NASK
PAŃSTWOWY INSTYTUT BADAWCZY

Poradnik dla samorządów - ustawa o krajowym systemie cyberbezpieczeństwa

SPIS TREŚCI:

I. Ustawa o Krajowym Systemie Cyberbezpieczeństwa

Ustawa o krajowym systemie cyberbezpieczeństwa (KSC), z 5 lipca 2018 roku, to pierwszy akt prawny w tym zakresie w Polsce. Jest to implementacja do porządku krajowego tzw. Dyrektywy NIS[1]. Ustawa obowiązuje od 28 sierpnia 2018 roku. Dotyczy m.in. organizacji krajowego systemu cyberbezpieczeństwa, zadań i obowiązków podmiotów wchodzących w skład tego systemu oraz sposobów sprawowania nadzoru i kontroli nad stosowaniem ustawy. W zakres ustawy została włączona również administracja publiczna oraz sektor telekomunikacyjny.

II. Trzy zespoły CSIRT poziomu krajowego

Dyrektywa NIS nakłada na państwa członkowskie obowiązek wyznaczenia zespołu lub zespołów CSIRT - Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego. W Polsce ustawa wyznacza trzy zespoły CSIRT poziomu krajowego. Każdy CSIRT ma jasno określony zakres podmiotów, którym zapewniają wsparcie.

- **CSIRT GOV** w strukturach Agencji Bezpieczeństwa Wewnętrznego - koordynuje incydenty zgłaszane przez administrację rządową, Narodowy Bank Polski, Bank Gospodarstwa Krajowego oraz operatorów infrastruktury krytycznej

[1] Dyrektywy Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii

- **CSIRT MON** w strukturach Ministerstwa Obrony Narodowej (MON) - koordynuje obsługę incydentów zgłaszanych przez podmioty podległe Ministrowi Obrony Narodowej i przedsiębiorstwa o szczególnym znaczeniu gospodarczo–obronnym
- **CSIRT NASK** w strukturach Państwowego Instytutu Badawczego NASK - koordynuje natomiast incydenty zgłaszane przez pozostałe podmioty, w tym m.in. operatorów usług kluczowych[2], dostawców usług cyfrowych[3], **samorząd terytorialny**, . Do CSIRT NASK incydenty mogą także zgłaszać osoby fizyczne – zwykli obywatele.

Podstawowym zadaniem zespołów CSIRT jest monitorowanie zagrożeń cyberbezpieczeństwa i incydentów na poziomie krajowym, a także reagowanie na zaistniałe incydenty i szacowanie ryzyka. Zespoły CSIRT przekazują informacje dotyczące incydentów i ryzyk podmiotom krajowego systemu cyberbezpieczeństwa oraz wydają komunikaty o zidentyfikowanych zagrożeniach. W uzasadnionych przypadkach CSIRT może zapewnić wsparcie w obsłudze incydentu, albo przekazać informacje o podatnościach i sposobach ich usunięcia.

III. Podmioty ustawy o KSC

Podmiotami ustawy o Krajowym Systemie Cyberbezpieczeństwa są:

1. Operatorzy usług kluczowych
2. Dostawcy usług cyfrowych
3. Podmioty publiczne

1. Operatorzy usług kluczowych

Operatorzy usług kluczowych to firmy lub instytucje świadczące usługi o istotnym znaczeniu dla utrzymania krytycznej działalności społecznej lub gospodarczej. Wyznaczenia operatorów usług kluczowych dokonają organy właściwe[4], które po przeprowadzeniu postepowania administracyjnego, wydają w tym zakresie decyzję administracyjną. Podstawą do wydania decyzji jest spełnienie (łącznie) przez dany podmiot następujących kryteriów:

- podmiot świadczy usługę kluczową w jednym z sektorów: sektor energetyczny, sektor transportowy, sektor bankowy i infrastruktury rynków finansowych, sektor ochrony zdrowia, sektor zaopatrzenia w wodę pitną (wraz z dystrybucją), sektor infrastruktury cyfrowej;
- **świadczenie usługi zależy od systemów informacyjnych;**
- wystąpienie incydentu miałoby istotny skutek zakłócający[5] dla świadczenia usługi kluczowej.Operatorzy usług kluczowych są zobowiązani do zapewnienia bezpieczeństwa i ciągłości świadczonych usług kluczowych. Szczegółowy wykaz obowiązków operatorów usług kluczowych jest określony w ustawie o KSC.

