwa publicznego).

Z poważaniem.

Prezes Zarządu

Stefan Kamiński

Załącznik: Załącznik do uchwały Rady Ministrów „Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019 – 2024" z naniesionymi propozycjami w trybie rejestracji zmian.

Załącznik do uchwały nr ....
Rady Ministrów
z dnia ..... 2019 r. (poz. ...)

Strategia Cyberbezpieczeństwa

Rzeczypospolitej Polskiej

na lata 2019-2024

Ministerstwo
Cyfryzacji

Projekt z dnia 2 sierpnia 2019 r.

PROJEKT

UCHWAŁA NR ...

RADY MINISTRÓW

z dnia ..... 2019 r.

w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019 – 2024

Na podstawie art. 68 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. 1560) Rada Ministrów uchwala, co następuje:

§ 1. Przyjmuje się Strategię Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019 – 2024, zwaną dalej „Strategią Cyberbezpieczeństwa", stanowiącą załącznik do uchwały.

§ 2. Członkowie Rady Ministrów oraz organy i jednostki organizacyjne im podległe lub przez nich nadzorowane współpracują z ministrem właściwym do spraw informatyzacji przy realizacji Strategii Cyberbezpieczeństwa.

§ 3. Minister właściwy do spraw informatyzacji przedstawia Radzie Ministrów, w terminie do dnia 30 września danego roku, informację o realizacji Strategii Cyberbezpieczeństwa.

§ 4. Pierwszą informację o realizacji Strategii Cyberbezpieczeństwa minister właściwy do spraw informatyzacji przedstawi Radzie Ministrów w terminie sześciu miesięcy od dnia wejścia w życie niniejszej uchwały.

§ 5. Traci moc uchwała nr 52/2017 Rady Ministrów z dnia 27 kwietnia 2017 r. w sprawie Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017 – 2022.

§ 6. Uchwała wchodzi w życie z dniem 31 października 2019 r.

PREZES RADY MINISTRÓW

Spis treści

1. Wstęp – przesłanki do działań zwiększających cyberbezpieczeństwo

Z komentarzem [AP1]: Sugerujemy wprowadzenie odnośnika do infrastruktury krytycznej już we wprowadzeniu

Rozwój społeczny i gospodarczy w coraz większym stopniu zależny jest od szybkiego i nieskrępowanego dostępu do informacji oraz jej wykorzystania w zarządzaniu, produkcji, sektorze usług oraz sektorze publicznym. Dynamiczny rozwój systemów informacyjnych, a także zwiększanie wydajności centrów przetwarzania danych, służą rozwojowi gospodarki narodowej, w szczególności w obszarze komunikacji, handlu, transportu czy też usług finansowych. Z wykorzystaniem technologii cyfrowych tworzących cyberprzestrzeń[1] tworzone są i kształtowane relacje społeczne, a usługi w sieci Internet stały się narzędziem do wpływania na zachowania grup społecznych, a także oddziaływania w sferze politycznej.

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

Ochrona systemów informacyjnych oraz przetwarzanych w nich informacji jest wyzwaniem dla wszystkich podmiotów tworzących krajowy system cyberbezpieczeństwa, a więc podmiotów gospodarczych świadczących usługi przy wykorzystaniu systemów teleinformatycznych, użytkowników cyberprzestrzeni, organów władzy publicznej, organów odpowiedzialnych za bezpieczeństwo narodowe, a także wyspecjalizowanych podmiotów zajmujących się cyberbezpieczeństwem w sferze operacyjnej. Jest to tym istotniejsze, iż Polska jest ściśle powiązana z innymi państwami poprzez współpracę międzynarodową w ramach takich organizacji jak Unia Europejska, Organizacja Traktatu Północnoatlantyckiego (NATO), Organizacja Narodów Zjednoczonych czy Organizacja Bezpieczeństwa i Współpracy w Europie. Współpraca ta odgrywa istotną rolę w reagowaniu na zwiększającą się liczbę incydentów powodowanych nielegalnymi działaniami w cyberprzestrzeni, powodujących rosnące rokrocznie straty materialne i wizerunkowe. W działaniach tych uczestniczą pojedyncze osoby, zorganizowane grupy przestępcze oraz grupy sponsorowane przez instytucje rządowe i siły zbrojne państw prowadzących ofensywne działania w cyberprzestrzeni, ukierunkowane w szczególności na cyberszpiegostwo oraz rozpoznanie zdolności obronnych innych państw.

---

[1] Przez cyberprzestrzeń rozumie się przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne i elektroniczne, określone w art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. Nr 64, poz. 565, z późn. zm.2), wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami – art. 1 ust. 1b ustawy z dnia 30 sierpnia 2011 r. o zmianie ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw (Dz. U. Nr 222 z 2011 r., poz. 1323).

2. Kontekst strategiczny cyberbezpieczeństwa w Rzeczypospolitej Polskiej

Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019 – 2024 jest kontynuacją i rozszerzeniem działań, podejmowanych przez administrację rządową, mających na celu podniesienie poziomu cyberbezpieczeństwa w RP. Poprzednie działania obejmowały wejście w życie ustawy z dnia 5 lipca 2018 o krajowym systemie cyberbezpieczeństwa[2] oraz przyjęcie przez rząd:

- w roku 2013 *Polityki Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej*
- w roku 2017 *Krajowych Ramach Polityki Cyberbezpieczeństwa Rzeczpospolitej Polski na lata 2017–2022.*

Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019 – 2024 zastępuje *Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczpospolitej Polski na lata 2017–2022 przyjęte uchwałą nr 52/2017 Rady Ministrów z dnia 27 kwietnia 2017 r. w sprawie Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017 – 2022.*

Zamierzeniem niniejszego dokumentu jest określenie celów strategicznych oraz odpowiednich środków politycznych i regulacyjnych, mających na celu uzyskanie wysokiego poziomu cyberbezpieczeństwa – czyli przede wszystkim odporności systemów informacyjnych, operatorów usług kluczowych, operatorów infrastruktury krytycznej, dostawców usług cyfrowych oraz administracji publicznej na incydenty w cyberprzestrzeni, a także zwiększyć poziom ochrony informacji w systemach informacyjnych poprzez standaryzację zabezpieczeń. Realizacja celów strategicznych ma również wpływać na podniesienie bezpieczeństwa narodowego, zwiększenie skuteczności organów ścigania i wymiaru sprawiedliwości w wykrywaniu i zwalczaniu cyberprzestępstw oraz działań o charakterze terrorystycznym i szpiegowskim w cyberprzestrzeni.

Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019 – 2024 jest spójna z prowadzonymi działaniami dotyczącymi systemów teleinformatycznych operatorów infrastruktury krytycznej oraz uwzględnia potrzeby zapewnienia zdolności Siłom Zbrojnym Rzeczypospolitej Polskiej w układzie krajowym, sojuszniczym i koalicyjnym do prowadzenia działań militarnych w przypadku zagrożenia cyberbezpieczeństwa powodującego konieczność działań obronnych.

Podejmując działania mające na celu wdrożenie *Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019 – 2024*, rząd będzie w pełni ~~respektował~~ gwarantował prawo do prywatności oraz stał na stanowisku, że wolny i otwarty Internet jest istotnym elementem funkcjonowania współczesnego społeczeństwa.

---

[2] Ustawa o krajowym systemie cyberbezpieczeństwa jest transpozycją do polskiego porządku prawnego Dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz. Urz UE L 194 z 19.07.2016).

3. Zakres *Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019 – 2024*

Strategia uwzględnia, w szczególności[3]:

1) cele i priorytety państwa w zakresie cyberbezpieczeństwa,
2) podmioty zaangażowane we wdrażanie i realizację Strategii,
3) środki służące realizacji celów Strategii,
4) określenie środków w zakresie gotowości, reagowania i przywracania stanu normalnego, w tym zasady współpracy między sektorem publicznym i prywatnym,
5) podejście do oceny ryzyka,
6) działania odnoszące się do programów edukacyjnych, informacyjnych i szkoleniowych dotyczących cyberbezpieczeństwa,
7) działania odnoszące się do planów badawczo-rozwojowych w zakresie cyberbezpieczeństwa,

Ponadto Strategia uwzględnia międzynarodową współpracę w zakresie cyberbezpieczeństwa.

Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019 – 2024 wprowadzona w drodze uchwały Rady Ministrów, oddziałuje w sposób bezpośredni na podmioty administracji rządowej, a w sposób pośredni, po przyjęciu z inicjatywy Rady Ministrów przepisów prawa powszechnego, na pozostałe podmioty władzy publicznej, przedsiębiorców i obywateli.

---

[3] Art. 69 ust. 2 o krajowym systemie cyberbezpieczeństwa.

4. Wizja, cel główny, cele szczegółowe

4.1. Wizja

Pomyślny rozwój Polski, wzrost jej zasobności, efektywności gospodarki, sprawności działania instytucji, podmiotów, w tym i aktywność społeczna oraz codzienne funkcjonowanie indywidualnego członka społeczeństwa są związane ze sprawnym i bezpiecznym działaniem systemów informacyjnych i środków komunikacji elektronicznej. Dlatego w ramach działań zaplanowanych w Strategii do roku 2024 rząd RP będzie systematycznie wzmacniał i rozwijał Krajowy System Cyberbezpieczeństwa. Działania uwzględniają systemowe rozwiązania organizacyjne, operacyjne, technologiczne, prawne, kreowanie postaw społecznych, prowadzenie badań naukowych, tak aby zapewnić spełnienie wysokich standardów cyberbezpieczeństwa w obszarze wsparcia/utrzymania sieci, oprogramowania, urządzeń i usług ~~cyfrowych~~. Działania rządu będą podejmowane z poszanowaniem praw i wolności obywateli oraz poprzez budowę zaufania pomiędzy poszczególnymi sektorami rynkowymi a administracją publiczną.

Z komentarzem [AP2]: Wizja powinna uwzględniać również fakt, że zagrożenia wynikające z działalności kryminalnej mają zasadniczo różny charakter, skalę i poziom zaawansowania technologicznego od zagrożeń wynikających z ataków dywersyjnych i militarnych przeprowadzanych przez jednostki organizacyjne korzystające ze wsparcia technologicznego, finansowego i ochrony prawnej państwa. To oznacza, że te typy zagrożeń powinny być uwzględnione odrębnie zarówno w Krajowym Systemie Cyberbezpieczeństwa jak i w ramach zmian, jakich wymaga dyrektywa NIS.

4.2. Cel główny

Podniesienie poziomu odporności na cyberzagrożenia[4] oraz zwiększenie poziomu ochrony informacji w sektorze publicznym, militarnym, prywatnym oraz promowanie wiedzy i dobrych praktyk umożliwiających obywatelom lepszą ochronę ich informacji.

4.3. Cele szczegółowe

Cel szczegółowy 1. Rozwój Krajowego Systemu Cyberbezpieczeństwa.

Cel szczegółowy 2. Stymulowanie podniesienia poziomu odporności ~~systemów informacyjnych~~ cyberprzestrzeni administracji publicznej i sektora prywatnego oraz osiągnięcie zdolności do skutecznego zapobiegania incydentom.

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

---

[4] „Cyberzagrożenie" oznacza wszelkie potencjalne okoliczności, zdarzenie lub działanie, które mogą wyrządzić szkodę, spowodować zakłócenia lub w inny sposób niekorzystnie wpłynąć w przypadku sieci i systemów teleinformatycznych, użytkowników takich systemów oraz innych osób – Rozporządzenie Parlamentu Europejskiego i Rady w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie), (Dz. Urz. UE L 151 z 07.06.2019), str. 15

Cel szczegółowy 4. Budowanie świadomości i kompetencji społecznych w zakresie cyberbezpieczeństwa

Cel szczegółowy 5. Aktywna rola RP na arenie międzynarodowej w obszarze cyberbezpieczeństwa.

5. Cel szczegółowy 1 – rozwój Krajowego Systemu Cyberbezpieczeństwa

5.1. Wdrożenie i ocena funkcjonowania przepisów o Krajowym Systemie Cyberbezpieczeństwa

Podstawą rozwoju Krajowego Systemu Cyberbezpieczeństwa jest dokonanie pełnego wdrożenia i oceny funkcjonowania przepisów ustanawiających ten system, w powiązaniu z innymi przepisami, w szczególności z ustawą o zarządzaniu kryzysowym, ustawą o ochronie informacji niejawnych, strategią bezpieczeństwa narodowego. Rezultatem dokonanej oceny może być konieczność przygotowania niezbędnych zmian przepisów usuwających bariery dla skutecznej wymiany informacji oraz skoordynowanego i niezakłóconego reagowania na incydenty.

Zmiany przepisów regulujących funkcjonowanie Krajowego Systemu Cyberbezpieczeństwa będą również wynikały z praktyki funkcjonowania na szczeblu europejskim *Dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii* (Dz. U. L 194 z 19.7.2016, str. 1), zwanej dalej „Dyrektywą NIS". Doświadczenia związane ze stosowaniem przepisów prawa w tym zakresie będą również przesłanką do wnioskowania na poziomie Unii Europejskiej w sprawie zmiany przepisów samej Dyrektywy NIS, tak aby zwiększyć skuteczność jej oddziaływania – jednym z obszarów wymagających zmian zwiększających efektywność Dyrektywy NIS będzie doprecyzowanie obowiązków dostawców usług cyfrowych, w szczególności świadczących usługi chmur obliczeniowych, które w coraz większym stopniu będą wykorzystywane jako model przetwarzania danych dla usług kluczowych.

Z komentarzem [AP3]: publicznych

Za przygotowanie propozycji zmian prawnych w zakresie cyberbezpieczeństwa w swych obszarach kompetencyjnych odpowiadają ministrowie według właściwości wynikającej z ustawy o działach administracji rządowej.

W ramach prac legislacyjnych minister właściwy do spraw informatyzacji, we współpracy z innymi resortami, dokona przeglądu regulacji sektorowych i szczególnych, które dotyczą omawianej problematyki oraz regulacji prawnych, które mogą mieć oddziaływanie na inne obszary, na przykład na ochronę danych osobowych, czy infrastrukturę krytyczną w kontekście Narodowego Programu Ochrony Infrastruktury Krytycznej. Niezbędne będzie również podjęcie prac legislacyjnych mających na celu uregulowanie obszaru z zakresu wytwarzania, posiadania, pozyskiwania oraz wykorzystywania specjalistycznych narzędzi podwójnego zastosowania do prowadzenia działań defensywno-ofensywnych w cyberprzestrzeni.

Z komentarzem [AP4]: Sugerujemy, że legislacja w dziedzinie narzędzi podwójnego zastosowania powinna odbyć się na poziomie ogólnoeuropejskim (tak jak na poziomie europejskim regulowany jest eksport dóbr podwójnego zastosowania) Legislacja zagrożeń o charakterze militarnym i dywersyjnym powinna być spójna w ramach systemu cyber-obrony NATO.

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

Z uwagi na dynamikę procesów zachodzących w obszarze cyberbezpieczeństwa niezbędne będzie okresowe monitorowanie zjawisk tam zachodzących i inicjowanie ewentualnych zmian w przepisach prawa. Propozycje kierunków i planów na rzecz przeciwdziałania zagrożeniom cyberbezpieczeństwa będą opiniowane przez Kolegium, działające przy Radzie Ministrów, jako organ opiniodawczo-doradczy w sprawach cyberbezpieczeństwa oraz działalności w tym zakresie CSIRT MON, CSIRT NASK,

Z komentarzem [AP5]: ciągłe

CSIRT GOV, sektorowych zespołów cyberbezpieczeństwa i organów właściwych do spraw cyberbezpieczeństwa.

