

Wymagania Infrastruktury i Cyberbezpieczeństwa do dokumentu RFP – Pilotaż VPP (wymagania wstępne)

1. Preferowane jest, żeby dedykowane serwery pośredniczące w wymianie danych pomiędzy on-prem a usługami chmurowymi były umieszczone w DMZ.
2. Preferowane jest, żeby serwery pośredniczące w przekazywaniu danych nie pobierały danych bezpośrednio ze źródeł, tylko przez bazę/stację przesiadkową, lub na bazie widoków przygotowanych po stronie bazy źródłowej.
3. W przypadku konieczności przekazywania danych z „on-prem” oraz „chmury” należy udzielić najniższych możliwych uprawnień na źródłach danych.
4. Preferowane jest, żeby przesyłanie danych do chmury odbywało się cyklicznie ze środowisk „on-prem” do „chmury”.
5. Konta techniczne, dedykowane dla każdego systemu źródłowego, powinny mieć ograniczone możliwości logowania się tylko do wskazanych usług, powinny być kontami zarządzanymi (ustalony cykl życia konta).
6. Rozwiązanie powinno umożliwiać podział uprawnień w kontekście użytkownika i administratora (RBAC).
7. Dane w ruchu („in-transit”) powinny być zabezpieczone z wykorzystaniem protokołu co najmniej TLS 1.2 (lub nowszego) z wykorzystaniem certyfikatów wydawanych przez Publicly Trusted CA.
8. Wskazany przez Orlen dostawca tożsamości powinien być jedynym źródłem tożsamości użytkowników dla środowisk chmurowych.
9. Projektowane rozwiązania „chmurowe” powinny tam, gdzie to wynika ze specyfiki projektowanej aplikacji utylizować model trzy warstwowy (prezentacja, aplikacja, dane – „three tiers model”).
10. Aplikacje wdrażane w chmurze zarządzanej przez Orlen, powinny być zabezpieczane adekwatnymi narzędziami cyberbezpieczeństwa które będą przysyłać logi bezpieczeństwa do systemu klasy SIEM.
11. Zalecane jest wykorzystanie dostępu prywatnego do usług chmurowych.
12. Dla projektowanego systemu należy przygotować proces odtworzenia systemu w przypadku awarii lub czasowego braku dostępności oraz analizę wykonalności planu wyjścia z chmury (Exit Plan).
13. Dane w projektowanym systemie muszą być przetwarzane tylko w Europejskim Obszarze Gospodarczym (EOG).

14. Dane uwierzytelniające wykorzystywane w systemach chmurowych muszą być przechowywane i przetwarzane w sposób bezpieczny - niedozwolone jest przechowywanie haseł i sekretów w formie jawnej.
15. Ruch w ramach komponentów chmurowych należy ograniczyć tylko do niezbędnych portów oraz adresów.
16. Rozwiązania powinny być wdrażane w modelu IaC.
17. Projektowanie rozwiązań bez pojedynczych punktów awarii z użyciem mechanizmów nadmiarowości np. Load Balancer.
18. Wdrażane rozwiązania powinny być wyposażone w mechanizmy monitoringu z możliwością udostępniania alarmów do systemów HelpDesk on-prem.
19. Zalecane jest przygotowanie architektury zgodnie z pryncypiami podejścia Zero Trust Architecture.
20. Dostawca będzie musiał współpracować z zamawiającym w obszarach które są konfigurowane wyłącznie przez personel zamawiającego: uprawnienia, tożsamości użytkowników, konta serwisowe, konta techniczne/serwisowe, konfiguracja sieci, zapory sieciowe, polityki organizacyjne oraz inne pokrewne obszary w zależności od zaproponowanej technologii.