Warszawa, 29 maja 2026 r.

ZESTAW ODPOWIEDZI NR 2

Dotyczy postępowania nr 44/PN/2026 na wybór Wykonawcy zamówienia obejmującego zakresem dostawę, instalację, konfigurację oraz uruchomienie kompletnej infrastruktury serwerowo-macierzowej wraz z systemem kopii zapasowych i archiwizacji danych na potrzeby Polskiego Holdingu Nieruchomości S.A.

W związku z ogłoszeniem ww. postępowania, Zamawiający otrzymał następujące pytania od Podmiotów zainteresowanych udziałem w postępowaniu:

Pytanie nr 3:
W punkcie dotyczącym ochrony przed ransomware wskazano, że rozwiązanie ma realizować ochronę „natywnie na poziomie dysku", podając jako przykład „sprzętowo wspierane niezmienne migawki (immutable snapshots)".

Zwracamy uwagę, iż mechanizmy typu immutable snapshots są standardowo realizowane na poziomie systemu macierzowego (kontrolerów i oprogramowania macierzy), a nie na poziomie pojedynczych dysków.

W związku z powyższym prosimy o doprecyzowanie, czy Zamawiający:
a) dopuszcza rozwiązania realizujące ochronę przed ransomware na poziomie macierzy (np. immutable snapshots),
oraz
b) wymaga, aby ochrona była realizowana bezpośrednio na poziomie nośników danych (np. mechanizmy typu WORM lub sprzętowe blokady zapisu na dyskach).

Odpowiedź na pytanie nr 3:
Zamawiający dopuszcza rozwiązania realizujące ochronę przed ransomware zarówno na poziomie systemu macierzowego (np. immutable snapshots), jak i bezpośrednio na poziomie nośników danych. Jednocześnie Zamawiający wyjaśnia, że w kryterium punktowym „Sprzętowa odporność na ransomware" dodatkowo punktowane będą rozwiązania posiadające mechanizmy ochrony realizowane natywnie na poziomie nośników danych lub wspierane sprzętowo przez architekturę storage, wykraczające poza standardową realizację funkcji wyłącznie na poziomie kontrolera macierzy.

Pytanie nr 4:
7 Kryteria Oceny Ofert i 7.1 SPRZĘTOWA ODPORNOŚĆ NA RANSOMEWARE: Prosimy o wyjaśnienie, czym z perspektywy Zamawiającego różni się ochrona przed ransomware realizowana na poziomie dysków, od tej realizowanej na poziomie kontrolerów? Skoro jest dodatkowo punktowane aż 15 punktami.
Ile punktów w takim razie należy przyjąć dla rozwiązania realizującego ochronę przed ransomware na poziomie systemu operacyjnego macierzy, a ile takie które realizuję na poziomie portów połączeniowych? To są szczegóły architektoniczne macierzy (zupełnie pominięte w specyfikacji w pkt 4.1, 4.2), a ujęte jedynie w ramach dodatkowej punktacji.
Jeżeli efektem końcowym jest utworzenie nieusuwalnej kopii migawkowej to nie ma znaczenia który komponent macierzy odpowiada za jego realizację.

Wnosimy o usunięcie tego kryterium punktowego, ponieważ wskazuje ono w bardzo sztuczny sposób na IBM i stanowi zabieg nieuczciwej konkurencji promujący rozwiązania IBM FlashSystem: https://www.ibm.com/support/pages/ibm-flashsystems-flashcore-module-4-and-integrated-ransomware-threat-detection.

Odpowiedź na pytanie nr 4:
Zamawiający informuje, że Zapytanie ofertowe w powyższym zakresie pozostaje bez zmian.

Pytanie nr 5:
Pytanie dotyczące 7. Kryteria Oceny Ofert i 7.2 ODPORNOŚĆ NA AWARIĘ UKŁADU PAMIĘCI IBM stosuje dyski FCM zbudowane z komórej QLC które (co wynika z fizyki układów NAND) wypalają się szybciej niż komórki TLC. Dlatego też IBM FlashSystem wraz ze swoją technologią FCM stosuje metody przeciwdziałania uszkodzeniu dysków które polegają na monotażu nadmiarowych komórek – dokładnie w sposób opisany przez Państwa w tym kryterium punktowym.
Wnosimy o usunięcie wymagania lub chociaż zrównania go z równowa, tj.:
5 pkt – każdy oferowany dysk posiada mechanizm redundancji na poziomie układów scalonych (chip-level redundancy), dzięki któremu awaria pojedynczego chipa pamięci nie powoduje awarii ani wyłączenia całego dysku LUB zaoferowanie macierzy podstawowej wykonanej w technologii dysków NVMe SSD TLC
Wtedy efekt będzie jednolity – otrzymacie Państwo nośniki o zwiększonej trwałości.

Odpowiedź na pytanie nr 5:
Zamawiający podtrzymuje wymaganie dotyczące odporności na awarię układów pamięci, przy czym dopuszcza rozwiązania równoważne zapewniające podwyższoną odporność i trwałość nośników danych.
W związku z powyższym zapis otrzymuje brzmienie:
„5 pkt – każdy oferowany dysk posiada mechanizm redundancji na poziomie układów scalonych (chip-level redundancy), dzięki któremu awaria pojedynczego chipa pamięci nie powoduje awarii ani wyłączenia całego dysku, lub zastosowano rozwiązania równoważne zapewniające podwyższoną trwałość i odporność nośników klasy enterprise/datacenter, w szczególności oparte o technologię NVMe SSD TLC lub równoważną.”