5.2. Podniesienie efektywności funkcjonowania Krajowego Systemu Cyberbezpieczeństwa

Podniesienie efektywności funkcjonowania Krajowego Systemu Cyberbezpieczeństwa będzie realizowane poprzez uruchomienie w roku 2021 przez ministra właściwego do spraw informatyzacji systemu teleinformatycznego wspierającego[5]:

1) współpracę podmiotów wchodzących w skład Krajowego Systemu Cyberbezpieczeństwa,

2) generowanie i przekazywanie rekomendacji dotyczących działań podnoszących poziom cyberbezpieczeństwa,

3) zgłaszanie i obsługę incydentów,

4) szacowanie ryzyka na poziomie krajowym,

5) ostrzeganie o zagrożeniach cyberbezpieczeństwa.

Organy właściwe, odpowiedzialne za sprawowanie nadzoru ~~w zakresie systemów teleinformatycznych~~ nad bezpieczeństwem cyberprzestrzeni w sektorach, w których świadczone są usługi kluczowe i usługi cyfrowe, będą prowadziły działania mające wspierać operatorów i dostawców w zapewnieniu bezpieczeństwa świadczonych przez nich usług. Organy właściwe będą mogły w tym celu wydawać zalecenia organizacyjne i techniczne, a także udostępniać narzędzia i wiedzę dotyczącą najlepszych praktyk sektorowych i ponadsektorowych podnoszących cyberbezpieczeństwo.

Z komentarzem [AP6]: W jakiej procedurze organy te będą wyznaczone?

Z komentarzem [AP7]: Sugerujemy wypracowanie definicji/katalogu usług kluczowych

Rozwój Krajowego Systemu Cyberbezpieczeństwa wiąże się również ze zwiększaniem zdolności struktur zajmujących się cyberbezpieczeństwem na poziomie operacyjnym, w tym trzech zespołów CSIRT poziomu krajowego, współpracujących z nimi sektorowych zespołów reagowania na incydenty, regionalnych i lokalnych zespołów cyberbezpieczeństwa, a także centrów analizy i wymiany informacji. Niezbędne jest wdrożenie systemowych rozwiązań pozwalających na wymianę informacji pomiędzy interesariuszami i dzielenie się wiedzą, co do zagrożeń i incydentów.

Rząd w ramach współpracy administracji rządowej z administracją samorządową będzie rekomendował i działał na rzecz jednostek samorządu terytorialnego w zakresie podnoszenia kompetencji w doborze, wdrażaniu i utrzymaniu środków technicznych zwiększających cyberbezpieczeństwo, w tym korzystania z nowoczesnych i bezpiecznych modeli przetwarzania w chmurach obliczeniowych, tworzenia bezpiecznych aplikacji wykorzystujących technologie mikroelektroniczne oraz korzystania z bezpiecznych systemów mobilnych.

Efektywność funkcjonowania Krajowego Systemu Cyberbezpieczeństwa ma również podnieść wprowadzenie standaryzacji rozwiązań zabezpieczających, w tym wprowadzenie minimalnych wymagań bezpieczeństwa dla sieci i systemów teleinformatycznych używanych przez administrację publiczną. Standaryzacja i wymagania cyberbezpieczeństwa, opracowane i wykorzystywane przez

[5] Art. 46 ust. 1 ustawy o krajowym systemie cyberbezpieczeństwa.

administrację publiczną w ramach Narodowych Standardów Cyberbezpieczeństwa, powinny stać się także wyznacznikiem dobrych praktyk dla sektora prywatnego oraz dla obywateli.

Efektywność funkcjonowania Krajowego Systemu Cyberbezpieczeństwa będzie weryfikowana podczas ćwiczeń sektorowych oraz ćwiczeń krajowych, inicjowanych przez Pełnomocnika Rządu ds. Cyberbezpieczeństwa. W ramach ćwiczeń krajowych i międzynarodowych będą także podnoszone zdolności Sił Zbrojnych Rzeczypospolitej Polskiej do prowadzenia operacji defensywnych w cyberprzestrzeni.

Z komentarzem [AP8]: Czy sektor prywatny automatycznie przyjmie/zaakceptuje standardy wprowadzone przez administrację publiczną? Opracowane standardy mogą stać się obligatoryjne tylko wtedy, gdy zostaną wprowadzone jako specyfikacje techniczne poprzez odpowiednie rozporządzenia. To wymaga również postawienia pytania o delegację ustawową do takich rozporządzeń i ich spójność w ramach systemu prawnego UE.

5.3. Rozbudowa systemu wymiany informacji na potrzeby kierowania bezpieczeństwem narodowym

W celu usprawnienia zarządzania bezpieczeństwem, prowadzone będą działania mające na celu wymianę informacji i uzgadnianie reakcji, tak na poziomie strategicznym jak i poziomie operacyjnym, w szczególności pomiędzy podmiotami sferyą cywilnejją, policją i służbami przeciwdziałającymi przestępczości oraz służbami odpowiadającymi za bezpieczeństwo wewnętrzne i obronność ~~i sferą wojskową~~. Niezbędna jest budowa odpornego na cyberzagrożenia systemu wymiany informacji dla potrzeb administracji publicznej wykorzystującego najnowocześniejsze technologie wymiany informacji, technologie mikroelektroniczne, uwzględniające konieczność wysokiej mobilności. System ten będzie wykorzystywany w różnych stanach nadzwyczajnych oraz stanach podwyższonej gotowości obronnej państwa.

5.4. Zwiększenie cyberbezpieczeństwa usług kluczowych i cyfrowych oraz infrastruktury krytycznej

Technologie informatyczne (IT)[6] wykorzystywane przez operatorów usług kluczowych, dostawców usług cyfrowych, operatorów infrastruktury krytycznej (w tym operatorów telekomunikacyjnych), stanowią element krytyczny dla ciągłości działania państwa oraz zapewniania bezpieczeństwa obywatelom. Co więcej, bezpieczeństwo najważniejszych sektorów gospodarki, ze szczególnym uwzględnieniem sektora energii, zależy od zapewnienia niezakłóconego działania przemysłowych systemów sterowania (OT)[7]. Dlatego zapewnienie cyberbezpieczeństwa zarówno IT, jak i OT, w tym rozwiązań systemowych mających na celu podnoszenie bezpieczeństwa sprzętowych mikroelektronicznych komponentów systemów teleinformatycznych, będzie traktowane przez Radę Ministrów jako priorytet. Wyrazem tego są przygotowywane już analizy dotyczące doprecyzowania wymagań bezpieczeństwa niezbędnych do spełnienia przez operatorów telekomunikacyjnych, szczególnie przy budowie sieci 5G, która w przyszłości będzie podstawą funkcjonowania państwa. Zakłada się, że będą w tym obszarze konieczne zmiany prawne, aby umożliwić odpowiednią kontrolę nad zapewnieniem cyberbezpieczeństwa.

Oprócz tego, mając na uwadze, że odpowiedzialność za zapewnienie bezpieczeństwa usług leży przede wszystkim po stronie podmiotów je świadczących, rząd podejmie działania wspierające

---

[6] IT – ang. Information technologies

[7] OT – ang. operational technologies

budowanie zdolności i kompetencji w zakresie cyberbezpieczeństwa wśród operatorów usług kluczowych, operatorów infrastruktury krytycznej oraz dostawców usług cyfrowych, uwzględniając ich różnorodną specyfikę i różny stopień dojrzałości w zakresie cyberbezpieczeństwa. Ponadto, rząd będzie wspierał te podmioty w reagowaniu na incydenty poważne, szczególnie w przypadku wystąpienia incydentów ponadsektorowych.

W pierwszej kolejności zostanie zapewniona spójność działań w zakresie opracowywania kryteriów identyfikacji operatorów infrastruktury krytycznej i usług kluczowych, uwzględniająca potrzebę włączenia tych podmiotów do systemu zarządzania kryzysowego. Proces ten przebiegał będzie we współpracy ze wszystkimi sektorami. Wykorzystując mechanizmy przewidziane prawem rekomendowane będą minimalne wymagania w zakresie cyberbezpieczeństwa ze szczególnym uwzględnianiem zarządzania ciągłością działania.

