

Szkolenie on-line - „Operatorzy usług kluczowych w jednostce samorządu terytorialnego” - 19 czerwca 2020 r.



Na wstępie prowadzący przypomniał podstawowe definicje dotyczące omawianej tematyki zawarte w ustawie z dnia 5 lipca 2018 o krajowym systemie cyberbezpieczeństwa. Przypomniał, że cyberbezpieczeństwo to odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy. Nie zabrakło również definicji usługi kluczowej czyli usługi, która ma kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej, wymienioną w wykazie usług kluczowych.

Do najważniejszych obowiązków operatorów usług kluczowych należą: zarządzanie ryzykiem (w tym szacowanie ryzyka); wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych (w tym utrzymanie i bezpieczną eksploatację systemu informacyjnego; bezpieczeństwo fizyczne i środowiskowe; bezpieczeństwo i ciągłość dostaw; wdrażanie, dokumentowanie i utrzymywanie planów działania); zbieranie informacji o zagrożeniach cyberbezpieczeństwa i podatnościach na incydenty; obsługa incydentów i współpraca w tym zakresie z właściwym CSIRT; wyznaczenie osoby kontaktowej na potrzeby KSC.

Ustawa nakłada na operatorów obowiązek przeprowadzenia raz na dwa lata, audytu bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej. Audyt może przeprowadzić: jednostka oceniająca zgodność: akredytowana we właściwym zakresie, sektorowy zespół cyberbezpieczeństwa, co najmniej dwóch audytorów o określonych kompetencjach.