*(WZÓR)*

**WNIOSEK**

**o udzielenie wsparcia ze środków Funduszu Cyberbezpieczeństwa**

**na rok \_\_\_\_**

**Wniosek[[1]](#footnote-1)**

|  |  |  |
| --- | --- | --- |
| **SKŁADANY PO RAZ PIERWSZY** | **UZUPEŁNIONY LUB POPRAWIONY (art. 3 ust. 4 lub art. 3 ust. 5 pkt 2** **ustawy[[2]](#footnote-2))** | **ZMIENIONY[[3]](#footnote-3)****(art. 4 ust. 4 ustawy)** |
| [ ]  | [ ]  | [ ]  |

|  |  |
| --- | --- |
| **NAZWA PODMIOTU** |  |
| **Adres** |  |
| **Wniosek dotyczy osób uprawnionych do otrzymania świadczenia teleinformatycznego na podstawie[[4]](#footnote-4)** | **Art. 5 pkt 1 ustawy** | **Art. 5 pkt 2 ustawy** |
| [ ]  | [ ]  |
| **Liczba osób realizujących zadania:** | **w podmiocie określonym** **w art. 5 pkt 1 ustawy** | **w podmiocie określonym** **w art. 5 pkt 2 ustawy** |
| Aktywne poszukiwanie zagrożeń cyberbezpieczeństwa (Cyber Threat Intelligence i Threat Hunting) |  |  |
| Analiza złośliwego oprogramowania |  |  |
| Badanie bezpieczeństwa, podatności i testowanie sprzętu lub oprogramowania |  |  |
| Ocena bezpieczeństwa systemów informacyjnych – w tym testy penetracyjne i audyty bezpieczeństwa |  |  |
| Prowadzenie specjalistycznych analiz cyberbezpieczeństwa i wykrywanie nowych podatności |  |  |
| Rozwijanie specjalistycznych narzędzi technicznych wspomagających realizację zadań z zakresu cyberbezpieczeństwa |  |  |
| Kierowanie jednostką lub komórką organizacyjną przeznaczoną do realizacji zadań z zakresu cyberbezpieczeństwa |  |  |
| Prowadzenie działań prewencyjnych zwiększających cyberbezpieczeństwo |  |  |
| Prowadzenie zaawansowanych działań z zakresu aktywnej obrony systemów informacyjnych |  |  |
| Zaawansowana obsługa incydentów |  |  |
| Analiza powłamaniowa |  |  |
| Badanie i ocena bezpieczeństwa rozwiązań ICT |  |  |
| Projektowanie, budowa i utrzymanie systemów monitorowania i detekcji incydentów oraz wsparcia funkcjonowania operacyjnego centrum bezpieczeństwa (SOC)/Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT) |  |  |
| Korelacja danych, prowadzenie analiz lub tworzenie map sytuacyjnych |  |  |
| Monitorowanie zagrożeń cyberbezpieczeństwa i incydentów na poziomie krajowym |  |  |
| Prowadzenie analiz incydentów poważnych, powiązań pomiędzy incydentami oraz opracowywanie wniosków |  |  |
| Przyjmowanie zgłoszeń i obsługa incydentów poważnych |  |  |
| Reagowanie na incydenty oraz ich klasyfikacja |  |  |
| Analiza i zarządzanie w zakresie reagowania na wykryte podatności sprzętu i oprogramowania |  |  |
| Koordynacja obsługi zgłoszonych incydentów |  |  |
| Obsługa zgłoszeń i analiza treści przypadków dystrybucji, rozpowszechniania lub przesyłania pornografii dziecięcej za pośrednictwem technologii informacyjno-komunikacyjnych |  |  |
| Specjalistyczne zadania realizowane w ramach SOC lub Centrum Zarządzania Siecią (NOC) obejmujące: monitoring bezpieczeństwa (analiza i korelacja logów), identyfikację i wstępną obsługę incydentów |  |  |
| Szacowanie ryzyka w obszarze cyberbezpieczeństwa |  |  |
| Opracowywanie i wdrażanie planów ciągłości działania i odbudowy oraz systemu zarządzania bezpieczeństwem informacji |  |  |
| Nadzór nad procesem szacowania ryzyka w obszarze cyberbezpieczeństwa |  |  |
| Przygotowywanie rekomendacji, standardów i dobrych praktyk w zakresie cyberbezpieczeństwa w szczególności podnoszących poziom bezpieczeństwa systemów informacyjnych będących w dyspozycji podmiotów krajowego systemu cyberbezpieczeństwa |  |  |
| Bieżące utrzymanie i rozwój własnych, istotnych systemów informacyjnych |  |  |
| Poszukiwanie znanych podatności sprzętu i oprogramowania w nadzorowanych systemach teleinformatycznych |  |  |
| Wstępna obsługa incydentów |  |  |
| Zabezpieczenie śladów cyfrowych |  |  |
| Rozpoznawanie zagrożeń cyberbezpieczeństwa |  |  |
| Identyfikacja oraz prowadzenie postępowań wobec operatorów usług kluczowych |  |  |
| Nadzór nad podmiotami krajowego systemu cyberbezpieczeństwa |  |  |
| Nadzór nad podmiotami świadczącymi usługi z zakresu cyberbezpieczeństwa |  |  |
| Prowadzenie akcji podnoszących świadomość w obszarze cyberbezpieczeństwa w szczególności organizacja ćwiczeń i szkoleń |  |  |
| Prowadzenie analiz w zakresie funkcjonowania krajowego systemu cyberbezpieczeństwa w tym w zakresie rozwiązań prawnych, organizacyjnych, standardów oraz certyfikacji w obszarze cyberbezpieczeństwa wraz z przygotowywaniem projektów aktów normatywnych |  |  |
| Prowadzenie analiz w zakresie spełniania przez podmioty z sektora lub podsektora warunków kwalifikujących podmiot jako operatora usługi kluczowej |  |  |
| Prowadzenie kontroli w podmiotach krajowego systemu cyberbezpieczeństwa, w tym w podmiotach świadczących usługi z zakresu cyberbezpieczeństwa |  |  |
| Współpraca krajowa lub międzynarodowa w obszarze cyberbezpieczeństwa |  |  |
| **Liczba stanowisk (pełne etaty), na których są realizowane zadania z zakresu cyberbezpieczeństwa** | **Art. 5 pkt 1 ustawy** | **Art. 5 pkt 2 ustawy** |
|  |  |
| **Maksymalna kwota prognozowanych kosztów związanych z przyznaniem świadczenia teleinformatycznego[[5]](#footnote-5)** |  |
| **Oczekiwany termin otrzymania środków na wypłatę świadczenia teleinformatycznego** | \_\_-\_\_-\_\_\_\_*dd-mm-rrrr* |
| **Liczba załączników****(w tym oświadczenie, o którym mowa w art. 3 ust. 1 pkt 2 ustawy)** |  |
| **Nr rachunku bankowego, na który mają zostać przekazane środki na wypłatę świadczenia, w przypadku pozytywnego rozpatrzenia wniosku** |  |
| **Data i czytelny podpis osoby uprawnionej[[6]](#footnote-6) do złożenia wniosku** | \_\_-\_\_-\_\_\_\_*dd-mm-rrrr* |  |

