

Dyrektywa NIS2

Nowelizacja ustawy o KSC

Podmioty kluczowe i ważne



MGR INŻ.

MICHAŁ ŁONIEWSKI

Kierownik Wydziału
Rozwoju Technicznego
Przewodniczący Zespołu
Zadaniowego
ds. Cyberbezpieczeństwa
Departament
Innowacji i Rozwoju
Urząd Dozoru Technicznego

Dyrektywa NIS2

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (NIS), czyli **DYREKTYWA NIS2 2022/2555** została opublikowana w Dzienniku Urzędowym UE L333/80 z 27 grudnia 2022 r. Co ważne, wraz z publikacją NIS2 w tym samym Dz. Urz. UE opublikowana została również **DYREKTYWA CER 2022/2557 – dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE.**

Dyrektywa NIS2 wraz z dyrektywą CER tworzą spójne i zharmonizowane ramy prawne w zakresie zapewniania ciągłości świadczenia usług kluczowych dla państwa, kreując przy tym odporność podmiotów świadczących te usługi na zagrożenia fizyczne i incydenty cyberbezpieczeństwa. Z uwagi na powiązanie między bezpieczeństwem fizycznym a cyberbezpieczeństwem podmiotów krytycznych obydwie akty prawne wzajemnie się uzupełniają, przy czym dyrektywy CER nie stosuje się do kwestii objętych dyrektywą NIS2.

Dyrektywy weszły w życie 16 stycznia 2023 r., a państwa członkowskie zostały zobowiązane do implementacji wymagań unijnych do prawa krajowego do 17 października 2024 r. Przedmiotem dalszych rozważań będzie dyrektywa NIS2 oraz nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa wdrażająca wymagania NIS2 do prawa polskiego.

Celem nadrzędnym dyrektywy NIS2 jest osiągnięcie wspólnego wysokiego poziomu cyberbezpieczeństwa w całej Unii, zmierzającego do poprawy funkcjonowania rynku wewnętrznego.

Dążąc do realizacji powyższych zapisów, dyrektywa określa:

- obowiązki państw członkowskich, które dotyczą:
 - przyjęcia krajowych strategii cyberbezpieczeństwa,
 - wyznaczenia lub powołania właściwych organów, organów ds. zarządzania kryzysowego w cyberbezpieczeństwie, pojedynczych punktów kontaktowych ds. cyberbezpieczeństwa (pojedyncze punkty kontaktowe) oraz zespołów reagowania na incydenty bezpieczeństwa komputerowego (ang. Computer Security Incident Response Team – CSIRT);
- **środki zarządzania ryzykiem w cyberbezpieczeństwie oraz obowiązki w zakresie zgłaszania incydentów**, które spoczywają na podmiotach w rodzaju tych, o których mowa w załączniku I lub II dyrektywy (podmioty kluczowe lub ważne), jak również na podmiotach zidentyfikowanych jako podmioty o charakterze krytycznym na podstawie dyrektywy CER 2022/2557;
 - zasady i obowiązki w zakresie wymiany informacji o cyberbezpieczeństwie;
 - obowiązki w zakresie nadzoru i egzekwowania przepisów spoczywające na państwach członkowskich.

Dyrektywa NIS2 rozszerza znacznie zakres pierwszej dyrektywy NIS, zaostrza wymogi w zakresie bezpieczeństwa i sprawozdawczości dla przedsiębiorstw, wprowadza bardziej rygorystyczne środki nadzoru dla organów krajowych i surowsze wymogi w zakresie egzekwowania przepisów oraz poprawia wymianę informacji i współpracę między organami państw członkowskich.

Nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa

Polskim aktem prawnym implementującym dyrektywę NIS2 będzie nowelizacja pierwszej ustawy o krajowym systemie cyberbezpieczeństwa z dnia 5 lipca 2018 r. (Dz. U. z 2024 r. poz. 1077 i 1222), której najnowszy projekt pochodzi z dnia 16 kwietnia 2025 r. (projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw, zwany dalej projektem ustawy o zmianie ustawy o KSC). Według aktualnych informacji z Ministerstwa Cyfryzacji (czerwiec 2025 r.), projekt w wersji z kwietnia 2025 r. będzie aktem powszechnie obowiązującym, a jego publikacji należy spodziewać się w ciągu kilku najbliższych miesięcy. Poniżej najważniejsze zapisy tego projektu.

