CyberPOLICY NASK

Nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa - najważniejsze zmiany dla podmiotów

23 kwietnia 2024 r. udostępniono projekt nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw, która ma implementować do polskiego porządku prawnego dyrektywę NIS 2[1]. Czas na jej wdrożenie do krajowych porządków prawnych mija 17 października 2024 roku.

Wprowadzenie

Dyrektywa NIS 2 przekształca dotychczasowe ramy systemu cyberbezpieczeństwa w Unii Europejskiej. Wprowadza m.in. nowe zadania dla państw członkowskich, rozszerza zakres podmiotów objętych obowiązkami z zakresu cyberbezpieczeństwa oraz redefiniuje kompetencje organów UE. Kolejnym krokiem jest wdrożenie dyrektywy do krajowych porządków prawnych – państwa mają na to czas do 17 października 2024 r. Polski projekt nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa ma służyć realizacji tego wymogu. W związku z tym, rozszerza on krąg podmiotów objętych przepisami ustawy oraz katalog obowiązków, które powinny one spełniać. W nowelizacji przewidziano również utworzenie nowych struktur realizujących zadania z zakresu cyberbezpieczeństwa oraz wdrożenie nowych kanałów komunikacyjnych. Nowe przepisy uszczegóławiają także zasady w zakresie nadzoru i egzekwowania przepisów.

Wyznaczanie podmiotów kluczowych i ważnych

Nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa (dalej: Ustawy o KSC) wprowadza nowy podział podmiotów objętych obowiązkami wynikającymi z jej przepisów. Dotychczasowe rozdzielenie na operatorów usług kluczowych i dostawców usług cyfrowych ustępuje miejsca podziałowi na podmioty kluczowe i ważne. Mają być one wyznaczane w sektorach i podsektorach określonych w załącznikach do ustawy.

W stosunku do obecnie obowiązującej ustawy o krajowym systemie cyberbezpieczeństwa, katalog sektorów objętych przepisami uległ rozszerzeniu. Wynika to bezpośrednio z dyrektywy NIS 2, w której obok sektorów energii, transportu, zdrowia, bankowości, infrastruktury rynków finansowych, zaopatrzenia w wodę, infrastruktury cyfrowej, znalazły się także sektory: ścieków, zarządzania ICT, przestrzeni kosmicznej, poczty, produkcji, produkcji i dystrybucji chemikaliów, produkcji i dystrybucji żywności.

[1] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (Dz.U. L 333 z 27.12.2022).

Sektor		Ustawa o KSC	Ustawa o KSC 2.0 – sektory kluczowe	Ustawa o KSC 2.0 – sektory ważne
	Energia	✓	✓	
	Transport	✓	✓	
	Bankowość	✓	✓	
	Infrastruktura rynków finansowych	✓	✓	
	Ochrona zdrowia	✓	✓	
	Zaopatrzenie w wodę pitną i jej dystrybucja	✓	✓	
	Infrastruktura cyfrowa	✓	✓	
	Ścieki		✓	
	Zarządzanie usługami ICT		✓	
	Administracja publiczna		✓	
	Przestrzeń kosmiczna		✓	
	Usługi pocztowe i kurierskie			✓
	Gospodarowanie odpadami			✓

	Produkcja, wytwarzanie i dystrybucja chemikaliów		✓	
	Produkcja, przetwarzanie i dystrybucja żywności		✓	
	Produkcja		✓	
	Dostawcy usług cyfrowych			✓
	Badania naukowe			✓

Nowe przepisy określają warunki objęcia danego podmiotu obowiązkami wynikającymi z ustawy, a także procedurę umieszczenia go w wykazie podmiotów kluczowych lub ważnych.

Co do zasady podmiotem kluczowym jest osoba fizyczna, osoba prawna albo jednostka organizacyjna nieposiadająca osobowości prawnej:

- wskazana w załączniku nr 1 lub nr 2 do ustawy,
- przewyższająca wymogi dla średniego przedsiębiorstwa określone w art. 2 ust. 1 załącznika I do rozporządzenia 651/2014/UE[2].

Zachowana została zatem wynikająca z dyrektywy NIS 2 zasada *size-cap rule*, wprowadzająca kryterium wielkości jako ogólną zasadę identyfikowania podmiotów kluczowych i ważnych. Oprócz tego, do podmiotów kluczowych zalicza się także:

- przedsiębiorcę komunikacji elektronicznej, który co najmniej spełnia wymogi dla średniego przedsiębiorcy określone w rozporządzeniu 651/2014/UE;
- niezależnie od wielkości podmiotu:
    - dostawcę usług DNS,
    - dostawcę usług zarządzanych w zakresie cyberbezpieczeństwa,
    - kwalifikowanego dostawcę usług zaufania w rozumieniu art. 3 pkt 20 rozporządzenia nr 910/2014 (eIDAS)[3],

[2] Zgodnie z art. 2 ust. 1 załącznika I do rozporządzenia 651/2014/UE za średnie przedsiębiorstwa uznaje się przedsiębiorstwa zatrudniające co najmniej 250 osób i których roczny obrót przekracza 50 milionów EUR, lub których roczna suma bilansowa przekracza 43 miliony EUR. Za: Rozporządzenie Komisji (UE) nr 651/2014 z dnia 17 czerwca 2014 r. uznające niektóre rodzaje pomocy za zgodne z rynkiem wewnętrznym w zastosowaniu art. 107 i 108 Traktatu (Dz.U. L 187 z 26.6.2014).

[3] Rozporządzenie Parlamentu Europejskiego I Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (Dz.U. L 257 z 28.8.2014).

- podmiot krytyczny, zidentyfikowany zgodnie z art. 6 dyrektywy 2022/2557 (CER)[4],
- podmiot publiczny,
- podmiot zidentyfikowany jako podmiot kluczowy przez organ właściwy do spraw cyberbezpieczeństwa,
- rejestr nazw domen najwyższego poziomu (TLD).

W odróżnieniu od przepisów dyrektywy NIS 2, w projekcie nowelizacji przewidziano, że dostawca usług zarządzanych w zakresie cyberbezpieczeństwa (podmiot typu *Security Operations Center, Computer Emerge Response Team* itp.) jest podmiotem kluczowym niezależenie od wielkości. Zmianą w stosunku do postanowień dyrektywy jest również objęcie przepisami ustawy wszystkich podmiotów publicznych, niezależnie od wielkości.

Z kolei podmiotem ważnym, co do zasady, jest osoba fizyczna, osoba prawna albo jednostka organizacyjna nieposiadająca osobowości prawnej

- wskazana w załączniku nr 1 lub nr 2 do ustawy,
- spełniająca wymogi dla średniego przedsiębiorstwa określone w art. 2 ust. 1 załącznika I do rozporządzenia 651/2014/UE.

Oprócz tego, za podmioty ważne uznaje się także:

- mikro-, małego lub średniego przedsiębiorcę w rozumieniu rozporządzenia 651/2014/UE, który jest:
  - niekwalifikowanym dostawcą usług zaufania,
  - przedsiębiorcą komunikacji elektronicznej,
- podmiot zidentyfikowany jako podmiot ważny przez organ właściwy do spraw cyberbezpieczeństwa.

Projekt nowelizacji ustawy, podobnie jak dyrektywa NIS 2, zakłada samoidentyfikację podmiotów, które zobowiązane są następnie złożyć wniosek o wpis do wykazu podmiotów kluczowych i ważnych. Nowe przepisy umożliwiają jednak wpisanie określonego podmiotu do wykazu, jeżeli nie złożył on wniosku o wpis, a spełnia przesłanki uznania go za kluczowy lub ważny.

To rozwiązanie ma pozwolić na objęcie obowiązkami wynikającymi z ustawy nawet tych podmiotów, które z jakichś względów nie będą chciały samodzielnie zidentyfikować się jako kluczowe lub ważne. Wpisanie do wykazu w ten sposób jest inną czynnością z zakresu administracji publicznej, na którą przysługuje skarga do sądu administracyjnego.

