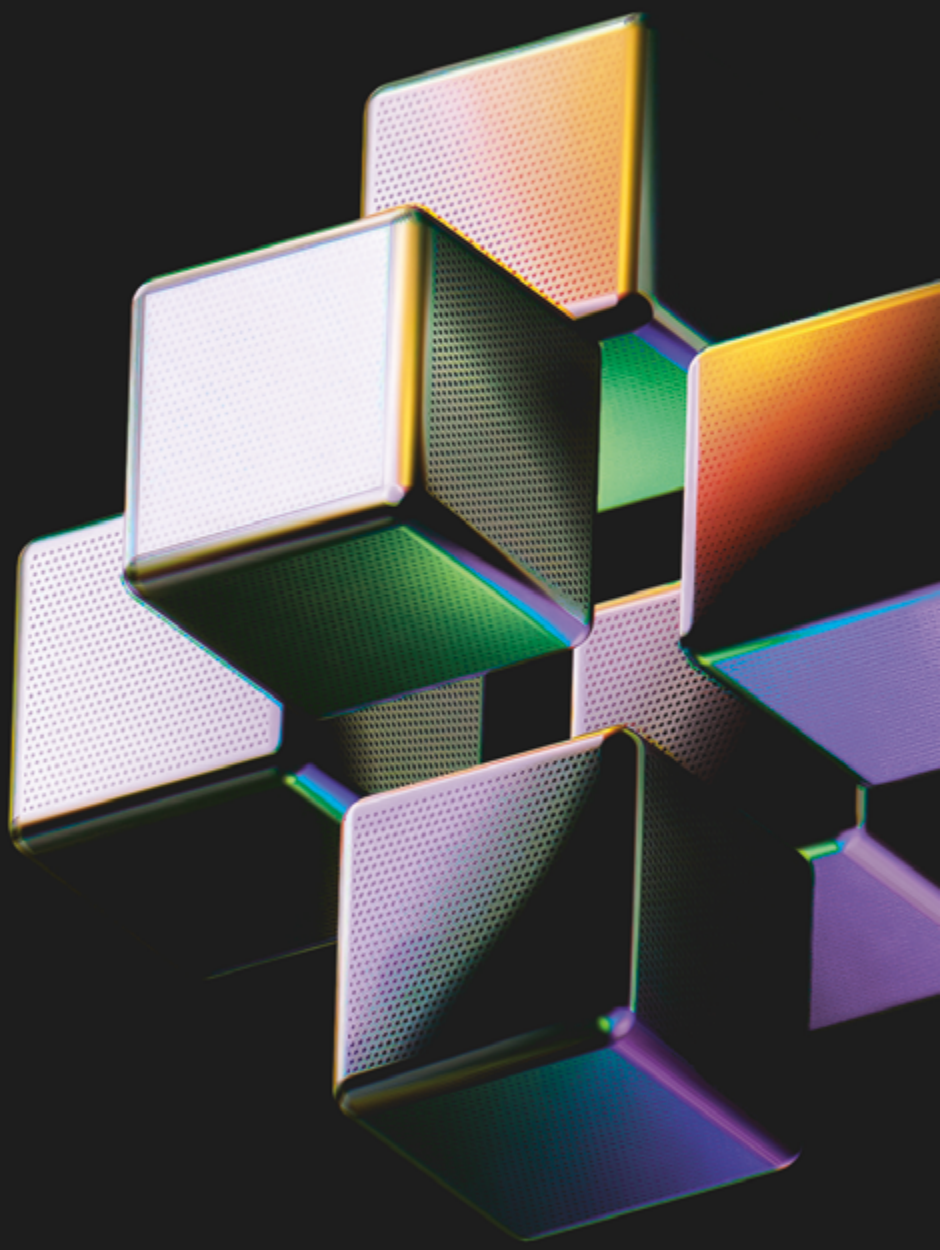
Od wymagań do działania

Praktyczny przewodnik po nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa (KSC 2.0)



NASK

Ministerstwo Cyfryzacji

PROJEKT FINANSOWANY ZE ŚRODKÓW MINISTERSTWA CYFRYZACJI

Od wymagań do działania

Praktyczny przewodnik po nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa (KSC 2.0)

NASK

Ministerstwo Cyfryzacji

PROJEKT FINANSOWANY ZE ŚRODKÓW MINISTERSTWA CYFRYZACJI

Publikacja wyraża jedynie poglądy autorów i nie może być utożsamiana z oficjalnym stanowiskiem Ministerstwa Cyfryzacji.

TYTUŁ
Od wymagań do działania. Praktyczny przewodnik po nowelizacji ustawy
o krajowym systemie cyberbezpieczeństwa (KSC 2.0)

AUTORZY
Anna Kwaśnik (red.), Sylwia Adamczyk, Beata Frankiewicz, Katarzyna Grabowska, Agnieszka Wrońska

KONSULTACJA PRAWNA
Aleksandra Szczęsna

WSPARCIE MERYTORYCZNE
Piotr Słowiński oraz Ministerstwo Cyfryzacji – Departament Cyberbezpieczeństwa

KOREKTA
Katarzyna Nakonieczna, Łukasz Szczęsny

OPRACOWANIE GRAFICZNE
NASK – PIB

NASK – Państwowy Instytut Badawczy

Warszawa 2026

ISBN: 978-83-68356-77-9

Publikacja jest rozpowszechniana na zasadach licencji Creative Commons.
Uznanie autorstwa – Użycie niekomercyjne (CC BY-NC) 4.0 Międzynarodowe

NASK – Państwowy Instytut Badawczy
ul. Kolska 12
01-045 Warszawa

Poradnik ma charakter praktyczny. Opiera się na przepisach ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2026 poz. 20 z późn. zm.), zwanej dalej: KSC 2.0, oraz materiałach informacyjnych i edukacyjnych, a jego treść została zweryfikowana pod kątem zgodności z obowiązującymi przepisami. Jego celem jest pomoc organizacjom w zrozumieniu i realizacji obowiązków wynikających z KSC 2.0. Treści przedstawiono w przystępny sposób, z naciskiem na praktyczne wskazówki. Poradnik nie stanowi komentarza do ustawy ani interpretacji prawnej i nie wyczerpuje wszystkich zagadnień związanych z jej stosowaniem.

Spis treści

6 **KSC 2.0 w praktyce – 6 pytań na start**

8 **Wstęp**

CZĘŚĆ I.

10 **Czy moja organizacja podlega pod KSC 2.0?**

11 Kogo obejmuje ustawa?

13 Jak sprawdzić swoją kwalifikację?

19 Wykaz podmiotów kluczowych i podmiotów ważnych (Wykaz KSC) i System S46

24 Materiały uzupełniające

CZĘŚĆ II.

25 **Obowiązki podmiotów**

29 Zarządzanie cyberbezpieczeństwem

34 Budowanie świadomości cyberbezpieczeństwa i zarządzanie wiedzą

38 Ochrona systemów i informacji

43 Cyberbezpieczeństwo dostawców i usług zewnętrznych

48 Reagowanie i odporność organizacji

54 Zgłaszanie incydentów

61 Nadzór i doskonalenie działania SZBI

65 Przykłady dokumentów związanych z realizacją wymagań KSC 2.0

67 Wymogi SZBI dla podmiotu ważnego będącego podmiotem publicznym

CZĘŚĆ III.

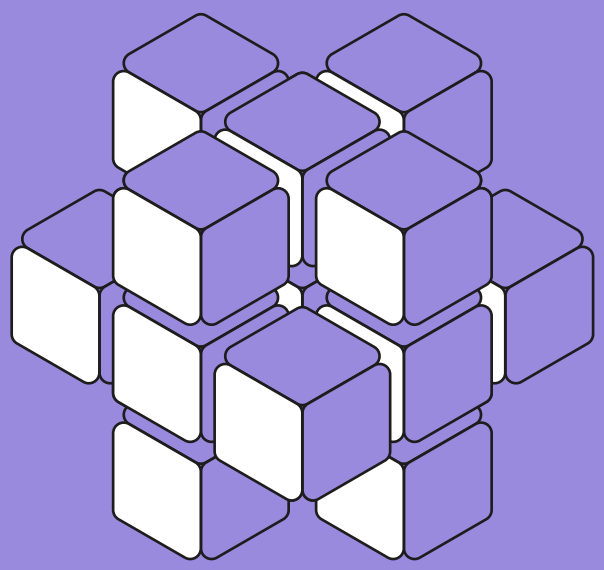
72 **Odpowiedzialność za niewykonanie obowiązków**

75 Kary pieniężne

76 Nie tylko kara – konsekwencje dla organizacji

79 **KSC 2.0 w praktyce. Słowniczek najważniejszych pojęć**

82 **Baza wiedzy i źródła rekomendowane**



KSC 2.0 w praktyce – 6 pytań na start

Czy moja firma ma obowiązek wpisu do Wykazu KSC?

Kluczowe jest sprawdzenie, czy firma działa w sektorze objętym KSC 2.0 i spełnia kryteria podmiotu kluczowego lub podmiotu ważnego. Znaczenie może mieć sektor, skala działalności, rodzaj świadczonych usług, liczba pracowników oraz powiązania z innymi podmiotami.

Czy mała firma również może podlegać KSC 2.0?

Tak. Mała firma również może podlegać przepisom KSC 2.0, jeśli działa w sektorze objętym ustawą i spełnia określone kryteria. Znaczenie ma nie tylko wielkość przedsiębiorstwa, ale także rodzaj świadczonych usług i charakter prowadzonej działalności.

Wpis do Wykazu KSC – kto i kiedy musi złożyć wniosek?

Wniosek o wpis do Wykazu KSC składają podmioty kluczowe i podmioty ważne, które spełniają kryteria określone w ustawie i nie zostały wpisane do wykazu z urzędu. Składa go kierownik podmiotu lub osoba przez niego upoważniona. Samorejestracja odbywa się wyłącznie online za pośrednictwem strony wykaz-ksc.gov.pl. Termin samodzielnej rejestracji dla takich podmiotów upływa 3 października 2026 r.

Jakie obowiązki mają podmioty kluczowe i podmioty ważne?

Podmioty kluczowe i podmioty ważne są zobowiązane m.in. do wpisu do Wykazu KSC, wdrożenia wymagań cyberbezpieczeństwa – w tym systemu zarządzania bezpieczeństwem informacji (SZBI) – i procedur zgłaszania oraz obsługi incydentów, wyznaczenia osób odpowiedzialnych za kontakty w ramach KSC 2.0 i weryfikacji niekaralności personelu wykonującego określone zadania oraz korzystania z Systemu S46.

Czy samorejestracja dotyczy wszystkich podmiotów?

Część podmiotów, w tym m.in. podmioty publiczne, przedsiębiorcy telekomunikacyjni, dostawcy usług zaufania oraz dotychczasowi operatorzy usług kluczowych, jest wpisywana do Wykazu KSC z urzędu i otrzymuje stosowne zawiadomienie. Jeśli twoja firma spełnia kryteria, ale nie należy do grupy wpisywanej z urzędu, ma obowiązek samodzielnie dokonać wpisu do Wykazu KSC.

Brak zgodności z KSC 2.0 – jakie konsekwencje grożą twojej firmie?

Niezastosowanie się do wymagań KSC 2.0 może skutkować zastosowaniem środków przewidzianych w ustawie oraz odpowiedzialnością po stronie organizacji. W określonych przypadkach odpowiedzialność mogą ponosić również osoby zarządzające, w tym kierownik podmiotu. Brak zgodności z wymaganiami to także większe ryzyko cyberataków, przestojów, strat finansowych, utraty danych i reputacji.

?

Wstęp

KSC 2.0 – NOWE ZASADY CYBERBEZPIECZEŃSTWA DLA FIRM I INSTYTUCJI

Cyberbezpieczeństwo stało się strategicznym elementem zarządzania organizacją. Wpływa na ciągłość działania, ochronę danych oraz poziom ryzyka biznesowego i regulacyjnego, a odpowiedzialność za ten obszar spoczywa nie tylko na specjalistach IT, lecz na całej organizacji – pracownikach oraz kierownictwie.

Odpowiedzią na te wyzwania jest **ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa**, która tworzy ramy prawne i organizacyjne służące zwiększaniu odporności państwa, gospodarki i organizacji na cyberzagrożenia oraz usprawnieniu współpracy i reagowania na incydenty. Jej nowelizacja z **2026 r.**, wdrażająca dyrektywę NIS2, rozszerzyła zakres jej stosowania, obejmując obowiązkami w zakresie cyberbezpieczeństwa znacznie szerszą grupę przedsiębiorstw i instytucji działających w kluczowych sektorach gospodarki i administracji.

Znowelizowana ustawa (KSC 2.0) obejmuje 19 sektorów i obszarów działalności, w tym **10 sektorów kluczowych i 9 ważnych**. Są to m.in.: energia, transport, bankowość, infrastruktura rynków finansowych, ochrona zdrowia, gospodarka wodno-ściekowa, infrastruktura cyfrowa, administracja publiczna, usługi ICT, usługi pocztowe, gospodarowanie odpadami, przemysł, produkcja i dystrybucja żywności, dostawcy usług cyfrowych oraz działalność badawczo-rozwojowa.

Jedną z kluczowych zmian wprowadzonych przez nowelizację ustawy KSC 2.0 jest podział organizacji objętych regulacją na **podmioty kluczowe i podmioty ważne**. To, do której kategorii zostanie zakwalifikowana dana organizacja, zależy m.in. od przynależności do sektora, rodzaju prowadzonej działalności oraz wielkości podmiotu. Dlatego jednym z pierwszych kroków dla firmy powinno być sprawdzenie, czy spełnia ustawowe kryteria i czy ciąży na niej obowiązek wpisu do **Wykazu podmiotów kluczowych i podmiotów ważnych (Wykazu KSC)**.

KSC 2.0 to nie tylko nowe obowiązki. To również system współpracy, którego istotnym elementem są **zespoły CSIRT, w tym CSIRT-y sektorowe**. Monitorują one bieżącą sytuację w kraju, wymieniają informacje o zagrożeniach i incydentach oraz wspierają podmioty krajowego systemu cyberbezpieczeństwa w identyfikowaniu cyberzagrożeń, reagowaniu na incydenty oraz wzmacnianiu odporności organizacji.

Podmioty objęte ustawą są między innymi zobowiązane zarządzać ryzykiem, wdrażać zabezpieczenia, zgłaszać incydenty oraz współpracować z właściwymi zespołami CSIRT i organami odpowiedzialnymi za cyberbezpieczeństwo.

Nowe przepisy oznaczają więc dla wielu organizacji konieczność odpowiedzi na podstawowe pytanie: **czy KSC 2.0 dotyczy także naszej firmy, a jeśli tak, to co powinniśmy zrobić?**

Odpowiedź na te i inne pytania zawarliśmy w niniejszej publikacji. Poradnik został podzielony na trzy części, które prowadzą czytelnika od ustalenia, czy organizacja podlega ustawie KSC 2.0, przez poznanie wynikających z niej obowiązków, aż po kwestie odpowiedzialności, kontroli i sankcji. Krok po kroku pokazujemy, **jak ustalić status organizacji, sprawdzić obowiązek wpisu do Wykazu KSC i przygotować się do nowych wymagań**. Struktura pozwala korzystać z poradnika zarówno kompleksowo, jak i w odniesieniu do wybranych zagadnień.

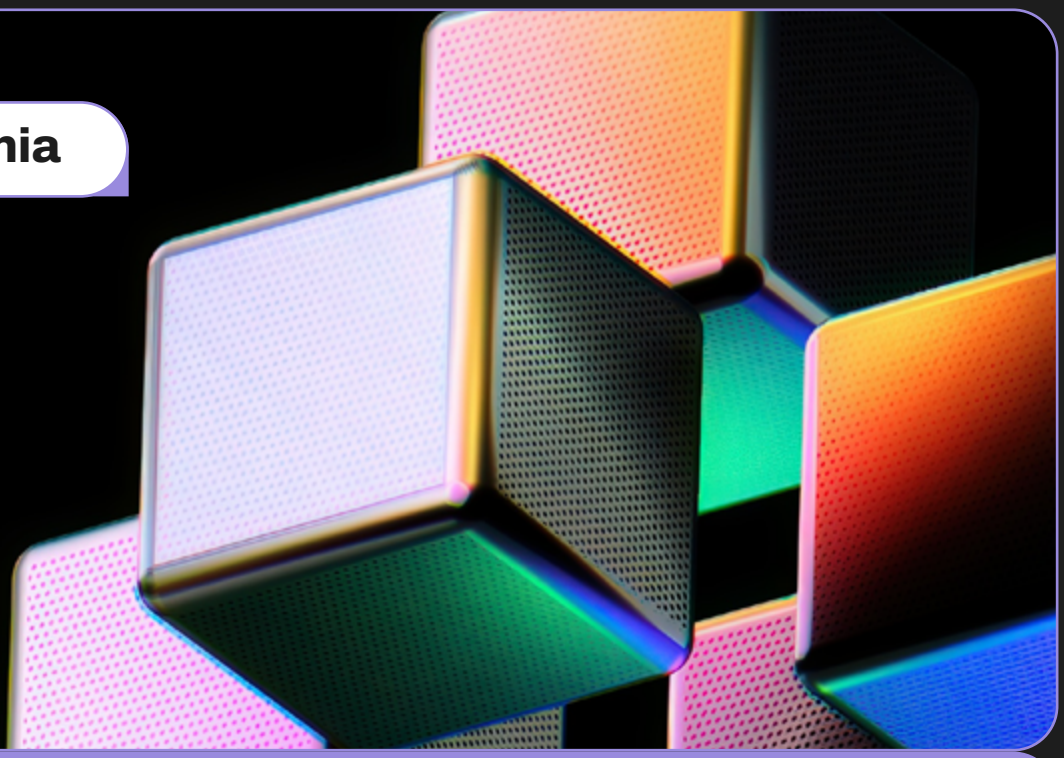
Część pierwsza – **„Czy moja organizacja podlega KSC 2.0?”** – wyjaśnia, jakie podmioty i sektory obejmuje ustawa oraz jak określić status organizacji. Przedstawia kryteria kwalifikacji, zasady samoidentyfikacji, przypadki graniczne, a także informacje o Wykazie KSC i Systemie S46. Część tę uzupełniają praktyczna checklista i przykłady samoidentyfikacji.

Część druga – **„Obowiązki podmiotów”** – omawia najważniejsze wymagania systemu zarządzania bezpieczeństwem informacji (SZBI) oraz pokazuje, jak przełożyć je na konkretne działania. Rozdziały zawierają wyjaśnienie wymagań ustawowych, dobre praktyki, propozycje dokumentacji, źródła wiedzy oraz najczęstsze błędy i pułapki. Obowiązki są przedstawiane z różnych perspektyw, uwzględniając m.in. zarządzanie, zasady postępowania, zabezpieczenia techniczne oraz codzienną działalność organizacji. Wskazano także wyjątki dla podmiotów ważnych będących podmiotami publicznymi, które w określonych przypadkach podlegają uproszczonej ścieżce wdrażania SZBI.

Część trzecia – **„Odpowiedzialność za niewykonanie obowiązków”** – przedstawia zasady kontroli, odpowiedzialności i sankcji, w tym odpowiedzialność kadry kierowniczej. Wskazuje również możliwe konsekwencje niezgodności i incydentów dla działalności i reputacji organizacji. Całość uzupełnia baza wiedzy pozwalająca pogłębić omawiane zagadnienia.

Publikacja odwołuje się do stanu prawnego aktualnego na dzień 28.09.2026 r.

Zapraszamy do lektury!



Czy moja organizacja podlega pod KSC 2.0?

Kogo obejmuje ustawa?

Znowelizowana w 2026 r. ustawa o krajowym systemie cyberbezpieczeństwa (KSC 2.0) obejmuje 10 sektorów kluczowych i 9 sektorów ważnych, które zostały wymienione w załącznikach nr 1 i 2 do ustawy. Jej zakres nie ogranicza się tylko do infrastruktury krytycznej, lecz obejmuje także wiele organizacji realizujących usługi istotne dla funkcjonowania państwa, gospodarki i społeczeństwa.

Podmioty objęte ustawą są klasyfikowane jako podmioty kluczowe lub podmioty ważne. Od przyporządkowania do danej kategorii zależą nałożone na nie obowiązki, zakres nadzoru oraz potencjalne środki egzekwowania przepisów.

CZYM SĄ PODMIOTY KLUCZOWE I PODMIOTY WAŻNE?

Podmioty kluczowe i podmioty ważne są organizacjami, których działalność ma szczególne znaczenie dla funkcjonowania i bezpieczeństwa państwa, gospodarki i społeczeństwa. Zatem merytoryczne obowiązki podmiotu kluczowego i podmiotu ważnego są takie same. Jednak należy zauważyć, że czynnikiem, który różnicuje te podmioty, są czynności nadzorcze i audyty, prowadzone przez organy właściwe do spraw cyberbezpieczeństwa (art. 15 i rozdz. 11 ustawy KSC 2.0).

§

→ WAŻNE

Ustawa przewiduje także kategorie podmiotów uznawanych za kluczowe mimo nieprzekraczania wymogów dla średniego przedsiębiorstwa lub niezależnie od ich wielkości.

Do kategorii podmiotów ważnych mogą należeć niektóre mikro-, małe i średnie przedsiębiorstwa, takie jak niekwalifikowani dostawcy usług zaufania czy przedsiębiorcy komunikacji elektronicznej.