Analogicznym reżimem objęci zostaną dostawcy usług cyfrowych, jednak rząd ma pełną świadomość międzynarodowej specyfiki tych podmiotów oraz konieczności zapewnienia takich regulacji, które będą sprzyjały rozwojowi rynku cyfrowego w Polsce – stąd działania w tym obszarze będą prowadzone na forum europejskim przede wszystkim w ramach Grupy Współpracy Dyrektywy NIS, a także w ramach współpracy transatlantyckiej z brytyjskimi i amerykańskimi instytucjami stymulującymi podnoszenie standardów cyberbezpieczeństwa przez dostawców usług cyfrowych.

5.5. Wypracowanie i wdrożenie metodyki szacowania ryzyka na poziomie krajowym

Na potrzeby zarządzania cyberbezpieczeństwem na poziomie krajowym wdrożona zostanie wspólna metodyka statycznego i dynamicznego szacowania ryzyka, uwzględniająca specyfikę poszczególnych sektorów, a także operatorów infrastruktury krytycznej, usług kluczowych i dostawców usług cyfrowych. Zapewni to porównywalność szacowań, w tym określenie poziomu ryzyka, w szczególności na potrzeby raportu o zagrożeniach bezpieczeństwa narodowego, sporządzanego na podstawie przepisów o zarządzaniu kryzysowym. Szacowanie ryzyka stanie się procesem ciągłym i umożliwi zobrazowanie poziomu ryzyka w czasie zbliżonym do czasu rzeczywistego.

Metodyka i narzędzia umożliwiające statyczne i dynamiczne szacowania ryzyka dla systemów teleinformatycznych powstają w ramach projektu Narodowej Platformy Cyberbezpieczeństwa finansowanego przez Narodowe Centrum Badań i Rozwoju – zakończenie prac planowane jest do końca 2020 roku.

Z komentarzem [AP9]: Bardzo ważny punkt - w miarę możliwości postulujemy jak najszybsze (jeszcze przed 2020) wypracowanie takiej metodyki i narzędzi

5.6. Zwiększanie zdolności do zwalczania cyberprzestępczości, w tym cyberszpiegostwa i zdarzeń o charakterze terrorystycznym

W zakresie zwiększania zdolności do zwalczania cyberprzestępczości, w tym cyberszpiegostwa, zdarzeń o charakterze terrorystycznym (w tym działań o charakterze hybrydowym), ważne jest zapewnienie wsparcia dla operatorów usług kluczowych, dostawców usług cyfrowych oraz operatorów infrastruktury krytycznej w wykrywaniu oraz zwalczaniu incydentów we wszystkich ich fazach. W tym celu wymagana jest współpraca oraz koordynacja działań organów ścigania niezależnie od motywów, którymi kierują się sprawcy przestępstw, a szczególnie istotne znaczenie

ma prawidłowe zabezpieczenie dowodów cyfrowych wykorzystujących bezpieczne krajowe rozwiązania mikroelektroniczne, oraz zapewnienie "łańcucha zaufania".

Zwiększenie efektywności czynności procesowych i operacyjnych wymaga podjęcia i poszerzenia współdziałania organów ścigania z innymi podmiotami, które mogą posiadać wiedzę w zakresie ustalenia istoty przestępstwa lub mogą przyczynić się do ustalenia jego sprawcy. Dotyczy to współpracy z krajowymi oraz międzynarodowymi podmiotami prywatnymi, szczególnie z sektora telekomunikacyjnego, bankowego i ubezpieczeniowego. Niezbędne jest także zapewnienie, ciągłej wymiany informacji o zagrożeniach i podatnościach zarówno na poziomie krajowym, jak i międzynarodowym.

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

Biorąc pod uwagę dużą dynamikę przestępstwa w cyberprzestrzeni i związana z tym konieczność podejmowania czynności operacyjnych i procesowych niezbędne jest wprowadzenie przepisów umożliwiających przetwarzanie dokumentów procesowych w postaci elektronicznej i przesyłanie ich w takiej postaci.

Szybko zmieniające się metody popełniania przestępstw wymagają rozwijania badań naukowych w obszarze zwalczania cyberprzestępczości, których wyniki zapewnią wsparcie dla organów ścigania. Wyniki tych badań będą wykorzystywane w pracy organów ścigania i wymiaru sprawiedliwości, jak też będą stanowić materiał do opracowania działań profilaktycznych. Wdrożone zostaną, skierowane do społeczeństwa, programy informacyjne o zagrożeniach cyberprzestępczością oraz metodach unikania skutków tych zagrożeń. Wskazane zostaną sposoby postępowania dla osób dotkniętych przestępstwem. Ważną rolę do odegrania w tego typu działalności będą mieli operatorzy usług kluczowych, dostawcy usług cyfrowych, dostawcy usługi dostępu do Internetu oraz organizacje pozarządowe.

6. Cel szczegółowy 2 – Podniesienie poziomu odporności systemów informacyjnych administracji publicznej i sektora prywatnego oraz osiągnięcie zdolności do skutecznego zapobiegania incydentom

6.1. Opracowanie i wdrożenie Narodowych Standardów Cyberbezpieczeństwa oraz promowanie dobrych praktyk i zaleceń

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

Z komentarzem [AP10]: Dla systemów/produktów dla których istnieją odpowiednie normy międzynarodowe powinny być one bezpośrednio przyjęte poprzez ich umieszczenie w odpowiednich standardach (specyfikacjach technicznych). Sugerujemy zatem przeformułowanie: PKN we współpracy z ośrodkami akademickimi... powinien skatalogować istniejące normy międzynarodowe dla poszczególnych kategorii oraz przyjąć konkretne rekomendacje w zakresie ich wdrażania.

W celu zwiększenia odporności systemów informacyjnych administracji publicznej na cyberzagrożenia niezbędne jest opracowanie Narodowych Standardów Cyberbezpieczeństwa jako zbioru wymagań organizacyjnych i technicznych dotyczących w szczególności bezpieczeństwa:

1) aplikacji,
2) urządzeń mobilnych,
3) stacji roboczych,
4) serwerów i sieci,
5) modeli chmur obliczeniowych,
~~5)~~ 6) Wsparcie i Utrzymanie sieci/systemów teleinformatycznych.

W celu zapewnienia bezpiecznej i optymalnej kosztowo infrastruktury przetwarzania systemów IT administracji publicznej, która już w bliskiej przyszłości rozpocznie korzystanie z nowych form przetwarzania i przechowywania informacji m.in. poprzez wykorzystywanie usług chmury obliczeniowej, niezbędne będzie przygotowanie zaleceń i promowanie dobrych praktyk podnoszących odporność na potencjalne cyberzagrożenia.

Realizacja zadań publicznych, w szczególności związanych z cyberbezpieczeństwem będzie wspierana poprzez stosowanie Polskich Norm, bazujących na normach europejskich i międzynarodowych. Odwołania do norm powinny być szeroko stosowanie na wszystkich etapach cyklu życia systemu teleinformatycznego. Istotne jest również wspieranie wdrożenia rekomendacji wydawanych przez regulatorów rynkowych.

6.2. Bezpieczeństwo łańcucha dostaw

Zapewnienie cyberbezpieczeństwa wymaga, stosowania zabezpieczeń organizacyjnych i technicznych na wszystkich etapach cyklu życia systemów teleinformatycznych. Działania te składają się na tak zwany bezpieczny łańcuch dostaw budowy, który obejmuje projektowanie, budowę, wdrażanie, eksploatację oraz wycofywanie z użycia. Pod pojęciem łańcucha dostaw należy rozumieć system, na który składają się podsystemy produkcji, dystrybucji, transportu, magazynowania oraz recyklingu komponentów systemów teleinformatycznych, jak również ich instalacja, uruchomienie, bieżące utrzymanie, serwisowanie oraz naprawy.

