

Warszawa, 03 września 2021 r.

CCil.51.1.2021

Szanowny Pan
Robert Kośla
Dyrektor Departamentu Cyberbezpieczeństwa
Kancelarii Prezesa Rady Ministrów

Dotyczy: uwag RA do opisu założeń projektu informatycznego S46 w ramach REACT-EU

Szanowny Panie Dyrektorze,

w załączeniu przekazuję odniesienie się do uwag wskazanych w „Karcie oceny projektu nr p310 przez zespół zadaniowy Rada Architektury IT” oraz zmodyfikowany (uwzględniający ww. uwagi) opis założeń projektu informatycznego pn. „Podłączenie podmiotów krajowego systemu cyberbezpieczeństwa do zintegrowanego systemu zarządzania cyberbezpieczeństwem S46 (S46-react)” (wersje xml, pdf i docx). Projekt jest realizowany w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020, Oś priorytetowa V „Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU”.

Zwracam się z uprzejmą prośbą o przekazanie do zaopiniowania ww. dokumentu przez Członków Komitetu Rady Ministrów ds. Cyfryzacji.

Poniżej odniesienie się do uwag i zaleceń zgłoszonych przez RA.

1. Rozdział 1.1: Identyfikacja problemu i potrzeb

- **Wskazano liczby interesariuszy:**
„Jednostki samorządu terytorialnego i jednostki im podległe (Urzędy Marszałkowskie, JST zarządzające większymi miastami, spółki wodno-kanalizacyjne itp.), urzędy współpracujące przy zagadnieniach związanych z cyberbezpieczeństwem JST, a także uczestniczące w zintegrowanym systemie zarządzania kryzysowego (Urzędy Wojewódzkie, RCB), większe szpitale” – 100
„Przedstawiciele JST i jednostek im podległych, urzędów współpracujące przy zagadnieniach związanych z cyberbezpieczeństwem JST, a także uczestniczących w zintegrowanym systemie zarządzania kryzysowego (Urzędy Wojewódzkie, RCB)” - 200

Uwaga.

„Należy rozważyć zmianę zapisów w Kamieniach milowych (rozdział 3), bowiem przy zapisach „narastających” można łatwo wywieść, że zarówno grupa jednostek jak i przedstawiciele będzie znacznie większa (przewyższająca podaną w rozdziale 1.1.), czyli 230 – jednostek i 460 – przedstawicieli.”

Odpowiedź.

W rozdziale 3 dokonano odpowiednich modyfikacji, precyzyjnie rozróżniając liczby zrealizowanych podłączeń i szkoleń w danym okresie od liczb podanych narastająco.

Uwaga.

„Jednocześnie należy zwrócić uwagę na doprecyzowanie interesariuszy projektu zgodnie z art. 4 ustawy o KSC.”

Odpowiedź.

W pierwszym akapicie rozdziału 1.2 „Opis stanu obecnego” został dodany opis wskazujący na sposób określenia interesariuszy zgodnie z art. 4 ustawy o KSC. Doprecyzowanie ma na celu wskazanie istniejącego stanu prawnego w tej kwestii, a w szczególności doprecyzowanie określenia grupy „podmiotów wchodzących w skład krajowego systemu cyberbezpieczeństwa”, do której odnosi się art. 46 ust. 1 pkt 1 ustawy o KSC.

Opis projektu w treści osi priorytetowej V POPC, czyli Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU mówi: „**podłączenie wybranych podmiotów, w tym jednostek podległych JST (np. urzędy, szpitale), a także operatorów usług kluczowych do zintegrowanego systemu zarządzania cyberbezpieczeństwem na poziomie krajowym (system S46), co umożliwi m.in. zgłaszanie incydentów przez JST do zespołów reagowania na incydenty komputerowe poziomu krajowego w czasie rzeczywistym.**”

Zatem projekt ma na celu podłączenie WYBRANYCH podmiotów. Katalog podmiotów, spośród których zostanie wybranych docelowych 100 podmiotów wynika z art. 4 ustawy o krajowym systemie cyberbezpieczeństwa, w którym są m.in. operatorzy usług kluczowych, a także takie podmioty publiczne jak JST.

Ponadto, **docelową listę podmiotów do podłączenia w ramach projektu REACT-EU** – który co trzeba podkreślić jest mechanizmem interwencyjnym, nastawionym na wsparcie najbardziej dotkniętych podmiotów szczególnie w sektorze ochrony zdrowia oraz JST – **wskaże właściciel systemu S46 oraz koordynator krajowego systemu cyberbezpieczeństwa, czyli minister właściwy ds. informatyzacji.**

Uwaga.

