

Załącznik nr 1 do zapytania ofertowego

Opis przedmiotu zamówienia

świadczenia doradztwa informatyczno – technologicznego w zakresie wsparcia realizacji projektu „Cyberbezpieczny Powiat Słupski”

W ramach realizowanego przedmiotu zamówienia polegającego na doradztwie informatyczno – technologicznym w zakresie wsparcia realizacji projektu:

- a) Przeprowadzanie okresowych audytów konfiguracji i optymalizacji działania firewall w celu zapewnienia prawidłowego funkcjonowania sieci oraz wykrywania błędnych konfiguracji w celu zwiększenia poziomu cyberbezpieczeństwa;
- b) Konfigurowanie firewall w celu zapewniania odpowiedniego poziomu ochrony przed nieautoryzowanym dostępem, atakami zewnętrznymi oraz innymi zagrożeniami cybernetycznymi;
- c) Zarządzanie protokołami redundancji, takimi jak STP, RSTP;
- d) Konfiguracja, zarządzanie oraz optymalizacja środowisk Windows Server w celu zwiększenia poziomu cyberbezpieczeństwa;
- e) Administrowanie środowiskiem wirtualizacyjnym w celu zapewnienia zwiększenia poziomu cyberbezpieczeństwa środowiska;
- f) Zarządzanie systemem pamięci pod względem właściwego jej zabezpieczenia przed dostępem zewnętrznym;
- g) Zarządzanie systemem monitoringu infrastruktury IT w celu zapewnienia bezpieczeństwa funkcjonujących rozwiązań informatycznych;
- e) Monitoring nowo pojawiających się zagrożeń w cyberprzestrzeni, a następnie wdrożenie działań naprawczych w celu zwiększenia poziomu cyberbezpieczeństwa;
- f) Doradztwo w zakresie funkcjonującego sprzętu oraz możliwości zwiększania jego bezpieczeństwa poprzez odpowiednią konfigurację oraz realizowanie działań zabezpieczających.
- g) Okresowe sprawdzanie poprawności wykonania kopii zapasowych
- h) Doradztwo oraz wsparcie w dokonywaniu zmian konfiguracji w infrastrukturze sieciowej oraz serwerowej.

Wsparcie w ramach doradztwa informatycznego będzie realizowane przez Wykonawcę w formie zdalnej oraz stacjonarnej, przy czym przyjmuje się, iż przez cały okres realizacji umowy Wykonawca pojawi się minimum 56 razy w siedzibie Zamawiającego, a łączna liczba godzin spędzona w siedzibie Zamawiającego wyniesie 448. Dodatkowo Wykonawca będzie zobowiązany do reakcji zdalnej na pojawiające się zagrożenia w terminie:

- Czas reakcji dla incydentu krytycznego (3 godzin);
 - Całkowite unieruchomienie systemów krytycznych (np. EZD, Geo-Info).
 - Włamanie do systemu informatycznego lub nieautoryzowany dostęp do danych wrażliwych/osobowych.
 - Ransomware – zaszyfrowanie danych i żądanie okupu.
 - Utrata dostępności sieci urzędu lub serwera produkcyjnego.

- Czas reakcji dla incydentu istotnego (8 godzin);
 - Zidentyfikowane próby nieautoryzowanego logowania do systemów (np. ataki typu brute-force).
 - Częściowe zakłócenie działania systemu, np. spowolnienie aplikacji, ograniczona dostępność funkcji.
 - Utrata dostępu do niekrytycznych usług (np. systemy pomocnicze, dostęp do intranetu).
 - Wykrycie złośliwego oprogramowania na jednym stanowisku pracy.

- Czas reakcji dla stwierdzonej podatności w obszarze cyberbezpieczeństwa (24 godz).
 - Wykrycie niezłatanej podatności w systemie operacyjnym lub oprogramowaniu.
 - Zgłoszenie przez CERT lub CSIRT podatności w używanym systemie.
 - Brak silnych haseł lub nieprawidłowa konfiguracja uprawnień użytkowników.
 - Zidentyfikowanie systemu, który nie spełnia minimalnych wymagań bezpieczeństwa.
 - Błąd konfiguracyjny w firewallu, który umożliwia dostęp z zewnątrz.