Ważnym elementem zapewnienia jakości w łańcuchu dostaw jest ocena i certyfikacja produktów i systemów (w szczególności oprogramowania, urządzeń i usług). Priorytetowe w tym zakresie będzie utworzenie, a następnie utrzymanie i rozwój krajowego systemu oceny i certyfikacji cyberbezpieczeństwa, co umożliwi Polsce uzyskanie pełnego i rozpoznawanego na arenie europejskiej i międzynarodowej statusu państwa producenta w dziedzinie rozwiązań cyberbezpieczeństwa.

Polska aktywnie włączy się w prace nad ustanowieniem europejskich programów certyfikacji cyberbezpieczeństwa zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) Dz. Dz. Urz. UE L 151 z 07.06.2019.

Działania na poziomie krajowym będą obejmowały, w szczególności, wyznaczenie krajowego orangu ds. certyfikacji cyberbezpieczeństwa, który będzie wydawał europejskie certyfikaty cyberbezpieczeństwa oraz nadzorował krajowe jednostki oceniające zgodność produktów, usług i procesów z wymaganiami określonymi w europejskich programach certyfikacji cyberbezpieczeństwa.

Efektem tych działań będzie uzyskanie na poziomie krajowym zdolności do wspierania ~~polskich~~ producentów, którzy uzyskując europejskie certyfikaty cyberbezpieczeństwa będą mogli skuteczniej konkurować na jednolitym rynku cyfrowym UE.

Z komentarzem [AP11]: Proponujemy dodać paragraf o konieczności weryfikowania poziomu zaufania sprzętu przeznaczonego do infrastruktury, uwzględniając jego podatność na cyberataki.

6.3. Testy i audyty cyberbezpieczeństwa

Jednym ze środków, który pozwala na dokonanie oceny skuteczności wdrożonych systemów zarządzania bezpieczeństwem i adekwatności ustanowionych zabezpieczeń, są okresowe audyty. Metodyki audytów powinny uwzględniać normy, dobre praktyki oraz specyfikę poszczególnych sektorów. Celem takiego podejścia jest uzyskanie porównywalności wyników audytów.

Kolejnym środkiem oceny bezpieczeństwa są okresowe testy (w tym testy penetracyjne), które pozwalają na rzeczywistą ocenę odporności systemu na zagrożenia. Ich wyniki stanowią podstawę weryfikacji przyjętych założeń w zakresie ustanowionych zabezpieczeń. W celu wykorzystania potencjału społecznego w zakresie cyberbezpieczeństwa propagowane będzie testowanie zabezpieczeń w modelu tzw. *bug-bounty*[8].

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

7. Cel szczegółowy 3 – Zwiększenie potencjału narodowego w zakresie technologii cyberbezpieczeństwa

7.1. Rozbudowa zasobów przemysłowych i technologicznych na potrzeby cyberbezpieczeństwa

Rząd Polski stawia sobie za cel inwestowanie w rozbudowę zasobów przemysłowych i technologicznych na potrzeby cyberbezpieczeństwa poprzez stwarzanie warunków dla rozwoju działających w Polsce przedsiębiorstw, ośrodków naukowo-badawczych, jak i *start-upów*, których przedmiotem działalności jest tworzenie nowych rozwiązań w obszarze cyberbezpieczeństwa. Jednym z priorytetów jest wzrost zdolności w obszarze projektowania i wytwarzania oprogramowania, projektowania i wytwarzania mikroelektronicznych przyrządów półprzewodnikowych w tym bezpiecznych układów scalonych, urządzeń i usług wykorzystywanych we wszystkich gałęziach polskiego przemysłu, zwiększających jego konkurencyjność. Pozyskiwanie nowych technologii dla rozwoju rodzimych przedsięwzięć będzie realizowane poprzez udział w inicjatywach międzynarodowych kładących nacisk na innowacyjność, w drodze współpracy dwustronnej oraz w ramach organizacji międzynarodowych, w tym w ramach planowanego przez Komisję Europejską i Państwa Członkowskie Europejskiego Centrum Kompetencji Cyberbezpieczeństwa.

Stymulowane będzie podnoszenie kompetencji ośrodków naukowych oraz wyższych uczelni w obszarze cyberbezpieczeństwa. Poprzez instrumenty prawne rząd będzie stymulował na wyższych uczelniach nauczanie służące pozyskiwaniu specjalistów z zakresu cyberbezpieczeństwa, w ramach studiów pierwszego i drugiego stopnia oraz studiów doktoranckich i podyplomowych.

W celu wyrównania szans polskich przedsiębiorców na globalnym rynku rząd będzie wspierać rozwój polskiego biznesu w uzyskiwaniu zdolności cyfrowych oraz zapewniał pomoc w ubieganiu się o środki na rozwój innowacyjnych rozwiązań, a także doradztwo w dostępie do nowych rynków jak i pomoc w nawiązaniu współpracy z innymi przedsiębiorcami.

7.2. Zbudowanie mechanizmów współpracy między sektorem publicznym i prywatnym

Zapewnienie bezpieczeństwa w cyberprzestrzeni wymaga wspólnego wysiłku sektora prywatnego, publicznego oraz obywateli. Rząd będzie kontynuował budowanie efektywnego systemu partnerstwa publiczno-prywatnego opartego na zaufaniu i wspólnej odpowiedzialności za cyberbezpieczeństwo. Jednocześnie administracja publiczna będzie doskonaliła swój potencjał w zakresie inicjowania i prowadzenia projektów w dziedzinie cyberbezpieczeństwa. Rząd będzie również aktywnie angażować się w istniejące i powstające formy europejskiej współpracy publiczno-prywatnej i tym samym będzie promować polski biznes na arenie międzynarodowej.

Realizując nową wizję rozwoju kraju i wspierając innowacyjność polskiej gospodarki, istotna będzie budowa systemu wsparcia przedsięwzięć badawczo-rozwojowych w dziedzinie cyberbezpieczeństwa, prowadzonych we współpracy świata nauki oraz przedsiębiorstw komercyjnych.

7.3. Stymulowanie badań i rozwoju w obszarze cyberbezpieczeństwa

W związku z dynamicznie rozwijającym się rynkiem informatycznym, w szczególności w związku z perspektywą zmiany aktualnie użytkowanego w sieci Internet protokołu IPv4 na rzecz protokołu IPv6, a także w związku z rozwojem idei Internetu Rzeczy, Inteligentnych Miast, Przemysłu 4.0, jak również chmury obliczeniowych, sieci mobilnej łączności szerokopasmowej (5G i kolejnych generacji), czy megadanych (*Big Data)* zachodzi konieczność intensyfikacji działań badawczych i rozwojowych oraz wytwórczych w zakresie cyberbezpieczeństwa. W tym celu wspólnie z Narodowym Centrum Badań i Rozwoju kontynuowane będą programy badawcze, mające na celu przygotowanie i wdrożenie nowych metod ochrony przed cyberzagrożeniami.

W obliczu dynamicznie rozwijających się technologii związanych m.in. z Internetem Rzeczy należy zwrócić szczególną uwagę na konieczność zapewnienia bezpieczeństwa produktu, usługi lub procesu już na etapie projektowania (*Security by Design*[9]). Rząd RP będzie promował i wspierał podejście uwzględniające bezpieczeństwo już od etapu projektowania.

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

- ocenę skuteczności zabezpieczeń i odporności na cyberzagrożenia,
- ocenę skuteczności reagowania na incydenty,
- metody wykrywania i analizy nowych typów cyberprzestępstw, cyberterroryzmu i cyberszpiegostwa,
- badanie metod ataków (w tym ataków o charakterze hybrydowym) oraz sposobów przeciwdziałania i minimalizowania skutków tych ataków,
- ochronę procesów demokratycznych przed zakłóceniami z wykorzystaniem cyberzagrożeń

Działalność badawcza i rozwojowa realizowana będzie także w obszarze współpracy międzynarodowej w ramach UE i NATO.

