

Streszczenie menadżerskie

Niniejszy dokument ma na celu podsumowanie prac zrealizowanych przez Zespół COI w terminie od 10 marca 2016 r. do 24 marca 2016 r. w ramach zlecenia z pisma MC z dnia 29.02.2016 roku, znak SAS.512.2.2016.

Zakres prac obejmował przegląd przejmowanych przez COI do utrzymania systemów (ePUAP, SG BIP, PAP, SSDIP). W ramach przeglądu uwzględniono poniższe obszary:

- Funkcjonalności systemów,
- Infrastrukturę systemów,
- Bezpieczeństwo,
- Organizacja.

W wyniku przeglądu określono status dla ww. obszarów, który zestawiono poniżej:

Funkcjonalności	Przetestowano 83% funkcjonalności	Zidentyfikowano: brak kompletnego „katalogu usług”, brak wszystkich opisów funkcjonalnych (niektóre funkcjonalności „odkrywane” w ramach testów), brak potwierdzenia poziomu świadczonych usług SLA (niejasne kryteria przydziału kategorii „utrudnienia” i „niedostępność” – niedostępność PZ jest kategoryzowana, jako „utrudnienie”) i monitoringu wydajności funkcjonalności i użyteczności, brak spójności pomiędzy środowiskami produkcyjnymi i testowymi, braki dokumentacyjne.
Infrastruktura	Przejmowana infrastruktura pozwala na funkcjonowanie systemów po wykonaniu niezbędnych konfiguracji, a docelowo migracji na ZIR	Złożona architektura systemu, urozmaicona nieaktualnymi systemami i serwerami oraz brakiem krytycznych procedur administracyjnych. Niezbędne jest wykonanie konfiguracji, a w szczególności strojenia baz danych oraz serwerów aplikacyjnych. Niezbędne uruchomienie alternatywnego rozwiązania w miejsce obecnego systemu zarządzania tożsamością.
Bezpieczeństwo	Obecne rozwiązania wymagają znaczących i natychmiastowych korekt	W krótkim okresie należy rozwiązać podstawowe problemy związane z bezpieczeństwem (konfiguracja, zarządzanie kontami administracyjnymi, aktualizacja oprogramowania – ssh, http). W średniej i długiej perspektywie niezbędne jest doprowadzenie systemu do oczekiwanego poziomu bezpieczeństwa, które będzie wymagało znaczących zmian w konfiguracjach, systemach, jak i samej architekturze.
Organizacja	Zagrożenie braku ciągłości osobowej do czasu zbudowania kompetencji w COI	W krótkim czasie niezbędne jest: zrekrutowanie osób do COI celem zapewnienia ciągłości działania, przejście z aplikacji OTRS na kompleksową aplikację ITSM, budowa kompetencji po stronie MC (właścicielstwo biznesowe) i COI (utrzymanie, rozwój), pilne uruchomienie linii wsparcia (ServiceDesk, Utrzymanie, Zespoły administratorów infrastruktury,

aplikacji, analityków biznesowych, testów funkcjonalnych). Niezbędne jest wypracowanie procedur obsługi użytkowników (indywidualnych, instytucjonalnych). Jest to kluczowy obszar dla całości utrzymania i przyszłego rozwoju systemu.

W ramach przeglądu dla poszczególnych obszarów zidentyfikowano inicjatywy krótko-, średnio- i długoterminowe, które przypisano do projektów Projekt A dla krótkoterminowych (do 3 miesięcy) działań mających na celu zapewnienie bieżącej eksploatacji i utrzymania przejmowanych systemów. Projekt B dla długoterminowych działań mających na celu: wypracowanie docelowego rozwiązania, architektury systemowej i funkcjonalnej oraz analizy z punktu widzenia potrzeb użytkownika (User Experience).

