NASK

CYBERPOLICY

Analiza

Ustawa o krajowym systemie cyberbezpieczeństwa

28 sierpnia 2018

Spis treści

CYBERPOLICY

Ustawa o krajowym systemie cyberbezpieczeństwa

Wstęp

Ustawa o krajowym systemie cyberbezpieczeństwa to pierwszy akt prawny w tym zakresie w Polsce. Jest to implementacja do porządku krajowego tzw. Dyrektywy NIS[1]. Ponieważ Dyrektywa NIS jest harmonizacją minimalną, polski ustawodawca skorzystał z możliwości bardziej szczegółowej regulacji. Dlatego w zakres ustawy została włączona administracja publiczna oraz sektor telekomunikacyjny. Dodatkowo celem ustawodawcy było wyraźne rozdzielenie obowiązków pomiędzy poszczególne CSIRT poziomu krajowego, ustanowienie nadzoru w zakresie cyberbezpieczeństwa (organy właściwe oraz wprowadzenie kar finansowych), a także stworzenie polityczno–strategicznych ram zarządzania cyberbezpieczeństwem w Polsce (strategia cyberbezpieczeństwa RP, powołanie Pełnomocnika i Kolegium ds. Cyberbezpieczeństwa).

Prace nad ustawą prowadzone były przez zespół międzyresortowy, a sam akt nie wyczerpuje złożonego tematu cyberbezpieczeństwa w Polsce. Wiele kwestii, jak na przykład wyznaczenie operatorów usług kluczowych czy budowa kompetencji w zakresie organów właściwych, wciąż wymaga wytężonej pracy po stronie administracji. Podobnie jest po stronie sektora prywatnego, który musi dostosować się do nowej regulacji przede wszystkim w zakresie obowiązkowego raportowania incydentów do właściwego CSIRT poziomu krajowego (do tej pory raportowanie, z wyjątkiem sektora telekomunikacji i operatorów infrastruktury krytycznej, nie było obowiązkowe).

Ustawa obowiązuje od 28 sierpnia 2018 roku.

1. Zakres ustawy

1.1. Operatorzy Usług Kluczowych

Operatorzy usług kluczowych to firmy i instytucje świadczące usługi o istotnym znaczeniu dla utrzymania krytycznej działalności społecznej lub gospodarczej. Usługa kluczowa jest zależna od systemów informatycznych[2]. Ustawa wskazuje sektory, w których dokonana zostanie identyfikacja operatorów usług kluczowych. Są to **sektor energetyczny, transportowy, bankowy i infrastruktury rynków finansowych, ochrony zdrowia, zaopatrzenia w wodę pitną (wraz z dystrybucją) i infrastruktury cyfrowej**[3]. Dokładna lista usług kluczowych zostanie zawarta w rozporządzeniu

[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. Czas na implementacje Dyrektywy NIS do krajowych porządków prawnych państw członkowskich upłynął 9 maja 2018 roku.

[2] operatorzy usług kluczowych (OUK) nie są więc tożsami z operatorami infrastruktury krytycznej (IK). Kwestie ochrony infrastruktury krytycznej regulowane są na mocy ustawy z 27 kwietnia 2007 o zarządzaniu kryzysowym. Zawarta tam definicja określa IK jako systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców. Obecnie Rządowe Centrum Bezpieczeństwa prowadzi prace mające na celu przejście od modelu obiektowego do usługowego w dziedzinie ochrony IK.

[3] W ramach infrastruktury cyfrowej wymieniono Punkty Wymiany Ruchu internetowego, rejestrację nazw domen najwyższego poziomu i usługi DNS.

wykonawczym do ustawy[4]. **Wykaz operatorów usług kluczowych będzie prowadzony przez ministra właściwego do spraw informatyzacji**. Wpisanie i wykreślenie operatora z listy odbywa się na wniosek organu właściwego do spraw cyberbezpieczeństwa (więcej informacji na ten temat w rozdziale 3.1).

Identyfikacji operatorów usług kluczowych dokonają organy właściwe[5], które wydadzą w tym zakresie decyzję administracyjną[6]. Podstawą do wydania decyzji będą następujące kryteria:

- podmiot świadczy usługę kluczową w jednym z sektorów,
- świadczenie usługi zależy od systemów informacyjnych,
- wystąpienie incydentu miałoby istotny skutek zakłócający dla świadczenia usługi kluczowej.

Ocena istotności skutku zależy od tzw. „progów istotności skutku zakłócającego", które zostaną wyznaczone przez Radę Ministrów z uwzględnieniem przede wszystkim:

- liczby użytkowników zależnych od usługi kluczowej świadczonej przez dany podmiot,
- zależności innych sektorów od usługi świadczonej przez ten podmiot,
- wpływu, jaki mógłby mieć incydent, ze względu na jego skalę i czas trwania, na działalność gospodarczą i społeczną lub bezpieczeństwo publiczne,
- udziału podmiotu świadczącego usługę kluczową w rynku,
- zasięgu geograficznego obszaru, którego mógłby dotyczyć incydent,
- zdolności podmiotu do utrzymywania wystarczającego poziomu świadczenia usługi kluczowej, przy uwzględnieniu dostępności alternatywnych sposobów jej świadczenia,
- innych czynników charakterystycznych dla danego sektora lub podsektora.

Obowiązki operatorów usług kluczowych

Wdrożenie systemu zarządzania bezpieczeństwem

Operatorzy usług kluczowych zobowiązani są wdrożyć system zarządzania bezpieczeństwem w systemie informacyjnym, wykorzystywanym do świadczenia usługi kluczowej. W ramach zarządzania wymagane jest **systematyczne szacowanie ryzyka** i **dostosowanie do niego środków bezpieczeństwa**, takich jak bezpieczna eksploatacja systemu, bezpieczeństwo fizyczne systemu (w tym kontrola dostępu), bezpieczeństwo i ciągłość dostaw usług, które mają wpływ na świadczenie usługi kluczowej, utrzymanie planów działania umożliwiających ciągłość świadczenia usługi, ciągłe monitorowanie systemu zapewniającego świadczenie usługi.