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

---

[9] Security by design – podejście do rozwoju produktów lub systemów, które polega na myśleniu o bezpieczeństwie i integracji funkcji bezpieczeństwa od samego początku. Komunikat Komisji - „Europejski program badań i innowacji w dziedzinie bezpieczeństwa" – wstępne stanowisko Komisji w sprawie głównych ustaleń i zaleceń europejskiego forum badań i innowacji w dziedzinie bezpieczeństwa, COM(2009)691 final.

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

Siły Zbrojne RP, jako podstawowy element systemu obronnego państwa, powinny angażować się w działania w cyberprzestrzeni na tym samym poziomie co w powietrzu, na lądzie i na morzu. Zdolności do prowadzenia pełnego spektrum działań militarnych w cyberprzestrzeni muszą więc obejmować: rozpoznawanie zagrożeń, ochronę i obronę systemów teleinformatycznych oraz zwalczanie źródeł zagrożeń.

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

Z komentarzem [AP12]: Proponujemy nowy element strategii (7.5.) skupiony na poprawie cyberbezpieczeństwa sektora Public Safety (bezpieczeństwa publicznego)

8. Cel szczegółowy 4 – Budowanie świadomości i kompetencji społecznych w zakresie cyberbezpieczeństwa

8.1. Zwiększanie kompetencji kadry podmiotów istotnych dla cyberbezpieczeństwa RP

Podnoszenie kompetencji kadry podmiotów istotnych dla cyberbezpieczeństwa RP będzie realizowane poprzez stworzenie i wdrożenie takiego modelu funkcjonowania systemu edukacji akademickiej i doskonalenia zawodowego, który zapewni odpowiednie do wyzwań kwalifikacje pracowników. W tym celu opracowane zostaną modelowe programy edukacji akademickiej dla dedykowanego kierunku cyberbezpieczeństwo.

W ramach szeroko rozumianej edukacji eksperckiej, aby skuteczniej przeciwdziałać rozwijającej się cyberprzestępczości, zostanie wzmocniony system szkoleń dla wszystkich pracowników podmiotów istotnych dla cyberbezpieczeństwa oraz dla przedstawicieli organów ścigania i wymiaru sprawiedliwości, poprzez wdrożenie dedykowanego programu edukacyjnego zawierającego zarówno szkolenia teoretyczne jak i praktyczne na realnych przykładach zagrożeń.

W celu utrzymania w administracji publicznej pracowników o wysokich kompetencjach, równolegle z wykorzystaniem innych instrumentów wspierających ich aktywność, podjęte będą działania w celu zbliżenia zarobków tych pracowników do poziomu, jaki mogliby uzyskać zatrudniając się w sektorze prywatnym.

Równocześnie rząd RP przygotuje i wdroży systemowe rozwiązanie w celu zapewnienia merytorycznego wsparcia dla podniesienia kompetencji pracowników jednostek administracji samorządowej w zakresie cyberbezpieczeństwa.

Kierownictwo jednostek administracji rządowej będzie dynamicznie określało odpowiedzialność i uprawnienia dla osób pełniących istotną rolę w zakresie zarządzania cyberbezpieczeństwem i odpowiednio komunikowało te ustalenia wszystkim interesariuszom.

8.2. Stworzenie warunków do bezpiecznego korzystania z cyberprzestrzeni przez obywateli

Edukacja w zakresie cyberbezpieczeństwa powinna być dostępna na jak najwcześniejszym etapie dostępu dzieci i młodzieży do usług cyfrowych – najlepiej jeśli byłaby prowadzona przed wejściem świat cyfrowy, a w praktyce często wymagana jest na etapie kształcenia wczesnoszkolnego. Uwzględniając tematykę bezpiecznego korzystania z cyberprzestrzeni zakłada się ciągłe doskonalenie podstaw programowych nauczania w ramach różnych kierunków kształcenia. Konieczne jest wprowadzenie systemowych działań doszkalających dla nauczycieli.

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

8.3. Rozwijanie świadomości społecznej w kierunku bezpiecznego korzystania z cyberprzestrzeni

We współpracy z organizacjami pozarządowymi, sektorem prywatnym oraz ośrodkami akademickimi, administracja publiczna kontynuować będzie systemowe działania uwrażliwiające społeczeństwo na zagrożenia płynące z w cyberprzestrzeni, a także działania edukacyjne w zakresie praw i wolności w środowisku cyfrowym. Kontynuowane będą m.in. kampanie społeczne, skierowane do różnych grup docelowych (między innymi dzieci, rodziców, seniorów).

W obliczu coraz liczniejszych zagrożeń nakierowanych na wywarcie określonego wpływu na społeczeństwo, a także mając na uwadze konsekwencje celowego wykorzystywania narzędzi z obszaru inżynierii społecznej, do działań o charakterze manipulacyjnym, w postaci m.in. kampanii dezinformacyjnych, lub działań inspiracyjnych bądź dezintegracyjnych, potrzebne jest podjęcie systemowych działań pozwalających na rozwijanie świadomości obywateli w kontekście weryfikacji autentyczności informacji oraz reagowania na próby jej zakłócenia. W kontekście obrony przed działaniami manipulacyjnymi, które mogą być jednym z elementów działań hybrydowych, ważne jest budowanie w społeczeństwie zdolności do identyfikacji działań oddziaływujących na świadomość, bądź ukierunkowanych na przekształcanie lub dezintegrację określonych środowisk.

9. Cel szczegółowy 5 – Zbudowanie silnej pozycji międzynarodowej Polski w obszarze cyberbezpieczeństwa

9.1. Aktywna współpraca międzynarodowa na poziomie strategiczno-politycznym

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

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

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

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

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

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

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

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

9.2. Aktywna współpraca międzynarodowa na poziomie operacyjnym i technicznym

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

Doskonalenie współpracy międzynarodowej możliwe jest także poprzez uczestnictwo podmiotów publicznych zaangażowanych w zapewnienie cyberbezpieczeństwa w oficjalnych międzynarodowych forach wymiany informacji o zagrożeniach i podatnościach.

10. Zarządzanie Strategią Cyberbezpieczeństwa RP

Strategia uchwalana jest na okres 5 lat.

Koordynatorem wdrażania Strategii jest minister właściwy do spraw informatyzacji.

Po dwóch latach od przyjęcia oraz w czwartym roku obowiązywania dokument podlega przeglądowi i ocenie efektów jego oddziaływania. Wyniki przeglądu przedstawiane są Radzie Ministrów. W wyniku dokonanego przeglądu minister właściwy do spraw informatyzacji opracowuje propozycję działań korygujących lub projekt dokumentu na kolejny okres pięcioletni. W przypadku wystąpienia uzasadnionych okoliczności Strategia Cyberbezpieczeństwa może być aktualizowana w innych terminach, niż te o których mowa powyżej.

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

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

Plan działań obejmuje działania o charakterze projektowym, charakteryzujące się początkiem i końcem okresu realizacji oraz produktami powstałymi w wyniku realizacji danego działania.

Minister Obrony Narodowej w uzgodnieniu z Koordynatorem może opracować odrębny *Plan działań,* który podlega akceptacji Prezesa Rady Ministrów. W stosunku do pozycji *Planu* zawierających informacje o charakterze niejawnym zastosowanie mają przepisy ustawy o ochronie informacji niejawnych. Minister Obrony Narodowej przesyła, w celach informacyjnych i zapewnienia koordynacji, zaakceptowany *Plan działań* ministrowi właściwego do spraw informatyzacji i Pełnomocnikowi Rządu do spraw Cyberbezpieczeństwa.

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

W przypadku opracowania odrębnego *Planu Działań* Minister Obrony Narodowej przedkłada sprawozdanie z jego realizacji Radzie Ministrów za pośrednictwem Koordynatora.