Krajowy system cyberbezpieczeństwa

Projekt ustawy o zmianie ustawy o KSC w art. 1.1 podaje informacje o podstawowym zakresie zagadnień objętych ustawą.

<p>„Art. 1.1 ustawa określa:</p> <ol style="list-style-type: none"> 1) organizację krajowego systemu cyberbezpieczeństwa oraz zadania i obowiązki podmiotów wchodzących w skład tego systemu; 2) sposób sprawowania nadzoru i kontroli w zakresie stosowania przepisów ustawy; 3) zakres Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej; 4) zakres Krajowego planu reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę”. 	<p>Art. 4 natomiast informuje nas o podmiotach tworzących krajowy system cyberbezpieczeństwa i wymienia je w podanej poniżej kolejności (czcionką zieloną zmiany względem ustawy o KSC z 2018 r.).</p> <p>„Krajowy system cyberbezpieczeństwa obejmuje:</p> <ol style="list-style-type: none"> 1) podmioty kluczowe; 2) podmioty ważne; 3) CSIRT MON; 4) CSIRT NASK; 5) CSIRT GOV; 6) CSIRT sektorowe; 7)-16) uchylone; 17) organy właściwe do spraw cyberbezpieczeństwa; 17a) Połączone Centrum Operacyjne Cyberbezpieczeństwa, zwane dalej „PCOC”; 18) Pojedynczy Punkt Kontaktowy do spraw cyberbezpieczeństwa, zwany dalej „Pojedynczym Punktem Kontaktowym”; 19) Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa, zwanego dalej „Pełnomocnikiem”; 20) Kolegium do Spraw Cyberbezpieczeństwa, zwane dalej „Kolegium”.
---	---

Na wszystkie wymienione wyżej podmioty nałożone będą obowiązki oraz konkretne zadania do realizacji, co – wraz ze sprawowaniem nadzoru i kontrolą realizacji tychże zadań – określa organizację krajowego systemu cyberbezpieczeństwa. **Podmioty kluczowe i ważne** występują tutaj w roli podmiotów, w których potencjalny incydent cyberbezpieczeństwa powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi przez te podmioty. Również może powodować straty finansowe dla tych podmiotów lub wpływać na inne osoby fizyczne, osoby prawne, jednostki organizacyjne (nieposiadające osobowości prawnej) poprzez wywołanie poważnej szkody materialnej lub niematerialnej (tzw. **incydent poważny**).

Podstawowa różnica między podmiotem kluczowym a podmiotem ważnym wyraża się w kwestiach nadzorczych.

- Wobec podmiotu kluczowego można prowadzić czynności nadzorcze uprzednie *ex ante* (przed faktem) i następcze *ex post* (po fakcie).

- Wobec podmiotu ważnego czynności nadzorcze można prowadzić tylko *ex post* (po fakcie).

Pozostałe obowiązki podmiotów kluczowych i podmiotów ważnych są identyczne z wyjątkiem kwestii obowiązkowych audytów, o czym będzie mowa w dalszej części artykułu.

Podmioty kluczowe i ważne

Rodzaje podmiotów kluczowych i ważnych precyzują załączniki I i II dyrektywy NIS2, a w prawie krajowym odpowiednio załączniki nr 1 i 2 do projektu ustawy o zmianie ustawy o KSC, podając sektory oraz podsektory, w których realizowane są usługi istotne z punktu widzenia bezpieczeństwa państwa. Sektory oraz podsektory podmiotów kluczowych i ważnych według projektu ustawy przedstawia tabela 1. Podsektory wymieniane są po myślniku.

Tab. 1. Sektory oraz podsektory podmiotów kluczowych i ważnych według projektu ustawy o zmianie ustawy o KSC (czcionka zielona - zmiany w stosunku do ustawy o KSC z 2018 r.) (źródło: Projekt ustawy o zmianie ustawy o KSC z dnia 16 kwietnia 2025 r.)