Ponadto operator jest zobowiązany do stosowania środków zapobiegających i ograniczających wpływ incydentów na bezpieczeństwo systemu informacyjnego, w tym zbierania informacji o zagrożeniach cyberbezpieczeństwa i podatności systemu. Operator jest także odpowiedzialny za opracowanie

[4] Konsultacje publiczne projektu rozporządzenia zakończyły się w lipcu 2018r. Aktualnie projekt znajduje się na etapie opiniowania (https://legislacja.rcl.gov.pl/projekt/12312201 – dostęp w dniu 10.08.2018r.)

[5] art 5 Ustawy o Krajowym systemie cyberbezpieczeństwa

[6] Przy czym jeśli dany operator został już wcześniej zidentyfikowany jako operator infrastruktury krytycznej, realizowane przez niego obowiązki wynikające z o Ustawy o zarzadzaniu kryzysowym, takie jak przygotowanie dokumentacji bezpieczeństwa zostaną uznane za zrealizowane.

dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego, uaktualnianie jej i przechowywanie przez okres co najmniej 2 lat[7].

Obsługa incydentu

W przypadku wystąpienia incydentu, operator zapewnia jego obsługę poprzez:

- klasyfikację incydentu na podstawie kryteriów określonych przez Radę Ministra na drodze rozporządzenia[8],
- w przypadku zakwalifikowania incydentu jako poważny - zgłoszenie do właściwego CSIRT nie później niż **w ciągu 24 godzin** od momentu wykrycia,
- współdziałanie z CSIRT w ramach obsługi incydentu wraz z zapewnieniem odpowiedniego dostępu do informacji,
- usunięcie podatności systemu.

W przypadku powołania **sektorowego zespołu cyberbezpieczeństwa** operator dodatkowo przekazuje zgłoszenie do zespołu, współdziała z zespołem wysyłając niezbędne dane i zapewnia zespołowi dostęp do informacji o rejestrowanych incydentach. Oznacza to de facto, że ustawa wprowadza dowolność w zakresie powoływania sektorowych zespołów bezpieczeństwa, to od samego sektora zależało będzie czy taki sektorowy CSIRT zostanie powołany.

Zgłoszenie incydentu

Zgłoszenie incydentu powinno zawierać:

- informacje identyfikujące (dane teleadresowe podmiotu zgłaszającego, dane osoby zgłaszającej, dane osoby uprawnionej do wyjaśnień),
- opis wpływu incydentu na świadczenie usługi kluczowej (opis usługi, liczbę użytkowników, zasięg geograficzny, wpływ incydentu, przyczynę incydentu, przebieg i skutki),
- informację dla właściwego CSIRT o możliwości wpływu incydentu na większą liczbę państw członkowskich UE,
- w przypadku incydentu, który mógł mieć wpływ na świadczenie usługi kluczowej – opis przyczyn, przebiegu i skutków oddziaływania incydentu,
- informację o podjętych działaniach zapobiegawczych i naprawczych.

Gdy jest to niezbędne, operator usługi kluczowej jest zobowiązany do przekazania informacji stanowiących tajemnice prawnie chronione w zakresie koniecznym do realizacji zadań właściwego CSIRT oraz sektorowego zespołu cyberbezpieczeństwa.

Struktura wewnętrzna operatora

Do realizacji zadań określonych w Ustawie operator powołuje struktury wewnętrzne odpowiedzialne za cyberbezpieczeństwo, o czym informuje zarówno organ właściwy jak i sektorowy zespół cyberbezpieczeństwa (jeśli został powołany). Możliwe jest także zawarcie umowy z podmiotem zewnętrznym, który świadczy usługi z zakresu cyberbezpieczeństwa. Ustawa dopuszcza więc

[7] Z tego zapisu wyłączeni są operatorzy posiadający obiekty, instalacje, urządzenia lub usługi wchodzące w skład infrastruktury krytycznej, którzy posiadają zatwierdzony plan ochrony infrastruktury krytycznej wraz z dokumentacją.

[8] Rada Ministrów określi progi uznania incydentu za poważny na podstawie liczby użytkowników zaangażowanych, czasu oddziaływania incydentu, zasięgu geograficznego, a także innych czynników charakterystycznych dla sektora (tj. ochrona życia lub zdrowia, ochrona majątku, jakość świadczonej usługi).

outsourcing usług bezpieczeństwa. Informację na temat podpisania umowy z podmiotem zewnętrznym należy przekazać w analogiczny sposób wraz z danymi kontaktowymi podmiotu i zakresem świadczonej usługi w terminie 14 dni od daty zawarcia umowy.

Minister właściwy do spraw informatyzacji określi warunki organizacyjne i techniczne dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa, a także dla wewnętrznych struktur operatorów.

Audyt i kontrola

Operator ma **obowiązek przeprowadzenia audytu bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej raz na 2 lata**[9], przy czym pierwszy audyt powinien zostać przeprowadzony w ciągu roku od dnia doręczenia decyzji o uznaniu za operatora usługi kluczowej. Pisemne sprawozdanie z audytu wraz z dokumentacją jest przechowywane przez operatora i może być udostępnione na uzasadniony wniosek organu właściwego do spraw cyberbezpieczeństwa, dyrektora RCB i szefa ABW.

Organy właściwe do spraw cyberbezpieczeństwa są upoważnione do nadzoru operatorów usług kluczowych w zakresie wynikających z ustawy obowiązków, dotyczących przeciwdziałania zagrożeniom cyberbezpieczeństwa i zgłaszania incydentów poważnych. W ramach nadzoru organy właściwe mogą przeprowadzać kontrolę, a także nakładać kary pieniężne.