Projekt nowelizacji dopuszcza również jeszcze inną formę uznania osoby fizycznej, osoby prawnej albo jednostki organizacyjnej nieposiadającej osobowości prawnej za podmiot kluczowy lub podmiot ważny, jeżeli jest ona mikro- lub małym przedsiębiorcą, prowadzi działalność określoną w załączniku nr 1 lub nr 2 do ustawy oraz spełnia chociaż jedną z poniższych przesłanek:

- jako jedyna świadczy usługę, która ma kluczowe znaczenie dla krytycznej działalności społecznej lub gospodarczej,

[4] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE (Dz.U. L 333 z 27.12.2022)

- zakłócenie świadczenia przez nią usługi spowoduje poważne zagrożenie dla bezpieczeństwa państwa, bezpieczeństwa i porządku publicznego lub obronności,
- zakłócenie świadczenia przez nią usługi spowoduje ryzyko systemowe zaprzestania świadczenia usług przez podmioty kluczowe lub podmioty ważne,
  świadczenie przez nią usług ma istotne znaczenie na poziomie krajowym lub województwa lub ma znaczenie dla dwóch lub więcej sektorów określonych w załączniku nr 1 lub nr 2 do ustawy.

Wykaz podmiotów kluczowych i ważnych

Do tej pory operatorzy usług kluczowych byli wyznaczani w drodze decyzji administracyjnej organu właściwego do spraw cyberbezpieczeństwa. Nowelizacja odchodzi jednak od tej zasady i wprowadza samoidentyfikację podmiotów kluczowych i ważnych, nakładając na nie obowiązek samodzielnej rejestracji w wykazie prowadzonym przez ministra właściwego do spraw informatyzacji.

Podmioty zobowiązane będą do złożenia wniosku o wpis do rejestru w terminie 2 miesięcy od spełnienia przesłanek uznania za podmiot kluczowy lub ważny.

Wykaz będzie zawierał wszystkie informacje niezbędne do skutecznego nadzoru nad tymi podmiotami oraz do wykonywania ustawowych zadań nałożonych na zespoły CSIRT poziomu krajowego oraz CSIRT sektorowe. Oprócz danych identyfikujących podmiot, w wykazie znajdzie się m.in. informacja o ewentualnych zawartych porozumieniach w sprawie wymiany informacji o zdarzeniach z zakresu cyberbezpieczeństwa (m.in. porozumienie w sprawie inicjatyw typu ISAC) oraz informacja czy podmiot jest podmiotem krytycznym w rozumieniu dyrektywy CER. Oprócz tego, podmiot będzie musiał zadeklarować, czy wykonuje działalność w innych państwach członkowskich UE, co pozwoli określić m.in. wpływ transgraniczny potencjalnych incydentów.

Część informacji w wykazie będzie uzupełniana z urzędu przez ministra właściwego do spraw informatyzacji.

Aby uniknąć nakładania zbędnych obowiązków na podmioty, w niektórych przypadkach minister sam dokona rejestracji podmiotów z grup, które w całości znajdą się w wykazie, np. przedsiębiorców telekomunikacyjnych, podmiotów krytycznych, dostawców usług zaufania czy podmiotów publicznych. Dane wykorzystane w tym celu będą pochodzić z rejestrów publicznych.

Wykaz będzie prowadzony w systemie teleinformatycznym S46, a wnioski do niego składane mają być w formie elektronicznej, również z wykorzystaniem tego systemu.

Dane z wykazu będą udostępniane zespołom CSIRT poziomu krajowego (CSIRT MON, CSIRT NASK i CSIRT GOV) oraz CSIRT sektorowemu w zakresie sektora lub podsektora, dla którego został ustanowiony. Oprócz tego dostęp do danych z wykazu będzie miał również organ właściwy do spraw cyberbezpieczeństwa w zakresie nadzorowanego sektora lub podsektora, a także podmiot kluczowy lub ważny w zakresie go dotyczącym. Ponadto, o dostęp do tych danych będą mogły wnioskować inne organy państwa takie jak np. policja, prokuratura i sądy. Aby zagwarantować podmiotom bezpieczeństwo i zapewnić ochronę ich interesów, do

wykazu nie będą miały zastosowania przepisy ustawy o dostępie do informacji publicznej[5] oraz ustawy o otwartych danych[6].

Wpis do wykazu będzie równoznaczny z uznaniem podmiotu za kluczowy lub ważny i będzie dokonywał się automatycznie, z chwilą złożenia poprawnego wniosku. Organ właściwy do spraw cyberbezpieczeństwa będzie mógł weryfikować dane zawarte w wykazie i w razie potrzeby wzywać podmiot do ich zmiany pod rygorem nałożenia administracyjnej kary pieniężnej.

Ocena bezpieczeństwa

Nowym rozwiązaniem zaproponowanym w nowelizacji, mającym zwiększać bezpieczeństwo systemów informacyjnych wykorzystywanych przez podmioty krajowego systemu cyberbezpieczeństwa, jest ocena bezpieczeństwa, przeprowadzana w celu identyfikacji podatności danego systemu informacyjnego.

Co do zasady, może być ona przeprowadzana prze CSIRT GOV, CSIRT MON lub CSIRT NASK po poinformowaniu organu właściwego do spraw cyberbezpieczeństwa o takim zamiarze. Przepisy dopuszczają także możliwość przeprowadzenia oceny bezpieczeństwa przez CSIRT sektorowy za zgodą właściwego CSIRT poziomu krajowego, przy zachowaniu wymogu poinformowania organu właściwego dla danego sektora.

Aby zapewnić spójność krajowych przepisów, wyłączono możliwość prowadzenia oceny bezpieczeństwa w dwóch przypadkach:

- dla systemów teleinformatycznych podmiotów krajowego systemu cyberbezpieczeństwa, które znajdują się w zbiorze organów i podmiotów wymienionych w art. 32a ustawy o ABW i AW[7],
- dla systemów teleinformatycznych akredytowanych na podstawie art. 48 ustawy o ochronie informacji niejawnych[8].

Ocena bezpieczeństwa będzie mogła być przeprowadzona wyłącznie za zgodą podmiotu krajowego systemu cyberbezpieczeństwa, wyrażoną w postaci pisemnej lub elektronicznej pod rygorem nieważności. Dopuszcza się jednak wykonanie takiej oceny na zlecenie organu właściwego do spraw cyberbezpieczeństwa, co wypełnia wprowadzone dyrektywą NIS 2 przepisy dotyczące tzw. *security scans*. Nie może ona jednak zakłócać pracy systemu informacyjnego, ograniczać jego dostępności lub prowadzić do nieodwracalnego zniszczenia danych przetwarzanych w systemie. Tryb i ramowe warunki przeprowadzania oceny muszą zostać ustalone z podmiotem w drodze porozumienia.

Zespołowi CSIRT nadano dwa ważne uprawnienia, które są niezbędne do skutecznego przeprowadzenia oceny bezpieczeństwa. Po pierwsze, w celu zbadania podatności systemu, będzie on mógł wytwarzać lub pozyskiwać urządzenia bądź oprogramowanie przystosowane

[5] Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2022 r. poz. 902).
[6] Ustawa z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego (Dz. U. z 2023 r. poz. 1524).
[7] Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. 2002 Nr 74 poz. 676).
[8] Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. 2010 Nr 182 poz. 1228).

do popełnienia przestępstw określonych w art. 165 § 1 pkt 4[9], art. 267 § 3[10], art. 268a[11] § 1 albo § 2 w związku z § 1, art. 269 § 1[12] lub 2 albo art. 269a[13] ustawy z dnia 6 czerwca 1997 r. – Kodeks karny. Po drugie, CSIRT będzie mógł zyskać dostęp do informacji dla niego nieprzeznaczonej, przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie, a także uzyskać dostęp do całości lub części systemu informacyjnego.

Informacje uzyskane w wyniku oceny stanowić będą tajemnicę prawnie chronioną, a CSIRT nie będzie mógł wykorzystać ich do realizacji innych ustawowych zadań. Wprowadza się jednak zasadę informowania ministra właściwego do spraw informatyzacji oraz Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa o ujawnionych podczas oceny bezpieczeństwa podatnościach, które mogą występować w systemach informacyjnych innych podmiotów.

CSIRT sektorowy

Nowelizacja ustawy wprowadza także obowiązek powołania przez organ właściwy do spraw cyberbezpieczeństwa CSIRT sektorowego, właściwego dla danego sektora lub podsektora. Jest to istotna zmiana w stosunku do obecnie obowiązujących przepisów, które nie przewidują takiej konieczności. Do tej pory powstały dwa takie zespoły – CSIRT KNF (dla sektora finansowego) oraz Centrum e-Zdrowia (dla sektora ochrony zdrowia).

Na powołanie CSIRT sektorowych organy właściwe mają 18 miesięcy.

