|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ***Nazwa dokumentu:*** Opis założeń projektu informatycznego: Podłączenie 385 nowych podmiotów krajowego systemu Cyberbezpieczeństwa do zintegrowanego systemu zarządzania cyberbezpieczeństwem (system S46) oraz dalszy rozwój tego systemu. | | | | | |
| **Lp.** | **Organ wnoszący uwagi** | **Jednostka redakcyjna, do której wnoszone są uwagi** | **Treść uwagi** | **Propozycja zmian zapisu** | **Odniesienie do uwagi** |
| **1** | **GUS** | 2.2. Udostępnione e-usługi, pkt. 2 | Brak uwzględnienia w założeniach projektu systemu modułu alertowego, obejmującego ochroną systemy przypisane do poszczególnych podmiotów publicznych, tj. wysyłanie alertów tylko do tych podmiotów, w których przypadku występuje konkretna podatność. | Po treści:  Usługa wymiany wiadomości pomiędzy podmiotami kluczowymi i ważnymi – dostosowana do potrzeb podmiotów kluczowych i ważnych wymiana wiadomości będzie realizowana co najmniej w formie tekstowej z załącznikami, umożliwi podmiotom kluczowym i ważnym dwustronną komunikację indywidualną lub grupową (kierowaną do grup użytkowników zgodnie z klasyfikacją podmiotów KSC).  **Dodać zapis:**  *„Wprowadzenie usługi alertów, obejmującej ochroną systemy przypisane do poszczególnych podmiotów publicznych, dystrybucja alertów do podmiotów, w których przypadku występuje konkretna podatność.”* |  |
| **2** | **GUS** | 7.5. Bezpieczeństwo | Brak informacji o stosowaniu uwierzytelniania dwuskładnikowego (2FA) lub wieloskładnikowego (MFA) oraz kwestii odzyskiwania kont i haseł użytkowników podmiotów publicznych. | Po treści:  „System oparty jest na mechanizmie RBAC w obsłudze użytkowników.”  **Dodać zapis:**  *„System stosuje do logowania użytkowników uwierzytelnianie dwuskładnikowe oraz umożliwia odzyskiwanie kont i haseł”* |  |
| **3** | **GUS** | 2.1. Cele i korzyści wynikające z projektu,  Cel - 2 | Brak informacji o cykliczności szkoleń w założeniach projektu. Niezbędne są cykliczne szkolenia dla pracowników podmiotów publicznych (Zarówno w przypadku zmian w zatrudnieniu pracowników lub wprowadzenia nowych funkcjonalności, czy też podnoszenia wersji), które byłyby realizowane w ramach wskazanej w założeniach projektu platformy szkoleniowej  i e-learningowej. | Po treści:  „Zwiększenie liczby pracowników posiadających umiejętność posługiwania się systemem S46, w podmiotach krajowego systemu cyberbezpieczeństwa”  **Dodać zapis:**  *„(…) w tym realizowanie cyklicznych i obligatoryjnych szkoleń dla pracowników podmiotów krajowego systemu cyberbezpieczeństwa, zarówno w przypadku zmian w zatrudnieniu pracowników, jak i w przypadku wdrażania aktualizacji oprogramowania wprowadzających nowe funkcjonalności.”* |  |
| **4** | **GUS** | 7.5. Bezpieczeństwo | Brak doprecyzowania konkretnych norm jako podstawy w zakresie projektowania i eksploatacji systemu. Należy wymienić wszystkie normy, w oparciu o które projekt będzie realizowany, np. wskazać konkretnie m.in. normę 27002. W treści założeń znajduje się informacja określona w sposób ogólny, iż:  „*Projektowanie i eksploatacja systemu wg założeń projektu ma się odbywać z uwzględnieniem Polskich Norm dotyczących*  *bezpieczeństwa (w szczególności PN-EN ISO/IEC 27001) jak również dobrych praktyk ITIL*.” | Po treści:  Projektowanie i eksploatacja systemu odbywa się z uwzględnieniem Polskich Norm dotyczących  bezpieczeństwa (w szczególności PN-EN ISO/IEC 27001) (…)  **Dodać zapis:**  *„(…) ale również z uwzględnieniem normy ISO 27002 oraz norm (…)”*– szczegółowe wskazanie które normy będą miały zastosowanie powinno być opisane przez projektodawców |  |
| **6** | **GUS** | 5.1. Ryzyka wpływające na realizację projektu | Brak odniesienia do planowanych zmian legislacyjnych, tj. m.in.: założeń Dyrektywy NIS 2, która zostanie wdrożona do 17 października 2024 r. | Po treści:  „ścisła współpraca z ministrem właściwym do spraw informatyzacji, dostosowywanie zakresu do sygnalizowanych potrzeb”  **Dodać zapis:**  *„(…) w tym m.in. dostosowanie systemu do planowanych zmian związanych z wdrożeniem założeń Dyrektywy NIS 2.*” |  |
| **7** | **GUS** | 1.2. Opis stanu obecnego | Brak informacji dot. sposobu szyfrowania. MPLS sam w sobie nie zapewnia szyfrowania ruchu, a tym samym nie chroni przed atakami typu man-in-the-middle oraz nie zapewnia poufności danych. | Po treści:  „System S46 składa się z redundantnego systemu centralnego, wydzielonej sieci teleinformatycznej opartej na MPLS, podłączonych z jej wykorzystaniem uczestników (z zainstalowanymi u nich urządzeniami dostępowymi – SBU) oraz podłączonymi do systemu centralnego podmiotami KSC: CSIRT GOV, CSIRT MON, CSIRT NASK, organami właściwymi, Pełnomocnikiem Rządu ds. Cyberbezpieczeństwa i innymi.”  **Dodać zapis:**  *„System posiada mechanizmy szyfrowania (…)”* – szczegółowy opis mechanizmu szyfrowania powinien być opisany przez projektodawców |  |
| **8** | **GUS** | 2.1. Cele i korzyści wynikające z projektu, Cel – 3, Korzyść | Brak informacji o kosztach podłączenia podmiotu krajowego systemu cyberbezpieczeństwa do Systemu S46. | Po treści:  „(…) c) Udostępnienie mechanizmów komunikacji dostosowanych do potrzeb  podmiotów kluczowych i ważnych;”  **Dodać zapis** dot. kosztów ponoszonych przez podmioty krajowego systemu cyberbezpieczeństwa. |  |