Załącznik nr 9

Wymogi dotyczące cyberbezpieczeństwa dostarczonego systemu

1. Wykonawca w przedmiocie zamówienia jest zobowiązany do stosowania praktyk i technologii mających na celu ochronę systemów komputerowych, sieci i danych przed nieuprawnionym dostępem, atakami i szkodami. Obejmuje ono ochronę poufności, integralności i dostępności informacji.
   - Ograniczanie dostępu do informacji (funkcjonalności zapewniające możliwość ograniczenia dostępu do systemu);
   - Należy stosować zasady najmniejszego przywileju, ograniczając uprawnienia użytkowników do minimum niezbędnego do wykonywania ich zadań;
   - Procedury bezpiecznego logowania;
   - Dokumentowanie procedur eksploatacyjnych (dokumentacja systemu);
   - Zarządzanie pojemnością (zapewnienie odpowiedniej wydajności systemu i jej monitorowania);
   - Oddzielanie środowisk rozwojowych, testowych i produkcyjnych;
   - Rejestrowanie zdarzeń (np. zapewnienie mechanizmów rejestrowania zdarzeń);
   - możliwość eksportu logów do analizy z użyciem narzędzi SIEM do korelacji zdarzeń i wykrywania potencjalnych zagrożeń;
   - Ochrona informacji w dziennikach zdarzeń (funkcjonalność zabezpieczenia logów zawierających informacje wrażliwe);
   - Rejestrowanie działań administratorów i operatorów (działania wykonywane administratorów i operatorów systemów muszą być rejestrowane, a logi zabezpieczone);
   - Synchronizacja zegarów;
   - Ochrona transakcji usług aplikacyjnych (zastosowanie mechanizmów zabezpieczających przed przerwaniem transmisji, nieuprawnionymi zmianami wiadomości, powieleniem itp.);
   - Testowanie bezpieczeństwa systemów;
   - Ochrona danych testowych;
   - Prywatność i ochrona danych identyfikujących osobę (w zakresie zapewnienia przez system zabezpieczeń danych osobowych zgodnych z wymogami prawnymi).

- Należy zaplanować procedury oceny bezpieczeństwa dostarczanych przez dostawców systemów i usług, które będą zgodne z polityką bezpieczeństwa organizacji oraz wymogami Dyrektywy NIS2. W umowach z dostawcami należy jasno określić wymagania dotyczące cyberbezpieczeństwa oraz odpowiedzialność za ich naruszenie;
- Należy stosować uwierzytelnianie dwuskładnikowe (2FA) jako standard dostępu dla osób uprawnionych do modyfikacji systemu oraz dla kont o najwyższym poziomie dostępu.
- Konieczność zastosowania prywatnego APN dla dostarczonych kart SIM.Dostęp do prywatnej sieci APN realizowana poprzez szyfrowany tunel VPN zestawiony pomiędzy Zamawiającym, a dostawcą APN. Reazlizacja tunelu po stronie dostawcy.