Sektory i podsektory podmiotów kluczowych	Sektory i podsektory podmiotów ważnych
Energia: – wydobywanie kopalin – energia elektryczna – ciepło – ropa i paliwa – gaz – energetyka jądrowa – wodór	Usługi pocztowe
Transport: – transport lotniczy – transport kolejowy – transport wodny – transport drogowy	Inwestycje energetyki jądrowej
Bankowość i infrastruktura rynków finansowych	Gospodarowanie odpadami: – zbieranie odpadów – transport odpadów – przetwarzanie odpadów, w tym sortowanie, wraz z nadzorem nad wymienionymi działaniami, a także późniejsze postępowanie z miejscami unieszkodliwiania odpadów – działania wykonane w charakterze sprzedawcy odpadów lub pośrednika w obrocie odpadami
Ochrona zdrowia: – udzielanie świadczeń zdrowotnych i zdrowie publiczne – produkcja i dystrybucja substancji czynnych, produktów leczniczych i wyrobów medycznych	Produkcja, wytwarzanie i dystrybucja chemikaliów
Zaopatrzenie w wodę pitną i jej dystrybucja	Produkcja, przetwarzanie i dystrybucja żywności
Zbiorowe odprowadzanie ścieków	Produkcja: – produkcja wyrobów medycznych i wyrobów medycznych do diagnostyki in vitro – produkcja komputerów, wyrobów elektronicznych i optycznych – produkcja urządzeń elektrycznych – produkcja maszyn i urządzeń (gdzie indziej nieklasyfikowana) – produkcja pojazdów samochodowych, przyczep i naczep – produkcja pozostałego sprzętu transportowego
Infrastruktura cyfrowa: – infrastruktura cyfrowa z wyłączeniem komunikacji elektronicznej – komunikacja elektroniczna	Dostawcy usług cyfrowych
Zarządzanie usługami ICT	Badania naukowe
Przestrzeń kosmiczna	Podmioty publiczne (m.in. samorządowe jednostki i zakłady budżetowe, instytucje kultury, spółki prawa handlowego)
Podmioty publiczne (m.in. jednostki sektora finansów publicznych, instytuty badawcze, NBP, BGK, UDT, PAŻP, PCA, UKNF, PAP, Wody Polskie, PFR, NFOŚiGW, wojewódzkie samorządowe jednostki budżetowe)	

Do tej pory operatorzy usług kluczowych (podmioty ustawy o KSC z 2018 r.) byli wyznaczani w drodze decyzji administracyjnej organu właściwego do spraw cyberbezpieczeństwa. Aby ułatwić identyfikację podmiotów kluczowych i podmiotów ważnych, w projekcie ustawy o zmianie ustawy o KSC wprowadzono obowiązek samorejestracji tych podmiotów.

Rejestracja będzie dokonywała się w wykazie podmiotów kluczowych i podmiotów ważnych, który będzie prowadzony przez ministra właściwego do spraw informatyzacji. Podmioty spełniające wymogi dla podmiotów kluczowych i podmiotów ważnych będą zobowiązane do zarejestrowania się w tym wykazie w terminie 3 miesięcy od dnia spełnienia przesłanek uznania za podmiot kluczowy albo podmiot ważny (art. 7c. 1).

Inną formą identyfikacji będzie wpis do wykazu podmiotów i ważnych z urzędu, gdzie zawiadomienie o wpisie doręczy minister właściwy do spraw informatyzacji (art. 7b. 1). Ścieżka ta będzie dotyczyć jednak znacznie mniejszej liczby podmiotów, przede wszystkim tych, które bezpośrednio wskazuje projekt ustawy o zmianie ustawy o KSC.

Obowiązki podmiotów kluczowych i ważnych

Dyrektywa NIS2 odeszła od wdrażania środków zapewniających bezpieczeństwo systemów informacyjnych tylko w zakresie świadczonych usług kluczowych. Podmiot kluczowy lub ważny musi dbać o bezpieczeństwo wszystkich swoich systemów wykorzystywanych do prowadzenia działalności. W związku z powyższym, system zarządzania bezpieczeństwem informacji (SZBI) i ciągłością działania (SZCD) będzie musiał być wdrożony w systemach informacyjnych wykorzystywanych w procesach wpływających na świadczenie usług przez te podmioty.

Podstawowym obowiązkiem podmiotów kluczowych i podmiotów ważnych będzie zatem wdrożenie systemu, o którym mowa w art. 8.1 projektu ustawy o zmianie ustawy o KSC.