Takie zespoły mają wspierać podmioty kluczowe i ważne w obszarze przyjmowania zgłoszeń i reagowania na incydenty. Do czasu osiągnięcia zdolności operacyjnej przez CSIRT sektorowe, podmioty kluczowe i ważne będą jednak zgłaszały incydenty poważne do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV, tak jak obecnie.

Ważnym obowiązkiem dla CSIRT sektorowych w przypadku przyjęcia wczesnego ostrzeżenia o incydencie poważnym jest przekazanie podmiotowi zgłaszającemu wytycznych dotyczących wdrożenia odpowiednich środków lub udzielenie wsparcia technicznego. W przypadku incydentu poważnego, wyczerpującego znamiona przestępstwa, CSIRT sektorowy przekazuje podmiotowi również informacje o sposobie zgłoszenia organom ścigania.

CSIRT sektorowy, który przyjął wczesne ostrzeżenie, może także zwrócić się do zgłaszającego podmiotu o uzupełnienie potrzebnych informacji, w tym tych stanowiących tajemnice prawnie chronione, w zakresie niezbędnym do realizacji ustawowych zadań.

---

[7] Przestępstwo polegające na sprowadzeniu niebezpieczeństwa dla życia lub zdrowia wielu osób albo dla mienia w wielkich rozmiarach w ramach którego sprawca zakłóca, uniemożliwia lub w inny sposób wpływaj na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych.

[10] Przestępstwo, w którym sprawca w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem.

[11] Przestępstwo, w którym sprawca nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa, zmienia lub utrudnia dostęp do danych informatycznych albo w istotnym stopniu zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych.

[12] Przestępstwo, w którym sprawca niszczy, uszkadza, usuwa lub zmienia dane informatyczne o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego albo zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych.

[13] Przestępstwo, w którym sprawca nie będąc do tego uprawnionym, przez transmisję, zniszczenie, usunięcie, uszkodzenie, utrudnienie dostępu lub zmianę danych informatycznych, w istotnym stopniu zakłóca pracę systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej.

Do pozostałych zadań CSIRT sektorowych należeć będzie również:

- gromadzenie informacji o podatnościach i cyberzagrożeniach, które mogą mieć negatywny wpływ na bezpieczeństwo systemów informacyjnych,
- współpraca z podmiotami kluczowymi i podmiotami ważnymi w zakresie wymiany dobrych praktyk oraz informacji o podatnościach i cyberzagrożeniach, organizacja i uczestniczenie w ćwiczeniach oraz wspieranie inicjatyw szkoleniowych,
- współpraca z CSIRT MON, CSIRT NASK i CSIRT GOV w zakresie koordynowanego przez nie reagowania na incydenty, w szczególności w obszarze wymiany informacji o cyberzagrożeniach oraz stosowanych środkach zapobiegających i ograniczających wpływ incydentów;
- współpraca z innymi CSIRT sektorowymi w zakresie wymiany informacji o podatnościach i cyberzagrożeniach.

CSIRT sektorowe otrzymały także szereg fakultatywnych kompetencji. Wśród najważniejszych można wymienić:

- możliwość prowadzenia dynamicznej analizy ryzyka i analizy incydentów we współpracy z CSIRT MON, CSIRT NASK i CSIRT GOV,
- wspomaganie podmiotów kluczowych i ważnych w podnoszeniu świadomości w obszarze cyberzagrożeń,
- wspieranie podmiotów kluczowych i ważnych, w uzgodnieniu z nimi, wykonywania przez nie obowiązków i uprawnień określonych w art. 11[14], art. 12[15] i art. 13[16] ustawy;
- wystąpienie do organu właściwego z wnioskiem o wezwanie podmiotu kluczowego i ważnego do usunięcia wykrytych podatności - w ramach reagowania na incydent poważny;
- prowadzenie działań na rzecz podnoszenia poziomu bezpieczeństwa systemów informacyjnych podmiotów kluczowych i ważnych.

Do działań w ramach ostatniego punktu można zaliczyć m.in. wykonywanie oceny bezpieczeństwa oraz identyfikowanie podatności systemów dostępnych w otwartych sieciach teleinformatycznych i powiadamianie ich właścicieli o wykrytych podatnościach oraz cyberzagrożeniach.

CSIRT sektorowe otrzymały także ustawowe upoważnienie do prowadzenia audytu bezpieczeństwa systemu informacyjnego w podmiotach kluczowych lub ważnych. W tym przypadku zastrzeżono jednak, że osoba prowadząca audyt, w okresie roku przed jego rozpoczęciem, nie może realizować zadań wdrożenia systemu zarządzania bezpieczeństwem lub obsługi incydentów w podmiocie audytowanym.

CSIRT sektorowe uprawnione zostały również do zawierania porozumień w sprawie wymiany informacji dotyczących cyberbezpieczeństwa, w tym informacje o cyberzagrożeniach, potencjalnych zdarzeniach dla cyberbezpieczeństwa, podatnościach, technikach i procedurach, oznakach naruszenia integralności systemu, wrogich taktykach, a także informacje o grupach przestępczych, ostrzeżenia dotyczące cyberbezpieczeństwa i zalecenia dotyczące konfiguracji narzędzi bezpieczeństwa mających wykrywać cyberataki.

[14] Obowiązek obsługi incydentów, zgłaszania incydentów poważnych i współdziałania przy obsłudze incydentu poważnego i incydentu krytycznego.
[15] Obowiązek zgłoszenia wczesnego ostrzeżenia.
[16] Możliwość fakultatywnego przekazywania informacji do CSIRT krajowych lub sektorowych.

Oznacza to, że podmioty te mogą być członkami np. ISAC tworzonych w konkretnym sektorze lub podsektorze.

Wprowadzenie prawnego obowiązku utworzenia CSIRT sektorowych dla wszystkich sektorów określonych w załącznikach 1 i 2 do ustawy ma na celu usprawnienie funkcjonowania i zwiększenie skuteczności systemu reagowania na incydenty. W połączeniu z powstałą poprzez gromadzenie informacji bazą wiedzy o cyberzagrożeniach i podatnościach pozwoli skrócić czas obsługi incydentów oraz uwzględnić szczególne uwarunkowania danego sektora.

System teleinformatyczny S46

Projekt nowelizacji Ustawy o KSC zawiera szereg dodatkowych działań, które po jej przyjęciu w procedurze ustawodawczej, będą wymagały wykorzystania systemu teleinformatycznego, o którym mowa w art. 46 ust.1 Ustawy o KSC (w skrócie **system S46)**. Prowadzony jest on przez **ministra właściwego do spraw informatyzacji** lub za pomocą właściwych w tym zakresie **jednostek jemu podległych lub przez niego nadzorowanych**. System ten będzie stanowił podstawowy środek przetwarzania określonych rodzajów informacji w ramach funkcjonowania krajowego systemu cyberbezpieczeństwa. Zostało to wprost podkreślone przez wnioskodawców w uzasadnieniu do przedstawionego 24 kwietnia projektu nowelizacji. Zgodnie z pkt. 2.17.2 uzasadnienia „system S46 zostanie dostosowany do tego aby stać się głównym środkiem komunikacji pomiędzy podmiotami krajowego systemu cyberbezpieczeństwa".

W praktyce oznaczać to będzie wykorzystanie S46 do wymiany informacji zarówno o charakterze operacyjnym, jak i organizacyjnym przez wszystkie podmioty KSC. Przykładem tego drugiego typu danych będzie **prowadzenie wykazu podmiotów kluczowych i ważnych** (art. 46 ust. 1a projektu). Znaczenie S46 dla prawidłowego funkcjonowania KSC potwierdza także **obowiązkowe** (zamiast wcześniejszego, fakultatywnego) **korzystanie z systemu przez CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT sektorowe, organy właściwe do spraw cyberbezpieczeństwa oraz Prezesa Urzędu Ochrony Danych Osobowych** w celu realizacji ich zadań ustawowych (art. 46 ust. 2 projektu). Podmioty kluczowe i ważne będą korzystać z S46 **w terminie 14 dni od dokonania wpisu do wykazu**, a nieprzestrzeganie tego obowiązku narazi je (oraz organy zarządzające) na karę pieniężną.