Nadzór i audyty – kluczowe różnice

Podmioty kluczowe	Podmioty ważne
→ podlegają szerszemu zakresowi czynności nadzorczych,	→ nadzór jest podejmowany w przypadku przesłanek wskazujących na naruszenie przepisów,
→ przeprowadzają audyt co najmniej raz na 3 lata oraz na żądanie właściwego organu.	→ przeprowadzają audyt na żądanie właściwego organu.

JAKIE SĄ PODSTAWOWE KRYTERIA KWALIFIKACJI?

Kwalifikacja podmiotu jako podmiotu kluczowego lub podmiotu ważnego zależy przede wszystkim od rodzaju prowadzonej działalności i wielkości. W niektórych przypadkach status podmiotu wynika z charakteru świadczonych usług lub pełnionej funkcji, niezależnie od wielkości organizacji.

TABELA 1. Porównanie wybranych kryteriów kwalifikacji podmiotów kluczowych i podmiotów ważnych.

Lp.	Podmiot kluczowy	Podmiot ważny
1	Wskazany w załączniku nr 1 do ustawy KSC 2.0, większy niż średnie przedsiębiorstwo.	Wskazany w załączniku nr 1 lub nr 2 do ustawy KSC 2.0, spełniający wymogi dla średniego przedsiębiorstwa i nie będący podmiotem kluczowym.
2	Średni lub większy przedsiębiorca komunikacji elektronicznej, mały lub większy dostawca usług zarządzanych w zakresie cyberbezpieczeństwa.	Niekwalifikowany dostawca usług zaufania będący mikro-, małym lub średnim przedsiębiorcą; mniejszy niż średni przedsiębiorca komunikacji elektronicznej.
3	Niezależnie od wielkości: m.in. dostawca usług DNS, kwalifikowany dostawca usług zaufania, podmiot krytyczny, podmiot publiczny wskazany w załączniku nr 1 do ustawy KSC 2.0 w sektorze podmioty publiczne, rejestr nazw domen najwyższego poziomu (TLD).	Podmiot zidentyfikowany jako podmiot ważny na podstawie art. 7l ust. 2 pkt 2 ustawy KSC 2.0.

ŹRÓDŁO: Opracowanie własne NASK – PIB.

JAKI STATUS MAJĄ PODMIOTY PUBLICZNE?

Podmioty publiczne zostały wskazane w załączniku nr 1 i załączniku nr 2 do ustawy KSC 2.0 (osobny sektor „Podmioty publiczne"). Znajdują się zarówno w grupie podmiotów kluczowych, jak i podmiotów ważnych. Dlatego ten sam podmiot może być jednocześnie podmiotem publicznym i podmiotem kluczowym albo podmiotem publicznym i podmiotem ważnym.

Nie każda jednostka publiczna automatycznie jest podmiotem publicznym w rozumieniu ustawy KSC 2.0. Do tej grupy należą m.in. wybrane jednostki sektora finansów publicznych, państwowe instytucje kultury, instytuty badawcze, wojewódzkie fundusze ochrony środowiska i gospodarki wodnej.

JAKIE ISTNIEJĄ WYJĄTKI?

- Ustawa przewiduje szczególne zasady kwalifikacji określonych kategorii podmiotów, w tym niektórych podmiotów publicznych, leczniczych oraz związanych z energetyką jądrową.

- Odrębne zasady ustalenia wielkości przedsiębiorstwa dotyczą przedsiębiorstw partnerskich i powiązanych. Dla jednostek podległych i nadzorowanych przez MON nie obowiązują odrębne kryteria dotyczące wielkości podmiotu. MON samodzielnie wskaże podmioty kluczowe i ważne, bez stosowania kryteriów wielkościowych.

- Organ właściwy w drodze decyzji może, w określonych ustawą przypadkach, uznać organizację za podmiot kluczowy lub podmiot ważny, nawet jeżeli nie spełnia ona standardowych kryteriów kwalifikacyjnych.

Jak sprawdzić swoją kwalifikację?

Jednym z pierwszych kroków w przygotowaniu do wymagań wynikających z KSC 2.0 jest ustalenie, czy organizacja podlega jej przepisom – a jeśli tak – czy kwalifikuje się jako podmiot kluczowy czy podmiot ważny.

W większości przypadków organizacja dokonuje takiej oceny samodzielnie. Proces ten nazywany jest **samoidentyfikacją** i polega na analizie prowadzonej działalności oraz sprawdzeniu kryteriów określonych w ustawie.

Opis procesu przygotowało Ministerstwo Cyfryzacji w artykule: Jak dokonać samoidentyfikacji? dostępnym na portalu gov.pl.

ELEMENTY PROCESU SAMOIDENTYFIKACJI

→ Rodzaj prowadzonej działalności

Pierwszym krokiem jest sprawdzenie, czy organizacja prowadzi działalność w sektorze lub podsektorze wskazanym w załącznikach nr 1 lub 2 do ustawy KSC 2.0. Obejmują one m.in. energię, transport, bankowość, ochronę zdrowia, infrastrukturę cyfrową, zarządzanie usługami ICT, a także wybrane rodzaje działalności produkcyjnej i usługowej.

A

Kod PKD – co warto wiedzieć?

PKD (Polska Klasyfikacja Działalności) służy do określania rodzaju prowadzonej działalności. W procesie samoidentyfikacji na potrzeby KSC 2.0 właściwy kod PKD może być pomocną wskazówką, jednak decydujący jest faktyczny zakres świadczonych usług lub wykonywanych zadań.

→ Wielkość organizacji

Kolejnym elementem jest ustalenie wielkości organizacji.
Pod uwagę bierze się przede wszystkim:

- liczbę pracowników,
- roczny obrót,
- roczną sumę bilansową.

Przy określaniu wielkości organizacji stosuje się definicję mikro-, małych i średnich przedsiębiorstw wynikającą z przepisów unijnych (rozporządzenia Komisji (UE) 651/2014). Co do zasady:

- za **mikroprzedsiębiorstwo** uznaje się podmiot zatrudniający mniej niż 10 pracowników oraz osiągający roczny obrót lub sumę bilansową nieprzekraczające 2 mln euro;
- za **małe przedsiębiorstwo** uznaje się podmiot zatrudniający mniej niż 50 pracowników oraz osiągający roczny obrót lub sumę bilansową nieprzekraczające 10 mln euro;
- za **średnie przedsiębiorstwo** uznaje się podmiot zatrudniający mniej niż 250 pracowników oraz osiągający roczny obrót nieprzekraczający 50 mln euro lub sumę bilansową nieprzekraczającą 43 mln euro.

Przy ustalaniu wielkości przedsiębiorstwa należy również uwzględnić przedsiębiorstwa partnerskie i powiązane. Ma to szczególne znaczenie w przypadku organizacji należących do większych grup. Sama liczba pracowników nie zawsze jest wystarczająca do prawidłowego określenia wielkości podmiotu.

TABELA 2. Kategorie przedsiębiorstw według wielkości.

Kategoria przedsiębiorstwa	Liczba pracowników	Roczny obrót	Roczna suma bilansowa
Mikroprzedsiębiorstwo	< 10	do 2 mln EUR	do 2 mln EUR
Małe przedsiębiorstwo	< 50	do 10 mln EUR	do 10 mln EUR
Średnie przedsiębiorstwo	< 250	do 50 mln EUR	do 43 mln EUR
Duże przedsiębiorstwo	niespełniające kryteriów MŚP	powyżej 50 mln EUR	powyżej 43 mln EUR

ŹRÓDŁO: Opracowanie własne NASK – PIB na podstawie rozporządzenia Komisji (UE) 651/2014/UE z dnia 17 czerwca 2014 r. dotyczącego definicji mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw.

Tabela ma charakter poglądowy. Ostateczna kwalifikacja przedsiębiorstwa następuje zgodnie z przepisami UE i wymaga uwzględnienia liczby pracowników, danych finansowych oraz przedsiębiorstw partnerskich i powiązanych.

→ WARTO WIEDZIEĆ

Po ustaleniu, że organizacja podlega przepisom ustawy KSC 2.0 jako podmiot kluczowy lub podmiot ważny, kolejnym krokiem jest wpis do wykazu podmiotów kluczowych i podmiotów ważnych (Wykaz KSC). Wpis ten umożliwia korzystanie z Systemu S46, który służy do realizacji wybranych obowiązków ustawowych, w tym związanych ze zgłaszaniem incydentów.

CO TO OZNACZA W PRAKTYCE?

Samoidentyfikacji nie należy traktować jako działania jednorazowego. Warto przeprowadzić ją ponownie w przypadku istotnej zmiany rodzaju, wielkości lub skali działalności organizacji albo jej powiązań z innymi podmiotami, ponieważ może to wpłynąć na kwalifikację w KSC 2.0. Każda zmiana danych wpisanych do Wykazu wymaga ich aktualizacji w terminie 14 dni.

SYTUACJE WYMAGAJĄCE DODATKOWEJ ANALIZY

Nie w każdym przypadku ustalenie kwalifikacji będzie proste. Dodatkowej analizy mogą wymagać szczególnie organizacje, które:

- prowadzą kilka rodzajów działalności,
- działają w więcej niż jednym sektorze,
- należą do grupy kapitałowej,
- łączą działalność produkcyjną z usługami ICT lub cyfrowymi,
- wykonują działalność w innym zakresie niż ten wynikający z CEIDG, KRS, statutu czy umowy spółki.

W takich sytuacjach analiza powinna obejmować cały rzeczywisty zakres działalności organizacji, a nie tylko jej główny profil biznesowy.

Może się również zdarzyć, że organizacja spełnia kryteria kwalifikacji w więcej niż jednym obszarze. Przykładowo przedsiębiorstwo może prowadzić działalność produkcyjną, a jednocześnie świadczyć usługi ICT. Każdy z tych obszarów powinien zostać uwzględniony podczas samoidentyfikacji.

PRZYKŁADY SAMOIDENTYFIKACJI W PRAKTYCE

PRZYKŁAD 1. **Działalność jednoznacznie wskazana w ustawie**

Szpital prowadzi działalność w sektorze ochrony zdrowia, który został wskazany w ustawie jako sektor kluczowy. Sam fakt działania w tym sektorze nie przesądza jednak jeszcze o statusie podmiotu jako kluczowego. Konieczne jest również sprawdzenie, czy organizacja spełnia pozostałe kryteria określone w ustawie, w tym dotyczące rodzaju działalności i statusu podmiotu.

Działalność w sektorze objętym KSC 2.0 ułatwia wstępną ocenę kwalifikacji podmiotu, ale nie zastępuje analizy pozostałych przesłanek wskazanych w ustawie.

PRZYKŁAD 2. **Działalność wymagająca dokładniejszej analizy**

Przedsiębiorstwo prowadzi działalność produkcyjną. Nie każda produkcja znajduje się w zakresie KSC 2.0, dlatego konieczne jest ustalenie jej konkretnego rodzaju (np. produkcja komputerów, wyrobów elektronicznych i optycznych czy produkcja pojazdów samochodowych, przyczep i naczep) i sprawdzenie, czy została wskazana w załącznikach do ustawy. Następnie należy zweryfikować pozostałe kryteria.

KSC 2.0 może obejmować również organizacje spoza sektorów najczęściej kojarzonych z cyberbezpieczeństwem czy infrastrukturą krytyczną.

PRZYKŁAD 3. **Działalność prowadzona w kilku obszarach**

Przedsiębiorstwo prowadzi działalność produkcyjną, a jednocześnie świadczy usługi ICT dla klientów biznesowych. W takim przypadku analizie powinny podlegać oba obszary działalności.

Kwalifikacja może wynikać z więcej niż jednego rodzaju działalności, dlatego analiza nie powinna ograniczać się wyłącznie do działalności dominującej.

CHECKLISTA – CZY MOJA ORGANIZACJA PODLEGA KSC 2.0?

Checklista ma charakter pomocniczy i nie jest testem punktowym. Odpowiedzi nie należy sumować ani ustalać na ich podstawie progu kwalifikacji. Każde pytanie dotyczy innego elementu samoidentyfikacji, dlatego wynik należy oceniać łącznie, biorąc pod uwagę rodzaj prowadzonej działalności, wielkość organizacji, jej powiązania oraz szczególne przesłanki określone w art. 5 ustawy KSC 2.0.

Pytania najlepiej analizować po kolei – od rodzaju prowadzonej działalności, przez wielkość organizacji i jej powiązania, aż po szczególne przesłanki określone w ustawie.

- ☑ Czy działalność organizacji znajduje się w sektorze lub podsektorze wskazanym w załączniku nr 1 lub 2 do ustawy KSC 2.0?
- ☑ Czy przeanalizowano faktycznie prowadzoną działalność i świadczone usługi?
- ☑ Czy zweryfikowano liczbę pracowników, roczny obrót i sumę bilansową?
- ☑ Czy uwzględniono przedsiębiorstwa partnerskie i powiązane?
- ☑ Czy przeanalizowano wszystkie istotne obszary działalności?
- ☑ Czy organizacja prowadzi działalność w więcej niż jednym sektorze objętym KSC 2.0?
- ☑ Czy występują szczególne kryteria, które mają zastosowanie niezależnie od wielkości organizacji?
- ☑ Czy na podstawie przeprowadzonej analizy można wstępnie określić status organizacji jako podmiotu kluczowego, podmiotu ważnego albo podmiotu pozostającego poza zakresem KSC 2.0?

→ WAŻNE

Wynik samoidentyfikacji ma istotne znaczenie praktyczne, ponieważ decyduje o obowiązku wpisu do Wykazu KSC. Podmioty, które **w dniu wejścia w życie nowelizacji ustawy, tj. 3 kwietnia 2026 r.**, spełniały określone w niej przesłanki, powinny złożyć wniosek o wpis do wykazu **do 3 października 2026 r.** Pozostałe podmioty mają na to **6 miesięcy od momentu spełnienia kryteriów określonych w ustawie.**

W przypadku istotnych zmian w działalności, wielkości organizacji lub jej powiązaniach z innymi podmiotami, kwalifikacja powinna zostać ponownie zweryfikowana.

Terminy dotyczące dalszych obowiązków, w tym wpisu do Wykazu KSC, zostały opisane w kolejnej części poradnika.

→ WARTO WIEDZIEĆ

Sama wielkość przedsiębiorstwa nie przesądza o objęciu przepisami KSC 2.0. Oprócz kryterium wielkości należy uwzględnić również rodzaj prowadzonej działalności, przynależność do sektorów wskazanych w załączniku nr 1 i załączniku nr 2 do ustawy oraz szczególne przypadki określone w art. 5 ustawy KSC 2.0. Chociaż regulacja obejmuje głównie średnie i duże podmioty prowadzące działalność w sektorach objętych ustawą, to w określonych przypadkach może dotyczyć również mniejszych organizacji.

Materiały uzupełniające

- Pełne zestawienie sektorów, podsektorów oraz rodzajów podmiotów objętych ustawą. Ministerstwo Cyfryzacji – Kogo obejmuje nowelizacja KSC 2.0?
- Praktyczny przewodnik dotyczący ustalania statusu podmiotu kluczowego lub ważnego. Ministerstwo Cyfryzacji – Jak dokonać samoidentyfikacji?

Wykaz podmiotów kluczowych i podmiotów ważnych (Wykaz KSC) i System S46

W ustawie KSC 2.0 pojawiają się dwa powiązane ze sobą rozwiązania – **Wykaz KSC oraz System S46**. Pełnią jednak różne funkcje. Wykaz KSC służy przede wszystkim identyfikacji podmiotów kluczowych i podmiotów ważnych, natomiast System S46 jest narzędziem teleinformatycznym wspierającym realizację obowiązków wynikających z ustawy.

Wykaz KSC – definicja i zasady wpisu

Wykaz KSC jest wykazem podmiotów kluczowych i podmiotów ważnych prowadzonym przez ministra właściwego do spraw informatyzacji (obecnie Ministra Cyfryzacji) na podstawie ustawy o krajowym systemie cyberbezpieczeństwa.

Wpis do Wykazu KSC stanowi jeden z podstawowych obowiązków podmiotów kluczowych i podmiotów ważnych objętych ustawą.

Wykaz KSC – do czego służy?

Identyfikacja podmiotów kluczowych i ważnych

Gromadzi informacje o podmiotach spełniających kryteria uznania za podmiot kluczowy lub ważny określone w ustawie.

Nadzór nad realizacją obowiązków

Umożliwia organom właściwym prowadzenie działań nadzorczych w zakresie cyberbezpieczeństwa.

Aktualizacja danych podmiotów

Zapewnia aktualność informacji w Wykazie KSC.

JAKIE SĄ ZASADY WPISU?

Istnieją dwie ścieżki wpisania podmiotu do wykazu.

→ **SAMOREJESTRACJA** (samodzielny wpis do wykazu) – kierownik podmiotu lub osoba przez niego upoważniona składa wniosek o wpis do Wykazu KSC – w terminie 6 miesięcy od spełnienia przesłanek uznania za podmiot kluczowy lub podmiot ważny.

→ **WPIS Z URZĘDU** (uzupełnienie danych po wezwaniu) – minister właściwy do spraw informatyzacji lub organ właściwy do spraw cyberbezpieczeństwa wpisuje podmiot do Wykazu KSC na podstawie danych pochodzących z rejestrów publicznych. Dotyczy to podmiotów publicznych, podmiotów krytycznych, przedsiębiorców telekomunikacyjnych oraz dostawców usług zaufania. Po dokonaniu wpisu podmiot otrzymuje zawiadomienie wraz z wezwaniem do uzupełnienia danych.

Zarówno wpisu do Wykazu KSC, jak i uzupełnienia danych dokonuje się za pośrednictwem strony: wykaz-ksc.gov.pl.

→ WARTO WIEDZIEĆ

Przed rozpoczęciem uzupełniania wpisu warto przygotować wszystkie wymagane informacje i dokumenty. Dzięki temu proces przebiegnie sprawnie i bez konieczności ponownego wypełniania formularza.

CO JEST POTRZEBNE DO WPISU DO WYKAZU KSC?

Przed rozpoczęciem wypełniania formularza warto przygotować następujące informacje:

- dane identyfikacyjne podmiotu – nazwę, NIP, REGON oraz dane adresowe;
- dane kontaktowe podmiotu – adres e-mail, numer telefonu, stronę internetową oraz adres do doręczeń elektronicznych, jeżeli dotyczy;
- dane osób odpowiedzialnych za kontakt z podmiotami KSC;
- pełnomocnictwo w postaci elektronicznej – jeżeli jest wymagane;
- informacje o działalności regulowanej i właściwych rejestrach, w których figuruje podmiot – jeśli dotyczy;
- informacje o sektorze, podsektorze i rodzaju działalności zgodnie z załącznikami do ustawy;
- zakresy publicznych adresów IP i domen internetowych;

- informacje o dostawcach usług zarządzanych w zakresie cyberbezpieczeństwa – jeżeli podmiot z nich korzysta;
- informacje o współpracy z innymi podmiotami w zakresie wymiany informacji o cyberbezpieczeństwie.

Podmioty posiadające już konto w Systemie S46 powinny dodatkowo przygotować:

- dane osoby pełniącej rolę administratora konta w Systemie S46;
- kod przestrzeni w S46 – jeżeli podmiot posiada już utworzoną przestrzeń w systemie.

Dane te potrzebne są przede wszystkim do Wykazu KSC. System S46 jest narzędziem wykorzystywanym do przekazywania tych informacji oraz do realizacji innych obowiązków wynikających z ustawy, w szczególności zgłaszania incydentów.

→ WAŻNE

Aktualizacja danych wymaga złożenia wniosku o zmianę danych w wykazie. Powinien być on składany przez osoby upoważnione do dokonania wpisu. Na aktualizacje danych przewidzianych jest 14 dni od dnia dokonania zmiany.

System S46 – definicja i zasady wpisu

§

CZYM JEST SYSTEM S46?

Zgodnie z art. 46 ustawy KSC 2.0 System S46 to system teleinformatyczny, który łączy podmioty objęte ustawą i wspiera współpracę między nimi. Służy do zgłaszania i obsługi incydentów, wymiany informacji o cyberzagrożeniach oraz współpracy między CSIRT-em, organami właściwymi i podmiotami.

A

CSIRT

Computer Security Incident Respond Team – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego jest podmiotem odpowiedzialnym za przyjmowanie zgłoszeń o incydentach, wspieranie organizacji podczas ich obsługi oraz koordynowanie działań służących ograniczaniu skutków incydentów. Zgłoszenia incydentów poważnych mogą być przekazywane do właściwego CSIRT-u za pośrednictwem Systemu S46. W krajowym systemie cyberbezpieczeństwa funkcjonują CSIRT-y poziomu krajowego (CSIRT GOV, CSIRT NASK oraz CSIRT MON) oraz CSIRT-y sektorowe, które realizują zadania związane z obsługą incydentów i wspierają podmioty w poszczególnych sektorach gospodarki.

Co umożliwia System S46?

Zgłaszanie incydentów zgłaszanie i obsługa incydentów	**Wymiana informacji** komunikacja między podmiotami, CSIRT-em i organami właściwymi	**Ostrzeganie o zagrożeniach** przekazywanie informacji o cyberzagrożeniach
Przekazywanie rekomendacji wsparcie podmiotów w zakresie cyberbezpieczeństwa	**Wsparcie nadzoru** wspieranie czynności nadzorczych	SYS 46 CYBER HUB

Wykaz KSC a System S46 – czym się różnią?

System S46 (S46 Cyber Hub), Wykaz KSC i portal cyber.gov.pl tworzą ekosystem usług wspierających informowanie i współpracę podmiotów w ramach KSC. Rozwiązania te zapewniają dostęp do wiedzy, usług cyfrowych oraz procesów związanych z realizacją zadań wynikających z krajowego systemu cyberbezpieczeństwa.