„Art. 8. 1. Podmiot kluczowy lub podmiot ważny wdraża system zarządzania bezpieczeństwem informacji (SZBI) w systemie informacyjnym wykorzystywanym w procesach wpływających na świadczenie usługi przez ten podmiot, zapewniający:

- 1) prowadzenie systematycznego szacowania ryzyka wystąpienia incydentu oraz zarządzanie tym ryzykiem;
- 2) wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych, uwzględniających najnowszy stan wiedzy (...), w szczególności:
 - a) polityki szacowania ryzyka oraz bezpieczeństwa systemu informacyjnego (...),
 - b) bezpieczeństwo w procesie nabywania, rozwoju, utrzymania i eksploatacji systemu informacyjnego, w tym testowanie systemu informacyjnego,
 - c) bezpieczeństwo fizyczne i środowiskowe uwzględniające kontrole dostępu,
 - d) bezpieczeństwo zasobów ludzkich,
 - e) bezpieczeństwo i ciągłość łańcucha dostaw produktów ICT, usług ICT i procesów ICT, od których zależy świadczenie usługi (...),
 - f) wdrażanie, dokumentowanie, testowanie i utrzymywanie planów ciągłości działania umożliwiających ciągłe i niezakłócone świadczenie usługi (...),
 - g) objęcie systemu informacyjnego wykorzystywanego do świadczenia usługi systemem monitorowania w trybie ciągłym,
 - h) polityki i procedury oceny skuteczności środków technicznych i organizacyjnych,
 - i) edukację z zakresu cyberbezpieczeństwa dla personelu podmiotu,
 - j) podstawowe zasady cyberhigieny,
 - k) polityki i procedury stosowania kryptografii, w tym w stosownych przypadkach szyfrowania,
 - l) stosowanie bezpiecznych środków komunikacji elektronicznej w ramach krajowego systemu cyberbezpieczeństwa oraz wewnątrz podmiotu, uwzględniających uwierzytelnianie wieloskładnikowe w stosownych przypadkach,
 - m) zarządzanie aktywami,
 - n) polityki kontroli dostępu;
- 3) zbieranie informacji o cyberzagrożeniach i podatnościach na incydenty systemu informacyjnego wykorzystywanego do świadczenia usługi;
- 4) zarządzanie incydentami;
- 5) stosowanie środków zapobiegających i ograniczających wpływ incydentów na bezpieczeństwo systemu informacyjnego wykorzystywanego do świadczenia usługi, w tym:
 - a) stosowanie mechanizmów zapewniających poufność, integralność, dostępność i autentyczność danych przetwarzanych w systemie informacyjnym,
 - b) regularne przeprowadzanie aktualizacji oprogramowania (...),
 - c) ochronę przed nieuprawnioną modyfikacją w systemie informacyjnym,
 - d) niezwłoczne podejmowanie działań po dostrzeżeniu podatności lub cyberzagrożeń (...).”

Innymi obowiązkami będą ponadto (art. 9.1):

- wyznaczenie co najmniej dwóch osób odpowiedzialnych za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa (wyjątek stanowią mikro- i małe przedsiębiorstwa będące podmiotami kluczowymi i ważnymi oraz podmioty publiczne będące podmiotami ważnymi – te wyznaczają co najmniej jedną osobę),
- zapewnienie użytkownikowi usługi dostępu do wiedzy pozwalającej na zrozumienie cyberzagrożeń i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami w zakresie związanym ze świadczonymi usługami, w szczególności przez udostępnianie informacji na ten temat na swojej stronie internetowej,
- zapewnienie użytkownikowi usługi możliwości zgłoszenia cyberzagrożenia, incydentu lub podatności związanych ze świadczoną usługą,
- korzystanie z systemu teleinformatycznego, o którym mowa w art. 46 ust. 1 (**system S46** – system teleinformatyczny rozwijany lub utrzymywany przez ministra właściwego ds. informatyzacji, służący także do prowadzenia wykazu podmiotów kluczowych i ważnych, realizacji zadań ustawowych zespołów reagowania CSIRT i organów właściwych, zgłaszania i obsługi incydentów, szacowania ryzyka na poziomie krajowym, ostrzegania o cyberzagrożeniach).

Ważnym obowiązkiem będzie również prowadzenie dokumentacji dotyczącej bezpieczeństwa systemu informacyjnego wykorzystywanego w procesie świadczenia usługi, na którą składają się dokumentacja normatywna i operacyjna (art. 10.1-10.4), co szczegółowo przedstawia tabela 2.