Poza powyżej wymienionymi do katalogu informacji przetwarzanych z użyciem systemu S46 należeć będą:

- **informacje o osiągnieciu zdolności operacyjnej przez CSIRT sektorowy** (art. 25 ustawy nowelizującej),
- **wnioski o wpis, zmianę wpisu albo o wykreślenie z wykazu podmiotów kluczowych i ważnych** (art. 7 ust. 11 projektu),
- **informacje dotyczące cyberbezpieczeństwa**, w tym informacji o cyberzagrożeniach, potencjalnych zdarzeniach dla cyberbezpieczeństwa, podatnościach, technikach i procedurach, oznakach naruszenia integralności systemu, wrogich taktykach, a także informacje o grupach przestępczych, **ostrzeżenia dotyczące cyberbezpieczeństwa i zalecenia dotyczące konfiguracji narzędzi bezpieczeństwa mających wykrywać cyberataki** (art. 8h ust. 3 projektu),
- **wczesne ostrzeżenie o incydencie poważnym -** przekazywane niezwłocznie, nie później niż w ciągu 24 godzin od momentu jego wykrycia, do właściwego CSIRT sektorowego (art. 11 ust. 1 pkt 4 i ust. 2 projektu),

- **zgłoszenie incydentu poważnego -** przekazywane niezwłocznie, nie później niż w ciągu 72 godzin od momentu jego wykrycia, do właściwego CSIRT sektorowego (art. 11 ust. 1 pkt 4a i ust. 2 projektu),
- **sprawozdania z obsługi incydentu poważnego** (art. 11 ust. 1 pkt. 4b-4c i ust. 2 projektu):
  - **okresowe**, na wniosek właściwego CSIRT sektorowego,
  - **końcowe**, nie później niż w ciągu miesiąca od dnia zgłoszenia incydentu poważnego,
  - **z postępu obsługi**,
- **informacje przekazywane do właściwego CSIRT poziomu krajowego lub sektorowego** o innych incydentach, cyberzagrożeniach, podatnościach, potencjalnych zdarzeniach dla cyberbezpieczeństwa, wykorzystywanych technologiach oraz dotyczące szacowania ryzyka (art. 13 ust. 2 projektu).

Dodatkowo, według propozycji nowych przepisów system S46 będzie wspierał, poza dotychczasowymi zadaniami, także **czynności nadzorcze organów właściwych do spraw cyberbezpieczeństwa** oraz **dokonywanie zgłoszenia naruszenia ochrony danych osobowych**, o którym mowa w art. 33 rozporządzenia 2016/679 (RODO).

Minister właściwy ds. informatyzacji udostępnia **wykaz usług świadczonych przez podmioty kluczowe i ważne, stosowany w systemie S46,** w Biuletynie Informacji Publicznej na swojej stronie.

Wymogi techniczne S46

Zgodnie z projektem nowelizacji minister właściwy do spraw informatyzacji udostępnia w swoim Biuletynie Informacji Publicznej minimalne wymagania techniczne i funkcjonalne korzystania z systemu S46. Jednocześnie przepisy nakładają **obowiązek na podmioty kluczowe i ważne zapewnienia zgodności** ze wspomnianymi wymaganiami i mają na to **3 miesiące od ich udostępnienia**.

Uwierzytelnienie do systemu S46 ma następować za pomocą:

- środka identyfikacji elektronicznej wydanego w systemie identyfikacji elektronicznej przyłączonym do węzła krajowego identyfikacji elektronicznej lub
- środka identyfikacji elektronicznej wydanego w notyfikowanym systemie identyfikacji elektronicznej lub
- danych weryfikowanych za pomocą kwalifikowanego certyfikatu podpisu elektronicznego, jeżeli te dane pozwalają na identyfikację i uwierzytelnienie wymagane w celu realizacji usługi online.

Dostawcy wysokiego ryzyka

Projekt nowelizacji zawiera propozycję mechanizmu uznania za dostawcę wysokiego ryzyka określonego dostawcy sprzętu lub oprogramowania dla szczególnego rodzaju podmiotów gospodarczych i społecznych. W szczególności chodzi tutaj, zgodni z uzasadnieniem do projektu, o sytuację zagrożenia bezpieczeństwa kluczowych podmiotów w Polsce, a przez to w konsekwencji także funkcjonowaniu państwa. Proponowana procedura jest odpowiedzią na zidentyfikowane tak na poziomie krajowym, jak i unijnym, ryzyka związane choćby z rozwojem sieci 5G, niskiej jakości lub nieadekwatnie zabezpieczonych względem zagrożeń produktów i rozwiązań, a także coraz poważniejszych cyberzagrożeń.

Podmiotem uprawnionym do wszczęcia postępowania za dostawcę wysokiego ryzyka (HRV) jest **minister właściwy ds. informatyzacji**. Może to nastąpić **z urzędu** lub **na wniosek** przewodniczącego Kolegium do Spraw Cyberbezpieczeństwa. Postępowanie musi być wszczęte w określonym ustawowo celu – **ochrony bezpieczeństwa państwa** lub **bezpieczeństwa i porządku publicznego**.

Przedmiotem postępowania w sprawie uznania za dostawcę wysokiego ryzyka jest sprzęt lub oprogramowanie wykorzystywane przez:

- podmioty kluczowe lub podmioty ważne, z wyłączeniem podsektora komunikacji elektronicznej lub
- przedsiębiorców telekomunikacyjnych, których roczne przychody z tytułu wykonywania działalności telekomunikacyjnej w poprzednim roku obrotowym były wyższe od kwoty 10 milionów złotych.

Stroną postępowania uznania za HRV jest każdy wobec kogo wszczęto postępowanie – czyli kto został zawiadomiony lub który jest wskazany w BIP na stronie ministra właściwego ds. informatyzacji.

Decyzja o uznaniu za dostawcę wysokiego ryzyka

Decyzja o uznaniu za dostawcę wysokiego ryzyka jest wydawana przez ministra właściwego ds. informatyzacji i **zawiera w szczególności wskazanie produktów, rodzajów usług lub procesów ICT**. Ogłasza się ją w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski" oraz udostępnia w Biuletynie Informacji Publicznej ministra i na stronie internetowej urzędu go obsługującego.

W przypadku uznania za HRV podmioty kluczowe i ważne mają **obowiązek wycofania typów produktów, rodzajów usług i procesów ICT,** objętych decyzją ministra, **nie później niż 7 lat od dnia ogłoszenia decyzji lub udostępnienia o niej informacji**. Z kolei w przypadku określonych przedsiębiorców telekomunikacyjnych ten termin ulega skróceniu **do 4 lat** i obejmuje również **produkty, usługi i procesy ujęte w wykazie kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług**[17]. Wszystkie te podmioty mają także **zakaz wprowadzania do użytkowania** rzeczonych produktów, usług i procesów objętych decyzją. Nie ogranicza to jednak dopuszczalności korzystania, naprawy, modernizacji wymiany elementu lub aktualizacji rozwiązań objętych decyzją, pod warunkiem, że jest to niezbędne dla zapewnienia odpowiedniej jakości i ciągłości świadczonych usług.

W zakresie produktów, usług lub procesów ICT nabytych w drodze **postępowań na gruncie przepisów prawa zamówień publicznych ogólny termin na wycofanie ich nie ulega zmianie** i wynosi 7 lat od dnia ogłoszenia decyzji lub udostępnienia o niej informacji. Natomiast różni się w zakresie produktów, usług i procesów wykorzystywanych do wykonywania funkcji krytycznych dla bezpieczeństwa sieci i usług – **wynosi on 5 lat**.

Opinia Kolegium do Spraw Cyberbezpieczeństwa w postępowaniu

W opiniowaniu w sprawach z zakresu uznania za HRV uczestniczy także Kolegium – musi zostać poproszone o opinię przez ministra właściwego ds. informatyzacji przez rozstrzygnięciem przez

[17] Załącznik nr 3 do projektu nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa (UC32)

niego sprawy. Termin na jej sporządzenie wynosi 3 miesiące od dnia, kiedy minister o nią wystąpi.