11. Finansowanie

Na mocy obowiązujących przepisów, podmioty realizujące zadania publiczne są zobowiązane do ujmowania w swoich planach finansowych nakładów na cyberbezpieczeństwo. Koszty te powiększyły się o nakłady przeznaczone na działania związane z budową Krajowego Systemu Cyberbezpieczeństwa oraz o nakłady ponoszone na realizację pozostałych przedsięwzięć *Planu działań na rzecz wdrożenia Strategii Cyberbezpieczeństwa*.

Szczegółowa wielkość i struktura kosztów poszczególnych przedsięwzięć będzie określona w procesie inicjowania konkretnych projektów. Oszacowanie kosztów finansowania wdrażania Strategii Cyberbezpieczeństwa nastąpi w ramach *Planu działań*.

Źródłami finansowania realizacji działań opisanych w dokumencie będą plany finansowe poszczególnych jednostek zaangażowanych we wdrażanie Strategii Cyberbezpieczeństwa, a także środki pochodzące z Narodowego Centrum Badań i Rozwoju oraz środki Unii Europejskiej[10], w miarę zaistnienia takich możliwości.

[10] Programy Unii Europejskiej umożliwiające finansowanie projektów związanych z cyberbezpieczeństwem, w szczególności: program Horyzont2020, program Connecting Europe Facilities (CEF Telcom) – oba w ramach Wieloletnich Ram Finansowych UE 2014-2021. Natomiast w kolejnej perspektywie finansowej UE (na lata 2021-2028) planowane są do uruchomienia dwa duże programy: program „Cyfrowa Europa" oraz program „Horyzont Europa".

UZASADNIENIE

Opracowanie i przyjęcie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej jest wymogiem realizacji przepisu art. 68 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. poz. 1560). Przepis ustawowy (art. 90) określa także datę graniczną, do której ww. Strategia ma zostać przyjęta tj.: do 31 października 2019 r.

Strategia określa cele strategiczne oraz odpowiednie środki polityczne, które mają na celu osiągniecie i utrzymanie wysokiego poziomu cyberbezpieczeństwa RP. Pojawiła się również konieczność dokonania oceny i przeglądu w 2019 r. dotychczasowego dokumentu o charakterze strategicznym, czyli przyjętych uchwałą Nr 52/2017 Rady Ministrów z dnia 27 kwietnia 2017 r. Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017 – 2022 oraz wynikającego z tego Planu działań na rzecz wdrożenia Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017 – 2022.

Stale zmieniające się uwarunkowania związane z bezpieczeństwem w cyberprzestrzeni wymagają szybkiej i zdecydowanej reakcji organów państwa. Również przeprowadzone kontrole Najwyższej Izby Kontroli wskazują na potrzebę aktualizacji oraz zapewnienia spójnej strategii działania RP w dziedzinie cyberbezpieczeństwa. W kontekście spójności, ważne jest przede wszystkim zapewnienie jak najszerszej współpracy przy wdrażaniu i rozwijaniu Krajowego Systemu Cyberbezpieczeństwa ze strony ministerstw i innych organów władzy państwowej.

Projekt uchwały nie jest sprzeczny z prawem Unii Europejskiej.

Projektowana regulacja nie zawiera przepisów technicznych w rozumieniu rozporządzenia Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz. U. poz. 2039 oraz z 2004 r. poz. 597) i nie podlega notyfikacji Komisji Europejskiej.

Projektowana regulacja nie będzie wymagała notyfikacji Komisji Europejskiej w trybie ustawy z dnia 30 kwietnia 2004 r. o postępowaniu w sprawach dotyczących pomocy publicznej (Dz. U. z 2018 r. poz. 362).

Projekt nie wymaga przedłożenia instytucjom i organom Unii Europejskiej, w tym Europejskiemu Bankowi Centralnemu, w celu uzyskania opinii, dokonania powiadomienia, konsultacji albo uzgodnienia.

Projekt uchwały nie będzie miał wpływu na działalność mikroprzedsiębiorców, małych i średnich przedsiębiorców.

Projekt zostanie udostępniony w Biuletynie Informacji Publicznej na stronie podmiotowej Ministra Cyfryzacji.

Uchwała wchodzi w życie z dniem 31 października 2019 r.

Nazwa projektu Uchwała Rady Ministrów w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019 – 2024 **Ministerstwo wiodące i ministerstwa współpracujące** Ministerstwo Cyfryzacji **Osoba odpowiedzialna za projekt w randze Ministra, Sekretarza Stanu lub Podsekretarza Stanu** Karol Okoński, Sekretarz Stanu w Ministerstwie Cyfryzacji **Kontakt do opiekuna merytorycznego projektu** Robert Kośla, Dyrektor Departamentu Cyberbezpieczeństwa tel. (22) 245 59 22, e-mail: sekretariat.dc@mc.gov.pl Tomasz Wlaź, Departament Cyberbezpieczeństwa tel. (22) 556 84 48, e-mail: tomasz.wlaz@mc.gov.pl	**Data sporządzenia** 02.08.2019 **Źródło:** Upoważnienie ustawowe art. 68 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. poz. 1560) **Nr w wykazie prac** ID210

OCENA SKUTKÓW REGULACJI

1. Jaki problem jest rozwiązywany?

Opracowanie i przyjęcie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej jest wymogiem realizacji przepisu art. 68 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Przepis ustawowy (art. 90) określa także datę graniczną, do której ww. Strategia ma zostać przyjęta tj.: do 31 października 2019 r.
Strategia określa cele strategiczne oraz odpowiednie środki polityczne, które mają na celu osiągniecie i utrzymanie wysokiego poziomu cyberbezpieczeństwa RP. Pojawiła się również konieczność dokonania oceny i przeglądu w 2019 r. dotychczasowego dokumentu o charakterze strategicznym, czyli przyjętych uchwałą Nr 52/2017 Rady Ministrów z dnia 27 kwietnia 2017 r. Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017 – 2022 oraz wynikającego z tego Planu działań na rzecz wdrożenia Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017 – 2022.
Stale zmieniające się uwarunkowania związane z bezpieczeństwem w cyberprzestrzeni wymagają szybkiej i zdecydowanej reakcji organów państwa. Również przeprowadzone kontrole Najwyższej Izby Kontroli wskazują na potrzebę aktualizacji oraz zapewnienia spójnej strategii działania RP w dziedzinie cyberbezpieczeństwa. W kontekście spójności, ważne jest przede wszystkim zapewnienie jak najszerszej współpracy przy wdrażaniu i rozwijaniu Krajowego Systemu Cyberbezpieczeństwa ze strony ministerstw i innych organów władzy państwowej.

2. Rekomendowane rozwiązanie, w tym planowane narzędzia interwencji, i oczekiwany efekt

Projektowana uchwała ma na celu ustanowienie Strategii Cyberbezpieczeństwa. Strategia ma charakter polityczno-strategiczny, natomiast na poziomie operacyjnym realizację jego zapisów zapewni szczegółowy plan działań. Plan działań opisze podmioty zaangażowane w realizację strategii oraz środki pozwalające na jej wdrożenie. Przy opracowywaniu strategii korzystano z dobrych praktyk i rozwiązań proponowanych przez Międzynarodowy Związek Telekomunikacyjny oraz doświadczeń innych państw.

Strategia uwzględni następujące kwestie:
a) cele i priorytety w zakresie cyberbezpieczeństwa, czyli opisane zostaną wizja, cel główny oraz cele szczegółowe strategii;
b) podmioty zaangażowane we wdrażanie i realizację Strategii;
c) środki służące realizacji celów Strategii;
d) określenie środków w zakresie gotowości, reagowania i przywracania stanu normalnego, w tym zasady współpracy między sektorem publicznym i prywatnym;
e) podejście do oceny ryzyka, czyli m.in. stworzenie systemu zarządzania ryzykiem na poziomie krajowym;
f) działania odnoszące się do programów edukacyjnych, informacyjnych i szkoleniowych dotyczących cyberbezpieczeństwa, czyli m.in. zwiększenie kompetencji kadr (w sektorze publicznym i prywatnym), cyberbezpieczeństwo obywateli (edukacja i budowanie świadomości);
g) działania odnoszące się do planów badawczo-rozwojowych w zakresie cyberbezpieczeństwa, czyli m.in. rozbudowa zasobów przemysłowych i technologicznych na potrzeby cyberbezpieczeństwa, stymulowanie badań i rozwoju.