Cyber.gov.pl to ogólnodostępny rządowy portal łączący najważniejsze informacje, ostrzeżenia, poradniki i usługi z zakresu cyberbezpieczeństwa. Serwis jest skierowany do obywateli, przedsiębiorców i podmiotów KSC oraz zapewnia szybki dostęp do narzędzi takich jak System S46, moje.cert.pl i bezpiecznedane.gov.pl.

TABELA 3. Wykaz KSC a System S46 – podmioty podległe pod KSC 2.0

	Wykaz KSC	System S46
Czym jest?	Wykaz podmiotów kluczowych i podmiotów ważnych	System teleinformatyczny wspierający funkcjonowanie krajowego systemu cyberbezpieczeństwa
Główny cel	Ewidencja i dane kontaktowe podmiotów	Realizacja określonych obowiązków m.in. informowanie o incydentach i zagrożeniach, raportowanie, przekazywanie ostrzeżeń, rekomendacji
Do czego jest wykorzystywany?	Rejestracja i aktualizacja danych podmiotu	Współpraca, komunikacja podczas realizacji określonych obowiązków ustawowych

ŹRÓDŁO: Opracowanie własne NASK – PIB.

Wykaz KSC jest prowadzony z wykorzystaniem Systemu S46. System S46 ma jednak szersze zastosowanie – służy również m.in. do obsługi incydentów i wymiany informacji.

HARMONOGRAM NAJWAŻNIEJSZYCH TERMINÓW

Poza koniecznością realizacji nowych wymogów instytucje i organizacje powinny zwrócić szczególną uwagę na terminy wskazane w ustawie. Niedotrzymanie ustawowych terminów może skutkować sankcjami regulacyjnymi oraz finansowymi, dlatego rekomendowane jest odpowiednio wczesne przygotowanie i wdrożenie niezbędnych działań.

Harmonogram wdrożenia obowiązków KSC 2.0

Materiały uzupełniające

- Informacje o Wykazie podmiotów kluczowych i podmiotów ważnych oraz zasadach wpisu, oraz o Systemie S46
- Instrukcja Uzyskanie dostępu do Systemu oraz rozpoczęcie pracy z platformą
- Szkolenie e-learningowe Jak dokonać wpisu do Wykazu KSC? (wymaga zalogowania)

Obowiązki podmiotów

W tej części omówiono kluczowe obowiązki organizacji wynikające z ustawy KSC 2.0, obejmujące wymagania związane z zarządzaniem cyberbezpieczeństwem, organizacją procesów, personelem, dokumentacją oraz środkami technicznymi i organizacyjnymi służącymi zapewnieniu odporności na zagrożenia cybernetyczne.

Artykuł 8 ustawy KSC 2.0 nakłada na podmioty kluczowe i podmioty ważne obowiązek wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji (SZBI). SZBI to zbiór wzajemnie powiązanych zasad, procesów, procedur oraz środków organizacyjnych i technicznych, służących zapewnieniu odpowiedniego poziomu ochrony informacji w organizacji. Jego celem jest systematyczne zarządzanie ryzykiem oraz zapewnienie poufności, integralności i dostępności informacji poprzez planowanie, wdrażanie, monitorowanie i ciągłe doskonalenie działań związanych z bezpieczeństwem.

Na potrzeby poradnika obowiązki wynikające z ustawy zostały pogrupowane w 7 kategorii odpowiadających najważniejszym obszarom funkcjonowania organizacji. Obejmują one:

- Zarządzanie cyberbezpieczeństwem;
- Budowanie świadomości i zarządzanie wiedzą;
- Ochronę systemów i informacji;
- Cyberbezpieczeństwo dostawców i usług zewnętrznych;
- Reagowanie i odporność organizacji;
- Zgłaszanie incydentów;
- Nadzór i doskonalenie działania systemu zarządzania bezpieczeństwem informacji.

Dla podmiotów ważnych będących podmiotami publicznymi przedstawiono również uproszczone wymagania dotyczące SZBI wynikające z Załącznika nr 4 do ustawy.

W przypadku niektórych podmiotów wymagania dotyczące SZBI zostały doprecyzowane w rozporządzeniu Komisji (UE) 2024/2690. Obejmuje ono m.in. dostawców usług DNS, usług zarządzanych (i zarządzanych w zakresie cyberbezpieczeństwa), internetowych platform handlowych, usług zaufania oraz inne kategorie podmiotów wskazane w rozporządzeniu.

Warto pamiętać, że dla części podmiotów Rada Ministrów może wprowadzić odrębne wymagania dotyczące SZBI. Dlatego należy na bieżąco monitorować zmiany przepisów w tym zakresie.

TABELA 4. Zestawienie wymagań wynikających z ustawy KSC 2.0 według obszarów tematycznych wraz z odniesieniem do właściwych przepisów.

Kategorie	Obszar	Odniesienie do ustawy
Zarządzanie cyberbezpieczeństwem		
	Zarządzanie aktywami	art. 8 ust. 1 pkt 2 lit. m
	Systematyczne szacowanie i zarządzanie ryzykiem	art. 8 ust 1 pkt. 1
	Polityki szacowania ryzyka oraz bezpieczeństwa systemu informacyjnego	art. 8 ust. 1 pkt 2 lit. a
	Określenie kompetencji, uprawnień i zakresu odpowiedzialności personelu	art. 8 ust. 1 pkt 2 lit. d
	Zarządzanie ciągłością działania	art. 8 ust. 1 pkt 2 lit. f
Budowanie świadomości i zarządzanie wiedzą		
	Podstawowe zasady cyberhigieny	art. 8 ust. 1 pkt 2 lit. j
	Edukacja z zakresu cyberbezpieczeństwa dla personelu podmiotu	art. 8 ust. 1 pkt 2 lit. i
Ochrona systemów i informacji		
	Bezpieczeństwo w procesie nabywania, rozwoju, utrzymania i eksploatacji systemów informacyjnych, w tym testowanie	art. 8 ust. 1 pkt 2 lit. b
	Bezpieczeństwo fizyczne i środowiskowe	art. 8 ust. 1 pkt 2 lit. c
	Polityki i procedury stosowania kryptografii, w tym szyfrowania	art. 8 ust. 1 pkt 2 lit. k
	Bezpieczne środki komunikacji elektronicznej, w tym MFA	art. 8 ust. 1 pkt 2 lit. l
	Polityki kontroli dostępu	art. 8 ust. 1 pkt 2 lit. n
	Ochrona informacji i danych	art. 8 ust. 1 pkt 5 lit. a
	Zarządzanie aktualizacjami	art. 8 ust. 1 pkt 5 lit. b
	Integralność i ochrona systemów	art. 8 ust. 1 pkt 5 lit. c
Bezpieczeństwo dostawców i usług zewnętrznych		
	Bezpieczeństwo i ciągłość łańcucha dostaw produktów, usług i procesów ICT	art. 8 ust. 1 pkt 2 lit. e
	Ocena ryzyka dostawców i usług ICT	art. 8 ust. 2 pkt 1
	Jakość produktów usług i procesów	art. 8 ust. 2 pkt 2
	Monitorowanie i nadzór nad dostawcami	art. 8 ust. 2 pkt 3
	Zarządzanie zależnościami od dostawców ICT, w tym uwzględnianie dostawców wysokiego ryzyka	art. 8 ust. 2 pkt 4

Kategorie	Obszar	Odniesienie do ustawy
Reagowanie i odporność organizacji		
	Ciągłość działania i odtwarzanie po awarii	art. 8 ust. 1 pkt 2 lit. f
	Monitorowanie systemów	art. 8 ust. 1 pkt 2 lit. g
	Zbieranie informacji o cyberzagrożeniach i podatnościach	art. 8 ust. 1 pkt 3
	Zarządzanie incydentami	art. 8 ust. 1 pkt 4, art. 8 ust. 1 pkt 5 lit. d
Zgłaszanie incydentów		
	Zgłaszanie incydentów do CSIRT-u sektorowego	art. 11 ust. 1 pkt 4, 4a, 4b, 4c, art. 46 ust. 1, art. 12
	Współpraca z CSIRT-em	art. 11 ust. 1 pkt 2 oraz pkt 5
	Raportowanie	art. 11 ust. 1 pkt 4b i 4c, art. 12a, art. 12b
	Wyjątki dla podmiotów ważnych będących podmiotami publicznymi	art. 12c
Nadzór i doskonalenie		
	Ocena skuteczności środków	art. 8 ust. 1 pkt 2 lit. h
	Wyznaczenie i utrzymywanie osób kontaktowych ds. cyberbezpieczeństwa	art .9
	Audyty bezpieczeństwa dla podmiotów kluczowych	art. 15 ust. 1

ŹRÓDŁO: Opracowanie własne NASK – PIB.

W celu ułatwienia interpretacji i praktycznego wdrażania wymagań ustawy każdy z siedmiu obszarów został przedstawiony z czterech perspektyw: decyzji i odpowiedzialności, zasad i procedur, systemów i bezpieczeństwa technicznego oraz usług, ludzi i codziennej działalności. Przedstawione w poradniku przykłady pytań kontrolnych, działań, dokumentów i dobrych praktyk mają charakter pomocniczy i nie są zamkniętym katalogiem wymagań. Ich zakres powinien być dostosowany do charakteru działalności organizacji, wykorzystywanych systemów oraz poziomu ryzyka.

TABELA 5. Obowiązki wynikające z ustawy KSC 2.0 – wybrane aspekty.

Perspektywa	Na co zwrócić uwagę	Najczęściej zaangażowane role i zespoły
Decyzje i odpowiedzialność	Jakie decyzje należy podjąć i kto za nie odpowiada?	Zarząd, kierownictwo, osoby decyzyjne.
Zasady i procedury	Jakie reguły powinny obowiązywać w organizacji?	Dział prawny, IOD, compliance, zarządzanie ryzykiem, audyt.
Systemy i bezpieczeństwo techniczne	Jakie działania dotyczą systemów, infrastruktury i bezpieczeństwa?	Zespół IT, bezpieczeństwa/ cyberbezpieczeństwa.
Usługi, ludzie i codzienna działalność	Jak wymagania wpływają na codzienną pracę organizacji?	Zespół zakupów, kadr, ciągłości działania, szkoleń itp.

ŹRÓDŁO: Opracowanie własne NASK – PIB.

Zarządzanie cyberbezpieczeństwem

Artykuł 8 ustawy KSC 2.0 określa **obowiązek wdrożenia systemu zarządzania bezpieczeństwem informacji (SZBI)** oraz wskazuje szereg działań, które organizacja powinna realizować.

Zarządzanie cyberbezpieczeństwem stanowi fundament działań związanych z ochroną systemów, informacji i usług oraz zapewnia spójne podejście do bezpieczeństwa w całej organizacji.

Czego wymaga ustawa?

Ustawa wymaga, aby podmioty kluczowe i podmioty ważne zarządzały cyberbezpieczeństwem w sposób systematyczny, udokumentowany i oparty na analizie ryzyka. Oznacza to konieczność identyfikacji aktywów wymagających ochrony, oceny ryzyka, określenia zasad bezpieczeństwa informacji, przypisania odpowiedzialności oraz zapewnienia nadzoru nad działaniami związanymi z cyberbezpieczeństwem.

TABELA 6. Zarządzanie cyberbezpieczeństwem – wybrane aspekty wraz z odniesieniem do właściwych przepisów.

Kategoria	Obszar	Odniesienie do ustawy
Zarządzanie cyberbezpieczeństwem		
	Zarządzanie aktywami	art. 8 ust. 1 pkt 2 lit. m
	Systematyczne szacowanie i zarządzanie ryzykiem	art. 8 ust 1 pkt. 1
	Polityki szacowania ryzyka oraz bezpieczeństwa systemu informacyjnego	art. 8 ust. 1 pkt 2 lit. a
	Określenie kompetencji, uprawnień i zakresu odpowiedzialności personelu	art. 8 ust. 1 pkt 2 lit. d
	Zarządzanie ciągłością działania	art. 8 ust. 1 pkt 2 lit. f

ŹRÓDŁO: Opracowanie własne NASK – PIB.

Co to oznacza w praktyce?

Aby skutecznie chronić organizację, nie wystarczy pozostawić cyberbezpieczeństwa specjalistom IT. **Konieczne jest zaangażowanie kierownictwa**, które wyznacza kierunek działań, określa priorytety, przydziela odpowiedzialność i nadzoruje zarządzanie ryzykiem.

§

W praktyce oznacza to zwrócenie uwagi na kilka kluczowych obszarów, które stanowią fundament zarządzania cyberbezpieczeństwem:

→ **Ustalenie, co wymaga ochrony** (art. 8 ust. 1 pkt 2 lit. m)

Punktem wyjścia powinna być **inwentaryzacja** aktywów wykorzystywanych w organizacji. Należy ustalić, jakie dane, systemy, urządzenia, oprogramowanie i usługi są wykorzystywane w działalności organizacji oraz określić osoby odpowiedzialne za poszczególne zasoby. Warto prowadzić rejestr zasobów, który ułatwi ocenę ryzyka, planowanie zabezpieczeń i dalsze działania związane z cyberbezpieczeństwem. Bez wiedzy o tym, jakie zasoby posiada organizacja, trudno właściwie ocenić ryzyko i zaplanować skuteczne działania zabezpieczające.

→ **Ocena, przed czym należy się chronić** (art. 8 ust. 1 pkt 1)

Należy rozpoznać możliwe zagrożenia i ocenić ich wpływ na działalność organizacji. Warto przeanalizować, jak realne jest wystąpienie danego zdarzenia oraz jakie może ono spowodować skutki np. przestój w działalności, utratę danych, straty finansowe, odpowiedzialność prawną czy utratę zaufania klientów. Pozwala to określić, które ryzyka są najistotniejsze i wymagają podjęcia działań w pierwszej kolejności.

- **Określenie kompetencji, uprawnień i zakresu odpowiedzialności personelu** (art. 8 ust. 1 pkt 2 lit. d)

  Należy jasno określić role, zakres odpowiedzialności i uprawnienia osób uczestniczących w realizacji działań związanych z cyberbezpieczeństwem. Organizacja powinna zapewnić, aby pracownicy i współpracownicy mieli kompetencje adekwatne do wykonywanych zadań, byli świadomi swoich obowiązków oraz posiadali dostęp wyłącznie do zasobów niezbędnych do ich realizacji. Istotne jest również regularne przeglądanie uprawnień oraz dostosowywanie ich do zmian organizacyjnych, kadrowych i zakresu wykonywanych obowiązków.

- **Określenie zasad bezpieczeństwa** (art. 8 ust. 1 pkt 2 lit. a)

  Wyniki inwentaryzacji zasobów, oceny ryzyka oraz przypisania odpowiedzialności powinny znaleźć odzwierciedlenie w politykach i procedurach bezpieczeństwa. Dokumentacja ta porządkuje sposób zarządzania cyberbezpieczeństwem i określa zasady postępowania obowiązujące w organizacji, w tym działania na wypadek awarii, incydentów oraz zakłóceń mogących wpływać na ciągłość działania. Dzięki temu organizacja wie nie tylko jak zapobiegać zagrożeniom, ale również jak reagować, gdy do nich dojdzie.

- **Regularne sprawdzanie skuteczności** (art. 8 ust. 1 pkt 1 oraz pkt 2 lit. f)

  Samo wdrożenie zabezpieczeń nie kończy procesu. Cyberbezpieczeństwo wymaga systematycznych działań. Organizacja powinna regularnie sprawdzać, czy stosowane zabezpieczenia rzeczywiście działają, analizować incydenty i wykryte słabości oraz na bieżąco aktualizować ocenę ryzyka. Dzięki temu może dostosowywać swoje działania do zmian zachodzących w organizacji oraz nowych zagrożeń pojawiających się w otoczeniu.

Jak sprawdzić, czy organizacja spełnia ten obowiązek?

Zarządzanie cyberbezpieczeństwem stanowi fundament systemu zarządzania bezpieczeństwem informacji i obejmuje działania związane z identyfikacją ryzyka, organizacją odpowiedzialności oraz nadzorem nad stosowanymi zabezpieczeniami.

TABELA 7. Zarządzanie cyberbezpieczeństwem – wybrane aspekty.

Perspektywa	Co należy sprawdzić	Konsekwencje zaniedbania
Decyzje i odpowiedzialność	• Czy prowadzony jest aktualny rejestr aktywów oraz ich właścicieli? • Czy zidentyfikowano aktywa kluczowe dla realizacji procesów i świadczenia usług? • Czy określono poziom ryzyka akceptowalny dla organizacji? • Czy wyniki analizy ryzyka są uwzględniane przy podejmowaniu decyzji dotyczących bezpieczeństwa? • Czy ryzyko jest regularnie oceniane i aktualizowane? • Czy określono osoby odpowiedzialne za realizację działań związanych z cyberbezpieczeństwem? • Czy kierownictwo uczestniczy w przeglądzie najważniejszych ryzyk?	• Brak wiedzy o kluczowych zasobach organizacji. • Pominięcie istotnych zagrożeń. • Koncentracja działań na mniej istotnych ryzykach. • Opóźnione lub niespójne decyzje. • Niejasny podział odpowiedzialności.
Zasady, procedury i dokumentacja	• Czy wdrożono polityki bezpieczeństwa informacji oraz zarządzania ryzykiem? • Czy określono zasady i procedury postępowania w obszarze cyberbezpieczeństwa? • Czy opracowano plany ciągłości działania i odtwarzania po awarii? • Czy pracownicy znają i stosują obowiązujące zasady oraz procedury? • Czy określono sposób oceny skuteczności zabezpieczeń? • Czy dokumentacja jest regularnie aktualizowana?	• Niejednolite zasady postępowania w organizacji. • Trudności podczas audytów i kontroli. • Brak przygotowania na sytuacje kryzysowe. • Stosowanie nieaktualnych lub nieskutecznych zabezpieczeń i procedur.
Systemy i bezpieczeństwo techniczne	• Czy stosowane zabezpieczenia odpowiadają zidentyfikowanym ryzykom? • Czy uwzględniono cały cykl życia systemów i urządzeń, od wdrożenia po wycofanie z użytkowania? • Czy określono wymagania bezpieczeństwa dla wykorzystywanych systemów i urządzeń? • Czy oceniana jest skuteczność środków technicznych?	• Nieskuteczne lub źle dobrane zabezpieczenia. • Korzystanie z przestarzałych lub niewspieranych systemów i urządzeń. • Występowanie luk i podatności bezpieczeństwa. • Zwiększone ryzyko incydentów i awarii.

Perspektywa	Co należy sprawdzić	Konsekwencje zaniedbania
Usługi, ludzie i codzienna działalność	• Czy zasady cyberbezpieczeństwa są stosowane w codziennej pracy? • Czy wymagania bezpieczeństwa są uwzględniane przy realizacji usług i wprowadzaniu zmian? • Czy pracownicy są świadomi swoich obowiązków związanych z cyberbezpieczeństwem?	• Błędy w codziennej pracy zwiększające ryzyko incydentów. • Zakłócenia realizacji zadań i świadczenia usług. • Wprowadzanie zmian powodujących nowe zagrożenia lub niezgodności.

ŹRÓDŁO: Opracowanie własne NASK – PIB

Działania wspierające realizację wymagań ustawowych

- Regularne identyfikowanie i aktualizowanie ryzyk związanych z cyberbezpieczeństwem;
- Monitorowanie poziomu ryzyka oraz jego zgodności z przyjętymi kryteriami akceptacji;
- Wykorzystywanie wyników analizy ryzyka przy wyborze i doskonaleniu zabezpieczeń;
- Omawianie najważniejszych ryzyk i incydentów na poziomie kierownictwa;
- Aktualizowanie informacji o zasobach wykorzystywanych przez organizację;
- Uwzględnianie cyberbezpieczeństwa przy planowaniu nowych usług i rozwiązań;
- Aktualizowanie ocen ryzyka po istotnych zmianach, incydentach lub pojawieniu się nowych zagrożeń;
- Sprawdzanie gotowości organizacji do działania w sytuacjach awaryjnych oraz wyciąganie wniosków z przeprowadzonych testów.

Najczęstsze błędy i pułapki

- Traktowanie analizy ryzyka jako jednorazowego działania zamiast regularnego procesu;
- Niewystarczające zaangażowanie kadry kierowniczej w obszar cyberbezpieczeństwa;
- Pozostawienie kwestii cyberbezpieczeństwa wyłącznie specjalistom IT;

- Brak aktualnej wiedzy o wykorzystywanych systemach, usługach i danych;
- Niejasny podział ról i odpowiedzialności w obszarze cyberbezpieczeństwa;
- Zapominanie o aktualizacji procedur po zmianach w organizacji, technologii lub przepisach;
- Opracowanie planów awaryjnych, które nigdy nie zostały sprawdzone w praktyce.

Materiały uzupełniające

- Poradnik NASK Firma Bezpieczna Cyfrowo.

Budowanie świadomości cyberbezpieczeństwa i zarządzanie wiedzą

Człowiek pozostaje jednym z najważniejszych elementów cyberbezpieczeństwa. Dlatego ustawa podkreśla znaczenie edukacji personelu, rozwijania kompetencji oraz budowania kultury cyberbezpieczeństwa w całej organizacji.

Czego wymaga ustawa?