Opinia Kolegium w sprawie decyzji musi zawierać analizę szeregu kwestii, mających związek z celem wszczęcia postępowania. Wobec tego jej przedmiotem musi być rozważenie kwestii **zagrożeń bezpieczeństwa narodowego** o charakterze ekonomicznym, wywiadowczym i terrorystycznym oraz **zagrożeń dla realizacji zobowiązań sojuszniczych i europejskich**, jakie stanowi dostawca, a także **prawdopodobieństwa** z jakim dostawca sprzętu lub oprogramowania **znajduje się pod kontrolą państwa spoza UE i NATO**. Ta ostatnia kwestia uwzględniać musi rozważenie **przepisów prawa oraz praktyk ich stosowania** w zakresie regulującym **stosunki pomiędzy dostawcą a krajem** spoza UE i NATO. Dotyczy to także **regulacji z zakresu ochrony danych osobowych**, zwłaszcza jeśli brak jest porozumień z UE w tym przedmiocie. Do tego istotne jest przeanalizowanie **struktury własnościowej** dostawcy oraz **zdolności ingerencji tego państwa w swobodę działalności gospodarczej** takiego podmiotu.

Kolejnym koniecznym do uwzględnienia zagadnieniem są **powiązania dostawcy z podmiotami lub osobami znajdującymi się w załączniku do rozporządzenia Rady (UE) 2019/796**[18] jak np. podmioty i osoby powiązane z działaniami typu APT. Do tego należy wziąć pod uwagę **liczbę i rodzaje wykrytych podatności i incydentów** dotyczących typów produktów, rodzajów usług lub konkretnych procesów ICT dostarczanych przez dostawcę oraz procedury ich eliminowania, szczególnie pod kątem sposobu i czasu poświęconego na te działania.

Dodatkowo niezbędne jest uwzględnienie **trybu i zakresu, w jakim dostawca sprawuje nadzór nad procesem wytwarzania i dostarczania sprzętu lub oprogramowania** oraz ryzyka dla tych procesów. Obowiązkiem jest także zawarcie analizy treści wydanych przez Pełnomocnika Rządu ds. Cyberbezpieczeństwa **rekomendacji dot. stosowania produktów, usług lub procesów ICT**. Sporządzając opinię Kolegium musi uwzględnić także **analizy** przeprowadzone przez CSIRT poziomu krajowego, **dotyczące wpływu konkretnych produktów, usług lub procesów ICT na bezpieczeństwo usług świadczonych przez podmioty kluczowe, ważne i niektórych przedsiębiorców telekomunikacyjnych**, jak również **certyfikaty wydane lub uznawane dla produktów, usług lub procesów ICT w państwa UE lub NATO**, w szczególności te, które były efektem europejskich programów certyfikacji cyberbezpieczeństwa.

Sama **procedura opiniowania** jest wieloetapowa i zakłada przede wszystkim, jako pierwszy krok, powołanie przez przewodniczącego Kolegium zespołu opiniującego spośród przedstawicieli członków tego organu. Każda wybrana osoba przygotowuje **stanowisko w zakresie swojej właściwości**, przekazywane następnie do całego zespołu. Zlecane jest także wykonanie niezbędnych ustawowo analiz. Projekt sporządzonej opinii jest następnie **uzgadniany na posiedzeniu Kolegium**, a po przeprowadzeniu tego procesu gotowy dokument **trafia do ministra właściwego ds. informatyzacji**.

Wyłączenie niektórych przepisów procedury administracyjnej

W ramach postępowania w sprawie uznania za HRV co do zasady stosuje się przepisy kodeksu postępowania administracyjnego, jednak nie wszystkie. Wyłączeniu podlegają przepisy dot.:

- definicji strony postępowania (art. 28 kpa),

[18] Rozporządzenie Rady (UE) 2019/796 z dnia 17 maja 2019 r. w sprawie środków ograniczających w celu zwalczania cyberataków zagrażających Unii lub jej państwom członkowskim

- możliwości udziału organizacji społecznej w postępowaniu administracyjnym (art. 31 kpa),
- obowiązku osobistego stawiennictwa (art. 51 kpa),
- metryki sprawy (art. 66a kpa),
- zawiadomienia i udziału strony w postępowaniu dowodowym (art. 79 kpa).

Polecenie zabezpieczające

Kolejnym nowym środkiem wprowadzonym w projekcie nowelizacji jest możliwość wydania polecenia zabezpieczającego. W przypadku wystąpienia **incydentu krytycznego** minister właściwy do spraw informatyzacji może **fakultatywnie** wydać **w drodze decyzji polecenie zabezpieczające**. Dotyczy ono nieokreślonej liczby podmiotów kluczowych i ważnych, a strony zawiadamia się o czynnościach w sprawie poprzez publiczne udostępnienie informacji w Biuletynie Informacji Publicznej ministra właściwego do spraw informatyzacji. Jest **ogłaszane w dzienniku urzędowym ministra** i udostępnia się o nim informacje na stronie internetowej urzędu go obsługującego. Polecenie podlega **natychmiastowej wykonalności**, a uznaje się je za doręczone **z chwilą jego ogłoszenia**.

Polecenie zabezpieczające musi zawierać określone ustawowo elementy takie jak wskazanie **rodzaju lub rodzajów podmiotów** których dotyczy, a także **obowiązek określonego zachowania** zmniejszającego skutki incydentu krytycznego lub zapobiegającego jego rozprzestrzenianiu się oraz termin jego wdrożenia.

Przed wydaniem polecenia zabezpieczającego **minister, we współpracy z Zespołem do spraw Incydentów Krytycznych** (ZIK), ma obowiązek przeprowadzić **analizę** istotności cyberzagrożenia, rodzajów ryzyk, przewidywanych lub zaistniałych skutków incydentu krytycznego i skuteczności obowiązku określonego zachowania zmniejszającego skutki incydentu krytycznego lub zapobiegającego jego rozprzestrzenianiu się. Ponadto dyrektor RCB, szef ABW oraz minister mogą fakultatywnie wzywać podmioty objęte poleceniem lub organy administracji publicznej do udzielenia informacji niezbędnych do przeprowadzenia analizy. Dodatkowym uprawnieniem dyrektora RCB jest także możliwość zaproszenia przedstawicieli wspomnianych podmiotów lub organów do udziału w pracach lub posiedzeniach ZIK w związku z przygotowywaniem analizy.

Polecenie zabezpieczające wydaje się na **czas koordynacji obsługi incydentu krytycznego** lub na **czas oznaczony**, nie dłużej jednak niż na **2 lata**. Wygasa ono w dwóch sytuacjach: z dniem wskazanym w ogłoszeniu o zakończeniu koordynacji obsługi incydentu w dzienniku urzędowym ministra właściwego do spraw informatyzacji lub po upływie czasu, na który zostało wydane.

Od polecenia zabezpieczającego nie przysługuje wniosek o ponowne rozpatrzenie sprawy, aczkolwiek skargę na nie można wnieść do sądu administracyjnego. Termin na to wynosi **2 miesiące** od dnia, w którym decyzja została ogłoszona w dzienniku urzędowym ministra właściwego do spraw informatyzacji.

Obowiązek określonego zachowania zmniejszającego skutki incydentu krytycznego lub zapobiegającego jego rozprzestrzenianiu się

Projekt nowelizacji wskazuje katalog nakazów lub zakazów określonego zachowania, zmniejszającego skutki incydentu krytycznego lub zapobiegającego jego rozprzestrzenianiu się, możliwe do umieszczenia w poleceniu zabezpieczającym. Należą do nich:

- nakaz przeprowadzenia szacowania ryzyka związanego ze stosowaniem określonego produktu, usługi lub procesu ICT i wprowadzenie środków ochrony proporcjonalnych do zidentyfikowanych ryzyk,
- nakaz przeglądu planów ciągłości działania i planów odtworzenia działalności pod kątem ryzyka wystąpienia incydentu krytycznego związanego z daną podatnością;
- nakaz zastosowania określonej poprawki bezpieczeństwa w produkcie, procesie lub usłudze ICT posiadającym daną podatność,
- nakaz szczególnej konfiguracji produktu, usługi lub procesu ICT, zabezpieczającej przed wykorzystaniem określonej podatności,
- nakaz wzmożonego monitorowania zachowania systemu,
- zakaz korzystania z określonego produktu, usługi lub procesu ICT, które posiada podatność, która przyczyniła się do zaistnienia incydentu krytycznego,
- nakaz wprowadzenia ograniczenia ruchu sieciowego z adresów IP lub adresów URL wchodzącego do infrastruktury podmiotu kluczowego lub podmiotu ważnego, który skutkując zakłóceniem usług świadczonych przez ten podmiot został sklasyfikowany przez CSIRT MON, CSIRT NASK lub CSIRT GOV jako przyczyna trwającego incydentu krytycznego,
- nakaz wstrzymania dystrybucji lub zakaz instalacji określonej wersji oprogramowania,
- nakaz zabezpieczenia określonych informacji, w tym dzienników systemowych,
- nakaz wytworzenia obrazów stanu określonych urządzeń zainfekowanych złośliwym oprogramowaniem.