1.2. Dostawcy Usług Cyfrowych

Do usług cyfrowych zaliczane są: internetowe platformy handlowe, usługi przetwarzania w chmurze i wyszukiwarki internetowe. Zgodnie z art. 17 ustawy Dostawcą usługi cyfrowej (DSP) jest osoba prawna albo jednostka organizacyjna świadcząca usługę cyfrową, która:

- nie posiada osobowości prawnej,
- ma siedzibę lub zarząd na terytorium Polski lub,
- ma przedstawiciela, który prowadzi jednostkę organizacyjną na terytorium RP.

Z zakresu ustawy zostały wyjęte małe i mikroprzedsiębiorstwa[10].

Obowiązki dostawców usług cyfrowych

Ze względu na transgraniczny charakter usług cyfrowych i międzynarodową specyfikę podmiotów świadczących tego rodzaju usługi, DSP zostały objęte lżejszą regulacją, niż operatorzy usług kluczowych. Mają oni obowiązek stosować środki bezpieczeństwa proporcjonalne do ryzyka, uwzględniając szczególnie:

[9] Wytyczne do audytu zostały określone w Ustawie.

[10] Art. 104 ustawy o swobodzie gospodarczej z dnia 2 lipca 2004 r. określa **mikroprzedsiębiorcę** jako przedsiębiorcę, który w co najmniej jednym z dwóch ostatnich lat obrotowych **zatrudniał średniorocznie mniej niż 10 pracowników** oraz osiągnął roczny obrót netto ze sprzedaży towarów, wyrobów i usług oraz operacji finansowych nieprzekraczający równowartości w złotych 2 milionów euro, lub sumy aktywów jego bilansu sporządzonego na koniec jednego z tych lat nie przekroczyły równowartości w złotych 2 milionów euro.
Art. 105 ustawy o swobodzie gospodarczej z dnia 2 lipca 2004 r. określa **małego przedsiębiorcę** jako przedsiębiorcę, który zatrudniał średniorocznie **mniej niż 250 pracowników** oraz osiągnął roczny obrót netto ze sprzedaży towarów, wyrobów i usług oraz operacji finansowych nieprzekraczający równowartości w złotych 50 milionów euro, lub sumy aktywów jego bilansu sporządzonego na koniec jednego z tych lat nie przekroczyły równowartości w złotych 43 milionów euro

- **bezpieczeństwo systemów informacyjnych i obiektów** – W skład systemów informacyjnych wchodzą systemy teleinformatyczne, o których mowa w art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2017 r. poz. 570 oraz z 2018 r. poz. 1000)[11], wraz z przetwarzanymi w nich danymi w postaci elektronicznej.
- **postępowanie w przypadku obsługi incydentu**, czyli czynności umożliwiające wykrywanie, rejestrowanie, analizowanie, klasyfikowanie, priorytetaryzację, podejmowanie działań naprawczych i ograniczenie skutków incydentu.
- **zarządzanie ciągłością działania dostawcy w celu świadczenia usługi cyfrowej**. Zgodnie z treścią art. 17 pkt 3 ustawy o krajowym systemie cyberbezpieczeństwa, dostawca usługi cyfrowej podejmuje środki zapobiegające i minimalizujące wpływ incydentów na usługę cyfrową w celu zapewnienia ciągłości świadczenia tej usługi.
- **najnowszy stan wiedzy** w tym zgodność z normami międzynarodowymi, o których mowa w rozporządzeniu wykonawczym 2018/151. W treści niniejszego rozporządzenia zostały doprecyzowane elementy, jakie mają zostać uwzględnione przez DSP przy określaniu i podejmowaniu środków, mających na celu zapewnienie poziomu bezpieczeństwa sieci i systemów informatycznych wykorzystywanych przez nich w kontekście oferowania usług, jak również parametry, które należy wziąć pod uwagę w celu ustalenia, czy incydent ma istotny wpływ na świadczenie tych usług.
- **monitorowanie, audyt i testowanie.**

Oprócz odpowiedniego zarządzania ryzykiem systemów informacyjnych, wykorzystywanych do świadczenia usługi cyfrowej, DSP mają obowiązek prowadzenia czynności umożliwiających wykrywanie, rejestrowanie, analizowanie oraz klasyfikowanie incydentów. W przypadku wystąpienia istotnego incydentu, dostawca usługi kluczowej ma obowiązek przekazania informacji do właściwego CSIRT nie później niż w ciągu 24 godzin od momentu wykrycia.

Podobnie jak w przypadku operatorów usług kluczowych, DSP zostaną objęte nadzorem przez organy właściwe, które mają uprawnienie do prowadzenia kontroli i nakładania kar pieniężnych.

1.3. Podmioty publiczne

W skład krajowego systemu cyberbezpieczeństwa wchodzą również podmioty publiczne takie jak: Narodowy Bank Polski, Bank Gospodarstwa Krajowego, Urząd Dozoru Technicznego, Polska Agencja Żeglugi Powietrznej, Polskie Centrum Akredytacji, Narodowy Fundusz Ochrony Środowiska i Gospodarki Wodnej oraz wojewódzkie fundusze ochrony środowiska i gospodarki wodnej, a także instytuty badawcze i spółki prawa handlowego, wykonujące zadania o charakterze użyteczności publicznej.

Zgodnie z treścią art. 21 każdy z powyższych podmiotów ma obowiązek wyznaczenia osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa w zakresie zadań publicznych zależnych od systemów informacyjnych.

[11] system teleinformatyczny – zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu przepisów ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2016 r. poz. 1489, 1579, 1823, 1948, 1954 i 2003).