Tab. 2. Dokumentacja bezpieczeństwa systemu informacyjnego podmiotów kluczowych i ważnych (źródło: Uzasadnienie do projektu ustawy o zmianie ustawy o KSC z dnia 16 kwietnia 2025 r.)

Dokumentacja normatywna
Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)
Dokumentacja ochrony infrastruktury, z wykorzystaniem której świadczona jest usługa
Dokumentacja Systemu Zarządzania Ciągłością Działania (SZCD)
Dokumentacja techniczna systemu informacyjnego wykorzystywanego w procesie świadczenia usługi
Dokumentacja wynikająca ze specyfiki świadczonej usługi w danym sektorze/podsektorze
Dokumentacja operacyjna
Zapisy poświadczające wykonywanie czynności wymaganych przez postanowienia zawarte w dokumentacji normatywnej, w tym automatycznie generowane zapisy w dziennikach systemów informacyjnych (logi)

Kolejnym bardzo istotnym obowiązkiem podmiotów kluczowych i ważnych jest obsługa incydentu. W pierwszej kolejności podmiot kluczowy i podmiot ważny zobowiązani będą do zgłoszenia wczesnego ostrzeżenia o incydencie poważnym – niezwłocznie, nie później niż w ciągu 24 godzin od momentu wykrycia incydentu poważnego. Natomiast w ciągu 72 godzin podmiot kluczowy i podmiot ważny zgłaszają incydent poważny wraz z dodatkowymi informacjami o tym incydencie, m.in. opis wpływu incydentu na świadczone usługi, opis przyczyn incydentu, a także informacje o podjętych działaniach. Progi uznania incydentu za incydent poważny zostaną określone w drodze rozporządzenia przez Radę Ministrów. Zgodnie z proponowanymi rozwiązaniami incydenty poważne zgłaszane będą do CSIRT sektorowego. CSIRT sektorowy zobowiązany będzie do udzielenia wsparcia, zgodnie z treścią wniosku podczas zgłoszenia wczesnego ostrzeżenia, w ciągu 24 godzin. Zgłoszenia wczesnego ostrzeżenia i incydentu poważnego będą dokonywane za pośrednictwem systemu S46. Takie rozwiązanie spowoduje, że informacja o tych zgłoszeniach będzie dostępna dla pozostałych CSIRT, w tym również CSIRT poziomu krajowego.

Obsługa incydentu opisana jest w art. 11.1 projektu ustawy.



„Art. 11.1. Podmiot kluczowy i podmiot ważny:

- 1) zapewnia obsługę incydentu;
- 2) zapewnia dostęp do informacji o rejestrowanych incydentach właściwemu CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT sektorowemu w zakresie niezbędnym do realizacji jego zadań;
- 3) klasyfikuje incydent jako poważny na podstawie progów uznawania incydentu za poważny;
- 4) zgłasza wczesne ostrzeżenie o incydencie poważnym niezwłocznie, nie później niż w ciągu 24 godzin od momentu jego wykrycia, do właściwego CSIRT sektorowego;
- 4a) zgłasza incydent poważny niezwłocznie, nie później niż w ciągu 72 godzin od momentu jego wykrycia, do właściwego CSIRT sektorowego;
- 4b) przekazuje, na wniosek właściwego CSIRT sektorowego, sprawozdanie okresowe z obsługi incydentu poważnego;
- 4c) przekazuje właściwemu CSIRT sektorowemu sprawozdanie końcowe z obsługi incydentu poważnego, nie później niż w ciągu miesiąca od dnia zgłoszenia, o którym mowa w pkt 4a;
- 5) współdziała podczas obsługi incydentu poważnego i incydentu krytycznego z właściwym CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT sektorowym, przekazując niezbędne dane, w tym dane osobowe;
- 6) usuwa podatności, o których mowa w art. 32 ust. 2, oraz informuje o ich usunięciu organ właściwy do spraw cyberbezpieczeństwa”.

W celu realizacji powyższych zadań podmiot kluczowy lub ważny będzie musiał powołać wewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo lub zawrzeć umowę z dostawcą usług zarządzanych w zakresie cyberbezpieczeństwa.

Taki dostawca usług zarządzanych będzie również podlegał obowiązkom niniejszej, projektowanej ustawy jako podmiot kluczowy sektora: zarządzanie usługami ICT.