Przy doborze nakazów lub zakazów z powyższego katalogu niezbędne jest uwzględnienie adekwatności środków, co w szczególności powinno wynikać z analizy przeprowadzanej przez ministra we współpracy z ZIK.

Wyłączenie niektórych przepisów procedury administracyjnej

W ramach postępowania w sprawie wydania polecenia zabezpieczającego nie stosuje się określonych przepisów z zakresu procedury administracyjnej, tj.:

- zasada zapewnienia przez organy czynnego udziału stron w postępowaniu (art. 10 kpa),
- obowiązek zapewnienia reprezentacji strony (art. 34 kpa),
- zawiadomienie i udział strony w postępowaniu dowodowym (art. 79 kpa),
- udowodnienie okoliczności faktycznej (art. 81 kpa),
- zasada rozstrzygania wątpliwości faktycznych na korzyść strony (art. 81a kpa),
- oznaczenie strony lub stron w decyzji administracyjnej (art. 107 § 1 pkt 3 kpa),
- wznowienie postępowania w przypadku niebrania przez stronę udziału w postępowaniu bez jej winy (art. 145 § 1 pkt 4),
- stwierdzenie nieważności decyzji w przypadku gdy decyzja została skierowana do osoby niebędącej stroną w sprawie (art. 156 § 1 pkt 4),
- przepisy dot. ugody administracyjnej (rozdział 8 kpa).

Strategia Cyberbezpieczeństwa RP i Krajowy plan reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę

Strategia Cyberbezpieczeństwa RP

Tak samo jak na gruncie przepisów obecnie obowiązującej ustawy, w jej znowelizowanej wersji przewidziano przyjęcie przez Radę Ministrów w formie uchwały Strategii Cyberbezpieczeństwa RP. Ma ona obejmować sektory kluczowe i ważne.

Nowe przepisy przeformułowują niektóre z obszarów, które mają zostać określone w Strategii – m. in. dodany został zapis o konieczności wskazania mechanizmu służącego określeniu istotnych zasobów i szacowaniu ryzyka.

Istotnie rozbudowany został również katalog zagadnień, które powinny zostać uwzględnione przy opracowywaniu Strategii. Należą do nich m. in.:

- rozwiązania dotyczące cyberbezpieczeństwa w łańcuchu dostaw produktów ICT i usług ICT wykorzystywanych przez podmioty do świadczenia usług,
- rozwiązania dotyczące zarządzania podatnościami, obejmujące promowanie i ułatwianie skoordynowanego ujawniania podatności na podstawie art. 12 ust. 1 dyrektywy 2022/2555 (NIS 2),
- promowanie rozwoju i integracji odpowiednich zaawansowanych technologii służących wdrożeniu najnowocześniejszych środków zarządzania ryzykiem w cyberbezpieczeństwie,
- kształcenie i szkolenia w dziedzinie cyberbezpieczeństwa, umiejętności z tego zakresu, podnoszenie świadomości oraz inicjatywy badawczo-rozwojowe, a także wytyczne dotyczące dobrych praktyk i kontroli w zakresie higieny cyfrowej,
- zapewnienie odpowiednich procedur oraz narzędzi służących wymianie informacji.

W przeciwieństwie do obecnie obowiązujących przepisów ustawy, które przewidują, że Strategia ustalana jest na okres pięciu lat, z możliwością wprowadzenia zmian w okresie jej obowiązywania, w nowelizacji nie wskazano okresu, na który ma ona zostać uchwalona.

Dodatkowo, znowelizowana ustawa przewiduje obowiązek dla CSIRT: MON, NASK, GOV i sektorowych oraz organów właściwych do spraw cyberbezpieczeństwa do przekazania ministrowi właściwemu do spraw informatyzacji, w terminie do dnia 30 marca, informacji o realizacji celów Strategii w poprzednim roku.

Krajowy plan reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę

W nowelizacji został dodany zupełnie nowy w stosunku do obowiązującej wersji ustawy rozdział 13a, dotyczący Krajowego planu reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę (dalej w tekście jako ,,Krajowy plan"). Podobnie jak w przypadku Strategii Cyberbezpieczeństwa RP, Rada Ministrów przyjmuje ten dokument w drodze uchwały. Jest on opracowywany przez ministra właściwego do spraw informatyzacji we współpracy z Pełnomocnikiem, Rządowym Centrum Bezpieczeństwa oraz innymi

ministrami i właściwymi kierownikami urzędów centralnych. Krajowy Plan podlega aktualizacji nie rzadziej niż raz na dwa lata.

Obejmuje on w szczególności:

1) cele krajowych środków i działań służących w zakresie gotowości,
2) zadania organów zaangażowanych w zarządzanie kryzysowe w cyberbezpieczeństwie,
3) procedury zarządzania kryzysowego w cyberprzestrzeni, w tym ich włączenie do ogólnych krajowych ram zarządzania kryzysowego oraz kanały wymiany informacji,
4) krajowe środki służące zapewnieniu gotowości na wypadek wystąpienia incydentów na dużą skalę, w tym ćwiczenia i szkolenia,
5) zasady współpracy między sektorem publicznym i prywatnym w obszarze zarządzania kryzysowego,
6) rodzaje krytycznej infrastruktury informatycznej,
7) krajowe procedury i ustalenia między odpowiednimi organami i instytucjami krajowymi mające na celu zapewnienie efektywnego uczestnictwa danego państwa członkowskiego w skoordynowanym zarządzaniu incydentami i zarządzaniu kryzysowym w cyberbezpieczeństwie na dużą skalę na poziomie Unii oraz efektywnego wsparcia ze strony danego państwa członkowskiego dla tego rodzaju skoordynowanego zarządzania.

Nadzór i kontrola

Nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa zawiera rozbudowany – w porównaniu do obecnej wersji – rozdział dotyczący nadzoru i kontroli. W szczególności rozszerzony i doprecyzowany został katalog czynności nadzorczych i środków egzekwowania przepisów, które mogą zostać zastosowane przez podmioty pełniące funkcje w tym zakresie. Uprawnienia nadzorcze wobec podmiotów kluczowych i ważnych przyznane zostały wyłącznie **organom właściwym do spraw cyberbezpieczeństwa (dalej w tekście jako „organy właściwe")**.

Nadzór

W ramach nadzoru nad podmiotami kluczowymi i ważnymi organ właściwy może:

1) prowadzić kontrole, w tym doraźne, w siedzibie podmiotu, miejscu wykonywania działalności gospodarczej lub zdalnie – w przypadku przedsiębiorców; czas takiej kontroli nie może przekroczyć 48 dni roboczych w jednym roku kalendarzowym,
2) zobowiązać podmiot w drodze decyzji do przeprowadzenia audytu bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi (art. 15 ust. 1), w szczególności w sytuacji wystąpienia poważnego incydentu lub naruszenia przepisów ustawy przez podmiot,
3) zlecić CSIRT: MON, NASK, GOV lub sektorowym dokonanie oceny bezpieczeństwa systemu informacyjnego podmiotu,
4) wystąpić z wnioskiem o udzielenie informacji niezbędnych do oceny:
    - wdrożonych środków technicznych i organizacyjnych, odpowiednich i proporcjonalnych do oszacowanego ryzyka (art. 8 ust. 1 pkt 2),
    - stosowanych środków zapobiegających i ograniczających wpływ incydentów na bezpieczeństwo systemu informacyjnego wykorzystywanego do świadczenia usługi (art. 8 ust. 1 pkt 5),

- stosowanych środków komunikacji elektronicznej w ramach krajowego systemu cyberbezpieczeństwa (art. 8 ust. 1 pkt 6),
- zgodności z obowiązkiem przedkładania informacji właściwym organom zgodnie z przepisami o wykazie podmiotów kluczowych i ważnych (art. 7),

5) wystąpić z wnioskiem o udzielenie dostępu do danych, dokumentów i informacji koniecznych do wykonywania nadzoru;
6) wystąpić z wnioskiem o przedstawienie dowodów realizacji wymogów dotyczących wdrażania systemu zarządzania bezpieczeństwem informacji w procesach wpływających na świadczenie usług przez podmiot (art. 8 ust. 1).

