# Operatorzy usług kluczowych – decyzje wydane, co dalej?

**9 listopada 2018 r. upłynął termin wydawania decyzji dotyczących uznania za operatora usługi kluczowej. Podstawą do ich wydawania jest ustawa o krajowym systemie cyberbezpieczeństwa, implementująca postanowienia Dyrektywy NIS. Adresaci takich decyzji muszą teraz podjąć działania zmierzające do spełnienia szeregu obowiązków, które nakłada na nich ustawa.**

**Pierwsze spośród wskazanych ustawą terminów upłyną już po 3 miesiącach od dnia, w którym decyzja o uznaniu za operatora usługi kluczowej zostanie doręczona.**

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa przewiduje szereg obowiązków służących zapewnieniu cyberbezpieczeństwa systemów informacyjnych w sektorach usług mających kluczowe znaczenie dla utrzymania działalności państwa, do których zaliczono m.in. energetykę, transport, bankowość, ochronę zdrowia, zaopatrzenie w wodę i infrastrukturę cyfrową. Obowiązki te spoczywają na operatorach usług kluczowych, którzy status ten uzyskują na podstawie decyzji wydawanych przez organy właściwe do spraw cyberbezpieczeństwa (takim organem jest np. Minister właściwy ds. gospodarki wodnej dla sektora zaopatrzenia w wodę pitną i jej dystrybucję oraz Minister właściwy ds. energii dla sektora energetycznego).

Organ właściwy wydając decyzję bierze pod uwagę następujące kryteria: podmiot świadczy usługę kluczową z punktu widzenia działalności państwa; świadczenie tej usługi uzależnione jest od systemów informacyjnych a incydent miałby istotny skutek dla ciągłości świadczenia usługi.

Podmioty, które otrzymały lub otrzymają w nadchodzących dniach takie decyzje zobowiązane są do spełnienia wymagań przewidzianych w ustawie (decyzja jest wykonalna z chwilą doręczenia). Od decyzji przysługuje środek zaskarżenia w trybie administracyjnym tj. w terminie 30 dni od doręczenia decyzji oraz możliwość złożenia wniosku o wstrzymanie wykonania decyzji.

## Obowiązki operatorów usług kluczowych

W terminie 3 miesięcy od otrzymania decyzji operatorzy zobowiązani są:

- dokonać szacowania ryzyka dla usług kluczowych w zakresie cyberbezpieczeństwa,
- przygotować procedurę zarządzania incydentami,
- wyznaczyć osobę kontaktową z właściwym Zespołem Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT),
- przeprowadzić szkolenia użytkowników;
- uzyskać gotowość do obsługi incydentów we własnych systemach (zgłaszając incydenty uznane za poważne, usuwając wykryte podatności);

W terminie 6 miesięcy operatorzy mają obowiązek:

- na podstawie oszacowanego ryzyka wdrożyć odpowiednie i adekwatne środki techniczne i organizacyjne, aby takie ryzyko wyeliminować lub zminimalizować lub nim zarządzić,
- zebrać informacje o zagrożeniach i podatnościach systemu informatycznego,
- zastosować środki zapobiegające i ograniczające wpływ incydentów na bezpieczeństwo systemu informacyjnego,
- przygotować dokumentację dotyczącą cyberbezpieczeństwa systemów informatycznych.

W terminie 12 miesięcy operatorzy zobowiązani są:

- przeprowadzić pierwszy audyt bezpieczeństwa systemu (kolejne co najmniej raz na 2 lata);
- na wniosek organu właściwego do spraw cyberbezpieczeństwa, dyrektora Rządowego Centrum Bezpieczeństwa lub szefa Agencji Bezpieczeństwa Wewnętrznego przekazać sprawozdanie z audytu bezpieczeństwa systemu.

## Kary za niespełnianie obowiązków

Obowiązki wskazane powyżej mają zapewnić minimalny poziom cyberbezpieczeństwa w przedsiębiorstwach, które zostały uznane za kluczowe dla działalności państwa. Ich spełnienie jest nadzorowane przez właściwy organ ds. cyberbezpieczeństwa i ministra właściwego do spraw informatyzacji, którzy wykonują to zadanie w szczególności poprzez prowadzenie kontroli. W wyniku kontroli mogą zostać wydane zalecenia pokontrolne lub może zostać nałożona kara za naruszenie przepisów ustawy.

Kary wskazane w ustawie o krajowym systemie cyberbezpieczeństwa nakładane są w drodze decyzji administracyjnej i sięgają aż **1 000 000 zł dla podmiotu zobowiązanego do wdrożenia określonych wymagań określonych w ustawie**. Dodatkowo, na kierownika operatora usługi kluczowej, który nie dochował należytej staranności w wypełnianiu nałożonych na niego obowiązków może zostać nałożona kara w wysokości 200% miesięcznego wynagrodzenia.

Na dalsze pytania odpowiedzą eksperci z zakresu cyberbezpieczeństwa z zespołu prawa własności intelektualnej i TMT kancelarii WKB:

**Agnieszka Wiercińska-Krużewska**
adwokat, senior partner
agnieszka.wiercinska@wkb.pl

**dr Marek Porzeżyński**
prawnik
marek.porzezynski@wkb.pl