Podmiot kluczowy lub ważny na wykonanie powyższych obowiązków będzie miał 6 miesięcy od dnia spełnienia przesłanek uznania go za podmiot kluczowy lub podmiot ważny.

Audyty

Podmiot kluczowy będzie miał obowiązek przeprowadzenia, na własny koszt, audytu bezpieczeństwa systemu informacyjnego wykorzystywanego w procesie świadczenia usługi, co najmniej raz na 3 lata. Będzie on mógł być audytem wewnętrznym lub zewnętrznym. Przeprowadzenie audytu po raz pierwszy podmiot będzie musiał zapewnić w terminie 24 miesięcy od dnia spełnienia przesłanek uznania go za podmiot kluczowy.

Organ właściwy do spraw cyberbezpieczeństwa będzie mógł nakazać przeprowadzenie audytu doraźnego przez podmiot kluczowy lub podmiot ważny. Audyt ten będzie audytem zewnętrznym. W stosunku do podmiotów kluczowych będzie on mógł zostać zlecony w każdym czasie. W stosunku do podmiotów ważnych taki audyt będzie mógł zostać zlecony wyłącznie w przypadku wystąpienia incydentu poważnego lub innego naruszenia przepisów ustawy.



Informacje z projektu ustawy o zmianie ustawy o KSC

„Art. 15.2. Audyt może być przeprowadzony przez:

- 1) jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz.U. z 2022 r. poz. 1854) (...);
- 2) co najmniej dwóch audytorów posiadających:
 - a) certyfikaty określone w przepisach wydanych na podstawie ust. 8, lub
 - b) co najmniej trzyletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych, lub
 - c) co najmniej dwuletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych i legitymujących się dyplomem ukończenia studiów podyplomowych w zakresie audytu bezpieczeństwa systemów informacyjnych (...);
- 3) CSIRT sektorowy, ustanowiony w ramach sektora lub podsektora wymienionego w załączniku nr 1 do ustawy, jeżeli audytorzy spełniają warunki, o których mowa w pkt 2”.

Podsumowanie

Musimy pamiętać, że nieprzerwane świadczenie usługi, istotnej z punktu widzenia państwa i obywateli, w przypadku większości podmiotów sektora energii, transportu, produkcji i wody pitnej zależy nie tylko od bezpieczeństwa komputerowych systemów biurowych IT (ang. Information Technology), ale także od bezpieczeństwa przemysłowych sieci i systemów sterowania ICS (ang. Industrial Control Systems), czyli od bezpieczeństwa OT (ang. Operational Technology). Pełna dostępność takich systemów to skoordynowane działania podnoszące poziom bezpieczeństwa w znaczeniu angielskiego „safety”, czyli bezpieczeństwa funkcjonalnego (zagrożenia takie jak przypadkowe awarie sprzętu i oprogramowania, błędy ludzkie) oraz ochrony w znaczeniu „security”, czyli bezpieczeństwa fizycznego i cyberbezpieczeństwa (zagrożenia takie jak nieuprawnione działania i dostęp, sabotaż, zła wola), co wpisuje się w zasadę „No safety without security”.

Urząd Dozoru Technicznego, wychodząc naprzeciw wymaganiom projektowanej ustawy o zmianie ustawy o KSC, opracował Poradnik dobrych praktyk w zakresie cyberbezpieczeństwa urządzeń podlegających dozorowi technicznemu. Poradnik ma za zadanie zapewnić dostęp do wiedzy pozwalającej na zrozumienie cyberzagrożeń przez eksploatujących urządzenia techniczne. Informuje także o skutecznych sposobach zabezpieczania się przed tymi zagrożeniami w zakresie związanym ze świadczonymi usługami. Ponadto w ramach działań wspierających realizację obowiązkowego audytu bezpieczeństwa systemu informacyjnego przez podmioty kluczowe, Urząd Dozoru Technicznego oferuje audyt według metodyki opisanej w dokumencie Framework UDTCyber. Poradnik, jak i metodyka dostępne są bezpłatnie na stronie internetowej urzędu pod adresem: <https://www.udt.gov.pl/cyberbezpieczenstwo>.