[2] CSIRT NASK obsługuje operatorów usług kluczowych, którzy nie są operatorami infrastruktury krytycznej.
[3] Poza tymi, którzy są w zakresie kompetencji CSIRT MON.
[4] Ustawa określa 7 organów właściwych: Ministerstwo Energii, Ministerstwo Infrastruktury, Ministerstwo Gospodarki Morskiej i Żeglugi Śródlądowej, Ministerstwo Cyfryzacji, Ministerstwo Obrony Narodowej, Ministerstwo Zdrowia oraz Komisja Nadzoru Finansowego.
[5] Progi istotności skutku zakłócającego dla usługi kluczowej zostały wyznaczone w Rozporządzeniu Rady Ministrów z dnia 11 września 2018 r. w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych.

2. Operatorzy usług cyfrowych

Operatorami usług cyfrowych są podmioty świadczące usługę cyfrową w rozumieniu ustawy o świadczeniu usług drogą elektroniczną. Są to internetowe platformy handlowe, usługi przetwarzania w chmurze i wyszukiwarki internetowe.

3. Podmioty publiczne

W skład krajowego systemu cyberbezpieczeństwa wchodzą również podmioty publiczne takie jak:

- jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 1–6, 8, 9, 11 i 12 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2017 r. poz. 2077 oraz z 2018 r. poz. 62 i 1000);
- instytuty badawcze;
- Narodowy Bank Polski;
- Bank Gospodarstwa Krajowego;
- Urząd Dozoru Technicznego;
- Polską Agencję Żeglugi Powietrznej;
- Polskie Centrum Akredytacji;
- Narodowy Fundusz Ochrony Środowiska i Gospodarki Wodnej oraz wojewódzkie fundusze ochrony środowiska i gospodarki wodnej;
- spółki prawa handlowego wykonujące zadania o charakterze użyteczności publicznej w rozumieniu art. 1 ust. 2 ustawy z dnia 20 grudnia 1996 r. o gospodarce komunalnej (Dz. U. z 2017 r. poz. 827);

Podmiot publiczny, o którym mowa w ustawie o KSC i realizuje zadanie publiczne zależne od systemu informacyjnego jest zobowiązany do obsługi incydentu w podmiocie publicznym.

Incydent w podmiocie publicznym – incydent, który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez podmiot publiczny.

IV. Obowiązki podmiotów publicznych

1. Wyznaczenie osoby do kontaktu

Podmiot publiczny realizujący zadanie publiczne zależne od systemu informacyjnego jest obowiązany do wyznaczenia osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa.

Organ administracji publicznej ma obowiązek wyznaczyć jedną osobę kontaktową w zakresie zadań publicznych zależnych od systemów informacyjnych, realizowanych przez jednostki jemu podległe lub przez niego nadzorowane.

Jednostka samorządu terytorialnego może wyznaczyć jedną osobę kontaktową w zakresie zadań publicznych zależnych od systemów informacyjnych realizowanych przez jej jednostki organizacyjne.

Dane osoby kontaktowej należy przekazać do właściwego CSIRT (dla samorządów będzie to CSIRT NASK).

NASK
PAŃSTWOWY INSTYTUT BADAWCZY

Zgłoszenie osoby kontaktowej odbywa się w dwóch krokach:

- **Przesłanie wiadomości e-mail** na adres ksc@cert.pl następujących informacji: nazwa podmiotu/organizacji, sektor (energia, transport, finanse itd.), imię, nazwisko, telefon kontaktowy oraz służbowy e-mail osoby kontaktowej.
- **Przesłanie pisma** z wyżej wymienionymi informacjami. Pismo stanowi potwierdzenie zgłoszenia.

Zgłoszenie osoby kontaktowej należy złożyć w terminie 14 dni od daty wyznaczenia osoby. Wszystkie zmiany również należy przekazać w terminie 14 dni.

2. Zarządzanie incydentem

Podmiot publiczny, który realizuje zadanie publiczne zależne od systemu informacyjnego, ma obowiązek zapewnić zarządzanie incydentem w podmiocie publicznym**.**

a. Zgłoszenie incydentu

Incydent powinien zostać zgłoszony niezwłocznie, nie później niż w ciągu 24 godzin od momentu wykrycia do właściwego CSIRT. Zgłoszenie przekazywane jest w postaci elektronicznej, poprzez uzupełnienie formularza internetowego znajdującego się na stronie: https://incydent.cert.pl.

