**Załącznik nr 1.1 do SWZ**

Pakiet nr 12 - Przeprowadzenie końcowego audytu w obszarze cyberbezpieczeństwa

Nazwa producenta: ……………

Typ, model, numer katalogowy: ………………

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **L.p.** | **Przedmiot zamówienia** | **J.m.** | **Cena jednostkowa netto** | **Stawka podatku VAT** | **Cena jednostkowa brutto** | **Wartość netto** | **Wartość brutto** |
| ***1*** | ***2*** | ***3*** | ***4*** | ***5*** | ***6*** | ***7*** | ***8*** |
| **1.** | Przeprowadzenie końcowego audytu w obszarze cyberbezpieczeństwa | **Przedmiot zamówienia** |  |  |  |  |  |

**Przeprowadzenie końcowego audytu w obszarze cyberbezpieczeństwa**

## Audyt zgodności z Ustawą o Krajowym Systemie Cyberbezpieczeństwa (UKSC) z uwzględnieniem dyrektywy NIS2

W zakresie dokumentacji dla oceny zgodności z UKSC oraz dyrektywy NIS2 wymagane jest wykonanie sprawdzenia zgodności systemu zarzadzania bezpieczeństwem informacji według kryteriów normy ISO/IEC 27001, oraz dodatkowych kryteriów wskazanych we wspomnianej ustawie wraz z rozporządzeniem.

Audyt musi obejmować aspekty organizacyjne oraz techniczne.

W zakresie organizacyjnym audyt powinien objąć procesy, procedury, politykę wewnętrzną organizacji oraz stosowanie się do zapisów zawartych w dokumentacji jak i w przepisach prawa. Działania audytowe musza obejmować:

* przegląd i analizę polityk bezpieczeństwa organizacji,
* weryfikację zgodności z aktualną Ustawą o UKSC oraz dyrektywą NIS2,
* zarządzanie systemami teleinformatycznymi,
* zarządzanie incydentami bezpieczeństwa,
* zarządzanie ciągłością działania,
* zarządzaniem bezpieczeństwem fizycznym organizacji.

W zakresie wymagań NIS2 audytowi muszą być poddane szczegółowo następujące wymagania:

* polityka bezpieczeństwa informacji,
* obsługa incydentu,
* ciągłość działania, np. zarządzanie kopiami zapasowymi i przywracanie normalnego działania po wystąpieniu sytuacji nadzwyczajnej, zarządzanie kryzysowe,
* bezpieczeństwo łańcucha dostaw, w tym aspekty związane z bezpieczeństwem dotyczące stosunków między każdym podmiotem a jego bezpośrednimi dostawcami lub usługodawcami,
* bezpieczeństwo w procesie nabywania, rozwoju i utrzymania sieci i systemów informatycznych, w tym postępowanie w przypadku podatności i ich ujawnianie,
* polityki i procedury służące ocenie skuteczności środków zarządzania ryzykiem w cyberbezpieczeństwie,
* podstawowe praktyki cyberhigieny i szkolenia w zakresie cyberbezpieczeństwa,
* polityki i procedury stosowania kryptografii i w stosownych przypadkach, szyfrowania,
* bezpieczeństwo zasobów ludzkich, politykę kontroli dostępu i zarządzanie aktywami,
* w stosownych przypadkach – stosowanie uwierzytelniania wieloskładnikowego lub ciągłego, zabezpieczonych połączeń głosowych, tekstowych i wideo oraz zabezpieczonych systemów łączności wewnątrz podmiotu w sytuacjach nadzwyczajnych.

Wynikiem audytu powinno być stworzenie raportu zawierającego stwierdzone nieprawidłowości oraz rekomendacje w zakresie rozwiązań zwiększających bezpieczeństwo.

Wymagania prawne stanowiące kryteria audytu:

* Dyrektywa Parlamentu Europejskiego I Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r.   
  w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148.
* Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. 1560).
* Rozporządzenie Rady Ministrów z dnia 11 września 2018 r. w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych (Dz. U. poz. 1806).
* Rozporządzenie Rady Ministrów z dnia 31 października 2018 r. w sprawie progów uznania incydentu za poważny (Dz. U. poz. 2180).
* Rozporządzenie Rady Ministrów z dnia 16 października 2018 r. w sprawie rodzajów dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej (Dz. U. poz. 2080).
* Rozporządzenie Ministra Cyfryzacji z dnia 4 grudnia 2019 r. w sprawie warunków organizacyjnych   
  i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo (Dz.U. 2019 poz. 2479).
* Rozporządzenie Ministra Cyfryzacji z dnia 20 września 2018 r. w sprawie kryteriów uznania naruszenia bezpieczeństwa lub integralności sieci lub usług telekomunikacyjnych za naruszenie   
  o istotnym wpływie na funkcjonowanie sieci lub usług (Dz. U. poz. 1830).

Podstawowe wymagania normatywne stanowiące kryteria audytu:

* PN-EN ISO/IEC 27001:2017-06 - „Technika informatyczna - Techniki bezpieczeństwa - Systemy zarządzania bezpieczeństwem informacji - Wymagania
* ISO/IEC 27001:2022 - Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności - System zarządzania bezpieczeństwem informacji - Wymagania
* PN-EN ISO 22301:2020-04 - „Bezpieczeństwo i odporność - Systemy zarządzania ciągłością działania - Wymagania”.

## Przeprowadzenie skanu systemów widocznych z internetu

1. Podstawowa analiza konfiguracji systemów UTM - Fortinet