Ustawa wymaga budowania świadomości cyberbezpieczeństwa w organizacji poprzez edukację personelu oraz stosowanie podstawowych zasad cyberhigieny. Oznacza to, że pracownicy powinni znać najczęstsze cyberzagrożenia, potrafić rozpoznawać podejrzane sytuacje i wiedzieć, jak bezpiecznie korzystać z systemów informatycznych. Działania te powinny być prowadzone regularnie i stanowić stały element funkcjonowania organizacji, a nie ograniczać się do jednorazowych szkoleń.

TABELA 8. Budowanie świadomości cyberbezpieczeństwa i zarządzanie wiedzą – wybrane aspekty wraz z odniesieniem do właściwych przepisów.

Kategoria	Obszar	Odniesienie do ustawy
Budowanie świadomości i zarządzanie wiedzą		
	Podstawowe zasady cyberhigieny	art. 8 ust. 1 pkt 2 lit. j
	Edukacja z zakresu cyberbezpieczeństwa dla personelu podmiotu	art. 8 ust. 1 pkt 2 lit. i

ŹRÓDŁO: Opracowanie własne NASK – PIB.

Co to oznacza w praktyce?

Budowanie świadomości cyberbezpieczeństwa powinno być realizowane jako ciągły proces, a nie jednorazowe działanie. Program edukacyjny należy regularnie dostosowywać do ról, obowiązków oraz poziomu ryzyka poszczególnych grup pracowników, tak aby wspierać ich przygotowanie do aktualnych zagrożeń i wyzwań związanych z cyberbezpieczeństwem.

W praktyce mogą to być m.in.:

- szkolenia wstępne i okresowe, dostosowane do roli, zakresu obowiązków i poziomu uprawnień użytkowników,
- krótkie komunikaty o aktualnych zagrożeniach,
- kampanie i materiały edukacyjne,
- ćwiczenia praktyczne i symulacje phishingu,
- przypominanie zasad zgłaszania incydentów,
- testy wiedzy i sprawdzanie skuteczności działań.

Nawet dobre zabezpieczenia techniczne nie wystarczą, jeśli pracownicy nie potrafią rozpoznać zagrożenia lub nie wiedzą, jak na nie zareagować. Phishing i inne formy oszustw opartych na socjotechnice wykorzystują przede wszystkim zachowania użytkowników. Świadomy pracownik może rozpoznać próbę ataku, szybko ją zgłosić i ograniczyć jej skutki.

Edukacja pomaga też przełożyć procedury i zabezpieczenia na codzienną praktykę. Nie wystarczy bowiem wdrożyć uwierzytelnianie wieloskładnikowe czy procedurę zgłaszania incydentów – personel musi wiedzieć, jak z nich prawidłowo korzystać.

Dlatego edukacja i cyberhigiena są ważnym elementem zarządzania ryzykiem i budowania odporności organizacji.

Jak sprawdzić, czy organizacja spełnia ten obowiązek?

W praktyce skuteczny program budowania świadomości cyberbezpieczeństwa obejmuje planowanie, realizację oraz ocenę działań edukacyjnych, z uwzględnieniem różnych grup odbiorców, aktualnych zagrożeń i potrzeb organizacji.

TABELA 9. Budowanie świadomości cyberbezpieczeństwa – wybrane aspekty.

Perspektywa	Co należy sprawdzić	Konsekwencje zaniedbania
Decyzje i odpowiedzialność	• Czy wyznaczono osoby odpowiedzialne za działania edukacyjne i budowanie świadomości cyberbezpieczeństwa? • Czy zapewniono odpowiednie zasoby na realizację działań edukacyjnych? • Czy kwestie związane z cyberbezpieczeństwem są regularnie omawiane na poziomie kierownictwa? • Czy wnioski z ćwiczeń i testów są wykorzystywane do planowania kolejnych działań edukacyjnych?	• Brak spójnego podejścia do budowania świadomości cyberbezpieczeństwa. • Niski poziom zaangażowania pracowników. • Większa podatność organizacji na błędy ludzkie. • Niska skuteczność działań edukacyjnych.
Zasady, procedury i dokumentacja	• Czy określono zasady cyberhigieny obowiązujące w organizacji? • Czy istnieje plan lub program działań edukacyjnych? • Czy prowadzone są rejestry szkoleń i innych działań edukacyjnych? • Czy oceniana jest skuteczność prowadzonych działań edukacyjnych?	• Brak systematycznego podejścia do edukacji personelu. • Luki w wiedzy i świadomości pracowników. • Trudności w wykazaniu realizacji wymagań ustawowych.
Systemy i bezpieczeństwo techniczne	• Czy pracownicy są regularnie informowani o nowych zagrożeniach i sposobach ochrony? • Czy prowadzone są ćwiczenia lub symulacje związane z cyberbezpieczeństwem? • Czy analizowane są wyniki tych działań?	• Wiedza pracowników pozostaje wyłącznie teoretyczna. • Trudności z rozpoznawaniem rzeczywistych zagrożeń. • Nieprawidłowe reakcje na incydenty i sytuacje kryzysowe.
Usługi, ludzie i codzienna działalność	• Czy wszyscy pracownicy są objęci działaniami edukacyjnymi? • Czy nowe osoby przechodzą szkolenia z zakresu cyberbezpieczeństwa? • Czy zakres edukacji jest dostosowany do pełnionych ról i obowiązków? • Czy personel zna sposób zgłaszania incydentów i zagrożeń? • Czy pracownicy stosują zasady cyberhigieny w codziennej pracy?	• Zwiększone ryzyko incydentów wynikających z błędów użytkowników. • Nieprawidłowe reagowanie na zagrożenia i incydenty. • Spadek skuteczności wdrożonych zabezpieczeń. • Wzrost ryzyka naruszenia bezpieczeństwa informacji.

ŹRÓDŁO: Opracowanie własne NASK – PIB.

Działania wspierające realizację wymagań ustawowych

- Prowadzenie regularnych działań edukacyjnych dostosowanych do potrzeb organizacji;
- Dostosowywanie zakresu edukacji do roli pracownika, zakresu jego obowiązków, poziomu posiadanych uprawnień oraz ryzyka związanego z wykonywanymi zadaniami;
- Informowanie pracowników o aktualnych zagrożeniach, nowych metodach ataków oraz zasadach bezpiecznego postępowania;
- Rozwijanie umiejętności rozpoznawania zagrożeń oraz zgłaszania incydentów;
- Wykorzystywanie ćwiczeń, testów oraz analizy przypadków do utrwalania wiedzy oraz doskonalenia praktycznych umiejętności z zakresu budowania świadomości cyberbezpieczeństwa.

Najczęstsze błędy i pułapki

- Traktowanie edukacji i budowania świadomości jako jednorazowego działania;
- Ograniczanie działań wyłącznie do szkoleń e-learningowych;
- Przekazywanie tych samych treści wszystkim pracownikom, bez uwzględnienia ich roli i zakresu obowiązków;
- Skupianie się wyłącznie na teorii, bez ćwiczeń i praktycznych przykładów;
- Pomijanie informacji o nowych zagrożeniach i aktualnych metodach ataków;
- Brak weryfikacji, czy pracownicy potrafią wykorzystać zdobytą wiedzę w praktyce;
- Ocenianie skuteczności działań wyłącznie na podstawie frekwencji lub ukończenia szkolenia;
- Pomijanie kierownictwa w działaniach związanych z budowaniem świadomości;
- Traktowanie cyberbezpieczeństwa jako zadania wyłącznie działu IT lub zespołu bezpieczeństwa.

Ochrona systemów i informacji

Czego wymaga ustawa?

Ustawa wymaga zapewnienia odpowiedniego poziomu ochrony systemów, urządzeń, informacji i danych wykorzystywanych do świadczenia usług. Obejmuje to bezpieczeństwo systemów na każdym etapie ich funkcjonowania, kontrolę dostępu do zasobów, ochronę informacji przed utratą lub nieuprawnionym ujawnieniem oraz stosowanie rozwiązań gwarantujących poufność, integralność i dostępność danych.

TABELA 10. Ochrona systemów i informacji – wybrane aspekty wraz z odniesieniem do właściwych przepisów.

Kategoria	Obszar	Odniesienie do ustawy
Ochrona systemów i informacji		
	Bezpieczeństwo w procesie nabywania, rozwoju, utrzymania i eksploatacji systemów informacyjnych, w tym testowanie	art. 8 ust. 1 pkt 2 lit. b
	Bezpieczeństwo fizyczne i środowiskowe	art. 8 ust. 1 pkt 2 lit. c
	Polityki i procedury stosowania kryptografii, w tym szyfrowania	art. 8 ust. 1 pkt 2 lit. k
	Bezpieczne środki komunikacji elektronicznej, w tym MFA	art. 8 ust. 1 pkt 2 lit. l
	Polityki kontroli dostępu	art. 8 ust. 1 pkt 2 lit. n
	Ochrona informacji i danych	art. 8 ust. 1 pkt 5 lit. a
	Zarządzanie aktualizacjami	art. 8 ust. 1 pkt 5 lit. b
	Integralność i ochrona systemów	art. 8 ust. 1 pkt 5 lit. c

ŹRÓDŁO: Opracowanie własne NASK – PIB.

§

Co to oznacza w praktyce?

→ **Bezpieczeństwo systemów przez cały cykl życia**
(art. 8 ust. 1 pkt 2 lit. b oraz lit. m)

Wymagania bezpieczeństwa powinny być uwzględniane na każdym etapie życia systemu: od zakupu lub projektowania, przez wdrożenie, utrzymanie, rozwój i testowanie, aż po jego wycofanie z użytkowania. Oznacza to m.in. uwzględnianie bezpieczeństwa przy wyborze nowych rozwiązań, zarządzaniu zmianami oraz bezpiecznym usuwaniu danych i urządzeń. Wymaga to również utrzymywania aktualnych informacji o wykorzystywanych systemach, urządzeniach i oprogramowaniu oraz planowania ich utrzymania,

rozwoju i wycofania z użytkowania. Niezbędne jest także regularne aktualizowanie systemów, urządzeń i oprogramowania w celu usuwania znanych podatności i utrzymania odpowiedniego poziomu bezpieczeństwa.

→ **Ochrona infrastruktury, urządzeń i środowiska** (art. 8 ust. 1 pkt 2 lit. c)

Bezpieczeństwo informacji zależy nie tylko od systemów informatycznych. Znaczenie mają również urządzenia, pomieszczenia oraz infrastruktura wykorzystywana do świadczenia usług. Warto uwzględnić zagrożenia, takie jak kradzież sprzętu, nieuprawniony dostęp do pomieszczeń, awarie zasilania, pożar, zalanie lub inne zdarzenia mogące zakłócić funkcjonowanie organizacji.

→ **Szyfrowanie i ochrona informacji** (art. 8 ust. 1 pkt 2 lit. k)

Mechanizmy kryptograficzne, w tym szyfrowanie, powinny być stosowane zgodnie z poziomem ryzyka i rodzajem przetwarzanych informacji. Dotyczy to m.in. danych przechowywanych na laptopach, urządzeniach mobilnych i nośnikach zewnętrznych, a także informacji przesyłanych pocztą elektroniczną. Poziom zabezpieczeń kryptograficznych powinien być dostosowany do wartości chronionych informacji oraz skutków ich ewentualnego ujawnienia lub utraty.

→ **Bezpieczna komunikacja i uwierzytelnianie** (art. 8 ust. 1 pkt 2 lit. l)

Wymiana informacji wymaga korzystania z bezpiecznych kanałów komunikacji oraz rozwiązań ograniczających ryzyko nieuprawnionego dostępu. Bezpieczeństwo poczty elektronicznej wymaga stosowania mechanizmów SPF, DKIM i DMARC, które umożliwiają weryfikację autentyczności wiadomości i ograniczają ryzyko podszywania się pod domenę organizacji. Ich brak może ułatwiać prowadzenie kampanii phishingowych oraz wykorzystywanie nazwy organizacji do działań oszukańczych.

Istotną rolę odgrywa uwierzytelnianie wieloskładnikowe (MFA), które oprócz hasła wymaga dodatkowego potwierdzenia tożsamości, np. kodem z aplikacji mobilnej lub kluczem sprzętowym. Jest to szczególnie ważne przy ochronie poczty elektronicznej, usług chmurowych, połączeń VPN, usług zdalnego pulpitu (RDP) oraz kont administracyjnych. Dzięki temu przejęcie samego hasła nie wystarcza do uzyskania dostępu do systemu.

→ **Kontrola dostępu do systemów i danych** (art. 8 ust. 1 pkt 2 lit. n)

Dostęp do informacji i systemów powinien być ograniczony do osób, które rzeczywiście potrzebują go do wykonywania swoich obowiązków. Zakres uprawnień warto dopasowywać do pełnionej roli, regularnie go weryfikować oraz aktualizować przy zmianie stanowiska lub zakończeniu współpracy. Dobrą praktyką jest także ograniczanie korzystania z kont administracyjnych i stosowanie zasady minimalnych uprawnień.

→ **Ochrona informacji i danych** (art. 8 ust. 1 pkt 5 lit. a)

Ochrona informacji obejmuje nie tylko zabezpieczenia techniczne, ale również sposób zarządzania danymi w organizacji. W praktyce oznacza to:

- klasyfikację informacji według ich znaczenia i wrażliwości,
- określenie zasad przechowywania i udostępniania danych,
- wykonywanie i zabezpieczanie kopii zapasowych,
- monitorowanie dostępu do informacji,
- bezpieczne usuwanie danych i nośników informacji,
- stosowanie zasad ochrony danych przez cały okres ich przetwarzania.

Działania te pomagają ograniczyć ryzyko utraty informacji, wycieku danych oraz ich nieuprawnionego wykorzystania. Ich celem jest również zapewnienie, aby dane były dostępne dla uprawnionych osób wtedy, kiedy są potrzebne, nie były modyfikowane w sposób nieuprawniony oraz aby możliwe było potwierdzenie ich pochodzenia i autentyczności.

→ **Zarządzanie aktualizacjami** (art. 8 ust. 1 pkt 5 lit. b)

Regularne aktualizowanie systemów, aplikacji i urządzeń pomaga usuwać znane luki w zabezpieczeniach i ograniczać ryzyko cyberataków. Istotne jest również monitorowanie, czy wykorzystywane rozwiązania są nadal wspierane przez producenta i otrzymują niezbędne aktualizacje.

→ **Integralność i ochrona systemów** (art. 8 ust. 1 pkt 5 lit. c)

Integralność systemów oznacza pewność, że dane i konfiguracje nie zostaną zmienione przez osoby nieuprawnione ani uszkodzone w wyniku błędu, awarii lub ataku. Osiągnięcie tego celu wymaga połączenia wielu działań: kontroli dostępu, ochrony informacji, stosowania szyfrowania, bezpiecznej komunikacji oraz właściwego zabezpieczenia urządzeń i infrastruktury. Dodatkowym mechanizmem ograniczającym skutki incydentów jest segmentacja sieci, polegająca na oddzielaniu od siebie systemów i usług o różnym poziomie krytyczności. Ich wspólnym celem jest utrzymanie stabilnego i bezpiecznego działania systemów wykorzystywanych do świadczenia usług.

Jak sprawdzić, czy organizacja spełnia ten obowiązek?

Skuteczna ochrona systemów i informacji opiera się na połączeniu działań organizacyjnych, procesowych, technicznych i dokumentacyjnych, dostosowanych do specyfiki organizacji oraz poziomu ryzyka.

TABELA 11. Ochrona systemów i informacji – wybrane aspekty.

Perspektywa	Co należy sprawdzić	Konsekwencje zaniedbania
Decyzje i odpowiedzialność	• Czy określono, kto odpowiada za podejmowanie decyzji dotyczących ochrony systemów i informacji? • Czy określono, kto zatwierdza odstępstwa od wymagań bezpieczeństwa?	• Dopuszczenie do użytkowania rozwiązań o podwyższonym poziomie ryzyka. • Niekontrolowane odstępstwa od przyjętych zasad bezpieczeństwa. • Brak jednoznacznej odpowiedzialności za ochronę kluczowych zasobów.
Zasady, procedury i dokumentacja	• Czy określono wymagania bezpieczeństwa dla nowych systemów i usług przed ich wdrożeniem? • Czy opisano sposób postępowania z informacjami o różnym poziomie wrażliwości? • Czy opisano wymagania dotyczące szyfrowania informacji i bezpiecznej komunikacji? • Czy organizacja posiada jasno określone zasady obsługi incydentów, współpracy z właściwym CSIRT-em oraz realizacji obowiązków z wykorzystaniem Systemu S46?	• Niejednolite zasady ochrony informacji. • Niewłaściwe postępowanie z informacjami o podwyższonej wrażliwości. • Chaos organizacyjny podczas incydentu. • Ryzyko niewypełnienia obowiązków ustawowych. • Utrudniona współpraca z właściwym CSIRT-em.
Systemy i bezpieczeństwo techniczne	• Czy zabezpieczenia opisane w dokumentacji zostały faktycznie wdrożone? • Czy podatności bezpieczeństwa są regularnie identyfikowane i usuwane? • Czy systemy wymuszają stosowanie mechanizmów bezpieczeństwa, takich jak MFA, szyfrowanie czy polityki haseł? • Czy systemy, urządzenia i oprogramowanie są regularnie aktualizowane, a niewspierane rozwiązania wycofywane z użytkowania? • Czy zapewniono ochronę przed zagrożeniami fizycznymi i środowiskowymi, takimi jak pożar, zalanie czy awarie zasilania?	• Nieskuteczne lub niewdrożone zabezpieczenia. • Luki i podatności bezpieczeństwa. • Nieuprawniony dostęp do systemów i danych. • Korzystanie z przestarzałych lub niewspieranych systemów i urządzeń. • Zakłócenia działania systemów spowodowane awariami lub zdarzeniami środowiskowymi.

Perspektywa	Co należy sprawdzić	Konsekwencje zaniedbania
Usługi, ludzie i codzienna działalność	• Czy każdy użytkownik korzysta z indywidualnego konta z zakresem uprawnień dostosowanym do wykonywanych obowiązków? • Czy pracownicy korzystają wyłącznie ze sprzętu służbowego lub urządzeń dopuszczonych do pracy zgodnie z zasadami organizacji? • Czy użytkownicy stosują wymagane mechanizmy bezpieczeństwa podczas codziennej pracy? • Czy pracownicy korzystają z wyłącznie zatwierdzonego oprogramowania? • Czy urządzenia mobilne używane do pracy są odpowiednio zabezpieczone?	• Korzystanie ze współdzielonych kont. • Nadmierne uprawnienia użytkowników. • Niekontrolowane kopiowanie lub przenoszenie danych. • Ujawnienie informacji poza organizację. • Instalowanie nieautoryzowanego oprogramowania. • Utrata lub nieuprawniony dostęp do danych. przechowywanych na urządzeniach mobilnych.

ŹRÓDŁO: Opracowanie własne NASK – PIB.

Działania wspierające realizację wymagań ustawowych

- Regularne monitorowanie podatności, wycieków danych oraz błędów konfiguracji z wykorzystaniem dostępnych narzędzi, np. moje.cert.pl;
- Systematyczne zapoznawanie się z rekomendacjami Pełnomocnika Rządu ds. Cyberbezpieczeństwa;
- Śledzenie komunikatów o podatnościach publikowanych przez CERT Polska lub producentów wykorzystywanych systemów;
- Uwzględnianie wymagań bezpieczeństwa już na etapie planowania nowych usług, systemów i zmian organizacyjnych;
- Prowadzenie okresowych przeglądów konfiguracji systemów, urządzeń i usług;
- Regularna weryfikacja uprawnień użytkowników oraz usuwanie zbędnych dostępów;
- Określenie i egzekwowanie zasad korzystania z prywatnych urządzeń do celów służbowych (BYOD).

Najczęstsze błędy i pułapki

- Traktowanie bezpieczeństwa jako działania punktowego, a nie ciągłego procesu – skupianie się na wymaganiach bezpieczeństwa głównie na etapie zakupu, wdrożenia lub audytu, zamiast zarządzania nim przez cały cykl życia systemu.
- Pozostawianie otwartego dostępu do paneli administracyjnych z internetu;
- Pozostawianie niepotrzebnych uprawnień użytkowników i administratorów;
- Korzystanie z niewspieranego lub nieaktualnego oprogramowania;
- Brak kontroli nad urządzeniami mobilnymi wykorzystywanymi do pracy;
- Traktowanie kopii zapasowych jako wystarczającego zabezpieczenia bez testowania ich odtwarzania;
- Brak dostosowania poziomu zabezpieczeń do znaczenia systemów i danych.

Materiały uzupełniające

- Usługa moje.cert.pl, bezpłatne narzędzie CERT Polska (NASK), które umożliwia monitorowanie i ocenę poziomu cyberbezpieczeństwa domen, stron internetowych oraz infrastruktury sieciowej organizacji;
- Wykaz rekomendacji Wykaz Rekomendacji Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa;
- Poradnik NASK Sprzęt firmowy pod kontrolą – 12 filarów bezpieczeństwa.

Cyberbezpieczeństwo dostawców i usług zewnętrznych

Współczesne organizacje korzystają z wielu produktów, usług i rozwiązań z obszaru ICT (Information and Communication Technologies), czyli technologii informacyjno-komunikacyjnych. Obejmują one m.in. systemy informatyczne, usługi chmurowe, sieci teleinformatyczne, oprogramowanie, centra danych oraz usługi świadczone przez podmioty zewnętrzne. Oznacza to, że poziom cyberbezpieczeństwa organizacji zależy nie tylko od stosowanych przez nią zabezpieczeń, ale także od bezpieczeństwa dostawców, wykorzystywanych produktów i świadczonych usług.

Czego wymaga ustawa?