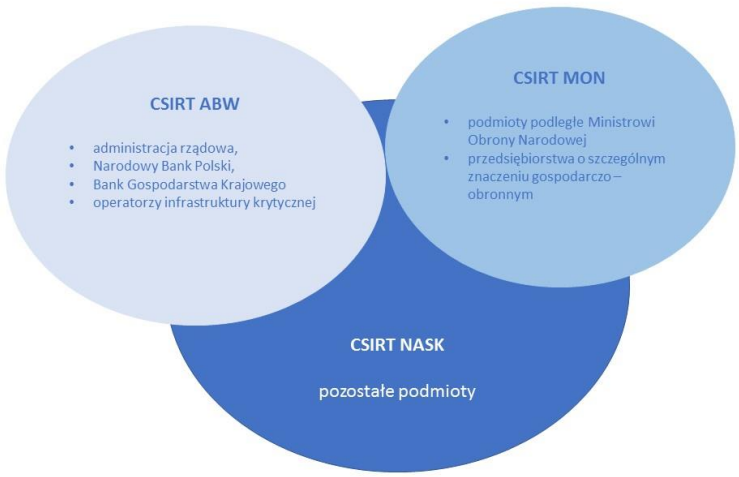
Dodatkowo na każdym z podmiotów publicznych będzie spoczywać obowiązek zarządzania incydentem w podmiocie publicznym, w tym zapewnienia jego obsługi. Czas na zgłoszenie incydentu do właściwego CSIRT nie może przekroczyć 24 godzin od momentu wykrycia.

2. Raportowanie incydentów

2.1. Trzy CSIRT poziomu krajowego

Dyrektywa NIS daje państwom członkowskim dowolność w zakresie liczby powołanych CSIRT, z zastrzeżeniem, że operatorzy usług kluczowych i dostawcy usług cyfrowych muszą mieć wyznaczony CSIRT do którego będą raportować. Ustawa wyznacza więc **trzy CSIRT poziomu krajowego: CSIRT NASK w strukturach Państwowego Instytutu Badawczego NASK, CSIRT GOV w strukturach Agencji Bezpieczeństwa oraz CSIRT MON w strukturach Resortu Obrony Narodowej (RON)**. Każdy CSIRT poziomu krajowego ma jasno określone *constituency* – zakres podmiotów, które zobowiązane są raportować i którym świadczy on wsparcie.

CSIRT MON koordynuje obsługę incydentów zgłaszanych przez podmioty podległe Ministrowi Obrony Narodowej i przedsiębiorstwa o szczególnym znaczeniu gospodarczo–obronnym. CSIRT GOV koordynuje incydenty zgłaszane przez administrację rządową, Narodowy Bank Polski, Bank Gospodarstwa Krajowego oraz operatorów infrastruktury krytycznej[12]. CSIRT NASK koordynuje natomiast incydenty zgłaszane przez pozostałe podmioty, w tym m.in. operatorów usług kluczowych[13], dostawców usług cyfrowych, samorząd terytorialny. Do CSIRT NASK incydenty mogą także zgłaszać osoby fizyczne – zwykli obywatele. Można więc powiedzieć, że CSIRT NASK stanowi tzw. „cert ostatniej szansy" (CERT of last resort[14]). Dodatkowo w przypadku incydentów o charakterze terrorystycznym właściwe są CSIRT MON i CSIRT GOV (zgodnie z zapisami ustawy o działaniach antyterrorystycznych i ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego). W przypadku incydentów związanych z obronnością kraju zawsze właściwy jest CSIRT MON. Poniższy schemat przestawia podział *constituency* pomiędzy trzy CSIRT poziomu krajowego.



Rys. 1. podział constituency pomiędzy trzy CSIRT poziomu krajowego

[12] zgodnie z Ustawą o zarządzaniu kryzysowym
[13] nie będących operatorami infrastruktury krytycznej
[14] zgodnie z nomenklaturą ENISA, zawartą w dokumencie *Deployment of Baseline Capabilities of National/ Governmental CERTs* oznacza to, że w przypadku kiedy jakiś podmiot nie jest w stanie uzyskać bezpośredniego kontaktu lub oczekiwanej pomocy od podmiotu, który jest zaangażowany w incydent bezpośrednio, zgłaszający przekazuje zapytanie do CSIRT „ostatniej szansy"

Wszystkie trzy CSIRT poziomu krajowego mają za zadanie współpracować z organami właściwymi (więcej informacji na ten temat w rozdziale 3.1.), ministrem właściwym ds. informatyzacji oraz Pełnomocnikiem ds. Cyberbezpieczeństwa. Poza tym do ich zadań należy:

- monitorowanie zagrożeń cyberbezpieczeństwa i incydentów na poziomie krajowym;
- szacowanie ryzyka w skali kraju;
- przekazywanie informacji na temat incydentów i ryzyk innym podmiotom wchodzącym w skład krajowego systemu cyberbezpieczeństwa;
- wydawanie komunikatów o zidentyfikowanych zagrożeniach cyberbezpieczeństwa;
- reagowanie na zgłoszone incydenty;
- koordynowanie obsługi incydentów krytycznych (po wcześniejszym ich zakwalifikowaniu jako incydenty krytyczne);
- w uzasadnionych przypadkach badanie urządzenia informatycznego lub oprogramowania w celu identyfikacji podatności, której wykorzystanie może zagrozić integralności, poufności, rozliczalności, autentyczności lub dostępności przetwarzanych danych, które może mieć wpływ na bezpieczeństwo publiczne lub istotny interes bezpieczeństwa państwa;
- składanie wniosków w sprawie „rekomendacji dotyczących stosowania urządzeń informatycznych lub oprogramowania" dla podmiotów krajowego systemu cyberbezpieczeństwa w zakresie wpływu na bezpieczeństwo publiczne lub istotny interes bezpieczeństwa państwa;
- współpraca z sektorowymi zespołami cyberbezpieczeństwa zarówno w zakresie koordynowania obsługi incydentów poważnych i incydentów krytycznych, jak i w zakresie wymiany informacji pozwalających przeciwdziałać zagrożeniom cyberbezpieczeństwa;
- współpraca z innymi państwami UE w zakresie wymiany informacji o incydentach poważnych i istotnych;
- przekazywanie do Pojedynczego Punktu Kontaktowego (ministra właściwego ds. informatyzacji) zestawienia incydentów (poważnych i istotnych) zgłoszonych w poprzednim roku kalendarzowym;
- wspólne opracowywanie i przekazywanie ministrowi właściwemu do spraw informatyzacji części Raportu o zagrożeniach bezpieczeństwa narodowego, o którym mowa w art. 5a ust. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, dotyczącej cyberbezpieczeństwa.