Zgłoszenie zawiera:

- dane podmiotu zgłaszającego, w tym nazwę podmiotu, numer we właściwym rejestrze, siedzibę i adres;
- imię i nazwisko, numer telefonu oraz adres poczty elektronicznej osoby składającej zgłoszenie;
- imię i nazwisko, numer telefonu oraz adres poczty elektronicznej osoby uprawnionej do składania wyjaśnień dotyczących zgłaszanych informacji;
- opis wpływu incydentu w podmiocie publicznym na realizowane zadanie publiczne (wskazanie zadania publicznego, na które incydent miał wpływ, liczbę osób, na które incydent miał wpływ, moment wystąpienia i wykrycia incydentu oraz czas jego trwania, zasięg geograficzny obszaru, którego dotyczy incydent, przyczynę zaistnienia incydentu i sposób jego przebiegu oraz skutki jego oddziaływania na systemy informacyjne podmiotu publicznego;
- informacje o przyczynie i źródle incydentu;

- informacje o podjętych działaniach zapobiegawczych;
- informacje o podjętych działaniach naprawczych;
- inne istotne informacje.

W momencie zgłoszenia podmiot podaje znane sobie informacje, które mogą być uzupełniane w trakcie obsługi incydentu.

b. Dane osobowe i tajemnice prawnie chronione

Poszczególne zespoły CSIRT mają prawo przetwarzać dane osobowe, w tym także tajemnice prawnie chronione, które są niezbędne do obsługi incydentów i zagrożeń cyberbezpieczeństwa. Ustawodawca skorzystał w tym przypadku z art. 23 RODO, umożliwiającego wyłączenie niektórych podmiotów z części przepisów rozporządzenia.

Zgłoszenie incydentu powinno zawierać zarówno dane osobowe, a także tajemnice prawnie chronione (w tym tajemnice przedsiębiorstwa), jeżeli jest to konieczne do realizacji zadań CSIRT. W zgłoszeniu należy oznaczyć informacje, które są prawnie chronione.

CSIRT może zwrócić się do podmiotu publicznego o uzupełnienie zgłoszenia o informacje, które stanowią tajemnice prawnie chronione.

Właściwy CSIRT, publikując informacje o incydentach nie może naruszać przepisów o ochronie danych osobowych, przepisów o ochronie informacji niejawnych oraz innych tajemnic prawnie chronionych.

3. Obowiązek informacyjny

Obsługa incydentu wiąże się również z obowiązkiem przekazania informacji osobom, na rzecz których realizuje się zadanie publiczne. Osoby mają prawo dostępu do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami.

Obowiązek informacyjny może zostać spełniony poprzez publikacje stosownego komunikatu na stronie internetowej.

V. Podmiot publiczny operatorem usługi kluczowej

Podmiot publiczny może być jednocześnie operatorem usługi kluczowej. Procedura wyznaczenia jest identyczna z tą opisaną w części dotyczącej operatorów usług kluczowych.

Podmiot publiczny, który zostanie uznany za operatora usługi kluczowej zobowiązany jest do wypełnienia ustawowych obowiązków przewidzianych dla operatorów usług kluczowych[6], w zakresie świadczenia usługi kluczowej.

VI. Podmiot publiczny operatorem infrastruktury krytycznej

Podmiot publiczny może być równocześnie także operatorem infrastruktury krytycznej. Mówimy tutaj o sytuacji gdy jest właścicielem, posiadaczem samoistnym albo posiadaczem zależnym obiektów, instalacji, urządzeń lub usług wchodzących w skład infrastruktury krytycznej,

[6] Obowiązki operatorów usług kluczowych są określone w rozdziale 3 ustawy o KSC.

wymienionych w wykazie, o którym mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2017 r. poz. 209 i 1566 oraz z 2018 r. poz. 1118). Podmiot, który posiada już zatwierdzony plan ochrony infrastruktury krytycznej uwzględniający dokumentację dotyczącą cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej, nie ma obowiązku opracowania takiej dokumentacji ponownie.

Zgłaszanie incydentów odbywa się na tych samych zasadach jak dotychczas tzn. operatorzy infrastruktury krytycznej zgłaszają je do zespołu CSIRT GOV zarządzanego przez ABW.