Pouczenie

1. Wniosek należy złożyć wypełniony elektronicznie lub odręcznie w sposób czytelny.
2. Informacje ujęte we wniosku w przypadku pozytywnej opinii Kolegium do spraw Cyberbezpieczeństwa, m.in. nazwa podmiotu oraz numer rachunku bankowego, będą wykorzystane do sporządzenia umowy, o której mowa w art. 2 ust. 10 ustawy o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa.
3. Przy podawaniu liczby osób realizujących określone zadania oraz liczby stanowisk w przeliczeniu na pełne etaty, na których są realizowane zadania z zakresu cyberbezpieczeństwa, osoba uprawniona do podpisania wniosku powinna rozważyć, czy dane te spełniają przesłanki objęcia ochroną zgodnie z ustawą z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych.
4. Wniosek musi zostać podpisany w sposób umożliwiający identyfikację pełnionej przez osobę funkcji w podmiocie składającym wniosek. Ponadto, jeśli wniosek jest składany w imieniu kierownika podmiotu, do wniosku należy dołączyć upoważnienie do jego złożenia.
1. Właściwe zaznaczyć [↑](#footnote-ref-1)
2. Ustawa z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa Dz.U. 2021 r. poz. 2333 [↑](#footnote-ref-2)
3. Zaznaczany w przypadku składania skorygowanego wniosku po negatywnej opinii Kolegium do Spraw Cyberbezpieczeństwa [↑](#footnote-ref-3)
4. Właściwe zaznaczyć [↑](#footnote-ref-4)
5. Należy wpisać kwotę w rozumieniu art. 3 ust. 2 – to jest kwotę prognozowanych kosztów stanowiącą limit kosztów, jakie mógłby ponieść Fundusz w związku z finansowaniem świadczenia teleinformatycznego, o którym mowa w art. 5, dla danego podmiotu w danym roku [↑](#footnote-ref-5)
6. W przypadku, gdy wniosek jest składany w imieniu kierownika podmiotu, do wniosku należy dołączyć upoważnienie do jego złożenia [↑](#footnote-ref-6)