Ustawa nakłada obowiązek zarządzania ryzykiem związanym z dostawcami produktów, usług i procesów ICT. Obejmuje to zapewnienie bezpieczeństwa i ciągłości łańcucha dostaw, ocenę ryzyka dostawców i świadczonych przez nich usług, ocenę jakości wykorzystywanych rozwiązań, monitorowanie dostawców oraz zarządzanie zależnościami od podmiotów zewnętrznych, w tym dostawców wysokiego ryzyka. Działania te mają ograniczać ryzyko zakłóceń, incydentów oraz negatywnego wpływu problemów po stronie dostawców na funkcjonowanie organizacji.

TABELA 12. Bezpieczeństwo dostawców i usług zewnętrznych – wybrane aspekty wraz z odniesieniem do właściwych przepisów.

Kategoria	Obszar	Odniesienie do ustawy
Bezpieczeństwo dostawców i usług zewnętrznych		
	Bezpieczeństwo i ciągłość łańcucha dostaw produktów, usług i procesów ICT	art. 8 ust. 1 pkt 2 lit. e
	Ocena ryzyka dostawców i usług ICT	art. 8 ust. 2 pkt 1
	Jakość produktów usług i procesów	art. 8 ust. 2 pkt 2
	Monitorowanie i nadzór nad dostawcami	art. 8 ust. 2 pkt 3
	Zarządzanie zależnościami od dostawców ICT, w tym uwzględnianie dostawców wysokiego ryzyka	art. 8 ust. 2 pkt 4

ŹRÓDŁO: Opracowanie własne NASK – PIB.

§

Co to oznacza w praktyce?

→ **Bezpieczeństwo i ciągłość łańcucha dostaw produktów, usług i procesów ICT** (art. 8 ust. 1 pkt 2 lit. e oraz art. 8 ust. 2 pkt 3)

Organizacja powinna wiedzieć, od których dostawców jest zależna i które rozwiązania są niezbędne do jej działania. Warto przygotować listę najważniejszych zależności i zastanowić się, jakie byłyby skutki ich niedostępności. Przy ocenie ryzyka związanego z dostawcami i usługami ICT należy brać pod uwagę nie tylko własne analizy i doświadczenia, ale także informacje i oceny bezpieczeństwa publikowane na poziomie Unii Europejskiej. Mogą one pomóc w identyfikacji zagrożeń, podatności oraz innych ryzyk związanych z konkretnymi produktami, usługami lub dostawcami. Dzięki temu można wcześniej zaplanować działania ograniczające ryzyko i wspierające ciągłość działania.

→ **Ocena ryzyka dostawców i usług ICT** (art. 8 ust. 2 pkt 1)

Przed wyborem dostawcy warto sprawdzić, jak dba on o bezpieczeństwo informacji i czy zapewnia odpowiedni poziom ochrony swoich usług. Należy ocenić, jakie konsekwencje dla organizacji mogłaby mieć awaria systemu lub wyciek danych po stronie dostawcy. Taką ocenę warto powtarzać również w trakcie współpracy, szczególnie gdy zmienia się zakres usług lub pojawiają się nowe zagrożenia.

→ **Jakość produktów, usług i procesów ICT** (art. 8 ust. 2 pkt 2)

Przed zakupem lub wdrożeniem systemu, oprogramowania lub usługi warto sprawdzić, czy są one regularnie aktualizowane, wspierane przez dostawcę lub producenta oraz spełniają wymagania bezpieczeństwa organizacji. Powinno się także zwrócić uwagę na sposób utrzymania i rozwijania wykorzystywanych rozwiązań, w tym proces wprowadzania aktualizacji i usuwania podatności. Dobrą praktyką jest określenie wymagań już na etapie zapytania ofertowego lub umowy, tak aby dostawca od początku znał oczekiwania organizacji.

→ **Zarządzanie zależnościami od dostawców ICT, w tym dostawców wysokiego ryzyka** (art. 8 ust. 2 pkt 4)

Organizacja powinna identyfikować sytuacje, w których jest zależna od jednego dostawcy oraz podejmować działania ograniczające związane z tym ryzyko, szczególnie jeśli mogłoby to zakłócić lub sparaliżować realizację zadań. Warto rozważyć rozwiązania alternatywne i przygotować sposób działania na wypadek zakończenia współpracy lub dłuższej niedostępności usługi. Należy zwrócić uwagę na ryzyko uznania dostawcy za dostawcę wysokiego ryzyka i konsekwencje związane z koniecznością wycofania z użytkowania produktu, usługi lub procesu ICT dostarczanych przez ten podmiot.

Jak sprawdzić, czy organizacja spełnia ten obowiązek?

Zapewnienie bezpieczeństwa dostawców i usług zewnętrznych wymaga uwzględniania i ryzyka związanego z produktami, usługami i procesami ICT wykorzystywanymi przez organizację. Obejmuje to identyfikację kluczowych zależności od dostawców, ocenę ryzyka, monitorowanie współpracy oraz planowanie działań ograniczających wpływ potencjalnych problemów po stronie dostawcy.

TABELA 13. Cyberbezpieczeństwo dostawców i usług zewnętrznych – wybrane aspekty.

Perspektywa	Co należy sprawdzić	Konsekwencje zaniedbania
Decyzje i odpowiedzialność	• Którzy dostawcy mają kluczowe znaczenie dla funkcjonowania organizacji? • Kto odpowiada za akceptację ryzyka związanego ze współpracą z dostawcami? • Kto odpowiada za współpracę z najważniejszymi dostawcami? • Na ile kwestie bezpieczeństwa wpływają na wybór dostawców?	• Nieuwzględnienie istotnych zagrożeń przy planowaniu działań. • Zakłócenie działalności organizacji i przerwy w świadczeniu usług. • Straty finansowe i wizerunkowe.
Zasady, procedury i dokumentacja	• W jaki sposób wymagania bezpieczeństwa są uwzględniane podczas wyboru dostawców? • Jakie wymagania w zakresie bezpieczeństwa są zapisane w umowach? • Czy wymagania obejmują również podwykonawców? • Czy określono wymagania dotyczące miejsca przechowywania i przetwarzania danych? • Czy określono zasady okresowej oceny dostawców?	• Brak jednolitych zasad współpracy z dostawcami. • Trudności w egzekwowaniu wymagań dotyczących bezpieczeństwa. • Pominięcie istotnych zagrożeń związanych z dostawcami i podwykonawcami.
Systemy i bezpieczeństwo techniczne	• Czy wiadomo, do jakich systemów i danych mają dostęp dostawcy? • Czy bezpieczeństwo rozwiązań dostawców jest okresowo weryfikowane? • Czy organizacja wie, jaki wpływ na jej systemy może mieć awaria lub incydent po stronie dostawcy? • Czy poziom bezpieczeństwa rozwiązań dostarczanych przez podmioty zewnętrzne jest oceniany przed ich wdrożeniem i w trakcie użytkowania?	• Niekontrolowany dostęp do systemów i danych. • Niewykryte podatności i słabe punkty. • Nieznany poziom bezpieczeństwa wykorzystywanych rozwiązań. • Nieprzewidziane skutki awarii lub incydentów po stronie dostawcy.

Perspektywa	Co należy sprawdzić	Konsekwencje zaniedbania
Usługi, ludzie i codzienna działalność	• Czy pracownicy wiedzą, gdzie zgłaszać problemy związane z usługami dostawców? • Czy dostawca zapewnia wsparcie odpowiednie do potrzeb organizacji? • Czy organizacja zna czas reakcji dostawcy na zgłoszenia i awarie? • Jaki wpływ na codzienną pracę mogą mieć problemy po stronie dostawcy? • Czy użytkownicy są informowani o planowanych przerwach i zmianach w usługach?	• Utrudnienia w codziennej pracy. • Opóźnione usuwanie problemów. • Wydłużony czas niedostępności usług. • Spadek jakości świadczonych usług. • Niezadowolenie użytkowników.

ŹRÓDŁO: Opracowanie własne NASK – PIB.

Działania wspierające realizację wymagań ustawowych

- Uwzględnianie ryzyka cyberbezpieczeństwa przy wyborze i kwalifikacji dostawców;
- Systematyczne zapoznawanie się z rekomendacjami Pełnomocnika Rządu ds. Cyberbezpieczeństwa;
- Monitorowanie bezpieczeństwa i zgodności działań dostawców z przyjętymi wymaganiami;
- Nadzorowanie i okresowa weryfikacja uprawnień dostawców do systemów, sieci i danych;
- Ograniczanie zależności od pojedynczych dostawców oraz przygotowanie rozwiązań alternatywnych;
- Analizowanie wpływu incydentów i awarii dostawców na działalność organizacji;
- Podejmowanie działań doskonalących na podstawie wyników ocen, przeglądów i incydentów związanych z dostawcami.

Najczęstsze błędy i pułapki

- Traktowanie oceny bezpieczeństwa dostawcy jako jednorazowego działania wykonywanego wyłącznie przed rozpoczęciem współpracy;

- Koncentrowanie się na kosztach i funkcjonalności usług, z pominięciem wymagań dotyczących cyberbezpieczeństwa;
- Pozostawianie dostawcom nadmiernych lub nieaktualnych uprawnień do systemów, sieci i danych organizacji;
- Uzależnienie kluczowych procesów od jednego dostawcy bez przygotowania rozwiązań alternatywnych;
- Pomijanie podwykonawców dostawcy w ocenie ryzyka i wymaganiach bezpieczeństwa;
- Zakładanie, że korzystanie z usług zewnętrznych zwalnia organizację z odpowiedzialności za cyberbezpieczeństwo;
- Ignorowanie sygnałów ostrzegawczych, takich jak incydenty, problemy techniczne lub pogorszenie jakości usług dostawcy.

Reagowanie i odporność organizacji

Nie wszystkie awarie, błędy i cyberataki można przewidzieć lub całkowicie wyeliminować. Kluczowe znaczenie ma więc zdolność organizacji do szybkiego wykrywania zagrożeń, skutecznego reagowania na incydenty oraz ograniczania ich skutków.

Czego wymaga ustawa?

Ustawa nakłada obowiązki związane z monitorowaniem systemów, rozpoznawaniem podatności i zagrożeń, zarządzaniem incydentami, wykonywaniem kopii zapasowych oraz przygotowaniem organizacji do utrzymania ciągłości działania i odtworzenia usług po awarii.

TABELA 14. Reagowanie i odporność organizacji – wybrane aspekty wraz z odniesieniem do właściwych przepisów.

Kategoria	Obszar	Odniesienie do ustawy
Reagowanie i odporność organizacji		
	Ciągłość działania i odtwarzanie po awarii	art. 8 ust. 1 pkt 2 lit. f
	Monitorowanie systemów	art. 8 ust. 1 pkt 2 lit. g
	Zbieranie informacji o cyberzagrożeniach i podatnościach	art. 8 ust. 1 pkt 3
	Zarządzanie incydentami	art. 8 ust. 1 pkt 4, art. 8 ust. 1 pkt 5 lit. d

ŹRÓDŁO: Opracowanie własne NASK – PIB.

Co to oznacza w praktyce?

W ustawie KSC 2.0 kluczową rolę odgrywa pojęcie incydentu. Obejmuje ono zdarzenia, które mogą negatywnie wpływać na bezpieczeństwo systemów informacyjnych, danych lub świadczonych usług. Incydent może wynikać zarówno z cyberataku, jak i awarii, błędu użytkownika czy innych niepożądanych zdarzeń.

Rodzaj incydentu i jego znaczenie

INCYDENT	Zdarzenie, które ma lub może mieć niekorzystny wpływ na bezpieczeństwo systemów informacyjnych.
INCYDENT POWAŻNY	Incydent, który powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi, straty finansowe lub wpływa na inne osoby lub podmioty przez wywołanie poważnej szkody materialnej lub niematerialnej. O tym, kiedy incydent będzie kwalifikowany jako poważny, będą decydować szczegółowe progi określone w rozporządzeniu Rady Ministrów.
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.

Działania organizacji nie powinny jednak koncentrować się wyłącznie na samym incydencie. Aby lepiej zrozumieć wymagania ustawowe, można je podzielić na trzy etapy:

§

1. **Zanim dojdzie do incydentu – monitorowanie systemów** (art. 8 ust. 1 pkt 2 lit. g) **oraz zbieranie informacji o cyberzagrożeniach i podatnościach** (art. 8 ust. 1 pkt 3)

Skuteczne wykrywanie incydentów wymaga bieżącej obserwacji środowiska IT oraz śledzenia informacji o zagrożeniach, które mogą wpływać na bezpieczeństwo organizacji. Celem nie jest gromadzenie jak największej liczby danych, lecz możliwie szybkie zauważenie nieprawidłowości i podjęcie działań zanim doprowadzą one do zakłócenia działania usług. Oznacza to m.in.:

- monitorowanie komunikatów publikowanych przez CERT Polska, właściwy CSIRT oraz producentów wykorzystywanych rozwiązań,
- wykorzystywanie mechanizmów automatycznego powiadamiania o zdarzeniach wymagających uwagi administratorów,
- regularne przeglądanie logów oraz informacji pochodzących z systemów bezpieczeństwa, urządzeń sieciowych i usług krytycznych,
- identyfikowanie zdarzeń i anomalii mogących świadczyć o awarii, błędzie konfiguracji lub incydencie, np. zwiększonej liczby nieudanych logowań, logowań z nowych lokalizacji, nieoczekiwanych zmian konfiguracji, nagłego wzrostu ruchu sieciowego lub nietypowej aktywności kont administracyjnych,
- ocenę, czy wykryte podatności i zagrożenia mają znaczenie dla organizacji oraz wymagają podjęcia działań ograniczających ryzyko.

§

2. **Gdy incydent zostanie wykryty – wykrywanie incydentów oraz zarządzanie nimi** (art. 8 ust. 1 pkt 4, art. 8 ust. 1 pkt 5 lit. d)

Po wykryciu incydentu organizacja powinna być przygotowana do szybkiego podjęcia działań ograniczających jego skutki oraz skoordynowanej obsługi zdarzenia m.in. poprzez:

- rejestrowanie i klasyfikowanie zgłoszeń dotyczących incydentów,
- określenie skali incydentu, jego wpływu na organizację oraz priorytetu działań,
- wyznaczenie osób odpowiedzialnych za koordynację działań związanych z obsługą incydentu,
- ograniczanie skutków incydentu poprzez odizolowanie zagrożonych systemów, urządzeń, kont lub usług,

- zabezpieczanie logów, zapisów systemowych i innych informacji niezbędnych do analizy zdarzenia,
- zapewnienie sprawnej wymiany informacji pomiędzy osobami i zespołami zaangażowanymi w obsługę incydentu,
- **realizację obowiązków związanych z przekazywaniem informacji o incydencie z wykorzystaniem Systemu S46 (szczegóły przedstawiono w kolejnym rozdziale),**
- dokumentowanie przebiegu incydentu oraz podjętych działań.

§

3. **Po incydencie lub awarii – ciągłość działania** (art. 8 ust. 1 pkt 2 lit. f)

Po opanowaniu incydentu lub usunięciu skutków awarii organizacja powinna możliwie szybko przywrócić dostępność danych, systemów i usług. Celem jest ograniczenie przestojów oraz powrót do bezpiecznego funkcjonowania organizacji m.in. poprzez:

- określenie dopuszczalnego czasu niedostępności usług,
- uruchomienie alternatywnych sposobów realizacji kluczowych procesów w okresie niedostępności systemów, jeśli to możliwe,
- przywracanie systemów do działania z wykorzystaniem wcześniej wykonanych i przetestowanych kopii zapasowych,
- potwierdzenie poprawności i kompletności odtworzonych danych,
- weryfikację, czy usunięto przyczynę incydentu lub awarii przed ponownym uruchomieniem systemów,
- analiza przebiegu zdarzenia i identyfikacja działań ograniczających ryzyko podobnych incydentów w przyszłości.

Jak sprawdzić, czy organizacja spełnia ten obowiązek?

Spełnienie obowiązku dotyczącego monitorowania systemów, zarządzania incydentami i podatnościami, wykonywania kopii zapasowych oraz zapewnienie ciągłości działania można ocenić poprzez sprawdzenie, czy organizacja posiada i stosuje rozwiązania umożliwiające monitorowanie systemów, identyfikowanie zagrożeń i podatności, skuteczne reagowanie na incydenty oraz odtwarzanie danych i usług po awarii. Kluczowe obszary podlegające weryfikacji przedstawiono w tabeli poniżej.

TABELA 15. Reagowanie i odporność organizacji – wybrane aspekty.

Perspektywa	Co należy sprawdzić	Konsekwencje zaniedbania
Decyzje i odpowiedzialność	• Kto odpowiada za wykrywanie i obsługę incydentów? • Kto podejmuje kluczowe decyzje podczas incydentu? • Czy określono, kiedy i w jaki sposób należy informować kierownictwo? • Czy organizacja analizuje przyczyny incydentów i wykorzystuje zdobyte doświadczenia do wprowadzania usprawnień?	• Niejasny podział odpowiedzialności. • Sprzeczne decyzje podejmowane przez różne osoby. • Wydłużenie czasu przywracania usług. • Powtarzanie się podobnych incydentów w przyszłości.
Zasady, procedury i dokumentacja	• Czy organizacja posiada jasno określone zasady obsługi incydentów, współpracy z właściwym CSIRT-em oraz realizacji obowiązków z wykorzystaniem Systemu S46?	• Chaos organizacyjny podczas incydentu. • Ryzyko niewypełnienia obowiązków ustawowych. • Utrudniona współpraca z właściwym CSIRT-em.
Systemy i bezpieczeństwo techniczne	• Czy systemy są monitorowane pod kątem awarii, anomalii i zagrożeń? • Czy wykorzystywane są mechanizmy alertowania? • Czy możliwe jest szybkie odizolowanie zagrożonych systemów i usług? • Czy regularnie sprawdzana jest możliwość odtworzenia danych i systemów z kopii zapasowych? • Czy organizacja jest przygotowana do przywrócenia działania usług po incydencie lub awarii?	• Opóźnione wykrycie incydentu. • Eskalacja skutków awarii lub cyberataku. • Utrata danych lub brak możliwości ich odtworzenia. • Wydłużona niedostępność systemów i usług.
Usługi, ludzie i codzienna działalność	• Czy pracownicy wiedzą, jak rozpoznać i zgłaszać incydenty oraz nieprawidłowości w funkcjonowaniu systemów? • Czy użytkownicy/klienci są informowani o zakłóceniach w działaniu usług oraz planowanym czasie ich przywrócenia? • Czy określono zasady komunikacji z użytkownikami, klientami lub opinią publiczną w przypadku poważnego incydentu?	• Opóźnione zgłaszanie incydentów. • Dezinformacja i chaos komunikacyjny podczas incydentu. • Utrata zaufania użytkowników i interesariuszy.

ŹRÓDŁO: Opracowanie własne NASK – PIB.

Działania wspierające realizację wymagań ustawowych

- Określenie jasnych ról i odpowiedzialności związanych z obsługą incydentów;
- Regularne testowanie procedur ciągłości działania i odtwarzania po awarii;
- Ciągłe monitorowanie kluczowych systemów i usług;
- Regularne skanowanie podatności oraz usuwanie wykrytych nieprawidłowości.
- Przeprowadzanie ćwiczeń i symulacji incydentów cyberbezpieczeństwa;
- Korzystanie z informacji o nowych cyberzagrożeniach publikowanych przez CSIRT-y poziomu krajowego oraz CSIRT-y sektorowe, producentów oprogramowania oraz inne zweryfikowane źródła informacji;
- Regularne wykonywanie i testowanie kopii zapasowych;
- Regularne szkolenie pracowników z rozpoznawania zagrożeń i zasad reagowania na incydenty.

Najczęstsze błędy i pułapki

- Niedostateczne zaangażowanie kierownictwa w kwestie cyberbezpieczeństwa;
- Niedokumentowanie podejmowanych działań i wyników przeprowadzanych analiz;
- Bagatelizowanie incydentów i założenie, że „skoro nic się nie stało, to nie ma problemu”;
- Ukrywanie błędów, niezgłaszanie incydentów lub odkładanie działań naprawczych zamiast rzetelnej analizy przyczyn i skutków zdarzeń;
- Skupianie się wyłącznie na rozwiązaniach technicznych z pominięciem aspektów organizacyjnych i procesowych;
- Traktowanie cyberbezpieczeństwa jako jednorazowego zadania, a nie ciągłego procesu zarządzania bezpieczeństwem.

Zgłaszanie incydentów

Zgłaszanie incydentów jest jednym z obowiązków wynikających z ustawy, ale jego znaczenie wykracza poza sam wymóg prawny. Pełni ono również istotną funkcję w zarządzaniu cyberbezpieczeństwem, gdyż pozwala szybciej reagować na zagrożenia, ograniczać skutki incydentów, utrzymywać ciągłość działania organizacji oraz wzmacniać bezpieczeństwo całego ekosystemu cyberbezpieczeństwa.

Czego wymaga ustawa?

Ustawa zobowiązuje do niezwłocznego zgłaszania **incydentów poważnych** do właściwego CSIRT-u oraz do współpracy z tym zespołem podczas całego procesu obsługi incydentu. Oznacza to konieczność terminowego przekazywania informacji o zdarzeniu, jego skutkach oraz podejmowanych działaniach naprawczych, a także uwzględnianie zaleceń i rekomendacji wydawanych przez właściwy CSIRT.

Dla niektórych podmiotów ważnych będących jednocześnie podmiotami publicznymi przepisy przewidują odrębne zasady raportowania.