Ponadto CSIRT poziomu krajowego zapewniają zaplecze analityczne oraz badawczo-rozwoje dla krajowego systemu cyberbezpieczeństwa. Jest to związane z:

- prowadzeniem zaawansowanej analizy złośliwego oprogramowania i podatności,
- monitorowaniem wskaźników zagrożeń,
- rozwijaniem narzędzi i metod do wgrywania i zwalczania zagrożeń cyberbezpieczeństwa,
- prowadzeniem analiz i opracowywaniem standardów, rekomendacji i dobrych praktyk w zakresie cyberbezpieczeństwa,
- wspieraniem podmiotów krajowego systemu cyberbezpieczeństwa w budowaniu potencjału i zdolności w obszarze cyberbezpieczeństwa,
- prowadzeniem działań z zakresu budowania świadomości w obszarze cyberbezpieczeństwa.

Bardzo istotne jest, że CSIRT poziomu krajowego mają możliwość wykonywania niezbędnych działań technicznych związanych z analizą zagrożeń, koordynacją obsługi incydentu poważnego, istotnego i

krytycznego. W trakcie koordynacji tych incydentów mogą także występować do organów właściwych z wnioskiem o wezwanie operatora usługi kluczowej lub dostawcy usługi cyfrowej, aby podatność została usunięta.

2.2. Rodzaje incydentów

Ustawa wprowadza trzy poziomy incydentów.

Poziom pierwszy to wszystkie zdarzenia o niekorzystnym wpływie na cyberbezpieczeństwo.

Poziom drugi to incydenty poważne[15], występujące u operatorów usług kluczowych; incydenty istotne[16] występujące u dostawców usług cyfrowych oraz incydenty w podmiocie publicznym[17] występujące w podmiotach publicznych. Te incydenty są klasyfikowane odpowiednio przez operatorów usług kluczowych, dostawców usług cyfrowych i podmioty publiczne. Klasyfikacja ta odbywa się w oparciu o konkretne kryteria. W przypadku operatorów usług kluczowych kryteria te wyznaczy rozporządzenie wykonawcze do ustawy, w przypadku dostawców usług cyfrowych są to progi wyznaczone w Rozporządzeniu Wykonawczym Komisji (UE) 2018/151[18].

Kolejny poziom incydentów (**trzeci**) to incydenty krytyczne[19]. Są to incydenty o większej skali i niosące za sobą większe zagrożenie, niż trzy pozostałe. Ustawa definiuje je jako te, które mogą skutkować znaczną szkodą dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów gospodarczych, działania praw i wolności obywatelskich lub życia i zdrowia ludzi. Klasyfikacji incydentu jako krytycznego nie dokonują operatorzy, ani dostawcy usług kluczowych, ale właściwy CSIRT poziomu krajowego (CSIRT MON, CSIRT NASK lub CSIRT GOV). Poniższa tabela przedstawia poziomy incydentów.

Poziom incydentu	definicja	nadawanie klasyfikacji	konieczność raportowania
Poziom pierwszy	incydent - zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo	brak	brak

[15] incydent poważny – incydent, który powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi kluczowej; Ustawa o krajowym Systemie Cyberbezpieczeństwa art. 2.7

[16] incydent istotny – incydent, który ma istotny wpływ na świadczenie usługi cyfrowej w rozumieniu art. 4 rozporządzenia wykonawczego Komisji (UE) 2018/151 z dnia 30 stycznia 2018 r. ustanawiającego zasady stosowania dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 w odniesieniu do dalszego doprecyzowania elementów, jakie mają być uwzględnione przez dostawców usług cyfrowych w zakresie zarządzania istniejącymi ryzykami dla bezpieczeństwa sieci i systemów informatycznych, oraz parametrów służących do określenia, czy incydent ma istotny wpływ (Dz. Urz. UE L 26 z 31.01.2018, str. 48), zwanego dalej „rozporządzeniem wykonawczym 2018/151"; Ustawa o krajowym Systemie Cyberbezpieczeństwa art. 2.8

[17] incydent, który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez podmiot publiczny, o którym mowa w art. 4 pkt 7–15; Ustawa o krajowym Systemie Cyberbezpieczeństwa art. 2.9

[18] https://cyberpolicy.nask.pl/cp/ramy-prawne/dyrektywa-nis/96,Rozporzadzenie-Wykonawcze-Komisji-UE-2018151.html

[19] incydent krytyczny – incydent skutkujący znaczną szkodą dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, praw i wolności obywatelskich lub życia i zdrowia ludzi, klasyfikowany przez właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV; Ustawa o krajowym Systemie Cyberbezpieczeństwa art. 2.6

Poziom drugi	incydent poważny - powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi kluczowej	operator usługi kluczowej	CSIRT GOV – operatorzy infrastruktury krytycznej CSIRT MON – podmioty podległe RON CSIRT NASK – pozostałe na podstawie kryteriów z rozporządzenia do ustawy o krajowym systemie cyberbezpieczeństwa
	incydent istotny - ma istotny wpływ na świadczenie usługi cyfrowej	dostawca usługi cyfrowej	CSIRT NASK
	incydent w podmiocie publicznym - powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego	podmiot publiczny	CSIRT GOV CSIRT NASK CSIRT MON (zgodnie z constituency)
Poziom trzeci	incydent krytyczny - skutkujący znaczną szkodą dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, praw i wolności obywatelskich lub życia i zdrowia ludzi	CSIRT MON/ CSIRT GOV/ CSIRT NASK	tak, przy czym raportujący operator/ dostawca usługi nie zawsze będzie miał świadomość, że jest to incydent krytyczny (np. zaraportuje incydent poziomu drugiego, a właściwy CSIRT poziomu krajowego zmieni jego klasyfikację)