Ponadto, podmioty kluczowe i ważne mają obowiązek przekazywania, na żądanie organu właściwego, danych, informacji i dokumentów niezbędnych do wykonywania przez organ jego ustawowych uprawnień i obowiązków z zakresu sprawowania nadzoru i kontroli. Żądanie organu powinno być proporcjonalne do celu, któremu ma służyć oraz zawierać m. in. wskazanie zakresu żądanych danych, informacji lub dokumentów oraz uzasadnienie.

Zasadnicza różnica w nadzorze nad podmiotami kluczowymi i ważnymi dotyczy jego charakteru. Nadzór sprawowany nad podmiotami kluczowymi może być bowiem zarówno prewencyjny, jak i następczy, podczas gdy w przypadku podmiotów ważnych może być on prowadzony jedynie następczo, w szczególności, gdy wystąpi uzasadnione podejrzenie, że zachodzi możliwość naruszenia przepisów ustawy.

Środki egzekwowania przepisów

W pierwszej kolejności organ właściwy informuje podmiot kluczowy lub ważny o wstępnych ustaleniach, które mogą prowadzić do zastosowania wobec podmiotu środków egzekwowania przepisów. Może on jednak odstąpić od przekazania takiej informacji, jeżeli utrudniłoby to natychmiastowe działanie w celu zapobieżenia incydentom, reakcji na nie lub mogłoby mieć niekorzystny wpływ na bezpieczeństwo państwa lub porządek publiczny.

Podmiot w odpowiedzi może niezwłocznie, nie później niż w terminie 7 dni od dnia poinformowania o wstępnych ustaleniach, przedstawić organowi swoje stanowisko. Następnie ten może albo uwzględnić stanowisko podmiotu i odstąpić od zastosowania środków egzekwowania przepisów, albo odrzucić to stanowisko i zastosować takie środki.

W przypadku uzasadnionego podejrzenia, że działania lub zaniechania podmiotu kluczowego lub ważnego mogą stanowić naruszenie przepisów ustawy, organ właściwy kieruje do tego podmiotu **pismo w formie elektronicznej z ostrzeżeniem**. Wskazuje w nim czynności, jakie podmiot powinien podjąć, aby zapobiec takim naruszeniom lub ich zaprzestać.

Niezależnie od możliwości wydawania ostrzeżeń, organ właściwy dysponuje **szeregiem innych środków egzekwowania przepisów** wobec podmiotów kluczowych i ważnych. Może on:

- nakazać podjęcie określonych czynności dotyczących obsługi incydentu,
- nakazać, w drodze decyzji:
  - zaniechanie naruszania przepisów ustawy,
  - zapewnienie zgodności systemu zarządzania bezpieczeństwem informacji z wymogami w zakresie środków technicznych i organizacyjnych, odpowiednich i proporcjonalnych do oszacowanego ryzyka (zgodnie z art. 8 ust. 1 pkt. 2) lub realizacji obowiązku zgłaszania incydentu poważnego,

  - poinformowanie odbiorców usług, których dotyczy znaczące cyberzagrożenie, o charakterze tego zagrożenia oraz o możliwych środkach ochronnych lub naprawczych, jakie należy podjąć w reakcji na to zagrożenie,
  - wdrożenie, w określonym terminie, zaleceń wydanych w wyniku audytu bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi,
  - podanie do wiadomości publicznej informacji o naruszeniach przepisów ustawy,
  - podanie do publicznej wiadomości informacji o incydencie poważnym,
- wyznaczyć, w drodze decyzji, na określony czas urzędnika monitorującego do nadzorowania wykonywania obowiązków podmiotu, o których mowa w rozdziale 3 ustawy, ,
- nałożyć, w drodze decyzji, karę pieniężną niezależnie od pozostałych środków egzekwowania przepisów wskazanych w ustawie i ostrzeżenia.

Postępowanie w zakresie zastosowania przez organ właściwy środków egzekwowania przepisów ma charakter jednoinstancyjny, a **na jego decyzje przysługuje skarga do sądu administracyjnego**. Organ wyznacza podmiotowi kluczowemu lub ważnemu termin na podjęcie określonych czynności, usunięcie uchybień lub doprowadzenie do stanu zgodności z postawionymi przez niego wymogami. W przypadku gdy podmiot nie zastosuje się do nakazów lub decyzji organu właściwego, może on zwrócić się do:

1) **organu, który udzielił koncesji podmiotowi kluczowemu lub ważnemu** - o jej zawieszenie, ograniczenie jej zakresu albo cofnięcie do czasu, gdy podmiot podejmie działania niezbędne do usunięcia uchybień lub zaprzestania naruszeń,
2) **organu, który dokonał wpisu podmiotu kluczowego lub ważnego do rejestru działalności regulowanej** - o wykreślenie podmiotu z tego rejestru;
3) **organu, który wydał podmiotowi kluczowemu lub ważnemu zezwolenie na prowadzenie działalności gospodarczej** - o cofnięcie tego zezwolenia do czasu, gdy podmiot podejmie działania niezbędne do usunięcia uchybień lub zaprzestania naruszeń;
4) **sądu** - o nałożenie tymczasowego zakazu zajmowania stanowiska przez osoby kierujące podmiotem.

Stosując środki egzekwowania przepisów, organ właściwy powinien wziąć pod uwagę czynniki takie jak: wagę naruszenia i znaczenie naruszonych przepisów ustawy, czas trwania naruszenia, spowodowane szkody majątkowe i niemajątkowe, umyślny bądź nieumyślny charakter czynu itd.

Metodyki nadzoru i hierarchia priorytetów

Znowelizowana wersja ustawy przewiduje, że organy właściwe mogą, samodzielnie lub wspólnie, tworzyć metodyki nadzoru, określające szczegółowy sposób jego sprawowania nad podmiotami kluczowymi i ważnymi, w tym zakres i przyjęte kryteria oceny. Skuteczność metodyk powinna być co dwa lata oceniana przez organy właściwe w oparciu o ocenę efektywności.

Ponadto, organy właściwe mogą ustalać hierarchię priorytetów w sprawowaniu nadzoru w oparciu o opracowaną metodykę oraz analizę ryzyka dla konkretnego podmiotu kluczowego lub ważnego. Taka analiza powinna uwzględniać w szczególności:

- znaczenie usługi dla bezpieczeństwa narodowego i porządku publicznego,
- wpływ usługi na gospodarkę i społeczeństwo,

- prawdopodobieństwo wystąpienia incydentu w podmiocie nadzorowanym oraz rodzaj tego incydentu,
- potencjalne skutki incydentu, takie jak straty finansowe, szkody wizerunkowe, utrata danych osobowych lub zakłócenia w funkcjonowaniu systemów i infrastruktury.

Pomoc innym państwom członkowskim

W przypadku gdy podmiot kluczowy lub ważny świadczy usługi na terenie Polski, ale jego siedziba, zarząd lub systemy informacyjne znajdują się na terenie innego państwa członkowskiego Unii Europejskiej, organ właściwy może, za pośrednictwem Pojedynczego Punktu Kontaktowego, zwrócić się do organów tego państwa o przeprowadzenie czynności nadzorczych. Analogicznie, polskie organy właściwe udzielają pomocy organom innych państw członkowskich w sprawowaniu nadzoru nad podmiotami, których systemy informacyjne znajdują się w Polsce.

Kary pieniężne

Obecnie obowiązująca wersja ustawy przewiduje szereg kar pieniężnych za naruszenie jej przepisów. Nowelizacja wprowadza jednak dość szerokie zmiany w tym zakresie.

Kary pieniężne dla podmiotów kluczowych i ważnych

Po pierwsze, znacząco zwiększone zostały górne granicy kary możliwej do nałożenia na podmiot kluczowy lub ważny. Według aktualnych przepisów, najwyższa dopuszczalna kara wynosi 1 milion złotych i można ją nałożyć w przypadku najcięższych naruszeń, które prowadzą do skutków takich jak spowodowanie bezpośredniego i poważnego zagrożenia w dziedzinie cyberbezpieczeństwa dla obronności, bezpieczeństwa państwa lub życia i zdrowia ludzi, czy też zagrożenia wywołania poważnej szkody majątkowej. W znowelizowanej wersji ustawy, na podmiot, który dopuści się tego rodzaju naruszeń, organ może nałożyć karę w maksymalnej wysokości aż do 100 milionów złotych.