Zgłoszenia incydentów przekazuje się za pośrednictwem Systemu S46, służącego do raportowania incydentów i wymiany informacji pomiędzy podmiotami a właściwymi zespołami CSIRT.

TABELA 16. Zgłaszanie incydentów – wybrane aspekty wraz z odniesieniem do właściwych przepisów.

Kategoria	Obszar	Odniesienie do ustawy
Zgłaszanie incydentów		
	Zgłaszanie incydentów do CSIRT-u sektorowego	art. 11 ust. 1 pkt 4, 4a, 4b, 4c, art. 46 ust. 1, art. 12
	Współpraca z CSIRT-em	art. 11 ust. 1 pkt 2 oraz pkt 5
	Raportowanie	art. 11 ust. 1 pkt 4b i 4c, art. 12a, art. 12b
	Wyjątki dla podmiotów ważnych będących podmiotami publicznymi	art. 12c

ŹRÓDŁO: Opracowanie własne NASK – PIB.

Co to oznacza w praktyce?

§

Zgłaszanie incydentów do CSIRT-u sektorowego i raportowanie (art. 11 ust. 1 pkt 4, 4a, 4b, 4c, art. 46 ust. 1, art. 12, art. 12a oraz art. 12b).

Każdy wykryty incydent poważny należy zgłosić przez System S46. Zgłoszenie trafia obecnie do odpowiedniego CSIRT-u poziomu krajowego (NASK, GOV lub MON), a docelowo trafi do CSIRT-u sektorowego.

Proces ten składa się z trzech etapów.

Etapy zgłaszania incydentu poważnego

↓ **WYKRYCIE INCYDENTU POWAŻNEGO**

ETAP 1.

Wczesne ostrzeżenie

do 24 godzin od wykrycia incydentu

CEL
Szybkie poinformowanie CSIRT-u sektorowego o wystąpieniu incydentu.

CO NALEŻY PODAĆ?

- dane podmiotu zgłaszającego,
- dane kontaktowe osoby dokonującej zgłoszenia i osoby uprawnionej do składania wyjaśnień,
- moment wystąpienia i wykrycia incydentu oraz czas jego trwania,
- informacje, czy incydent mógł zostać wywołany działaniem bezprawnym lub działaniem w złej wierze (jeżeli możliwa jest taka ocena),
- informacje, czy incydent może dotyczyć innych państw członkowskich UE.

W zgłoszeniu można również zwrócić się do CSIRT-u sektorowego o wsparcie techniczne lub wskazanie działań ograniczających skutki incydentu.

↓ 01

ETAP 2.

Zgłoszenie incydentu poważnego

do 72 godzin od wykrycia incydentu

CEL
Przekazanie szczegółowych informacji umożliwiających ocenę zdarzenia i wsparcie jego obsługi.

CO NALEŻY PODAĆ?

- opis wpływu incydentu na świadczone usługi,
- opis przyczyn i przebiegu incydentu,
- przewidywane skutki incydentu,
- informacje o podjętych działaniach zapobiegawczych i naprawczych,
- aktualizację informacji przekazanych we wczesnym ostrzeżeniu.

Należy przekazywać wszystkie dostępne informacje oraz uzupełniać je w miarę postępu prac związanych z obsługą incydentu.

↓

02

ETAP 3

Sprawozdanie końcowe z obsługi incydentu

do 1 miesiąca od dnia zgłoszenia incydentu

Po zakończeniu obsługi incydentu należy przekazać do właściwego CSIRT-u sektorowego sprawozdanie końcowe z obsługi incydentu poważnego.

CEL
Podsumowanie przebiegu incydentu, jego przyczyn, skutków oraz wdrożonych działań naprawczych.

CO NALEŻY PODAĆ?

- szczegółowy opis incydentu oraz spowodowanych zakłóceń i szkód,
- źródło lub prawdopodobną przyczynę incydentu,
- zastosowane i planowane środki ograniczające ryzyko,
- informacje o skutkach transgranicznych, jeżeli wystąpiły.

Raport końcowy pozwala wyciągnąć wnioski z incydentu i wykorzystać je do zwiększenia poziomu bezpieczeństwa organizacji.

↓

Zgodnie z art. 12b KSC 2.0, jeśli obsługa incydentu poważnego nie zakończy się w terminie składania sprawozdania końcowego, podmiot przekazuje właściwemu CSIRT sektorowemu, sprawozdanie z postępu obsługi tego incydentu.

W przypadku gdy obsługa incydentu poważnego nie zakończy się w terminie składania sprawozdania końcowego, podmiot przekazuje właściwemu CSIRT sektorowemu sprawozdanie końcowe niepóźniej niż w ciągu miesiąca od zakończenia obsługi incydentu poważnego.

03

Właściwy CSIRT sektorowy może zawnioskować o sprawozdanie okresowe z obsługi incydentu poważnego.

§

WSPÓŁPRACA Z CSIRT (art. 11 ust. 1 pkt 2 oraz pkt 5)
Po zgłoszeniu incydentu należy współpracować z właściwym CSIRT-em, przekazywać wymagane informacje i wspólnie podejmować działania ograniczające skutki zdarzenia.

W praktyce oznacza to:

- udostępnianie informacji dotyczących incydentu,
- przekazywanie dodatkowych wyjaśnień i danych technicznych,
- realizację zaleceń związanych z obsługą incydentu,
- korzystanie ze wsparcia eksperckiego właściwego CSIRT-u.

→ WAŻNE

W zgłoszeniu należy przekazać również informacje objęte tajemnicą prawnie chronioną, w tym tajemnicą przedsiębiorstwa, jeżeli są one niezbędne do obsługi incydentu. Informacje takie powinny być odpowiednio oznaczone. CSIRT jest zobowiązany do zachowania ich poufności.

§

WYJĄTKI DLA PODMIOTÓW WAŻNYCH BĘDĄCYCH PODMIOTAMI PUBLICZNYMI (art. 12c)
Niektóre podmioty ważne będące jednocześnie podmiotami publicznymi podlegają odrębnym zasadom raportowania określonym w ustawie KSC 2.0. Szczegółowe wymagania w tym zakresie zostały opisane w art. 12c.

Jak sprawdzić, czy organizacja spełnia ten obowiązek?

Organizacja spełnia ten obowiązek, jeśli posiada i stosuje procedury umożliwiające monitorowanie systemów, identyfikowanie zagrożeń i podatności, wykrywanie oraz obsługę incydentów, a także zapewnia odtwarzanie danych i utrzymanie ciągłości działania po awarii. Weryfikacja powinna obejmować zarówno wdrożone rozwiązania techniczne, jak i organizacyjne.

TABELA 17. Zgłaszanie incydentów – wybrane aspekty.

Perspektywa	Co należy sprawdzić	Konsekwencje zaniedbania
Decyzje i odpowiedzialność	• Czy wyznaczono osoby odpowiedzialne za ocenę, klasyfikację i zgłaszanie incydentów? • Czy określono, kto odpowiada za kontakt z właściwym CSIRT-em? • Czy zapewniono zastępstwo dla osób odpowiedzialnych za zgłaszanie incydentów? • Czy określono zasady informowania kierownictwa o incydentach?	• Opóźnienie lub brak zgłoszenia incydentu w wymaganym terminie. • Błędna ocena lub klasyfikacja incydentu. • Utrudniona współpraca z właściwym CSIRT-em. • Opóźnienia w podejmowaniu decyzji i obsłudze incydentu. • Ryzyko niewykonania obowiązków wynikających z KSC 2.0.
Zasady, procedury i dokumentacja	• Czy istnieją procedury identyfikacji, klasyfikacji i zgłaszania incydentów? • Czy procedury określają sposób współpracy z właściwym CSIRT-em? • Czy organizacja prowadzi rejestr incydentów? • Czy określono sposób dokumentowania działań oraz przygotowywania raportów i sprawozdań? • Czy procedury uwzględniają wymagane terminy: 24 h, 72 h oraz 1 miesiąc?	• Brak lub niepełna dokumentacja incydentów. • Trudności w odtworzeniu przebiegu incydentu i podjętych działań. • Niespójne lub opóźnione działania podczas obsługi incydentu. • Utrudniona współpraca z właściwym CSIRT-em. • Ryzyko niedotrzymania terminów zgłoszeń i sprawozdań. • Trudności w wykazaniu realizacji obowiązków wynikających z KSC 2.0.

Perspektywa	Co należy sprawdzić	Konsekwencje zaniedbania
Systemy i bezpieczeństwo techniczne	• Czy wdrożono mechanizmy wykrywania incydentów? • Czy zapewniono gromadzenie i zabezpieczanie logów oraz innych informacji o incydencie? • Czy możliwa jest szybka ocena skali i wpływu incydentu? • Czy zapewniono narzędzia wspierające obsługę i dokumentowanie incydentów? • Czy zapewniono bezpieczne przekazywanie informacji o incydentach?	• Zbyt późne wykrycie incydentu. • Brak informacji potrzebnych do oceny sytuacji. • Trudności w ustaleniu przyczyn i skutków incydentu. • Wolniejsza reakcja i dłuższy czas przywracania usług. • Większa skala i skutki incydentu.
Usługi, ludzie i codzienna działalność	• Czy pracownicy wiedzą, jak rozpoznać i zgłosić incydent? • Czy znają zasady eskalacji i wiedzą, kogo poinformować? • Czy prowadzone są szkolenia i ćwiczenia dotyczące reagowania na incydenty? • Czy zapewniono ciągłość kontaktu z właściwym CSIRT-em? • Czy po incydentach analizowane są wnioski i wprowadzane potrzebne usprawnienia?	• Zbyt późne rozpoznanie i zgłoszenie incydentu. • Błędna ocena lub klasyfikacja zdarzenia. • Utrata czasu na ustalanie, kto i jak powinien zareagować. • Problemy z komunikacją podczas obsługi incydentu. • Powtarzanie tych samych błędów przy kolejnych incydentach.

ŹRÓDŁO: Opracowanie własne NASK – PIB.

Działania wspierające realizację wymagań ustawowych

→ Przygotowanie jasnych procedur, które określają sposób postępowania w przypadku incydentu, podział odpowiedzialności, zasady eskalacji oraz kontaktu z właściwym CSIRT-em;

→ Dokumentowanie incydentu od momentu jego wykrycia, tak aby możliwe było odtworzenie przebiegu zdarzenia, podjętych decyzji i działań;

→ Bieżące aktualizowanie informacji o incydencie wraz z pojawianiem się nowych ustaleń, bez opóźniania zgłoszenia w oczekiwaniu na pełny obraz sytuacji;

→ Przeanalizowanie incydentu po zakończeniu jego obsługi, w tym jego przyczyn, skutków i skuteczności podjętych działań, oraz wykorzystanie wniosków do poprawy zabezpieczeń i procedur;

- Regularne przeglądanie i aktualizowanie procedur, tak aby uwzględniały zmiany w organizacji, wykorzystywanych systemach oraz doświadczenia z wcześniejszych incydentów.

Najczęstsze błędy i pułapki

- Zbyt późne wykrycie lub wewnętrzne przekazanie informacji o incydencie, przez co organizacja traci czas potrzebny na jego ocenę i zgłoszenie;
- Błędna klasyfikacja incydentu i nierozpoznanie, że spełnia on kryteria incydentu poważnego;
- Niedotrzymanie terminów na przekazanie wczesnego ostrzeżenia, zgłoszenia incydentu poważnego lub sprawozdania końcowego;
- Czekanie na zebranie kompletu informacji przed przekazaniem wczesnego ostrzeżenia – na tym etapie należy przekazać informacje, które są już dostępne;
- Brak aktualizowania przekazanych informacji, gdy w trakcie obsługi incydentu pojawiają się nowe ustalenia;
- Niejasny podział odpowiedzialności – brak wskazania, kto ocenia incydent, kto podejmuje decyzję o zgłoszeniu i kto kontaktuje się z właściwym CSIRT-em;
- Nieaktualne lub nieprzetestowane procedury, które w sytuacji rzeczywistego incydentu okazują się trudne do zastosowania;
- Brak ćwiczeń i testów sprawdzających, czy pracownicy wiedzą, jak rozpoznać podejrzane zdarzenie, gdzie je zgłosić i jak zareagować.

Materiały uzupełniające

- CyberPolicy NASK – Rola i constituency CSIRT NASK w krajowym systemie cyberbezpieczeństwa po nowelizacji KSC 2.0 – opracowanie wyjaśniające rolę CSIRT NASK, zasady współpracy, zgłaszanie incydentów oraz wykorzystanie Systemu S46 w praktyce.
- Materiały informacyjne Cyberbezpieczna Polska z cybergov.pl Twoje Centrum Cyberbezpieczeństwa.

Nadzór i doskonalenie działania SZBI

Zmieniające się zagrożenia, technologie i potrzeby organizacji sprawiają, że stosowane zabezpieczenia powinny być regularnie oceniane i doskonalone. Dzięki temu SZBI pozostaje skutecznym narzędziem wspierającym ochronę informacji oraz odporność organizacji na incydenty.

Czego wymaga ustawa?

Ustawa nakłada obowiązki związane z oceną skuteczności wdrożonych środków bezpieczeństwa, ich okresową weryfikacją oraz zapewnieniem sprawnej komunikacji w sprawach związanych z cyberbezpieczeństwem. W przypadku podmiotów kluczowych przewiduje również obowiązek przeprowadzania audytów bezpieczeństwa.

→ WARTO WIEDZIEĆ

Na podmioty ważne również może zostać nałożony obowiązek przeprowadzenia audytu w drodze nakazu organu nadzoru w przypadku wystąpienia incydentu poważnego lub innego naruszenia przepisów ustawy przez ten podmiot.

TABELA 18. Nadzór i doskonalenie – wybrane aspekty wraz z odniesieniem do właściwych przepisów.

Kategoria	Obszar	Odniesienie do ustawy
Nadzór i doskonalenie		
	Ocena skuteczności środków	art. 8 ust. 1 pkt 2 lit. h
	Wyznaczenie i utrzymywanie osób kontaktowych ds. cyberbezpieczeństwa	art .9
	Audyty bezpieczeństwa dla podmiotów kluczowych	art. 15 ust. 1

ŹRÓDŁO: Opracowanie własne NASK – PIB.

Co to oznacza w praktyce

→ **Ocena skuteczności i doskonalenie środków bezpieczeństwa** (art. 8 ust. 1 pkt 2 lit. h)

Organizacja powinna regularnie oceniać, czy wdrożone środki techniczne i organizacyjne nadal zapewniają odpowiedni poziom bezpieczeństwa oraz odpowiadają jej aktualnym potrzebom. Taka ocena może obejmować m.in.:

- zmiany zachodzące w organizacji oraz jej otoczeniu,
- zmiany wymagań prawnych, biznesowych i organizacyjnych,
- nowe zagrożenia oraz ryzyka wpływające na działalność organizacji,
- wyniki monitorowania, kontroli, testów, ćwiczeń i audytów,
- informacje zwrotne od pracowników, użytkowników, dostawców i innych podmiotów współpracujących,
- incydenty, awarie oraz ocenę skuteczności stosowanych środków bezpieczeństwa.

Wyniki przeprowadzonych ocen powinny stanowić podstawę do podejmowania działań mających na celu utrzymanie skuteczności stosowanych zabezpieczeń. Jeżeli ocena wykaże obszary wymagające poprawy, organizacja powinna:

- usuwać przyczyny stwierdzonych problemów,
- planować i wdrażać działania korygujące,
- weryfikować skuteczność podjętych działań,
- aktualizować procedury i dokumentację,
- wprowadzać niezbędne zmiany wynikające z przeprowadzonych ocen.

Warto pamiętać
Celem doskonalenia SZBI jest nie tylko usuwanie zidentyfikowanych problemów, ale również zapewnienie, że stosowane rozwiązania pozostają skuteczne i adekwatne do zmieniających się warunków funkcjonowania organizacji.

§

→ **Audyt bezpieczeństwa** (art. 15)

Jednym z narzędzi wspierających ocenę skuteczności wdrożonych środków bezpieczeństwa są niezależne audyty bezpieczeństwa.
W przypadku podmiotów kluczowych ich przeprowadzanie stanowi obowiązek wynikający z ustawy KSC 2.0.

Audyt należy przeprowadzać co najmniej raz na 3 lata, a pierwszy powinien zostać wykonany nie później niż w ciągu 24 miesięcy od objęcia organizacji przepisami ustawy. Dla podmiotów, które zostały objęte przepisami od 3 kwietnia 2026 r. oznacza to termin do 3 kwietnia 2028 r.

Audyt stanowi niezależną ocenę skuteczności wdrożonych środków bezpieczeństwa i musi zostać przeprowadzony przez niezależnych

audytorów lub jednostkę oceniającą zgodność. Po jego zakończeniu podmiot kluczowy przekazuje kopię raportu właściwemu organowi ds. cyberbezpieczeństwa. W określonych przypadkach organ może również nakazać przeprowadzenie dodatkowego audytu i wskazać jego zakres. Dotyczyć to może zarówno podmiotów kluczowych jak i ważnych.

Należy pamiętać, że audyt nie zastępuje obowiązku bieżącego utrzymywania zgodności z ustawą i nie powinien być traktowany jako jednorazowa weryfikacja cyberbezpieczeństwa.

Warto pamiętać
Obowiązek cyklicznego audytu dotyczy wyłącznie podmiotów kluczowych. Podmioty ważne mogą jednak wykorzystywać audyty wewnętrzne do oceny skuteczności stosowanych zabezpieczeń i dokumentowania realizacji wymagań ustawowych.

§

→ **Wyznaczenie i utrzymywanie osób kontaktowych ds. cyberbezpieczeństwa** (art. 9)

Ustawa wymaga wyznaczenia osób odpowiedzialnych za kontakty w sprawach związanych z cyberbezpieczeństwem. Obowiązek ten nie kończy się jednak na podaniu danych kontaktowych podczas wpisu do Wykazu KSC.

Organizacja powinna:

- wyznaczyć osoby odpowiedzialne za kontakty w sprawach cyberbezpieczeństwa (co do zasady co najmniej dwie osoby kontaktowe),
- zgłosić ich dane podczas wpisu do Wykazu KSC,
- na bieżąco aktualizować dane w przypadku zmian kadrowych lub zmian danych kontaktowych,
- zapewnić możliwość sprawnej komunikacji z CSIRT-em oraz właściwymi organami.

Osoby kontaktowe pełnią istotną rolę w realizacji obowiązków ustawowych. To za ich pośrednictwem mogą być przekazywane informacje dotyczące incydentów, zagrożeń, podatności, działań naprawczych. Od sprawności tej komunikacji może zależeć terminowe wykonanie obowiązków wynikających z ustawy oraz skuteczna współpraca z uczestnikami krajowego systemu cyberbezpieczeństwa.

Jak przełożyć ten obowiązek na działania organizacji?

Regularna ocena skuteczności stosowanych rozwiązań pozwala szybciej identyfikować obszary wymagające poprawy i planować działania doskonalące.

TABELA 19. Nadzór i doskonalenie – wybrane aspekty.

Perspektywa	Co należy sprawdzić	Konsekwencje zaniedbania
Decyzje i odpowiedzialność	• Czy kierownictwo regularnie dokonuje przeglądu skuteczności stosowanych środków bezpieczeństwa? • Czy podejmowane są decyzje dotyczące usprawnień i dalszego rozwoju SZBI? • Czy określono odpowiedzialność za realizację działań doskonalących?	• Brak decyzji o wdrożeniu usprawnień lub aktualizacji SZBI. • Działania doskonalące nie są realizowane lub nie wiadomo, kto za nie odpowiada.
Zasady, procedury i dokumentacja	• Czy organizacja posiada procedury oceny skuteczności środków bezpieczeństwa? • Czy dokumentowane są wyniki przeglądów i podejmowane decyzje? • Czy procedury i dokumentacja są aktualizowane po wprowadzeniu zmian?	• Nieaktualna dokumentacja. • Trudności w wykazaniu realizacji obowiązków ustawowych. • Niespójność pomiędzy dokumentacją a rzeczywistymi działaniami.
Systemy i bezpieczeństwo techniczne	• Czy wyniki ocen są wykorzystywane do doskonalenia stosowanych zabezpieczeń? • Czy po wdrożeniu zmian sprawdzana jest ich skuteczność?	• Utrzymywanie nieskutecznych zabezpieczeń. • Powtarzanie się tych samych problemów pomimo podejmowanych działań.
Usługi, ludzie i codzienna działalność	• Czy dane osób kontaktowych w Wykazie KSC są aktualne? • Czy zapewniono zastępowalność osób kontaktowych podczas ich nieobecności?	• Utrudniona komunikacja z CSIRT-em i właściwymi organami. • Przekazywanie informacji do nieaktualnych osób kontaktowych.

ŹRÓDŁO: Opracowanie własne NASK – PIB.

Działania wspierające realizację wymagań ustawowych

- Okresowa ocena skuteczności stosowanych zabezpieczeń;
- Analiza zmian mogących wpływać na poziom bezpieczeństwa;
- Przegląd wyników audytów i działań weryfikacyjnych;
- Monitorowanie realizacji działań korygujących.

Najczęstsze błędy i pułapki

- Traktowanie oceny skuteczności środków bezpieczeństwa jako jednorazowego działania;
- Brak regularnej weryfikacji, czy stosowane zabezpieczenia nadal odpowiadają aktualnym potrzebom organizacji oraz poziomowi ryzyka;
- Niewykorzystywanie wyników ocen, kontroli i audytów do wprowadzania usprawnień;
- Odkładanie przygotowań do audytu do momentu wyznaczenia jego terminu;
- Nieaktualizowanie danych osób kontaktowych po zmianach kadrowych lub organizacyjnych;
- Błędne przekonanie, że obowiązek dotyczący osób kontaktowych kończy się na zgłoszeniu ich danych do Wykazu KSC.