„Określenie grupy docelowej projektu na **poziomie min. 100 JST.**”

Odpowiedź.

Wskazana wielkość grup docelowych jest oszacowana „od dołu” i zakłada się, że jest ona większa, choć ze względu na dobrowolny charakter podłączania się podmiotów do S46 (wskazany w ustawie o KSC), oszacowanie tej liczby jest dość trudne. W celu odniesienia się do uwagi odnotowano w rozdziale 1.1 dla każdej z pierwszych dwóch grup interesariuszy, że „Szacowana wielkość grupy wskazana jest jako liczba minimalna”.

- **Zapis: “niewystarczający poziom wiedzy pracowników jednostek organizacyjnych samorządów terytorialnych oraz innych – wskazanych podmiotów o cyberbezpieczeństwie”**

Uwaga.

„W projekcie zaplanowano tylko szkolenie z zakresu wykorzystania systemu oraz jako wskaźnik podaje się podniesienie kompetencji cyfrowych podczas gdy w zidentyfikowanych problemach jest mowa o niewystarczającym poziomie wiedzy pracowników JST. Wydaje się, że przeszkolenie z wykorzystania systemu jest zatem niewystarczającą odpowiedzią na tak zidentyfikowany problem.”

Odpowiedź.

Szkolenie w ramach projektu skupia się na zaznajomieniu z działaniem samego systemu S46 i jego przyszłych użytkowników.

Zidentyfikowany problem, czyli „niewystarczający poziom wiedzy pracowników jednostek organizacyjnych samorządów terytorialnych oraz innych – wskazanych podmiotów o cyberbezpieczeństwie”, jest właśnie przyczyną rosnącej liczby incydentów cyberbezpieczeństwa w JST. JST nie są w stanie same poradzić sobie z obsługą tych incydentów, stąd też zidentyfikowana potrzeba podłączenia jak największej liczby podmiotów do zintegrowanego systemu poziomu krajowego, czyli S46. Umożliwi to m.in. dostęp do mapy zagrożeń utworzonej na bazie danych wpływających do S46. Ponadto umożliwi się bezpośrednio zgłaszanie incydentów bezpieczeństwa do CSIRT poziomu krajowego oraz otrzymanie tą drogą wsparcia np. w postaci rekomendacji, najlepszych praktyk czy ostrzeżeń.

Przeszkolenie pracowników podłączanych jednostek z obsługi S46 oczywiście nie może i nie jest jedyną reakcją na zidentyfikowany problem, jaka będzie podejmowana ogólnie przez Państwo. W ramach innych projektów ten problem też musi być zaadresowany. Jednak S46 ma na celu wdrożenie konkretnego systemu i przedmiotowy projekt może zapewnić reakcję na zidentyfikowany problem w zakresie związanym z systemem teleinformatycznym S46.

2. Rozdział 1.2: Opis stanu obecnego

- W pierwszym akapicie wskazano jako cel systemu m.in.: *„zapewniającego obserwację ryzyka na poziomie krajowym”*,

Uwaga.

„Zgodnie z ustawą KSC system ma zapewnić **szacowanie** ryzyka na poziomie krajowym – sformułowanie „obserwacja” jest niewystarczające.”

Odpowiedź.

Zgodnie z uwagą zmieniono wyraz „obserwację” na „szacowanie”.

3. Rozdział 2.1: Cele i korzyści wynikające z projektu

- W podsumowaniu Celu 1 wpisano: *„Zwiększenie liczby połączeń do systemu S46 wraz z przeszkoleniem użytkowników i tym samym wzrost poziomu cyberbezpieczeństwa RP, wpisuje się bezpośrednio w zakres osiągnięcia wyżej wymienionych celów strategicznych.”*

Uwaga.

„Brak informacji w ustawie o możliwości korzystania z systemu przez JST – mowa jest, że CSIRT MON, CSIRT NASK, CSIRT GOV, sektorowe zespoły cyberbezpieczeństwa i Prezes Urzędu Komunikacji Elektronicznej mogą korzystać z systemu teleinformatycznego na podstawie porozumienia zawartego z ministrem właściwym do spraw informatyzacji. W porozumieniu określa się zakres i warunki korzystania z systemu teleinformatycznego. W związku z powyższym wydaje się, że może być konieczna zmiana ustawy lub należy podać odpowiednią inną formalną podstawę precyzyjnie określającą rolę i relacje KSC v. JST.”