2.3. Współpraca CSIRT poziomu krajowego

Ustawa zakłada ścisłą współpracę CCIRT poziomu krajowego. Jej elementem jest opracowanie procedur postępowania w przypadku incydentu, którego koordynacja wymaga współpracy CSIRT. Poza tym ustawa wprowadza formułę Zespołu ds. Incydentów Krytycznych, będącego organem pomocniczym w sprawach obsługi incydentów krytycznych. W jego skład wchodzą CSIRT poziomu krajowego oraz Rządowe Centrum Bezpieczeństwa jako sekretariat – taka formuła zapewnia współpracę z Rządowym Zespołem Zarządzania Kryzysowego (RZZK)[20]. Dodatkowo do udziału w pracach Zespołu mogą być zaproszeni przedstawiciele organów właściwych.

[20]Zgodnie z ustawą o zarzadzaniu kryzysowym przewodniczący RZZK jest premier, a jego członkami odpowiedni ministrowie działowi. Wprowadzenie formuły Zespołu ds. Incydentów Krytycznych pozwala na szybkie przekazanie informacji o tzw. incydentach krytycznych, czyli „skutkujących znaczną szkodą dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, praw i wolności obywatelskich lub życia i zdrowia ludzi" na poziom Rady Ministrów, za pośrednictwem RCB. Pozwoli to łatwiej zarządzać kryzysem, który najprawdopodobniej w przypadku incydentów krytycznych będzie miał także skutki kinetyczne.

Powołanie Zespołu ds. Incydentów Krytycznych służy wyznaczeniu CSIRT, który będzie wiodącym w obsłudze incydentu krytycznego oraz podziałowi zadań związanych z tą obsługą. Na posiedzeniu może też zostać podjęta decyzja o wystąpieniu z wnioskiem do Prezesa Rady Ministrów w sprawie zwołania Rządowego Zespołu Zarządzania Kryzysowego. De facto jest to więc ujęcie problematyki cyberbezpieczeństwa w systemie zarządzania kryzysowego w Polsce.

2.4. RODO, a obsługa incydentów

Ustawa o Krajowym Systemie Cyberbezpieczeństwa uwzględnia nowe regulacje, które wprowadziło Rozporządzenie Ogólne o Ochronie Danych Osobowych (RODO/GDPR). Poszczególne CSRIT (MON, NASK, GOV), a także sektorowe zespoły bezpieczeństwa będą przetwarzać dane osobowe pozyskane w związku z incydentami i zagrożeniami cyberbezpieczeństwa. Będą to m.in. informacje o użytkownikach systemów informatycznych, telekomunikacyjnych urządzeniach końcowych czy dane operatorów usług kluczowych, dostawców usług cyfrowych czy podmiotów publicznych.

CSRIT oraz sektorowe zespoły bezpieczeństwa mogą przetwarzać tylko takie informacje, które są niezbędne do realizacji zadania, a dane mają zostać usunięte lub zanonimizowane maksymalnie 5 lat po zakończeniu obsługi incydentu, którego dotyczą.

Ustawa obliguje również do opublikowania na stronie internetowej m.in. namiarów na administratora danych osobowych, celu i podstawy prawnej przetwarzania, kategorii przetwarzanych danych, okresu ich przetwarzania czy źródła pochodzenia. Co ważne, podmioty muszą również poinformować **o ograniczeniach obowiązków i praw osób, których dotyczą dane osobowe**.

CSIRT mogą również przetwarzać informacje prawnie chronione, np. tajemnicę przedsiębiorstwa, jeśli jest to konieczne do realizacji ich zadań. Muszą jednak zachować tajemnicę informacji.

Oznacza to de facto, że ustawodawca skorzystał z art. 23 GDPR, umożliwiającego wyłączenie niektórych podmiotów z części przepisów rozporządzenia. W tym celu muszą być jednak spełnione dwa warunki:

1. Realizacja tych obowiązków uniemożliwiłaby podmiotom wykonywanie zadań.
2. Podmioty przetwarzające dane osobowe muszą prowadzić analizę ryzyka, stosować środki ochrony przed złośliwym oprogramowaniem oraz mechanizmy kontroli dostępu, a także opracować procedury bezpiecznej wymiany informacji.

Czytaj więcej o Rozporządzeniu Ogólnym o Ochronie Danych Osobowych

2.5. Obsługa incydentów a dostęp do informacji publicznej

Ustawa stwierdza, że informacje o podatnościach, incydentach i ryzyku ich wystąpienia oraz zagrożeniach cyberbezpieczeństwa **nie podlegają ustawie o dostępie do informacji publicznej**. Znaczy to, że nikt nie będzie mógł wymagać od zespołów CSRIT, aby te przekazywały dane dotyczące incydentów w drodze dostępu do informacji publicznej. Takie rozwiązanie przyczyni się do budowania zaufania w obrębie systemu, jako że operatorzy usług kluczowych nie będą musieli obawiać się, że zgłoszone przez nich podatności zostają ujawnione.

Właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV może jednak opublikować takie informacje w Biuletynie Informacji Publicznej, jeśli jest to **niezbędne, aby zapobiec incydentowi lub zapewnić jego obsługę**. Musi taką decyzję wcześniej skonsultować z operatorem usługi kluczowej lub dostawcą usługi cyfrowej, który zgłosił incydent.