Przykłady dokumentów związanych z realizacją wymagań KSC 2.0

§

Dokumenty są ważnym elementem systemu zarządzania bezpieczeństwem informacji, jednak o jego skuteczności nie decyduje samo ich posiadanie. Równie istotna jest możliwość wykazania, że przyjęte zasady są stosowane w praktyce. Takie podejście ułatwia również spełnienie wymagań art. 10 ustawy, który zobowiązuje podmioty kluczowe i ważne do dokumentowania działań związanych z cyberbezpieczeństwem.

DOKUMENTY NORMATYWNE – OKREŚLAJĄCE ZASADY DZIAŁANIA M.IN.:

- polityki i procedury dotyczące cyberbezpieczeństwa,

- programy i plany działań związanych z cyberbezpieczeństwem,
- wymagania bezpieczeństwa dla dostawców i usług zewnętrznych,
- plany ciągłości działania i odtwarzania działalności po awarii,
- dokumenty dotyczące ochrony infrastruktury,
- opisy i specyfikacje techniczne wykorzystywanych systemów informacyjnych.

DOKUMENTY OPERACYJNE – POTWIERDZAJĄCE REALIZACJĘ DZIAŁAŃ M.IN.:

- rejestry i wykazy dotyczące zasobów, dostawców, dostępów i incydentów,
- analizy ryzyka oraz dokumentacja zarządzania ryzykiem,
- dokumentacja szkoleń i działań podnoszących świadomość personelu,
- wyniki monitorowania, testów i przeglądów bezpieczeństwa,
- raporty i sprawozdania dotyczące incydentów oraz ich obsługi,
- raporty z audytów i działań kontrolnych,
- dokumentacja działań naprawczych, korygujących i doskonalących,
- protokoły, notatki i decyzje potwierdzające zaangażowanie kierownictwa w zarządzanie.

WAŻNE

W praktyce „wdrożone" oznacza również „udokumentowane i możliwe do wykazania".

Ministerstwo Cyfryzacji w celu wsparcia podmiotów kluczowych i podmiotów ważnych w realizacji obowiązków ustawowych opublikowało zaktualizowane zestawienie dokumentów normalizacyjnych. Materiał wskazuje normy i wytyczne oraz inne dokumenty wspierające realizację wymogów uKSC, w tym wdrażanie i doskonalenie SZBI.

Wymogi SZBI dla podmiotu ważnego będącego podmiotem publicznym

Ochrona informacji, systemów oraz zapewnienie ciągłości działania usług publicznych mają kluczowe znaczenie dla prawidłowego funkcjonowania państwa. Podmioty publiczne przetwarzają m.in. dane osobowe, prowadzą rejestry publiczne, zarządzają dokumentacją oraz realizują procesy związane z finansami i świadczeniem usług publicznych. Utrata tych informacji, ich nieuprawnione ujawnienie lub niedostępność systemów mogą wywołać poważne skutki dla działalności instytucji, obywateli, a w niektórych przypadkach również dla funkcjonowania państwa.

Dlatego ustawa KSC 2.0 wymaga od podmiotów publicznych wdrożenia systemu zarządzania bezpieczeństwem informacji (SZBI). Jego celem jest zapewnienie odpowiedniego poziomu ochrony informacji i systemów oraz ograniczanie ryzyka cyberzagrożeń.

W przypadku podmiotów ważnych będących podmiotami publicznymi ustawodawca przewidział uproszczony model SZBI opisany w załączniku nr 4 do ustawy. Nie oznacza to rezygnacji z wymagań w zakresie cyberbezpieczeństwa, lecz zastosowanie prostszego sposobu organizacji realizacji obowiązków wynikających z ustawy.

Jak zbudowany jest uproszczony SZBI?

Wymagania zostały podzielone na trzy grupy:

1. **Wymogi obowiązkowe**
   Są to działania, które organizacja musi wdrożyć i realizować w celu zapewnienia podstawowego poziomu bezpieczeństwa informacji i systemów.

2. **Wymogi dodatkowe**
   Są to działania, które warto wdrożyć w zależności od charakteru działalności organizacji, poziomu ryzyka oraz dostępnych zasobów organizacyjnych, finansowych i kadrowych.

3. **Przegląd i aktualizacja SZBI**
   Cyberbezpieczeństwo wymaga ciągłego doskonalenia. Dlatego organizacja powinna regularnie oceniać skuteczność wdrożonych rozwiązań oraz aktualizować je w odpowiedzi na zmieniające się zagrożenia i potrzeby.

Wymogi obowiązkowe

→ Por. część I załącznika nr 4 do ustawy KSC 2.0

1. **Zarządzanie zasobami**
Organizacja powinna wiedzieć, jakie systemy, urządzenia, usługi i oprogramowanie wykorzystuje do realizacji swoich zadań. Trudno skutecznie chronić zasoby, których nie zidentyfikowano lub nie są objęte nadzorem.

W szczególności warto:

- prowadzić inwentaryzację produktów, usług i procesów ICT,
- kontrolować wykorzystywane wersje oprogramowania i usług,
- korzystać z mechanizmów kontroli instalacji produktów i usług, jeżeli jest to możliwe,
- stosować wspierane i aktualne wersje produktów oraz monitorować występowanie krytycznych podatności.

2. **Ochrona przetwarzanych informacji**
Bezpieczeństwo informacji wymaga ochrony zarówno samych danych, jak i miejsc oraz urządzeń wykorzystywanych do ich przetwarzania.

W szczególności warto:

- zapewnić ochronę fizyczną pomieszczeń, w których przetwarzane są informacje,
- zabezpieczyć urządzenia wykorzystywane do przetwarzania informacji,
- zapewnić udokumentowaną ochronę danych przechowywanych u dostawców usług chmurowych lub w centrach danych.

3. **Kontrola dostępu**
Dostęp do informacji powinny mieć wyłącznie osoby, które potrzebują go do wykonywania swoich obowiązków.

W szczególności warto:

- nadawać dostęp wyłącznie osobom uprawnionym,
- stosować zasadę minimalnych uprawnień,
- regularnie weryfikować przyznane uprawnienia,
- usuwać lub modyfikować uprawnienia po zmianie zakresu obowiązków lub zakończeniu współpracy.

4. **Bezpieczeństwo pracy**
Nawet najlepsze zabezpieczenia techniczne nie zapewnią odpowiedniego poziomu ochrony, jeżeli użytkownicy nie będą korzystać z systemów w bezpieczny sposób.

W szczególności warto:

- określić zasady bezpiecznej pracy zdalnej i mobilnej,
- zapewnić odpowiedni poziom bezpieczeństwa poczty elektronicznej,
- stosować oprogramowanie chroniące przed złośliwym oprogramowaniem,
- promować i egzekwować zasady cyberhigieny.

5. **Kopie zapasowe**
Kopie zapasowe są jednym z podstawowych mechanizmów umożliwiających odtworzenie danych po awarii, błędzie lub incydencie cyberbezpieczeństwa.

W szczególności warto:

- wykonywać kopie zapasowe danych,
- przechowywać kopie oddzielnie od środowiska produkcyjnego,
- regularnie sprawdzać możliwość odtworzenia danych oraz kompletność kopii.

6. **Reagowanie na incydenty**
Każda organizacja powinna wiedzieć, jak postępować w przypadku cyberzagrożenia lub incydentu.

W szczególności warto:

- określić zasady postępowania na wypadek wystąpienia incydentu,
- przygotować procedury awaryjne,
- regularnie testować przyjęte zasady działania.

7. **Szkolenia i budowanie świadomości**
Cyberbezpieczeństwo zależy nie tylko od stosowanych technologii, ale również od wiedzy i zachowań użytkowników.

Działania edukacyjne powinny obejmować w szczególności:

- rodzaje cyberzagrożeń,
- zasady cyberhigieny,
- sposoby reagowania na incydenty,
- skutki naruszenia zasad bezpieczeństwa informacji.

Wymogi dodatkowe

→ Por. część II załącznika nr 4 do ustawy KSC 2.0

Działania dodatkowe nie są obowiązkowe, jednak warto rozważyć ich wdrożenie, jeżeli pozwalają na to potrzeby i możliwości organizacji.

1. **Minimalizacja ryzyka błędów ludzkich**
   - stosowanie dodatkowych środków organizacyjnych i technicznych ograniczających ryzyko błędów użytkowników.

2. **Bezpieczeństwo usług poczty elektronicznej**
   - korzystanie z dedykowanych usług poczty elektronicznej przeznaczonych do realizacji zadań organizacji.

3. **Zapewnienie dostępności systemów informacyjnych**
   - określenie wymaganego poziomu dostępności systemów,
   - zapewnienie możliwości działania w przypadku awarii lub incydentu.

4. **Korzystanie z usług chmurowych i sztucznej inteligencji**
   - określenie zasad korzystania z usług chmurowych,
   - określenie zasad korzystania z dużych generatywnych modeli sztucznej inteligencji,
   - monitorowanie przestrzegania przyjętych zasad.

5. **Monitorowanie i testowanie**
   - monitorowanie dostępu do informacji i działania systemów,
   - testowanie zabezpieczeń technicznych,
   - testowanie poziomu cyberhigieny użytkowników.

6. **Dodatkowe środki bezpieczeństwa**
   - uwzględnianie wymagań bezpieczeństwa w umowach z dostawcami,
   - aktualizowanie produktów i usług,
   - stosowanie dodatkowych środków organizacyjnych i technicznych adekwatnych do poziomu ryzyka.

Przegląd i doskonalenie SZBI

→ Por. część III załącznika nr 4 do ustawy KSC 2.0

SZBI nie jest rozwiązaniem wdrażanym jednorazowo. Powinien być regularnie oceniany i doskonalony w odpowiedzi na zmieniające się zagrożenia oraz potrzeby organizacji.

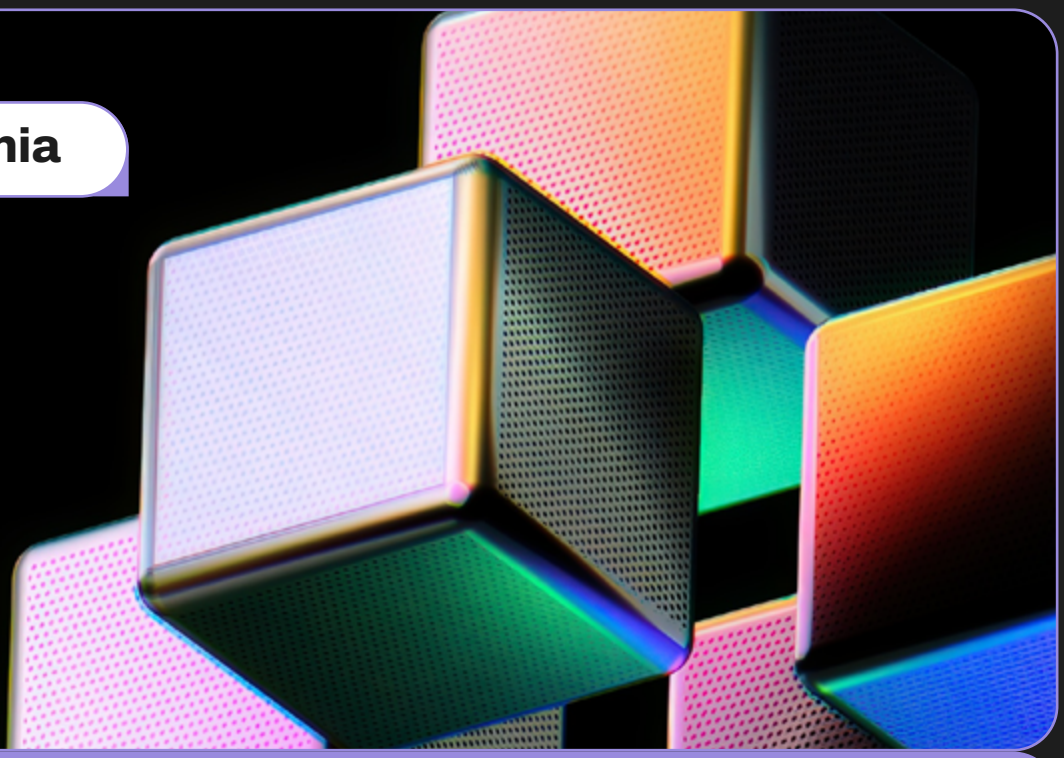
PRZEGLĄD SYSTEMU POWINIEN BYĆ REALIZOWANY

- nie rzadziej niż raz w roku,
- po opublikowaniu rekomendacji Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa dotyczących stosowanych produktów, usług lub systemów,
- po wystąpieniu okoliczności mogących wpływać na poziom ryzyka lub sposób realizacji obowiązków związanych z cyberbezpieczeństwem.

→ WAŻNE

Podmiot ważny będący podmiotem publicznym powinien dokumentować realizację działań wynikających z uproszczonego SZBI. Dokumentacja stanowi dowód wdrożenia wymagań oraz podstawę do ich oceny i doskonalenia.

Warto pamiętać, że SZBI nie jest pojedynczym dokumentem ani projektem wdrożeniowym. To proces obejmujący planowanie, wdrażanie, monitorowanie, przegląd i ciągłe doskonalenie działań związanych z bezpieczeństwem informacji i cyberbezpieczeństwem.



Odpowiedzialność za niewykonanie obowiązków

Obowiązki wynikające z ustawy KSC 2.0 nie kończą się na przygotowaniu dokumentacji. Organizacja powinna faktycznie stosować wymagane rozwiązania i być w stanie wykazać, że działają one w praktyce. Niewykonanie obowiązków wynikających z KSC 2.0 może prowadzić do kar pieniężnych i innych działań przewidzianych w ustawie. Skutki mogą być jednak znacznie szersze – od przestoju w działalności i utraty danych, przez dodatkowe koszty, aż po utratę zaufania klientów i partnerów. Dlatego cyberbezpieczeństwo to nie tylko kwestia technologii i działań IT. To element zarządzania organizacją, wymagający przede wszystkim zaangażowania i nadzoru ze strony kierownictwa.

ODPOWIEDZIALNOŚĆ KIEROWNICTWA

§

Zgodnie z ustawą KSC 2.0 odpowiedzialność za realizację obowiązków z zakresu cyberbezpieczeństwa spoczywa na kierowniku podmiotu kluczowego lub podmiotu ważnego (art. 8c ust. 1 ustawy KSC 2.0). Odpowiedzialność ta obejmuje zarówno zapewnienie realizacji obowiązków wynikających z ustawy, jak i nadzór nad ich wykonywaniem.

KIM JEST „KIEROWNIK PODMIOTU KLUCZOWEGO LUB WAŻNEGO”?

Kierownik podmiotu kluczowego lub podmiotu ważnego to osoba lub osoby formalnie zarządzające organizacją i odpowiadające za najważniejsze decyzje dotyczące jej działalności. Może to być m.in. członek zarządu lub cały zarząd, wspólnicy prowadzący sprawy spółki, właściciel firmy, a także likwidator, syndyk lub zarządca (jeśli podmiot znajduje się w szczególnej sytuacji prawnej). W jednostkach sektora publicznego jest to osoba kierująca daną jednostką. W praktyce przez „kierownika podmiotu” należy rozumieć osobę lub organ zarządzający organizacją i ponoszący odpowiedzialność za jej zarządzanie, a nie pełnomocnika czy doradcę.

OBOWIĄZKI KIEROWNIKA

§

Podstawową rolą kierownika jest zapewnienie właściwej organizacji cyberbezpieczeństwa w podmiocie. Nie oznacza to konieczności osobistego wykonywania wszystkich zadań, lecz zapewnienie ich skutecznej realizacji poprzez odpowiednie delegowanie obowiązków oraz sprawowanie nadzoru nad ich wykonaniem. Zadania związane z cyberbezpieczeństwem mogą być wykonywane przez wyznaczone osoby lub komórki organizacyjne, jednak odpowiedzialność za realizację obowiązków wynikających z ustawy nadal spoczywa na kierowniku podmiotu (art. 8c ust. 1 ustawy KSC 2.0). Powierzenie wykonywania obowiązków innym osobom nie zwalnia kierownika podmiotu z odpowiedzialności za ich realizację.

W praktyce oznacza to m.in.:

- zapewnienie zgodności działania organizacji z przepisami prawa oraz wewnętrznymi regulacjami dotyczącymi cyberbezpieczeństwa,
- zapewnienie odpowiednich środków finansowych i organizacyjnych,

- przydzielenie zadań i nadzór nad ich realizacją,
- zapewnienie funkcjonowania systemu zarządzania bezpieczeństwem informacji,
- dbanie o świadomość personelu i zgodność działania organizacji z wymaganiami KSC 2.0.

Ponadto kierownik podmiotu kluczowego lub ważnego ma obowiązek raz w roku kalendarzowym odbyć szkolenie z zakresu cyberbezpieczeństwa. Jego udział w szkoleniu powinien zostać udokumentowany (art. 8e ust. 1–3 ustawy KSC 2.0).

→ WAŻNE

Powierzenie zadań CISO, pełnomocnikowi ds. bezpieczeństwa, działowi IT czy zewnętrznemu dostawcy nie zwalnia kierownictwa z odpowiedzialności.

CO TO OZNACZA W PRAKTYCE?

Odpowiedzialności za cyberbezpieczeństwo nie można delegować, można natomiast delegować zadania. Kierownictwo powinno znać najważniejsze ryzyka i zagrożenia dotyczące organizacji, wiedzieć, kto odpowiada za poszczególne obszary cyberbezpieczeństwa, wyznaczać zadania, zapewniać niezbędne zasoby oraz stale monitorować i nadzorować realizację obowiązków z zakresu cyberbezpieczeństwa.

Cyberbezpieczeństwo powinno być stałym elementem zarządzania organizacją, a nie tematem podejmowanym dopiero wtedy, gdy wydarzy się incydent.

KONTROLA I ŚRODKI NADZORCZE

Podmioty kluczowe i podmioty ważne podlegają nadzorowi organów właściwych. Oznacza to, że nie wystarczy posiadać wymagane polityki i procedury. Organizacja powinna być w stanie wykazać, że przyjęte rozwiązania są rzeczywiście stosowane. Powinna również opracowywać i dokumentować m.in. analizy ryzyka, polityki i procedury, szkolenia personelu, obsługę incydentów, wyniki audytów i kontroli oraz działania naprawcze.

ŚRODKI NADZORCZE I KONSEKWENCJE NARUSZEŃ

Stwierdzenie nieprawidłowości nie musi od razu oznaczać kary pieniężnej. Organ właściwy do spraw cyberbezpieczeństwa może zastosować również środki nadzorcze służące usunięciu naruszeń i przywróceniu zgodności z KSC 2.0 (art. 53 ust. 2 i 5 ustawy).

§

W zależności od sytuacji może to oznaczać m.in.:

- nakaz usunięcia uchybień lub zaprzestania naruszania przepisów,
- nakaz wdrożenia zaleceń wynikających z audytu lub przeprowadzenia audytu bezpieczeństwa,
- obowiązek poinformowania o naruszeniu podmiotów, na które może ono mieć wpływ,
- w określonych przypadkach – podanie informacji o naruszeniu do wiadomości publicznej,
- ustanowienie przez organ urzędnika monitorującego.

§

Wobec podmiotów kluczowych możliwe są również dalej idące środki, w tym – w określonych przypadkach – czasowe ograniczenie działalności podmiotu do czasu usunięcia uchybień lub zaprzestania naruszeń, wstrzymanie koncesji czy zezwolenia albo czasowy zakaz pełnienia funkcji zarządczych przez kierownika (art. 53 ust. 9 ustawy KSC 2.0). Środków tych nie stosuje się do podmiotów publicznych (art. 53 ust. 10 ustawy KSC 2.0).

Kary pieniężne

§

Niezależnie od zastosowania środków nadzorczych niewykonanie obowiązków wynikających z ustawy KSC 2.0 może skutkować nałożeniem kary pieniężnej na organizację, a w określonych przypadkach, kara finansowa może być jednocześnie nałożona również na kierownika podmiotu (art. 73–73a ustawy KSC 2.0). Dodatkowo, wobec osób kierujących podmiotem kluczowym organ nadzoru może zastosować szczególny środek nadzorczy polegający na tymczasowym zakazie zajmowania stanowiska.

→ WAŻNE

Maksymalna kara dla podmiotu kluczowego lub podmiotu ważnego jest ustalana jako wyższa z dwóch wartości: określona kwota w euro albo odpowiedni procent rocznych przychodów podmiotu. W praktyce oznacza to, że jeżeli kwota wynikająca z procentu przychodów jest wyższa niż kwota wskazana w ustawie, to właśnie ona stanowi górny limit kary.

TABELA 20. Przykładowe kary za naruszenie obowiązków wynikających z ustawy KSC 2.0.

Kogo dotyczy?	Możliwa kara
Podmiot kluczowy	Od 20 tys. zł; maksymalnie równowartość 10 mln euro lub 2% przychodów
Podmiot ważny	Od 15 tys. zł; maksymalnie równowartość 7 mln euro lub 1,4% przychodów
Kwalifikowane przypadki	Kara może sięgać 100 mln zł
Kierownik podmiotu (np. prezes, zarząd spółki, dyrektor)	W określonych przypadkach do 300% otrzymywanego wynagrodzenia
Kierownik podmiotu publicznego (np. starosta, wójt, prezydent miasta, naczelnik urzędu, dyrektor)	Co do zasady do 100% wynagrodzenia

ŹRÓDŁO: Opracowanie własne NASK – PIB.