Rys. 1. Publikacje UDT w zakresie cyberbezpieczeństwa

Informacje uzupełniające

CSIRT GOV – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym i prowadzony przez Szefa Agencji Bezpieczeństwa Wewnętrznego (infrastruktura krytyczna);

CSIRT MON – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym i prowadzony przez Ministra Obrony Narodowej (infrastruktura wojskowa);

CSIRT NASK – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym i prowadzony przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy (infrastruktura cywilna);

CSIRT sektorowy – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego, działający na poziomie sektora lub podsektora, ustanowiony przez organ właściwy do spraw cyberbezpieczeństwa dla danego sektora lub podsektora (podmiotów kluczowych i ważnych);

Organy właściwe ds. cyberbezpieczeństwa

Organami właściwymi do spraw cyberbezpieczeństwa, na mocy ustawy o zmianie ustawy o KSC, będą:

- Sektor energii – minister właściwy do spraw energii;
- Sektor inwestycji energii jądrowej – minister właściwy do spraw energii;
- Sektor transportu z wyłączeniem podsektora transportu wodnego – minister właściwy do spraw transportu;
- Podsektor transportu wodnego – minister właściwy do spraw gospodarki morskiej i minister właściwy do spraw żeglugi śródlądowej;
- Sektor bankowy i infrastruktury rynków finansowych – Komisja Nadzoru Finansowego;
- Sektor ochrony zdrowia z wyłączeniem podmiotów, o których mowa w art. 26 ust. 5 (podmioty podległe Ministrowi Obrony Narodowej) – minister właściwy do spraw zdrowia;
- Sektor ochrony zdrowia obejmujący podmioty, o których mowa w art. 26 ust. 5 – Minister Obrony Narodowej;
- Sektor zaopatrzenia w wodę pitną i jej dystrybucji – minister właściwy do spraw gospodarki wodnej;
- Sektor infrastruktury cyfrowej z wyłączeniem podmiotów, o których mowa w art. 26 ust. 5 oraz z wyłączeniem podsektora komunikacji elektronicznej – minister właściwy do spraw informatyzacji;
- Podsektor komunikacji elektronicznej z wyłączeniem podmiotów, o których mowa w art. 26 ust. 5 – Prezes Urzędu

Komunikacji Elektronicznej;

- Sektor infrastruktury cyfrowej obejmujący podmioty, o których mowa w art. 26 ust. 5 – Minister Obrony Narodowej;
- Sektor zbiorowego odprowadzania ścieków – minister właściwy do spraw gospodarki wodnej;
- Sektor zarządzania usługami ICT – minister właściwy do spraw informatyzacji;
- Sektor przestrzeni kosmicznej – minister właściwy do spraw gospodarki;
- Sektor produkcji, wytwarzania i dystrybucji chemikaliów – minister właściwy do spraw gospodarki;
- Sektor produkcji, przetwarzania i dystrybucji żywności – minister właściwy do spraw rolnictwa;
- Sektor produkcji, z wyłączeniem podsektora produkcja wyrobów medycznych i wyrobów medycznych do diagnostyki in vitro – minister właściwy do spraw gospodarki;
- Podsektor produkcji wyrobów medycznych i wyrobów medycznych do diagnostyki in vitro – minister właściwy do spraw zdrowia;
- Sektor usług pocztowych – Prezes Urzędu Komunikacji Elektronicznej;
- Sektor gospodarowania odpadami – minister właściwy do spraw klimatu;
- Sektor dostawców usług cyfrowych – minister właściwy do spraw informatyzacji;
- Sektor badań naukowych – minister właściwy do spraw szkolnictwa wyższego i nauki;
- Sektor podmiotów publicznych, z wyłączeniem podmiotów podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych oraz urzędu obsługującego tego ministra – minister właściwy do spraw informatyzacji;
- Sektor podmiotów publicznych dla podmiotów podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych oraz dla urzędu obsługującego tego ministra – Minister Obrony Narodowej;
- Podmiot publiczny, który jest wymieniony w innym sektorze niż sektor podmiotów publicznych – organ właściwy dla danego sektora.

Literatura:

1. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (dyrektywa NIS)
2. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2)
3. Dyrektywa parlamentu europejskiego i rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE (dyrektywa CER)
4. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1077 i 1222)
5. Ustawa o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (projekt z dnia 16 kwietnia 2025 r.)
6. Uzasadnienie do ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (projekt z dnia 16 kwietnia 2025 r.)