Rodzaj incydentu	Kto zgłasza incydent	Kto udostępnia informację	Sposób publikacji

Incydent poważny	Operator usługi kluczowej	CSRIT MON CSRIT NASK CSRIT GOV	BIP MON BIP PIB NASK BIP ABW
Incydent istotny	Dostawca usługi cyfrowej	CSRIT MON CSRIT NASK CSRIT GOV	BIP MON BIP PIB NASK BIP ABW
		Dostawca usługi cyfrowej	CSRIT występuje do organu właściwego o zobowiązanie dostawcy usługi cyfrowej do upublicznienia informacji

Publikacja w BIP nie może naruszać przepisów o ochronie informacji niejawnych oraz innych tajemnic prawnie chronionych ani przepisów o ochronie danych osobowych. A zatem nawet jeśli informacja o incydencie zostanie po konsultacjach podana do publicznej wiadomości, nie zostaną ujawnione żadne wrażliwe dane, które mogłyby niekorzystnie wpłynąć na działalność operatorów usług kluczowych.

3. Nadzór

3.1. Organy właściwe

Nadzór nad każdym z kluczowych sektorów gospodarki sprawować będzie organ właściwy ds. cyberbezpieczeństwa. 11 sektorów wymienionych w ustawie podlega kompetencji konkretnych ministrów działowych[21], zgodnie z poniższą tabelą:

Organ właściwy ds. cyberbezpieczeństwa	**Sektor/podsektor**
Minister właściwy ds. energii	Energia
Minister właściwy ds. transportu	Transport
Minister właściwy ds. gospodarki morskiej i minister właściwy ds. żeglugi śródlądowej	Transport wodny
Komisja Nadzoru Finansowego	Bankowy, Infrastruktura rynków finansowych
Minister właściwy ds. zdrowia	Ochrona zdrowia
Minister właściwy ds. gospodarki wodnej	Zaopatrzenie w wodę pitną i jej dystrybucja
Minister właściwy ds. informatyzacji	Infrastruktura cyfrowa
	Dostawcy usług cyfrowych
Minister Obrony Narodowej (podmioty podległe MON oraz przedsiębiorcy o szczególnym znaczeniu gospodarczo-obronnym)	Ochrona zdrowia
	Infrastruktura cyfrowa
	Dostawcy usług cyfrowych

Oznacza to, że organami właściwymi będą ministrowie właściwi dla konkretnych działów administracji, którzy na podstawie porozumienia mogą powierzyć realizację niektórych zadań jednostkom podległym lub nadzorowanym. Oznacza to, że regulatorzy sektorowi (jeśli istnieją) mogą realizować te funkcje zamiast ministra właściwego.

Zadaniem Organu właściwego ds. cyberbezpieczeństwa jest analiza podmiotów funkcjonujących w danym sektorze i **wydawanie decyzji, które z nich otrzymają status operatora usługi kluczowej**. Poza tym organ właściwy przygotowuje także rekomendacje działań, które wzmocnią cyberbezpieczeństwo sektora.

Do obowiązków organu należy też:

- wzywanie podmiotu do usunięcia podatności, które mogą lub mogły doprowadzić do poważnego incydentu,
- prowadzenie kontroli operatorów usług kluczowych,
- współpraca z innymi państwami UE za pośrednictwem Pojedynczego Punktu Kontaktowego,
- udział w ćwiczeniach oraz przetwarzanie danych osobowych niezbędnych do realizacji zadań.

3.2. Sektorowy zespół cyberbezpieczeństwa

Ustawa przewiduje powołanie sektorowych zespołów cyberbezpieczeństwa przez organy właściwe. Dużą zaletą działania takiego zespołu jest uwzględnienie specyfiki danego sektora, co pozwala dostosować wsparcie dla operatorów usług kluczowych.

[21] Ustawa z dnia 4 września 1997 r. o działach administracji rządowej (Dz.U. 1997 nr 141 poz. 943) ustala łącznie 28 działów administracji rządowej w Polsce. Dokument opisuje ich zakres oraz właściwość ministrów kierujących danymi działami.

Zespół nie tylko przyjmuje zgłoszenia o incydentach i pomaga w obsłudze, ale również analizuje ich skutki, wypracowuje wnioski oraz współpracuje z właściwym CSRIT. Może też wymieniać informacje o incydentach poważnych z innymi krajami Unii Europejskiej.

3.3. Minister ds. informatyzacji

Minister właściwy ds. informatyzacji zajmuje się cywilnymi aspektami cyberbezpieczeństwa RP. Do jego zadań należy monitorowanie wdrażania Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej, rekomendowanie obszarów współpracy z sektorem prywatnym, prowadzenie działań informacyjnych nas temat dobrych praktyk, programów edukacyjnych, kampanii i szkoleń z poszerzania wiedzy i budowania świadomości w zakresie cyberbezpieczeństwa.

Poza tym to właśnie minister właściwy ds. informatyzacji zapewnia rozwój i utrzymanie systemu teleinformatycznego, którego zadaniem jest wsparcie podmiotów wchodzących w skład systemu cyberbezpieczeństwa. System ten ma zapewnić wymianę informacji o incydentach, szacowanie ryzyka na poziomie krajowym, pozwolić na zgłaszanie incydentów i wsparcie ich obsługi, a także umożliwiać generowanie i przekazywanie rekomendacji oraz ostrzeżeń o zagrożeniach.

Minister prowadzi także Pojedynczy Punkt Kontaktowy (PPK). PPK odpowiada za współpracę z Komisją Europejską i przekazywanie corocznych raportów, współpracuje z innymi państwami członkowskimi w zakresie cyberbezpieczeństwa oraz koordynuje współpracę pomiędzy organami właściwymi w kraju.