3. Jak problem został rozwiązany w innych krajach, w szczególności krajach członkowskich OECD/UE?

Posiadanie krajowej strategii odnoszącej się do bezpieczeństwa sieci i systemów informatycznych jest wymagane przepisem art. 7 dyrektywy Parlamentu Europejskiego i Rady (UE) w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (NIS). Przyjęcie dyrektywy przez PE nastąpiło w dniu 7 lipca 2016 r. (Dz. U. UE 2016 r., L194).

Państwa UE w większości posiadają strategie tego typu. Część z nich przyjęła je przed wejściem w życie dyrektywy NIS, np. Estonia (2009, później w 2014), Holandia (2011, później w 2014 oraz 2018), Niemcy (2011, później w 2016), Wielka Brytania (2011, później w 2016), Litwa (2011), Belgia (2012), Cypr (2012), Hiszpania (2013), Włochy (2013), Austria (2013), Węgry (2013), Rumunia (2013), Finlandia (2013), Łotwa (2014), Portugalia (2015), Francja (2015), Irlandia (2015), Słowacja (2015), Chorwacja (2015), Słowenia (2016) oraz Bułgaria (2016). Część z państw UE przyjęła swoje strategie cyberbezpieczeństwa dopiero po przyjęciu nakładającej taki obowiązek dyrektywy NIS przez PE, np. Szwecja (2017) Grecja (2017) oraz Dania (2018).

Dokument o charakterze strategicznym w obszarze cyberbezpieczeństwa posiadają również państwa europejskie spoza UE, np. Szwajcaria (2012), Islandia (2015), Norwegia (2019) oraz państwa pozaeuropejskie, np. USA - „Cyber Intelligence Sharing and Protection Act" (2013) oraz „National Cyber Strategy of the United States of America" z 2018 r.

4. Podmioty, na które oddziałuje projekt

Grupa	Wielkość	Źródło danych	Oddziaływanie
Centralna administracja rządowa	Ministerstwa (19) oraz jednostki im podległe i nadzorowane	-	Opracowanie wkładu do Planu działania na rzecz wdrożenia Strategii i udział w jego realizacji.
Terenowa administracja rządowa	Wojewodowie (16) i ich jednostki podległe i nadzorowane, administracja zespolona i niezespolona w województwie	-	Udział w działaniach wg Planu działania na rzecz wdrożenia Strategii.

5. Informacje na temat zakresu, czasu trwania i podsumowanie wyników konsultacji

Projekt uchwały Rady Ministrów poddany zostanie uzgodnieniom międzyresortowym, opiniowaniu oraz konsultacjom publicznym, a także zostanie udostępniony w Biuletynie Informacji Publicznej na stronie podmiotowej Ministra Cyfryzacji.

6. Wpływ na sektor finansów publicznych

(ceny stałe z …… r.)	Skutki w okresie 10 lat od wejścia w życie zmian [mln zł]											
	0	1	2	3	4	5	6	7	8	9	10	*Łącznie (0-10)*
Dochody ogółem	0	0	0	0	0	0	0	0	0	0	0	0
budżet państwa	0	0	0	0	0	0	0	0	0	0	0	0
JST	0	0	0	0	0	0	0	0	0	0	0	0
pozostałe jednostki (oddzielnie)	0	0	0	0	0	0	0	0	0	0	0	0
Wydatki ogółem	0	0	0	0	0	0	0	0	0	0	0	0
budżet państwa	0	0	0	0	0	0	0	0	0	0	0	0
JST	0	0	0	0	0	0	0	0	0	0	0	0
pozostałe jednostki (oddzielnie)	0	0	0	0	0	0	0	0	0	0	0	0
Saldo ogółem	0	0	0	0	0	0	0	0	0	0	0	0
budżet państwa	0	0	0	0	0	0	0	0	0	0	0	0
JST	0	0	0	0	0	0	0	0	0	0	0	0
pozostałe jednostki (oddzielnie)	0	0	0	0	0	0	0	0	0	0	0	0

Źródła finansowania	Przyjęte rozwiązania nie spowodują dodatkowych skutków finansowych dla sektora finansów publicznych, w tym budżetu państwa i budżetów jednostek samorządu terytorialnego
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	Nie dotyczy.

7. Wpływ na konkurencyjność gospodarki i przedsiębiorczość, w tym funkcjonowanie przedsiębiorców oraz na rodzinę, obywateli i gospodarstwa domowe

		Skutki						
Czas w latach od wejścia w życie zmian		0	1	2	3	5	10	*Łącznie (0-10)*
W ujęciu pieniężnym (w mln zł, ceny stałe z …… r.)	duże przedsiębiorstwa	0	0	0	0	0	0	0
	sektor mikro-, małych i średnich przedsiębiorstw	0	0	0	0	0	0	0
	rodzina, obywatele oraz gospodarstwa domowe	0	0	0	0	0	0	0
W ujęciu niepieniężnym	duże przedsiębiorstwa	Brak wpływu.						
	sektor mikro-, małych i średnich przedsiębiorstw	Brak wpływu.						
	rodzina, obywatele oraz gospodarstwa domowe	Brak wpływu.						
Niemierzalne								

Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	Projekt rozporządzenia nie ma wpływu na konkurencyjność gospodarki i przedsiębiorczość, w tym funkcjonowanie przedsiębiorców oraz na sytuację ekonomiczną i społeczną rodziny, osób niepełnosprawnych oraz osób starszych, a także na obywateli i gospodarstwa domowe.

8. Zmiana obciążeń regulacyjnych (w tym obowiązków informacyjnych) wynikających z projektu

☒ nie dotyczy

Wprowadzane są obciążenia poza bezwzględnie wymaganymi przez UE (szczegóły w odwróconej tabeli zgodności).	☐ tak ☐ nie ☒ nie dotyczy
☐ zmniejszenie liczby dokumentów ☐ zmniejszenie liczby procedur ☐ skrócenie czasu na załatwienie sprawy ☐ inne: …	☐ zwiększenie liczby dokumentów ☐ zwiększenie liczby procedur ☐ wydłużenie czasu na załatwienie sprawy ☐ inne: …
Wprowadzane obciążenia są przystosowane do ich elektronizacji.	☐ tak ☐ nie ☐ nie dotyczy
Komentarz:	

9. Wpływ na rynek pracy

Brak wpływu projektowanej regulacji na rynek pracy.

10. Wpływ na pozostałe obszary

☐ środowisko naturalne ☐ sytuacja i rozwój regionalny ☐ inne: …	☐ demografia ☐ mienie państwowe	☒ informatyzacja ☐ zdrowie
Omówienie wpływu	Realizacja przedsięwzięć z Planu działań na rzecz wdrożenia strategii przyczyni się do zwiększenia bezpieczeństwa e-usług.	
11. Planowane wykonanie przepisów aktu prawnego		
Harmonogram wdrożenia działań wykonania Strategii będzie wynikał z Planu działań na rzecz wdrożenia strategii.		
12. W jaki sposób i kiedy nastąpi ewaluacja efektów projektu oraz jakie mierniki zostaną zastosowane?		
Minister właściwy do spraw informatyzacji we współpracy z Pełnomocnikiem Rządu do Spraw Cyberbezpieczeństwa, innymi ministrami i właściwymi kierownikami urzędów centralnych, dokonuje przeglądu Strategii co 2 lata.		
13. Załączniki (istotne dokumenty źródłowe, badania, analizy itp.)		
Brak załączników.		