Po drugie, zaostrzeniu uległy również sankcje za inne rodzaje uchybień przepisom ustawy. Za niewypełnianie obowiązków na podmiot kluczowy może zostać nałożona kara w wysokości do 10 milionów euro (wyrażona w złotych) lub 2% przychodów z działalności gospodarczej w roku obrotowym poprzedzającym wymierzenie kary, a na podmiot ważny – do 7 milionów euro lub 1,4% przychodu. Co więcej, taka kara nie może być niższa niż 20 000 złotych w przypadku podmiotu kluczowego i 15 000 złotych w przypadku ważnego.

Osobista odpowiedzialność kierowników podmiotów kluczowych i ważnych

W nowelizacji zaproponowane zostały także zmiany w przepisach dotyczących kary pieniężnej, która może zostać nałożona na kierownika podmiotu objętego obowiązkami wynikającymi z ustawy. Zgodnie z obecną wersją przepisów, za niedochowanie należytej staranności w zakresie wypełnienia określonych obowiązków, na kierownika operatora usługi kluczowej może zostać nałożona kara w kwocie nie większej niż 200% jego miesięcznego wynagrodzenia. Według znowelizowanej wersji przepisów, karze pieniężnej może podlegać kierownik podmiotu kluczowego lub ważnego za niewykonanie wskazanych w ustawie obowiązków, jeżeli przemawia za tym czas, zakres lub charakter naruszenia. Zwiększeniu ulega również maksymalna kwota kary możliwej do wymierzenia – do 600% otrzymywanego przez kierownika wynagrodzenia, obliczanego według zasad obowiązujących przy ustalaniu ekwiwalentu pieniężnego za urlop.

Co więcej, kara pieniężna może zostać nałożona na kierownika podmiotu kluczowego lub ważnego niezależnie od kary nałożonej na sam podmiot.

Okresowe kary pieniężne

Niezależnie od wymierzenia kary za naruszenia ustawy, organ właściwy może ukarać podmiot kluczowy lub ważny okresową karą pieniężną, jeżeli opóźnia się on z wykonaniem obowiązków nałożonych na niego w ramach czynności nadzorczych lub środków egzekwowania przepisów. Taka kara wynosi od 500 do 100 000 złotych za każdy dzień opóźnienia.

Inne istotne zmiany w zakresie kar pieniężnych

Oprócz opisanych wyżej zmian, w nowelizacji wprowadzono dodatkowe przepisy dotyczące kar pieniężnych, które mają służyć zwiększeniu ich skuteczności i egzekwowalności.

Jednym z takich rozwiązań jest przyznanie organowi właściwemu kompetencji do nadania decyzji o wymierzeniu kary rygoru natychmiastowej wykonalności w całości lub w części. Może on jednak skorzystać z tego uprawnienia jedynie w przypadku, gdy wymaga tego ochrona bezpieczeństwa lub porządku publicznego.

Ponadto, podmiot kluczowy lub ważny, wobec którego wszczęto postępowanie o nałożenie kary lub zatrudniający kierownika, wobec którego je wszczęto, jest zobowiązany do dostarczenia organowi na każde jego żądanie, we wskazanym przez niego terminie, danych niezbędnych do określenia podstawy wymiaru kary pieniężnej. W przypadku gdy podmiot ich nie dostarczy lub będą one niewystarczające, organ właściwy ustali podstawę wymiaru kary pieniężnej w sposób szacunkowy, uwzględniając w szczególności wielkość danego podmiotu, specyfikę jego działalności lub ogólnodostępne dane finansowe.

Nałożona na podmiot lub jego kierownika kara pieniężna musi zostać uiszczona w terminie 14 dni od dnia, w którym decyzja o jej wymierzeniu stała się ostateczna lub od dnia doręczenia decyzji z klauzulą natychmiastowej wykonalności.

Warto dodatkowo zwrócić uwagę na przepis, który ma służyć uniknięciu sytuacji, w której podmiot kluczowy lub ważny, lub jego kierownik zostanie podwójnie ukarany za ten sam czyn. Wyłączona została bowiem możliwość nałożenia kary przez organ właściwy za naruszenie wskazanych w ustawie obowiązków, jeżeli za ten sam czyn została już na podmiot lub jego kierownika nałożona prawomocna kara pieniężna przez Prezesa Urzędu Ochrony Danych Osobowych w związku z naruszeniem ochrony danych osobowych.

Podsumowanie

- **Dotychczasowy podział podmiotów objętych obowiązkami ustawy o KSC** na operatorów usług kluczowych i dostawców usług cyfrowych **ustępuje miejsca podziałowi na podmioty kluczowe i ważne.** Podstawową zasadą ich wyznaczania jest samoidentyfikacja, a następnie wpis do wykazu. Nowelizacja dopuszcza jednak także inne możliwości identyfikacji podmiotów kluczowych i ważnych.
- **Nowelizacja ustawy wprowadza obowiązek powołania przez organ właściwy do spraw cyberbezpieczeństwa CSIRT sektorowego**, właściwego dla danego sektora lub podsektora. Czas na osiągnięcie zdolności operacyjnej wynosi 18 miesięcy. Takie zespoły docelowo mają wspierać podmioty kluczowe i ważne w obszarze

przyjmowania zgłoszeń i reagowania na incydenty oraz stanowić ogniwo łączące te podmioty z CSIRT poziomu krajowego.

- **Jednym z nowych rozwiązań**, mającym zwiększać bezpieczeństwo systemów informacyjnych wykorzystywanych przez podmioty krajowego systemu cyberbezpieczeństwa, **jest ocena bezpieczeństwa**. Dokonywana ma być przez CSIRT poziomu krajowego lub CSIRT sektorowy w celu identyfikacji podatności.
- **System S46** według założeń nowelizacji ma być **głównym środkiem komunikacji pomiędzy podmiotami KSC** – zarówno w zakresie informacji o charakterze **operacyjnym** (w tym wczesne ostrzeżenia, zgłoszenia incydentów poważnych i sprawozdania z ich obsługi), jak i **organizacyjnym** (informacje o gotowości operacyjnej CSIRT sektorowych oraz wnioski o wpis, jego zmianę lub wykreślenia z wykazu podmiotów) i **nadzorczym**
- Decyzja o uznaniu za **dostawcę wysokiego ryzyka** jest wydawana przez ministra właściwego ds. informatyzacji i zawiera w szczególności wskazanie **produktów, rodzajów usług** lub **procesów ICT**, które należy wycofać w określonym terminie (od 4 do 7 lat, w zależności od rodzaju podmiotu lub przeznaczenia produktów, usług i procesów) oraz nie wprowadzać do użytkowania
- Minister może wydać na określony ustawowo czas w drodze decyzji **polecenie zabezpieczające** w przypadku wystąpienia **incydentu krytycznego**, które to zawiera m.in. obowiązek określonego zachowania – ich przykłady są wskazane w projekcie nowelizacji. Podlega natychmiastowej wykonalności i uznawane jest za doręczone z chwilą jego ogłoszenia w **dzienniku urzędowym ministra.** Wydanie polecenia musi natomiast poprzedzać analiza przeprowadzana we współpracy z Zespołem do spraw Incydentów Krytycznych.
- W nowelizacji **rozbudowano katalog zagadnień**, które powinny zostać objęte **Strategią Cyberbezpieczeństwa RP**. Oprócz niej, Rada Ministrów będzie uchwalać również **Krajowy plan reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę**, który będzie obejmował obszary związane z zarządzaniem kryzysowym w cyberbezpieczeństwie.
- **Rozbudowany został katalog środków nadzoru i egzekwowania przepisów** wobec podmiotów kluczowych i ważnych. Obejmują one m. in. możliwość prowadzenia kontroli, zlecania audytu bezpieczeństwa systemów informacyjnych oraz wydawania szeregu nakazów celem wyegzekwowania realizacji przez podmiot obowiązków wynikających z przepisów ustawy.
- **Znacznie podwyższone zostały górne granice kar pieniężnych** możliwych do nałożenia na podmiot kluczowy lub ważny, lub kierownika podmiotu za naruszenie przepisów ustawy. Przewidziano także możliwość stosowania **okresowych kar pieniężnych** za każdy dzień opóźnienia w wykonaniu przez podmiot obowiązków nałożonych w ramach czynności nadzorczych lub środków egzekwowania przepisów.