3.4. Minister Obrony Narodowej

Do głównych zadań Ministra Obrony Narodowej należy prowadzenie międzynarodowej współpracy Sił Zbrojnych Rzeczypospolitej Polskiej z właściwymi organami NATO, UE i innych organizacji międzynarodowych w obszarze obrony narodowej w zakresie cyberbezpieczeństwa. Minister Obrony Narodowej jest także odpowiedzialny za:

- Zapewnienie zdolności Siłom Zbrojnym RP w układzie krajowym, sojuszniczym i koalicyjnym do prowadzenia działań militarnych w przypadku zagrożenia cyberbezpieczeństwa powodującego konieczność działań obronnych,
- Rozwijanie umiejętności Sił Zbrojnych RP w zakresie zapewnienia cyberbezpieczeństwa przez organizację specjalistycznych przedsięwzięć szkoleniowych,
- Pozyskiwanie i rozwój narzędzi służących budowaniu zdolności zapewnienia cyberbezpieczeństwa w Siłach Zbrojnych RP,
- Ocenę wpływu incydentów na system obrony państwa,
- Kierowanie działaniami związanymi z obsługą incydentów w czasie stanu wojennego,

3.5. Sankcje

Operatorzy usług kluczowych i dostawcy usług cyfrowych za zaniechanie lub niedopełnienie obowiązków wynikających z treści ustawy, mogą zostać ukarani karą pieniężną w wysokości od 1000 zł do 1 000 000 zł. Kara pieniężna jest nakładana w drodze decyzji przez organ właściwy do spraw cyberbezpieczeństwa, a wpływy pochodzące z tytułu kar będą stanowić dochód budżetu państwa.

4. Strategia i koordynacja polityki w zakresie cyberbezpieczeństwa

4.1. Strategia Cyberbezpieczeństwa RP

Projekt strategii opracowuje minister właściwy ds. informatyzacji we współpracy z pełnomocnikiem ds. cyberbezpieczeństwa oraz innymi ministrami. Strategia przyjmowana jest uchwałą Rady Ministrów.

Dokument określa cele strategiczne oraz odpowiednie środki polityczne i regulacyjne, które pozwolą osiągnąć i utrzymać wysoki poziom cyberbezpieczeństwa. Strategia uwzględnia również priorytety, podmioty zaangażowane w jej wdrażanie oraz działania odnoszące się do programów edukacyjnych, informacyjnych oraz planów badawczo-rozwojowych.

Dokument obowiązuje przez 5 lat, jednak co 2 lata dokonywany jest przegląd jego aktualności. Do czasu przyjęcia strategii, jej rolę pełni uchwała Rady Ministrów w sprawie Krajowych Ram Polityki Cyberbezpieczeństwa RP na lata 2017-2022.

4.2. Pełnomocnik i Kolegium ds. Cyberbezpieczeństwa

Ponieważ tematyka cyberbezpieczeństwa jest horyzontalna – dotyczy wielu ministerstw i agencji rządowych, ustawa wprowadza Kolegium ds. Cyberbezpieczeństwa i Pełnomocnika ds. Cyberbezpieczeństwa w celu koordynacji polityki w skali państwa.

Pełnomocnik jest powoływany i dowoływany przez Prezesa Rady Ministrów w randze sekretarza lub podsekretarza stanu i podlega Radzie Ministrów. Do jego zdań należy:

- analiza i ocena funkcjonowania krajowego systemu cyberbezpieczeństwa;
- nadzór nad procesem zarządzania ryzykiem krajowego systemu cyberbezpieczeństwa;
- opiniowanie dokumentów rządowych, w tym projektów aktów prawnych, mających wpływ na realizację zadań z zakresu cyberbezpieczeństwa;
- upowszechnianie nowych rozwiązań i inicjowanie działań w zakresie zapewnienia cyberbezpieczeństwa na poziomie krajowym;
- inicjowanie krajowych ćwiczeń w zakresie cyberbezpieczeństwa;
- wydawanie rekomendacji dotyczących stosowania urządzeń informatycznych lub oprogramowania na wniosek CSIRT.

Dodatkowo Pełnomocnik prowadzi współpracę międzynarodową, wspiera badania naukowe i rozwój technologii z zakresu cyberbezpieczeństwa i działa na rzecz podnoszenia świadomości społeczeństwa w zakresie zagrożeń cyberbezpieczeństwa i bezpiecznego korzystania z Internetu.

Kolegium ds. Cyberbezpieczeństwa jest organem opiniodawczo-doradczym Rady Ministrów. Przewodniczy mu Prezes Rady Ministrów, a w jego skład wchodzą: minister właściwy do spraw wewnętrznych, minister właściwy do spraw informatyzacji, Minister Obrony Narodowej, minister właściwy do spraw zagranicznych, Szef Kancelarii Prezesa Rady Ministrów, Szef Biura Bezpieczeństwa Narodowego oraz minister odpowiedzialny za koordynację działalności służb specjalnych. W posiedzeniach Kolegium uczestniczą dodatkowo Dyrektor Rządowego Centrum Bezpieczeństwa; Szef Agencji Bezpieczeństwa Wewnętrznego albo jego zastępca; Szef Służby Kontrwywiadu Wojskowego albo jego zastępca oraz Dyrektor Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego.

5. Podsumowanie

Wdrożenie ustawy o krajowym systemie cyberbezpieczeństwa to wyzwanie zarówno dla administracji, jak i sektora prywatnego.

Przede wszystkim wciąż nie zostali wyznaczeni operatorzy usług kluczowych. Organy właściwe mają na to czas do listopada 2018 roku.

Dodatkowo dużym wyzwaniem jest organizacja systemu w poszczególnych sektorach, związana z ustanowieniem sektorowych zespołów cyberbezpieczeństwa oraz zmianami prawnymi w prawie sektorowym. Organy właściwe muszą także zbudować kompetencje w zakresie nadzoru nad cyberbezpieczeństwem, co może być dużym wyzwaniem w związku z niedoborem specjalistów w dziedzinie cyberbezpieczeństwa.

Trwają prace nad rozporządzeniami wykonawczymi, określającymi progi raportowania oraz wymogi dla sektorowych zespołów cyberbezpieczeństwa.

Obowiązek raportowania incydentów to spora zmiana dla sektora prywatnego i wyzwanie dla administracji w zakresie opracowania konkretnych narzędzi – systemu teleinformatycznego, który w założeniu ma wspierać krajowy system cyberbezpieczeństwa.

CYBERPOLICY

NASK