Przy ustalaniu wysokości kary uwzględnia się okoliczności konkretnego naruszenia, m.in. jego wagę i czas trwania, skutki, wcześniejsze naruszenia oraz działania podjęte w celu ograniczenia szkód i usunięcia nieprawidłowości.

→ WAŻNE

Kary pieniężne przewidziane w znowelizowanych przepisach KSC 2.0 mogą być po raz pierwszy nakładane po upływie dwóch lat od wejścia w życie nowelizacji, czyli od 3 kwietnia 2028 r.

Nie dotyczy to szczególnych naruszeń, które powodują poważne zagrożenie dla bezpieczeństwa, życia lub zdrowia ludzi albo ryzyko poważnych szkód lub zakłóceń w świadczeniu usług – w takich przypadkach kara może wynieść do 100 mln zł (art. 73 ust. 5 ustawy KSC 2.0).

Nie tylko kara – konsekwencje dla organizacji

Kara pieniężna to tylko jedna z możliwych konsekwencji. Incydent cyberbezpieczeństwa może bezpośrednio wpłynąć na działalność organizacji, jej finanse i reputację.

Konsekwencje dla organizacji

KONSEKWENCJE BIZNESOWE

- przestój w świadczeniu usług lub produkcji
- utrata lub niedostępność danych
- koszty przywracania systemów
- opóźnienia w realizacji umów
- utrata przychodów

KONSEKWENCJE WIZERUNKOWE

- utrata zaufania klientów
- pogorszenie relacji z partnerami
- negatywne publikacje medialne
- spadek wiarygodności organizacji
- osłabienie pozycji organizacji na rynku

Skutki incydentu mogą być odczuwalne jeszcze długo po przywróceniu działania systemów. Jedno zdarzenie może również uruchomić obowiązki wynikające z kilku regulacji jednocześnie – np. KSC 2.0, przepisów dotyczących ochrony danych osobowych czy regulacji sektorowych.

KSC 2.0 to znacznie więcej niż zbiór obowiązków i potencjalnych kar. Dobrze wdrożone wymagania przekładają się na większą odporność organizacji na cyberataki, szybsze reagowanie w sytuacjach kryzysowych oraz lepszą ochronę tego, co dla każdej organizacji najcenniejsze: ciągłości działania, zaufania klientów i reputacji.

Twoja droga do cyberbezpieczeństwa

ZACZNIJ TUTAJ

01 SPRAWDŹ SWÓJ STATUS

Ustal, czy KSC dotyczy Twojej organizacji.

02 DOPEŁNIJ FORMALNOŚCI

Dokonaj/uzupełnij wpis do Wykazu KSC, pamiętaj o terminach.

START DZIAŁAŃ

03 ZARZĄDZANIE CYBERBEZPIECZEŃSTWEM

Inwentaryzacja | szacowanie ryzyka | odpowiedzialność

Poznaj zasoby, ustal priorytety, zasady i plan działania.

04 BUDOWANIE CYBERŚWIADOMOŚCI I ZARZĄDZANIE WIEDZĄ

Kompetencje | szkolenia | cyberhigiena

Rozwijaj kompetencje pracowników i zadbaj o ich szkolenia.

05 OCHRONA SYSTEMÓW I INFORMACJI

Zabezpieczenia | dostęp | ochrona danych

Chroń systemy i informacje przed zagrożeniami oraz nieuprawnionym dostępem.

06 BEZPIECZEŃSTWO USŁUG I DOSTAWCÓW ZEWNĘTRZNYCH

Dostawcy | usługi | ryzyko

Oceniaj ryzyko współpracy z dostawcami i dbaj o bezpieczeństwo usług zewnętrznych.

07 REAGOWANIE I ODPORNOŚĆ ORGANIZACJI

Monitoring | ciągłość działania

Przygotuj organizację na incydenty i ograniczaj ich skutki.

08 ZGŁASZANIE INCYDENTÓW

Zgłaszanie | raportowanie | współpraca z CSIRT

Rozpoznawaj incydenty i zgłaszaj je zgodnie z wymaganiami ustawy.

09 NADZÓR I DOSKONALENIE

Audyty | wnioski | usprawnienia

Regularnie oceniaj skuteczność działań i wprowadzaj usprawnienia.

Cyberbezpieczeństwo to proces ciągły

Skuteczne działania to ciągłe doskonalenie

01 PLANUJ

Określ zasoby, oceń ryzyka i zaplanuj działania

02 DZIAŁAJ

Wdrażaj zaplanowane zabezpieczenia i procedury

03 SPRAWDZAJ

Monitoruje, analizuj i oceniaj skuteczność działań

04 DOSKONAL

Wyciągaj wnioski i wprowadzaj udoskonalenia

KSC 2.0 w praktyce. Słowniczek najważniejszych pojęć

B

Bezpieczeństwo systemów informacyjnych – odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy.

C

CSIRT – Computer Security Incident Response Team. Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego. Zespół odpowiedzialny m.in. za przyjmowanie zgłoszeń dotyczących incydentów, ich analizę, reagowanie na zagrożenia oraz wspieranie podmiotów w obsłudze incydentów. W Polsce wyróżniamy trzy CSIRT-y poziomu krajowego.

- **CSIRT GOV** – prowadzony przez Szefa Agencji Bezpieczeństwa Wewnętrznego i realizuje zadania określone w KSC 2.0 wobec podmiotów pozostających w zakresie jego właściwości.

- **CSIRT MON** –prowadzony przez Ministra Obrony Narodowej i realizuje zadania określone w KSC 2.0 wobec podmiotów pozostających w zakresie jego właściwości, w szczególności związanych z obronnością i Siłami Zbrojnymi RP.

- **CSIRT NASK** – prowadzony przez NASK – Państwowy Instytut Badawczy i realizuje zadania określone w KSC 2.0 wobec podmiotów pozostających w zakresie jego właściwości. Przyjmuje i analizuje zgłoszenia incydentów oraz prowadzi działania związane z reagowaniem na cyberzagrożenia.

CSIRT sektorowy – zespół reagowania na incydenty bezpieczeństwa komputerowego działający w określonym sektorze lub podsektorze. Jest ustanawiany przez właściwy organ ds. cyberbezpieczeństwa w celu zapewnienia wsparcia podmiotom kluczowym i podmiotom ważnym funkcjonującym w danym sektorze lub podsektorze.

Cyberbezpieczeństwo – działania niezbędne do ochrony sieci i systemów informatycznych, użytkowników takich systemów oraz innych osób przed cyberzagrożeniami.

Cyberhigiena – podstawowe, regularnie stosowane działania i dobre praktyki pomagające zwiększać cyberbezpieczeństwo. Obejmuje m.in. aktualizowanie oprogramowania, stosowanie bezpiecznych metod

uwierzytelniania, wykonywanie kopii zapasowych oraz ostrożność podczas korzystania z poczty elektronicznej, stron internetowych i innych usług cyfrowych.

I

Incydent – zdarzenie, które ma lub może mieć niekorzystny wpływ na bezpieczeństwo systemów informacyjnych.

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.

Incydent poważny – incydent, który powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi, straty finansowe lub wpływa na inne osoby lub podmioty przez wywołanie poważnej szkody materialnej lub niematerialnej. O tym, kiedy incydent będzie kwalifikowany jako poważny, będą decydować szczegółowe progi określone w rozporządzeniu Rady Ministrów.

K

Krajowy System Cyberbezpieczeństwa (KSC) – system obejmujący podmioty, organy i instytucje realizujące zadania związane z zapewnieniem cyberbezpieczeństwa w Polsce. Ustawa o krajowym systemie cyberbezpieczeństwa określa m.in. obowiązki podmiotów objętych regulacją, zasady zarządzania ryzykiem, obsługi i zgłaszania incydentów oraz współpracy z właściwymi organami i CSIRT poziomu krajowego.

M

MFA (Multi-Factor Authentication) uwierzytelnianie wieloskładnikowe – metoda logowania wymagająca wykorzystania co najmniej dwóch różnych elementów potwierdzających tożsamość użytkownika, np. hasła i kodu jednorazowego lub hasła i potwierdzenia w aplikacji.

N

NIS2 – dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 ustanawiająca wspólne dla państw UE wymagania w zakresie cyberbezpieczeństwa. Wprowadza m.in. obowiązki dotyczące zarządzania ryzykiem w cyberbezpieczeństwie, zgłaszania incydentów oraz nadzoru nad podmiotami objętymi regulacją. Jej wymagania zostały wdrożone do polskiego prawa poprzez zmiany w ustawie o krajowym systemie cyberbezpieczeństwa.

O

Organ właściwy do spraw cyberbezpieczeństwa – organ administracji publicznej odpowiedzialny za realizację określonych w KSC 2.0 zadań wobec podmiotów z danego sektora lub podsektora. Sprawuje m.in. nadzór nad wykonywaniem obowiązków wynikających z ustawy oraz może prowadzić działania kontrolne.

P

Phishing – rodzaj oszustwa, w którym sprawca podszywa się pod zaufaną osobę, firmę lub instytucję, aby skłonić odbiorcę do określonego działania, np. podania danych logowania, wykonania płatności, kliknięcia w link lub otwarcia albo otwarcia niebezpiecznego załącznika.

Phishing może być prowadzony m.in. za pomocą wiadomości e-mail, SMS-ów, komunikatorów czy fałszywych stron internetowych.

Polska Klasyfikacja Działalności (PKD) – uporządkowane pogrupowanie typów działalności gospodarczej, branż czy sektorów, służące do określenia prowadzonej działalności określone w rozporządzeniu. PKD jest stosowana w statystyce publicznej, ewidencji oraz rachunkowości. Każdy przedsiębiorca powinien w niej odnaleźć kod, najlepiej opisujący jego działalność.

S

System S46 – centralny system teleinformatyczny wykorzystywany do realizacji zadań w ramach krajowego systemu cyberbezpieczeństwa. Służy m.in. do komunikacji pomiędzy podmiotami KSC 2.0, przekazywania informacji dotyczących incydentów oraz obsługi Wykazu KSC.

Samoidentyfikacja – samodzielna ocena czy organizacja podlega pod KSC 2.0 i czy kwalifikuje się jako podmiot kluczowy lub ważny. Polega na analizie prowadzonej działalności oraz sprawdzeniu kryteriów określonych w ustawie.

Samorejestracja (samodzielny wpis do Wykazu KSC) – kierownik podmiotu lub osoba przez niego upoważniona składa wniosek o wpis do wykazu – w terminie 6 miesięcy od spełnienia przesłanek uznania za podmiot kluczowy lub podmiot ważny.

System Zarządzania Bezpieczeństwem Informacji (SZBI) – zorganizowany system zarządzania obejmujący m.in. zasady, procesy, procedury, role i zabezpieczenia służące ochronie informacji oraz zarządzaniu związanym z nimi ryzykiem. Jego celem jest zapewnienie odpowiedniego poziomu poufności, integralności i dostępności informacji.

U

Urzędnik monitorujący – osoba wyznaczona przez organ właściwy do spraw cyberbezpieczeństwa do monitorowania wykonywania obowiązków przez podmiot kluczowy. Może nadzorować realizację zaleceń i działań naprawczych oraz informować organ o postępach w usuwaniu stwierdzonych nieprawidłowości. Mechanizm ten został wprowadzony w ramach nowelizacji ustawy KSC 2.0 wdrażającej dyrektywę NIS2.

W

Wykaz KSC – wykaz podmiotów kluczowych i podmiotów ważnych prowadzony przez ministra właściwego do spraw informatyzacji z wykorzystaniem Systemu S46. Zawiera informacje o podmiotach kluczowych i ważnych objętych obowiązkami wynikającymi z KSC 2.0.

Baza wiedzy i źródła rekomendowane

Akty prawne i interpretacje prawne

1. **Cyber.gov.pl**
   Oficjalny portal państwowy poświęcony cyberbezpieczeństwu i KSC 2.0.

2. **FAQ KSC**
   Najczęściej zadawane pytania i odpowiedzi dotyczące obowiązków wynikających z KSC 2.0.

3. **Nowelizacja ustawy o KSC 2.0**
   Omówienie zmian wynikających z wdrożenia dyrektywy NIS2.

4. **Obowiązki podmiotów kluczowych i ważnych**
   Praktyczny przewodnik po wymaganiach i terminach wdrożenia KSC 2.0.

5. **Samorejestracja w Wykazie KSC**
   Instrukcja samodzielnego wpisu do Wykazu KSC.

6. **System S46 i Wykaz KSC**
   Informacje o rejestracji podmiotów i korzystaniu z Systemu S46.

7. **System S46 – dostęp**
   Instrukcja dostępu do Systemu S46.

8. **Rekomendacje**
   Wykaz Rekomendacji Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa wydanych na podstawie art. 33 i 67a ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

9. **Rozporządzenie wykonawcze Komisji (UE) 2024/2690**
   Rozporządzenie wykonawcze Komisji (UE) 2024/2690 z dnia 17 października 2024 r. ustanawiające zasady stosowania dyrektywy (UE) 2022/2555 w odniesieniu do wymogów technicznych i metodycznych dotyczących środków zarządzania ryzykiem w cyberbezpieczeństwie oraz doprecyzowujące przypadki, w których incydent uznaje się za poważny w odniesieniu do dostawców usług DNS, rejestrów nazw TLD, dostawców usług chmurowych, dostawców usług ośrodka przetwarzania danych, dostawców sieci dostarczania treści, dostawców

usług zarządzanych, dostawców usług zarządzanych w zakresie bezpieczeństwa, dostawców internetowych platform handlowych, wyszukiwarek internetowych i platform usług sieci społecznościowych oraz dostawców usług zaufania (Dz. U. UE. L. z 2024 r. poz. 2690, z późn. zm.).

10. **Ustawa o krajowym systemie cyberbezpieczeństwa (KSC 2.0)**
Podstawowy akt prawny regulujący wymagania cyberbezpieczeństwa w Polsce oraz wdrażający dyrektywę NIS2.

11. **Załącznik I do rozporządzenia Komisji (UE) nr 651/2014**
Art. 2 ust. 1 załącznika I do rozporządzenia Komisji (UE) nr 651/2014 z dnia 17 czerwca 2014 r. uznającego niektóre rodzaje pomocy za zgodne z rynkiem wewnętrznym w zastosowaniu art. 107 i 108 Traktatu (Dz. Urz. UE L 187 z 26.06.2014, str. 1, z późn. zm.).

Materiały edukacyjne i narzędzia

1. **Bezpieczny Miesiąc (ECSM Polska)**
Materiały edukacyjne i kampanie budujące świadomość cyberbezpieczeństwa.

2. **Biznes.gov.pl – NIS2 i KSC 2.0 dla przedsiębiorców**
Praktyczne informacje dla przedsiębiorców dotyczące obowiązków wynikających z NIS2 i KSC 2.0.

3. **CERT Polska**
Ostrzeżenia, raporty o incydentach i rekomendacje bezpieczeństwa.

4. **Firma Bezpieczna Cyfrowo**
Program NASK wspierający organizacje w podnoszeniu poziomu cyberbezpieczeństwa i certyfikacji.

   Poradnik Firma Bezpieczna Cyfrowo.

   Certyfikacja https://certyfikacja.nask.pl/firma-bezpieczna-cyfrowo/.

5. **moje.cert.pl**
Bezpłatne narzędzie do monitorowania domen i wykrywania podatności.

6. **Informacje o działaniach CSIRT NASK, edukacji i cyberbezpieczeństwie**

7. **Samoidentyfikacja – materiały pomocnicze**
Praktyczny przewodnik dotyczący ustalania statusu podmiotu kluczowego lub podmiotu ważnego przygotowany przez Ministerstwo Cyfryzacji dostępny na portalu gov.pl.

8. **Sprzęt firmowy pod kontrolą – 12 filarów bezpieczeństwa**
   Praktyczny poradnik dotyczący bezpiecznego korzystania z urządzeń służbowych i podstawowych zasad cyberhigieny w organizacji.

9. **Szkolenia dla podmiotów krajowego systemu cyberbezpieczeństwa, organizowane przez Departament Cybrbepbezpieczenstwa Ministerstwa Cyfryzacji.**

10. **Szkolenie e-learning**
    Bezpłatne szkolenie instruktażowe nt. Jak dokonać wpisu do Wykazu KSC? dostępne na platformie e-learningowej, które krok po kroku wyjaśnia proces wpisu do Wykazu KSC. Wymaga zalogowania do platformy e-learningowej.

11. **wiedza.cert.pl**
    Baza wiedzy CERT Polska. Zawiera praktyczne materiały, procedury i narzędzia z zakresu cyberbezpieczeństwa tworzone przez zespół CERT Polska działający w ramach NASK – PIB.

12. **Zgłaszanie incydentów za pośrednictwem Systemu S46 – instrukcja**

Materiały eksperckie i standardy

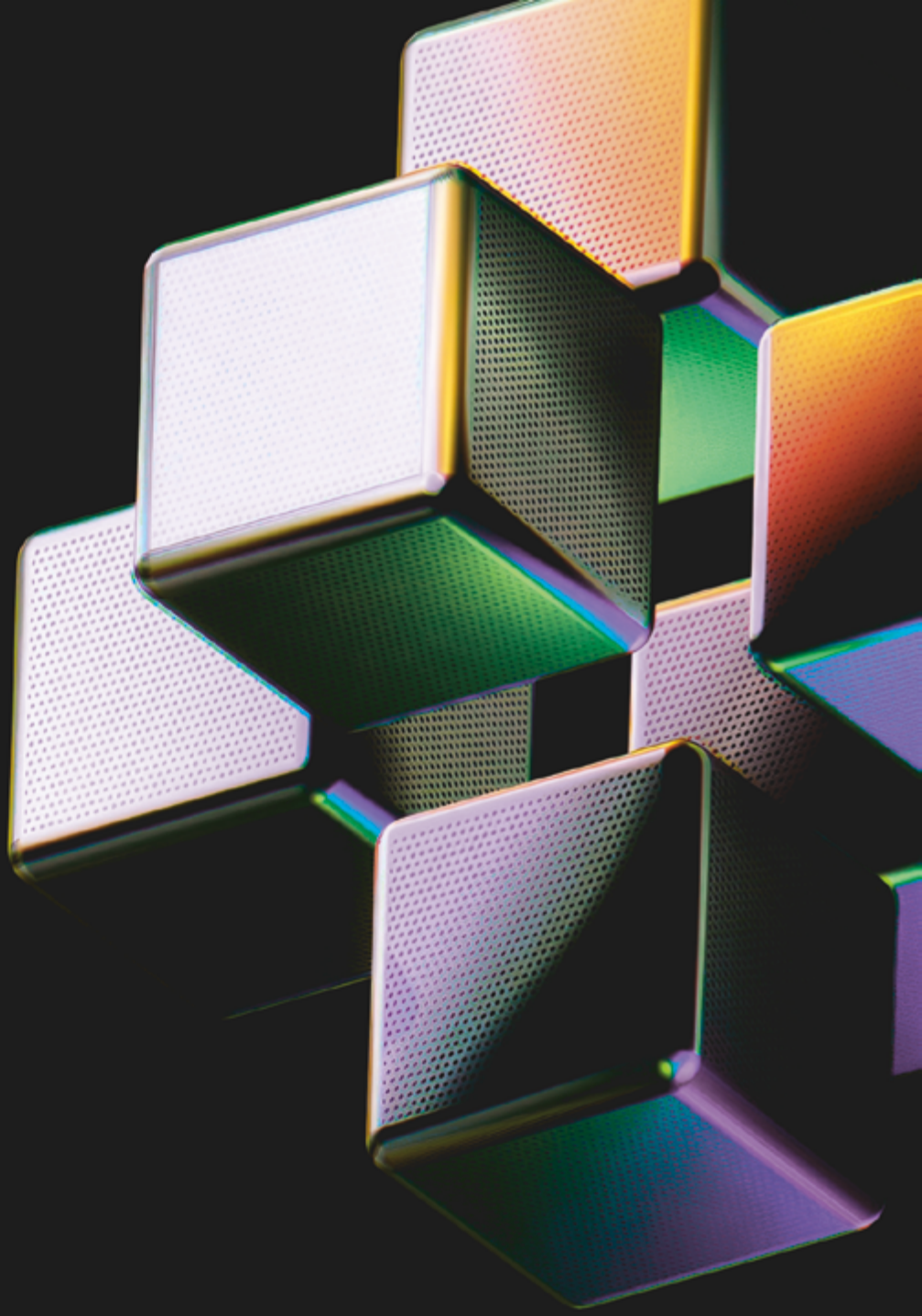
1. **Applied Cybersecurity & Internet Governance (ACIG)**
   Międzynarodowe czasopismo naukowe NASK – PIB publikujące artykuły i analizy dotyczące cyberbezpieczeństwa, odporności cyfrowej, sztucznej inteligencji i zarządzania internetem.

2. **CyberPolicy NASK**
   Analizy, komentarze i opracowania dotyczące cyberbezpieczeństwa, regulacji oraz nowych technologii.

3. **ISO/IEC 27001**
   Międzynarodowy standard określający wymagania dla Systemu Zarządzania Bezpieczeństwem Informacji (SZBI).

4. **NIST Cybersecurity Framework (CSF)**
   Popularny model wspierający zarządzanie cyberbezpieczeństwem i cyberodpornością organizacji.

5. **Poradnik ENISA dotyczący bezpieczeństwa łańcucha dostaw w kontekście NIS2**



NASK