Odpowiedź.

W pierwszym akapicie rozdziału 1.2 „Opis stanu obecnego” został dodany opis wskazujący na sposób określenia interesariuszy zgodnie z art. 4 ustawy o KSC. Doprecyzowanie ma na celu wskazanie istniejącego stanu prawnego w tej kwestii, a w szczególności doprecyzowanie określenia grupy „podmiotów wchodzących w skład krajowego systemu cyberbezpieczeństwa”, do której odnosi się art. 46 ust. 1 pkt 1 ustawy o KSC.

W ustawie o KSC zapisano: „Art. 46. 1. Minister właściwy do spraw informatyzacji zapewnia rozwój lub utrzymanie systemu teleinformatycznego wspierającego:

1) współpracę podmiotów wchodzących w skład krajowego systemu cyberbezpieczeństwa”.

Zapis ten oznacza, że system teleinformatyczny, czyli S46, skierowany jest do wszystkich podmiotów krajowego systemu cyberbezpieczeństwa, wymienianych w art. 4.

Podmioty takie jak: zespoły CSIRT poziomu krajowego, sektorowe zespoły cyberbezpieczeństwa i Prezes Urzędu Komunikacji Elektronicznej, są podmiotami szczególnymi w systemie KSC, stąd też oddzielny ust. 2 wskazujący te podmioty.

Jednakże, na potrzeby doprecyzowania zapisów odnoszących się do S46, w procedowanej obecnie nowelizacji ustawy o KSC znajduje się sprecyzowanie o treści: „Podmioty krajowego systemu cyberbezpieczeństwa, inne niż wskazane w ust. 2 i 2a, mogą korzystać z systemu teleinformatycznego, o którym mowa w ust. 1, na podstawie porozumienia zawartego z ministrem właściwym do spraw informatyzacji”.

4. Rozdział 5.1: Ryzyka wpływające na realizację projektu

- Dla ryzyka „Wzrost kursu” wskazano sposób zarządzania ryzykiem: **„Przeniesienie – realizacja postępowań zakupowych odpowiednio wcześniej i z odpowiednim budżetem, tak aby dodatkowe ryzyko przenieść na Wykonawcę.”**

Uwaga.

„Wskazany sposób zarządzania ryzykiem bardziej pasuje do kategorii „Mitygacja”, a nie „Przeniesienie”.”

Odpowiedź.

Zmieniono opis sposobu reakcji na „Mitygacja”.

5. Rozdział 5.2: Ryzyka wpływające na utrzymanie efektów

- Dla ryzyka „Brak chęci do użytkowania systemu S46 przez podłączone podmioty” wskazano sposoby zarządzania ryzykiem jako: **Akceptacja – podejmowanie działań zaradczych na bieżąco i Przeniesienie – zaangażowanie innych podmiotów w uświadamianie roli systemu S46**

Uwaga.

„Należy uszczegółowić na czym mają polegać działania zaradcze oraz o jakie inne podmioty chodzi oraz wskazania w jaki sposób ma to działanie wpłynąć na podniesienie chęci użytkowania systemem. Przyjęta zasada dobrowolności udziału JST sprowadza niekontrolowane zagrożenie dla powodzenia projektu.”

Odpowiedź.

Zgodnie z zaleceniem odpowiednio rozszerzono opisy sposobów radzenia z ryzykiem.

Dobrowolność podłączania do S46 jest konsekwencją zapisów ustawy o KSC i stanowi zagrożenie, wprowadzając ryzyko w projekcie w postaci niechęci podmiotów KSC do podłączania do S46, które jednak podlega kontroli – jest wskazane jako pierwsze w rozdziale 5.1. Tam też wskazano na sposoby reakcji na tak zidentyfikowane ryzyko, co pozwala na minimalizację zagrożenia dla powodzenia projektu. Zagrożenie to jest więc kontrolowane.

6. Rozdział 6: Otoczenie prawne

- **Zgodnie z zapisem Ustawa o Krajowym Systemie Cyberbezpieczeństwa (t. j. Dz. U. 2020 poz. 1369) nie wymaga zmiany**

Uwaga.

