



Biała Piska, dn. 20.12.2024 r.

Zamawiający:  
Gmina Biała Piska  
ul. Pl. A. Mickiewicza 25  
12-230 Biała Piska

Znak sprawy: **Or.ZP.271.27.2024**

Odpowiedź na pytanie dotyczące postępowania prowadzonego pn.  
**Zakup sprzętu i oprogramowania informatycznego związany z realizacją projektu  
w ramach grantu Cyberbezpieczny Samorząd**

Zamawiający informuje, że w terminie określonym zgodnie z art. 284 ust. 2 ustawy z 11 września 2019 r. – Prawo zamówień publicznych (Dz.U. 2024 r. poz. 1320), Wykonawca zwrócił się do zamawiającego z zapytaniem o wyjaśnienie treści SWZ.

W związku z powyższym, zamawiający udziela następujących wyjaśnień:

**Pytanie:**

1) Zamawiający w OPZ oczekuje "Wykonawca przygotuje projekt techniczny realizacji koncepcji, uwzględniający dobre praktyki i rekomendacje eksploatacyjne, po wykonaniu analizy istniejącego u Zamawiającego rozwiązania wraz z koncepcją uruchomienia produkcyjnego klastra serwerowego, migracji maszyn wirtualnych, migracji baz danych SQL, Firebird, PostgreSQL, aktualizacji systemów operacyjnych Windows Serwer 2021 i 2019 uwzględniając obecne u Zamawiającego uwarunkowania organizacyjne i sprzętowe, łącznie zwane dalej projektem technicznym." "Klaster zostanie tak skonfigurowany, aby można było nim zdalnie zarządzać i zostanie uruchomione dwuskładnikowe uwierzytelnianie na klastrze. Klaster zostanie tak skonfigurowany, aby jak najbardziej automatycznie zgłaszał problemy dla administratora pocztą email oraz automatycznie naprawiał błędy z wbudowanymi dyskami lub serwerami, i w przypadku problemów z serwerem, drugi serwer automatycznie przejmował pracę serwera uszkodzonego" "43. Oprogramowanie wirtualizacyjne musi automatycznie przenosić bezprzerwowo maszyny wirtualne pomiędzy węzłami w klastrze w zależności od ich obciążenia." wobec powyższego: a) czy Zamawiający chce na serwerach pracujących w klastrze w trybie ciągłej dostępności korzystać i obsługiwać aplikacje dziedzinowe i bazy danych pod aplikacje dziedzinowe oprócz systemów bezpieczeństwa jakie Zamawiający zamierza kupić ? b) jeśli tak to czy wykonawca będzie również zobowiązany do migracji ze starych serwerów oprogramowania do maszyn wirtualnych na nowych serwerach w klastrze HA (jest to na tyle ważne z uwagi na przestoje pracy Urzędu podczas migracji i dostępu niektórych pracowników w celu przetestowania takiej migracji)?

**Odpowiedź:**

Zamawiający zamierza przeznaczyć produkcyjny klaster serwerowy głównie na cele instalacji i użytkowania oprogramowania do cyberbezpieczeństwa, zarówno kupowanego w ramach grantu Cyberbezpieczny Samorząd, tj. oprogramowania SIEM, EDR i analizy podatności, a także innego, które Zamawiający posiada lub będzie posiadał w zakresie cyberbezpieczeństwa. W ten sposób Zamawiający posiadać będzie bezpieczne środowisko oparte o hiperkonwergency klaster. Dodatkowo, realizując cele grantu Cyberbezpieczny Samorząd w celu ograniczenia ryzyka utraty informacji (wymaganie W16 określone w



Poradniku „Cyberbezpieczny Samorząd”) hiperkonwergency klaster umożliwi stosowanie redundancji poprzez posiadanie duplikatów danych, systemów i infrastruktury w celu zapewnienia dostępności w przypadku awarii także dla systemów informatycznych, z których korzysta Urząd w bieżącej pracy zapewniając wsparcie sprzętowe dla krytycznie ważnych z perspektywy bezpiecznego działania urzędu baz danych i aplikacji i w związku z tym Wykonawca będzie również zobowiązany do migracji ze starych serwerów oprogramowania do maszyn wirtualnych na nowych serwerach w klastrze HA. Taka organizacja środowiska informatycznego podniesie istotnie cyberbezpieczeństwo urzędu gdyż:

- Skoncentrowanie zasobów krytycznych w jednym klastrze ułatwi zarządzanie bezpieczeństwem, ponieważ wszystkie maszyny wirtualne i dane będą dostępne z jednego środowiska, co ograniczy potencjalne luki wynikające z rozproszenia danych;
- Umożliwi zintegrowane monitorowanie, co da administratorom szerszy wgląd w cały system, pozwalając na szybsze wykrywanie i reagowanie na zagrożenia;
- Wysoka dostępność i redundancja, które zapewnia HCI, zminimalizują ryzyko utraty danych i przestojów. Zabezpieczenie danych w takich systemach obejmuje automatyczne backupy, kopie zapasowe oraz możliwość ich odtworzenia w przypadku awarii;
- Możliwość szybkiego skalowania i dodawania nowych zasobów umożliwi łatwe wdrażanie nowych środków bezpieczeństwa. Aktualizacje zabezpieczeń będą szybciej wdrażane i testowane w takim zintegrowanym środowisku.

BURMISTRZ  
  
Franciszek Paweł Romankiewicz

Sporządził: Damian Modzelewski 