	ORGANIZACJA	FUNKCJONALNOŚCI	INFRASTRUKTURA	BEZPIECZEŃSTWO
Inicjatywy krótkoterminowe (Projekt A)	O1 - Powołanie Linii wsparcia – z uwzględnieniem opracowania procedur O2 - Wdrożenie ITSM Atmosfera zamiast OTRS O3 –Wskazanie właściciela biznesowego po stronie MC O4 –Budowa Zespołu Wsparcia (cz. 1 – SD administratorzy infrastruktury, administratorzy aplikacji i analitycy biznesowi)	F1 - Przygotowanie opisu procesu zarządzania poziomem usług F2 - Opracowanie szablonu raportu poziomów świadczenia usług F3 – Analiza funkcjonalności ePUAP vs. obywatel.gov.pl	I1 - Skatalogowanie procedur administracyjnych i ich opracowanie I2 - Aktualizacja serwerów i aplikacji (w tym ich konfiguracji) I3 - Poprawienie kodu aplikacji (niezbędne zmiany) I4- Przygotowanie koncepcji dot. systemu zarządzania tożsamością	B1- Weryfikacja poprawa konfiguracji urządzeń w niezbędnym, możliwym w krótkim terminie okresie B2 - Aktualizacja systemów operacyjnych, oprogramowania układowego, usług zainstalowanych na poszczególnych serwerach B3 - Opracowanie i wdrożenie podstawowych standardów bezpieczeństwa B4- Uruchomienie monitoringu 24h bezpieczeństwa środowiska produkcyjnego
Inicjatywy średnio- i długoterminowe (Projekt B)	O5 - Wypracowanie zasad współpracy i struktur organizacyjnych dla docelowego modelu ePUAP po stronie MC i COI O6 - Weryfikacja wypracowanych	F4 - Ustalenie po stronie MC kompletnego katalogu usług i funkcjonalności F5 - Uzgodnienie z MC warunków SLA i zbudowanie kompletnego systemu raportowego	I5 - Uruchomienie nowego wydzielonego Profilu Zaufanego I6 - Wirtualizacja serwerów I7- Migracja infrastruktury ePUAP na środowisko Zintegrowanej	B5 - Eliminacja luk bezpieczeństwa (konfiguracja i wymiana urządzeń) B6 - Ponowne przeprowadzenie pełnych testów bezpieczeństwa B7 - Opracowanie Polityki

	<p>standardów i narzędzi O7 - Szkolenia merytoryczne i miękkie dla zespołu wsparcia O8 - Budowa bazy wiedzy O9- Budowa Zespołu Wsparcia(docelowego)</p>	<p>F6 - Opracowanie 100% brakujących opisów funkcji wykazanych w katalogu usług F7 - Kolekcjonowanie danych dot. dostępności i wydajności w celu określenia mierników F8 - Określenie docelowych wartości mierników wydajności F9 - Uruchomienie mechanizmów monitorowania wydajności F10 - Stworzenie referencyjnych środowisk testowych F11 - Uruchomienie procesu zarządzania poziomem usług w zakresie parametrów wydajnościowych</p>	<p>Infrastruktury Rejestrów I8 - Optymalizacja kosztów utrzymania I9-Wdrożenie docelowego systemu zarządzania tożsamością</p>	<p>Bezpieczeństwa Systemów B8- Rozważenie i podjęcie decyzji dot. wdrożenia systemu klasy SIEM (ang. Security information and event management) B9 – Opracowanie planów Business Continuity Plan I Disaster Recovery</p>
--	---	---	---	--

Dla realizacji zidentyfikowanych inicjatyw w ramach projektów A i B niezbędne jest zapewnienie niżej wymienionych kluczowych czynników sukcesu:

- Zapewnienie zasobów osobowych dla utrzymania i rozwoju systemu
- Doprecyzowanie zasad współpracy pomiędzy MC i COI poprzez:
 - Wskazanie właściciela biznesowego po stronie MC,
 - Wypracowanie modelu współpracy pomiędzy MC i COI,
 - Wypracowanie skutecznych struktur zarządzania projektami A i B,
- Uzgodnienie docelowej wizji i funkcjonalności dla ePUAP:
 - Zakres realizacji projektów zależny od decyzji biznesowych MC
 - Decyzje związane z architekturą Profilu Zaufanego – zmiany wpłyną na integrację e-Uслуг z PZ
- Wyeliminowanie długotrwałej zależności od zewnętrznych podmiotów (vendor-lock).

Z uwagi na objętość i złożoność zakresu przeglądu jak również przygotowaną w formie prezentacji, proponujemy zorganizowanie spotkania, na którym przedstawimy wnioski i rekomendacje wynikające z przedmiotowego przeglądu oraz zaplanowany przez COI plan działania.