„Brak informacji w ustawie o możliwości korzystania z systemu przez JST – mowa jest, że CSIRT MON, CSIRT NASK, CSIRT GOV, sektorowe zespoły cyberbezpieczeństwa i Prezes Urzędu Komunikacji Elektronicznej mogą korzystać z systemu teleinformatycznego na podstawie porozumienia zawartego z ministrem właściwym do spraw informatyzacji. W porozumieniu określa się zakres i warunki korzystania z systemu teleinformatycznego. W związku z powyższym wydaje się, że może być konieczna zmiana ustawy lub jak w uwadze 2.1 należy podać odpowiednią inną podstawę formalną precyzyjnie określającą role i relacje KSC v. JST.”

Odpowiedź.

W pierwszym akapicie rozdziału 1.2 „Opis stanu obecnego” został dodany opis wskazujący na sposób określenia interesariuszy zgodnie z art. 4 ustawy o KSC. Doprecyzowanie ma na celu wskazanie istniejącego stanu prawnego w tej kwestii, a w szczególności doprecyzowanie określenia grupy „podmiotów wchodzących w skład krajowego systemu cyberbezpieczeństwa”, do której odnosi się art. 46 ust. 1 pkt 1 ustawy o KSC.

W ustawie o KSC zapisano: „Art. 46. 1. Minister właściwy do spraw informatyzacji zapewnia rozwój lub utrzymanie systemu teleinformatycznego wspierającego:

- 1) współpracę podmiotów wchodzących w skład krajowego systemu cyberbezpieczeństwa”.

Zapis ten oznacza, że system teleinformatyczny, czyli S46, skierowany jest do wszystkich podmiotów krajowego systemu cyberbezpieczeństwa, wymienianych w art. 4.

Podmioty takie jak: zespoły CSIRT poziomu krajowego, sektorowe zespoły cyberbezpieczeństwa i Prezes Urzędu Komunikacji Elektronicznej, są podmiotami szczególnymi w systemie KSC, stąd też oddzielny ust. 2 wskazujący te podmioty.

- Dla celu 2: **„Zwiększenie liczby podmiotów krajowego systemu cyberbezpieczeństwa posiadających umiejętność posługiwania się systemem S46.”** Sformułowano KPI: **„Liczba pracowników objętych szkoleniami w zakresie umiejętności cyfrowych.”**

Uwaga.

„W projekcie zaplanowano tylko szkolenie z zakresu wykorzystania systemu oraz jako wskaźnik podaje się podniesienie kompetencji cyfrowych podczas gdy w zidentyfikowanych problemach jest mowa o niewystarczającym poziomie wiedzy pracowników JST. Wydaje się, że przeszkolenie z wykorzystania systemu jest zatem niewystarczająca odpowiedzią na zidentyfikowany problem. Być może KPI powinno być inaczej zdefiniowane.”

Odpowiedź.

KPI „Liczba pracowników objętych szkoleniami w zakresie umiejętności cyfrowych” jest obowiązkowy i nie ma możliwości redefiniowania, czy zmiany jego treści. KPI jest narzucony przez Instytucję Zarządzającą, czyli Ministerstwo Funduszy i Polityki Regionalnej i każdy projekt w ramach REACT-EU musi ten KPI uwzględnić we wniosku.

Przeszkolenie pracowników z obsługi S46 oczywiście nie może i nie jest jedyną reakcją na zidentyfikowany problem, jaka będzie podejmowana ogólnie przez Państwo. W ramach innych projektów ten problem też musi być zaadresowany. Jednak S46 ma na celu wdrożenie konkretnego systemu i projekt ten może zapewnić reakcję na zidentyfikowany problem w zakresie związanym z systemem teleinformatycznym S46. W związku z powyższym przeszkolenie pracowników z działania S46 jest jak najbardziej przeszkoleniem z „umiejętności cyfrowych” – w zakresie ujętym w projekcie.

Dodatkowe zmiany w trybie autokorekty.

W rozdziale 2.1, w Celu 1, został zmodyfikowany opis metody pomiaru KPI poprzez uszczegółowienie opisu grupy podmiotów do których adresowany jest projekt. Grupę tę opisano jako **JST, jednostki podległe lub nadzorowane przez JST oraz jednostki realizujące zadania publiczne wspierające JST**. Użyte w poprzedniej wersji „JST, jednostek otoczenia JST i należących do JST” budziło wątpliwości interpretacyjne. Modyfikacja odpowiada na zalecenie RA, zgłoszone w uwadze 1, wskazująca konieczność doprecyzowanie interesariuszy projektu.

Z poważaniem

Wojciech Pawlak
p.o. Dyrektora NASK-PIB

/podpisano elektronicznie/