**OBOWIĄZKI OPERATORA USŁUGI KLUCZOWEJ**

Wyznaczony decyzją administracyjną przez organ właściwy ds. cyberbezpieczeństwa operator usługi kluczowej jest zobligowany do spełnienia szeregu zadań określonych Ustawą o krajowym systemie cyberbezpieczeństwa. Przewiduje się różny czas na wypełnienie poszczególnych obowiązków.

Rozpatrując najważniejsze z nich, od chwili otrzymania od organu właściwego decyzji administracyjnej, operator usługi kluczowej zobowiązany jest do podjęcia następujących działań:

|  |  |  |
| --- | --- | --- |
| **OBOWIĄZKI OPERATORA USŁUGI KLUCZOWEJ** | | |
| **Po 3 miesiącach** | **Po 6 miesiącach** | **Po 12 miesiącach** |
| Dokonuje szacowania ryzyka dla swoich usług kluczowych | Wdraża odpowiednie i adekwatne do oszacowanego ryzyka środki techniczne i organizacyjne | Przygotowuje pierwszy audyt  w rozumieniu ustawy |
| Wyznacza osobę kontaktową z właściwymi CSIRT i organem właściwym ds. cyberbezpieczeństwa |
| Zbiera informacje o zagrożeniach i podatnościach |
| Stosuje środki zapobiegające i ograniczające wpływ incydentów na bezpieczeństwo systemu informacyjnego |
| Zarządza incydentami |
| Przekazuje sprawozdanie z audytu  wskazanym w ustawie podmiotom |
| Prowadzi działania edukacyjne wobec użytkowników |
| Stosuje wymaganą dokumentację |
| Obsługuje incydenty we własnych systemach |
| Zgłasza incydenty poważne |
| Usuwa wskazywane podatności |

|  |
| --- |
| OBOWIĄZKI TRWAŁE/CYKLICZNE  OPERATORA USŁUGI KLUCZOWEJ |
| Zarządzanie ryzykiem |
| Utrzymywanie i bezpieczna eksploatacja systemu informacyjnego |
| Kontynuowanie obsługi incydentów |
| Klasyfikowanie incydentów jako poważne na podstawie progów uznawania incydentu za poważny |
| Współdziałanie podczas obsługi incydentu poważnego i incydentu krytycznego z właściwym CSIRT MON/NASK/GOV |
| Gromadzenie informacji o zagrożeniach i podatnościach |
| Usuwanie podatności oraz informowanie o ich usunięciu organ właściwy ds. cyberbezpieczeństwa |
| Operator usługi kluczowej ma obowiązek zapewnić przeprowadzenie, co najmniej raz na 2 lata, audytu bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej. |
| Zgłaszanie do organu właściwego zmiany danych osoby kontaktowej |
| Niezwłoczne podejmowanie działań po dostrzeżeniu podatności lub zagrożeń cyberbezpieczeństwa |
| Opracowywanie, stosowanie i aktualizowanie dokumentacji dot. cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczeni usługi kluczowej |
| Operator usługi kluczowej przechowuje dokumentację dotyczącą cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej przez co najmniej 2 lata od dnia jej wycofania z użytkowania lub zakończenia świadczenia usługi kluczowej, z uwzględnieniem przepisów ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach. |
| Operator usługi kluczowej w celu realizacji zadań powołuje wewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo lub zawiera umowę z podmiotem świadczącym usługi z zakresu cyberbezpieczeństwa. |
| Operator usługi kluczowej informuje organ właściwy do spraw cyberbezpieczeństwa i właściwy CSIRT MON, CSIRT NASK, CSIRT GOV i sektorowy zespół cyberbezpieczeństwa o podmiocie, z którym została zawarta umowa o świadczenie usług z zakresu cyberbezpieczeństwa, danych kontaktowych tego podmiotu, zakresie świadczonej usługi oraz o rozwiązaniu umowy w terminie 14 dni od dnia zawarcia lub rozwiązania umowy. |